Groupe de travail Réseau	T. Narten, IBM
Request for Comments : 2461	E. Nordmark, Sun Microsystems
RFC rendue obsolète : 1970	W. Simpson, Daydreamer
Catégorie : En cours de normalisation	décembre 1998
Traduction Claude Brière de L'Isle	

Découverte de voisin pour IP version 6 (IPv6)

Statut du présent mémoire

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

Résumé

Le présent document spécifie le protocole de découverte de voisin pour IP version 6. Les nœuds IPv6 sur la même liaison utilisent la découverte de voisin pour découvrir leur présence mutuelle, pour déterminer leurs adresses de couche liaison, pour trouver les routeurs et pour entretenir les informations d'accessibilité sur les chemins vers les voisins actifs.

Table des matières

1. Introduction

La présente spécification définit le protocole de découverte de voisin (ND, *découverte de voisin*) 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 veulent transmettre des paquets en leur nom. Enfin, les nœuds utilisent le protocole pour garder activement trace des voisins qui sont joignables et de ceux qui ne le sont pas, et pour détecter les changements des adresses de couche liaison. Lorsque un routeur ou le chemin vers un routeur connaît une défaillance, un hôte recherche activement des solutions de remplacement.

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, comme ND utilise la diffusion groupée de couche de liaison pour certains de ses services, il est possible que sur certains types de liaisons (par exemple, les liaisons NBMA) des protocoles ou mécanismes de remplacement soient spécifiés pour mettre en œuvre ces services (dans le document approprié qui traite du 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, comme les redirections, la détermination du prochain bond, la détection d'inaccessibilité de voisin, etc., sont supposés être fournis comme spécifié dans le présent document. Le détail de la façon dont ils utilisent ND sur les liaisons NBMA est un domaine qui fera l'objet d'études ultérieures.

Les auteurs tiennent à remercier de leurs contributions les membres du groupe de travail IPNG et en particulier, (par ordre alphabétique) Ran Atkinson, Jim Bound, Scott Bradner, Alex Conta, Stephen Deering, Richard Draves, Francis Dupont, Robert Elz, Robert Gilligan, Robert Hinden, Allison Mankin, Dan McDonald, Charles Perkins, Matt Thomas, et Susan Thomson.

2. Terminologie

2.1 Généralités

IP Protocole Internet version 6. Les termes IPv4 et IPv6 ne sont utilisés que dans les contextes où il est nécessaire d'éviter les ambiguïtés.

ICMP Protocole de contrôle de message Internet pour le protocole Internet version 6. Les termes ICMPv4 et ICMPv6 ne sont utilisés que dans les contextes où il est nécessaire d'éviter les ambiguïtés.

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 en sont les protocoles de transport tels que TCP et UDP, les protocoles de contrôle tels que ICMP, les protocoles d'acheminement tels que OSPF, et les protocoles internet ou de couche inférieure étant "tunnelés" (c'est-à-dire, encapsulés dans) sur IP comme IPX, 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, la couche immédiatement en dessous de IP. Des exemples en sont les Ethernets (simples ou pontés) les liaisons en

point à point, X.25, les réseaux en relais de trame, ou ATM, ainsi que les "tunnels" de couche internet (ou supérieure) comme les tunnels sur IPv4 ou IPv6 lui-même.

interface le rattachement d'un nœud à une liaison.

voisins nœuds rattachés à la même liaison.

adresse identifiant de couche liaison pour une interface ou ensemble d'interfaces.

adresse d'envoi à la cantonade identifiant pour un ensemble d'interfaces (appartenant normalement à des nœuds différents). Un paquet envoyé à une adresse d'envoi 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 [RFC2373].

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'une adresse d'envoi à la cantonade est utilisée. Dans tout le reste de ce document, les références aux 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 des bits initiaux d'une adresse.

adresse de couche liaison identifiant de couche liaison pour une interface. Les exemples incluent les adresses IEEE 802 pour les liaisons Ethernet et les adresses E.164 pour les 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, ou
- si un routeur voisin spécifie l'adresse comme cible d'un message Redirection, ou
- un message d'annonce de voisin est reçu pour l'adresse (cible), ou
- un message de découverte de voisin est reçu de cette adresse.

hors-liaison l'opposé de "en-liaison"; une adresse qui n'est pas allouée à une des interfaces de la liaison spécifiée.

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

accessibilité aptitude au fonctionnement du chemin de transmission unidirectionnel vers un voisin. En particulier, l'accessibilité s'adresse au fait que les paquets envoyés à un voisin atteignent la couche IP sur la machine voisine et sont traités correctement par la couche IP receveuse. Pour les routeurs voisins, l'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 les paquets (c'est-à-dire qu'il est configuré comme un routeur, et pas comme un hôte). Pour les hôtes, l'accessibilité signifie que les paquets envoyés par la couche IP d'un nœud sont livrés à la couche IP de l'hôte voisin.

paquet c'est un en-tête IP plus une charge utile.

MTU de liaison unité maximum de transmission, c'est-à-dire, taille maximum de paquet en octets, qui peut être convoyée en un seul morceau sur une liaison.

cible adresse sur laquelle sont recherchées 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 agirait potentiellement comme un mandataire pour le nœud mobile.

Indication ICMP Destination injoignable c'est une indication d'erreur retournée à l'envoyeur d'origine d'un paquet qui ne peut pas être livré pour les raisons exposées dans la [RFC2463]. Si l'erreur survient sur un nœud autre que celui d'origine du paquet, un message ICMP d'erreur 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 la couche supérieure soit notifiée au moyen d'un mécanisme approprié (par exemple, le retour d'une valeur à partir d'un appel de procédure). Noter, cependant qu'une mise en œuvre peut trouver pratique dans certains cas 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 des sous-programmes génériques de traitement d'erreur.

délai aléatoire lors de l'envoi de messages, il est parfois nécessaire de retarder une transmission d'une durée aléatoire afin de prévenir l'envoi simultané par de multiples nœuds, ou d'empêcher la synchronisation de transmissions périodiques à longue portée [SYNC]. Lorsque un composant aléatoire est requis, un nœud calcule le délai réel de façon telle que le délai calculé forme une valeur aléatoire à distribution uniforme qui tombe entre les délais minimum et maximum spécifiés. La mise en œuvre doit veiller à s'assurer que la granularité du composant aléatoire calculé et la résolution du temporisateur utilisé sont toutes deux suffisamment élevées pour assurer que la probabilité que plusieurs nœuds retardent de la même durée soit faible.

germe de délai aléatoire si on utilise un générateur de nombres pseudo aléatoires pour calculer un composant de délai aléatoire, le générateur devrait être initialisé avec un germe unique avant l'utilisation. Noter qu'il n'est pas suffisant d'utiliser le seul jeton d'interface comme germe, car les jetons d'interface ne vont pas toujours être univoques. Pour réduire la probabilité que des jetons d'interface dupliqués causent l'utilisation du même germe, celui-ci devrait être calculé à partir de diverses sources d'entrée (par exemple, des composants machine) qui seront vraisemblablement différents même sur des "boîtes" identiques. Par exemple, le germe pourrait être formé par la combinaison du numéro de série du CPU avec un jeton d'interface.

2.2 Types de liaison

Les différentes couches de liaison ont des paramètres différents. Ceux qui concernent la découverte de voisin sont :

diffusion groupée *(multicast)* liaison qui accepte un mécanisme natif à la couche de liaison pour l'envoi des paquets à tous (c'est-à-dire, en diffusion) ou à un sous-ensemble de tous les voisins.

point à point liaison qui connecte exactement deux interfaces. Une liaison point à point est supposée avoir des capacités de diffusion groupée et avoir une adresse de liaison locale.

multi accès sans diffusion (NBMA, *non-broadcast multi-access*) liaison à laquelle plus de deux interfaces peuvent se rattacher, mais qui n'accepte pas une forme native 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 des services de diffusion groupée pour IP (par exemple, en utilisant des serveurs de diffusion groupée) mais savoir si ND devrait utiliser de telles facilités ou un autre mécanisme fournissant des service ND équivalents est une question qui devra être étudiée à l'avenir.

support partagé *(shared media)* liaison qui permet une communication directe parmi un certain nombre de nœuds, mais où les nœuds rattachés sont configurés de telle façon qu'il n'ont pas les informations complètes de préfixe pour toutes les destinations en liaison. C'est à dire qu'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 en sont de grands réseaux publics de données (commutés) tels que SMDS et le RNIS-LB. Connus aussi sous le nom de "grands nuages" *(large clouds)*. Voir aussi la [RFC1620].

MTU variable liaison qui n'a pas une MTU bien définie (par exemple, les anneaux à jetons IEEE 802.5). De nombreuses liaisons (par exemple, Ethernet) ont une MTU standard définie par le protocole de couche liaison ou par le document spécifique qui décrit la façon de faire fonctionner IP sur la couche liaison.

accessibilité asymétrique liaison où une accessibilité non réflexive et/ou non transitive fait partie du fonctionnement normal. (L'accessibilité non réflexive signifie que les paquets de A atteignent B mais que les paquets de B n'atteignent pas A. Accessibilité non transitive signifie que les paquets de A atteignent B, et que les paquets de B atteignent C, mais que 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 [RFC2373], par mi lesquelles :

adresse de diffusion groupée Tous-les-nœuds adresse de portée liaison locale pour joindre tous les nœuds. FF02::1

adresse de diffusion groupée Tous-les-routeurs adresse de portée liaison locale pour joindre tous les routeurs. FF02::2

adresse de diffusion groupée Nœuds-sollicités adresse de diffusion groupée de portée liaison locale qui est calculée comme une fonction de l'adresse de la cible sollicitée. La fonction est décrite dans la [RFC2373]. La fonction est choisie de telle sorte que les adresses IP qui ne diffèrent que par les bits de poids fort, par exemple, du fait que plusieurs préfixes de rang supérieur sont associés à des fournisseurs différents, vont se transposer en la même adresse de nœud sollicité, réduisant par là le nombre d'adresses de diffusion groupée que doit joindre un nœud.

adresse de liaison locale adresse d'envoi individuel qui a une portée limitée à la liaison et qui peut être utilisée pour atteindre les voisins. Toutes les interfaces sur les routeurs DOIVENT avoir une adresse de liaison locale. La [RFC2462] exige aussi que les interfaces sur les hôtes aient une adresse de liaison locale.

adresse non spécifiée c'est une 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 n'est pas utilisée durant l'autoconfiguration d'adresse [RFC2462]). L'adresse non spécifiée a une valeur de 0:0:0:0:0:0:0:0.

2.4 Exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS, "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" dans ce document sont à interpréter comme décrit dans la [RFC2119].

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

3. Vue d'ensemble du protocole

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

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

Découverte de préfixe : comment les hôtes découvrent l'ensemble de préfixes d'adresses qui définit les destinations qui sont en-liaison pour une liaison rattachée. (Les nœuds utilisent les préfixes pour distinguer les destinations qui résident en-liaison de celles qui ne sont accessibles que par un routeur.)

Découverte de paramètres : comment un nœud apprend ces paramètres de 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 : comment les nœuds configurent automatiquement une adresse pour une interface.

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

Détermination du prochain bond : c'est l'algorithme pour transposer une adresse de destination IP en adresse IP du voisin auquel le trafic pour la destination devrait être envoyé. Le prochain bond peut être un routeur pour 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. Aussi bien pour les routeurs que pour les hôtes, la résolution d'adresse peut être effectuée à nouveau.

Détection d'adresse dupliquée : comment un nœud détermine qu'une adresse qu'il souhaite utiliser n'est pas déjà prise 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 différents types de paquet ICMP : une paire de messages Sollicitation de routeur et Annonce de routeur, une paire de messages Sollicitation de routeur et Annonce de voisin, et un message Redirection. Les messages servent aux objets suivants :

Sollicitation de routeur : lorsque une interface devient activée, les hôtes peuvent envoyer des Sollicitations de routeur qui demandent aux routeurs de générer des Annonces de routeur immédiatement plutôt qu'au prochain instant programmé.

Annonce de routeur : les routeurs annoncent leur présence ainsi que divers paramètres de liaison et Internet, soit périodiquement, soit en réponse à un message Sollicitation de routeur. Les annonces de routeur contiennent des préfixes qui sont utilisés pour la détermination de ce qui est en-liaison et/ou de la configuration d'adresse, une valeur suggérée de limite de bonds, 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 toujours 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 : est utilisé par les routeurs pour informer les hôtes d'un meilleur premier bond pour une destination.

Sur les liaisons capables de diffusion groupée, chaque routeur diffuse périodiquement en diffusion groupée un paquet Annonce de routeur pour annoncer sa disponibilité. Un hôte qui reçoit des annonces de routeur de tous les routeurs construit une liste des routeurs par défaut. Les routeurs génèrent assez fréquemment des annonces de routeur pour que les hôtes apprennent leur présence en quelques minutes, mais pas assez fréquemment pour qu'on se fie à une absence d'annonce pour détecter une défaillance d'un routeur ; un algorithme distinct de détection de voisin injoignable s'occupe de la détection des défaillances.

Les annonces de routeur contiennent une liste des préfixes utilisés pour la détermination de ce qui est en-liaison et/ou de la configuration autonome d'adresse ; les fanions associés aux préfixes spécifient l'usage auquel est destiné chaque 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 pas couverte par un préfixe en-liaison annoncé. Dans de tels cas, un routeur peut envoyer une Redirection qui informe l'envoyeur de ce que la destination est un voisin.

Les annonces 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 états pleins (DHCPv6) et/ou autonome (sans état). La sémantique exacte et l'usage des informations qui se rapportent à la configuration d'adresse sont spécifiés dans la [RFC2462].

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

Les nœuds qui accomplissent la résolution d'adresse par l'envoi en diffusion groupée de sollicitations de voisin qui demandent au nœud cible de retourner son adresse de couche liaison. Les messages Sollicitation de voisin sont en diffusion groupée à l'adresse de diffusion groupée Nœuds-sollicités 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 de demande-réponse est suffisante pour que l'initiateur et la cible résolvent tous deux leurs adresses de couche liaison réciproques ; 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 plus d'un nœud a reçu la même adresse d'envoi individuel. L'utilisation des messages Sollicitation de voisin pour la détection d'adresse dupliquée est spécifiée dans la [RFC2462].

La détection d'inaccessibilité du voisin détecte la défaillance d'un voisin ou la défaillance du chemin de transmission vers ce voisin. L'effectuer exige une confirmation positive que les paquets envoyés à un voisin atteignent bien ce voisin et sont

traités de façon appropriée par sa couche IP. La détection d'inaccessibilité du voisin utilise la confirmation à partir de deux sources. Lorsque possible, les protocoles de couche supérieure fournissent une confirmation positive qu'une connexion fait des "progrès dans la transmission", c'est-à-dire que les données envoyées précédemment sont connues pour avoir été livrées correctement (par exemple, de nouveaux accusés de réception ont été reçus récemment). Lorsque la confirmation positive ne se fait pas par de telles "indications", un nœud envoie des messages de sollicitation de voisin en envoi individuel comme confirmation d'accessibilité à partir du prochain bond. Pour réduire le trafic réseau non indispensable, les messages de sondage ne sont envoyés qu'aux voisins auxquels le nœud est actif dans l'envoi de paquets.

En plus du traitement des problèmes généraux ci-dessus, la découverte de voisins 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 (non sollicités) d'annonce de voisin à tous les nœuds pour mettre rapidement à jour les adresses de couche liaison mises en antémémoire qui sont devenues invalides. Noter que l'envoi d'annonces non sollicitées est seulement une amélioration des performances (par exemple, non fiable). L'algorithme de détection d'inaccessibilité du voisin assure que tous les nœuds découvriront de façon fiable la nouvelle adresse, bien que le délai puisse être un peu plus long.

Équilibrage de charge entrante
Les nœuds qui ont des interfaces dupliquées peuvent vouloir un équilibrage de la charge de réception des paquets entrants entre plusieurs 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.

L'équilibrage de charge est traité en permettant aux routeurs d'omettre l'adresse de source de couche liaison des 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 selon ce qui a produit la sollicitation.

Adresses d'envoi à la cantonade
Les adresses d'envoi à la cantonade identifient un des nœuds 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 recouvrement. Cela invoque des règles spécifiques pour déterminer lesquelles des potentiellement multiples annonces devraient être utilisées.

