Groupe de travail Réseau
Request for Comments : 4861
RFC rendue obsolète : 2461
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

T. Narten, IBM
E. Nordmark, Sun Microsystems
W. Simpson, Daydreamer
H. Soliman, Elevate Technologies
septembre 2007

Découverte de voisin pour IP version 6 (IPv6)

Résumé
Le présent document spécifie le protocole de découverte de voisin pour IP version 6. Les nœuds IPv6 qui sont sur la même liaison utilisent la découverte de voisin pour découvrir la présence les uns des autres, pour déterminer leurs adresses de couche liaison, pour trouver les routeurs et pour l'entretien des informations d'accessibilité sur les chemins vers les voisins actifs.

Table des Matières

1. Introduction
2. Terminologie
2.1 Généralités
2.2 Types de liaison
2.3 Adresses
2.4 Exigences
3. Vue d'ensemble du protocole
3.1 Comparaison avec IPv4
3.2 Types de liaisons pris en charge
3.3 Sécuriser les messages de découverte de voisin
4. Formats de message
4.1 Format du message Sollicitation de routeur
4.2 Format du message Annonce de routeur
4.3 Format du message Sollicitation de voisin
4.4 Format du message Annonce de voisin
4.5 Format du message Redirection
4.6 Formats d'option
4.6.1 Adresse de source/cible de couche liaison
4.6.2 Informations de préfixe
4.6.3 En-tête rédirigé
4.6.4 MTU
5. Modèle conceptuel d'un hôte
5.1 Structures conceptuelles des données
5.2 Algorithme conceptuel d'envoi
5.3 Exigences pour le ramassage des déchets et les fins de temporisation
6. Découverte de routeur et de préfixe
6.1 Validation de message
6.1.1 Validation du message Sollicitation de routeurs
6.1.2 Validation des messages Annonce de routeur
6.2 Spécification du routeur
6.2.1 Variables de configuration de routeur
6.2.2 Devenir une interface d'annonce
6.2.3 Contenu du message Annonce de routeur
6.2.4 Envoi d'annonces de routeur non sollicitées
6.2.5 Cesser d'être une interface d'annonce
6.2.6 Traitement des sollicitations de routeur
6.2.7 Cohérence des annonces de routeur
6.2.8 Changement d'adresse de liaison locale

6.3 Spécification de l'hôte
6.3.1 Variables de configuration d'hôte
6.3.2 Variables d'hôte
6.3.3 Initialisation de l'interface
6.3.4 Traitement des Annonces de routeur reçues
6.3.5 Péremption des préfixes et des routeurs par défaut
6.3.6 Choix du routeur par défaut
6.3.7 Envoi des sollicitations de routeur
7. Résolution d'adresse et détection d'inaccessibilité du voisin
7.1 Validation de message
7.1.1 Validation de Sollicitation de voisins
7.1.2 Validation de Annonce de voisin
7.2 Résolution d'adresse
7.2.1 Initialisation d'interface
7.2.2 Envoi de Sollicitation de voisin
7.2.3 Réception des sollicitations de voisin
7.2.4 Envoi d'Annonce de voisin sollicitée
7.2.5 Réception d'annonce de voisin
7.2.6 Envoi non sollicité d'annonce de voisin
7.2.7 Envoi d'annonce de voisin à la cantonade
7.2.8 Mandataire d'Annonce de voisin
7.3 Détection d'inaccessibilité du voisin
7.3.1 Confirmation d'accessibilité
7.3.2 État des entrées d'antémémoire de voisin
7.3.3 Comportement des nœuds
8. Fonction REDIRECTION
8.1 Validation des messages Redirection
8.2 Spécification du routeur
8.3 Spécification de l'hôte
9. Extensibilité – Traitement des options
10. Constantes du protocole
11 Considérations pour la sécurité
11.1 Analyse des menaces
11.2 Sécuriser les messages de découverte de voisins
12. Considérations liées à la dénumérotation
13. Considérations relatives à l'IANA
14. Références
14.1 Références normatives
14.2 Références pour information
Appendice A Hôtes à rattachements multiples
Appendice B Extensions futures
Appendice C Automate à états pour l'état d'accessibilité
Appendice D Résumé des règles pour IsRouter
Appendice E Questions de mise en œuvre
Déclaration complète de droits de reproduction

1. Introduction

La présente spécification définit le protocole de découverte de voisin (ND, *Neighbor Discovery*) pour le protocole Internet version 6 (IPv6). Les nœuds (hôtes et routeurs) utilisent la découverte de voisin pour déterminer les adresses de couche liaison pour les voisins connus pour résider sur les liaisons rattachées et pour purger rapidement les valeurs en antémémoire qui deviennent invalides. Les hôtes utilisent aussi la découverte de voisin pour trouver les routeurs du voisinage qui sont volontaires pour transmettre les paquets en leur nom. Finalement, les nœuds utilisent le protocole pour garder activement trace des voisins qui sont accessibles et de ceux qui ne le sont pas, et pour détecter les changements d'adresse de couche liaison. Lorsque intervient une défaillance de routeur ou du chemin vers un routeur, un hôte recherche activement des solutions de remplacement pour le fonctionnement.

Sauf spécification contraire (dans un document qui traite du fonctionnement de IP sur un type de liaison particulier) le présent document s'applique à tous les types de liaison. Cependant, parce que ND utilise la diffusion groupée de couche liaison pour certains de ses services, il est possible que sur certains types de liaison (par exemple, les liaisons multi accès sans diffusion (NBMA)) soient spécifiés des protocoles ou mécanismes de remplacement pour mettre en œuvre ces services

(dans le document approprié couvrant le fonctionnement de IP sur un type de liaison particulier). Les services décrits dans le présent document qui ne dépendent pas directement de la diffusion groupée, tels que la redirection, la détermination du prochain bond, la détection d'inaccessibilité du voisin, etc., sont supposés être fournis comme spécifié dans le présent document. Les détails sur la façon d'utiliser ND sur les liaisons NBMA sont traités dans la [RFC2491]. De plus, les [RFC3313] et [RFC3316] discutent de l'utilisation de ce protocole sur certaines liaisons cellulaires, qui sont des exemples de liaisons NBMA.

2. Terminologie

2.1 Généralités

IP Protocole Internet version 6. Les termes IPv4 et IPv6 ne sont utilisés que dans les contextes où ils sont nécessaires pour éviter l'ambiguïté.

ICMP Protocole des messages de contrôle de l'Internet pour le protocole Internet version 6. Les termes ICMPv4 et ICMPv6 ne sont utilisés que dans les contextes où ils sont nécessaires pour éviter l'ambiguïté.

Nœud Appareil qui met en œuvre IP.

Routeur Nœud qui transmet les paquets IP qui ne lui sont pas explicitement adressés.

Hôte Tout nœud qui n'est pas un routeur.

Couche supérieure Couche de protocole immédiatement au dessus de IP. Des exemples sont des protocoles de transport tels que TCP et UDP, des protocoles de contrôle tels que ICMP, des protocoles d'acheminement tels que OSPF, et des protocoles de couche Internet ou inférieure qui sont "tunnelés" sur IP (c'est-à-dire, encapsulés dans IP) tels que l'échange de paquets inter réseau (IPX, *Internetwork Packet Exchange*), AppleTalk, ou IP lui-même.

Liaison Facilité ou support de communication sur lequel les nœuds peuvent communiquer à la couche liaison, c'est-à-dire, à la couche immédiatement en dessous de IP. Des exemples sont les réseaux Ethernets (simples ou pontés), de liaisons PPP, en X.25, en relais de trame, ou en ATM, aussi bien que les "tunnels" de couche Internet (ou supérieure), tels que les tunnels sur IPv4 ou IPv6 lui-même.

Interface Jonction d'un nœud à une liaison.

Voisins Nœuds rattachés à la même liaison.

Adresse Identifiant de couche IP d'une interface ou d'un ensemble d'interfaces.

Adresse d'envoi à la cantonade Identifiant d'un ensemble d'interfaces (appartenant normalement à différents nœuds). Un paquet envoyé à une adresse à la cantonade est livré à une des interfaces identifiées par cette adresse (la "plus proche", selon la mesure de distance du protocole d'acheminement). Voir la [RFC4291].

Noter qu'une adresse d'envoi à la cantonade est syntaxiquement indistingable d'une adresse d'envoi individuel. Donc, les nœuds qui envoient des paquets à des adresses d'envoi à la cantonade ne savent généralement pas qu'ils utilisent une adresse d'envoi à la cantonade. Tout au long du reste de ce document, les références à des adresses d'envoi individuel s'appliquent aussi aux adresses d'envoi à la cantonade dans les cas où le nœud ne sait pas qu'une adresse d'envoi individuel est en fait une adresse d'envoi à la cantonade.

Préfixe Chaîne binaire qui consiste en un certain nombre de bits initiaux d'une adresse.

Adresse de couche liaison Identifiant de couche liaison pour une interface. Par exemple des adresses IEEE 802 pour des liaisons Ethernet et des adresses E.164 pour des liaisons RNIS.

En liaison Adresse qui est allouée à une interface sur une liaison spécifiée. Un nœud considère une adresse comme en liaison si :

- elle est couverte par un des préfixes de la liaison (par exemple, comme indiqué par le fanion en liaison dans l'option d'information de préfixe), ou
- un routeur du voisinage spécifie l'adresse comme cible d'un message Redirectionu
- un message d'annonce de voisin est reçu pour l'adresse (cible), ou

- un message Découverte de voisin est reçu de l'adresse.

Hors liaison Contraire de "en liaison" ; adresse qui n'est allouée à aucune interface sur la liaison spécifiée.

Plus longue correspondance de préfixe Processus de détermination du préfixe qui (s'il en est) dans un ensemble de préfixes couvre une adresse cible. Une adresse cible est couverte par un préfixe si tous les bits dans le préfixe correspondent aux bits les plus à gauche de l'adresse cible. Lorsque plusieurs préfixes couvrent une adresse, le plus long préfixe est celui qui correspond.

Accessibilité C'est le fonctionnement correct ou non du chemin de"transmission" unilatéral vers un voisin. En particulier, que les paquets envoyés à un voisin atteignent la couche IP sur la machine voisine et soient traités correctement par la couche IP receveuse. Pour les routeurs du voisinage, accessibilité signifie que les paquets envoyés par la couche IP d'un nœud sont livrés à la couche IP du routeur, et que le routeur transmet bien sûr les paquets (c'est-à-dire, qu'il soit configuré comme un routeur, pas comme un hôte). Pour les hôtes, accessibilité signifie que les paquets envoyés par la couche IP d'un nœud sont livrés à la couche IP de l'hôte voisin.

Paquet Un en-tête IP plus une charge utile.

MTU de liaison Unité maximum de transmission, c'est-à-dire, la taille maximum de paquet en octets, qui peut être convoyée en une seule fois sur une liaison.

Cible Adresse dont on recherche les informations de résolution d'adresse, ou adresse qui est le nouveau premier bond lors d'une redirection.

Mandataire Routeur qui répond aux messages d'interrogation de découverte de voisin au nom d'un autre nœud. Un routeur qui agit au nom d'un nœud mobile qui s'est déplacé hors liaison pourrait éventuellement agir comme mandataire pour le nœud mobile.

Indication ICMP Destination inaccessible Indication d'erreur retournée à l'envoyeur d'origine d'un paquet qui ne peut pas être livré pour les raisons mentionnées dans la [RFC4443]. Si l'erreur survient sur un nœud autre que le nœud d'origine du paquet, un message d'erreur ICMP est généré. Si l'erreur survient sur le nœud d'origine, une mise en œuvre n'est pas obligée de créer réellement et d'envoyer un paquet d'erreur ICMP à la source, pour autant que l'envoyeur de couche supérieure est notifié par un mécanisme approprié (par exemple, une valeur retournée par un appel de procédure). Noter cependant que dans certains cas une mise en œuvre peut trouver pratique de retourner des erreurs à l'envoyeur en prenant le paquet fautif, en générant un message d'erreur ICMP, et en le livrant (localement) au moyen du programme générique de traitement d'erreurs.

Retard aléatoire Lors de l'envoi de messages, il est parfois nécessaire de retarder une transmission d'une durée aléatoire afin d'empêcher que plusieurs nœuds n'émettent exactement au même instant, ou d'empêcher des transmission périodiques à longue portée de se synchroniser [SYNC]. Lorsque un composant aléatoire est nécessaire, un nœud calcule le retard réel d'une façon telle que le retard calculé forme une valeur aléatoire à distribution uniforme qui tombe entre les valeurs minimum et maximum de retard spécifiées. La mise en œuvre doit veiller à s'assurer que la granularité du composant aléatoire calculé et la résolution du temporisateur utilisées soient toutes deux suffisamment élevées pour garantir que la probabilité que plusieurs nœuds retardent de la même quantité de temps soit faible.

Germe de retard aléatoire Si un générateur de nombres pseudo aléatoires est utilisé pour calculer un composant de retard aléatoire, le générateur devrait être initialisé avec un germe unique avant son utilisation. Noter qu'il n'est pas suffisant d'utiliser comme germe le seul jeton d'interface, car les jetons d'interface ne sont pas toujours uniques. Pour réduire la probabilité que des jetons d'interface en double causent l'utilisation du même germe, celui-ci devrait être calculé à partir de sources d'entrées diverses (par exemple, des composants machine) qui sont vraisemblablement différents même sur des "boîtes" identiques. Par exemple, le germe pourrait être formé en combinant le numéro de série de CPU avec un jeton d'interface. Des informations supplémentaires sur l'aléation et la génération de nombres aléatoires se trouvent dans la [RFC4086].

2.2 Types de liaison

Les couches de liaison différentes ont des propriétés différentes. Celles qui concernent la découverte de voisin sont :

À capacité de diffusion groupée Liaison qui prend d'origine en charge le mécanisme de couche liaison pour l'envoi des

paquets (c'est-à-dire, diffuse) à tous les voisins ou à un sous ensemble de tous les voisins.

Point à point Liaison qui connecte exactement deux interfaces. Une liaison en point à point est supposée avoir une capacité de diffusion groupée et avoir une adresse de liaison locale.

Multi accès sans diffusion (NBMA) Liaison à laquelle plus de deux interfaces peuvent se rattacher, mais qui ne prend pas en charge une forme de diffusion ou de diffusion groupée (par exemple, X.25, ATM, relais de trame, etc.).

Noter que tous les types de liaison (y compris NBMA) sont supposés fournir le service de diffusion groupée pour IP (par exemple, en utilisant des serveurs de diffusion groupée) mais des études complémentaires diront si ND devrait utiliser de telles facilités ou un autre mécanisme pour fournir des services ND équivalents.

Support partagé Liaison qui permet la communication directe parmi un certain nombre de nœuds, mais où les nœuds rattachés sont configurés d'une telle façon qu'ils n'ont pas les informations complètes de préfixe pour toutes les destinations en liaison. C'est-à-dire, au niveau IP, les nœuds sur la même liaison peuvent ne pas savoir qu'ils sont voisins ; par défaut, ils communiquent à travers un routeur. Des exemples sont les grands réseaux de données publics (commutés) tels que SMDS ou le RNIS-HD. On connaît aussi les "grands nuages". Voir [RFC1620].

MTU variable Liaison qui n'a pas une MTU bien définie (par exemple, anneaux à jetons IEEE 802.5). De nombreuses liaisons (par exemple, Ethernet) ont une MTU standard définie par les protocoles de couche liaison ou par les documents spécifiques qui décrivent comment faire fonctionner IP sur la couche liaison.

Accessibilité asymétrique Liaison où l'accessibilité non réfléchie et/ou non transitive fait partie du fonctionnement normal. (Accessibilité non réfléchie signifie que les paquets de A atteignent B mais les paquets de B n'atteignent pas A. Accessibilité non transitive signifie que les paquets de A atteignent B, et les paquets de B atteignent C, mais les paquets de A n'atteignent pas C.) De nombreuses liaisons radio ont ces propriétés.

2.3 Adresses

La découverte de voisin utilise un certain nombre d'adresses différentes définies dans la [RFC4291], y compris :

Adresse de diffusion groupée tous nœuds Adresse de portée de liaison locale pour atteindre tous les nœuds. FF02::1

Adresse de diffusion groupée tous routeurs Adresse de portée de liaison locale pour atteindre tous les routeurs. FF02::2

Adresse de diffusion groupée de nœuds sollicités Adresse de diffusion groupée à portée de liaison locale qui est calculée comme une fonction de l'adresse de la cible sollicitée. La fonction est décrite dans la [RFC4291]. La fonction est choisie de telle sorte que les adresses IP qui diffèrent seulement par les bits de plus fort poids, par exemple, du fait de plusieurs préfixes d'ordre élevé associés à des fournisseurs différents, vont se transposer en la même adresse de nœuds sollicités réduisant par là le nombre d'adresses de diffusion groupée qu'un nœud doit joindre à la couche liaison.

Adresse de liaison locale Adresse d'envoi individuel dont la portée sur la seule liaison peut être utilisée pour atteindre les voisins. Toutes les interfaces sur les routeurs DOIVENT avoir une adresse de liaison locale. Aussi la [RFC4862] exige des interfaces sur les hôtes qu'elles aient une adresse de liaison locale.

Adresse non spécifiée Valeur d'adresse réservée qui indique l'absence d'adresse (par exemple, l'adresse est inconnue). Elle n'est jamais utilisée comme adresse de destination, mais peut être utilisée comme adresse de source si l'envoyeur ne connaît pas (pas encore) sa propre adresse (par exemple, en vérifiant qu'une adresse est inutilisée durant une autoconfiguration d'adresse [RFC4862]). L'adresse non spécifiée a une valeur de 0:0:0:0:0:0:0:0.

Noter que la présente spécification ne se conforme pas de façon stricte aux exigences de cohérence de la [RFC3484] pour les portées des adresses de source et de destination. Il est possible que dans certains cas les hôtes utilisent une adresse de source pour une portée plus large que celle de l'adresse de destination dans l'en-tête IPv6.

2.4 Exigences

Les mots clés DOIT, NE DOIT PAS, EXIGE, DEVRA, NE DEVRA PAS, DEVRAIT, NE DEVRAIT PAS, RECOMMANDE, PEUT, et FACULTATIF, lorsqu'ils apparaissent dans le présent document, sont à interpréter comme décrit dans la [RFC2119].

Le présent document utilise aussi des variables conceptuelles internes pour décrire le comportement de protocole et des variables externes qu'une mise en œuvre doit permettre aux administrateurs de système de changer. Les noms spécifiques des variables, comment leur valeur change, et comment leur réglage influence le comportement du protocole, sont fournis pour montrer le comportement du protocole. Une mise en œuvre n'est pas obligée de les avoir sous la forme exacte décrite ici, pour autant que son comportement externe soit cohérent avec celui décrit dans le présent document.

3. Vue d'ensemble du protocole

Ce protocole résout un ensemble de problèmes relatifs à l'interaction entre les nœuds rattachés à la même liaison. Il définit les mécanismes pour résoudre chacun des problèmes suivants :

Découverte de routeur : comment les hôtes localisent les routeurs qui résident sur une liaison de rattachement.

Découverte de préfixe : comment les hôtes découvrent l'ensemble des préfixes d'adresses qui définissent quelles destinations sont en liaison pour une liaison de rattachement. (Les nœuds utilisent les préfixes pour distinguer les destinations qui résident en liaison de celles qui ne sont accessibles qu'à travers un routeur.)

Découverte de paramètre : comment un nœud apprend des paramètres de la liaison (tels que la MTU de liaison) ou des paramètres Internet (comme la valeur de limite de bonds) à placer dans les paquets sortants.

Autoconfiguration d'adresse : Introduit les mécanismes nécessaires pour permettre aux nœud de configurer une adresse pour une interface de façon sans état. L'autoconfiguration d'adresse sans état est spécifiée dans [RFC4862].

Résolution d'adresse : comment les nœuds déterminent l'adresse de couche liaison d'une destination en liaison (par exemple, un voisin) connaissant seulement l'adresse IP de destination.

Détermination du prochain bond : l'algorithme pour transposer une adresse IP de destination en adresse IP du voisin auquel devrait être envoyé le trafic pour la destination. Le prochain bond peut être un routeur ou la destination elle-même.

Détection d'inaccessibilité du voisin : comment les nœuds déterminent qu'un voisin n'est plus accessible. Pour les voisins utilisés comme routeurs, des routeurs de remplacement par défaut peuvent être essayés. Pour les routeurs et les hôtes, la résolution peut être effectuée à nouveau.

Détection d'adresse dupliquée : comment un nœud détermine qu'une adresse qu'il souhaite utiliser n'est pas déjà utilisée par un autre nœud.

Redirection : comment un routeur informe un hôte d'un meilleur nœud de premier bond pour atteindre une destination particulière.

La découverte de voisin définit cinq types différents de paquet ICMP : une paire de messages Sollicitation de routeur et Annonce de routeur, une paire de messages Sollicitation de voisin et Annonce de voisin, et un message Redirection. Les messages servent aux objets suivants :

Sollicitation de routeur : lorsque une interface devient active, les hôtes peuvent envoyer des sollicitations de routeur qui demandent aux routeurs de générer immédiatement des annonces de routeur plutôt qu'à leur prochaine période programmée.

Annonce de routeur : les routeurs annoncent leur présence ainsi que divers paramètres de liaison et Internet, soit de façon périodique, soit en réponse à un message Sollicitation de routeur. Les annonces de routeur contiennent des préfixes qui sont utilisés pour la détermination de en liaison et/ou la configuration d'adresse, une valeur de limite de bonds suggérée, etc.

Sollicitation de voisin : envoyée par un nœud pour déterminer l'adresse de couche liaison d'un voisin, ou pour vérifier qu'un voisin est encore accessible via une adresse de couche liaison en antémémoire. Les sollicitations de

voisin sont aussi utilisées pour la détection d'adresse dupliquée.

Annonce de voisin : c'est une réponse à un message Sollicitation de voisin. Un nœud peut aussi envoyer des annonces de voisin non sollicitées pour annoncer un changement d'adresse de couche liaison.

Redirection : utilisé par les routeurs pour informer les hôtes d'un meilleur premier bond pour une destination.

Sur les liaisons à capacité de diffusion groupée, chaque routeur envoie périodiquement en diffusion groupée un paquet d'annonce de routeur pour annoncer sa disponibilité. Un hôte reçoit des annonces de routeur de tous les routeurs, et construit une liste des routeurs par défaut. Les routeurs génèrent des annonces de routeur assez fréquemment pour que les hôtes apprennent leur présence en quelques minutes, mais pas assez fréquemment pour s'appuyer sur une absence d'annonce pour détecter une défaillance d'un routeur ; un algorithme distinct Détection d'inaccessibilité du voisin s'occupe de la détection des défaillances.

Le message Annonce de routeur contient une liste des préfixes utilisés pour déterminer les configurations en liaison et/ou d'adresse autonome ; les fanions associés aux préfixes spécifient les utilisations prévues pour un préfixe particulier. Les hôtes utilisent les préfixes en liaison annoncés pour construire et entretenir une liste qui est utilisée pour décider quand la destination d'un paquet est en liaison ou au delà d'un routeur. Noter qu'une destination peut être en liaison même si elle n'est couverte par aucun préfixe en liaison annoncé. Dans un tel cas un routeur peut envoyer une Redirection pour informer l'envoyeur que la destination est un voisin.

Le message Annonce de routeur (et les fanions par préfixe) permettent aux routeurs d'informer les hôtes de la façon d'effectuer l'autoconfiguration d'adresse. Par exemple, les routeurs peuvent spécifier si les hôtes devraient utiliser la configuration d'adresse à état plein (DHCPv6) et/ou autonome (sans état).

Les messages Annonce de routeur contiennent aussi des paramètres Internet tels que la limite de bonds que devraient utiliser les hôtes dans les paquets sortants, et facultativement, les paramètres de liaison tels que la MTU de liaison. Cela facilite l'administration centralisée des paramètres critiques qui peuvent être établis sur les routeurs et propagés automatiquement à tous les hôtes rattachés.

Les nœuds accomplissent la résolution d'adresse en envoyant en diffusion groupée une sollicitation de voisin qui demande au nœud cible de retourner son adresse de couche liaison. Les messages Sollicitation de voisin sont envoyés en diffusion groupée à l'adresse de diffusion groupée de nœud sollicité de l'adresse cible. La cible retourne son adresse de couche liaison dans un message Annonce de voisin en envoi individuel. Une seule paire de paquets demande/réponse est suffisante pour que l'initiateur et la cible résolvent tous deux les adresses de couche liaison l'un de l'autre ; l'initiateur inclut son adresse de couche liaison dans la sollicitation de voisin.

Les messages Sollicitation de voisin peuvent aussi être utilisés pour déterminer si la même adresse d'envoi individuel a été allouée à plus d'un nœud. L'utilisation des messages Sollicitation de voisin pour la détection d'adresse dupliquée est spécifiée dans la [RFC4862].

La détection d'inaccessibilité du voisin détecte la défaillance d'un voisin ou la défaillance du chemin de transmission vers le voisin. Faire ainsi exige une confirmation positive de ce que les paquets envoyés à un voisin atteignent réellement ce voisin et sont traités correctement par sa couche IP. La détection d'inaccessibilité du voisin utilise la confirmation provenant de deux sources. Lorsque c'est possible, les protocoles de couche supérieure fournissent une confirmation positive de ce qu'une connexion fait des "progrès de transmission", c'est-à-dire qu'il est connu que les données envoyées précédemment ont été correctement livrées (par exemple, de nouveaux accusés de réception ont été reçus récemment). Lorsque la confirmation positive n'arrive pas par de telles indications, un nœud envoie des messages Sollicitation de voisin en envoi individuel qui sollicitent des annonces de voisin comme confirmation d'accessibilité de la part du prochain bond. Pour réduire le trafic réseau inutile, les messages de sondage ne sont envoyés qu'aux voisins auxquels le nœud envoie activement des paquets.

En plus du traitement des problèmes généraux ci-dessus, la découverte de voisin traite aussi les situations suivantes :

Changement d'adresse de couche liaison - Un nœud qui sait que son adresse de couche liaison a changé peut envoyer en diffusion groupée quelques paquets Annonce de voisin (non sollicitée) à tous les nœuds pour mettre rapidement à jour les adresses de couche liaison en antémémoire qui sont devenues invalides. Noter que l'envoi d'annonces non sollicitées est seulement une amélioration des performances (par exemple, elles sont non fiables). L'algorithme de détection d'inaccessibilité du voisin assure que tous les nœuds vont fiablement découvrir la nouvelle adresse, bien que le délai puisse être un peu plus long.

Équilibrage de la charge entrante - Les nœuds qui ont des interfaces en double peuvent vouloir équilibrer la charge de réception des paquets entrants entre les diverses interfaces réseau sur la même liaison. De tels nœuds ont

plusieurs adresses de couche liaison allouées à la même interface. Par exemple, un seul pilote réseau pourrait représenter plusieurs cartes d'interface réseau comme une seule interface logique ayant plusieurs adresses de couche liaison.