Annonces de mandataire
Un routeur qui veut accepter des paquets au nom d'une adresse cible qui est dans l'incapacité de répondre aux sollicitations de voisin peut produire des annonces de voisin sans recouvrement. Il n'y a pas actuellement d'utilisation spécifiée de mandataire, mais l'annonce de mandataire pourrait être utilisée pour traiter des cas comme ceux des nœuds mobiles qui se sont déplacés hors-liaison. Cependant, ce n'est pas destiné à être le mécanisme général de traitement des nœuds qui, par exemple, ne mettent pas en œuvre le présent protocole.

3.1 Comparaison avec IPv4

Le protocole de découverte de voisin IPv6 correspond à une combinaison de l'ARP des protocoles IPv4 [RFC0826], de la découverte de routeur ICMP [RFC1256], et de la Redirection ICMP [RFC0792]. Dans IPv4, il n'y a pas de protocole ou mécanisme d'acceptation générale pour la détection d'inaccessibilité de voisin, bien que les exigences pour les hôtes de la [RFC1122] spécifient bien de possibles algorithmes pour la détection de passerelles mortes (un sous ensemble des matériels de détection du problème d'inaccessibilité de voisin).

Le protocole de découverte de voisin fournit une multitude d'améliorations par rapport à l'ensemble des protocoles IPv4 :

La découverte de routeur fait partie de l'ensemble de protocole de base ; les hôtes n'ont pas besoin "d'espionner" les protocoles d'acheminement.

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

Les annonces de routeur portent des préfixes pour une liaison ; il n'est pas nécessaire d'avoir un mécanisme distinct 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, 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 se "répandent" sur 4 milliards (2^32) d'adresses de diffusion groupée ce qui réduit considérablement les interruptions en relation 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, les routeurs peuvent être configuré pour omettre certains préfixes, ou tous, à partir des annonces de routeur. Dans de tels cas, les hôtes supposent que les destinations sont hors-liaison et envoient leur trafic aux routeurs. Un routeur peut alors produire des redirections s'il en est 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 les liaisons qui ne sont pas en diffusion et en support partagé dans lesquelles il n'est pas souhaitable ou possible que les nœuds connaissent tous les préfixes pour les destinations en-liaison.

La détection d'inaccessibilité de voisin fait partie des améliorations de base significatives de la robustesse de la livraison de paquet en présence de routeurs défaillants, partiellement défaillants ou de partitions de liaisons et de nœuds qui changent leurs adresses de couche liaison. Par exemple, les nœuds mobiles peuvent se mouvoir hors-liaison sans perdre la connexité du fait d'antémémoires ARP périmées.

À la différence de ARP, la découverte de voisin détecte les défaillances de demi-liaison (en utilisant la détection d'inaccessibilité de voisin) et évite d'envoyer du trafic aux voisins avec lesquels la connexité bidirectionnelle est absente.

À la différence de la découverte de routeur IPv4, les messages d'annonce de routeur ne contiennent pas de champ Préférence. Le champ Préférence n'est pas nécessaire pour traiter les routeurs de différentes "stabilité" ; la détection d'inaccessibilité de voisin va détecter les routeurs morts et passer à un routeur en état de marche.

L'utilisation des adresses de liaison locale pour identifier de façon univoque les routeurs (pour les annonces de routeur et les messages Redirection) rend possible aux hôtes le maintien des associations de routeurs dans l'éventualité d'une renumérotation de site pour utiliser les nouveaux préfixes mondiaux.

L'utilisation de la limite de bonds égale à 255 tours de découverte de voisin est indifférente pour les envoyeurs hors-liaison qui envoient accidentellement ou intentionnellement des messages ND. Dans IPv4, les envoyeurs hors-liaison peuvent envoyer aussi bien des messages ICMP Redirection que des annonces 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 de mécanismes IP standard d'authentification et de sécurité, selon ce qui est approprié [RFC2402], [RFC2406].

3.2 Types de liaison pris en charge

La découverte de voisin prend en charge des liaisons ayant des propriétés différentes. En présence de certaines propriétés seul un sous-ensemble des mécanismes du protocole de découverte de voisin est pleinement spécifié dans le présent document:

point à point
La découverte de voisin traite ces liaisons juste comme des liaisons de diffusion groupée. (La diffusion groupée peut être fournie de façon triviale sur les liaisons en point à point, et les interfaces peuvent recevoir des adresses de liaison locale.) La découverte de voisin devrait être mise en œuvre comme décrit dans le présent document.

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

accès multiple sans diffusion (NBMA)
Redirection, détection d'inaccessibilité de voisin et détermination du prochain bond devraient être mis en œuvre comme décrit dans le présent document. La résolution d'adresse, et le mécanisme pour la livraison des sollicitations et annonces de routeur sur les liaisons NBMA n'est pas spécifiée dans le présent document. Noter que si les hôtes acceptent la configuration manuelle d'une liste de routeurs par défaut, les hôtes peuvent acquérir dynamiquement les adresses de couche liaison pour leur 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'usage du protocole sur les liaisons en 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 une liaison en support partagé,
- comment un routeur détermine l'adresse de couche liaison d'un hôte, dont il a besoin pour envoyer les messages de redirection à 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 seront possibles à l'avenir.

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

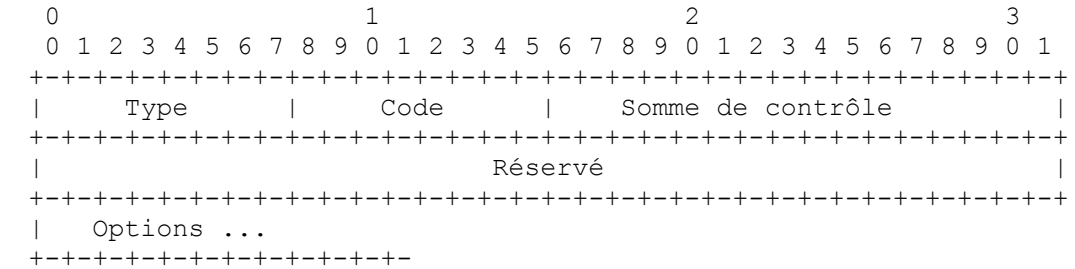
accessibilité asymétrique
La découverte de voisin détecte l'absence d'accessibilité symétrique ; un nœud évite les chemins vers un voisin avec lequel il n'a pas une connexité symétrique.
La détection d'inaccessibilité de voisin va normalement identifier de tels demies liaisons et le nœud va s'abstenir de les utiliser.

Le protocole peut vraisemblablement être étendu à l'avenir pour trouver des chemins viables dans des environnements qui manquent de connexité réflexive et transitive.

4. Formats de message

4.1 Format du message Sollicitation de routeur

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



Champs IP :
Adresse de source
C'est une adresse IP allouée à l'interface d'envoi, ou à l'adresse non spécifiée si aucune adresse n'est allouée à l'interface d'envoi.

Adresse de destination
C'est normalement l'adresse de diffusion groupée Tous les routeurs.

Limite de bonds : 255

En-tête d'authentification

Si une association de sécurité existe pour l'en-tête d'authentification IP entre l'envoyeur et l'adresse de destination, l'envoyeur DEVRAIT alors inclure cet en-tête.

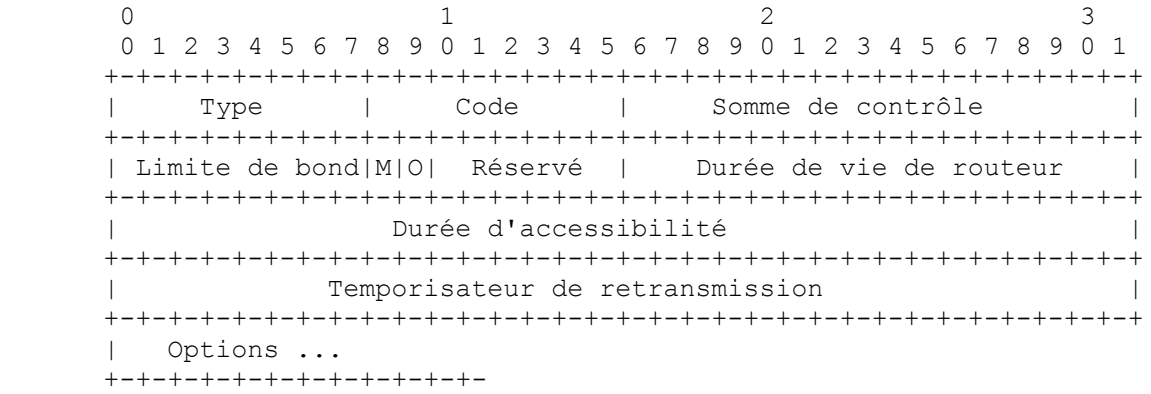
Champs ICMP :
Type : 133
Code : 0
Somme de contrôle : C'est la somme de contrôle ICMP. Voir la [RFC2463].
Réservé : Ce champ n'est pas utilisé. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré par le receveur.

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

Les versions futures 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.

4.2 Format du message d'annonce de routeur

Les routeurs envoient un message Annonce de routeur périodiquement, ou en réponse à une sollicitation de routeur.



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 : C'est normalement l'adresse de source d'une invocation de sollicitation de routeur ou l'adresse de diffusion groupée Tous les nœuds.
Limite de bond : 255
En-tête d'authentification : Si il existe une association de sécurité pour l'en-tête d'authentification IP entre l'envoyeur et l'adresse de destination, l'envoyeur DEVRAIT alors inclure cet en-tête.

Champs ICMP :
Type : 134
Code : 0
Somme de contrôle : C'est la somme de contrôle ICMP. Voir la [RFC2463].
Limite de bond : Entier non signé de 8 bits. La valeur par défaut qui devrait être placée dans le champ Compte de bond de l'en-tête IP pour les paquets IP sortants. Une valeur de zéro signifie "non spécifié" (par ce routeur).
M : Fanion "Configuration d'adresse gérée" de un bit. Lorsque il est mis (à un), les hôtes utilisent le protocole administré (à état plein) pour l'autoconfiguration d'adresse en plus de toutes adresses autoconfigurées en utilisant l'autoconfiguration d'adresse sans état. L'utilisation de ce fanion est décrite dans la [RFC2462].
O : Fanion "Autre configuration à état plein" de un bit. Lorsqu'il est mis (à un), les hôtes utilisent le protocole administré (à état plein) pour l'autoconfiguration des autres informations (autres que d'adresse). L'utilisation de ce fanion est décrite dans la [RFC2462].
Réservé : Champ de 6 bits non utilisé. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré à réception.
Durée de vie de routeur : Entier non signé de 16 bits. C'est la durée de vie associée au routeur par défaut en secondes. La valeur maximum correspond à 18,2 heures. 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 des routeurs par défaut. Durée de vie de routeur ne s'applique qu'à l'utilisation comme routeur par défaut ; elle ne s'applique pas aux informations contenues dans d'autres champs ou options de message. Les options qui ont besoin d'une limite temporelle pour leurs informations comportent leur propre champ de durée de vie.

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

Temporisateur de retransmission : Entier non signé de 32 bits. C'est la durée, en millisecondes, entre les messages Sollicitation de voisin retransmis. Utilisé par la résolution d'adresse et l'algorithme de détection d'inaccessibilité du voisin (voir aux paragraphes 7.2 et 7.3). Une valeur de zéro signifie "Non spécifié" (par ce routeur).

Options possibles :

Adresse de source de couche liaison : C'est l'adresse de couche liaison de l'interface de laquelle est envoyée l'annonce de routeur. N'est utilisée que sur les couches liaison qui ont des adresses. Un routeur PEUT omettre cette option afin de permettre un partage de charge entrante entre plusieurs adresses de couche liaison.

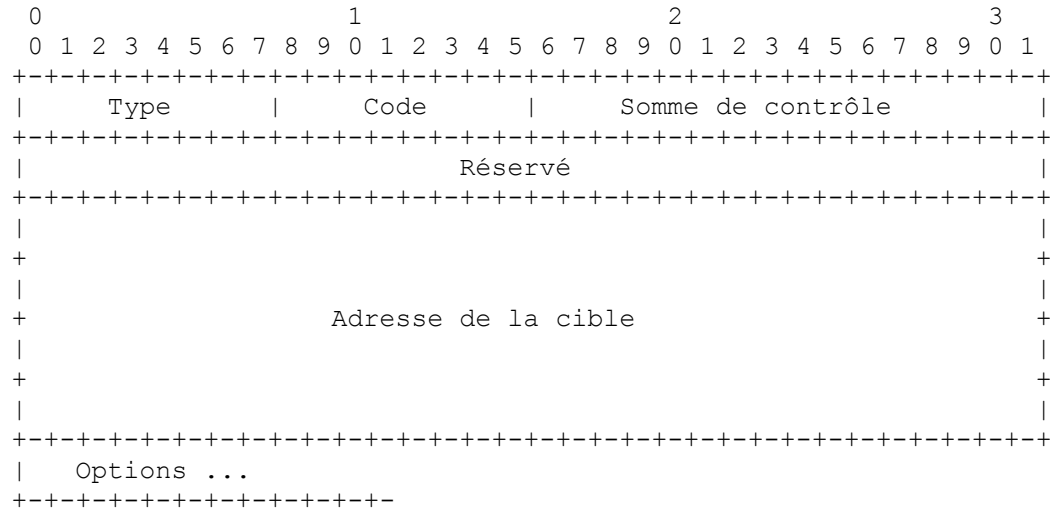
MTU : Elle DEVRAIT être envoyée sur les liaisons qui ont une MTU variable (comme spécifié dans le document qui décrit comment faire fonctionner IP sur le type de liaison particulier). PEUT être envoyé sur d'autres liaisons.

Informations de préfixe : 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 (sauf le préfixe de liaison locale) afin que les hôtes multi rattachements aient des informations de préfixe complètes sur les destinations en-liaison pour les liaisons auxquelles ils se rattachent. Si les 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 du présent 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 de sollicitation de routeur

Les nœuds envoient des sollicitations de voisin pour demander l'adresse de couche liaison d'un nœud cible tout en fournissant 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 : Adresse allouée à l'interface d'où ce message est envoyé ou (si la détection d'adresse dupliquée est en cours [RFC2462]) l'adresse non spécifiée.

Adresse de destination : C'est l'adresse de diffusion groupée du nœud sollicité correspondant à l'adresse cible, ou l'adresse cible.

Limite de bond : 255

En-tête d'authentification : Si une association de sécurité existe pour l'en-tête d'authentification IP entre l'envoyeur et l'adresse de destination, l'envoyeur DEVRAIT alors inclure cet en-tête.

Champs ICMP :

Type : 135

Code : 0

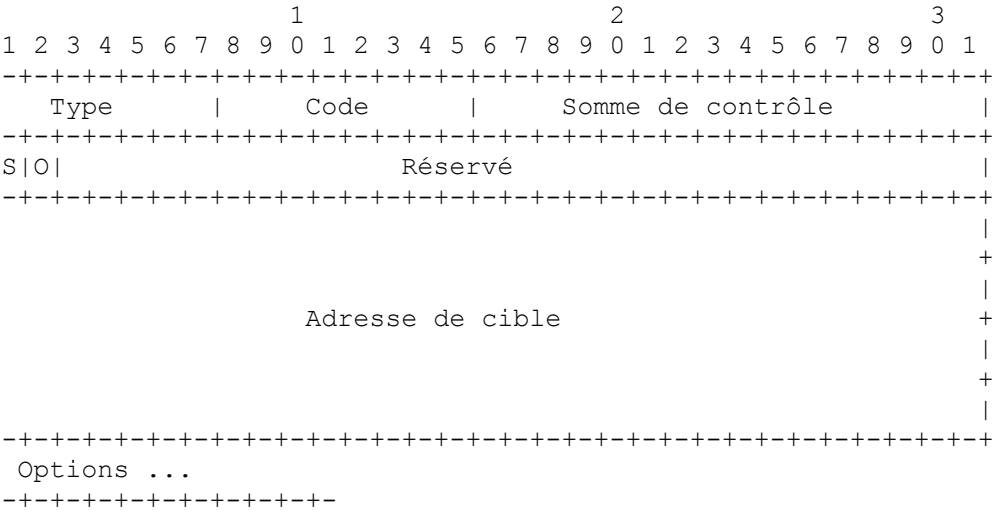
Somme de contrôle : C'est la somme de contrôle ICMP. Voir la [RFC2463].
Réservé : Ce champ est inutilisé. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré à réception.
Adresse de la cible : Adresse IP de la cible de la sollicitation. Elle NE DOIT PAS être une adresse de diffusion groupée.

Options possibles :
Adresse de couche liaison de source : Adresse de couche liaison de l'envoyeur. Elle NE DOIT PAS être incluse lorsque l'adresse IP de source est l'adresse non spécifiée. Autrement, dans les couches en-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.

Les versions futures 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 le traitement du message.

4.4 Format du message d'annonce de voisin

Un nœud envoie des Annonces de voisin en réponse aux Sollicitations 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 qui invoque 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 bond : 255
En-tête d'authentification : Si il existe une association de sécurité pour l'en-tête d'authentification IP entre l'envoyeur et l'adresse de destination, l'envoyeur DEVRAIT alors inclure cet en-tête.

Champs ICMP :
Type : 136
Code : 0
Somme de contrôle : Somme de contrôle ICMP. Voir la [RFC2463].
R : Fanion 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 de 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 de voisin. Il NE DOIT PAS être établi dans les annonces en diffusion groupée ou dans les 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 existante d'antémémoire de voisin pour laquelle il n'est pas connu d'adresse de couche liaison. Il NE DEVRAIT PAS être établi dans les annonces sollicitées pour les adresses d'envoi à la cantonade et dans les annonces de mandataire sollicitées. Il DEVRAIT être établi dans les autres annonces sollicitées et dans les

annonces non sollicitées.

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

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

Options possibles :

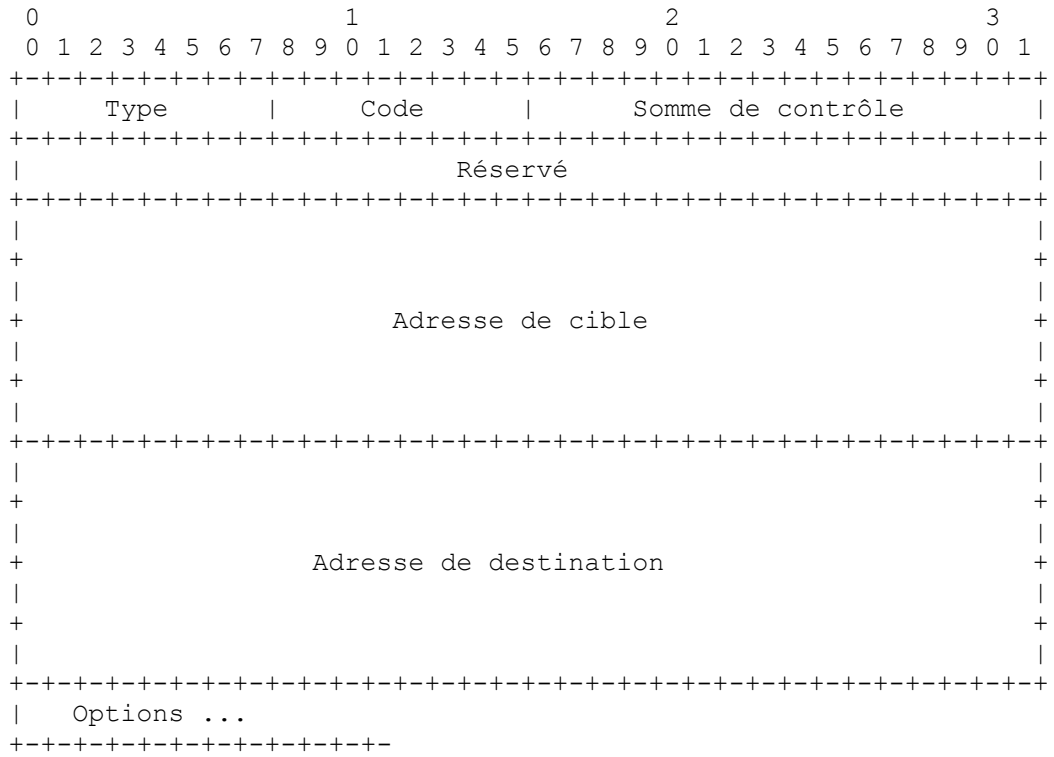
Adresse de couche liaison de la cible : Adresse de couche liaison pour la cible, c'est-à-dire, de l'envoyeur de l'annonce. Cette option DOIT être incluse sur les couches de liaison qui ont des adresses lorsque elles répondent à des sollicitations en diffusion groupée. Lors d'une réponse à une Sollicitation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

L'option DOIT être incluse pour les sollicitations en diffusion groupée afin d'éviter des sollicitations de voisins récurrentes à l'infini lorsque le nœud homologue n'a pas une entrée d'antémémoire à retourner dans 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 de couche liaison correcte ; autrement, il n'aurait pas été capable d'envoyer d'abord la sollicitation en envoi individuel. Cependant, inclure l'adresse de couche liaison dans ce cas ajoute peu de redondance et élimine une condition potentielle de concurrence où 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 vers une destination. Les hôtes peuvent être redirigés sur 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 de 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 déclanche la redirection.

Limite de bond : 255

En-tête d'authentification : Si il existe une association de sécurité pour l'en-tête d'authentification IP entre l'envoyeur et l'adresse de destination, l'envoyeur DEVRAIT alors inclure cet en-tête.

Champs ICMP :

Type : 137

Code : 0

Somme de contrôle : Somme de contrôle ICMP. Voir la [RFC2463].

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

Adresse de cible : Adresse IP qui est un meilleur premier bond à utiliser pour l'adresse de destination ICMP. Lorsque la cible est en fait le point d'extrémité de la communication, c'est-à-dire, lorsque la destination est un voisin, le champ Adresse de 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 de 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 vers la cible.

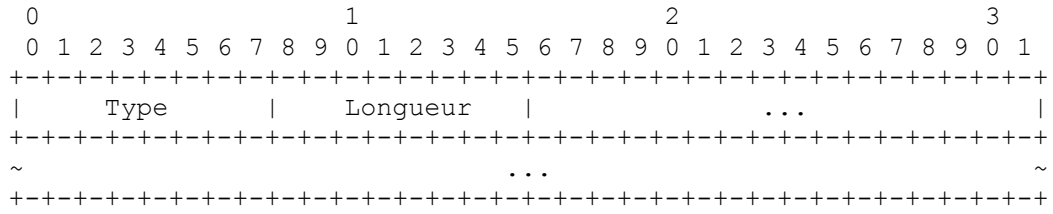
Options possibles :

Adresse de couche liaison de la cible : C'est l'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 de couche liaison de la cible dans les messages Redirection comme moyen pour 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 faire que le paquet redirigé dépasse 1280 octets.

4.6 Formats d'options

Les messages de découverte de voisin comportent zéro, une ou plusieurs options, dont certaines peuvent apparaître plusieurs fois dans le même message. Toutes les options sont de la forme :



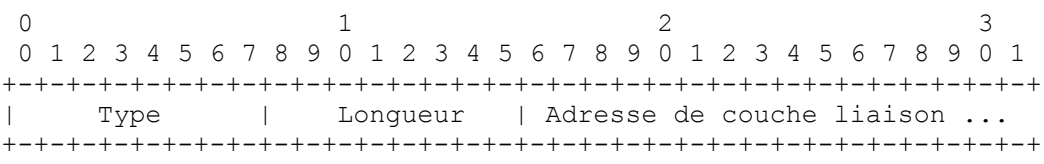
Champs :

Type : identifiant à 8 octets du type de l'option. Les options définies dans le présent document sont :

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

Longueur : Entier non signé de 8 bits. C'est la longueur de l'option (y compris les champs de type et de 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 l'adresse de source de couche liaison, 2 pour l'adresse de cible de couche liaison.

Longueur : C'est la longueur de l'option (y compris les champs Type et Longueur) en unités de 8 octets. Par exemple, la

longueur pour les adresses IEEE 802 est 1 [RFC2464].

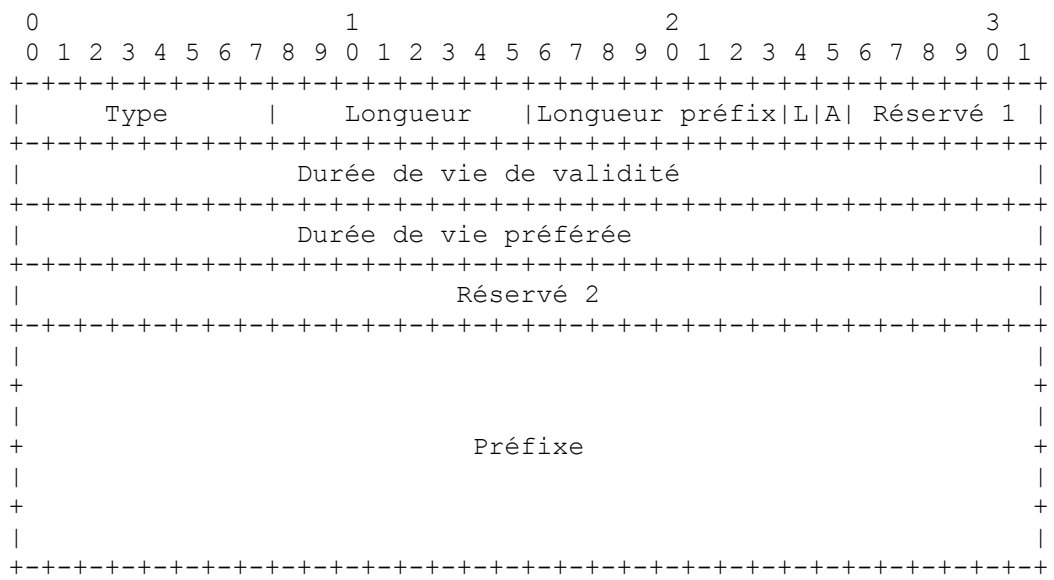
Adresse de couche liaison : C'est l'adresse de couche liaison de longueur variable. Le contenu et le format de ce champ (y compris l'ordre des octets et des bits) sont supposés spécifiés dans les documents spécifiques qui décrivent comment IPv6 fonctionne sur les différentes couches de liaison. Par exemple, la [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 de sollicitation de voisin, de sollicitation de routeur, et d'annonce de routeur.

L'option Adresse de 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 préfix : Entier non signé de 8 bits. Nombre de bits de tête du préfixe qui sont valides. La valeur est dans la gamme de 0 à 128.

L : Fanion en-liaison de 1 bit. Lorsque il est à 1, il indique que ce préfixe peut être utilisé pour la détermination de en-liaison. Lorsque il est à 0, l'annonce ne dit rien sur les propriétés en-liaison ou hors-liaison du préfixe. Par exemple, le préfixe peut être utilisé pour la configuration d'adresse avec certaines des adresses qui appartiennent au préfixe qui sont en-liaison et d'autre hors-liaison.

A : Fanion de 1 bit de configuration autonome d'adresse. Lorsque il est à 1, il indique que ce préfixe peut être utilisé pour la configuration autonome d'adresse comme spécifié dans la [RFC2462].

Réservé 1 : Champ non utilisé de 6 bits. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré à réception.

Durée de vie valide : Entier non signé de 32 bits. C'est la durée en secondes (par rapport à l'heure d'envoi du paquet) pendant laquelle le préfixe est valide pour les besoins de la détermination en-liaison. Une valeur toute de bits à un (0xffffffff) représente l'infini. La durée de vie valide est aussi utilisée par la [RFC2462].

Durée de vie préférée : Entier non signé de 32 bits. C'est la durée en secondes (par rapport à l'heure d'envoi du paquet) pendant laquelle les adresses générées à partir du préfixe via l'autoconfiguration d'adresse sans état restent préférées [RFC2462]. Une valeur toute de bits un (0xffffffff) représente l'infini. Voir la [RFC2462].

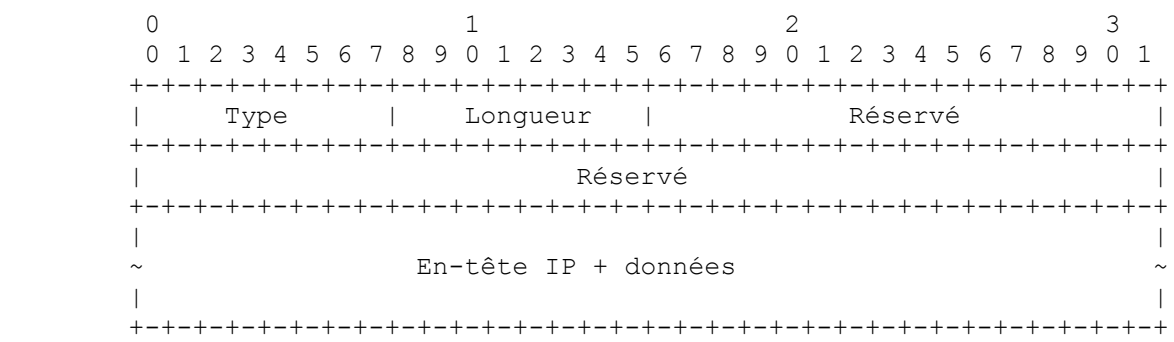
Réservé 2 : Ce champ est non utilisé. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré à réception.

Préfixe : C'est une adresse IP ou un préfixe d'adresse IP. Le champ Longueur de préfixe contient le nombre de bits d'en-tête valides dans le 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 la liaison locale et un hôte DEVRAIT ignorer une telle option de préfixe.

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.

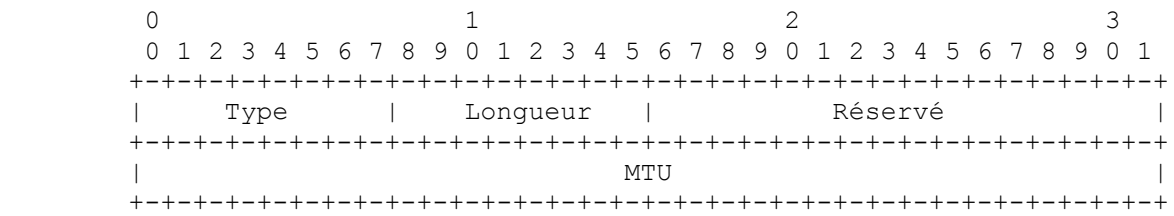
4.6.3 En-tête Redirigé



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 : Le paquet original tronqué pour assurer que la taille du message redirigé ne dépasse pas 1280 octets.
Description : L'option En-tête redirigé est utilisée dans un message 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 : Ce champ est non utilisé. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré à réception.
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 aboutées ensemble, la MTU maximum prise en charge peut différer d'un segment à l'autre. Si les ponts ne génèrent pas de messages ICMP Paquet trop gros, les nœuds communicants seront incapables d'utiliser la MTU de chemin pour déterminer de façon dynamique la MTU appropriée voisin par voisin. Dans de tels cas, les routeurs utilisent l'option MTU pour spécifier la valeur maximum de MTU qui est acceptée par tous les segments.

5. Modèle conceptuel d'un hôte

La présente section décrit un modèle conceptuel d'une organisation possible de structure des données que les hôtes (et dans une certaine mesure les routeurs) vont entretenir en interagissant avec les nœuds du voisinage. 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 l'adhésion des mises en œuvre à ce modèle pour autant que leur comportement externe soit en cohérence avec celui décrit dans le présent document.

Ce modèle ne concerne que les aspects du comportement des hôtes en rapport direct avec la découverte de voisin. En particulier, il ne s'intéresse pas à des questions comme le choix de l'adresse de source ou le choix d'une interface de sortie sur un hôte multi rattachements.

5.1 Structures des données conceptuelles

Les hôtes auront besoin de conserver les éléments d'information suivants pour chaque interface :

Antémémoire de voisin
C'est un ensemble d'entrées sur les voisins individuels auxquels du trafic a été envoyé récemment. Les entrées sont classées sur l'adresse IP d'envoi individuel en-liaison du voisin et contiennent des informations comme son adresse de couche liaison, un fanion qui indique si le voisin est un routeur ou un hôte (appelé IsRouter dans le présent document) un pointeur sur tout paquet mis en file d'attente pendant 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 de sondages sans réponse, et l'heure à laquelle est programmé le prochain événement de détection d'inaccessibilité du voisin.

Antémémoire de destination
C'est un ensemble d'entrées sur les destinations auxquelles du trafic a été envoyé récemment. L'antémémoire de destination comporte aussi bien des destinations en-liaison que hors-liaison et donne un niveau d'adressage indirect dans l'antémémoire de voisin ; l'antémémoire de destination transpose une adresse IP de destination en adresse IP 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, *Path MTU*) et les temporisateurs de délai d'aller-retour entretenus par les protocoles de transport.