La découverte de voisin permet à un routeur d'effectuer l'équilibrage de charge du trafic adressé à lui-même en permettant aux routeurs d'omettre l'adresse de couche liaison de source dans les paquets Annonce de routeur, forçant par là les voisins à utiliser les messages Sollicitation de voisin pour apprendre les adresses de couche liaison des routeurs. Les messages Annonce de voisin retournés peuvent alors contenir des adresses de couche liaison qui diffèrent, par exemple, selon celui qui a produit la sollicitation. La présente spécification ne définit pas de mécanisme permettant aux hôtes d'équilibrer la charge des paquets entrants. Voir [RFC4311].

Adresses d'envoi à la cantonade- Les adresses d'envoi à la cantonade identifient un des nœuds d'un ensemble qui fournissent un service équivalent, et plusieurs nœuds sur la même liaison peuvent être configurés pour reconnaître la même adresse d'envoi à la cantonade. La découverte de voisin traite les envois à la cantonade en faisant que les nœuds s'attendent à recevoir plusieurs annonces de voisin pour la même cible. Toutes les annonces pour les adresses d'envoi à la cantonade sont étiquetées comme étant des annonces sans outrepassement. Une annonce sans outrepassement est celle qui ne met pas à jour ni ne remplace les informations envoyées par une autre annonce. Ces annonces sont exposées plus loin dans le contexte des messages d'annonce de voisin. Cela invoque des règles spécifiques pour déterminer quelles annonces devraient être utilisées parmi cet ensemble éventuel.

Annonce de mandataire - Un routeur qui veut accepter des paquets au nom d'une adresse cible et qui n'est pas capable de répondre aux sollicitations de voisin peut produire des annonces de voisin sans outrepassement. Il n'y a pas actuellement d'utilisation de mandataire qui soit spécifiée, mais l'annonce de mandataire pourrait éventuellement être utilisée pour traiter les cas comme ceux de nœuds mobiles qui sont passés hors liaison. Cependant, ce n'est pas prévu comme un mécanisme général pour traiter les nœuds qui, par exemple, ne mettent pas en œuvre ce protocole.

3.1 Comparaison avec IPv4

Le protocole de découverte de voisin IPv6 correspond à une combinaison du protocole de résolution d'adresse IPv4 [RFC3484], du protocole de découverte de routeur ICMP [RFC1256], et de Redirection ICMP [RFC0792]. Dans IPv4, il n'y a pas de protocole ou de mécanisme de détection d'inaccessibilité du voisin d'acceptation générale, bien que le document d'exigences pour les hôtes [RFC1122] spécifie bien quelques algorithmes possibles pour la détection de routeurs morts (un sous-ensemble de ce à quoi s'attaque le problème de la détection d'inaccessibilité du voisin).

Le protocole de découverte de voisins apporte une multitude d'améliorations à l'ensemble des protocoles IPv4 :

La découverte de routeur fait partie de l'ensemble de base du protocole ; il n'est pas nécessaire que les hôtes "tripotent" les protocoles d'acheminement.

Les annonces de routeur portent les adresses de couche liaison ; aucun échange supplémentaire de paquets n'est nécessaire pour résoudre l'adresse de couche liaison du routeur.

Les annonces de routeur portent les préfixes pour une liaison ; il n'est pas nécessaire d'avoir des mécanismes distincts pour configurer le "gabarit de réseau".

Les annonces de routeur permettent l'autoconfiguration d'adresse.

Les routeurs peuvent annoncer une MTU pour que les hôtes l'utilisent sur la liaison, s'assurant que tous les nœuds utilisent la même valeur de MTU sur les liaisons qui n'ont pas de MTU bien définie.

Les diffusions groupées de résolution d'adresse sont "étalées" sur 16 millions (2^24) d'adresses de diffusion groupée, réduisant considérablement les interruptions en rapport avec la résolution d'adresse sur les nœuds autres que la cible. De plus, les machines non IPv6 ne devraient pas être interrompues du tout.

Les redirections contiennent l'adresse de couche liaison du nouveau premier bond ; une résolution d'adresse distincte n'est pas nécessaire à réception d'une redirection.

Plusieurs préfixes peuvent être associés à la même liaison. Par défaut, les hôtes apprennent tous les préfixes en liaison des

annonces de routeur. Cependant, des routeurs peuvent être configurés pour omettre certains préfixes des annonces de routeur, ou tous. Dans un tel cas, les hôtes supposent que les destinations sont hors liaison et envoient le trafic aux routeurs. Un routeur peut alors produire des redirections en tant que de besoin.

À la différence de IPv4, le receveur d'une redirection IPv6 suppose que le nouveau prochain bond est en liaison. Dans IPv4, un hôte ignore les redirections qui spécifient un prochain bond qui n'est pas en liaison conformément au gabarit de réseau de la liaison. Le mécanisme de redirection IPv6 est analogue à la facilité XRedirect spécifiée dans la [RFC1620]. Il est prévu qu'il soit utile sur des liaisons en non diffusion et en support partagé dans lesquelles il n'est pas souhaitable ou pas possible aux nœuds de savoir tous les préfixes pour les destinations en liaison.

La détection d'inaccessibilité du voisin fait partie de la base, améliorant de façon significative la robustesse de la livraison de paquet en présence de routeurs défaillants, partiellement défaillants, ou de liaisons fragmentées et de nœuds qui changent leurs adresses de couche liaison. Par exemple, les nœuds mobiles peuvent passer hors liaison sans perdre la connexité à cause d'antémémoires ARP périmées.

À la différence d'ARP, la découverte de voisin détecte des défaillances de demi liaison (en utilisant la détection d'inaccessibilité du voisin) et évite d'envoyer du trafic aux voisins avec lesquels il n'y a pas de connexité bidirectionnelle.

À la différence de la découverte de routeur dans IPv4, les messages d'annonce de routeur ne contiennent pas un champ de préférence. Le champ de préférence n'est pas nécessaire pour traiter les routeurs de différentes "stabilités" ; la détection d'inaccessibilité du voisin va détecter un routeur mort et passer à un qui fonctionne.

L'utilisation des adresses de liaison locale pour identifier de façon univoque les routeurs (pour les messages Annonce de routeur et Redirection) rend possible aux hôtes de maintenir les associations de routeurs dans le cas de dénumérotation de site pour utiliser de nouveaux préfixes mondiaux.

En réglant la limite de bonds à 255, la découverte de voisin est immunisée contre l'envoi accidentel ou intentionnel de messages ND par des envoyeurs hors liaison. Dans IPv4, les envoyeurs hors liaison peuvent envoyer les deux messages ICMP Redirection et Annonce de routeur.

Placer la résolution d'adresse à la couche ICMP rend le protocole plus indépendant du support que ARP et rend possible l'utilisation des mécanismes génériques d'authentification et de sécurité de couche IP comme approprié.

3.2 Types de liaisons pris en charge

La découverte de voisin accepte des liaisons avec différentes propriétés. En présence de certaines propriétés, seul un sous-ensemble des mécanismes du protocole ND est pleinement spécifié dans le présent document :

Point à point — La découverte de voisin traite de telles liaisons juste comme des liaisons de diffusion groupée. (La diffusion groupée peut être fournie extrêmement simplement sur les liaisons en point à point, et les interfaces peuvent recevoir des adresses de liaison locale.)

Diffusion groupée — La découverte de voisin devrait être mise en œuvre comme décrit dans le présent document.

Multi accès sans diffusion (NBMA) — Redirection, détection d'inaccessibilité du voisin et détermination du prochain bond devraient être mises en œuvre comme décrit dans le présent document. La résolution d'adresse, et le mécanisme de livraison des annonces et sollicitations de routeur sur des liaisons NBMA ne sont pas spécifiés dans le présent document. Noter que si les hôtes acceptent la configuration manuelle d'une liste de routeurs par défaut, les hôtes peuvent acquérir de façon dynamique les adresses de couche liaison pour leurs voisins à partir des messages Redirection.

Support partagé — Le message Redirection est modélisé d'après le message XRedirect de la [RFC1620] afin de simplifier l'utilisation du protocole sur les liaisons à support partagé. La présente spécification ne traite pas des questions de support partagé qui ne se rapportent qu'aux routeurs, telles que :

- Comment les routeurs échangent les informations d'accessibilité sur les liaisons à support partagé.
- Comment un routeur détermine l'adresse de couche liaison d'un hôte, dont il a besoin pour envoyer des messages de redirection pour l'hôte.
- Comment un routeur détermine qu'il est le routeur de premier bond pour un paquet reçu.

Le protocole est extensible (par la définition de nouvelles options) de sorte que d'autres solutions pourraient être possibles à l'avenir.

MTU variable La découverte de voisin permet à tous les routeurs de spécifier une MTU pour la liaison, que tous les nœuds utilisent alors. Tous les nœuds sur une liaison doivent utiliser la même MTU (ou la même unité de réception maximum) afin que la diffusion groupée fonctionne correctement. Autrement, lors d'une diffusion groupée, un envoyeur, qui peut ne pas savoir quels nœuds vont recevoir le paquet, ne pourrait pas déterminer une taille minimum (ou un unité maximum de réception) de paquet que tous les receveurs puissent traiter.

Accessibilité asymétrique La découverte de voisin détecte l'absence d'accessibilité asymétrique ; un nœud évite les chemins pour un voisin avec lequel il n'a pas de connexité symétrique. La détection d'inaccessibilité du voisin va normalement identifier de telles demi liaisons et le nœud s'abstiendra de les utiliser. Le protocole pourra vraisemblablement être étendu à l'avenir pour trouver des chemins viables dans des environnements qui manquent de connexité réflexive et transitive.

3.3 Sécuriser les messages de découverte de voisin

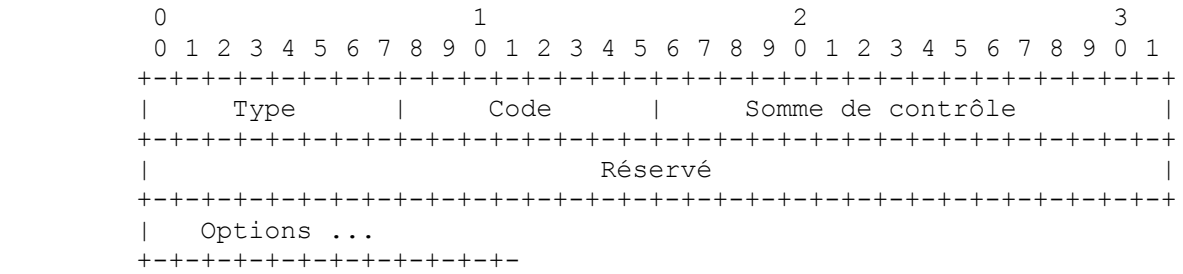
Les messages de découverte de voisin sont nécessaires pour diverses fonctions. Plusieurs fonctions sont conçues pour permettre aux hôtes de s'assurer du propriétaire d'une adresse ou de la transposition entre les adresses de couche de liaison et les adresses de couche IP. Les vulnérabilités qui se rapportent à la découverte de voisin sont exposées au paragraphe 11.1. Une solution générale pour sécuriser la découverte de voisin sortirait du domaine d'application de la présente spécification et est discutée dans la [RFC3971]. Cependant, le paragraphe 11.2 explique comment et sous quelles contraintes l'en-tête d'authentification (AH, *Authentication Header*) IPsec ou l'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) peuvent être utilisés pour sécuriser la découverte de voisin.

4. Formats de message

Cette section introduit les formats de message pour tous les messages utilisés dans cette spécification.

4.1 Format du message Sollicitation de routeur

Les hôtes envoient des Sollicitations de routeur afin de d'inviter les routeurs à générer rapidement des Annonces de routeur.



Champs IP :
Adresse de source : Adresse IP allouée à l'interface d'envoi, ou adresse non spécifiée si aucune adresse n'est allouée à l'interface d'envoi.
Adresse de destination : Normalement l'adresse de diffusion groupée Tous routeurs.
Limite de bonds : 255

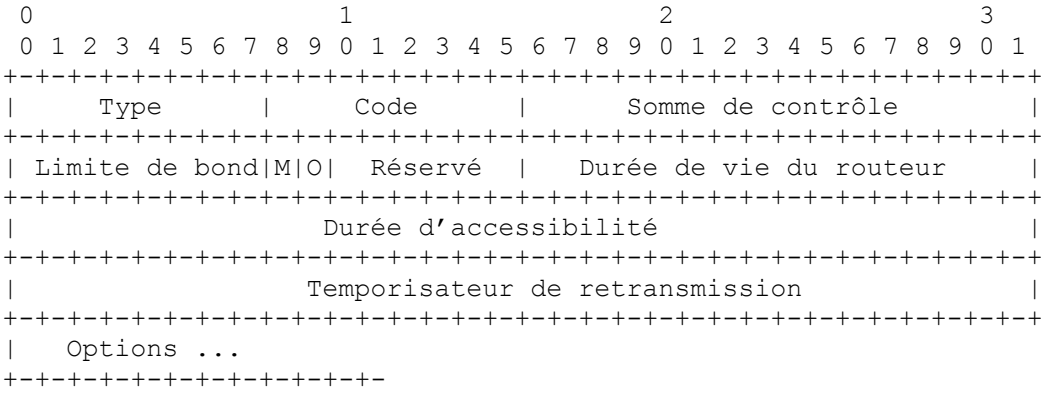
Champs ICMP :
Type : 133
Code : 0
Somme de contrôle : La somme de contrôle ICMP. Voir [RFC4443].
Réservé : Ce champ est inutilisé. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré par le receveur.

Options valides :
Adresse de source de couche liaison
Adresse de couche liaison de l'envoyeur, si elle est connue. NE DOIT PAS être incluse si l'adresse de source est l'adresse non spécifiée. Autrement, elle DEVRAIT être incluse dans les couches liaison qui ont des adresses.

De futures versions de ce protocole pourraient définir de nouveaux types d'option. Les receveurs DOIVENT ignorer en silence toute option qu'ils ne reconnaissent pas et continuer de traiter le message.

4.2 Format du message Annonce de routeur

Les routeurs envoient périodiquement le message Annonce de routeur, ou en réponse à une Sollicitation de routeur.



Champs IP :

Adresse de source : DOIT être l'adresse de liaison locale allouée à l'interface de laquelle ce message est envoyé.

Adresse de destination : Normalement l'adresse de source d'une sollicitation de routeur invoquée ou l'adresse de diffusion groupée Tous les nœuds.

Limite de bonds : 255

Champs ICMP :

Type : 134

Code : 0

Somme de contrôle : La somme de contrôle ICMP. Voir [RFC4443].

Limite de bond actuelle : Entier non signé de 8 bits. Valeur par défaut qui devrait être placée dans le champ Compte de bonds de l'en-tête IP pour les paquets IP sortants. La valeur zéro signifie non spécifié (par ce routeur).

M : Fanion de 1 bit "Configuration d'adresse gérée". Lorsque il est établi, il indique que les adresses sont disponibles via le protocole dynamique de configuration d'hôte [RFC3315].
Si le fanion M est établi, le fanion O est redondant et peut être ignoré parce que DHCPv6 va retourner toutes les informations de configuration disponibles.

O : Fanion de 1 bit "Autre configuration". Lorsque il est établi, il indique que d'autres informations de configuration sont disponibles via DHCPv6. Des exemples de telles informations sont celles qui se rapportent au DNS ou à d'autres serveurs dans le réseau.
Note : Si ni M ni O ne sont établis, cela indique qu'aucune information n'est disponible via DHCPv6.

Réservé : Champ de 6 bits non utilisé. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré par le receveur.

Durée de vie du routeur: Entier non signé de 16 bits. La durée de vie associée au routeur par défaut en secondes. Le champ peut contenir des valeurs allant jusqu'à 65 535 et les receveurs devraient traiter toutes les valeurs, bien que les règles d'envoi de la Section 6 limitent la durée de vie à 9 000 secondes. Une durée de vie de 0 indique que le routeur n'est pas un routeur par défaut et NE DEVRAIT PAS apparaître sur la liste de routeurs par défaut. La durée de vie du routeur ne s'applique qu'à l'utilité du routeur comme routeur par défaut ; elle ne s'applique pas aux informations contenues dans les autres champs ou options du message. Les options qui ont besoin de limites de temps pour leurs informations incluent leur propre champ de durée de vie.

Durée d'accessibilité : Entier non signé de 32 bits. Durée, en millisecondes, pendant laquelle un nœud suppose qu'un voisin est accessible après avoir reçu une confirmation d'accessibilité. Utilisé par l'algorithme Détection d'inaccessibilité du voisin (voir au paragraphe 7.3). La valeur zéro signifie non spécifié (par ce routeur).

Temporisateur de retransmission : Entier non signé de 32 bits. Durée, en millisecondes, entre les messages Sollicitation de voisin retransmis. Utilisé par les algorithmes de résolution d'adresse et de détection d'inaccessibilité du voisin (voir les paragraphes 7.2 et 7.3). La valeur zéro signifie non spécifié (par ce routeur).

Options possibles :

Adresse source de couche liaison

L'adresse de couche liaison de l'interface d'où l'annonce de routeur est envoyée. Seulement utilisé sur les couches de liaison qui ont des adresses. Un routeur PEUT omettre cette option afin de permettre un partage de charge en entrée à travers plusieurs adresses de couche liaison.

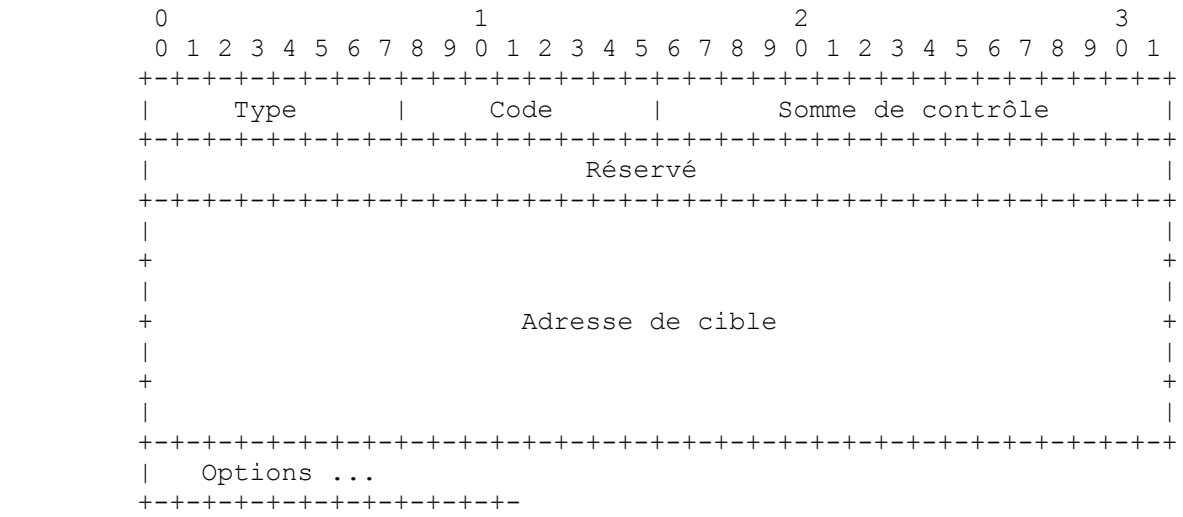
MTU : DEVRAIT être envoyée sur les liaisons qui ont une MTU variable (comme spécifié dans le document qui décrit comment fonctionne IP sur le type de liaison particulier). PEUT être envoyée sur d'autres liaisons.

Informations de préfixes
Ces options spécifient les préfixes qui sont en liaison et/ou sont utilisés pour l'autoconfiguration d'adresse. Un routeur DEVRAIT inclure tous ses préfixes en liaison (excepté le préfixe de liaison locale) afin que les hôtes multi rattachement aient des informations complètes de préfixes sur les destinations en liaison pour les liaisons auxquelles ils se rattachent. Si des informations complètes manquent, un hôte multi-rattachement peut n'être pas capable de choisir l'interface de sortie correcte lors de l'envoi de trafic à ses voisins.

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 de traiter le message.

4.3 Format du message Sollicitation de voisin

Les nœuds envoient des sollicitations de voisin pour demander l'adresse de couche liaison d'un nœud cible tout en fournissant aussi leur propre adresse de couche liaison à la cible. Les sollicitations de voisin sont en diffusion groupée lorsque le nœud a besoin de résoudre une adresse et en envoi individuel lorsque le nœud cherche à vérifier l'accessibilité d'un voisin.



Champs IP :
Adresse de source : Soit une adresse allouée à l'interface d'où ce message est envoyé, soit (si la détection d'adresse dupliquée est en cours [RFC4862]) l'adresse non spécifiée.
Adresse de destination : Soit l'adresse de diffusion groupée du nœud sollicité correspondant à l'adresse cible, soit l'adresse cible.
Limite de bonds :255

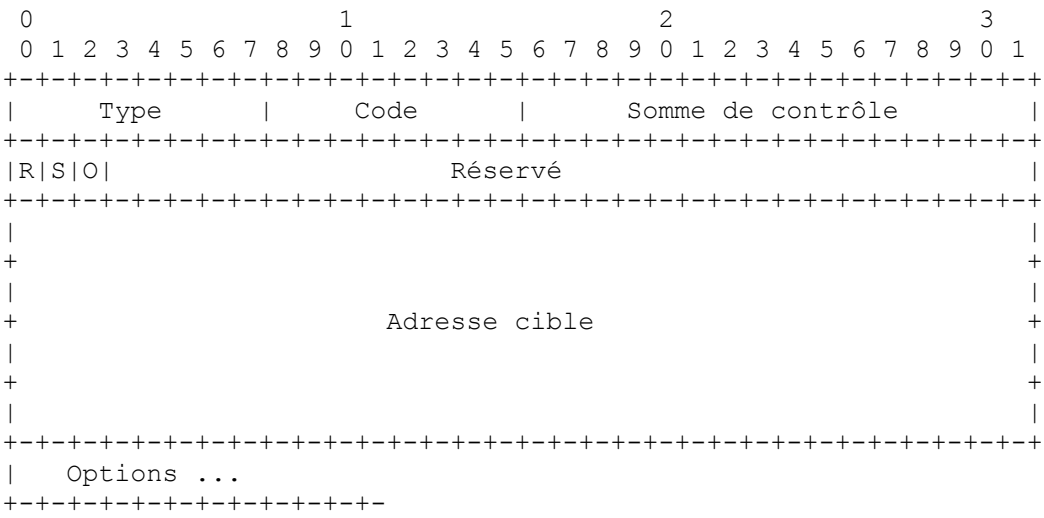
Champs ICMP :
Type ; 135
Code : 0
Somme de contrôle : La somme de contrôle ICMP. Voir [RFC4443].
Réservé : Ce champ n'est pas utilisé. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré par le receveur.
Adresse cible : Adresse IP de la cible de la sollicitation. Il NE DOIT PAS être une adresse de diffusion groupée.

Options possibles :
Adresse de source de couche liaison
Adresse de couche liaison pour l'envoyeur. Elle NE DOIT PAS être incluse lorsque l'adresse IP de source est l'adresse non spécifiée. Autrement, sur les couches de liaison qui ont des adresses, cette option DOIT être incluse dans les sollicitations en diffusion groupée et DEVRAIT être incluse dans les sollicitations en envoi individuel.

De futures versions de ce protocole pourraient définir de nouveaux types d'option. Les receveurs DOIVENT ignorer en silence toute option qu'ils ne reconnaissent pas et continuer de traiter le message.

4.4 Format du message Annonce de voisin

Un nœud envoie des annonces de voisin en réponse aux sollicitation de voisin et envoie des annonces de voisin non sollicitées afin de propager rapidement (de façon non fiable) de nouvelles informations.



Champs IP :

Adresse de source : Adresse allouée à l'interface d'où l'annonce est envoyée.

Adresse de destination ; Pour les annonces sollicitées, c'est l'adresse de source d'une sollicitation de voisin invoquante, ou, si l'adresse de source de la sollicitation est l'adresse non spécifiée, l'adresse de diffusion groupée Tous les nœuds. Pour les annonces non sollicitées, c'est normalement l'adresse de diffusion groupée Tous les nœuds.

Limite de bonds : 255

Champs ICMP :

Type : 136

Code : 0

Somme de contrôle : La somme de contrôle ICMP. Voir [RFC4443].

R : Fanion de routeur. Lorsque il est établi, le bit R indique que l'envoyeur est un routeur. Le bit R est utilisé par la détection d'inaccessibilité du voisin pour détecter un routeur qui se change en hôte.

S : Fanion Sollicité. Lorsque il est établi, le bit S indique que l'annonce a été envoyée en réponse à une sollicitation de voisin provenant de l'adresse de destination. Le bit S est utilisé comme confirmation d'accessibilité pour la détection d'inaccessibilité du voisin. Il NE DOIT PAS être établi dans les annonces en diffusion groupée ou dans des annonces non sollicitées en envoi individuel.

O : Fanion Outrepasser. Lorsque il est établi, le bit O indique que l'annonce devrait outrepasser une entrée d'antémémoire existante et mettre à jour l'adresse de couche liaison en antémémoire. Lorsque il n'est pas établi, l'annonce ne va pas mettre à jour une adresse de couche liaison en antémémoire bien qu'elle mette à jour une entrée de voisin existante en antémémoire pour laquelle aucune adresse de couche liaison n'est connue. Il NE DEVRAIT PAS être établi dans des annonces sollicitées pour des adresses d'envoi à la cantonade et dans des annonces de mandataire sollicitées. Il DEVRAIT être établi dans les autres annonces sollicitées et non sollicitées.

Réservé : Champ inutilisé de 29 bits. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré par le receveur.

Adresse cible : Pour les annonces sollicitées, le champ Adresse cible dans le message Sollicitation de voisin qui invite cette annonce. Pour une annonce non sollicitée, l'adresse dont l'adresse de couche liaison a changé. L'adresse cible NE DOIT PAS être une adresse de diffusion groupée.

Options possibles :

Adresse cible de couche liaison

L'adresse de couche liaison pour la cible, c'est-à-dire, l'envoyeur de l'annonce. Cette option DOIT être incluse sur les couches de liaison qui ont des adresses lors d'une réponse à des sollicitations en diffusion groupée. Lors d'une réponse à une sollicitation de voisin en envoi individuel, cette option DEVRAIT être incluse.