Liste des préfixes
C'est une liste des préfixes qui définissent un ensemble d'adresses qui sont en-liaison. Les entrées de la liste des préfixes sont créées à partir des informations reçues dans les annonces de routeur. Chaque entrée a une valeur associée de temporisateur d'invalidation (extraite de l'annonce) qui est utilisée pour périmer les préfixes lorsque ils deviennent invalides. Une valeur spéciale "infini" de 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 ce que les routeurs annoncent comme préfixe pour lui. Les annonces de routeur reçues NE DEVRAIENT PAS modifier le temporisateur d'invalidation pour le préfixe de liaison locale.

Liste de routeurs par défaut
C'est une liste des routeurs auxquels des paquets peuvent être envoyés. Les entrées de la liste des routeurs pointent sur des entrées dans l'antémémoire de voisins ; l'algorithme pour choisir un routeur par défaut favorise les routeurs connus pour être accessibles plutôt que 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 la structure conceptuelle des données ci-dessus peut être mise 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 critique que l'entrée d'antémémoire de voisin pour un routeur soit partagée par toutes les entrées d'antémémoire de destination qui utilisent ce routeur afin d'empêcher des sondages redondants de détection d'inaccessibilité de voisin.

Noter aussi que d'autres protocoles (par exemple, IPv6 Mobile) peuvent ajouter des structures de données conceptuelles supplémentaires. Une mise en œuvre a toute liberté pour appliquer à sa guise de telles structures. Par exemple, une mise en œuvre pourrait fusionner toutes les structures de données conceptuelles en un seul tableau d'acheminement.

L'antémémoire de voisin contient des informations entretenues par l'algorithme de détection d'inaccessibilité du voisin. Un élément d'information clé est l'état d'accessibilité de voisin, qui est une valeur parmi cinq possibles. Les définitions qui suivent 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 (une dizaine de secondes auparavant).

PÉRIMÉ
Le voisin n'est plus connu pour être accessible mais jusqu'à ce que du trafic soit envoyé au voisin, aucune tentative ne devrait être faite pour vérifier son accessibilité.

DELAI
Le voisin n'est plus connu comme accessible, et du trafic a récemment été envoyé au voisin. Plutôt que de sonder immédiatement le voisin, on retarde cependant les sondages pour un bref délai 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 sondages de sollicitation de voisin en envoi individuel vont être envoyés 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 destination, de la liste des préfixes, et de la liste des 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 pour des informations de couche liaison sur ce voisin.

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

Pour des raisons d'efficacité, la détermination du prochain bond n'est pas effectuée sur tous les paquets envoyés. Les résultats du calcul de la détermination du prochain bond sont plutôt sauvegardés dans l'antémémoire de destination (qui contient les mises à jour apprises des messages Redirection). Lorsque le nœud envoyeur a un paquet à envoyer, il examine d'abord l'antémémoire de destination. Si il n'existe aucune 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 du prochain bond est connue, l'envoyeur examine l'antémémoire de voisin pour trouver des 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 le paquet de données en file d'attente en attendant l'achèvement de la résolution d'adresse. Pour les interfaces capables de diffusion groupée, la résolution d'adresse consiste en l'envoi d'un message Sollicitation de voisin et en l'attente d'une annonce de voisin. Lorsque est reçue une réponse d'annonce de voisin, l'adresse de couche liaison est entrée 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 (de diffusion groupée) et elle est considérée comme étant en-liaison. La procédure de détermination de l'adresse de couche liaison correspondant à une adresse de diffusion groupée IP donnée sera trouvée dans un document distinct qui couvre le fonctionnement de IP sur un type de liaison particulier (par exemple, la [RFC2464]).

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

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

Noter que quand un nœud refait la détermination de prochain bond, il n'est pas nécessaire de supprimer l'entrée d'antémémoire de destination complète. En fait, il est généralement profitable de conserver des informations en antémémoire telles que la PMTU et les valeur du temporisateur d'aller-retour qui peuvent aussi être conservées dans l'entrée d'antémémoire de destination.

Les routeurs et les hôtes multi rattachements ont plusieurs interfaces. La suite du présent document 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 par l'interface sur laquelle la sollicitation a été reçue.

5.3 Collecte des déchets et exigences de temporisation

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

Pour être parfaitement exact, 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 de détection d'inaccessibilité du voisin assure que les informations périmées sont purgées rapidement si elles sont réellement utilisées.

Pour limiter la quantité de mémoire nécessaire pour le stockage des antémémoires de destination et de voisin, un nœud peut avoir besoin de mettre au rebut les vieilles entrées. Cependant, il faut faire attention à s'assurer qu'un espace suffisant est toujours présent pour contenir l'ensemble fonctionnel des entrées actives. Une antémémoire petite peut résulter en un nombre excessif de messages de découverte de voisin si les entrées sont éliminées et reconstruites en une succession rapide. Toute politique fondée sur le moins récemment utilisé (LRU, *Least Recently Used*) qui ne conserve que les entrées qui n'ont pas été utilisées pendant une certaine durée (par exemple, dix minutes ou plus) devrait être adéquate pour la mise au rebut des entrées inutilisées.

Un nœud devrait conserver les entrées dans la liste des routeurs par défaut et la liste des préfixes jusqu'à l'arrivée à expiration de leur durée de vie. Cependant, un nœud peut mettre prématurément au rebut des entrées si il est faible en mémoire. Si tous les routeurs ne sont pas conservés 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 maintenir une robuste connexité pour les destinations hors-liaison.

Lorsque une entrée est retirée de la liste des préfixes, il n'est pas besoin de mettre au rebut des entrées des antémémoires de destination ou de voisin. La détection d'inaccessibilité de voisin va purger efficacement toutes les entrées de ces antémémoires qui sont devenues invalides. Cependant, lorsque une entrée est retirée 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 de prochain bond pour choisir un nouveau routeur par défaut.

6. Découverte de routeur et de préfixe

La présente section décrit le comportement du routeur et de l'hôte par rapport à la portion découverte de routeur de la découverte de voisin. La découverte de routeur est utilisée pour localiser les routeurs du voisinage et apprendre les préfixes et les paramètres de configuration qui se rapportent à 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 des 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 d'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 d'information de préfixe. Voir dans la [RFC2462] les détails sur le traitement des informations d'autoconfiguration.

6.1 Validation du message

6.1.1 Validation des messages de sollicitation de routeur

Les hôtes DOIVENT éliminer en silence tous les messages de sollicitation de routeur reçus.

Un routeur DOIT éliminer en silence tous les messages de sollicitation de routeur 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 que le paquet n'aurait pas eu la possibilité d'être transmis

par un routeur.
- Si le message comporte un en-tête d'authentification IP, 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 d'au moins 8 octets.
- Toutes les options incluses ont une longueur supérieure à zéro.
- Si l'adresse de source IP 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 changements non rétro-compatibles peuvent utiliser des valeurs de code différentes.

Le contenu de toute option définie qui n'est pas spécifiée pour être utilisée avec les messages de sollicitation de routeur DOIT être ignoré et le paquet être traité normalement. La seule option définie qui peut apparaître est l'option d'adresse de couche liaison de source.

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

6.1.2 Validation des messages d'annonce de routeur

Un nœud DOIT éliminer en silence tout message Annonce de routeur reçu qui ne satisfait 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 Annonce de routeur et 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, le paquet n'aurait pas pu être retransmis par un routeur.
- Si le message comporte un en-tête Authentification IP, 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 d'au moins 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 au protocole peuvent spécifier le contenu du champ Réservé ou ajouter de nouvelles options ; les changements non rétro-compatibles peuvent 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 Adresse de source de couche liaison, Informations de préfixe 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 la configuration des variables conceptuelles suivantes par la gestion du système. Les noms des variables spécifiques sont utilisés pour les seuls besoins de la démonstration, et une mise en œuvre n'est pas obligée de les avoir, 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 pour certaines des variables énumérées ci-dessous peuvent être supplantées par des documents spécifiques qui décrivent comment fonctionne IPv6 sur 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 très différentes.

Pour chaque interface de diffusion groupée :

AdvSendAdvertisements
C'est un fanion qui indique si le routeur envoie ou non des annonces de routeur périodiques et répond aux sollicitations de routeur.
Par défaut : FAUX

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

MaxRtrAdvInterval
Durée maximum permise entre l'envoi d'annonces de routeur non sollicitées en diffusion groupée à partir de l'interface, en secondes. Elle DOIT n'être pas inférieure à 4 secondes ni supérieure à 1800 secondes.
Par défaut : 600 secondes

MinRtrAdvInterval
Durée minimum permise entre l'envoi d'annonces de routeur non sollicitées en diffusion groupée à partir de l'interface, en secondes. Elle DOIT n'être pas inférieure à 3 secondes ni supérieure à 0,75 * MaxRtrAdvInterval.
Par défaut : 0,33 * MaxRtrAdvInterval

AdvManagedFlag
C'est la valeur VRAI/FAUX à placer dans le champ fanion "Configuration d'adresse gérée" dans l'annonce de routeur. Voir la [RFC2462].
Par défaut : FAUX

AdvOtherConfigFlag
C'est la valeur VRAI/FAUX à placer dans le champ fanion "Autre configuration à état plein" dans l'annonce de routeur. Voir la [RFC2462].
Par défaut : FAUX

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

AdvReachableTime
C'est la valeur à placer dans le champ Durée d'accessibilité dans les messages Annonce de routeur envoyés 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).
Par défaut : 0

AdvRetransTimer
C'est la valeur à placer dans le champ Temporisateur de retransmission dans les messages Annonce de routeur envoyés par le routeur. La valeur zéro signifie non spécifié (par ce routeur).
Par défaut : 0

AdvCurHopLimit
C'est la valeur par défaut à placer dans le champ Limite de bonds en cours dans les messages Annonce de routeur envoyés par le routeur. La valeur devrait être réglée au diamètre actuel de l'Internet. La valeur zéro signifie non spécifié (par ce routeur).
Par défaut : La valeur spécifiée dans "Numéros alloués" [RFC1700] qui est en vigueur au moment de la mise en œuvre.

AdvDefaultLifetime
C'est la valeur à placer dans le champ Durée de vie du routeur des annonces de routeur envoyées 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.
Par défaut : 3 * MaxRtrAdvInterval

AdvPrefixList
C'est une liste de préfixes à placer dans les options Informations de préfixe dans les messages Annonce de routeur envoyés de cette interface.
Par défaut : Tous les préfixes que le routeur annonce via les protocoles d'acheminement comme étant en liaison pour l'interface à partir de laquelle l'annonce est envoyée. Le préfixe de liaison locale NE DEVRAIT PAS être inclus dans la liste des préfixes annoncés.
Chaque préfixe est associé à :

une AdvValidLifetime *(durée de validité de l'annonce)*

C'est la valeur à placer dans la durée de validité dans l'option Informations de préfixe, en secondes. La valeur désignée par des 1 (0xffffffff) représente l'infini. Les mises en œuvre DOIVENT permettre que AdvValidLifetime soit spécifié de deux façons :

- une durée qui se décrémente en temps réel, c'est-à-dire, qui va résulter en une durée de vie de zéro à l'heure

spécifiée, ou
- une durée fixée qui reste la même dans les annonces consécutives.

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

un AdvOnLinkFlag *(fanion d'annonce en liaison)*
C'est la valeur à placer dans le champ Fanion en liaison ("bit L") dans l'option Informations de préfixe.
Par défaut : VRAI

La configuration automatique d'adresse [RFC2462] définit les informations supplémentaires associées à chaque préfixe :

AdvPreferredLifetime
C'est la valeur à placer dans la durée de vie préférée dans l'option Informations de préfixe, en secondes. La valeur désignée par des uns (0xffffffff) représente l'infini. Voir dans la [RFC2462] les détails de la façon dont cette valeur est utilisée. Les mises en œuvre DOIVENT permettre que AdvPreferredLifetime soit spécifiée de deux façons :
- une durée décrémentée en temps réel, c'est-à-dire, qui va résulter en une durée de vie de zéro au moment spécifié, ou
- une durée fixe qui reste la même dans les annonces consécutives.

Par défaut : 604 800 secondes (7 jours), fixe (c'est-à-dire, qui reste la même dans les annonces consécutives).

AdvAutonomousFlag
C'est la valeur à placer dans le champ Fanion autonome dans l'option Informations de préfixe. Voir la [RFC2462].
Par 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 celui des hôtes 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 en état de fonctionnement et activée qui a au moins une adresse IP d'envoi individuel qui lui est allouée et dont le fanion AdvSendAdvertisements correspondant est VRAI. Un routeur NE DOIT PAS envoyer d'annonces de routeur en sortie sur une interface qui n'est pas une interface d'annonce.

Une interface peut devenir une interface d'annonce à d'autres moments que le démarrage du système. Par exemple :
- lors du changement du fanion AdvSendAdvertisements sur une interface activée de FAUX à VRAI, ou
- lors de l'activation administrative de l'interface, si elle a été désactivée administrativement, et si le fanion AdvSendAdvertisements est VRAI, o
- en activant la capacité de transmission IP (c'est-à-dire, en changeant le système de l'état d'hôte à celui de routeur) lorsque le fanion AdvSendAdvertisements de l'interface est VRAI.

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

6.2.3 Contenu du message d'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 conformes au format de message donné au paragraphe 4.2 :
- dans le champ Durée de vie du routeur : la AdvDefaultLifetime configurée de l'interface,
- dans les fanions M et O : respectivement les AdvManagedFlag et AdvOtherConfigFlag configurés de l'interface. Voir la [RFC2462],
- dans le champ Limite de bonds actuelle : la CurHopLimit configurée de l'interface,
- dans le champ Durée d'accessibilité : la AdvReachableTime configurée de l'interface,
- dans le champ Temporisateur de retransmission : le 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 entrante sur des interfaces dupliquées.

o Option MTU : la valeur AdvLinkMTU configurée de l'interface si la valeur est différente de zéro. Si AdvLinkMTU est zéro, l'option MTU n'est pas envoyée.
o Option Information de préfixe : une option Information de préfixe pour chaque préfixe énuméré dans AdvPrefixList avec les champs d'option réglés à partir des informations dans l'entrée de AdvPrefixList comme suit :
- dans le fanion "en-liaison" : le AdvOnLinkFlag de l'entrée,
- dans le champ Durée de validité : la AdvValidLifetime de l'entrée,
- dans le fanion "Configuration autonome d'adresse" : le AdvAutonomousFlag de l'entrée,
- dans le champ Durée de vie préférée : la AdvPreferredLifetime de l'entrée.

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

Un routeur PEUT choisir de ne pas inclure certaines options ou aucune lors de l'envoi d'annonces de routeur non sollicitées. Par exemple, si les durées de vie des préfixes 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 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 le dépassement de la taille de la MTU de liaison par l'annonce, plusieurs annonces peuvent être envoyées, chacune d'elles contenant un sous-ensemble des options.

6.2.4 Envoi d'annonces de routeur non sollicitées

Un hôte NE DOIT PAS 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 provenant d'autres routeurs sur la même liaison [SYNC]. Chaque interface d'annonce a son propre temporisateur. Chaque fois qu'une annonce est envoyée en diffusion groupée à partir d'une interface, le temporisateur est remis à une valeur aléatoire à répartition uniforme comprise entre les valeurs configurées MinRtrAdvInterval et MaxRtrAdvInterval 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 à partir d'une interface lorsque elle devient une interface d'annonce, si l'intervalle aléatoire choisi est supérieur à MAX_INITIAL_RTR_ADVERT_INTERVAL, le temporisateur DEVRAIT à la place être réglé à MAX_INITIAL_RTR_ADVERT_INTERVAL. L'utilisation d'un plus petit intervalle pour les annonces initiales augmente la probabilité qu'un routeur soit découvert rapidement lorsqu'il devient disponible, en présence de possibles pertes de paquets.

Les informations contenues dans les annonces de routeur peuvent changer grâce à des actions de la gestion de 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 de l'état 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 Cessation de l'état d'interface d'annonce

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

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

Noter que la gestion de système peut désactiver la capacité de transmission IP d'un routeur (c'est-à-dire, changer l'état du système de routeur à celui d'hôte) 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 du routeur à zéro.

6.2.6 Traitement des sollicitations de routeur

Un hôte DOIT éliminer en silence tous les messages de sollicitation de routeur reçus.

En plus de l'envoi d'annonces non sollicitées périodiques, un routeur envoie des annonces en réponse aux sollicitations valides reçues sur une interface d'annonce. Un routeur PEUT choisir d'envoyer directement la réponse en envoi individuel à l'adresse de l'hôte solliciteur (si l'adresse de source de la sollicitation n'est pas l'adresse non spécifiée) mais le cas usuel est d'envoyer la réponse en diffusion groupée au groupe 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 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 comprise entre 0 et MAX_RA_DELAY_TIME secondes. (Si une seule annonce est envoyée en réponse à plusieurs sollicitations, le délai est relatif 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 débit 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 une heure plus tardive que celle de la prochaine annonce de routeur en diffusion groupée dont l'envoi est programmé, ignorer le délai aléatoire et envoyer l'annonce à l'heure prévue.
- Si le routeur a envoyé en diffusion groupée une annonce de routeur (sollicitée ou non sollicitée) dans les dernières MIN_DELAY_BETWEEN_RAS secondes, programmer l'envoi de l'annonce à une heure correspondant à MIN_DELAY_BETWEEN_RAS plus la valeur aléatoire après l'envoi de l'annonce précédente. Cela assure la limitation du débit des annonces de routeur en diffusion groupée.
- Autrement, programmer l'envoi d'une annonce de routeur à l'heure donnée par la valeur aléatoire.

Noter qu'il est permis à un routeur d'envoyer en diffusion groupée des annonces de routeur plus fréquemment que ce qui est indiqué par la variable de configuration MinRtrAdvInterval pour autant que les annonces les plus fréquentes soient des réponses aux sollicitation de routeurs. Dans tous les cas, cependant, les annonces non sollicitées en diffusion groupées NE DOIVENT PAS être envoyées plus fréquemment qu'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 voisins du routeur ; les sollicitations qui ont une adresse de source appropriée 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 si 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. S'il n'existe pas d'entrée 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 que les routeurs annoncent des informations cohérentes sur une liaison. Les incohérences détectées indiquent qu'un ou plusieurs routeurs pourraient être mal configurés et DEVRAIENT faire l'objet d'une inscription sur le journal d'événements de gestion du système ou du réseau. L'ensemble minimum d'informations à vérifier inclut :

- les valeurs de Limite de bond actuelle (excepté pour la valeur non spécifiée de zéro),
- les valeurs des fanions M ou O,
- les valeurs de Durée d'accessibilité (excepté pour la valeur non spécifiée de zéro),
- les valeurs du temporisateur de retransmission (excepté pour la valeur non spécifiée de zéro),
- les valeurs dans les options de MTU,
- les durées de vie préférée et de validité pour le même préfixe. Si AdvPreferredLifetime et/ou AdvValidLifetime décrémentent en temps réel comme spécifié au paragraphe 6.2.7, la comparaison de durées de vie ne peut alors pas être comparée au contenu des champs dans l'annonce de routeur mais doit plutôt être comparée à l'heure à laquelle le préfixe va devenir, respectivement, déconseillé et invalidé. Du fait des délais de propagation et éventuellement d'horloges mal synchronisées entre les routeurs, de telles comparaisons DEVRAIENT permettre une plage de battement.

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

Toute autre action à réception des messages Annonce de routeur par un routeur sort du domaine d'application de ce document.

6.2.8 Changement d'adresse de liaison locale

Sur un routeur, l'adresse de liaison locale DEVRAIT changer rarement, si elle le doit jamais. Les nœuds qui reçoivent des 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 des comportements indésirables. Par exemple, un nœud va ignorer les messages Redirection dont il pense qu'ils ont été envoyés par un routeur autre que le routeur de premier bond actuel. 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 lors d'une redirection sur ce routeur.

Utiliser 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 l'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 partie de la vieille adresse de liaison locale avec le champ Durée de vie du routeur réglé à zéro et aussi envoyer en diffusion groupée quelques annonces de routeur à partir de la nouvelle adresse de liaison locale. L'effet global devrait être le même que si une interface cessait d'être une interface d'annonce et qu'une différente commence d'être une interface d'annonce.

6.3 Spécification de l'hôte

6.3.1 Variables de configuration de l'hôte

Aucune.

6.3.2 Variables d'hôte

Un hôte conserve 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 qu'aux fins de la démonstration et les mises en œuvre ne sont pas obligées de les suivre, pour autant que leur comportement externe est cohérent avec celui décrit dans le présent document.

Ces variables ont des valeurs par défaut qui sont subrogées 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 celles de documents spécifiques qui décrivent comment fonctionne IP sur différentes couches de liaison. Cette règle permet à la découverte de voisin de fonctionner sur des liaisons qui ont des caractéristiques de performances très variées.

Pour chaque interface :

LinkMTU
C'est la MTU de la liaison.
Par défaut : la valeur définie dans le document spécifique qui décrit comment IPv6 fonctionne sur la couche de liaison particulière (par exemple, la [RFC2464]).

CurHopLimit
C'est la limite de bonds par défaut à utiliser lors de l'envoi de paquets IP (en envoi individuel).
Par défaut : la valeur spécifiée dans les "Numéros alloués" [RFC1700] qui est en effet au moment de la mise en œuvre.

BaseReachableTime
Valeur de base utilisée pour calculer la valeur aléatoire de Durée d'accessibilité.
Par défaut : REACHABLE_TIME millisecondes.

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

RetransTimer
La durée entre les retransmissions de messages Sollicitation de voisin à un voisin lors de la résolution de l'adresse ou lors d'un essai d'accessibilité d'un voisin.
Par défaut : RETRANS_TIMER millisecondes

6.3.3 Initialisation de l'interface

L'hôte joint l'adresse de diffusion groupée Tous-les-nœuds sur toutes les interfaces capables 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 super ensemble des informations contenues dans une seule annonce de routeur. De plus, les informations peuvent aussi être obtenues par d'autres moyens dynamiques, tels qu'une 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 pour une option (par exemple, Durée de vie sur un préfixe spécifique) diffèrent de celles reçues antérieurement, et si le paramètre/option ne peut avoir qu'une seule valeur, l'information reçue en dernier est considérée faire autorité.

Certains champs d'annonce de routeur (par exemple, Limite de bonds actuelle, Durée d'accessibilité et Temporisateur de retransmission) peuvent contenir une valeur non spécifiée. Dans de tels cas, le paramètre devrait être ignoré et l'hôte devrait continuer d'utiliser la valeur quelle qu'elle soit qu'il utilisait déjà. En particulier, un hôte NE DOIT PAS interpréter la valeur non spécifié comme signifiant un retour à la valeur par défaut qui était utilisée 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 dans l'annonce n'est pas à zéro, créer une nouvelle entrée dans la liste, et initialiser sa valeur de temporisateur d'invalidation à partir du champ Durée de vie du 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 précédemment reçue, remettre son temporisateur d'invalidation à la valeur de la 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 reçue est de zéro, périmer immédiatement l'entrée comme spécifié au paragraphe 6.3.5.

Pour limiter la quantité de mémoire nécessaire pour la liste des routeurs par défaut, un hôte PEUT choisir de ne pas mémoriser toutes les adresses de routeur découvertes via les annonces. Cependant, un hôte DOIT retenir au moins deux adresses de routeur et DEVRAIT en conserver plus. Les sélections de routeur par défaut sont effectuées chaque fois qu'apparaît une défaillance de la communication avec une destination. Donc, plus il y a de routeurs sur la liste, plus il est probable de trouver rapidement un routeur de remplacement qui fonctionne (par exemple, sans avoir à attendre l'arrivée de la prochaine annonce).

Si la valeur de la 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 reçue 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 calculé comme une valeur aléatoire à répartition uniforme sur l'intervalle MIN_RANDOM_FACTOR à MAX_RANDOM_FACTOR fois le BaseReachableTime. Utiliser un composant aléatoire élimine la possibilité que les messages de détection d'inaccessibilité de voisin se synchronisent les uns avec les autres.

Dans la plupart des cas, la valeur de durée d'accessibilité annoncée sera la même dans les annonces de routeur consécutives et la BaseReachableTime d'un hôte change rarement. Dans de tels cas, une mise en œuvre DEVRAIT s'assurer qu'une nouvelle valeur aléatoire est recalculée au moins 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, l'annonce est examinée à la recherche d'options valides. 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 réglé à VRAI. Si aucune adresse de source de couche liaison n'est incluse, mais qu'il existe une entrée d'antémémoire de voisin correspondante, son fanion IsRouter DOIT être réglé à VRAI. Le fanion IsRouter est utilisé par la détection d'inaccessibilité de voisin pour déterminer quand un routeur change d'état pour devenir un hôte (c'est-à-dire, n'est plus capable de transmettre les 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 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 la valeur soit supérieure ou égale à la MTU minimum de liaison de la [RFC2460] et n'excède pas la valeur de LinkMTU par défaut spécifiée dans le document spécifique du type de liaison (par exemple, la [RFC2464]).

L'option Informations de préfixe qui a le fanion "en-liaison" (L) établi *(à 1)* indique 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'informations concernent la détermination "en-liaison" et NE DOIT PAS être interprétée comme signifiant que les adresses couvertes par le préfixe sont hors-liaison. La seule façon d'annuler une indication en-liaison précédente 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 n'est connue sur le statut en-liaison de l'adresse 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. Les raisons pour lesquelles une adresse est traitée comme en-liaison sont spécifiées dans la définition de "en-liaison" au paragraphe 2.1. Les préfixes avec le fanion en-liaison mis à zéro devraient normalement avoir le fanion Autonome établi et être utilisés selon la [RFC2462].

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

- Si le préfixe est celui de la liaison locale, ignorer 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 précédemment, 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 zéro, et si le préfixe n'est pas présent dans la liste de préfixes de l'hôte, ignorer l'option en silence.

L'autoconfiguration d'adresse sans état de la [RFC2462] peut dans certaines circonstances augmenter la durée de validité d'un préfixe ou l'ignorer complètement afin d'empêcher une attaque particulière de déni de service. Cependant, comme les effets du même déni de service ciblé sur la liste de préfixes "en-liaison" ne sont pas catastrophiques (les hôtes enverraient les paquets à un routeur par défaut et recevraient des redirections plutôt que d'envoyer les paquets directement à un voisin) le protocole de découverte de voisin n'impose pas une telle vérification sur les valeurs de durée de vie de préfixes.

Note : Les mises en œuvre peuvent choisir de traiter les aspects en-liaison des préfixes séparément des aspects d'autoconfiguration d'adresse des préfixes, par exemple, en passant une copie de chaque message Annonce de routeur valide aussi bien à la fonction "en-liaison" qu'à la fonction "addrconf". Chaque fonction peut alors fonctionner indépendamment sur les préfixes qui ont le fanion approprié établi.

6.3.5 Fin de temporisation 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 d'antémémoire de destination existante n'a cependant besoin d'être mise à jour. Si un problème d'accessibilité devait survenir avec une entrée d'antémémoire de voisin existante, la détection d'inaccessibilité de voisin effectuerait les actions de récupération nécessaires.

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

6.3.6 Choix du routeur par défaut

L'algorithme de sélection d'un routeur dépend en partie de ce que le routeur est connu pour être ou non 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 n'existe aucune entrée d'antémémoire de destination pour une destination hors-liaison ou lorsque la communication à travers un routeur existant paraît défaillante. Dans des conditions normales, un routeur serait 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 à l'antémémoire de destination causé par les messages Redirection.

La politique de choix des 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) DEVRAIT être préféré aux routeurs dont l'accessibilité est inconnue ou suspecte (c'est-à-dire, dans l'état INCOMPLET, ou pour lesquels il n'existe aucune entrée d'antémémoire de voisin). Une mise en œuvre peut choisir de toujours retourner le même routeur ou de parcourir la liste des routeurs à la façon d'un "round-robin" pour autant qu'elle retourne toujours un routeur accessible ou probablement accessible lorsqu'il en est un disponible.

2) Lorsque aucun routeur sur la liste n'est connu comme 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.

   Parcourir la liste des routeurs dans ce cas assure que tous les routeurs disponibles sont vérifiés 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 sera sondé sur son accessibilité comme effet collatéral.

3) Si la liste des 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 devient activée, un hôte peut ne pas vouloir attendre la prochaine annonce de routeur non sollicitée pour localiser les routeurs par défaut ou apprendre les préfixes. Pour obtenir rapidement les 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 sollicitation de routeurs peuvent être envoyées après n'importe lequel des événements suivants :

- l'interface est initialisée au démarrage du système,
- l'interface est réinitialisée après une défaillance temporaire ou après avoir été temporairement désactivée par la gestion de système,
- le système change de l'état de routeur à celui d'hôte, en ayant sa capacité de transmission IP supprimée par la gestion de système,
- l'hôte se rattache à la liaison pour la première fois,
- l'hôte se ré-attache à une liaison après en avoir été détaché pendant quelques temps.

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

Avant qu'un hôte envoie une sollicitation initiale, il DEVRAIT retarder la transmission d'une durée aléatoire comprise entre 0 et MAX_RTR_SOLICITATION_DELAY. Cela sert à minimiser l'encombrement lorsque de nombreux hôtes commencent sur une liaison au même moment, comme cela peut arriver lors de la récupération après une panne de courant.

Si un hôte a déjà effectué un retard aléatoire depuis que l'interface a été activée (ou réactivée) (par exemple, au titre de la détection d'adresse dupliquée de la [RFC2462]) il n'est pas nécessaire de retarder à nouveau avant d'envoyer le premier message de sollicitation de routeur.

Une fois que l'hôte a envoyé une sollicitation de routeur, et qu'il reçoit une annonce de routeur valide avec une durée de vie de routeur différente de zéro, l'hôte DOIT cesser d'envoyer des sollicitations supplémentaires sur cette interface, jusqu'à la prochaine fois que survient 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 annonces de routeur non sollicitées peuvent être incomplètes (voir au paragraphe 6.2.3) ; les annonces sollicitées sont supposées contenir des informations complètes.

Si un hôte envoie MAX_RTR_SOLICITATIONS sollicitations, et ne reçoit pas d'annonces de routeur après avoir attendu MAX_RTR_SOLICITATION_DELAY secondes après l'envoi de la dernière sollicitation, l'hôte en conclut qu'il n'y a pas de routeur sur la liaison pour les besoins de la [RFC2462]. Cependant, l'hôte continue de recevoir et traiter les messages Annonce de routeur pour le cas où des routeurs apparaîtraient sur la liaison.

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

La présente section décrit les fonctions qui se rapportent aux messages de sollicitation de voisin et d'annonce de voisin et inclut les descriptions de résolution d'adresse et d'algorithme de détection d'inaccessibilité du voisin.

Les messages de sollicitation et d'annonce de voisin sont aussi utilisés pour la détection d'adresse dupliquée telle que spécifiée par la [RFC2462]. En particulier, la détection d'adresse dupliquée envoie des messages de sollicitation de voisin avec une adresse de source non spécifiée qui cible 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 des sollicitations de voisin

Un nœud DOIT éliminer en silence tout message Sollicitation 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 que le paquet n'aurait pas pu avoir été transmis par un routeur,
- si le message comporte un en-tête d'authentification IP, 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 de cible n'est pas une adresse de diffusion groupée,
- toutes les options incluses ont une longueur supérieure à zéro;
- si l'adresse de source IP est l'adresse non spécifiée, l'adresse de destination IP est une adresse de diffusion groupée de nœud sollicité,
- si l'adresse de source IP est l'adresse non spécifiée, il n'y a pas d'option d'adresse de source de couche liaison dans le message.

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

Le contenu de toutes les options définies qui ne sont pas spécifiées pour être utilisées avec les messages Sollicitation de voisin DOIVENT être ignorées 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 les vérifications de validité est appelée une "sollicitation valide".

7.1.2 Validation des annonces de voisin

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

- le champ Limite de bond IP a une valeur de 255, c'est-à-dire que le paquet n'a pas pu avoir été transmis par un routeur,

- si le message comporte un en-tête Authentification IP, 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 d'au moins 24 octets,
- l'adresse cible n'est pas une adresse de diffusion groupée,
- si l'adresse de destination IP 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. Des changements futurs rétro-compatibles du protocole pourront spécifier le contenu du champ Réservé ou ajouter de nouvelles options ; les changements non rétro-compatibles peuvent utiliser des valeurs de code différentes.