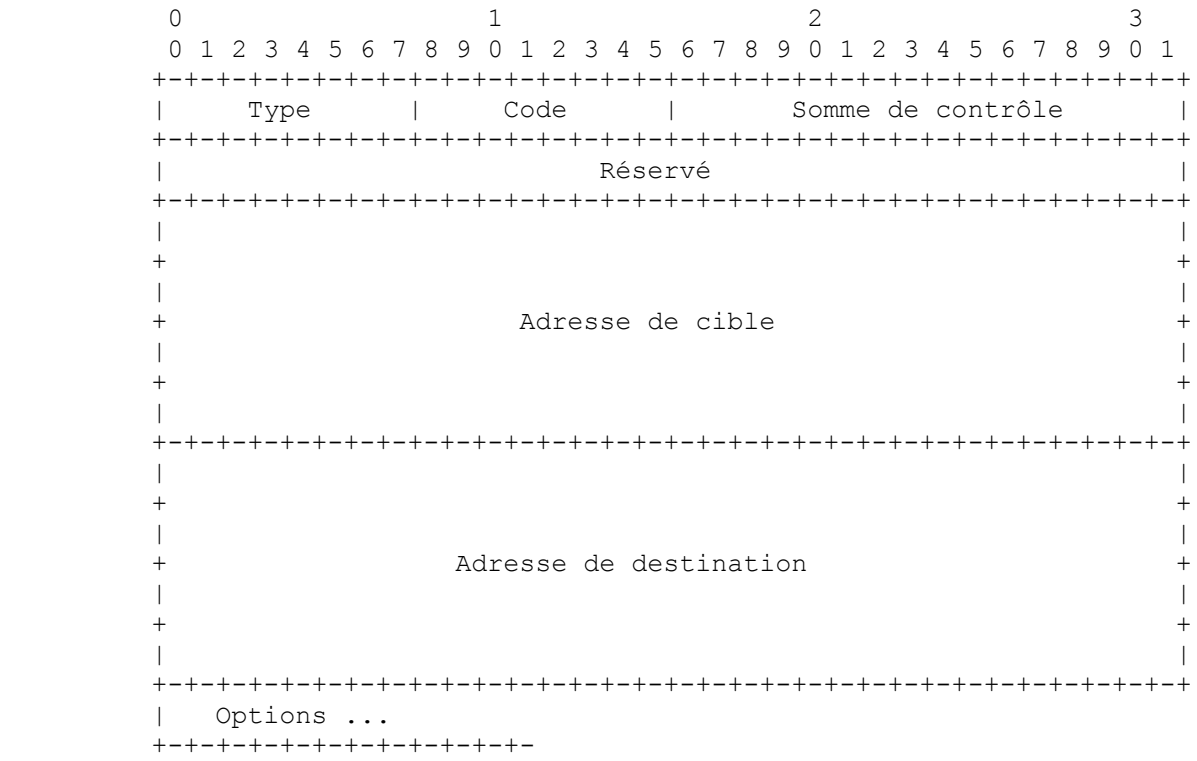
L'option DOIT être incluse pour les sollicitations en diffusion groupée afin d'éviter une récurrence infinie de sollicitations de voisin lorsque le nœud homologue n'a pas d'entrée d'antémémoire pour retourner un message d'annonce de voisin. Lors d'une réponse à des sollicitations en envoi individuel, l'option peut être omise car l'envoyeur de la sollicitation a l'adresse correcte de couche liaison ; autrement il n'aurait pas été capable d'envoyer en premier la sollicitation en envoi individuel. Cependant, inclure l'adresse de couche liaison dans ce cas ajoute peu de redondance et élimine une potentielle condition de concurrence dans laquelle l'envoyeur supprime l'adresse de couche

liaison en antémémoire avant de recevoir une réponse à une sollicitation précédente.

De futures versions de ce protocole pourraient définir de nouveaux types d'option. Les receveurs DOIVENT ignorer en silence toute option qu'ils ne reconnaissent pas et continuer de traiter le message.

4.5 Format du message Redirection

Les routeurs envoient des paquets Redirection pour informer un hôte d'un meilleur nœud de premier bond sur le chemin d'une destination. Les hôtes peuvent être redirigés vers un meilleur routeur de premier bond mais peuvent aussi être informés par une Redirection que la destination est en fait un voisin. Ceci est réalisé en réglant l'adresse cible ICMP égale à l'adresse de Destination ICMP.



Champs IP :

Adresse de source ; DOIT être l'adresse de liaison locale allouée à l'interface d'où ce message est envoyé.

Adresse de destination : Adresse de source du paquet qui a déclanché la redirection.

Limite de bond : 255

Champs ICMP :

Type : 137

Code : 0

Somme de contrôle : Somme de contrôle ICMP. Voir [RFC4443].

Réservé : Ce champ est inutilisé. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré par le receveur.

Adresse cible Adresse IP qui est un meilleur premier bond à utiliser pour l'adresse de destination ICMP. Lorsque la cible est le point d'extrémité réel de communication, c'est-à-dire que la destination est un voisin, le champ Adresse cible DOIT contenir la même valeur que le champ Adresse de destination ICMP. Autrement, la cible est un meilleur routeur de premier bond et l'adresse cible DOIT être l'adresse de liaison locale du routeur afin que les hôtes puissent identifier les routeurs de façon univoque.

Adresse de destination : Adresse IP de la destination qui est redirigée sur la cible.

Options possibles :

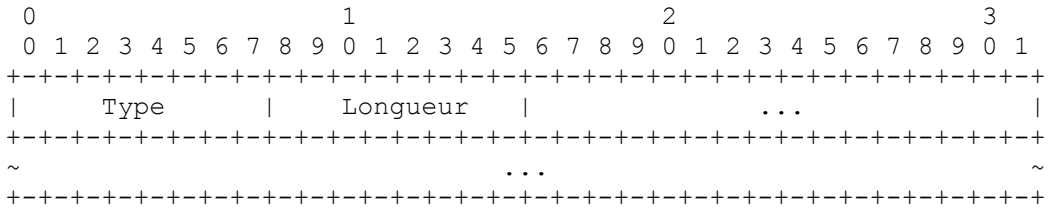
Adresse cible de couche liaison

Adresse de couche liaison pour la cible. Elle DEVRAIT être incluse (si elle est connue). Noter que sur les liaisons NBMA, les hôtes peuvent s'appuyer sur la présence de l'option Adresse cible de couche liaison dans les messages Redirection comme moyen de déterminer les adresses de couche liaison des voisins. Dans de tels cas, l'option DOIT être incluse dans les messages Redirection.

En-tête redirigé
Autant que possible du paquet IP qui a déclanché l'envoi de la Redirection, sans que cela fasse dépasser au paquet redirigé la MTU minimum spécifiée dans [RFC2460].

4.6 Formats d'option

Les messages de découverte de voisin comportent zéro, une ou plusieurs options, dont certaines peuvent apparaître plusieurs fois dans le même message. Les options devraient être bourrées lorsque nécessaire pour s'assurer qu'elles se terminent bien sur leur limite naturelle de 64 bits. Toutes les options sont de la forme :



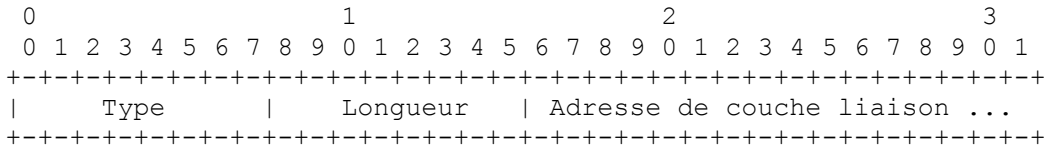
Champs :

Type : Identifiant de 8 bits du type d'option. Les options définies dans le présent document sont :

Nom d'option	Type
Adresse de source de couche liaison	1
Adresse cible de couche liaison	2
Informations de préfixe	3
En-tête redirigé	4
MTU	5

Longueur : Entier non signé de 8 bits. La longueur de l'option (y compris les champs type et longueur) en unités de 8 octets. La valeur 0 est invalide. Les nœuds DOIVENT éliminer en silence un paquet ND qui contient une option de longueur zéro.

4.6.1 Adresse de source/cible de couche liaison



Champs :

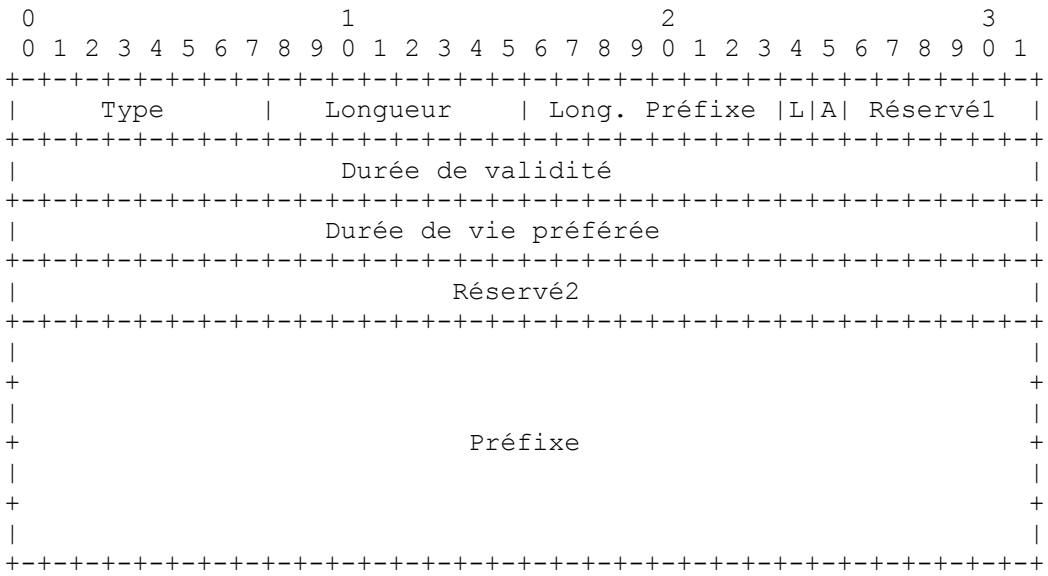
Type
1 pour une adresse de source de couche liaison
2 pour une adresse cible de couche liaison

Longueur : Longueur de l'option (y compris les champs Type et Longueur) en unités de 8 octets. Par exemple, la longueur d'une adresse IEEE 802 est 1 [RFC2464].

Adresse de couche liaison : Adresse de couche liaison de longueur variable. Le contenu et le format de ce champ (y compris l'ordre des octets et des bits) est supposé être spécifié dans des documents particuliers qui décrivent comment fonctionne IPv6 sur les différentes couches de liaison. Par exemple, [RFC2464].

Description
L'option Adresse de source de couche liaison contient l'adresse de couche liaison de l'envoyeur du paquet. Elle est utilisée dans les paquets Sollicitation de voisin, Sollicitation de routeur, et Annonce de routeur. L'option Adresse cible de couche liaison contient l'adresse de couche liaison de la cible. Elle est utilisée dans les paquets Annonce de voisin et Redirection. Ces options DOIVENT être ignorées en silence pour les autres messages de découverte de voisin.

4.6.2 Informations de préfixe



Champs :

Type : 3

Longueur : 4

Longueur de préfixe : Entier non signé de 8 bits. C'est le nombre de bits valides en tête du préfixe. Les valeurs vont de 0 à 128. Le champ Longueur de préfixe donne les informations nécessaires pour la détermination en liaison (lorsque elle est combinée au fanion L dans l'option d'informations de préfixe). Il aide aussi à l'autoconfiguration d'adresse comme spécifié dans la [RFC4862], pour laquelle il peut y avoir plus de restrictions sur la longueur du préfixe.

L : Fanion en liaison de 1 bit. Établi, il indique que ce préfixe peut être utilisé pour la détermination en liaison. Non établi, l'annonce ne fait pas de déclaration sur les propriétés en liaison ou hors liaison du préfixe. En d'autres termes, si le fanion n'est pas établi, un hôte NE DOIT PAS en conclure qu'une adresse déduite du préfixe est hors liaison. C'est-à-dire qu'il NE DOIT PAS mettre à jour une indication antérieure disant que l'adresse est hors liaison.

A : Fanion de 1 bit de configuration autonome d'adresse. Établi, il indique que ce préfixe peut être utilisé pour la configuration d'adresse sans état comme spécifié dans la [RFC4862].

Réservé1 : Champ inutilisé de 6 bits. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré par le receveur.

Durée de validité : Entier non signé de 32 bits. Durée en secondes (par rapport au moment de l'envoi du paquet) pendant laquelle le préfixe est valide pour les besoins de la détermination en liaison. Une valeur de tous les bits à un (0xffffffff) représente l'infini. La durée de validité est aussi utilisée par la [RFC4862].

Durée de vie préférée : Entier non signé de 32 bits. Durée en secondes (par rapport au moment de l'envoi du paquet) pendant laquelle les adresses générées à partir du préfixe via l'autoconfiguration d'adresse sans état restent préférées [RFC4862]. Une valeur de tous les bits à un (0xffffffff) représente l'infini. Voir [RFC4862].

Noter que la valeur de ce champ NE DOIT PAS excéder celle du champ Durée de validité pour éviter de préférer des adresses qui ne sont plus valides.

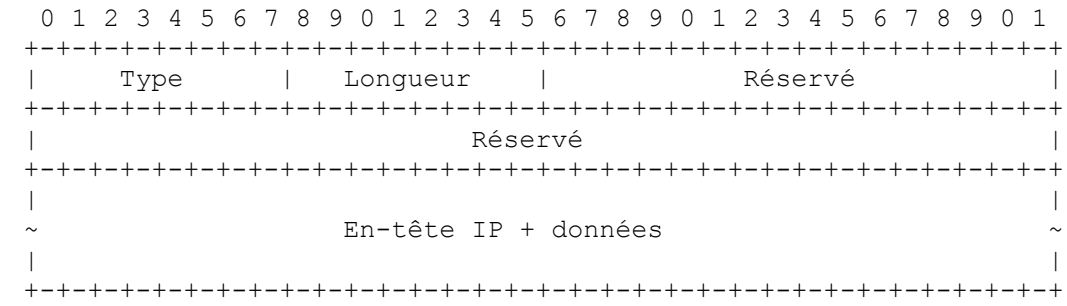
Réservé2 : Ce champ est inutilisé. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré par le receveur.

Préfixe : Adresse IP ou préfixe d'une adresse IP. Le champ Longueur de préfixe contient le nombre de bits valides en tête du préfixe. Les bits du préfixe après la longueur du préfixe sont réservés et DOIVENT être initialisés à zéro par l'envoyeur et ignorés par le receveur. Un routeur NE DEVRAIT PAS envoyer une option Préfixe pour le préfixe de liaison local et un hôte DEVRAIT ignorer une telle option.

Description

L'option Informations de préfixe fournit aux hôtes les préfixes en liaison et les préfixes pour l'autoconfiguration d'adresse. L'option Informations de préfixe apparaît dans les paquets Annonce de routeur et DOIT être ignorée en silence pour les autres messages.

4.6.3 En-tête redirigé



Champs :

Type : 4

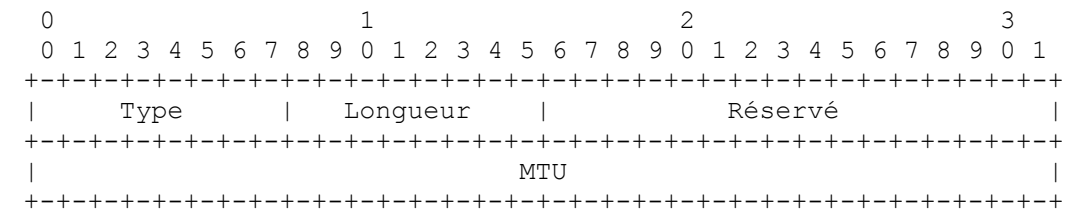
Longueur : Longueur de l'option en unités de 8 octets.

Réservé : Ces champs sont inutilisés. Ils DOIVENT être initialisés à zéro par l'envoyeur et DOIVENT être ignorés par le receveur.

En-tête IP + données : Paquet d'origine tronqué pour garantir que la taille du message redirigé n'excède pas la MTU minimum exigée pour la prise en charge de IPv6, comme spécifié dans [RFC2460].

Description : L'option En-tête redirigé est utilisée dans les messages Redirection et contient tout ou partie du paquet qui est redirigé. Cette option DOIT être ignorée en silence pour les autres messages de découverte de voisin.

4.6.4 MTU



Champs :

Type : 5

Longueur : 1

Réservé : Champ inutilisé. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré par le receveur.

MTU : Entier non signé de 32 bits. C'est la MTU recommandée pour la liaison.

Description

L'option MTU est utilisée dans les messages Annonce de routeur pour s'assurer que tous les nœuds sur une liaison utilisent la même valeur de MTU dans les cas où la MTU de la liaison n'est pas bien connue. Cette option DOIT être ignorée en silence pour les autres messages de découverte de voisin.

Dans les configurations dans lesquelles des technologies hétérogènes sont raccordées ensemble, la MTU maximum prise en charge peut différer d'un segment à un autre. Si les raccords ne génèrent pas de message ICMP Paquet trop gros, les nœuds communicants seront incapables d'utiliser la MTU du chemin pour déterminer de façon dynamique la MTU appropriée voisin par voisin. Dans de tels cas, les routeurs peuvent être configurés pour utiliser l'option MTU pour spécifier la valeur de MTU maximum qui est acceptée par tous les segments.

5. Modèle conceptuel d'un hôte

Cette section décrit un modèle conceptuel d'une organisation possible de structure des données que les hôtes (et dans une certaine mesure les routeurs) vont maintenir en interagissant avec les nœuds voisins. L'organisation décrite est fournie pour faciliter l'explication de la façon dont le protocole de découverte de voisin devrait se comporter. Le présent document ne rend pas obligatoire que les mises en œuvre adhèrent à ce modèle pour autant que leur comportement externe soit cohérent avec celui décrit dans le présent document.

Ce modèle ne traite que des aspects du comportement d'hôte directement en rapport avec la découverte de voisin. En particulier, il ne s'occupe pas de questions telles que le choix d'adresse de source ou le choix d'une interface sortante sur un hôte à rattachements multiples.

5.1 Structures conceptuelles des données

Les hôtes devront maintenir les informations suivantes pour chaque interface :

Antémémoire de voisin
- Ensemble d'entrées sur les voisins individuels auxquels du trafic a été envoyé récemment. Les entrées sont centrées sur l'adresse IP d'envoi individuel en liaison du voisin et contiennent des informations comme son adresse de couche liaison, un fanion indiquant si le voisin est un routeur ou un hôte (appelé IsRouter dans le présent document), un pointeur sur tout paquet en file d'attente de l'achèvement de la résolution d'adresse, etc. Une entrée d'antémémoire de voisin contient aussi des informations utilisées par l'algorithme de détection d'inaccessibilité du voisin, incluant l'état d'accessibilité, le nombre d'essais non acquittés, et le moment où le prochain événement de détection d'inaccessibilité du voisin est programmé.

Antémémoire de destination
- Ensemble d'entrées sur les destinations auxquelles du trafic a été envoyé récemment. L'antémémoire de destination comporte à la fois des destinations en liaison et hors liaison et fournit un niveau d'accès indirect dans l'antémémoire de voisin ; l'antémémoire de destination transpose une adresse IP de destination en l'adresse du voisin du prochain bond. Cette antémémoire est mise à jour avec les informations apprises des messages Redirection. Les mises en œuvre peuvent trouver pratique de mémoriser des informations supplémentaires non directement en rapport avec la découverte de voisin dans les entrées d'antémémoire de destination, comme la MTU de chemin (PMTU) et des temporisateurs de délai d'aller-retour entretenus par les protocoles de transport.

Liste de préfixes
- Une liste des préfixes qui définissent un ensemble d'adresses qui sont en liaison. Les entrées de la liste de préfixes sont créées à partir d'informations reçues dans les annonces de routeur. Chaque entrée a une valeur de temporisateur d'invalidation associée (extraite de l'annonce) utilisée pour périmer les préfixes lorsque ils deviennent invalides. Une valeur spéciale "infini" du temporisateur spécifie qu'un préfixe reste valide pour toujours, sauf si une nouvelle valeur (finie) est reçue dans une annonce ultérieure.

  Le préfixe de liaison locale est considéré comme étant sur la liste des préfixes avec un temporisateur d'invalidation infini, sans considération de l'annonce de préfixe que les routeurs ont pu faire pour lui. Les annonces de routeur reçues NE DEVRAIENT PAS modifier le temporisateur d'invalidation pour le préfixe de liaison locale.

Liste des routeurs par défaut
- Liste des routeurs auxquels des paquets peuvent être envoyés. Les entrées de la liste des routeurs pointent sur les entrées de l'antémémoire de voisins ; l'algorithme de sélection d'un routeur par défaut favorise les routeurs connus pour être accessibles au détriment de ceux dont l'accessibilité est suspecte. Chaque entrée a aussi une valeur de temporisateur d'invalidation associée (extraite des annonces de routeur) utilisée pour supprimer les entrées qui ne sont plus annoncées.

Noter que les structures conceptuelles de données ci-dessus peuvent être mises en œuvre en utilisant diverses techniques. Une mise en œuvre possible est d'utiliser un seul tableau d'acheminement à la plus longue correspondance pour toutes les structures de données ci-dessus. Sans considération de la mise en œuvre spécifique, il est très important que l'entrée d'antémémoire de voisin pour un routeur soit partagée par toutes les entrées de l'antémémoire de destination qui utilisent ce routeur afin d'empêcher des essais redondants de détection d'inaccessibilité du voisin.

Noter aussi que d'autres protocoles (par exemple, IPv6 Mobile) peuvent ajouter des structures conceptuelles de données supplémentaires .Une mise en œuvre est libre de développer de telles structures de données de la façon qu'il lui plaît. Par exemple, une mise en œuvre pourrait fusionner toutes les structures de données conceptuelles dans un seul tableau d'acheminement.

L'antémémoire de voisin contient des informations entretenues par l'algorithme de détection d'inaccessibilité du voisin. Une pièce maîtresse de ces informations est l'état d'accessibilité d'un voisin, qui a une valeur parmi cinq possibles. Les définitions suivantes sont informelles ; les définitions précises se trouvent au paragraphe 7.3.2.

INCOMPLET La résolution d'adresse est en cours et l'adresse de couche liaison du voisin n'a pas encore été déterminée.

ACCESSIBLE En gros, le voisin est connu pour avoir été accessible récemment (il y a quelques dizièmes de secondes).

PÉRIMÉ Le voisin n'est plus connu comme accessible mais jusqu'à ce que du trafic soit envoyé au voisin, aucune

tentative ne devrait être faite pour vérifier son accessibilité.

DÉLAI Le voisin n'est plus connu comme accessible, et du trafic a récemment été envoyé au voisin. Cependant, plutôt que de tester le voisin immédiatement, attendre un petit moment avant d'envoyer des sondes afin de donner aux protocoles de couche supérieure une chance de fournir une confirmation d'accessibilité.

SONDE Le voisin n'est plus connu comme accessible, et des sondes en envoi individuel de sollicitation de voisin sont envoyées pour vérifier l'accessibilité.

5.2 Algorithme conceptuel d'envoi

Lors de l'envoi d'un paquet à une destination, un nœud utilise une combinaison de l'antémémoire de destinations, de la liste des préfixes, et de routeurs par défaut pour déterminer l'adresse IP du prochain bond approprié, une opération appelée "détermination du prochain bond". Une fois que l'adresse IP du prochain bond est connue, l'antémémoire de voisins est consultée sur les informations de couche liaison au sujet de ce voisin.

La détermination du prochain bond pour une destination en envoi individuel donnée fonctionne comme suit. L'envoyeur effectue une recherche de plus longue correspondance de préfixe dans la liste des préfixes pour déterminer si la destination du paquet est en ou hors liaison. Si la destination est en liaison, l'adresse de prochain bond est la même que l'adresse de destination du paquet. Autrement, l'envoyeur choisit un routeur dans la liste des routeurs par défaut (suivant les règles décrites au paragraphe 6.3.6)

Pour des raisons d'efficacité, la détermination du prochain bond n'est pas effectuée sur tous les paquets qui sont envoyés. Les résultats des calculs de détermination du prochain bond sont plutôt sauvegardés dans l'antémémoire de destination (qui contient aussi les mises à jour apprises des messages Redirection). Lorsque le nœud d'envoi a un paquet à envoyer, il examine d'abord l'antémémoire de destination. Si il n'existe pas d'entrée pour la destination, la détermination du prochain bond est invoquée pour créer une entrée d'antémémoire de destination.

Une fois que l'adresse IP du nœud de prochain bond est connue, l'envoyeur examine dans l'antémémoire de voisins les informations de couche liaison sur ce voisin. Si il n'existe aucune entrée, l'envoyeur en crée une, règle son état à INCOMPLET, initie la résolution d'adresse, puis met en file d'attente le paquet de données en attendant l'achèvement de la résolution d'adresse. Pour les interfaces à capacité de diffusion groupée, la résolution d'adresse consiste à envoyer un message Sollicitation de voisin et à attendre une annonce de voisin. Lorsque une réponse d'annonce de voisin est reçue, les adresses de couche liaison sont ajoutées dans l'entrée d'antémémoire de voisin et le paquet en file d'attente est transmis. Le mécanisme de résolution d'adresse est décrit en détail au paragraphe 7.2.

Pour les paquets en diffusion groupée, le prochain bond est toujours l'adresse de destination (en diffusion groupée) et est considéré comme étant en liaison. La procédure pour déterminer l'adresse de couche liaison correspondant à une adresse de diffusion groupée se trouve dans un document distinct qui traite du fonctionnement de IP sur des types de liaison particuliers (par exemple, [RFC2464]).

Chaque fois qu'il accède à une entrée d'antémémoire de voisin lors de la transmission d'un paquet en envoi individuel, l'envoyeur vérifie les informations se rapportant à la détection d'inaccessibilité du voisin conformément à l'algorithme de détection d'inaccessibilité du voisin (paragraphe 7.3). Cette vérification d'inaccessibilité peut résulter en la transmission par l'envoyeur d'une sollicitation de voisin en envoi individuel pour vérifier que le voisin est encore accessible.

La détermination du prochain bond est faite la première fois que du trafic est envoyé à une destination. Tant que les communications ultérieures vers cette destination se poursuivent avec succès, l'entrée d'antémémoire de destination continue d'être utilisée. Si à un moment donné la communication cesse de se faire, comme déterminé par l'algorithme Détection d'inaccessibilité du voisin, la détermination du prochain bond peut devoir être effectuée à nouveau. Par exemple, le trafic par un routeur défaillant devrait être passé sur un routeur qui fonctionne. De même, il est possible de réacheminer le trafic destiné à un nœud mobile sur un "agent de mobilité".

Noter que lorsque un nœud refait la détermination du prochain bond, il n'est pas nécessaire d'éliminer toute l'entrée d'antémémoire de destination. En fait, il est généralement bénéfique de garder des informations d'antémémoire telles que la PMTU et les valeurs de délai d'aller-retour qui peuvent aussi être conservées dans l'entrée d'antémémoire de destination.