Le contenu de toutes les options définies qui ne sont pas spécifiées pour être utilisées avec les messages Annonce de voisin DOIVENT être ignorées et le paquet traité normalement. La seule option définie qui peut apparaître est l'option Adresse de cible de couche liaison.

Une annonce de voisin qui satisfait aux 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 connaissant seulement son adresse IP. 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. La résolution d'adresse n'est jamais effectuée sur des adresses de diffusion groupée.

7.2.1 Initialisation d'interface

Lorsque une interface capable 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 correspondante pour chacune des adresses IP allouées à l'interface.

L'ensemble des adresses allouées à une interface peut changer dans le temps. De nouvelles adresses peuvent être ajoutées et de vieilles adresses peuvent être retirées [RFC2462]. Dans de tels cas, le nœud DOIT, respectivement, se joindre et abandonner l'adresse de diffusion groupée du nœud sollicité correspondant aux nouvelles et aux anciennes adresses. Noter que plusieurs adresses d'envoi individuel peuvent se transposer en la même adresse de diffusion groupée de nœud sollicité; un nœud NE DOIT PAS laisser le groupe de diffusion groupée du nœud sollicité tant que toutes les adresses allouées correspondant à cette adresse de diffusion groupée n'ont pas été supprimées.

7.2.2 Envoi des sollicitations de voisin

Lorsque un nœud a un paquet d'envoi individuel a faire parvenir à un voisin, mais qu'il ne connaît pas l'adresse de couche liaison du voisin, il effectue une résolution d'adresse. Pour les interfaces capables de diffusion groupée, cela entraîne la création d'une entrée d'antémémoire de voisin dans l'état INCOMPLET et la transmission d'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 invitant à la sollicitation est la même qu'une des adresses allouées à l'interface sortante, cette adresse DEVRAIT être placée dans l'adresse de source IP de la sollicitation sortante. Autrement, toute adresse allouée de l'interface devrait être utilisée. Utiliser l'adresse de source du paquet déclencheur lorsque possible assure que le receveur de la sollicitation de voisin installe dans son antémémoire de voisin l'adresse IP qui sera très vraisemblablement utilisée dans le trafic de retour ultérieur et qui appartient à la "connexion" du paquet déclencheur.

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 d'adresse de source de couche liaison. Autrement, l'envoyeur DEVRAIT inclure son adresse de couche liaison (si il en a une) comme option d'adresse de source de couche liaison. Inclure l'adresse de source de couche liaison dans une sollicitation en diffusion groupée est exigé pour donner à la cible une adresse à laquelle il 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 est ici que si l'envoyeur a l'adresse de couche liaison de l'homologue dans son antémémoire, il y a de fortes chances pour que l'homologue ait aussi une entrée dans son antémémoire pour l'envoyeur. Par conséquent, elle n'a pas besoin d'être envoyée.

Tout en attendant que la résolution d'adresse s'achève, l'envoyeur DOIT, pour chaque voisin, conserver une petite file

d'attente de paquets attendant 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 faible valeur. Lorsque une file d'attente déborde, le nouvel arrivant DEVRAIT remplacer la plus ancienne entrée. Une fois que la résolution d'adresse est achevée, le nœud transmet tous les paquets mis en file d'attente.

Tout en attendant une réponse, l'envoyeur DEVRAIT retransmettre les messages Sollicitation de voisin approximativement toutes les RetransTimer millisecondes, même en l'absence de trafic supplémentaire pour le voisin. Les retransmissions DOIVENT être limitées en débit au plus à 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 des indications ICMP Destination injoignable avec le code 3 (Adresse injoignable) pour chaque paquet mis en file d'attente de la résolution d'adresse.

7.2.3 Réception des sollicitations de voisin

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

- l'adresse de cible est une adresse d'envoi individuel "valide" ou une adresse d'envoi à la cantonade allouée à l'interface receveuse [RFC2462],
- l'adresse de cible est une adresse d'envoi individuel pour laquelle le nœud offre un service de mandataire, ou
- l'adresse de cible est une "tentative" d'adresse sur laquelle la détection d'adresse dupliquée est en cours [RFC2462].

Si l'adresse cible est une tentative, la sollicitation de voisin devrait être traitée comme décrit dans la [RFC2462]. Autrement, la description suivante s'applique. Si l'adresse de source n'est pas l'adresse non spécifiée, et sur les couches de 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 une entrée n'existe pas déjà, le nœud DEVRAIT en créer une nouvelle et régler son état d'accessibilité à PÉRIMÉ comme spécifié au paragraphe 7.3.3. Si une entrée existe déjà, et si l'adresse de couche liaison de l'antémémoire diffère de celle reçue dans l'option Adresse de source de couche liaison, 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 voisin est créée, le fanion IsRouter DEVRAIT être réglé à FAUX. Cela 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 sur le fait que l'envoyeur soit un routeur. Dans le cas où l'envoyeur est un routeur, les messages d'annonce de voisin ou d'annonce de routeur suivants seront réglés à la valeur correcte de IsRouter. Si une entrée d'antémémoire de voisin existe déjà, son fanion IsRouter NE DOIT PAS être modifié.

Si l'adresse de source est l'adresse non spécifiée, le nœud NE DOIT PAS créer ou mettre à jour une entrée d'antémémoire de voisin.

Après toute mise à jour de l'antémémoire de voisin, le nœud envoie une réponse d'annonce de voisin comme décrit au paragraphe suivant.

7.2.4 Envoi des annonces de voisin sollicitées

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 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 actuelle afin que la sollicitation ait été reçue. Si l'adresse de destination IP de la sollicitation est une adresse de diffusion groupée, l'option Adresse cible de couche liaison 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 le régler à zéro.

Si l'adresse cible est une adresse d'envoi à la cantonade ou une adresse d'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 mis à zéro. Autrement, le fanion Outrepasser DEVRAIT être mis à un. Le bon réglage du fanion Outrepasser assure que les nœuds donnent la préférence aux annonces qui ne viennent pas de mandataires, même lorsque elles sont reçues après des annonces de mandataire, et assure aussi que la première annonce pour une adresse d'envoi à la cantonade "gagne".

Si la source de la sollicitation est l'adresse non spécifiée, 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 d'envoi à la cantonade l'envoyeur DEVRAIT retarder l'envoi d'une réponse d'une durée

aléatoire comprise entre 0 et MAX_ANYCAST_DELAY_TIME secondes.

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

7.2.5 Réception des annonces de voisin

Lorsque est reçue une annonce de voisin valide (sollicitée ou non sollicitée) l'antémémoire de voisin est examinée pour chercher l'entrée cible. S'il n'existe pas d'entrée, l'annonce DEVRAIT être éliminée en silence. Il n'y a aucun besoin de créer une entrée si il n'en existe pas, car le receveur n'a apparemment initié aucune communication avec la cible.

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

Si l'entrée d'antémémoire de voisin de la cible est dans l'état INCOMPLET lors de la réception de l'annonce, il arrive une des deux choses suivantes : si la couche de liaison a des adresses et si l'option Adresse cible de couche liaison est 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 voisin,
- si le fanion Sollicité de l'annonce est établi, l'état de l'entrée est réglé à ACCESSIBLE, sinon, il est réglé à PÉRIMÉ,
- il règle le fanion IsRouter dans l'entrée d'antémémoire sur la base du fanion Routeur dans l'annonce reçue,
- il envoie tout paquet pour le voisin mis en file d'attente en attendant 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 voisin de la cible est dans un état autre que INCOMPLET lorsque l'annonce est reçue, le traitement devient un petit peu plus complexe. 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 : si l'état de l'entrée est ACCESSIBLE, le régler à PÉRIMÉ, mais ne mettre à jour l'entrée d'aucune autre façon ; autrement, l'annonce reçue devrait être ignorée et on NE DOIT PAS mettre à jour l'antémémoire. Si le fanion Outrepasser est à un, il est mis à zéro et l'adresse de couche liaison fournie est la même que celle de l'antémémoire, ou si aucune option Adresse cible de couche liaison n'a été fournie, l'annonce reçue DOIT mettre à jour l'entrée d'antémémoire de voisin 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 fournie une et qu'elle est différente de l'adresse déjà enregistrée).
- Si le fanion Sollicité est mis, 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 de 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 suggère cependant qu'un voisin a des informations urgentes à annoncer (par exemple, un changement d'adresse de couche liaison). Si l'information urgente indique un changement de ce qu'un nœud utilise actuellement, le nœud devrait vérifier l'accessibilité du (nouveau) chemin lorsque il envoie le prochain paquet. Il n'est pas nécessaire de mettre à jour les annonces non sollicitées qui ne changent pas le contenu de l'antémémoire.
- Le fanion IsRouter dans l'entrée d'antémémoire DOIT être réglé sur la base du fanion Routeur dans l'annonce reçue. Dans les 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 cesse de transmettre les 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 actuellement enregistrée dans l'antémémoire. Si aucune de ces règles ne s'applique, l'annonce invite à une future détection d'inaccessibilité de voisin (si il n'en est pas déjà une en cours) en changeant l'état dans l'entrée d'antémémoire.

7.2.6 Envoi des annonces de voisin non sollicitées

Dans certains cas, un nœud peut être capable de déterminer que son adresse de couche liaison a changé (par exemple, basculage à chaud d'une carte d'interface) et peut souhaiter informer rapidement ses voisins de la nouvelle adresse de couche liaison. Dans de tels cas, un nœud PEUT envoyer jusqu'à MAX_NEIGHBOR_ADVERTISEMENT messages

Annonce de voisin non sollicités 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 mis à zéro, afin d'éviter d'induire en erreur 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 voisin de 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 leur antémémoire. Autrement, ils vont ignorer la nouvelle adresse de couche liaison, choisissant plutôt de vérifier l'adresse en 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 des annonces soient perdues à cause de l'encombrement.

Un mandataire PEUT envoyer en diffusion groupée des annonces de voisin lorsque son adresse de couche liaison change ou quand il est configuré (par la gestion de système ou d'autres mécanismes) pour être mandataire pour une adresse. Si il y a plusieurs nœuds qui fournissent des services de mandataire pour le même ensemble d'adresses, les mandataires DEVRAIENT fournir un mécanisme qui empêche plusieurs mandataires d'envoyer des annonces en diffusion groupée pour une des adresses, afin de réduire le risque d'un trafic de diffusion groupée excessif.

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

Noter que parce que les annonces de voisin non sollicitées ne mettent pas à jour de façon fiable les antémémoires de 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 légèrement plus long.

7.2.7 Envoi des annonces de voisin à la cantonade

Du point de vue de la découverte de voisin, les adresses d'envoi à la cantonade sont traitées juste comme des adresses d'envoi individuel dans la plupart des cas. Comme une adresse d'envoi 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 de voisin sur une adresse d'envoi à la cantonade la traitent comme si c'était une adresse d'envoi individuel. Aucun traitement spécial n'a lieu.

Les nœuds qui ont une adresse d'envoi à la cantonade allouée à une interface la traitent exactement le la même façon que si c'était une adresse d'envoi individuel avec deux exceptions. D'abord, les annonces de voisin envoyées en réponse à une sollicitation de voisin DEVRAIENT être retardées d'une durée aléatoire comprise entre 0 et MAX_ANYCAST_DELAY_TIME secondes pour réduire la probabilité d'encombrement du réseau. Ensuite, le fanion Outrepasser dans les annonces de voisin DEVRAIT être réglé à 0, de sorte que lorsque plusieurs annonces sont reçues, la première annonce reçue soit utilisée plutôt que l'annonce reçue la plus récente.

Comme avec les adresses d'envoi individuel, la détection d'inaccessibilité de voisin assure qu'un nœud détecte rapidement quand le lien avec une adresse d'envoi à la cantonade actuelle devient invalide.

7.2.8 Annonces de voisin mandataire

Dans des circonstances limitées, un routeur PEUT être mandataire pour un ou plusieurs autres nœuds, c'est-à-dire qu'à travers des annonces de voisin, il indique qu'il accepte des paquets qui ne sont pas explicitement adressés à lui-même. Par exemple, un routeur peut accepter des paquets au nom d'un nœud mobile qui s'est déplacé hors-liaison. Les mécanismes utilisés par les mandataires sont identiques aux mécanismes 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 pour lequel il se porte mandataire.

Tous les messages Annonce de voisin mandataire sollicité 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 avoir la préséance sur toute annonce reçue d'un mandataire. Un mandataire PEUT envoyer des annonces non sollicitées avec le fanion Outrepasser réglé à un comme spécifié au paragraphe 7.2.6, mais le faire peut être cause que les annonces de

mandataire subrogent une entrée valide créée 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 comprise entre 0 et MAX_ANYCAST_DELAY_TIME secondes.

7.3 Détection d'inaccessibilité de voisin

La communication avec ou à travers un voisin peut échouer pour de nombreuses raisons à tout moment, y compris pour une défaillance du matériel, le changement à chaud d'une carte d'interface, etc. Si c'est la destination qui est défaillante, aucune récupération n'est possible et la communication échoue. D'un autre côté, si c'est le chemin qui est défaillant, la récupération peut n'être pas possible. Donc, un nœud suit activement l'état d'accessibilité des voisins avec lesquels il échange des paquets.

La détection d'inaccessibilité de 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 de voisin peut aussi être utilisée entre les routeurs, mais elle n'est pas obligée si un mécanisme équivalent est disponible, par exemple, au titre des protocoles d'acheminement.

Lorsque un chemin vers un voisin paraît être défaillant, la procédure spécifique de récupération dépend de la façon dont le voisin est utilisé. Si le voisin est la destination ultime, par exemple, la résolution d'adresse devrait être effectuée à nouveau. Cependant, si le voisin est un routeur, tenter de passer sur un autre routeur devrait être approprié. La récupération spécifique qui a lieu est traitée au titre de la détermination du prochain bond ; la détection d'inaccessibilité de voisin signale la nécessité de la détermination du prochain bond en supprimant une entrée d'antémémoire de voisin.

La détection d'inaccessibilité de voisin n'est effectuée que pour les voisins auxquels sont envoyés des paquets en individuel ; elle n'est pas utilisée lors de l'envoi à des adresses en 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. Une confirmation positive peut être obtenue de deux façons, des indications provenant des protocoles de couche supérieure qui indiquent qu'une connexion fait des "progrès de transmission", ou la réception d'un message Annonce de voisin qui est une réponse à un message Sollicitation de voisin.

Une connexion fait des "progrès de transmission" si les paquets reçus d'un homologue distant ne peuvent arriver que si les 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 précédemment envoyées ont atteint l'homologue. De même, l'arrivée de nouvelles données (non dupliquées) indique que les accusés de réception précédents sont livrés à l'homologue distant. Si les paquets atteignent l'homologue, ils doivent aussi atteindre le prochain bond voisin de l'envoyeur ; et donc les "progrès de transmission" sont une confirmation que le prochain bond voisin est accessible. Pour les destinations hors-liaison, les progrès de transmission impliquent que le routeur de prochain bond est accessible. Lorsque disponible, ces informations de couche supérieure DEVRAIENT être utilisées.

Dans certains cas (par exemple, les protocoles fondés sur UDP et les routeurs qui transmettent des paquets aux hôtes) de telles informations d'accessibilité ne peuvent pas être 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 l'utilisation par le voisin des messages 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 avec le fanion Sollicité réglé à un ne sont envoyées qu'en réponse à une sollicitation de voisin. La réception d'autres messages de découverte de voisin tels que des annonces de routeur et des annonces de voisin avec le fanion Sollicité réglé à zéro NE DOIT PAS être traitée comme une confirmation d'accessibilité. La réception de messages non sollicités ne confirme que le chemin dans la direction de l'envoyeur vers le nœud receveur. À l'opposé, la détection d'inaccessibilité de voisin exige qu'un nœud garde trace de l'accessibilité du chemin de transmission 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 le voisin. Du point de vue de la détection d'inaccessibilité de voisin, seule l'accessibilité du chemin de transmission présente un intérêt.

7.3.2 États des entrées d'antémémoire de voisin

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

INCOMPLET
La résolution d'adresse est 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 avec le voisin fonctionne correctement. Dans l'état ACCESSIBLE, aucune action particulière n'a lieu lorsque les paquets sont envoyés.

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

DELAI
Plus de ReachableTime millisecondes se sont écoulées depuis la réception de la dernière confirmation positive que le chemin de transmission fonctionne correctement, et qu'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 d'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 se sont écoulées depuis la dernière confirmation du fait de l'absence de trafic récent. Sans cette optimisation, l'ouverture d'une connexion TCP après une accalmie du trafic donnerait lieu à des sondages même si la prise de contact en trois phases suivante donnerait presque immédiatement une confirmation d'accessibilité.