Les routeurs et les hôtes multi-rattachement ont plusieurs interfaces. Dans la suite de ce document, on suppose que tous les messages de découverte de voisin envoyés et reçus se réfèrent à l'interface du contexte approprié. Par exemple, en répondant à une sollicitation de routeur, l'annonce de routeur correspondante est envoyée de l'interface sur laquelle la sollicitation a été reçue.

5.3 Exigences pour le ramassage des déchets et les fins de temporisation

Les structures de données conceptuelles décrites ci-dessus utilisent différents mécanismes pour éliminer les informations potentiellement périmées ou inutilisées.

Du point de vue de la correction du traitement, il n'est pas nécessaire de purger périodiquement les entrées d'antémémoire de destination et de voisin. Bien que les informations périmées puissent rester indéfiniment dans l'antémémoire, l'algorithme Détection d'inaccessibilité du voisin s'assure que les informations périmées sont purgées rapidement lorsque il est réellement utilisé.

Pour limiter la taille de mémoire nécessaire pour les antémémoires de destination et de voisin, un nœud peut avoir besoin de passer à la corbeille les vieilles entrées. Cependant, il faut faire attention de s'assurer qu'un espace suffisant est toujours présent pour détenir l'ensemble actif des entrées. Une petite antémémoire peut résulter en un nombre excessif de messages de découverte de voisin si les entrées sont éliminées et reconstruites en succession rapide. Toute politique fondée sur le moins récemment utilisé (LRU, *Least Recently Used*) qui ne réforme que les entrées qui n'ont pas été utilisées pendant un certain temps (par exemple, dix minutes ou plus) devrait être adéquate pour l'élimination des entrées non utilisées.

Un nœud devrait conserver les entrées dans la Liste des routeurs par défaut et la Liste des préfixes jusqu'à ce que leur durée de vie arrive à expiration. Cependant, un nœud peut purger les entrées prématurément si il est faible en mémoire. Si tous les routeurs ne sont pas gardés dans la Liste des routeurs par défaut, un nœud devrait conserver au moins deux entrées dans la liste des routeurs par défaut (et plus de préférence) afin de conserver une connexité robuste pour les destinations hors liaison.

Lors du retrait d'une entrée de la Liste des préfixes, il n'est pas nécessaire de purger des entrées des antémémoires de destination ou de voisin. La détection d'inaccessibilité du voisin va purger efficacement toutes les entrées de ces antémémoires qui sont devenues invalides. Cependant, lors de la suppression d'une entrée de la Liste des routeurs par défaut, toute entrée de l'antémémoire de destination qui passe par ce routeur doit effectuer à nouveau une détermination du prochain bond pour choisir un nouveau routeur par défaut.

6. Découverte de routeur et de préfixe

Cette section décrit le comportement de routeur et d'hôte en rapport avec la portion découverte de routeur de la découverte de voisin. La découverte de routeur est utilisée pour localiser les routeurs voisins ainsi que les préfixes et paramètres de configuration appris en rapport avec l'autoconfiguration d'adresse.

La découverte de préfixe est le processus par lequel les hôtes apprennent les gammes d'adresses IP qui résident en liaison et peuvent être atteintes directement sans passer par un routeur. Les routeurs envoient des annonces de routeur qui indiquent si l'envoyeur veut être un routeur par défaut. Les annonces de routeur contiennent aussi les options Informations de préfixe qui font la liste de l'ensemble des préfixes qui identifient les adresses IP en liaison.

L'autoconfiguration d'adresse sans état doit aussi obtenir les préfixes de sous réseau au titre de la configuration des adresses. Bien que les préfixes utilisés pour l'autoconfiguration d'adresse soient logiquement distincts de ceux utilisés pour la détermination en liaison, les informations d'autoconfiguration sont portées par les messages de découverte de routeur pour réduire le trafic réseau. Bien sûr, les mêmes préfixes peuvent être annoncés pour la détermination en liaison et l'autoconfiguration d'adresse en spécifiant les fanions appropriés dans les options Information de préfixe. Voir dans la [RFC4862] les détails de la façon dont sont traitées les informations d'autoconfiguration.

6.1 Validation de message

6.1.1 Validation du message Sollicitation de routeurs

Les hôtes DOIVENT éliminer en silence tous les messages Sollicitation de routeurs reçus.

Un routeur DOIT éliminer en silence tout message Sollicitation de routeurs reçu qui ne satisfait pas toutes les vérifications de validité suivantes :

- Le champ Limite de bonds IP a une valeur de 255, c'est-à-dire, le paquet ne pourrait pas avoir été transmis par un routeur.
- La somme de contrôle ICMP est valide.

- Le code ICMP est 0.
- La longueur ICMP (déduite de la longueur IP) est supérieure ou égale à 8 octets.
- Toutes les options incluses ont une longueur supérieure à zéro.
- Si l'adresse IP de source est l'adresse non spécifiée, il n'y a pas d'option d'adresse de couche liaison de source dans le message.

Le contenu du champ Réservé, et de toute option non reconnue, DOIT être ignoré. De futurs changements rétro compatibles du protocole pourraient spécifier le contenu du champ Réservé ou ajouter de nouvelles options ; les changement 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 le message Sollicitation de routeurs DOIT être ignoré et le paquet traité normalement. La seule option définie qui peut apparaître est l'option Adresse de source de couche liaison.

Une sollicitation qui réussit les vérifications de validité est appelée une "sollicitation valide".

6.1.2 Validation des messages Annonce de routeur

Un nœud DOIT éliminer en silence tout message Annonce de routeur reçue qui ne satisfait pas aux vérifications de validité suivantes :

- L'adresse IP de source est une adresse de liaison locale. Les routeurs doivent utiliser leur adresse de liaison locale comme source pour les messages Annonce de routeur et Redirection afin que les hôtes puissent identifier de façon univoque les routeurs.
- Le champ Limite de bond IP a la valeur 255, c'est-à-dire, le paquet ne pourrait pas avoir été transmis par un routeur.
- La somme de contrôle ICMP est valide.
- Le code ICMP est 0.
- La longueur ICMP (déduite de la longueur IP) est supérieure ou égale à 16 octets.
- Toutes les options incluses ont une longueur supérieure à zéro.

Le contenu du champ Réservé, et de toute option non reconnue, DOIT être ignoré. De futurs changements rétro compatibles du protocole pourraient 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 Annonce de routeur DOIT être ignoré et le paquet traité normalement. Les seules options définies qui peuvent apparaître sont les options Adresse de source de couche liaison, Informations de préfixes et MTU.

Une annonce qui réussit les vérifications de validité est appelée une "annonce valide".

6.2 Spécification du routeur

6.2.1 Variables de configuration de routeur

Un routeur DOIT permettre de configurer les variables conceptuelles suivantes par la gestion de système. Les noms des variables spécifiques ne sont donnés que pour les besoins de la démonstration, et une mise en œuvre n'est pas obligée de les reprendre, pour autant que son comportement externe soit cohérent avec celui décrit dans le présent document. Les valeurs par défaut sont spécifiées pour simplifier la configuration dans les cas courants.

Les valeurs par défaut de certaines des variables énumérées ci-dessous peuvent être outrepassées par des documents spécifiques qui décrivent comment fonctionne IPv6 sur les différentes couches de liaison. Cette règle simplifie la configuration de la découverte de voisin sur des types de liaison qui ont des caractéristiques de performances largement différentes.

Pour chaque interface de diffusion groupée :

IsRouter
Fanion qui indique si le routeur est activé sur cette interface. Activer l'acheminement sur l'interface impliquerait qu'un routeur puisse transmettre des paquets à ou de l'interface.
Défaut : FAUX

AdvSendAdvertisements
Fanion qui indique si le routeur envoie ou non des Annonces de routeur périodiques et répond aux Sollicitations de

routeur.
Défaut : FAUX

Noter que AdvSendAdvertisements DOIT être FAUX par défaut afin qu'un nœud ne commence pas accidentellement à agir comme un routeur sauf si il est explicitement configuré par la gestion du système à envoyer des Annonces de routeur.

MaxRtrAdvInterval
C'est le délai maximum permis entre l'envoi d'annonces de routeur non sollicitées en envoi groupé par l'interface, en secondes. Il DOIT être supérieur ou égal à 4 secondes et inférieur ou égal à 1800 secondes.
Défaut : 600 secondes

MinRtrAdvInterval
Délai minimum permis entre l'envoi d'annonces de routeur non sollicitées en envoi groupé par l'interface, en secondes. Il DOIT être supérieur ou égal à 3 secondes et inférieur ou égal à 0,75 * MaxRtrAdvInterval.
Défaut : 0,33 * MaxRtrAdvInterval si MaxRtrAdvInterval ≥ 9 secondes ; autrement, la valeur par défaut est MaxRtrAdvInterval.

AdvManagedFlag
La valeur VRAI/FAUX à placer dans le champ de fanion "Configuration d'adresse gérée" dans l'annonce de routeur. Voir dans [RFC4862].
Défaut : FAUX

AdvOtherConfigFlag
La valeur VRAI/FAUX à placer dans le champ de fanion "Autre configuration à état plein" dans l'annonce de routeur. Voir dans [RFC4862].
Défaut : FAUX

AdvLinkMTU
La valeur à placer dans les options MTU envoyées par le routeur. Une valeur de zéro indique qu'aucune option MTU n'est envoyée.
Défaut : 0

AdvReachableTime
Valeur à placer dans le champ Durée d'accessibilité dans le message Annonce de routeur envoyé par le routeur. La valeur zéro signifie non spécifié (par ce routeur). Elle DOIT n'être pas supérieure à 3 600 000 millisecondes (1 heure).
Défaut : 0

AdvRetransTimer
Valeur à placer dans le champ Temporisateur de retransmission dans le message Annonce de routeur envoyé par le routeur. La valeur zéro signifie non spécifié (par ce routeur).
Défaut : 0

AdvCurHopLimit
Valeur par défaut à placer dans le champ Limite de bons du message Annonce de routeur envoyé par le routeur. La valeur devrait être réglée au diamètre actuel de l'Internet. La valeur zéro signifie non spécifié (par ce routeur).
Défaut : La valeur spécifiée dans la RFC " Numéros alloués" [RFC3232] en vigueur au jour de la mise en œuvre.

AdvDefaultLifetime
Valeur à placer dans le champ Durée de vie du routeur de l'annonce de routeur envoyée de l'interface, en secondes. Elle DOIT être zéro ou entre MaxRtrAdvInterval et 9000 secondes. Une valeur de zéro indique que le routeur n'est pas à utiliser comme routeur par défaut. Ces limites peuvent être outrepassées par des documents spécifiques qui décrivent comment IPv6 opère sur différentes couches de liaison. Par exemple, dans une liaison point à point, les homologues peuvent avoir assez d'informations sur le nombre et l'état des appareils à l'autre extrémité pour que ces annonces soient moins fréquemment nécessaires.
Défaut : 3 * MaxRtrAdvInterval

AdvPrefixList
Liste de préfixes à placer dans l'option Informations de préfixe dans les messages Annonce de routeur envoyés de l'interface.
Défaut : Tous les préfixes que le routeur annonce via les protocoles d'acheminement comme étant en liaison pour l'interface de laquelle l'annonce est envoyée. Le préfixe de liaison locale NE DEVRAIT PAS être inclus dans la liste des préfixes annoncés.

Chaque préfixe a un associé :

AdvValidLifetime

La valeur à placer dans Durée de vie valide dans l'option Informations de préfixe, en secondes. La valeur désignée toute en uns (0xffffffff) représente l'infini. Les mises en œuvre PEUVENT permettre que AdvValidLifetime soit spécifié de deux façons :

- une durée qui est décrémentée en temps réel, c'est-à-dire, qui va résulter en une durée de vie de zéro à l'heure spécifiée dans le futur, ou
- une heure fixe qui va rester la même dans les annonces consécutives.

Défaut : 2 592 000 secondes (30 jours), fixe (c'est-à-dire, qui reste la même dans les annonces consécutives).

AdvOnLinkFlag

Valeur à placer dans le champ fanion en liaison ("bit L ") dans l'option Informations de préfixe.
Défaut : VRAI

La configuration d'adresse sans état [RFC4862] définit des informations supplémentaires associées à chaque préfixe :

AdvPreferredLifetime

Valeur à placer dans Durée de vie préférée dans l'option Informations de préfixe, en secondes. La valeur désignée de tout en uns (0xffffffff) représente l'infini. Voir dans la [RFC4862] les détails sur la façon dont cette valeur est utilisée. Les mises en œuvre PEUVENT permettre que AdvPreferredLifetime soit spécifié de deux façons :

- Une durée qui décrémente en temps réel, c'est-à-dire, qui va résulter en une durée de vie de zéro à une heure spécifiée dans le futur, ou
- une heure fixe qui reste la même dans les annonces consécutives.

Défaut : 604 800 secondes (7 jours), fixe (c'est-à-dire, qui reste la même dans les annonces consécutives). Cette valeur NE DOIT PAS être supérieure à AdvValidLifetime.

AdvAutonomousFlag

Valeur à placer dans le champ Fanion autonome dans l'option Informations de préfixe. Voir [RFC4862].
Défaut : VRAI

Les variables ci-dessus contiennent des informations qui sont placées dans les messages Annonce de routeur sortants. Les hôtes utilisent les informations reçues pour initialiser un ensemble de variables analogues qui contrôlent leur comportement externe (voir au paragraphe 6.3.2). Certaines de ces variables d'hôte (par exemple, CurHopLimit, RetransTimer, et ReachableTime) s'appliquent à tous les nœuds y compris les routeurs. En pratique, ces variables peuvent n'être pas réellement présentes sur les routeurs, car leur contenu peut être déduit des variables décrites ci-dessus. Cependant, le comportement externe du routeur DOIT être le même que le comportement de l'hôte par rapport à ces variables. En particulier, cela inclut l'aléation occasionnelle de la valeur de ReachableTime comme décrit au paragraphe 6.3.2.

Les constantes du protocole sont définies à la Section 10.

6.2.2 Devenir une interface d'annonce

Le terme " interface d'annonce" se réfère à toute interface de diffusion groupée qui fonctionne et est activée qui a au moins une adresse IP d'envoi individuel allouée et dont le fanion correspondant AdvSendAdvertisements est VRAI. Un routeur NE DOIT PAS envoyer d'annonces de routeur à partir d'une interface qui n'est pas une interface d'annonce.

Une interface peut devenir une interface d'annonce à des moments autres que le démarrage du système. Par exemple :

- en changeant le fanion AdvSendAdvertisements sur une interface activée de FAUX à VRAI, ou
- en activant administrativement l'interface, si elle a été administrativement désactivée et si son fanion AdvSendAdvertisements est VRAI, ou
- en activant la capacité de transmission IP (c'est-à-dire, en changeant le système de hôte à routeur), lorsque le fanion AdvSendAdvertisements de l'interface est VRAI.

Un routeur DOIT joindre l'adresse de diffusion groupée Tous routeurs sur une interface d'annonce. Les routeurs répondent aux Sollicitations de routeurs envoyées à l'adresse Tous routeurs et vérifient la cohérence des Annonces de routeur envoyées par les routeurs voisins.

6.2.3 Contenu du message Annonce de routeur

Un routeur envoie des Annonces de routeur périodiques aussi bien que sollicitées de ses interfaces d'annonce. Les annonces de routeur sortantes sont remplies avec les valeurs suivantes, cohérentes avec le format de message donné au paragraphe 4.2 :

- Dans le champ Durée de vie de routeur : la valeur de AdvDefaultLifetime configurée de l'interface.

- Dans les fanions M et O : respectivement, les valeurs de AdvManagedFlag et AdvOtherConfigFlag configurées de l'interface.

- Dans le champ Limite de bonds actuelle : la valeur de CurHopLimit configurée de l'interface.

- Dans le champ Durée d'accessibilité : la valeur de AdvReachableTime configurée de l'interface.

- Dans le champ Temporisateur de retransmission: la valeur de AdvRetransTimer configurée de l'interface.

- Dans les options :
  - o Option Adresse de source de couche liaison : l'adresse de couche liaison de l'interface d'envoi. Cette option PEUT être omise pour faciliter l'équilibrage de charge entrant sur des interfaces dupliquées.
  - o Option MTU: la valeur de AdvLinkMTU configurée de l'interface si cette valeur est différente de zéro. Si AdvLinkMTU est zéro, l'option MTU n'est pas envoyée.
  - o Option Informations de préfixe : une option Informations de préfixe pour chaque préfixe énuméré dans AdvPrefixList avec les champs Option réglés à partir des informations de l'entrée de AdvPrefixList comme suit :
    - Dans le fanion "en liaison" : la valeur AdvOnLinkFlag de l'entrée.
    - Dans le champ Durée de validité : la valeur de AdvValidLifetime de l'entrée.
    - Dans le fanion "Configuration autonome d'adresse" : la valeur de AdvAutonomousFlag de l'entrée.
    - Dans le champ Durée de vie préférée : la valeur de AdvPreferredLifetime de l'entrée.

Un routeur peut vouloir envoyer des annonces de routeur sans s'annoncer lui-même comme routeur par défaut. Par exemple, un routeur peut annoncer des préfixes pour l'autoconfiguration d'adresse tout en ne souhaitant pas transmettre de paquets. Un tel routeur va régler le champ Durée de vie de routeur à zéro dans les annonces sortantes.

Un routeur PEUT choisir de ne pas inclure certaines options, ou toutes, lors de l'envoi d'annonces de routeur non sollicitées. Par exemple, si les durées de vies de préfixe sont beaucoup plus longues que AdvDefaultLifetime, les inclure dans quelques annonces peut être suffisant. Cependant, en répondant à une Sollicitation de routeur ou lors de l'envoi des quelques premières annonces initiales non sollicitées, un routeur DEVRAIT inclure toutes les options afin que toutes les informations (par exemple, les préfixes) soient propagées rapidement durant l'initialisation du système.

Si l'inclusion de toutes les options cause à l'annonce un dépassement de la taille de la MTU de liaison, plusieurs annonces peuvent être envoyées, chacune contenant un sous ensemble des options.

6.2.4 Envoi d'annonces de routeur non sollicitées

Un hôte NE DOIT à aucun moment envoyer de messages Annonce de routeur.

Les annonces de routeur non sollicitées ne sont pas strictement périodiques : l'intervalle entre les transmissions successives est rendu aléatoire pour réduire la probabilité de synchronisation avec les annonces d'autres routeurs sur la même liaison [SYNC]. Chaque interface annonceuse a son propre temporisateur. Chaque fois qu'une annonce en diffusion groupée est envoyée d'une interface, le temporisateur est rétabli à une valeur aléatoire à répartition uniforme entre les valeurs de MinRtrAdvInterval et MaxRtrAdvInterval configurées de l'interface ; l'arrivée à expiration du temporisateur cause l'envoi de la prochaine annonce et le choix d'une nouvelle valeur aléatoire.

Pour les quelques premières annonces (jusqu'à MAX_INITIAL_RTR_ADVERTISEMENTS) envoyées d'une interface lorsque elle devient une interface d'annonce, si l'intervalle choisi au hasard est supérieur à MAX_INITIAL_RTR_ADVERT_INTERVAL, le temporisateur DEVRAIT à la place être réglé à MAX_INITIAL_RTR_ADVERT_INTERVAL. Utiliser un plus petit intervalle pour les annonces initiales augmente la probabilité de découverte rapide d'un routeur lorsqu'il devient disponible pour la première fois, en présence de pertes de paquet possibles.

Les informations contenues dans les annonces de routeur peuvent changer suite à des actions de gestion du système. Par exemple, la durée de vie des préfixes annoncés peut changer, de nouveaux préfixes peuvent être ajoutés, un routeur peut cesser d'être un routeur (c'est-à-dire, passer du statut de routeur à celui d'hôte), etc. Dans de tels cas, le routeur PEUT transmettre jusqu'à MAX_INITIAL_RTR_ADVERTISEMENTS annonces non sollicitées, en utilisant les mêmes règles que lorsque une interface devient une interface d'annonce.

6.2.5 Cesser d'être une interface d'annonce

Une interface peut cesser d'être une interface d'annonce, par des actions de la gestion du système telles que :
- changer le fanion AdvSendAdvertisements d'une interface activée de VRAI en FAUX, ou
- désactiver administrativement l'interface, ou
- fermer le système.

Dans de tels cas, le routeur DEVRAIT transmettre une ou plusieurs (mais pas plus que MAX_FINAL_RTR_ADVERTISEMENTS) annonces de routeur finales en diffusion groupée sur l'interface avec un champ Durée de vie de routeur de zéro. Dans le cas d'un routeur qui devient un hôte, le système DEVRAIT aussi quitter le groupe de diffusion groupée IP de Tous routeurs sur toutes les interfaces sur lesquelles le routeur prend en charge la diffusion groupée IP (que ces interfaces aient été ou non des interfaces d'annonce). De plus, l'hôte DOIT s'assurer que les messages Annonce de voisin envoyés ensuite de l'interface ont le fanion Routeur mis à zéro.

Noter que la gestion du système peut désactiver la capacité de transmission IP d'un routeur (c'est-à-dire, changer le système de routeur à hôte) une étape qui n'implique pas nécessairement que les interfaces du routeur cessent d'être des interfaces d'annonce. Dans de tels cas, les annonces de routeur suivantes DOIVENT régler le champ Durée de vie de routeur à zéro.

6.2.6 Traitement des sollicitations de routeur

Un hôte DOIT éliminer en silence tout message Sollicitation de routeur reçu.

En plus de l'envoi périodique d'annonces non sollicitées, un routeur envoie des annonces en réponse à des sollicitations valides reçues sur une interface d'annonce. Un routeur PEUT choisir d'envoyer la réponse en envoi individuel directement à l'adresse de l'hôte solliciteur (si l'adresse de source du solliciteur n'est pas l'adresse non spécifiée) mais le cas usuel est d'envoyer la réponse en diffusion groupée au groupe de Tous les nœuds. Dans ce dernier cas, le temporisateur d'intervalle de l'interface est remis à une nouvelle valeur aléatoire, comme si une annonce non sollicitée venait juste d'être envoyée (voir au paragraphe 6.2.4).

Dans tous les cas, les annonces de routeur envoyées en réponse à une sollicitation de routeur DOIVENT être retardées d'une durée aléatoire entre 0 et MAX_RA_DELAY_TIME secondes. (Si une seule annonce est envoyée en réponse à plusieurs sollicitations, le retard est par rapport à la première sollicitation.) De plus, les annonces de routeur consécutives envoyées à l'adresse de diffusion groupée Tous les nœuds DOIVENT être limitées en nombre à pas plus d'une annonce toutes les MIN_DELAY_BETWEEN_RAS secondes.

Un routeur peut traiter les sollicitations de routeur comme suit :

- À réception d'une sollicitation de routeur, calculer un délai aléatoire dans la gamme de 0 à MAX_RA_DELAY_TIME. Si la valeur calculée correspond à un instant postérieur à celui auquel l'envoi de la prochaine annonce de routeur en diffusion groupée est programmé, ignorer le délai aléatoire et envoyer l'annonce à l'instant déjà programmé.

- Si le routeur envoie une annonce de routeur en diffusion groupée (sollicitée ou non sollicitée) dans les dernières MIN_DELAY_BETWEEN_RAS secondes, programmer l'envoi de l'annonce à un instant correspondant à MIN_DELAY_BETWEEN_RAS, plus la valeur aléatoire, après l'envoi de la précédente annonce. Cela assure que le taux d'envoi des annonces de routeur en diffusion groupée est limité.

- Autrement, programmer l'envoi d'une annonce de routeur à l'instant donné par la valeur aléatoire.

Noter qu'il est permis à un routeur d'envoyer des annonces de routeur en diffusion groupée plus fréquemment qu'indiqué par la variable de configuration MinRtrAdvInterval pour autant que les annonces plus fréquentes soient des réponses aux sollicitations de routeur. Dans tous les cas cependant, des annonces en diffusion groupée non sollicitées NE DOIVENT PAS être envoyées plus fréquemment que ce qui est indiqué par MinRtrAdvInterval.

Les sollicitations de routeur dans lesquelles l'adresse de source est l'adresse non spécifiée NE DOIVENT PAS mettre à jour l'antémémoire de voisin du routeur ; les sollicitations avec une adresse de source propre mettent à jour l'antémémoire de voisin comme suit. Si le routeur a déjà une entrée d'antémémoire de voisin pour l'envoyeur de la sollicitation, la sollicitation contient une option Adresse de source de couche liaison, et l'adresse de couche liaison reçue diffère de celle qui est déjà dans l'antémémoire, l'adresse de couche liaison DEVRAIT être mise à jour dans l'entrée appropriée d'antémémoire de voisin, et son état d'accessibilité DOIT aussi être réglé à PÉRIMÉ. Si il n'y a pas d'entrée existante d'antémémoire de voisin pour l'envoyeur de la sollicitation, le routeur en crée une, installe l'adresse de couche liaison et règle son état d'accessibilité à PÉRIMÉ comme spécifié au paragraphe 7.3.3. Qu'une option Adresse de source de couche liaison soit fournie ou non, si une entrée d'antémémoire de voisin existe (ou est créée) pour l'envoyeur de la sollicitation, le fanion IsRouter de l'entrée DOIT être réglé à FAUX.

6.2.7 Cohérence des annonces de routeur

Les routeurs DEVRAIENT inspecter les annonces de routeur valides envoyées par les autres routeurs et vérifier qu'ils annoncent des informations cohérentes sur une liaison. Les incohérences détectées indiquent que un ou plusieurs routeurs pourraient être mal configurés et DEVRAIENT être signalés à la gestion du système ou du réseau. L'ensemble minimum des informations à vérifier comporte :

- Les valeurs de Limite de bonds actuelle (excepté pour la valeur non spécifiée de zéro).
- Les valeurs des fanions M ou O.
- Les valeurs de Durée d'accessibilité (excepté la valeur non spécifiée de zéro).
- Les valeurs du temporisateur de retransmission (excepté la valeur non spécifiée de zéro).
- Les valeurs de l'option MTU.
- Les durées de vie préférée et de validité pour le même préfixe. Si AdvPreferredLifetime et/ou AdvValidLifetime se décrémentent en temps réel comme spécifié au paragraphe 6.2.7, la comparaison des durées de vie ne peut pas comparer le contenu des champs dans l'annonce de routeur mais doit à la place comparer l'heure à laquelle le préfixe va devenir respectivement déconseillé et invalidé. Du fait du délai de propagation de la liaison et d'horloges éventuellement mal synchronisées entre les routeurs, une telle comparaison DEVRAIT permettre un certain biais temporel.

Noter que ce n'est pas une erreur que différents routeurs annoncent des ensembles de préfixes différents. Aussi, certains routeurs peuvent laisser certains champs non spécifiés, c'est-à-dire, avec la valeur zéro, alors que d'autres routeurs spécifient des valeurs. L'enregistrement d'erreurs DEVRAIT se restreindre aux conflits d'informations qui causent le passage des hôtes d'une valeur à une autre à chaque annonce reçue.

Toutes les autres actions à réception des messages d'annonce de routeur par un routeur sortent du domaine d'application de ce document.

6.2.8 Changement d'adresse de liaison locale

L'adresse de liaison locale sur un routeur devrait changer rarement, si elle le doit jamais. Les nœuds qui reçoivent les messages de découverte de voisin utilisent l'adresse de source pour identifier l'envoyeur. Si plusieurs paquets provenant du même routeur contiennent des adresses de source différentes, les nœuds vont supposer qu'ils viennent de routeurs différents, ce qui conduit à un comportement indésirable. Par exemple, un nœud va ignorer les messages Redirection dont il pense qu'ils ont été envoyés par un routeur autre que le routeur actuel de premier bond. Donc, l'adresse de source utilisée dans les annonces de routeur envoyées par un routeur particulier doit être identique à l'adresse cible dans un message Redirection lorsqu'elles redirigent sur ce routeur.

L'utilisation de l'adresse de liaison locale pour identifier de façon univoque les routeurs sur la liaison présente l'avantage que l'adresse par laquelle un routeur est connu ne devrait pas changer lorsque un site est dénuméroté.

Si un routeur change d'adresse de liaison locale pour une de ses interfaces, il DEVRAIT informer les hôtes de ce changement. Le routeur DEVRAIT envoyer en diffusion groupée quelques annonces de routeur à partir de la vieille adresse de liaison locale avec le champ Durée de vie de routeur réglé à zéro et également quelques annonces de routeur à partir de la nouvelle adresse de liaison locale. L'effet global devrait être le même que si une interface cesse d'être une interface d'annonce, et qu'une autre commence à être une interface d'annonce.

6.3 Spécification de l'hôte

6.3.1 Variables de configuration d'hôte

Aucune.

6.3.2 Variables d'hôte

Un hôte entretient un certain nombre de variables en rapport avec la découverte de voisin en plus des structures de données définies au paragraphe 5.1. Les noms spécifiques des variables ne sont utilisés que pour les besoins de la démonstration, et une mise en œuvre n'est pas obligée de les conserver, pour autant que le comportement externe soit cohérent avec celui décrit dans le présent document.

Ces variables ont des valeurs par défaut qui sont outrepassées par les informations reçues dans les messages Annonce de routeur. Les valeurs par défaut sont utilisées lorsque il n'y a pas de routeur sur la liaison ou lorsque toutes les Annonces de

routeur reçues ont laissé une valeur particulière non spécifiée.

Les valeurs par défaut dans la présente spécification peuvent être outrepassées par des documents spécifiques qui décrivent comment fonctionne IP sur les différentes couches de liaison. Cette règle permet à la découverte de voisin de fonctionner sur des liaisons avec des caractéristiques de performances très diverses.

Pour chaque interface :

LinkMTU MTU de la liaison.
Défaut : Valeur définie dans le document qui décrit comment fonctionne IPv6 sur la couche liaison particulière (par exemple, [RFC2464]).

CurHopLimit Limite de bond par défaut à utiliser lors de l'envoi de paquets IP (en envoi individuel).
Défaut : La valeur spécifiée dans la RFC "Numéros alloués" [RFC3232] en vigueur à la date de la mise en œuvre.

BaseReachableTime Valeur de base utilisée pour calculer la valeur aléatoire ReachableTime.
Défaut : REACHABLE_TIME millisecondes.

ReachableTime Durée pendant laquelle un voisin est considéré comme accessible après réception d'une confirmation d'accessibilité. Cette valeur devrait être une valeur aléatoire à distribution uniforme entre MIN_RANDOM_FACTOR et MAX_RANDOM_FACTOR multiplié par ReachableTime millisecondes. Une nouvelle valeur aléatoire devrait être calculée lorsque BaseReachableTime change (à cause d'une annonce de routeur) ou au moins toutes les quelques heures même si aucune annonce de routeur n'est reçue.

RetransTimer Temps entre les retransmissions de messages de sollicitation de voisin à un voisin lors de la résolution de l'adresse ou lors d'un sondage sur l'accessibilité d'un voisin.
Défaut : RETRANS_TIMER millisecondes

6.3.3 Initialisation de l'interface

L'hôte joint l'adresse de diffusion groupée Tous les nœuds sur les interfaces à capacité de diffusion groupée.

6.3.4 Traitement des Annonces de routeur reçues

Lorsque plusieurs routeurs sont présents, les informations annoncées collectivement par tous les routeurs peuvent être un sur-ensemble des informations contenues dans une seule annonce de routeur. De plus, les informations peuvent aussi être obtenues par d'autres moyens dynamiques, tels que l'autoconfiguration à états pleins. Les hôtes acceptent l'union de toutes les informations reçues ; la réception d'une annonce de routeur NE DOIT PAS invalider toutes les informations reçues dans une annonce précédente ou d'une autre source. Cependant, lorsque les informations reçues pour un paramètre spécifique (par exemple, la MTU de liaison) ou une option (par exemple, la durée de vie d'un préfixe spécifique) diffèrent de celles reçues antérieurement, et que le paramètre/option ne peut avoir qu'une seule valeur, les informations reçues les plus récentes sont considérées comme faisant autorité.

Un champ d'annonce de routeur (par exemple, Limite de bonds actuelle, Durée d'accessibilité et Temporisateur de retransmission) peut contenir une valeur marquée non spécifié. Dans ce cas, le paramètre devrait être ignoré et l'hôte devrait continuer d'utiliser la valeur qu'il utilise déjà. En particulier, un hôte NE DOIT PAS interpréter la valeur non spécifiée comme signifiant un retour à la valeur par défaut qui était en usage avant la réception de la première annonce de routeur. Cette règle empêche les hôtes de changer continuellement une variable interne lorsque un routeur annonce une valeur spécifique, mais que les autres routeurs annoncent la valeur non spécifiée.

À réception d'une annonce de routeur valide, un hôte extrait l'adresse de source du paquet et fait ce qui suit :

- Si l'adresse n'est pas déjà présente dans la liste des routeurs par défaut de l'hôte, et si la durée de vie de routeur de l'annonce est différente de zéro, créer une nouvelle entrée dans la liste, et initialiser sa valeur de temporisateur d'invalidation à partir du champ Durée de vie de routeur de l'annonce.

- Si l'adresse est déjà présente dans la liste des routeurs par défaut de l'hôte par suite d'une annonce reçue antérieurement, réinitialiser son temporisateur d'invalidation à la valeur de Durée de vie de routeur dans l'annonce nouvellement reçue.

- Si l'adresse est déjà présente dans la liste des routeurs par défaut de l'hôte et si la valeur de la durée de vie de routeur

est zéro, périmer immédiatement l'entrée comme spécifié au paragraphe 6.3.5.

Pour limiter la mémorisation nécessaire pour la liste des routeurs par défaut, un hôte PEUT choisir de ne pas mémoriser toutes les adresses de routeur découvertes via des annonces. Cependant, un hôte DOIT conserver au moins deux adresses de routeur et DEVRAIT en conserver plus. Les choix de routeurs par défaut sont effectués chaque fois que la communication avec une destination se révèle défaillante. Donc, plus il y a de routeurs sur la liste, plus il est probable qu'il sera possible de trouver rapidement un routeur de remplacement qui fonctionne (par exemple, sans avoir à attendre l'arrivée de la nouvelle annonce).

Si la valeur de limite de bonds actuelle reçue est différente de zéro, l'hôte DEVRAIT régler sa variable CurHopLimit à la valeur reçue.

Si la valeur de Durée d'accessibilité est différente de zéro, l'hôte DEVRAIT régler sa variable BaseReachableTime à la valeur reçue. Si la nouvelle valeur diffère de la valeur précédente, l'hôte DEVRAIT recalculer une nouvelle valeur aléatoire de ReachableTime. ReachableTime est calculée comme une valeur aléatoire à répartition uniforme entre MIN_RANDOM_FACTOR et MAX_RANDOM_FACTOR fois BaseReachableTime. Utiliser une composante aléatoire élimine la possibilité que les messages de détection d'inaccessibilité du voisin se synchronisent les uns avec les autres.

Dans la plupart des cas, la valeur de la durée d'accessibilité annoncée sera la même dans les annonces de routeur consécutives, et la BaseReachableTime d'un hôte change rarement. Dans ce cas, une mise en œuvre DEVRAIT s'assurer qu'une nouvelle valeur aléatoire est recalculée au moins une fois toutes les quelques heures.

La variable RetransTimer DEVRAIT être copiée du champ Temporisateur de retransmission si la valeur reçue est différente de zéro.

Après l'extraction des informations de la partie fixe du message Annonce de routeur, les options valides de l'annonce sont examinées. Si l'annonce contient une option Adresse de source de couche liaison, l'adresse de couche liaison DEVRAIT être enregistrée dans l'entrée d'antémémoire de voisin pour le routeur (en créant une entrée si nécessaire) et le fanion IsRouter dans l'entrée d'antémémoire de voisin DOIT être mis à VRAI. Si aucune adresse de source de couche liaison n'est incluse, mais s'il existe une entrée correspondante d'antémémoire de voisin, son fanion IsRouter DOIT être mis à VRAI. Le fanion IsRouter est utilisé par la détection d'inaccessibilité du voisin pour déterminer quand un routeur cesse d'être un hôte (c'est-à-dire, n'est plus capable de transmettre des paquets). Si une entrée d'antémémoire de voisin est créée pour le routeur, son état d'accessibilité DOIT être réglé à PÉRIMÉ comme spécifié au paragraphe 7.3.3. Si une entrée d'antémémoire existe déjà et si elle est mise à jour avec une adresse de couche liaison différente, l'état d'accessibilité DOIT aussi être réglé à PÉRIMÉ.

Si l'option MTU est présente, les hôtes DEVRAIENT copier la valeur de l'option dans LinkMTU pour autant que cette valeur soit supérieure ou égale à la MTU minimum de liaison [RFC2460] et ne dépasse pas la valeur de LinkMTU par défaut spécifiée dans le document spécifique du type de liaison (par exemple, [RFC2464]).

Les options Informations de préfixe qui ont le fanion "en liaison" (L) établi indiquent un préfixe qui identifie une gamme d'adresses qui devraient être considérées comme en liaison. Noter cependant, qu'une option Informations de préfixe avec le fanion en liaison mis à zéro ne porte pas d'information concernant la détermination de en liaison et NE DOIT PAS être interprétée comme signifiant que les adresses couvertes par le préfixe sont hors liaison. Le seul moyen d'annuler une précédente indication en liaison est d'annoncer ce préfixe avec le bit L établi et la Durée de vie réglée à zéro. Le comportement par défaut (voir au paragraphe 5.2) lors de l'envoi d'un paquet à une adresse pour laquelle aucune information sur le statut en liaison de l'adresse n'est connu est de transmettre le paquet à un routeur par défaut ; la réception d'une option Informations de préfixe avec le fanion "en liaison" (L) mis à zéro ne change pas ce comportement. La raison pour laquelle une adresse est traitée comme en liaison est spécifiée dans la définition de "en liaison" au paragraphe 2.1. Les préfixes avec le fanion en liaison mis à zéro auront normalement le fanion Autonome établi et seront utilisés par la [RFC4862].

Pour chaque option Informations de préfixe avec le fanion en liaison établi, un hôte fait ce qui suit :

- Si le préfixe est le préfixe de liaison locale, il ignore en silence l'option Informations de préfixe.

- Si le préfixe n'est pas déjà présent dans la liste des préfixes, et si le champ Durée de validité de l'option Informations de préfixe est différent de zéro, créer une nouvelle entrée pour le préfixe et initialiser son temporisateur d'invalidation à la valeur de Durée de validité dans l'option Informations de préfixe.

- Si le préfixe est déjà présent dans la liste des préfixes de l'hôte par suite d'une annonce reçue antérieurement, remettre son temporisateur d'invalidation à la valeur de Durée de validité dans l'option Informations de préfixe. Si la nouvelle valeur de durée de vie est zéro, périmer immédiatement le préfixe (voir au paragraphe 6.3.5).

- Si le champ Durée de validité de l'option Informations de préfixe est à zéro, et si le préfixe n'est pas présent dans la liste des préfixes de l'hôte, ignorer l'option en silence.

L'autoconfiguration d'adresse sans état [RFC4862] peut dans certaines circonstances utiliser une plus grande durée de validité d'un préfixe ou l'ignorer complètement afin d'empêcher une attaque de déni de service particulière. Cependant, comme l'effet de la même attaque de déni de service ciblée sur la liste de préfixes en liaison n'est pas catastrophique (les hôtes enverraient des paquets à un routeur par défaut et recevraient une redirection plutôt que d'envoyer les paquets directement à un voisin) le protocole de découverte de voisin n'impose pas une telle vérification des valeurs de durée de vie de préfixe. De même, la [RFC4862] peut imposer certaines restrictions à la longueur des préfixes pour les besoins de la configuration d'adresse. Donc, le préfixe peut être rejeté par une mise en œuvre de [RFC4862] chez l'hôte. Cependant, la longueur de préfixe est encore valide pour la détermination de en liaison lorsque elle est combinée avec d'autres fanions dans l'option de préfixe.

Note : Les mises en œuvre peuvent choisir de traiter les aspects en liaison des préfixes séparément de ceux de l'autoconfiguration d'adresse des préfixes en passant, par exemple, une copie de chaque message valide d'annonce de routeur à la fois à la fonction "en liaison" et à une fonction "addrconf". Chaque fonction peut alors opérer indépendamment sur les préfixes qui ont le fanion approprié établi.

6.3.5 Péremption des préfixes et des routeurs par défaut

Chaque fois que le temporisateur d'invalidation arrive à expiration pour une entrée de liste de préfixes, cette entrée est éliminée. Aucune entrée existante d'antémémoire de destination n'a cependant besoin d'être mise à jour. Si un problème d'accessibilité survient avec une entrée existante d'antémémoire de voisin, la détection d'inaccessibilité du voisin va effectuer la récupération nécessaire.

Chaque fois que la durée de vie d'une entrée de la liste des routeurs par défaut arrive à expiration, cette entrée est éliminée. Lors du retrait d'un routeur de la liste des routeurs par défaut, le nœud DOIT mettre à jour l'antémémoire de destination d'une façon telle que toutes les entrées qui utilisent le routeur effectuent à nouveau la détermination du prochain bond plutôt que de continuer à envoyer du trafic au routeur (supprimé).

6.3.6 Choix du routeur par défaut

L'algorithme de sélection de routeur dépend en partie de ce qu'un routeur est connu ou non comme accessible. Les détails exacts de la façon dont un nœud garde trace de l'état d'accessibilité d'un voisin sont traités au paragraphe 7.3. L'algorithme de sélection d'un routeur par défaut est invoqué durant la détermination du prochain bond lorsque aucune entrée d'antémémoire de destination n'existe pour une destination hors liaison ou lorsque la communication à travers un routeur existant paraît défaillante. Dans des conditions normales, un routeur sera choisi la première fois que du trafic est envoyé à une destination, le trafic ultérieur pour cette destination utilisant le même routeur qu'indiqué dans l'antémémoire de destination modulo tout changement de l'antémémoire de destination causé par les messages Redirection.

La politique pour le choix de routeurs à partir de la liste des routeurs par défaut est la suivante :

1) Les routeurs qui sont accessibles ou probablement accessibles (c'est-à-dire, dans tout état autre que INCOMPLET) DEVRAIENT être préférés aux routeurs dont l'accessibilité est inconnue ou suspecte (c'est-à-dire, dans l'état INCOMPLET, ou pour lesquels n'existe aucune entrée d'antémémoire de voisin). Une mise en œuvre peut choisir de toujours retourner le même routeur ou cycle à travers la liste de routeurs à la façon d'un round-robin pour autant qu'elle retourne toujours un routeur accessible ou probablement accessible quand il en est un disponible.

2) Lorsque la liste ne comporte aucun routeur connu pour être accessible ou probablement accessible, les routeurs DEVRAIENT être choisis à la façon d'un round-robin, afin que les demandes suivantes d'un routeur par défaut ne retournent pas le même routeur jusqu'à ce que tous les autres routeurs aient été choisis.

   Le passage cyclique parmi la liste des routeurs assure dans ce cas que tous les routeurs disponibles sont activement sondés par l'algorithme de détection d'inaccessibilité du voisin. Une demande de routeur par défaut est faite en conjonction avec l'envoi d'un paquet à un routeur, et le routeur choisi va être sondé sur son accessibilité par un effet collatéral.

3) Si la liste de routeurs par défaut est vide, on suppose que toutes les destinations sont en liaison comme spécifié au paragraphe 5.2.

6.3.7 Envoi des sollicitations de routeur

Lorsque une interface est activée, un hôte peut ne pas vouloir attendre que la prochaine annonce de routeur non sollicitée localise les routeurs par défaut ou les préfixes appris. Pour obtenir rapidement des annonces de routeur, un hôte DEVRAIT transmettre jusqu'à MAX_RTR_SOLICITATIONS messages de sollicitation de routeur, chacun séparé par au moins RTR_SOLICITATION_INTERVAL secondes. Les sollicitations de routeur peuvent être envoyées après un des événements suivants :

- L'interface est initialisée au moment du démarrage du système.
- L'interface est réinitialisée après une défaillance temporaire ou après une désactivation temporaire par la gestion du système.
- Le système change de routeur à hôte, en ayant sa capacité de transmission IP désactivée par la gestion du système.
- L'hôte se rattache à une liaison pour la première fois.
- l'hôte se ré-attache à une liaison après avoir été détaché pendant un certain temps.

Un hôte envoie des sollicitations de routeur à l'adresse de diffusion groupée Tous les routeurs. L'adresse IP de source est réglée à une des adresses d'envoi individuel de l'interface ou à l'adresse non spécifiée. L'option Adresse de source de couche liaison DEVRAIT être réglée à l'adresse de couche liaison de l'hôte, si l'adresse IP de source n'est pas l'adresse non spécifiée.

Avant qu'un hôte n'envoie une sollicitation initiale, il DEVRAIT retarder la transmission d'une durée aléatoire comprise entre 0 et MAX_RTR_SOLICITATION_DELAY. Cela sert à alléger l'encombrement lorsque de nombreux hôtes démarrent en même temps sur une liaison, comme cela peut arriver après récupération suite à une panne d'alimentation. Si un hôte a déjà attendu pendant un délai aléatoire depuis que l'interface a été (ré)-activée (par exemple, au titre d'une détection de duplication d'adresse [RFC4862]) il n'est pas nécessaire de respecter encore un délai avant d'envoyer le premier message Sollicitation de routeur.

Dans certains cas, le délai aléatoire PEUT être omis si nécessaire. Par exemple, un nœud mobile, utilisant la [RFC3775], qui passe à une nouvelle liaison aura besoin de découvrir un tel mouvement aussitôt que possible pour minimiser la quantité de paquets perdus à la suite du changement dû à son mouvement topologique. Les sollicitations de routeur fournissent un outil utile pour la détection de mouvement dans IPv6 mobile car elles permettent aux nœuds mobiles de déterminer le mouvement vers de nouvelles liaisons. Et donc, si un nœud mobile reçoit des informations de couche liaison qui indiquent qu'un mouvement pourrait avoir eu lieu, il PEUT envoyer immédiatement une sollicitation de routeur sans retard aléatoire. La force de telles indications devrait être affirmée par la mise en œuvre de nœud mobile en fonction du niveau de certitude des indications de couche de liaison, et elle sort du domaine d'application de la présente spécification. Noter que l'utilisation inappropriée de ce mécanisme (par exemple, fondée sur des indications faibles ou temporaires) peut résulter en tempêtes de sollicitations de routeur. De plus, la mobilité simultanée d'un grand nombre de nœuds mobiles utilisant ce mécanisme peut résulter en l'envoi simultané d'un grand nombre de sollicitations.

Une fois que l'hôte a envoyé une sollicitation de routeur, et a reçu une annonce de routeur valide avec une durée de vie de routeur différente de zéro, l'hôte DOIT s'abstenir d'envoyer des sollicitations supplémentaires sur cette interface, jusqu'à la prochaine occurrence d'un des événements ci-dessus. De plus, un hôte DEVRAIT envoyer au moins une sollicitation dans le cas où une annonce est reçue avant qu'il ait envoyé une sollicitation. Les réponses aux annonces sollicitées peuvent contenir plus d'informations que les annonces non sollicitées.

Si un hôte envoie MAX_RTR_SOLICITATIONS sollicitations, et ne reçoit pas d'annonce de routeur après avoir attendu MAX_RTR_SOLICITATION_DELAY secondes après l'envoi de la dernière sollicitation, l'hôte conclut qu'il n'y a pas de routeur sur la liaison pour les besoins de la [RFC4862]. Cependant, l'hôte continue de recevoir et traiter les messages d'annonces de routeur pour le cas où des routeurs apparaîtraient sur la liaison.

7. Résolution d'adresse et détection d'inaccessibilité du voisin

Cette section décrit les fonctions qui se rapportent aux messages Sollicitation de voisin et Annonce de voisin et inclut les descriptions des algorithmes de résolution d'adresse et de détection d'inaccessibilité du voisin.

Les messages Sollicitation et Annonce de voisin sont aussi utilisés pour la détection d'adresse dupliquée telle que spécifiée par la [RFC4862]. En particulier, la détection d'adresse dupliquée envoie des messages Sollicitation de voisin avec une adresse de source non spécifiée ciblant sa propre "tentative" d'adresse. De tels messages déclanchent la réponse des nœuds qui utilisent déjà l'adresse avec une Annonce de voisin en diffusion groupée qui indique que l'adresse est utilisée.

7.1 Validation de message

7.1.1 Validation de Sollicitation de voisins

Un nœud DOIT éliminer en silence tous les messages Sollicitation de voisin reçus qui ne satisfont pas à toutes les vérifications de validité suivantes :

- Le champ Limite de bonds IP a une valeur de 255, c'est-à-dire, le paquet n'a pas pu être transmis par un routeur.
- Si le message comporte un en-tête IP Authentification, le message s'authentifie correctement.
- La somme de contrôle ICMP est valide.
- Le code ICMP est 0.
- La longueur ICMP (déduite de la longueur IP) est au moins de 24 octets.
- l'adresse cible n'est pas une adresse de diffusion groupée.
- Toutes les options incluses ont une longueur supérieure à zéro.
- Si l'adresse IP de source est l'adresse non spécifiée, l'adresse IP de destination est une adresse en diffusion groupée de nœud sollicité.
- Si l'adresse IP de source est l'adresse non spécifiée, il n'y a pas d'option d'adresse de couche liaison de source dans le message.

Le contenu du champ Réservé, et de toute option non reconnue, DOIT être ignoré. De plus,les changements rétro compatibles au protocole pourraient spécifier le contenu du champ Réservé ou ajouter de nouvelles options ; les changements non rétro compatibles pourront seulement utiliser des valeurs de code différentes.

Le contenu de toute option définie dont l'utilisation n'est pas spécifiée avec les messages Sollicitation de voisin DOIT être ignoré et le paquet traité normalement. La seule option définie qui peut apparaître est l'option Adresse de source de couche liaison.

Une Sollicitation de voisin qui réussit aux vérifications de validité est appelée une " sollicitation valide".

7.1.2 Validation de Annonce de voisins

Un nœud DOIT éliminer en silence tout message d'annonce de voisin reçu qui ne satisfait pas à toutes les vérifications de validité suivantes :

- Le champ Limite de bonds IP a une valeur de 255, c'est-à-dire, le paquet ne pourrait pas avoir été transmis par un routeur.
- La somme de contrôle ICMP est valide.
- Le code ICMP est 0.
- La longueur ICMP (déduite de la longueur IP) est de 24 octets ou plus.
- L'adresse cible n'est pas une adresse de diffusion groupée.
- Si l'adresse IP de destination est une adresse de diffusion groupée, le fanion Sollicité est à zéro.
- Toutes les options incluses ont une longueur supérieure à zéro.

Le contenu du champ Réservé, et de toute option non reconnue, DOIT être ignoré. De futurs changements rétro compatibles au protocole pourraient spécifier le contenu du champ Réservé ou ajouter de nouvelles options ; des changements rétro-incompatibles pourraient utiliser des valeurs de code différentes.

Le contenu de toute option définie qui n'est pas spécifié pour être utilisé avec les messages d'annonce de voisin DOIT être ignoré et le paquet traité normalement. La seule option définie qui peut apparaître est l'option Adresse cible de couche liaison.

Une annonce de voisin qui réussit les vérifications de validité est appelée une "annonce valide".

7.2 Résolution d'adresse

La résolution d'adresse est le processus par lequel un nœud détermine l'adresse de couche liaison d'un voisin étant donnée son adresse IP seulement. La résolution d'adresse est effectuée seulement sur les adresses qui sont déterminées comme étant en liaison et pour lesquelles l'envoyeur ne connaît pas l'adresse de couche liaison correspondante (voir au paragraphe 5.2). La résolution d'adresse n'est jamais effectuée sur les adresses de diffusion groupée.

Il est possible qu'un hôte reçoive un message de sollicitation, d'annonce de routeur, ou de redirection sans qu'une option d'adresse de couche liaison soit incluse. Ces messages NE DOIVENT PAS créer ou mettre à jour des entrées d'antémémoire de voisin, sauf par rapport au fanion IsRouter comme spécifié aux paragraphes 6.3.4 et 7.2.5. Si il n'existe

pas d'entrée d'antémémoire de voisin pour la source d'un tel message, la résolution d'adresse sera requise avant que les communications en envoi individuel ne puissent commencer avec cette adresse. Ceci est particulièrement pertinent pour les réponses en envoi individuel aux sollicitations lorsque un échange de paquet supplémentaire est nécessaire pour annoncer la livraison.

7.2.1 Initialisation d'interface

Lorsque une interface à capacité de diffusion groupée est activée, le nœud DOIT joindre l'adresse de diffusion groupée Tous les nœuds sur cette interface, ainsi que l'adresse de diffusion groupée du nœud sollicité correspondant à chacune des adresses IP allouées à l'interface.

L'ensemble des adresses IP allouées à une interface peut changer avec le temps. De nouvelles adresses peuvent être ajoutées et de vieilles adresses peuvent être supprimées [RFC4862]. Dans de tels cas, le nœud DOIT joindre et quitter l'adresse de diffusion groupée du nœud sollicité correspondant respectivement aux nouvelles et anciennes adresses. Joindre l'adresse de diffusion groupée du nœud sollicité se fait en utilisant des protocoles de découverte d'écoutant de diffusion groupée tels que de la [RFC2710] ou de la [RFC3810]. Noter que plusieurs adresses d'envoi individuel peuvent se transposer en la même adresse de diffusion groupée du nœud sollicité ; un nœud NE DOIT PAS quitter le groupe de diffusion groupée du nœud sollicité jusqu'à ce que toutes les adresses allouées correspondant à cette adresse de diffusion groupée aient été retirées.