SONDE
Une confirmation d'accessibilité est activement recherchée au moyen de la retransmission de sollicitations de voisin toutes les RetransTimer millisecondes jusqu'à réception d'une confirmation d'accessibilité.

7.3.3 Comportement des nœuds

La détection d'inaccessibilité de 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 qui est en antémémoire. Si aucun trafic n'est envoyé au voisin, aucune sonde n'est envoyée.

Lorsque un nœud a besoin d'effectuer une résolution d'adresse sur l'adresse d'un voisin, il crée une entrée dans l'état INCOMPLET et initie la 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. Invoquer la détermination du prochain bond à ce moment assure que des routeurs par défaut de remplacement sont essayés.

Lorsque une confirmation d'accessibilité est reçue (par un avis de la couche supérieure ou par une annonce de voisin sollicitée) l'état d'une entrée se change en 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 aucune adresse de couche liaison n'est en antémémoire).

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

Note : Une mise en œuvre peut en fait différer de changer l'état de ACCESSIBLE en PÉRIMÉ jusqu'à ce qu'un paquet soit envoyé au voisin, c'est-à-dire qu'il n'est pas nécessaire qu'un événement de fin de temporisation explicite soit associé à l'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 règle un temporisateur à expirer dans DELAY_FIRST_PROBE_TIME secondes. Si l'entrée est encore dans l'état DELAI

lors de l'arrivée à expiration du temporisateur, l'état de l'entrée se change en SONDE. Si une 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 individuel au voisin en utilisant l'adresse de couche liaison de l'antémémoire. Lorsque il est dans l'état SONDE, un nœud retransmet les messages Sollicitation de voisin toutes les RetransTimer millisecondes jusqu'à l'obtention d'une confirmation d'accessibilité. Les sondes sont retransmises même si aucun paquet supplémentaire n'est envoyé au voisin. Si aucune réponse n'est reçue après une attente de RetransTimer millisecondes après l'envoi de MAX_UNICAST_SOLICIT sollicitations, les retransmissions cessent et l'entrée DEVRAIT être supprimée. Le trafic ultérieur vers ce voisin va recréer l'entrée et effectuer à nouveau la résolution d'adresse.

Note : Toutes les sollicitations de voisin sont limitées en débit voisin par voisin. Un nœud NE DOIT PAS envoyer de sollicitations de voisin au même voisin plus fréquemment que une fois toutes les RetransTimer millisecondes.

Une entrée d'antémémoire de voisin entre dans l'état PÉRIMÉ lorsque elle est créée par suite de la réception de paquets autres que d'annonces de voisin sollicitées (c'est-à-dire, des sollicitations de routeur, des annonces de routeur, des Redirections, et des sollicitations de voisin). Ces paquets contiennent l'adresse de couche liaison de l'envoyeur ou, dans le cas de Redirection, la cible de la redirection. Cependant, la réception de ces adresses de couche liaison ne confirme pas l'accessibilité du chemin dans la direction de la transmission vers ce nœud. Placer une entrée d'antémémoire de voisin nouvellement créée pour laquelle l'adresse de couche liaison est connue pour être dans l'état PÉRIMÉ donne l'assurance que les défaillances du chemin sont détectées rapidement. De plus, si une adresse de couche liaison en 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 vers la nouvelle adresse de couche liaison fonctionne.

Pour détecter correctement le cas où un routeur change de l'état de routeur à celui d'hôte (par exemple, si sa capacité de transmission IP est éteinte par la gestion de système) un nœud DOIT comparer le champ du fanion Routeur dans tous les messages Annonce de voisin reçus avec le fanion IsRouter enregistré dans l'entrée d'antémémoire de voisin. Lorsqu'un nœud détecte qu'un voisin a cessé d'être un routeur pour devenir un hôte, le nœud 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 sur la liste des routeurs par défaut même si une entrée d'antémémoire de destination l'utilise (par exemple, un hôte a été redirigé sur lui). Dans de tels cas, toutes les entrées d'antémémoire de destination qui font référence à cet (ancien) routeur doivent effectuer à nouveau la détermination de prochain bond avant d'utiliser l'entrée.

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

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, en-liaison). Ceci est accomplis en ayant l'adresse cible ICMP égale à l'adresse de destination ICMP.

Un routeur DOIT être capable de déterminer l'adresse de liaison locale pour chacun de ses routeurs voisins afin de s'assurer que l'adresse cible dans un message Redirection identifie le routeur voisin par son adresse de liaison locale. Pour l'acheminement statique, cette exigence implique que l'adresse du routeur de prochain bond devrait être spécifiée en utilisant l'adresse de liaison locale du routeur. Pour l'acheminement dynamique, cette exigence implique que tous les protocoles d'acheminement IPv6 doivent plus ou moins échanger les adresses de liaison locales des routeurs du voisinage.

8.1 Validation des messages Redirection

Un hôte DOIT éliminer en silence tout message Redirection reçu qui ne satisfait 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 Annonce de routeur et 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 avoir été transmis par un routeur.
- Si le message comporte un en-tête d'authentification IP, 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 d'au moins 40 octets.
- 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 Adresse de destination ICMP dans le message redirection ne contient pas une adresse de diffusion groupée.
- L'adresse cible ICMP est une adresse de liaison locale (lorsque elle redirige vers un routeur) ou la même que l'adresse de destination ICMP (lorsque elle redirige vers 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 futurs changements rétro-compatibles au protocole pourront spécifier le contenu du champ Réservé ou ajouter de nouvelles options ; les changements non rétro-compatibles peuvent utiliser des valeurs de code différentes.

Le contenu de toute option définie qui n'est pas spécifiée pour être utilisée avec les messages Redirection DOIT être ignoré et le paquet traité normalement. Les seules options définies qui peuvent apparaître sont les options Adresse cible de couche liaison et En-tête redirigé.

Un hôte NE DOIT PAS considérer une redirection comme invalide simplement 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 satisfait aux essais de validité est dite une "redirection valide".

8.2 Spécification de routeur

Un routeur DEVRAIT envoyer un message Redirection, sous réserve des limitations de débit, chaque fois qu'il transmet un paquet qui ne lui est pas explicitement adressé (c'est-à-dire un paquet qui n'est pas acheminé de source à travers le routeur) dans lequel :
- le champ Adresse de source du paquet identifie un voisin, et
- le routeur détermine qu'un meilleur nœud de premier bond réside sur la même liaison que le nœud envoyeur pour l'adresse de destination du paquet qui est transmis, et
- l'adresse de destination du paquet n'est pas une adresse de diffusion groupée, et

le paquet redirigé transmis contient, en cohérence avec le 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 réglé à la même valeur que le champ Adresse de destination.
- Dans le champ Adresse de destination : l'adresse de destination du paquet IP invoquant.
- Dans les options :
  - o option Adresse cible de couche liaison : l'adresse de couche liaison de la cible, si elle est connue.
    - o En-tête redirigé : autant du paquet transmis qu'il en peut tenir sans que le paquet redirigé excède 1280 octets.

Un routeur DOIT limiter le taux d'envoi des messages Redirection, afin de limiter la bande passante et les coûts de traitement induits par les messages Redirection lorsque la source ne répond pas correctement aux redirections, ou si la source choisit d'ignorer les messages Redirection non authentifiés. On trouvera d'autres détails sur la limitation du débit des messages d'erreur ICMP dans la [RFC2463].

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

8.3 Spécification d'hôte

Un hôte qui reçoit une redirection valide DEVRAIT mettre à jour son antémémoire de destination en conséquence afin que le trafic ultérieur aille sur la cible spécifiée. S'il n'existe pas une entrée d'antémémoire de destination 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. S'il existe déjà une entrée d'antémémoire et si 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 la même, 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 la même, on ne peut pas déterminer avec fiabilité si l'adresse cible est un routeur. Par conséquent, les entrées d'antémémoire de voisin nouvellement créées ne devraient pas régler le fanion IsRouter à FAUX, alors que les entrées d'antémémoire existantes devraient laisser le fanion inchangé. Si la cible est un routeur, les messages Annonce de voisin ou Annonce de routeur suivants vont mettre à jour IsRouter en conséquence.

Les messages Redirection s'appliquent à tous les flux qui sont envoyés vers une certaine destination. 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 le champ de l'option En-tête redirigé.

Un hôte PEUT avoir un commutateur de configuration qui peut être réglé de façon à lui faire ignorer un message Redirection qui n'a pas d'en-tête d'authentification IP.

Un hôte NE DOIT PAS envoyer de messages Redirection.

9. Extensibilité – traitement des options

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

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

L'ensemble actuel d'options est défini de telle façon que les receveurs peuvent traiter plusieurs options dans le même paquet indépendamment de chacune des autres. Afin de conserver ces propriétés, les futures options DEVRAIENT suivre la règle simple que les options NE DOIVENT PAS dépendre de la présence ou absence d'une autre option. La sémantique d'une option devrait ne 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 préfixes contenue dans un message Annonce de routeur dans un processus d'espace d'utilisateur alors que l'option Adresse de couche liaison dans le même message est traitée par les sous programmes dans le noyau.

2) Si le nombre d'options était cause qu'un paquet excède la MTU d'une liaison, plusieurs paquets peuvent porter des sous-ensembles des options sans aucun changement de sémantique.

3) Les envoyeurs PEUVENT envoyer un sous-ensemble des options dans différents paquets. Par exemple, si la Durée de validité et la Durée de vie préférée d'un préfixe sont assez élevées, il peut n'être pas nécessaire d'inclure l'option Informations de préfixe dans toutes les annonces de routeur. De plus, différents routeurs peuvent 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'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, les options Informations de préfixes).

Si le nombre d'options incluses dans une annonce de routeur cause le dépassement de la MTU de la liaison par la taille de l'annonce, 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 redirigé DOIT être limitée afin que le paquet redirigé entier ne dépasse pas 1280 octets.

La longueur de toute option est un multiple 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 pour s'aligner sur leur frontière naturelle (par exemple, un champ de 16 bits est aligné sur une limite de 16 bits) à l'exception de l'adresse/préfixe IP de 128 bits, qui est alignée 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 incluant l'en-tête IP est limitée à la MTU de la liaison (qui est d'au moins 1280 octets). Lors de l'ajout d'options à un paquet ND, un nœud NE DOIT PAS dépasser la MTU de la liaison.

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

10. Constantes du protocole

Constantes de 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 d'hôte :

MAX_RTR_SOLICITATION_DELAY :	1 seconde
RTR_SOLICITATION_INTERVAL :	4 secondes
MAX_RTR_SOLICITATIONS :	3 transmissions

Constantes de 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 susceptibles de changer dans de futures révisions du protocole.

Les constantes dans la présente spécification peuvent être outrepassées par des documents spécifiques qui décrivent comment IPv6 fonctionne sur différentes couches de liaison.

Cette règle permet à la découverte de voisin de fonctionner sur des liaisons qui ont des caractéristiques de performances variées.

11. Considérations pour la sécurité

La découverte de voisin est sujette à des attaques qui causent l'écoulement des paquets IP vers des lieux inattendus. De telles attaques peuvent être utilisées pour causer des dénis de service mais aussi permettre à des nœuds d'intercepter et éventuellement modifier des paquets destinés à d'autres nœuds.

Le protocole réduit l'exposition à de telles menaces en l'absence d'authentification en ignorant les paquets ND reçus d'envoyeurs hors-liaison. Il est vérifié que le champ Limite de bonds de tous les paquets reçus contient 255, la valeur légale maximum. Parce que les routeurs décrémentent la limite de bond sur tous les paquets qu'ils transmettent, les paquets reçus qui contiennent une limite de bond de 255 doivent avoir été générés à partir d'un voisin.

Un exemple d'attaque de déni de service est lorsque un nœud sur la liaison qui peut envoyer des paquets avec une adresse de source IP arbitraire peut à la fois s'annoncer lui-même comme routeur par défaut et envoyer des messages 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 par l'envoi de 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 champs Durée de vie préférée et Durée de validité réglés à zéro pour tous les préfixes. Une telle attaque serait cause que tous les paquets, à la fois pour les destinations en-liaison et hors-liaison, iraient sur le routeur félon. Ce routeur peut alors examiner de façon sélective, modifier ou éliminer tous les paquets envoyés sur la liaison. La détection d'inaccessibilité de voisin ne va pas détecter un tel trou noir tant que le routeur félon répond poliment aux sondes NUD par une annonce de voisin avec le bit R établi.

De nombreuses couches de liaison sont sujettes à différentes attaques de déni de service telles que d'occuper continuellement la liaison dans les réseaux CSMA/CD (par exemple, en envoyant des paquets étroitement dos à dos ou en envoyant le signal de collision sur la liaison) ou en générant des paquets avec l'adresse MAC de source de quelqu'un d'autre pour tromper, par exemple, les commutateurs Ethernet.

Le modèle de confiance pour les redirections est le même que dans IPv4. Une redirection n'est acceptée que si elle est reçue du routeur même qui est actuellement utilisé pour cette destination. Il est naturel de faire confiance aux routeurs sur la liaison. Si un hôte a été redirigé sur 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 ; l'hôte cible, une fois subverti, peut toujours agir comme routeur caché pour transmettre le 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 éventuellement en présence d'authentification, peut envoyer des messages Annonce de routeur, étant par là capable de causer des dénis de service. De plus, tout voisin peut envoyer des annonces de voisin mandataire aussi bien que des annonces de voisin non sollicitées comme attaque potentielle de déni de service.

Les échanges de paquet de protocole de découverte de voisin peuvent être authentifiés en utilisant l'en-tête d'authentification IP [RFC2402]. Un nœud DEVRAIT inclure un en-tête d'authentification lors de l'envoi de paquets de découverte de voisin si il existe une association de sécurité à utiliser avec l'en-tête d'authentification IP pour l'adresse de destination. Les associations de sécurité peuvent avoir été créées par configuration manuelle ou par l'opération d'un protocole de gestion de clés.

La correction des en-têtes d'authentification reçus dans les paquets de découverte de voisin DOIT être vérifiée et les paquets dont l'authentification est incorrecte DOIVENT être ignorés.

Il DEVRAIT être possible à l'administrateur du système de configurer un nœud pour qu'il ignore tout message de découverte de voisin qui n'est pas authentifié à l'aide de l'en-tête d'authentification ou de l'encapsulation de la charge utile de sécurité. La technique de configuration pour cela DOIT être documentée. Un tel commutateur DEVRAIT par défaut admettre des messages non authentifiés.

Les questions de confidentialité sont traitées par les documents d'architecture de sécurité IP et d'encapsulation de charge utile de sécurité IP [RFC2401], [RFC2406].

12. Considérations sur la dénumérotation

Le protocole de découverte de voisin conjointement avec l'autoconfiguration d'adresse IPv6 [RFC2462] donne des mécanismes qui aident lors des dénumérotages – 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 les nœuds sur la liaison reçoivent à temps les messages Annonce de routeur. Cependant, un hôte pourrait être éteint ou inaccessible pendant une longue période (c'est-à-dire, une machine n'est plus alimentée en énergie pendant des mois après l'achèvement d'un projet). Il est possible de préserver la robustesse du dénumérotage dans de tels cas mais cela fait peser certaines contraintes sur la façon dont les 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 premier août, il est déterminé que le préfixe doit être déconseillé et retiré à cause d'un dénumérotage le premier septembre. Cela peut se faire en réduisant la durée de vie annoncée à une semaine, qui débute le premier août et à mesure que la date limite se rapproche, la durée de vie peut être raccourcie jusqu'au premier 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 premier septembre, il peuvent toujours penser que le préfixe est valide car la dernière durée de vie qu'ils ont reçu était de deux mois. Donc, si un nœud a été débranche le 31 juillet, il pense que le préfixe est valide jusque au 30 septembre. Si ce nœud est rebranché avant le 30 septembre, il peut continuer d'utiliser le vieux préfixe. La seule façon de forcer un nœud à arrêter d'utiliser un préfixe qui été précédemment annoncé avec une durée de vie longue est de faire que ce nœud reçoive une annonce pour ce préfixe qui diminue la durée de vie. La solution dans cet exemple est simple : continuer d'annoncer le préfixe avec une durée de vie de 0 du premier septembre au premier octobre.