7.2.2 Envoi de Sollicitation de voisins

Lorsque un nœud a un paquet en envoi individuel à envoyer à un voisin, mais qu'il ne connaît pas l'adresse de couche de liaison du voisin, il effectue une résolution d'adresse. Pour les interfaces à capacité de diffusion groupée, cela implique de créer une entrée d'antémémoire de voisins dans l'état INCOMPLET et de transmettre un message Sollicitation de voisin ciblé sur le voisin. La sollicitation est envoyée à l'adresse de diffusion groupée de nœud sollicité correspondant à l'adresse cible.

Si l'adresse de source du paquet qui invite à la sollicitation est la même qu'une des adresses allouées à l'interface sortante, cette adresse DEVRAIT être placée dans Adresse IP de source de la sollicitation sortante. Autrement, toute adresse allouée à l'interface devrait être utilisée. Utiliser l'adresse de source du paquet invitant lorsque possible assure que le receveur de la sollicitation de voisin installe dans son antémémoire de voisins l'adresse IP qui va très vraisemblablement être utilisée dans le trafic de retour ultérieur qui appartient à la "connexion" du paquet invitant.

Si la sollicitation est envoyée à une adresse de diffusion groupée de nœud sollicité, l'envoyeur DOIT inclure son adresse de couche liaison (si il en a une) comme option Adresse de source de couche liaison. Autrement, l'envoyeur DEVRAIT inclure son adresse de couche liaison (si il en a une) comme option Adresse de source de couche liaison. Inclure l'adresse de source de couche liaison dans une sollicitation en diffusion groupée est nécessaire pour donner à la cible une adresse à laquelle elle puisse envoyer l'annonce de voisin. Sur les sollicitations en envoi individuel, une mise en œuvre PEUT omettre l'option Adresse de source de couche liaison. L'hypothèse ici est que si l'envoyeur a une adresse de couche liaison de l'homologue dans son antémémoire, il est hautement probable que l'homologue va aussi avoir une entrée pour l'envoyeur dans son antémémoire. Par conséquent, il n'y a pas besoin de l'envoyer.

Tout en attendant que s'achève la résolution d'adresse, l'envoyeur DOIT, pour chaque voisin, conserver une petite file d'attente de paquets qui attendent la fin de la résolution d'adresse. La file d'attente DOIT contenir au moins un paquet, et PEUT en contenir plus. Cependant, le nombre de paquets mis en file d'attente par voisin DEVRAIT être limité à une valeur faible. Lorsque une file d'attente déborde, le nouvel arrivant DEVRAIT remplacer la plus ancienne entrée. Une fois achevée la résolution d'adresse, le nœud transmet tous les paquets mis en file d'attente.

Tout en attendant une réponse, l'envoyeur DEVRAIT retransmettre les messages de sollicitation de voisin approximativement toutes les RetransTimer millisecondes, même en l'absence de trafic supplémentaire vers le voisin. Le taux de retransmissions DOIT être limité à au plus une sollicitation par voisin toutes les RetransTimer millisecondes.

Si aucune annonce de voisin n'est reçue après MAX_MULTICAST_SOLICIT sollicitations, la résolution d'adresse a échoué. L'envoyeur DOIT retourner l'indication ICMP Destination injoignable avec le code 3 (Adresse injoignable) pour chaque paquet en file d'attente qui attendait la résolution d'adresse.

7.2.3 Réception des sollicitations de voisin

Une sollicitation de voisin valide qui ne satisfait pas à une des exigences suivantes DOIT être éliminée en silence :

- L'adresse cible est une adresse d'envoi individuel ou d'envoi à la cantonade "valide" allouée à l'interface de réception [RFC4862],
- L'adresse cible est une adresse d'envoi individuel pour laquelle le nœud offre un service de mandataire, ou

- L'adresse cible est une "tentative" d'adresse sur laquelle la détection d'adresse dupliquée est en cours [RFC4862].

Si l'adresse cible est une tentative, la sollicitation de voisin devrait être traitée comme décrit dans la [RFC4862]. Autrement, la description suivante s'applique. Si l'adresse de source n'est pas l'adresse inspécifiée, et si sur les couches en liaison qui ont des adresses, la sollicitation comporte une option Adresse de source de couche liaison, le receveur DEVRAIT alors créer ou mettre à jour l'entrée d'antémémoire de voisin pour l'adresse IP de source de la sollicitation. Si il n'existe pas encore une entrée, le nœud DEVRAIT en créer une nouvelle et régler son état d'accessibilité à PÉRIMÉ comme spécifié au paragraphe 7.3.3. Si il existe déjà une entrée, et si l'adresse de couche liaison en antémémoire diffère de celle de l'option couche liaison de source reçue, l'adresse de l'antémémoire devrait être remplacée par l'adresse reçue et l'état d'accessibilité de l'entrée DOIT être réglé à PÉRIMÉ.

Si une entrée d'antémémoire de voisins est créée, le fanion IsRouter DEVRAIT être réglé à FAUX. Ce sera le cas même si la sollicitation de voisin est envoyée par un routeur car les messages Sollicitation de voisin ne contiennent pas d'indication de ce que l'envoyeur est ou non un routeur. Dans le cas où l'envoyeur est un routeur, les messages suivants d'annonce de voisin ou d'annonce de routeur vont régler IsRouter à la valeur correcte. Si une entrée d'antémémoire de voisins existe déjà, son fanion IsRouter NE DOIT PAS être modifié.

Si l'adresse de source est l'adresse inspécifiée, le nœud NE DOIT PAS créer ou mettre à jour l'entrée d'antémémoire de voisins.

Après toutes les mises à jour de l'antémémoire de voisins, le nœud envoie une réponse d'annonce de voisin comme décrit au paragraphe suivant.

7.2.4 Envoi d'Annonce de voisins sollicitée

Un nœud envoie une annonce de voisin en réponse à une sollicitation de voisin valide qui cible une des adresses allouées du nœud. L'adresse cible de l'annonce est copiée de l'adresse cible de la sollicitation. Si l'adresse IP de destination de la sollicitation n'est pas une adresse de diffusion groupée, l'option Adresse cible de couche liaison PEUT être omise ; la valeur en antémémoire du nœud voisin doit déjà être en cours pour que la sollicitation ait été reçue. Si l'adresse IP de destination de la sollicitation est une adresse de diffusion groupée, l'option Couche liaison cible DOIT être incluse dans l'annonce. De plus, si le nœud est un routeur, il DOIT régler le fanion Routeur à un ; autrement, il DOIT régler le fanion à zéro.

Si l'adresse cible est une adresse à la cantonade ou une adresse en envoi individuel pour laquelle le nœud fournit un service de mandataire, ou si l'option Adresse cible de couche liaison n'est pas incluse, le fanion Outrepasser DEVRAIT être réglé à zéro. Autrement, le fanion Outrepasser DEVRAIT être mis à un. Le réglage correct du fanion Outrepasser assure que les nœuds donnent la préférence aux annonces qui ne viennent pas de mandataires, même lorsque elles sont reçues après les annonces de mandataires, et assure aussi que la première annonce pour une adresse à la cantonade "gagne".

Si la source de la sollicitation est l'adresse inspécifiée, le nœud DOIT régler le fanion Sollicité à zéro et envoyer en diffusion groupée l'annonce à l'adresse Tous les nœuds. Autrement, le nœud DOIT régler le fanion Sollicité à un et envoyer l'annonce en envoi individuel à l'adresse de source de la sollicitation.

Si l'adresse cible est une adresse à la cantonade, l'envoyeur DEVRAIT retarder l'envoi d'une réponse d'un délai aléatoire entre 0 et MAX_ANYCAST_DELAY_TIME secondes.

Comme il n'est pas obligé que les sollicitations de voisin en envoi individuel comportent une adresse de source de couche liaison, il est possible qu'un nœud qui envoie une annonce de voisin sollicitée n'ait pas d'adresse de couche liaison correspondante pour son voisin dans son antémémoire de voisins. Dans une telle situation, un nœud devra d'abord utiliser la découverte de voisin pour déterminer l'adresse de couche liaison de son voisin (c'est-à-dire, envoyer une sollicitation de voisin en diffusion groupée).

7.2.5 Réception d'annonce de voisins

Lorsque une annonce de voisin valide est reçue (sollicitée ou non sollicitée) on cherche l'entrée de la cible dans l'antémémoire de voisins. Si il n'existe pas d'entrée, l'annonce DEVRAIT être éliminée en silence. Il n'est pas nécessaire de créer une entrée s'il n'en existe pas, car le receveur n'a apparemment pas initié de communication avec la cible.

Une fois que l'entrée d'antémémoire de voisins appropriée a été localisée, les actions spécifiques entreprises dépendent de l'état de l'entrée d'antémémoire de voisins, des fanions dans l'annonce et de l'adresse de couche liaison réelle fournie.

Si l'entrée d'antémémoire de voisins de la cible n'est pas dans l'état INCOMPLET lorsque l'annonce est reçue, une de deux

choses peuvent arriver. Si la couche de liaison a des adresses et si une option Adresse cible de couche liaison n'est pas incluse, le nœud receveur DEVRAIT éliminer en silence l'annonce reçue. Autrement, le nœud receveur effectue les étapes suivantes :

- Il enregistre l'adresse de couche liaison dans l'entrée d'antémémoire de voisins.
- Si le fanion Sollicité de l'annonce est établi, l'état de l'entrée est réglé à ACCESSIBLE, autrement, à PÉRIMÉ.
- Il règle le fanion IsRouter dans l'entrée d'antémémoire sur la base du fanion Routeur de l'annonce reçue.
- Il envoie tous les paquets en file d'attente pour le voisin qui attendaient la résolution d'adresse.

Noter que le fanion Outrepasser est ignoré si l'entrée est dans l'état INCOMPLET.

Si l'entrée d'antémémoire de voisins de la cible est dans un état autre que INCOMPLET lorsque l'annonce est reçue, les actions suivantes ont lieu :

I. Si le fanion Outrepasser est à zéro et si l'adresse de couche liaison fournie diffère de celle de l'antémémoire, une des deux actions suivantes a lieu :
   a) si l'état de l'entrée est ACCESSIBLE, la régler à PÉRIMÉ, mais ne pas mettre à jour l'entrée de quelque autre façon,
   b) autrement, l'annonce reçue devrait être ignorée et NE DOIT PAS mettre à jour l'antémémoire.

II Si le fanion Outrepasser est établi, ou si l'adresse de couche liaison fournie est la même que celle de l'antémémoire, ou si aucune option d'adresse cible de couche liaison n'est fournie, l'annonce reçue DOIT mettre à jour l'entrée d'antémémoire de voisins comme suit :
   - L'adresse de couche liaison dans l'option Adresse cible de couche liaison DOIT être insérée dans l'antémémoire (si il en est une de fournie et si elle est différente de l'adresse déjà enregistrée).
   - Si le fanion Sollicité est établi, l'état de l'entrée DOIT être réglé à ACCESSIBLE. Si le fanion Sollicité est à zéro et si l'adresse de couche liaison a été mise à jour avec une adresse différente, l'état DOIT être réglé à PÉRIMÉ. Autrement, l'état de l'entrée reste inchangé. Le fanion Sollicité d'une annonce ne devrait être établi que si l'annonce est une réponse à une sollicitation de voisin. Comme les sollicitations de détection d'inaccessibilité du voisin sont envoyées à l'adresse de couche liaison de l'antémémoire, la réception d'une annonce sollicitée indique que le chemin de transmission fonctionne. La réception d'une annonce non sollicitée peut cependant indiquer qu'un voisin a des informations urgentes à annoncer (par exemple, un changement d'adresse de couche liaison). Si les informations urgentes indiquent un changement de ce qu'un nœud utilise actuellement, le nœud devrait vérifier l'accessibilité du chemin (nouveau) lorsque il envoie le prochain paquet. Il n'est pas nécessaire de mettre à jour l'état pour les annonces non sollicitée qui ne changent pas le contenu de l'antémémoire.
   - Le fanion IsRouter de l'entrée d'antémémoire DOIT être réglé conformément au fanion Routeur de l'annonce reçue. Dans le cas où le fanion IsRouter change de VRAI à FAUX par suite de cette mise à jour, le nœud DOIT retirer ce routeur de la liste des routeurs par défaut et mettre à jour les entrées d'antémémoire de destination pour toutes les destinations qui utilisent ce voisin comme routeur, comme spécifié au paragraphe 7.3.3. Ceci est nécessaire pour détecter quand un nœud qui est utilisé comme routeur arrête de transmettre des paquets du fait qu'il est configuré comme hôte.

Les règles ci-dessus assurent que l'antémémoire est mise à jour quand l'annonce de voisin prend la préséance (c'est-à-dire, quand le fanion Outrepasser est établi) ou quand l'annonce de voisin se réfère à la même adresse de couche liaison que celle qui est actuellement enregistrée dans l'antémémoire. Si aucune des conditions ci-dessus ne s'applique, l'annonce invite à une future détection d'inaccessibilité du voisin (si elle n'est déjà en cours) en changeant l'état de l'entrée d'antémémoire.

7.2.6 Envoi non sollicité d'annonce de voisins

Dans certains cas, un nœud peut être capable de déterminer que son adresse de couche liaison a changé (par exemple, un changement à chaud sur une carte d'interface) et peut souhaiter informer rapidement ses voisins de la nouvelle adresse de couche liaison. Dans un tel cas, un nœud PEUT envoyer jusqu'à MAX_NEIGHBOR_ADVERTISEMENT messages non sollicités d'annonce de voisin à l'adresse de diffusion groupée Tous les nœuds. Ces annonces DOIVENT être séparées par au moins RetransTimer secondes.

Le champ Adresse cible de l'annonce non sollicitée est réglé à une adresse IP de l'interface, et l'option Adresse cible de couche liaison est remplie avec la nouvelle adresse de couche liaison. Le fanion Sollicité DOIT être réglé à zéro, afin d'éviter toute confusion à l'algorithme de détection d'inaccessibilité du voisin. Si le nœud est un routeur, il DOIT régler le fanion Routeur à un ; autrement, il DOIT le régler à zéro. Le fanion Outrepasser PEUT être réglé à zéro ou un. Dans l'un et l'autre cas, les nœuds voisins vont immédiatement changer l'état de leurs entrées d'antémémoire de voisins pour l'adresse cible en PÉRIMÉ, les invitant à vérifier l'accessibilité du chemin. Si le fanion Outrepasser est réglé à un, les nœuds voisins vont installer la nouvelle adresse de couche liaison dans leurs antémémoires. Autrement, ils vont ignorer la nouvelle adresse de couche liaison, choisissant plutôt de sonder l'adresse de l'antémémoire.

Un nœud qui a plusieurs adresses IP allouées à une interface PEUT envoyer en diffusion groupée une annonce de voisin

séparée pour chaque adresse. Dans un tel cas, le nœud DEVRAIT introduire un petit délai entre l'envoi de chaque annonce pour réduire la probabilité que les annonces se perdent à cause de l'encombrement.

Un mandataire PEUT envoyer en diffusion groupée une annonce de voisins lorsque son adresse de couche liaison change ou quand il est configuré (par la gestion du système ou d'autres mécanismes) en mandataire pour une adresse. Si il y a plusieurs nœuds qui fournissent les services de mandataire pour le même ensemble d'adresses, les mandataires devraient fournir un mécanisme qui empêche plusieurs mandataires pour les annonces en diffusion groupée pour une adresse, afin de réduire le risque d'un trafic de diffusion groupée excessif. C'est une exigence pour les autres protocoles qui ont besoin d'utiliser des mandataires pour les annonces de voisins. Un exemple d'un nœud qui effectue des annonces par mandataire est l'agent de rattachement spécifié dans la [RFC3775].

Aussi, un nœud qui appartient à une adresse d'envoi à la cantonade PEUT envoyer en diffusion groupée des annonces de voisins non sollicitées pour l'adresse à la cantonade lorsque change l'adresse de couche liaison du nœud.

Noter que comme les annonces de voisins non sollicitées ne mettent pas à jour de façon fiable les antémémoires dans tous les nœuds (les annonces peuvent n'être pas reçues par tous les nœuds) elles ne devraient être vues que comme une optimisation des performances pour mettre rapidement à jour les antémémoires chez la plupart des voisins. L'algorithme de détection d'inaccessibilité du voisin assure que tous les nœuds obtiennent une adresse de couche liaison accessible, bien que le délai puisse être un peu plus long.

7.2.7 Envoi d'annonce de voisin à la cantonade

Du point de vue de la découverte de voisin, les adresses d'envoi à la cantonade sont traitées dans la plupart des cas exactement comme les adresses en envoi individuel. Comme une adresse à la cantonade est syntaxiquement la même qu'une adresse d'envoi individuel, les nœuds qui effectuent la résolution d'adresse ou la détection d'inaccessibilité du voisin sur une adresse à la cantonade la traitent comme si elle était une adresse d'envoi individuel. Elle ne donne lieu à aucune traitement particulier.

Les nœuds qui ont une adresse d'envoi à la cantonade allouée à une interface la traitent exactement de la même façon que si elle était une adresse d'envoi individuel avec deux exceptions. D'abord, l'annonce de voisins envoyée en réponse à une sollicitation de voisin DEVRAIT être retardée d'une durée aléatoire de 0 à MAX_ANYCAST_DELAY_TIME pour réduire la probabilité d'encombrement du réseau. Ensuite, le fanion Outrepasser dans l'annonce de voisins DEVRAIT être à 0, afin que lorsque plusieurs annonces sont reçues, la première annonce reçue soit utilisée plutôt que la dernière.

Comme avec les adresses en envoi individuel, la détection d'inaccessibilité du voisin assure qu'un nœud détecte rapidement lorsque le lien actuel pour une adresse d'envoi à la cantonade devient invalide.

7.2.8 Mandataire d'Annonce de voisins

Dans des circonstances particulières, un routeur PEUT être mandataire pour un ou plusieurs autres nœuds, c'est-à-dire, indiquer par une annonce de voisins qu'il acceptera des paquets non explicitement adressés à lui-même. Par exemple, un routeur pourrait accepter des paquets au nom d'un nœud mobile qui est passé hors liaison. Les mécanismes utilisés par le mandataire sont identiques à ceux utilisés avec les adresses d'envoi à la cantonade.

Un mandataire DOIT joindre la ou les adresses de diffusion groupée de nœud sollicité qui correspondent à la ou aux adresses IP allouées au nœud dont il est le mandataire.

Tous les messages d'annonce de voisin mandataire sollicitée DOIVENT avoir le fanion Outrepasser réglé à zéro. Cela assure que si le nœud lui-même est présent sur la liaison, son annonce de voisin (avec le fanion Outrepasser réglé à un) va prendre le pas sur toute annonce reçue d'un mandataire. Un mandataire PEUT envoyer des annonces non sollicitées avec le fanion Outrepasser établi à un comme spécifié au paragraphe 7.2.6, mais le faire être cause que l'annonce de mandataire outrepasse les entrées valides créées par le nœud lui-même.

Finalement, lors de l'envoi d'une annonce de mandataire en réponse à une sollicitation de voisin, l'envoyeur devrait retarder sa réponse d'une durée aléatoire entre 0 et MAX_ANYCAST_DELAY_TIME secondes pour éviter des collisions dues à l'envoi simultané de plusieurs réponses par plusieurs mandataires. Cependant, dans certains cas (par exemple, IPv6 Mobile) où un seul mandataire est présent, un tel délai n'est pas nécessaire.

7.3 Détection d'inaccessibilité du voisin

La communication vers ou à travers un voisin peut échouer pour de nombreuses raisons à tout moment, y compris pour des défaillances de matériel, le remplacement à chaud d'une carte d'interface, etc. Si la destination est défaillante, aucune

récupération n'est possible et la communication échoue. D'un autre côté, si c'est le chemin qui est défaillant, il se peut que la récupération soit possible. Donc, un nœud suit activement l'état d'accessibilité des voisins auxquels il envoie des paquets.

La détection d'inaccessibilité du voisin est utilisée pour tous les chemins entre les hôtes et les nœuds voisins, y compris les communications d'hôte à hôte, d'hôte à routeur, et de routeur à hôte. La détection d'inaccessibilité du voisin peut aussi être utilisée entre routeurs, mais elle n'est pas exigée si un mécanisme équivalent est disponible, par exemple, au titre des protocoles d'acheminement.

Lorsque il apparaît que le chemin pour un voisin est défaillant, la procédure de récupération spécifique dépend de la façon dont le voisin est utilisé. Si le voisin est la destination finale, par exemple, la résolution d'adresse devrait être refaite. Cependant, si le voisin est un routeur, tenter de passer par un autre routeur serait approprié. La récupération spécifique qui a lieu est couverte par la détermination de prochain bond ; la détection d'inaccessibilité du voisin signale le besoin de la détermination du prochain bond en supprimant une entrée d'antémémoire de voisins.

La détection d'inaccessibilité du voisin n'est effectuée que pour les voisins auxquels sont envoyés des paquets en envoi individuel ; elle n'est pas utilisée lors d'envoi à des adresses de diffusion groupée.

7.3.1 Confirmation d'accessibilité

Un voisin est considéré comme accessible si le nœud a reçu récemment une confirmation que les paquets envoyés récemment au voisin ont été reçus par sa couche IP. Les confirmations positives peuvent être rassemblées de deux façons : des indications des protocoles de couche supérieure qui indiquent qu'une connexion fait des "progrès", ou la réception d'un message Annonce de voisin qui est une réponse à un message Sollicitation de voisin.

Une connexion fait des "progrès" si les paquets reçus d'un homologue distant ne peuvent arriver que si des paquets récents envoyés à cet homologue l'atteignent réellement. Dans TCP, par exemple, la réception d'un (nouvel) accusé de réception indique que les données envoyées précédemment ont atteint l'homologue. De même, l'arrivée de nouvelles données (non dupliquées) indique que les accusés de réception antérieurs sont livrés à l'homologue distant. Si les paquets atteignent l'homologue, ils doivent aussi atteindre le voisin de prochain bond de l'envoyeur ; donc "en progrès" est une confirmation que le voisin de prochain bond est accessible. Pour les destinations hors liaison, le progrès implique que le routeur de prochain bond est accessible. Lorsque elles sont disponibles, ces informations de couche supérieure DEVRAIENT être utilisées.

Dans certains cas (par exemple, ceux de paquets de protocoles fondés sur UDP et de routeurs transmettant des paquets aux hôtes) de telles informations d'accessibilité peuvent n'être pas directement disponibles à partir des protocoles de couche supérieure. Lorsque aucune indication n'est disponible et qu'un nœud envoie des paquets à un voisin, le nœud sonde activement le voisin en utilisant des messages de sollicitation de voisin en envoi individuel pour vérifier que le chemin de transmission fonctionne toujours.

La réception d'une annonce de voisin sollicitée sert de confirmation d'accessibilité, car les annonces faites avec le fanion Sollicité établi à un ne sont envoyées qu'en réponse à une sollicitation de voisin. La réception d'autres messages de découverte de voisin, tels que les annonces de routeur et les annonces de voisin avec le fanion Sollicité mis à zéro NE DOIT PAS être traitée comme une confirmation d'accessibilité. La réception de messages non sollicités confirme seulement le chemin unidirectionnel de l'envoyeur au nœud receveur. À l'opposé, la détection d'inaccessibilité du voisin exige qu'un nœud garde trace de l'accessibilité du chemin de transmission vers un voisin de son point de vue, et non du point de vue du voisin. Noter que la réception d'une annonce sollicitée indique qu'un chemin fonctionne dans les deux directions. La sollicitation doit avoir atteint le voisin, l'invitant à générer une annonce. De même, la réception d'une annonce indique que le chemin de l'envoyeur au receveur fonctionne. Cependant, ce dernier fait n'est connu que du receveur ; l'envoyeur de l'annonce n'a pas de moyen direct de savoir que l'annonce qu'il a envoyée a réellement atteint un voisin. Du point de vue de la détection d'inaccessibilité du voisin, seule l'accessibilité du chemin de transmission présente un intérêt.

7.3.2 État des entrées d'antémémoire de voisins

Une entrée d'antémémoire de voisins peut être dans l'un des cinq états suivants :

INCOMPLET La résolution d'adresse en en cours sur l'entrée. Précisément, une sollicitation de voisin a été envoyée à l'adresse de diffusion groupée de nœud sollicité de la cible, mais l'annonce de voisin correspondante n'a pas encore été reçue.

ACCESSIBLE Une confirmation positive a été reçue dans les dernières ReachableTime millisecondes que le chemin de

transmission vers le voisin fonctionne correctement. Dans l'état ACCESSIBLE, aucune action particulière n'a lieu lors de l'envoi des paquets.

PÉRIMÉ Plus de ReachableTime millisecondes se sont écoulées depuis la réception de la dernière confirmation positive que le chemin de transmission fonctionne correctement. Dans ce état, aucune action n'a lieu jusqu'à ce qu'un paquet soit envoyé. On entre dans l'état PÉRIMÉ à réception d'un message non sollicité de découverte de voisin qui met à jour l'adresse de couche liaison de l'antémémoire. La réception d'un tel message ne confirme pas l'accessibilité, et l'entrée dans l'état PÉRIMÉ assure que l'accessibilité est vérifiée rapidement si l'entrée est réellement utilisée. Cependant, l'accessibilité n'est pas réellement vérifiée tant que l'entrée n'est pas utilisée.

DELAI Plus de ReachableTime millisecondes se sont écoulées depuis la réception de la dernière confirmation positive que le chemin de transmission fonctionnait correctement, et un paquet a été envoyé dans les dernières DELAY_FIRST_PROBE_TIME secondes. Si aucune confirmation d'accessibilité n'est reçue dans les DELAY_FIRST_PROBE_TIME secondes de l'entrée dans l'état DELAI, envoyer une sollicitation de voisin et changer l'état en SONDE. L'état DELAI est une optimisation qui donne aux protocoles de couche supérieure du temps supplémentaire pour fournir une confirmation d'accessibilité dans les cas où ReachableTime millisecondes ont passé depuis la dernière confirmation du fait du manque de trafic récent. Sans cette optimisation, l'ouverture d'une connexion TCP après une pause de trafic initierait des sondages même si la prise de contact en trois phase ultérieure fournirait presque immédiatement une confirmation d'accessibilité.

SONDE Une confirmation d'accessibilité est activement recherchée par la retransmission de sollicitations de voisins toutes les RetransTimer millisecondes jusqu'à ce qu'une confirmation d'accessibilité soit reçue.

7.3.3 Comportement des nœuds

La détection d'inaccessibilité du voisin fonctionne en parallèle avec l'envoi de paquets à un voisin. Tout en réaffirmant l'accessibilité d'un voisin, un nœud continue d'envoyer des paquets à ce voisin en utilisant l'adresse de couche liaison de l'antémémoire. Si aucun trafic n'est envoyé à un voisin, aucune sonde n'est envoyée.

Lorsque un nœud a besoin d'effectuer une résolution d'adresse sur une adresse du voisinage, il crée une entrée dans l'état INCOMPLET et initie une résolution d'adresse comme spécifié au paragraphe 7.2. Si la résolution d'adresse échoue, l'entrée DEVRAIT être supprimée, afin que le trafic ultérieur pour ce voisin invoque à nouveau la procédure de détermination du prochain bond. L'invocation de la détermination de prochain bond à ce moment assure que des routeurs par défaut de remplacement seront essayés.

Lorsque une confirmation d'accessibilité est reçue (par un avis de couche supérieur ou par une annonce de voisin sollicitée) l'état d'une entrée change pour ACCESSIBLE. La seule exception est que l'avis de couche supérieure n'a pas d'effet sur les entrées dans l'état INCOMPLET (par exemple, celles pour lesquelles il n'y a pas d'adresse de couche liaison en antémémoire).

Lorsque ReachableTime millisecondes ont passé depuis la réception de la dernière confirmation d'accessibilité pour un voisin, l'état de l'entrée d'antémémoire de voisins change de ACCESSIBLE à PÉRIMÉ.

Note : Une mise en œuvre peut en fait différer le changement d'état de ACCESSIBLE à PÉRIMÉ jusqu'à ce qu'un paquet soit envoyé au voisin, c'est-à-dire qu'il n'est pas nécessaire que survienne un événement de fin de temporisation explicite associé à l'arrivée à expiration de ReachableTime.

La première fois qu'un nœud envoie un paquet à un voisin dont l'entrée est PÉRIMÉ, l'envoyeur change l'état en DELAI et établit un temporisateur qui arrive à expiration dans DELAY_FIRST_PROBE_TIME secondes. Si l'entrée est toujours dans l'état DELAI lorsque le temporisateur arrive à expiration, l'état de l'entrée se change en SONDE. Si la confirmation d'accessibilité est reçue, l'état de l'entrée se change en ACCESSIBLE.

En entrant dans l'état SONDE, un nœud envoie un message Sollicitation de voisin en envoi individuel au voisin en utilisant l'adresse de couche liaison de l'antémémoire. Alors que dans l'état SONDE, un nœud retransmet des messages Sollicitation de voisin toutes les RetransTimer millisecondes jusqu'à obtention de la confirmation d'accessibilité. Les sondes sont retransmises même si aucun paquet supplémentaire n'est envoyé au voisin. Si aucune réponse n'est reçue après avoir attendu RetransTimer millisecondes après l'envoi de MAX_UNICAST_SOLICIT sollicitations, les retransmissions cessent et l'entrée DEVRAIT être supprimée. Le trafic ultérieur pour ce voisin va recréer l'entrée et effectuer à nouveau la résolution d'adresse.

Noter que toutes les sollicitation de voisins sont à taux limité voisin par voisin. Un nœud NE DOIT PAS envoyer de sollicitation de voisins au même voisin plus fréquemment qu'une fois toutes les RetransTimer millisecondes.

Une entrée d'antémémoire de voisins entre dans l'état PÉRIMÉ lorsque elle est créée par suite de la réception de paquets autres que d'annonce de voisins sollicitée (c'est-à-dire, Sollicitations de routeur, Annonces de routeur, Redirections, et Sollicitation de voisins). Ces paquets contiennent l'adresse de couche liaison de l'envoyeur ou, dans le cas de Redirection, de la cible de la redirection. Cependant, la réception de ces adresses de couche liaison ne confirme pas l'accessibilité du chemin dans la direction aval vers ce nœud. Placer une entrée nouvellement créée d'antémémoire de voisins pour laquelle l'adresse de couche liaison est connue pour être dans l'état PÉRIMÉ donne l'assurance que les défaillances de chemin sont détectées rapidement. De plus, si une adresse de couche liaison de l'antémémoire devait être modifiée du fait de la réception d'un des messages ci-dessus, l'état DEVRAIT aussi être réglé à PÉRIMÉ pour donner une prompte vérification que le chemin pour la nouvelle adresse de couche liaison fonctionne.

Pour détecter correctement le cas où un routeur passe de l'état de routeur à celui d'hôte (par exemple, si sa capacité de transmission IP est désactivée par la gestion du système) un nœud DOIT comparer le champ du fanion Routeur dans tous les messages Annonce de voisin reçus au champ du fanion IsRouter enregistré dans l'entrée d'antémémoire de voisin. Lorsque un nœud détecte qu'un voisin est passé de l'état de routeur à celui d'hôte, il DOIT retirer ce routeur de la liste des routeurs par défaut et mettre à jour l'antémémoire de destination comme décrit au paragraphe 6.3.5. Noter qu'un routeur peut ne pas figurer dans la liste des routeurs par défaut, même si une entrée d'antémémoire de destination l'utilise (par exemple, parce qu'un hôte a été redirigé sur lui). Dans un tel cas, toutes les entrées d'antémémoire de destination qui font référence à ce (ex) routeur doivent effectuer à nouveau la détermination du prochain bond avant d'utiliser l'entrée.

Dans certains cas, des informations spécifiques de la liaison peuvent indiquer qu'un chemin pour un voisin est défaillant (par exemple, à cause de la réinitialisation d'un circuit virtuel). Des informations spécifiques de la liaison peuvent alors être utilisées pour purger les entrées d'antémémoire de voisins avant que ne le fasse la détection d'inaccessibilité du voisin. Cependant, les informations spécifiques de la liaison NE DOIVENT PAS être utilisées pour confirmer l'accessibilité d'un voisin ; de telles informations ne fournissent pas de confirmation de bout en bout entre les couches IP voisines.

8. Fonction REDIRECTION

La présente section décrit les fonctions qui se rapportent à l'envoi et au traitement des messages Redirection.

Les messages Redirection sont envoyés par les routeurs pour rediriger un hôte sur un meilleur routeur de premier bond pour une destination spécifique ou pour informer les hôtes qu'une destination est en fait un voisin (c'est-à-dire, est en liaison). Cette dernière fonction est accomplie en mettant l'adresse cible ICMP égale à l'adresse ICMP de destination.

Un routeur DOIT être capable de déterminer l'adresse de liaison locale pour chaque routeur du voisinage afin de s'assurer que l'adresse cible dans un message Redirection identifie le voisin routeur par son adresse de liaison locale. Pour l'acheminement statique, cette exigence implique que l'adresse du routeur du prochain bond soit spécifiée en utilisant l'adresse de liaison locale du routeur. Pour l'acheminement dynamique, cette exigence implique que tous les protocoles d'acheminement IPv6 échangent d'une façon ou d'une autre les adresses de liaison locale des routeurs du voisinage.

8.1 Validation des messages Redirection

Un hôte DOIT éliminer en silence tous les messages Redirection reçus qui ne satisfont pas à toutes les vérifications de validité suivantes :

- L'adresse IP de source est une adresse de liaison locale. Les routeurs doivent utiliser leur adresse de liaison locale comme source pour les messages d'annonce de routeur et de redirection afin que les hôtes puissent identifier les routeurs de façon univoque.
- Le champ Limite de bonds IP a une valeur de 255, c'est-à-dire que le paquet n'aurait pas pu être transmis par un routeur.
- La somme de contrôle ICMP est valide.
- Le code ICMP est 0.
- La longueur ICMP (déduite de la longueur IP) est 40 octets au moins.
- L'adresse IP de source de la Redirection est la même que celle du routeur de premier bond actuel pour l'adresse de destination ICMP spécifiée.
- Le champ Destination ICMP dans le message Redirection ne contient pas d'adresse de diffusion groupée.
- L'adresse cible ICMP est une adresse de liaison locale (lorsque la redirection est sur un routeur) ou la même que l'adresse de destination ICMP (lorsque la redirection est sur la destination en liaison).
- Toutes les options incluses ont une longueur supérieure à zéro.

Le contenu du champ Réservé, et de toute option non reconnue DOIT être ignoré. De futures modifications rétro compatibles au protocole pourraient 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 options définie qui n'est pas spécifiée comme étant à utiliser avec les messages Redirection DOIT être ignoré et le paquet traité normalement. Les seules options définies qui peuvent apparaître sont l'option Adresse cible de couche liaison et l'option En-tête redirigé.

Un hôte NE DOIT PAS considérer une redirection comme invalide juste parce que l'adresse cible de la redirection n'est pas couverte par un des préfixes de la liaison. Une partie de la sémantique du message Redirection est que l'adresse cible est en liaison.

Une redirection qui réussit les vérifications de validité est appelée une "redirection valide".

8.2 Spécification du routeur

Un routeur DEVRAIT envoyer un message de redirection, sous réserve des limitations du taux d'envoi, chaque fois qu'il transmet un paquet qui ne lui est pas explicitement adressé (c'est-à-dire un paquet qui n'a pas un acheminement de source à travers le routeur) dans lequel :
- le champ Adresse de source du paquet identifie un voisin, et
- le routeur détermine (par des moyens qui sortent du domaine d'application de la présente spécification) qu'un meilleur nœud de premier bond réside sur la même liaison que le nœud d'envoi pour l'adresse de Destination du paquet en cours de transmission, et
- l'adresse de destination du paquet n'est pas une adresse de diffusion groupée.

Le paquet redirigé transmis contient, conformément au format de message donné au paragraphe 4.5 :
- Dans le champ Adresse cible, l'adresse à laquelle les paquets suivants pour la destination devraient être envoyés. Si la cible est un routeur, l'adresse de liaison locale de ce routeur DOIT être utilisée. Si la cible est un hôte, le champ Adresse cible DOIT être réglée à la même valeur que le champ Adresse de destination.
- Dans le champ Adresse de destination, l'adresse de destination du paquet IP qui l'invoque.
- Dans les options :
  - Option Adresse cible de couche liaison: l'adresse de couche liaison de la cible, si elle est connue.
  - En-tête redirigé : autant du paquet transmis qu'il peut en tenir sans que le paquet redirigé excède 1280 octets.

Un routeur DOIT limiter le taux auquel les messages Redirection sont envoyés, afin de limiter la bande passante et les coûts de traitement impliqués par les messages Redirection lorsque la source ne répond pas correctement aux redirections, ou lorsque la source choisit d'ignorer les messages Redirection non authentifiés. Des précisions sur la limitation du taux de messages d'erreur ICMP se trouvent dans la [RFC4443].

Un routeur NE DOIT PAS mettre à jour ses tableaux d'acheminement suite à la réception d'une Redirection.

8.3 Spécification de l'hôte

Un hôte qui reçoit une demande de redirection valide DEVRAIT mettre à jour son antémémoire de destination en conséquence de sorte que le trafic ultérieur aille sur la cible spécifiée. Si aucune entrée d'antémémoire de destination n'existe pour la destination, une mise en œuvre DEVRAIT créer une telle entrée.

Si la redirection contient une option Adresse cible de couche liaison, l'hôte crée ou met à jour l'entrée d'antémémoire de voisin pour la cible. Dans les deux cas, l'adresse de couche liaison de l'antémémoire est copiée de l'option Adresse cible de couche liaison. Si une entrée d'antémémoire de voisin est créée pour la cible, son état d'accessibilité DOIT être réglé à PÉRIMÉ comme spécifié au paragraphe 7.3.3. Si une entrée d'antémémoire existait déjà et qu'elle est mise à jour avec une adresse de couche liaison différente, son état d'accessibilité DOIT aussi être réglé à PÉRIMÉ. Si l'adresse de couche liaison est la même que celle qui est déjà dans l'antémémoire, l'état de l'entrée d'antémémoire reste inchangé.

Si les adresses de cible et de destination sont identiques, l'hôte DOIT traiter la cible comme en liaison. Si l'adresse cible n'est pas la même que l'adresse de destination, l'hôte DOIT régler IsRouter à VRAI pour la cible. Cependant, si les adresses de cible et de destination sont identiques, on ne peut pas déterminer de façon fiable si l'adresse cible est un routeur. Par conséquent, les entrées d'antémémoire de voisin nouvellement créées devraient régler le fanion IsRouter à FAUX, alors que les entrées existantes d'antémémoire devraient laisser le fanion inchangé. Si la cible est un routeur, les messages Annonces de voisin ou Annonce de routeur vont mettre à jour IsRouter en conséquence.

Les messages Redirection s'appliquent à tous les flux qui sont envoyés sur une destination donnée. C'est-à-dire qu'à

réception d'une redirection pour une adresse de destination, toutes les entrées d'antémémoire de destination pour cette adresse devraient être mises à jour pour utiliser le prochain bond spécifié, sans considération du contenu du champ Étiquette de flux qui apparaît dans l'option En-tête redirigé.

Un hôte NE DOIT PAS envoyer de messages Redirection.

9. Extensibilité – Traitement des options

Les options fournissent un mécanisme de codage de champs de longueur variable, champs qui peuvent apparaître plusieurs fois dans le même paquet, ou d'informations qui peuvent ne pas apparaître dans tous les paquets. Les options peuvent aussi être utilisées pour ajouter des fonctions supplémentaires à de futures versions de ND.

Afin de s'assurer que les futures extensions coexistent de façon appropriée avec les mises en œuvre actuelles, tous les nœuds DOIVENT ignorer en silence toute option qu'ils ne reconnaissent pas en recevant des paquets ND et continuer le traitement du paquet. Toutes les options spécifiées dans le présent document DOIVENT être reconnues. Un nœud NE DOIT PAS ignorer les options valides simplement parce que le message ND contiendrait des options non reconnues.

L'ensemble actuel d'options est défini de telle façon que les receveurs puissent traiter plusieurs options dans le même paquet indépendamment les unes des autres. Afin de conserver ces propriétés, les options futures DEVRAIENT suivre la règle simple que une option NE DOIT PAS dépendre de la présence ou de l'absence de toute autre option. La sémantique d'une option ne devrait dépendre que des informations de la partie fixe du paquet ND et des informations contenues dans l'option elle-même.

L'adhésion à la règle ci-dessus présente les avantages suivants :

1) Les receveurs peuvent traiter les options indépendamment les unes des autres. Par exemple, une mise en œuvre peut choisir de traiter l'option Informations de préfixe contenue dans un message Annonce de routeur dans un processus d'espace d'utilisateur alors que l'option Adresse de couche liaison du même message est traitée par des sous-programmes du noyau.

2) Si le nombre d'options devait être cause qu'un paquet excède la MTU d'une liaison, plusieurs paquets peuvent porter des sous-ensembles des options sans en changer la sémantique.

3) Les envoyeurs PEUVENT envoyer un sous-ensemble des options dans différents paquets. Par exemple, si la durée de vie préférée et la durée de validité d'un préfixe sont suffisamment élevées, il pourrait n'être pas nécessaire d'inclure l'option Informations de préfixe dans toutes les annonces de routeur. De plus, différents routeurs pourraient envoyer différents ensembles d'options. Donc, un receveur NE DOIT PAS associer une action à l'absence d'une option dans un paquet particulier. Le présent protocole spécifie que les receveurs ne devraient agir qu'à l'arrivée à expiration des temporisateurs et sur les informations qui sont reçues dans les paquets.

Les options dans les paquets de découverte de voisin peuvent apparaître dans n'importe quel ordre ; les receveurs DOIVENT être prêts à les traiter indépendamment de leur ordre. Il peut aussi y avoir plusieurs instances de la même option dans un message (par exemple, des options Informations de préfixes).

Si le nombre d'options incluses dans une annonce de routeur est cause que la taille de l'annonce excède la MTU de la liaison, le routeur peut envoyer plusieurs annonces séparées, chacune d'elles contenant un sous ensemble des options.

La quantité de données à inclure dans l'option En-tête redirigée DOIT être limitée afin que le paquet redirigé entier n'excède pas la MTU minimum exigée pour la prise en charge de IPv6 tel que spécifié dans la [RFC2460].

Toutes les options ont des longueurs qui sont des multiples de 8 octets, ce qui assure un alignement approprié sans aucun "bourrage" des options. Les champs dans les options (ainsi que les champs dans les paquets ND) sont définis comme alignés sur leurs frontières naturelles (par exemple, un champ de 16 bits est aligné sur une limite de 16 bits) à l'exception des préfixes d'adresse IP de 128 bits, qui sont alignés sur une limite de 64 bits. Le champ Adresse de couche liaison contient une chaîne d'octets non interprétée; elle est alignée sur une limite de 8 bits.

La taille d'un paquet ND, y compris l'en-tête IP, est limitée à la MTU de liaison (qui est d'au moins 1280 octets). Lors de l'ajout des options à un paquet ND, un nœud NE DOIT PAS excéder la MTU de la liaison.

De futures versions du présent protocole pourraient définir de nouveaux types d'option. Les receveurs DOIVENT ignorer en silence toute option qu'ils ne reconnaissent pas et continuer de traiter le message.

10. Constantes du protocole

Constantes du routeur :

MAX_INITIAL_RTR_ADVERT_INTERVAL	16 secondes
MAX_INITIAL_RTR_ADVERTISEMENTS	3 transmissions
MAX_FINAL_RTR_ADVERTISEMENTS	3 transmissions
MIN_DELAY_BETWEEN_RAS	3 secondes
MAX_RA_DELAY_TIME	0,5 seconde

Constantes de l'hôte :

MAX_RTR_SOLICITATION_DELAY	1 seconde
RTR_SOLICITATION_INTERVAL	4 secondes
MAX_RTR_SOLICITATIONS	3 transmissions

Constantes du nœud :

MAX_MULTICAST_SOLICIT	3 transmissions
MAX_UNICAST_SOLICIT	3 transmissions
MAX_ANYCAST_DELAY_TIME	1 seconde
MAX_NEIGHBOR_ADVERTISEMENT	3 transmissions
REACHABLE_TIME	30 000 millisecondes
RETRANS_TIMER	1 000 millisecondes
DELAY_FIRST_PROBE_TIME	5 secondes
MIN_RANDOM_FACTOR	0,5
MAX_RANDOM_FACTOR	1,5

Des constantes de protocole supplémentaires sont définies avec les formats de message à la Section 4.

Toutes les constantes de protocole sont sujettes à être changées dans de futures révisions du protocole.

Les constantes de la présente spécification peuvent être outrepassées par les documents spécifiques qui décrivent le fonctionnement de IPv6 sur les différentes couches de liaison. Cette règle permet que la découverte de voisin fonctionne sur des liaisons qui ont des caractéristiques de performances très différentes.

11 Considérations pour la sécurité

La découverte de voisin est l'objet d'attaques qui causent l'écoulement des paquets IP vers des endroits inattendus. De telles attaques peuvent être utilisées pour causer des dénis de service mais aussi pour permettre à des nœuds d'intercepter et éventuellement modifier des paquets destinés à d'autres nœuds. Cette section traite des principales menaces relatives aux messages de découverte de voisin et des mécanismes de sécurité possibles qui peuvent atténuer ces menaces.

11.1 Analyse des menaces

Ce paragraphe expose les principales menaces qui sont associées à la découverte de voisin. Une analyse plus détaillée se trouve dans la [RFC3756]. Les principales faiblesses du protocole entrent dans trois catégories :

- Attaques de déni de service (DoS).
- Attaques d'usurpation d'adresse.
- Attaques d'usurpation de routeur.

Un exemple d'attaque de déni de service est celui d'un nœud sur la liaison qui peut envoyer des paquets avec une adresse IP de source arbitraire et peut à la fois s'annoncer comme un routeur par défaut et aussi envoyer des messages d'annonce de routeur "falsifiés" qui périment immédiatement tous les autres routeurs par défaut ainsi que tous les préfixes en liaison. Un intrus peut réaliser cela en envoyant plusieurs annonces de routeur, une pour chaque routeur légitime, avec l'adresse de source réglée à l'adresse d'un autre routeur, le champ Durée de vie du routeur réglé à zéro, et les durées de vie préférée et

durée de validité réglées à zéro pour tous les préfixes. Une telle attaque causerait l'envoi de tous les paquets, pour les destinations en liaison et hors liaison, au routeur falsifié. Ce routeur pourrait alors examiner de façon sélective, modifier, ou éliminer tous les paquets envoyés sur la liaison. La détection d'inaccessibilité de voisin (NUD, *Neighbor Unreachability Detection*) ne va pas détecter un tel trou noir tant que le routeur falsifié répond poliment aux sondes NUD par une annonce de voisin avec le bit R établi.

Il est aussi possible à tout hôte de lancer une attaque de DoS sur un autre hôte en l'empêchant de configurer une adresse avec [RFC4862]. Le protocole ne permet pas aux hôtes de vérifier si l'envoyeur d'une annonce de voisin est le véritable propriétaire de l'adresse IP incluse dans le message.

Des attaques de redirection peuvent aussi être réalisées par un hôte pour inonder une victime ou voler son trafic. Un hôte peut envoyer une annonce de voisin (en réponse à une sollicitation) qui contient son adresse IP et une adresse de couche liaison de la victime afin d'inonder la victime avec du trafic non désiré. Autrement, l'hôte peut envoyer une annonce de voisin qui comporte une adresse IP de la victime et sa propre adresse de couche liaison pour remplacer une entrée existante dans l'antémémoire de destination de l'envoyeur, le forçant ainsi à transmettre tout le trafic de la victime à lui-même.

Le modèle de confiance pour les redirections est le même que dans IPv4. Une redirection n'est acceptée que si elle est reçue du même routeur que celui qui est actuellement utilisé pour cette destination. Si un hôte a été redirigé vers un autre nœud (c'est-à-dire, si la destination est en liaison) il n'y a pas de moyen d'empêcher la cible de produire une autre redirection pour quelque autre destination. Cependant, ce risque n'est pas pire que ce qu'il était avant d'être redirigé ; l'hôte cible, une fois soumis, pourrait toujours agir comme routeur caché pour transmettre du trafic ailleurs.

Le protocole ne contient aucun mécanisme pour déterminer quels voisins sont autorisés à envoyer un type particulier de message (par exemple, des annonces de routeur) ; tout voisin, même vraisemblablement en présence d'authentification, peut envoyer des messages d'annonce de routeur, étant par là capable de causer un déni de service. De plus, tout voisin peut envoyer des annonces de voisin de mandataire aussi bien que des annonces de voisin non sollicitées au titre d'une attaque potentielle de déni de service.

De nombreuses couche de liaison sont aussi sujettes à différentes attaques de déni de service comme d'occuper en continu la liaison dans des réseaux en accès multiple avec surveillance de signal et détection de collision (CSMA/CD, *Carrier Sense Multiple Access with Collision Detection*) (par exemple, en envoyant des paquets étroitement accolés ou en affirmant le signal de collision sur la liaison) ou en générant des paquets avec l'adresse MAC de quelqu'un d'autre pour tromper, par exemple, des commutateurs Ethernet. D'un autre côté, de nombreuses menaces exposées dans ce paragraphe sont moins efficaces, ou non existantes, sur les liaisons en point à point, ou sur des liaisons cellulaires où un hôte partage une liaison avec un seul voisin, c'est-à-dire, le routeur par défaut.

11.2 Sécuriser les messages de découverte de voisins

Le protocole réduit l'exposition aux menaces ci-dessus en l'absence d'authentification en ignorant les paquets ND reçus d'envoyeurs hors liaison. On vérifie que le champ Limite de bonds de tous les paquets contient 255, la valeur légale maximum. Comme les routeurs décrémentent la limite de bonds sur tous les paquets qu'ils transmettent, les paquets reçus qui contiennent une limite de bonds de 255 doivent avoir été générés par un voisin.

Les mécanismes de sécurité cryptographique pour la découverte de voisin sortent du domaine d'application du présent document et sont définis dans la [RFC3971]. Autrement, IPsec peut être utilisé pour l'authentification de couche IP [RFC4301]. L'utilisation de l'échange de clé Internet (IKE, *Internet Key Exchange*) ne convient pas pour la création dynamique d'associations de sécurité qui puissent être utilisées pour sécuriser la résolution d'adresse ou les messages de sollicitation de voisins comme décrit dans [ICMPIKE].

Dans certains cas, il peut être acceptable d'utiliser des associations de sécurité à configuration statique avec la [RFC4302] ou la [RFC4303] pour sécuriser les messages de découverte de voisin. Cependant, il est important de noter que les associations de sécurité à configuration statique ne sont pas adaptables (en particulier lorsque on considère les liaisons de diffusion groupée) et elles sont donc limitées aux petits réseaux avec des hôtes connus. Dans tous les cas, si on utilise les [RFC4302] ou [RFC4303], les paquets ND DOIVENT être vérifiés aux fins d'authentification. Les paquets qui échouent à la vérification d'authentification DOIVENT être éliminés en silence.

12. Considérations liées à la dénumérotation

Le protocole de découverte de voisin joint à l'autoconfiguration d'adresse IPv6 [RFC4862] fournit des mécanismes qui aident à la dénumérotation – de nouveaux préfixes et adresses peuvent être introduits et les anciens peuvent être déconseillés et retirés.

La robustesse de ces mécanismes se fonde sur le fait que tous les nœuds sur la liaison reçoivent en temps utile les messages d'annonce de routeur. Cependant, un hôte peut être désactivé ou être injoignable pendant une longue période (c'est-à-dire, une machine est déconnectée pendant des mois après la fin d'un projet). Il est possible de préserver la robustesse de la dénumérotation dans de tels cas, mais cela introduit quelques contraintes sur la façon dont de longs préfixes doivent être annoncés.

Considérons l'exemple suivant dans lequel un préfixe est initialement annoncé avec une durée de vie de deux mois, mais le 1er août, il est déterminé que le préfixe doit être déconseillé et retiré du fait d'un dénumérotage le 1er septembre. Cela peut se faire en réduisant la durée de vie annoncée à une semaine commençant le 1er août et à mesure que la date se rapproche, la durée de vie peut être raccourcie jusqu'au 1er septembre où le préfixe est annoncé avec une durée de vie de zéro. Le problème est que si un ou plusieurs nœuds ont été débranchés de la liaison avant le 1er septembre, ils pourraient encore penser que le préfixe est valide car la dernière durée de vie qu'ils ont reçue était de deux mois. Donc, si un nœud a été débranché le 31 juillet, il pense que le préfixe est valide jusque au 30 septembre. Si ce nœud est rebranché avant le 30 septembre, il va continuer d'utiliser le vieux préfixe. La seule façon de forcer un nœud à arrêter d'utiliser un préfixe qui était précédemment annoncé avec une longue durée de vie est de faire que ce nœud reçoive une annonce pour ce préfixe qui change la durée de vie vers l'aval. La solution dans cet exemple est simple : continuer d'annoncer le préfixe avec une durée de vie de 0 du 1er septembre au 1er octobre.

En général, afin de résister au nœuds qui pourraient être débranchés de la liaison, il est important de se projeter un peu plus loin dans l'avenir d'un préfixe particulier qui peut être vu comme valide par n'importe quel nœud de la liaison. Le préfixe doit alors être annoncé avec une durée de vie de 0 jusqu'à ce point dans l'avenir. Ce "plus loin dans l'avenir" est simplement le maximum, sur toutes les annonces de routeur, du temps pendant lequel l'annonce a été envoyée plus la durée de vie du préfixe contenue dans l'annonce.