En général, afin d'être robuste à l'égard des nœuds qui pourraient être débranchés de la liaison, il est important de garder trace le plus loin dans l'avenir d'un préfixe particulier qui pourrait être vu comme valide par tout nœud sur la liaison. Le préfixe doit alors être annoncé avec une durée de vie de 0 jusqu'à ce moment dans le futur. Ce moment "plus loin dans l'avenir" est simplement le maximum, sur toutes les annonces de routeur, du moment où l'annonce a été envoyée plus la durée de vie du préfixe contenue dans l'annonce.

Ce qui vient d'être exposé a d'importantes implications sur l'utilisation des durées de vie infinies. Si un préfixe est annoncé avec une durée de vie infinie, et si ce préfixe a ultérieurement besoin d'être dénuméroté, il n'est pas souhaitable de continuer d'annoncer pour toujours ce préfixe avec une durée de vie de zéro. Donc, les durées de vie infinies devraient être évitées ou il doit y avoir une limite à la durée pendant laquelle un nœud peut être débranché de la liaison avant qu'il y soit rebranché. Cependant, on ne sait pas trop comment un administrateur de réseau peut mettre en application une limite à la durée pendant laquelle les hôtes comme des ordinateurs portables peuvent être débranchés de la liaison.

Les administrateurs de réseau devrait considérer très sérieusement la possibilité d'utiliser des durées de vie relativement courtes (c'est-à-dire, pas plus de quelques semaines). Bien qu'il puisse paraître que l'utilisation de longues durées de vie aiderait à assurer la robustesse, en réalité un hôte va être incapable de communiquer en l'absence de routeurs fonctionnant correctement. De tels routeurs vont envoyer des annonces de routeur qui contiennent des préfixes appropriés (et actuels). Un hôte connecté à un réseau qui n'a pas de routeur qui fonctionne aura vraisemblablement des problèmes plus sérieux que juste un manque de préfixes et d'adresses valides.

L'exposé ci-dessus ne fait pas la distinction entre les durées de vie préférée et de validité. Pour toutes les question pratiques il est probablement suffisant de suivre la durée de validité car la durée de vie préférée ne va jamais dépasser la durée de validité.

Références

[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.

[RFC1546] C. Partridge, T. Mendez, W. Milliken, "Service d'envoi à la cantonade pour les hôtes", novembre 1993. *(Information)*

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

[RFC1700] J. Reynolds et J. Postel, "Numéros alloués", STD 2, octobre 1994. *(Historique, voir www.iana.org))*

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

[RFC2373] R. Hinden, S. Deering, "Architecture d'adressage IP version 6", juillet 1998. (*Obsolète, voir* RFC3513) *(P.S.)*

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

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

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

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

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

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

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

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.
901 San Antonio Road
Palo Alto, CA 94303
USA
téléphone : +1 650 786 5166
mél : nordmark@sun.com

William Allen Simpson
Daydreamer
Computer Systems Consulting Services
1384 Fontaine
Madison Heights, Michigan 48071
USA
mél : Bill.Simpson@um.cc.umich.edu

Appendice A Hôtes multi rattachements

Un certain nombre de problèmes compliqués surviennent lorsque la découverte de voisin est utilisée par les hôtes qui ont plusieurs interfaces. La présente section n'essaye pas de définir le fonctionnement correct des hôtes multi rattachements par rapport à la découverte de voisin. Elle identifie plutôt les questions qui exigent des études complémentaires. 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) avoir appris des préfixes en-liaison pour les adresses qui résident sur chaque liaison. Lorsque un paquet doit être envoyé à travers un routeur, choisir le "mauvais" routeur peut cependant résulter en un chemin sous optimal ou non fonctionnel. Un certain nombre de problèmes doivent être pris en compte.

1) Afin qu'un routeur envoie une redirection, il doit déterminer si le paquet qu'il transmet a été généré par un voisin. Le test 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. Si l'hôte d'origine est multi rattachements, l'adresse de source qu'il utilise peut cependant appartenir à une interface autre que celle d'où il a été envoyé. Dans de tels cas, un routeur ne va pas envoyer de redirections, et un acheminement sous optimal est vraisemblable. Afin d'être redirigé, l'hôte envoyeur doit toujours envoyer les paquets de l'interface qui correspond à l'adresse de source du paquet sortant. Noter que ce problème ne survient jamais avec les hôtes mono rattachement ; ils n'ont qu'une seule interface.

2) Si le routeur de premier bond choisi n'a pas un chemin pour toutes les destinations, il sera incapable de livrer le paquet. Cependant, la destination peut être accessible à travers un routeur sur une des autres interfaces. La découverte de voisin ne traite pas de ce scénario ; il ne se produit pas dans le cas des non multi rattachement.

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

Si un hôte multi rattachements échoue à recevoir les 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 soulève un certain nombre de problèmes :

1) Si aucune annonce de routeur n'est reçue sur une des interfaces, un hôte multi rattachements n'a aucun moyen de savoir sur quelle interface envoyer les paquets en sortie, même pour des destinations en-liaison. Dans des conditions similaires pour le cas d'hôte mono rattachement, un nœud traite toutes les destinations comme résidant en-liaison, et la communication se poursuit. Dans le cas du multi rattachement, cependant, des informations supplémentaires sont nécessaires pour choisir l'interface sortante appropriée. Autrement, un nœud pourrait tenter d'effectuer la résolution d'adresse sur toutes les interfaces, une démarche d'une complexité significative qui ne se présente pas dans le cas de l'hôte mono rattachement.

2) Si les annonces de routeur sont reçues sur certaines interfaces, mais pas toutes, un hôte multi rattachement va choisir de n'envoyer les paquets que par les interfaces sur lesquelles il a reçu des annonces de routeur. Une hypothèse clé est cependant faite ici, qui est que les routeurs sur ces autres interfaces seront capables d'acheminer les paquets à leur destination ultime, même lorsque ces destinations résident sur le sous-réseau auquel l'envoyeur se connecte, mais sans avoir d'informations de préfixe en-liaison. Si cette hypothèse est FAUSSE, la communication va échouer. Même si l'hypothèse est vérifié, les paquets vont traverser un chemin sous optimal.

Appendice B : Futures extensions

Les extensions possibles pour les études futures sont :

o Utiliser des temporisateurs dynamiques pour être capable de s'adapter aux liaisons qui ont des délais très variables. Cependant, mesurer les délais d'aller-retour exige des accusés de réception et des numéros de séquence afin de faire correspondre les annonces de voisin reçues avec les sollicitation de voisin réelles qui ont déclanché l'annonce. Les développeurs qui souhaitent expérimenter une telle facilité pourraient le faire de façon rétro compatible en définissant une nouvelle option qui porterait les informations nécessaires. Les nœuds qui ne comprendront pas l'option l'ignorerait simplement.

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

o Ajouter des 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, par exemple, sur des liaisons radio.

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

Le présent 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 est cohérent avec celui décrit dans le présent document.

Lorsque on effectue la résolution d'adresse et la détection d'inaccessibilité de 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 une NS en diffusion groupée. Lancer le temporisateur de retransmission	INCOMPLET
INCOMPLET	Expiration du temporisateur de retransmission, moins de N retransmissions	Retransmettre la NS, lancer le temporisateur de retransmission	INCOMPLET
INCOMPLET	Expiration du temporisateur de retransmission, N retransmissions ou plus.	Éliminer l'entrée, Envoyer une erreur ICMP	-
INCOMPLET	NA, Sollicitée = 0, Outrepasser = tout	Enregistrer l'adresse de couche liaison. Envoyer les paquets en attente	PÉRIMÉ
INCOMPLET	NA, Sollicitée =1, Outrepasser = tout	Enregistrer l'adresse de couche liaison. Envoyer les paquets en	ACCESSIBLE

		attente	
!INCOMPLET	NA, Sollicitée =1, Outrepasser = 0 Même adresse de couche liaison qu'en antémémoire	-	ACCESSIBLE
ACCESSIBLE	NA, Sollicitée =1, Outrepasser = 0 Adresse de couche liaison différente de l'antémémoire.	-	PÉRIMÉ
PÉRIMÉ ou SONDE	NA, Sollicitée =1, Outrepasser = 0 Adresse de couche liaison différente de l'antémémoire.	-	inchangé
!INCOMPLET	NA, Sollicitée =1, Outrepasser = 1	Enregistrer l'adresse de couche liaison (si différente).	ACCESSIBLE
!INCOMPLET	NA, Sollicitée =0, Outrepasser = 0	-	inchangé
!INCOMPLET	NA, Sollicitée =0, Outrepasser = 1, Même adresse de couche liaison qu'en antémémoire.	inchangé	-
!INCOMPLET	NA, Sollicitée =0, Outrepasser = 1, Adresse de couche liaison différente 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 du délai.	Envoyer en individuel une sonde NS. Lancer le temporisateur de retransmission	SONDE
SONDE	Fin de temporisation de retransmission, moins de N retransmissions.	Retransmettre la 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 à la source du paquet (pour la sollicitation de voisin, la sollicitation de routeur, et l'annonce de routeur) ou à l'adresse cible (pour les messages Redirection) comme suit :

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

Appendice D Résumé des règles ISROUTER

Cet appendice présente un résumé des règles de gestion du fanion IsRouter comme spécifié dans ce document.

Le fondement de ces règles est que les messages de découverte de voisin 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 sollicitation de routeur est implicitement supposé être un hôte car les routeurs n'ont pas besoin d'envoyer de tels messages.

- L'envoyeur d'une annonce de routeur est implicitement supposé être un routeur.

- Les messages Sollicitation de voisin ne contiennent pas d'indication ni implicite ni explicite sur l'envoyeur. Les hôtes et les routeurs envoient tous deux de tels messages.

- Les messages Annonce de voisin contiennent un fanion IsRouter explicite, le bit R.

- La cible de la redirection, lorsque la cible diffère de l'adresse de destination dans le paquet qui est redirigé, est

implicitement supposée être un routeur. Ceci est une hypothèse naturelle car on s'attend à ce que ce nœud soit capable de transmettre le paquets vers sa destination.

- La cible de la redirection, lorsque la cible est la même que la destination, ne porte pas des informations d'hôte par opposition à des informations de routeur. Tout ce qu'on sait est que la destination (c'est-à-dire la cible) est en-liaison mais elle pourrait être aussi bien un hôte qu'un routeur.

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

Appendice E Questions de mise en œuvre

E.1 Confirmations d'accessibilité

La détection d'inaccessibilité de voisin exige une confirmation explicite du fonctionnement correct d'un chemin de transmission. Pour éviter d'avoir besoin des messages de sonde de sollicitation de voisin, les protocoles de couche supérieure devraient fournir une telle indication lorsque cela peut être fait à faible coût. Des protocoles fiables en mode connexion tels que TCP savent généralement lorsque le chemin de transmission fonctionne. Lorsque TCP envoie (ou reçoit) des données, par exemple, il met à jour ses numéros de séquence de fenêtre, établit et annule les temporisateurs de retransmission, etc. Les scénarios spécifiques qui indiquent habituellement un bon fonctionnement du chemin de transmission incluent :

- La réception d'un accusé de réception qui couvre un numéro de séquence (par exemple, des données) non acquitté précédemment indique que le chemin de transmission fonctionnait au moment où les données ont été envoyées.

- L'achèvement de la prise de contact initiale à 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 des numéros de séquence. Cela s'applique à SYN et à ACK pour l'ouverture active de l'ACK de ce paquet sur l'homologue à ouverture passive.

- La réception de nouvelles données (c'est-à-dire, de données non reçues précédemment) indique que le chemin de transmission fonctionnait au moment où un accusé de réception a été envoyé 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 d'envoi des confirmations d'accessibilités à 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 seul temporisateur d'aller-retour par connexion. Pour les mises en œuvre qui mettent les entrées d'antémémoire de destination en antémémoire au sein des blocs de contrôle, il serait possible de mettre à jour les entrées d'antémémoire de voisin directement (c'est-à-dire, sans une recherche coûteuse) une fois que le paquet TCP a été démultiplexé dans le bloc de contrôle correspondant. Pour les autres mises en œuvre, il serait possible de faire porter la confirmation d'accessibilité sur le prochain paquet soumis à IP en supposant que la mise en œuvre se prémunit contre la péremption de la confirmation portée lorsque aucun paquets n'est envoyé à IP pendant une longue durée.

TCP doit aussi se garder contre l'idée que des informations "périmées" indiquent l'accessibilité actuelle. Par exemple, les nouvelles données reçues 30 minutes après l'ouverture d'une fenêtre ne constituent pas une confirmation du fonctionnement actuel du chemin. Cela indique simplement qu'il y a 30 minutes de cela, la mise à jour de fenêtre a atteint l'homologue , c'est-à-dire que le chemin fonctionnait à ce moment. Une mise en œuvre doit aussi prendre en compte les sondes TCP de fenêtre zéro qui sont envoyées même 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 (RPC, 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 que le serveur ne peut pas déterminer si une demande reçue indique qu'une réponse précédente a éteint 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 échouerait à détecter que le chemin venant du receveur des données ne fonctionne pas, ce qui serait cause qu'aucun des paquets d'accusé de réception n'atteindrait l'envoyeur.

Appendice F Changements par rapport à la RFC1970

- Retrait de toutes les références au champ Priorité IPv6.

- Remplacement de la définition d'adresse de diffusion groupée de nœud sollicité par une référence à la [RFC2373]. Cette spécification dit que "l'adresse de diffusion groupée de nœud sollicité est formée en prenant les 24 bits de moindre poids de l'adresse (en envoi individuel ou en envoi à la cantonade) et en ajoutant ces bits au préfixe FF02:0:0:0:0:1:FF00::/104".

- Mise à jour de la section de références avec les nouveaux numéros de RFC.

- Mise à jour du texte du paragraphe 7.2.5 et des tableaux de l'appendice C pour que la réception d'un message NS ne mette à jour l'état d'une entrée existante d'antémémoire de voisin que si l'adresse de couche liaison est différente de l'adresse de couche liaison enregistrée.

- Ajout d'une vérification explicite au paragraphe 7.1.1 disant que les messages ND provenant d'une adresse non sollicitée doivent être envoyés à l'adresse de diffusion de nœud sollicité ; si ils sont envoyés à une destination en envoi individuel, éliminer en silence.

- Ajout d'une exigence au paragraphe 6.2.1 que les durées de vie soient configurables d'une de deux façons : comme valeur fixe qui ne change pas dans le temps, ou comme valeur qui se décrémente en temps réel.

- Ajout d'un texte au paragraphe 6.2.7 pour atténuer les vérifications de cohérence sur les durées de vie de préfixes lorsque les durées de vie sont configurées pour décrémenter en temps réel. Ceci est nécessaire pour éviter de fausses alarmes dues au délai de propagation de la liaison et au manque de synchronisation des horloges.

- Ajout de texte au paragraphe 6.3.4 pour souligner que la [RFC2462] pourrait ignorer les courte durées de vie mais que la découverte de voisin n'ignore pas les courtes durées de vie de préfixes.

- Précise les règles pour les paquets RS et NS avec une adresse de source non spécifiée. De tels paquets NE DOIVENT PAS inclure d'option Adresse de source de couche liaison ; à vérifier par les receveurs.

- Précision au paragraphe 7.2.3 que les adresses pour lesquelles les nœuds mandataires sont acceptables dans les messages de NS. Le texte précédent ne mentionnait que les adresses d'envoi individuel et à la cantonade allouées à l'interface (c'est-à-dire, il n'était pas clair que les adresses de mandataires soient admises).

- Précision d'une ambiguïté et d'une incohérence concernant le moment où régler le fanion IsRouter dans les entrées d'antémémoire de voisin. Ajout d'un appendice pour récapituler ces règles.

- Ajout d'un paragraphe sur les considérations de dénumérotage pour préciser la durée pendant laquelle les préfixes doivent être annoncés lorsque les durées de vie subissent une réduction.

- Ajout d'un texte sur les règles à la section 7 pour les paquets NS/NA utilisés pour les sondes de NUD afin que les options Adresse de couche de liaison puissent être omises de ces paquets dans certains cas sans causer une récurrence infinie de NS. Précisément, ajout d'un texte qui permet que l'adresse de couche de liaison soit omise dans les sollicitations en envoi individuel (c'est-à-dire, avec un PEUT).

- Changement de la valeur par défaut de AdvValidLifetime de l'infini à 30 jours.

- Changement de la constante "576" en "1280" dans les endroits où son contexte était que toutes les liaisons doivent être capables de porter les paquets IP de taille minimum.

Déclaration complète de droits de reproduction