Ceci a d' importantes implications sur l'utilisation de durées de vie infinies. Si un préfixe est annoncé avec une durée de vie infinie, et si ce préfixe doit ensuite être dénuméroté, il n'est pas souhaitable de continuer d'annoncer ce préfixe avec une durée de vie de zéro pour toujours. Donc, soit les durées de vie infinies devraient être évitées, soit il doit y avoir une limite à la durée pendant laquelle un nœud peut être débranché d'une liaison avant qu'il soit à nouveau rebranché. Cependant, on ne voit pas bien comment l'administrateur du réseau peut mettre en application une limite à la durée pendant laquelle des hôtes comme un ordinateur portable peuvent être débranchés de la liaison.

Les administrateurs de réseau devraient prendre sérieusement en considération l'utilisation de durées de vie relativement brèves (c'est-à-dire, pas plus de quelques semaines). Bien qu'il puisse paraître qu'utiliser de longues durées de vie aiderait à assurer la robustesse, en réalité, un hôte sera incapable de communiquer en l'absence de routeurs qui fonctionnent correctement. De tels routeurs vont envoyer des annonces de routeur qui contiennent les préfixes appropriés (et actuels). Un hôte connecté à un réseau qui n'a pas de routeurs en état de fonctionner va vraisemblablement avoir de plus sérieux problèmes que le simple manque de préfixe et d'adresse valide.

La discussion ci-dessus ne fait pas de distinction entre la durée de vie préférée et la durée de validité. En pratique, il est probablement suffisant de garder la trace de la durée de validité car la durée de vie préférée ne dépassera pas la durée de validité.

13. Considérations relatives à l'IANA

Le présent document n'exige l'allocation d'aucun nouveau type ou code ICMPv6. Cependant, les types ICMPv6 existants ont été mis à jour pour pointer sur le présent document plutôt que sur la [RFC2461]. La procédure pour l'allocation des types/codes ICMPv6 est décrite à la Section 6 de la [RFC4443].

Le présent document continue d'utiliser les types de message ICMPv6 suivants introduits dans la [RFC2461] et déjà alloués par l'IANA :

Nom du message	**Type ICMPv6**
Sollicitation de routeur	33
Annonce de routeur	34
Sollicitation de voisin	35
Annonce de voisin	36
Redirection	37

Le présent document continue d'utiliser les types d'option de découverte de voisin suivants introduits dans la [RFC2461] et déjà alloués par l'IANA :

Nom de l'option	Type
Adresse de source de couche liaison	1
Adresse cible de couche liaison	2
Informations de préfixe	3
En-tête redirigé	4
MTU	5

Les types d'option de découverte de voisin sont alloués en utilisant la procédure suivante :

1. L'IANA devrait allouer et enregistrer de façon permanente les nouveaux types d'option provenant de la publication de RFC de l'IETF. Ceci est pour tous les types de RFC incluant ceux en cours de normalisation, pour information, et expérimentaux qui proviennent de l'IETF et dont la publication a été approuvée par l'IESG.

2. Les groupes de travail de l'IETF avec consensus du groupe de travail et approbation du directeur de zone peuvent demander à l'IANA l'allocation de types récupérables d'option de découverte de voisin. L'IANA marquera ces valeurs comme "récupérables à l'avenir".

Le marquage "récupérable à l'avenir" sera retiré lorsque une RFC sera publiées en faisant référence au protocole comme défini en 1). Cela rendra l'allocation permanente et mettra à jour la référence sur le site IANA de la Toile.

Au moment où les valeurs de type d'option seront allouées à 85 %, l'IETF révisera les allocations marquées "récupérables à l'avenir" et informera l'IANA de celles qui devraient être récupérées et réallouées.

3. Les demandes d'allocations de valeur de type de nouvelle option provenant de l'extérieur de l'IETF ne sont possibles que par la publication d'un document de l'IETF, selon le point 1) ci-dessus. Noter aussi que les documents publiés comme "contributions de l'éditeur des RFC" [RFC3667] ne sont pas considérés comme des documents de l'IETF.

14. Références

14.1 Références normatives

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

[RFC2460] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6) ", décembre 1998. *(MàJ par RFC5095, D.S)*

[RFC4291] R. Hinden, S. Deering, "Architecture d'adressage IP version 6", février 2006. (Remplace RFC3513) *(D.S.)*

[RFC4443] A. Conta et autres, "Spécification du protocole de message de contrôle Internet (ICMPv6) pour la version 6 du protocole Internet (IPv6)", mars 2006. (Remplace RFC2463) (MàJ RFC2780) (*MàJ par* RFC4884) *(D.S.)*

14.2 Références pour information

[ICMPIKE] Arkko, J., "Effects of ICMPv6 on IKE", Travail en cours, mars 2003.

[RFC0792] J. Postel, "Protocole du message de contrôle Internet – Spécification du protocole du programme Internet DARPA", STD 5, septembre 1981.

[RFC0826] D. Plummer, "Protocole de résolution d'adresses Ethernet : conversion des adresses de protocole réseau en adresses Ethernet à 48 bits pour transmission sur un matériel Ethernet", STD 37, novembre 1982.

[RFC1122] R. Braden, "Exigences pour les hôtes Internet – couches de communication", STD 3, octobre 1989.

[RFC1256] S. Deering, éditeur, "Messages ICMP de découverte de routeur", septembre 1991.

[RFC1620] B. Braden, J. Postel, Y. Rekhter, "Extensions d'architecture Internet pour supports partagés", mai 1994. *(Info.)*

[RFC2464] M. Crawford, "Transmission de paquets IPv6 sur réseaux Ethernet", décembre 1998. *(P.S.)*

[RFC2491] G. Armitage et autres, "IPv6 sur réseaux en accès multiple sans diffusion (NBMA)", janvier 1999. *(P.S.)*

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

[RFC3232] J. Reynolds, "Numéros alloués : la RFC 1700 est remplacée par une base de données en ligne", janvier 2002.

[RFC3313] W. Marshall, éd., "Extensions privée du protocole d'initialisation de session (SIP) pour l'autorisation du support", janvier 2003. *(Information)*

[RFC3315] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins et M. Carney, "Protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)", RFC 3315, juillet 2003.

[RFC3316] J. Arkko et autres, "Protocole Internet version 6 (IPv6) pour hôtes cellulaires de 2ème et 3ème génération", avril 2003. *(Information)*

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

[RFC3667] S. Bradner, "Droits de l'IETF dans les contributions", février 2004. (*Obsolète, voir* RFC3978) (MàJ RFC2026)

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

[RFC3775] D. Johnson, C. Perkins, J. Arkko, "Prise en charge de la mobilité dans IPv6", juin 2004. *(P.S.)*

[RFC3810] R. Vida, L. Costa, éd., "Découverte d'écouteur de diffusion groupée version 2 (MLDv2) pour IPv6", juin 2004.

[RFC3971] J. Arkko et autres, "Découverte de voisin sûr (SEND)", mars 2005. *(P.S.)*

[RFC4086] D. Eastlake 3rd, J. Schiller, S. Crocker, "Exigences d'aléa pour la sécurité", juin 2005. (BCP0106)

[RFC4191] R. Draves, D. Thaler, "Préférences en matière de routeur par défaut et chemins plus spécifiques", novembre 2005. *(P.S.)*

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.)*

[RFC4302] S. Kent, "En-tête d'authentification IP", décembre 2005. *(P.S.)*

[RFC4303] S. Kent, "Encapsulation de charge utile de sécurité dans IP (ESP)", décembre 2005. *(P.S.)*

[RFC4311] R. Hinden, D. Thaler, "Partage de charge d'hôte à routeur dans IPv6", novembre 2005. (*MàJ* RFC2461) *(P.S.)*

[RFC4862] S. Thomson et autres, "Auto configuration d'adresse IPv6 sans état", septembre 2007. *(D.S.)*

[SYNC] S. Floyd, V. Jacobson, "The Synchronization of Periodic Routing Messages", IEEE/ACM Transactions on Networking, avril 1994. ftp://ftp.ee.lbl.gov/papers/sync_94.ps.Z

Appendice A Hôtes à rattachements multiples

Un certain nombre de problèmes compliqués surviennent lorsque la découverte de voisin est utilisée par des hôtes qui ont des interfaces multiples. Cette section n'essaye pas de définir le fonctionnement approprié des hôtes multi rattachements par rapport à la découverte de voisin. Elle identifie plutôt les problèmes qui exigent un travail complémentaire. Les développeurs sont invités à faire des expériences avec diverses approches pour faire fonctionner la découverte de voisin sur les hôtes multi rattachements et à faire rapport de leurs expériences.

Si un hôte multi rattachements reçoit des annonces de routeur sur toutes ses interfaces, il va (probablement) apprendre des préfixes en liaison pour les adresses qui résident sur chaque liaison. Cependant, lorsque un paquet doit être envoyé à travers un routeur, le choix du "mauvais" routeur peut résulter en un chemin sous optimal ou non opérationnel. Il faut considérer un certain nombre de problèmes :

1) Pour qu'un routeur envoie une redirection, il doit déterminer que le paquet qu'il transmet est généré par un voisin. L'essai standard dans ce cas est de comparer l'adresse de source du paquet à la liste des préfixes en liaison associés à l'interface sur laquelle le paquet a été reçu. Cependant, si l'hôte d'origine est multi rattachements, l'adresse de source qu'il utilise peut appartenir à une interface autre que l'interface d'où il a été envoyé. Dans un tel cas, un routeur ne va pas envoyer de redirections, et un acheminement sous optimal est vraisemblable. Afin qu'il soit redirigé, l'hôte envoyeur doit toujours envoyer les paquets par l'interface correspondant à l'adresse de source du paquet sortant. Noter que ce problème n'arrive jamais avec des hôtes non multi rattachements qui n'ont qu'une seule interface.

2) Si le routeur de premier bond choisi n'a pas de chemin du tout pour la destination, il ne sera pas capable de livrer le paquet. Cependant, la destination peut être joignable par un routeur sur une des autres interfaces. La découverte de voisin ne traite pas ce scénario ; il n'arrive pas dans le cas non multi rattachement.

3) Même si le routeur de premier bond a un chemin pour une destination, il peut y avoir une meilleure route via une autre interface. Aucun mécanisme n'existe pour que l'hôte multi rattachements détecte cette situation.

Si un hôte multi rattachement échoue à recevoir des annonces de routeur sur une ou plusieurs de ses interfaces, il ne va pas savoir (en l'absence d'informations configurées) quelles destinations sont en liaison sur la ou les interfaces affectées. Cela conduit à un certain nombre de problèmes: Si les annonces de routeur sont reçues sur certaines interfaces, mais pas toutes, un hôte multi rattachements pourrait choisir de n'envoyer de paquets que par les interfaces sur lesquelles il a reçu les annonces de routeur. Une hypothèse clé est cependant que les routeurs sur ces autres interfaces seront capables d'acheminer les paquets à la destination finale, même lorsque ces destinations résident sur le sous réseau auquel se connecte l'envoyeur, mais n'a pas d'informations de préfixe en liaison. Si l'hypothèse se révèle FAUSSE, la communication va échouer. Même si l'hypothèse tient, les paquets vont traverser un chemin sous optimal.

Appendice B Extensions futures

Les extensions possibles pour des travaux futurs sont :

- L'utilisation de temporisateurs dynamiques pour être capable de s'adapter aux délais très variables des liaisons. La mesure des délais d'aller-retour exige cependant des accusés de réception et des numéros de séquence afin de faire correspondre les annonces de voisin reçues avec la sollicitation de voisin réelle qui a déclanché l'annonce. Les développeurs qui souhaitent faire des expériences avec une telle facilité pourraient le faire de façon rétro-compatible en définissant une nouvelle option portant les informations nécessaires. Les nœuds qui ne comprennent pas l'option l'ignoreraient simplement.

- L'ajout de capacités pour faciliter le fonctionnement sur des liaisons qui exigent actuellement des hôtes qu'ils s'enregistrent auprès d'un serveur de résolution d'adresses. Cela pourrait par exemple permettre aux routeurs de demander aux hôtes de leur envoyer des annonces périodiques non sollicitées. Là encore, cela peut être fait en ajoutant une nouvelle option dans les annonces de routeur.

- L'ajout de procédures supplémentaires pour les liaisons où l'accessibilité asymétrique et non transitive fait partie du fonctionnement normal. De telles procédures pourraient permettre aux hôtes et aux routeurs de trouver des chemins utilisables sur, par exemple, des liaisons radio.

Appendice C Automate à états pour l'état d'accessibilité

Cet appendice contient un résumé des règles spécifiées aux paragraphes 7.2 et 7.3. Le présent document ne rend pas obligatoire que les mises en œuvre adhèrent à ce modèle pour autant que leur comportement externe soit cohérent avec celui décrit dans le présent document.

En effectuant la résolution d'adresse et la détection d'inaccessibilité du voisin, les transitions d'état suivantes s'appliquent en utilisant le modèle conceptuel:

État	**Événement**	**Action**	**Nouvel état**
-	Paquet à envoyer	Créer une entrée. Envoyer NS en diffusion groupée. Lancer le temporisateur de retransmission.	INCOMPLET
INCOMPLET	Fin de temporisation de retransmission, moins de N retransmissions.	Retransmettre NS, Lancer le temporisateur de retransmission	INCOMPLET
INCOMPLET	Fin de temporisation de retransmission, N retransmissions ou plus.	Élimer l'entrée, envoyer une erreur ICMP	-
INCOMPLET	NA, Sollicité=0, Outrepasser=0/1	Enregistrer l'adresse de couche liaison. Envoyer les paquets de la file d'attente.	PÉRIMÉ
INCOMPLET	NA, Sollicité=1, Outrepasser=0/1	Enregistrer l'adresse de couche liaison. Envoyer les paquets de la file d'attente.	ACCESSIBLE
INCOMPLET	NA, Sollicité=0/1, Outrepasser=0/1, pas d'adresse de couche liaison	Mettre à jour le contenu du fanion IsRouter.	Inchangé
-	NS, RS, Redirection pas d'adresse de couche liaison	-	-
INCOMPLET	NA, Sollicité=1,	Outrepasser=0. Même adresse de	ACCESSIBLE

		couche liaison que dans l'antémémoire	
INCOMPLET	NA, Sollicité=0/1, Outrepasser=0/1, Pas d'adresse de couche liaison	Mettre à jour le contenu du fanion IsRouter.	Inchangé
ACCESSIBLE	NA, Sollicité=1, Outrepasser=0 Adresse de couche liaison différente de celle de l'antémémoire.	-	PÉRIMÉ
PÉRIMÉ ou SONDE ou DELAI	NA, Sollicité=1, Outrepasser=0 Adresse de couche liaison différente de celle de l'antémémoire.	-	Inchangé
INCOMPLET	NA, Sollicité=1, Outrepasser =1	Enregistrer l'adresse de couche liaison (si différente).	ACCESSIBLE
INCOMPLET	NA, Sollicité=0, Outrepasser =0	-	Inchangé
INCOMPLET	NA, Sollicité=0, Outrepasser =1 Même adresse de couche liaison que dans l'antémémoire.	-	Inchangé
INCOMPLET	NA, Sollicité=0, Outrepasser =1 Adresse de couche liaison différente de celle de l'antémémoire.	Enregistrer l'adresse de couche liaison.	PÉRIMÉ
INCOMPLET	Confirmation d'accessibilité de couche supérieure	-	ACCESSIBLE
ACCESSIBLE	Fin de temporisation, plus de N secondes depuis la confirmation d'accessibilité.	-	PÉRIMÉ
PÉRIMÉ	Envoi de paquet	Lancer le temporisateur de délai	DELAI
DELAI	Fin de temporisation de délai.	Envoi d'une sonde NS en envoi individuel. Lancer le temporisateur de retransmission.	SONDE
SONDE	Fin de temporisation de retransmission, moins de N retransmissions.	Retransmission NS	SONDE
SONDE	Fin de temporisation de retransmission, N retransmissions ou plus.	Éliminer l'entrée	-

Les transitions d'état pour la réception d'informations non sollicitées autres que les messages Annonce de voisin s'appliquent aussi bien à la source du paquet (pour les messages Sollicitation de voisin, Sollicitation de routeur, et annonce de routeur) qu'à l'adresse cible (pour les messages Redirection) comme suit :

État	**Événement**	**Action**	**Nouvel état**
-	NS, RS, RA, Redirection	Créer l'entrée.	PÉRIMÉ
INCOMPLET	NS, RS, RA, Redirection	Enregistrer l'adresse de couche liaison. Envoyer les paquets en file d'attente.	PÉRIMÉ
!INCOMPLET	NS, RS, RA, Redirection Adresse de couche liaison différente de celle de l'antémémoire.	Mettre à jour l'adresse de couche liaison.	PÉRIMÉ
!INCOMPLET	NS, RS, RA, Redirection. Même adresse de couche liaison que dans l'antémémoire.	-	inchangé

Appendice D Résumé des règles pour IsRouter

Cet appendice présente un résumé des règles de maintenance du fanion IsRouter telles que spécifiées dans le présent document.

Le fondement de ces règles est que les messages ND contiennent, implicitement ou explicitement, des informations qui indiquent si l'envoyeur (ou l'adresse cible) est un hôte ou un routeur. On fait les hypothèses suivantes :

- L'envoyeur d'une annonce de routeur est implicitement supposé être un routeur.
- Les messages de sollicitation de voisin ne contiennent pas d'indication implicite ou explicite sur l'envoyeur. Les hôtes et les routeurs peuvent tous deux envoyer de tels messages.
- Les messages d'annonce de voisin contiennent un "fanion IsRouter" explicite, le bit R.
- La cible d'une redirection, lorsque la cible diffère de l'adresse de destination dans le paquet redirigé, est implicitement supposée être un routeur. C'est une hypothèse naturelle car ce nœud est supposé être capable de transmettre les paquets vers la destination.
- La cible de la redirection, lorsque elle est la même que la destination, ne porte aucune information sur la nature d'hôte/routeur. Tout ce qu'on sait est que la destination (c'est-à-dire la cible) est en liaison mais qu'elle peut aussi bien

être un hôte qu'un routeur.

Les règles pour établir le fanion IsRouter se fondent sur les informations ci-dessus. Si un message ND contient des informations explicites ou implicites, la réception du message causera la mise à jour du fanion IsRouter. Mais lorsque il n'y a pas d'information sur la nature d'hôte/routeur dans le message ND, la réception du message NE DOIT PAS causer un changement de l'état de IsRouter. Lorsque la réception d'un tel message cause la création d'une entrée d'antémémoire de voisins, le présent document spécifie que le fanion IsRouter est mis à FAUX. Il y a un plus grand potentiel de dommages lorsque un nœud pense à tort qu'un hôte est un routeur, que l'inverse. Dans ces cas, un message ultérieur d'annonce de voisin ou d'annonce de routeur va établir la valeur correcte de IsRouter.

Appendice E Questions de mise en œuvre

E.1 Confirmations d'accessibilité

La détection d'inaccessibilité du voisin exige la confirmation explicite qu'un chemin de transmission fonctionne correctement. Pour éviter d'avoir besoin de messages de sonde de sollicitation de voisin, les protocoles de couche supérieure devraient fournir une telle indication lorsque son coût est faible. Les protocoles orientés connexion fiables tels que TCP savent généralement quand le chemin de transmission fonctionne. Par exemple, lorsque TCP envoie (ou reçoit) des données, il met à jour ses numéros de séquence de fenêtre, lance et annule les temporisateurs de retransmission, etc. Des scénarios spécifiques qui indiquent généralement un fonctionnement correct du chemin de transmission comportent :

- La réception d'un accusé de réception qui couvre un numéro de séquence (par exemple, de données) qui n'avait pas été acquitté antérieurement indique que le chemin de transmission fonctionnait au moment de l'envoi des données.

- L'achèvement de la prise de contact initiale en trois phases est un cas particulier de la règle précédente; bien qu'aucune donnée ne soit envoyée durant la prise de contact, les fanions SYN sont comptés comme données du point de vue du numéro de séquence. Cela s'applique à la fois au SYN+ACK car l'actif ouvre le ACK de ce paquet sur l'ouverture passive de l'homologue.

- La réception de nouvelles données (c'est-à-dire, de données non reçues précédemment) indique que le chemin de transmission fonctionnait au moment de l'envoi d'un accusé de réception qui a fait avancer la fenêtre d'envoi de l'homologue qui a permis l'envoi des nouvelles données.

Pour minimiser le coût de communication des informations d'accessibilité entre les couches TCP et IP, une mise en œuvre peut souhaiter limiter le taux de confirmations d'accessibilité qu'elle envoie sur IP. Une possibilité est de ne traiter l'accessibilité que tous les quelques paquets. Par exemple, on peut mettre à jour les informations d'accessibilité une fois par délai d'aller retour, si une mise en œuvre n'a qu'un temporisateur d'aller-retour par connexion. Pour les mises en œuvre qui mettent en antémémoire les entrées d'antémémoire de destination au sein des blocs de contrôle, il est possible de mettre à jour l'entrée d'antémémoire de voisin directement (c'est-à-dire, sans une recherche coûteuse) une fois que le paquet TCP a été démultiplexé dans son bloc de contrôle correspondant. Pour d'autres mises en œuvre il est possible de porter la confirmation d'accessibilité sur le prochain paquet soumis à IP en supposant que la mise en œuvre se préserve contre la péremption de la confirmation portée lorsque aucun paquet n'est envoyé à IP pendant une longue période.

TCP doit aussi se garder de penser que les informations "périmées" indiquent l'accessibilité actuelle. Par exemple, de nouvelles données reçues 30 minutes après l'ouverture d'une fenêtre ne constituent pas une confirmation que le chemin fonctionne actuellement. Cela indique simplement que la mise à jour de fenêtre a atteint l'homologue il y a 30 minutes, c'est-à-dire que le chemin fonctionnait à ce moment. Une mise en œuvre doit aussi tenir compte des sondes TCP de fenêtre zéro qui sont envoyées mêmes si le chemin est interrompu et si la mise à jour de fenêtre n'a pas atteint l'homologue.

Pour les applications fondées sur UDP (Appel de procédure distant (RPC, *Remote Procedure Call*), DNS) il est relativement simple de faire que le client envoie des confirmations d'accessibilité lorsque le paquet de réponse est reçu. Il est plus difficile et dans certains cas, impossible au serveur de générer de telles confirmations car il n'y a pas de contrôle de flux, c'est-à-dire, le serveur ne peut pas déterminer si la réception d'une demande indique qu'une réponse précédente a atteint le client.

Noter qu'une mise en œuvre ne peut pas utiliser un avis négatif de couche supérieure en remplacement de l'algorithme de détection d'inaccessibilité du voisin. L'avis négatif (par exemple provenant de TCP lorsque il y a des retransmissions excessives) pourrait servir d'indication que le chemin de transmission venant de l'envoyeur des données pourrait ne pas fonctionner. Mais il ne réussirait pas à détecter lorsque le chemin venant du receveur des données ne fonctionne pas, ce qui serait cause qu'aucun des paquets d'accusé de réception n'atteint l'envoyeur.

Appendice F Changements depuis la RFC 2461

- Retrait des références aux AH et ESP IPsec pour la sécurisation des messages ou au titre de la validation du message reçu.
- Ajout du paragraphe 3.3.
- Mise à jour de la Section 11 pour inclure un exposé plus détaillé sur les menaces, les limitations d'IPsec, et l'utilisation de SEND.
- Retrait de l'hypothèse en liaison au paragraphe 5.2 sur la base de la RFC4942, "IPv6 : l'hypothèse en liaison de la découverte de voisin est considérée comme dommageable".
- Précision de la définition du champ Durée de vie de routeur au paragraphe 4.2.
- Mise à jour du texte des paragraphes 4.6.2 et 6.2.1 pour indiquer que la durée de vie préférée ne doit pas être supérieure à la durée de validité.
- Retrait de la référence à la configuration à états pleins et ajout à la place de la référence à DHCPv6.
- Ajout de la définition du fanion IsRouter au paragraphe 6.2.1 pour permettre le comportement mixte hôte/routeur.
- Permettre d'exempter les nœuds mobiles de l'ajout de délais aléatoires avant l'envoi d'un RS durant un transfert de cellule.
- Mise à jour de la définition de la longueur de préfixe dans l'option de préfixe.
- Mise à jour de l'applicabilité aux liaisons NBMA dans l'introduction et ajout des références aux RFC du 3GPP.
- Précision que la prise en charge de l'équilibrage de charge est limitée aux routeurs.
- Précisions sur le comportement du routeur lors de la réception d'une sollicitation de routeur sans option Adresse de source de couche liaison (SLLAO).
- Précision que les vérifications de cohérence pour CurHopLimit ne sont faites que pour les valeurs différentes de zéro.
- Réarrangement du paragraphe 7.2.5 pour le rendre plus clair, et description du processus à la réception du NA dans l'état INCOMPLET.
- Ajout de précision au paragraphe 7.2 sur la façon dont un nœud devrait réagir à réception d'un message sans SLLAO.
- Ajout d'une nouvelle section IANA.
- Diverses corrections rédactionnelles.

Remerciements

Les auteurs de la RFC 2461 tiennent à remercier de leurs contributions le groupe de travail IPv6, et en particulier, (dans l'ordre alphabétique) Ran Atkinson, Jim Bound, Scott Bradner, Alex Conta, Stephen Deering, Richard Draves, Francis Dupont, Robert Elz, Robert Gilligan, Robert Hinden, Tatuya Jinmei, Allison Mankin, Dan McDonald, Charles Perkins, Matt Thomas, et Susan Thomson.

L'éditeur de ce document (Hesham Soliman) tient à remercier le groupe de travail IPV6 de ses nombreuses contributions à la présente révision -- en particulier (par ordre alphabétique) Greg Daley, Elwyn Davies, Ralph Droms, Brian Haberman, Bob Hinden, Tatuya Jinmei, Pekka Savola, Fred Templin, et Christian Vogt.

Adresse des auteurs

Thomas Narten
IBM Corporation
P.O. Box 12195
Research Triangle Park, NC 27709-2195
USA
téléphone : +1 919 254 7798
mél : narten@raleigh.ibm.com

Erik Nordmark
Sun Microsystems, Inc.
17 Network Circle
Menlo Park, CA 94025
USA
téléphone : +1 650 786 2921
fax : +1 650 786 5896
mél : erik.nordmark@sun.com

William Allen Simpson
Daydreamer
Computer Systems Consulting Services
1384 Fontaine
Madison Heights, Michigan 48071
USA
mél : william.allen.simpson@gmail.com

Hesham Soliman
Elevate Technologies
mél : hesham@elevatemobile.com

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administratif (IASA) de l'IETF