Groupe de travail Réseau
Request for Comments : 2491
Catégorie : En cours de normalisation

Traduction Claude Brière de L'Isle

G. Armitage, Lucent Technologies
P. Schulter, Bright Tiger Technologies
M. Jork, Digital Equipment GmbH
G. Harter, Compaq
janvier 1999

IPv6 sur réseaux multi accès sans diffusion (NBMA)

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 décrit une architecture générale pour IPv6 sur des réseaux NBMA. Il forme une base pour des documents auxiliaires d'accompagnement qui décrivent les détails de diverses technologies spécifiques de NBMA (telles que l'ATM ou le relais de trame). IPv6 sur l'architecture NBMA permet le fonctionnement conventionnel côté hôte du protocole de découverte de voisin IPv6, tout en prenant aussi en charge l'établissement de "raccourcis" de chemins de transmission NBMA lorsque sont disponibles des liaisons NBMA signalées dynamiquement. Le fonctionnement sur des liaisons NBMA administrativement configurées en point à point est aussi décrit.

Les raccourcis dynamiques NBMA sont réalisés par l'utilisation des opérations du protocole de découverte de voisin IPv6 au sein de liaisons logiques, et de NHRP inter routeurs pour la découverte de destinations NBMA hors liaison. Les raccourcis déclanchés par les flux et les raccourcis explicitement déclanchés par la source sont tous deux pris en charge.

Table des Matières

1. Introduction.

Les réseaux multi accès sans diffusion (NBMA, *Non Broadcast Multiple Access*) peuvent être utilisés de diverses façons. À un extrême, ils peuvent être utilisés pour fournir simplement un service point à point administrativement configurable, suffisant pour interconnecter des routeurs IPv6 (et même des hôtes IPv6, dans certaines situations). À l'autre extrême, les réseaux NBMA qui prennent en charge l'établissement et la suppression dynamique de circuits virtuels (ou leurs équivalents fonctionnels) peuvent être utilisés pour émuler le service fourni à la couche IPv6 par les supports de diffusion conventionnels tels que Ethernet. Cette émulation exige normalement de complexes protocoles de convergence, en particulier pour la prise en charge de la diffusion groupée IPv6.

Le présent document décrit une architecture générale pour IPv6 sur les réseaux NBMA. Il forme une base pour les documents d'accompagnement qui fournissent les détails spécifiques des diverses technologies NBMA (par exemple, l'ATM [17] ou le relais de trame). IPv6 sur l'architecture NBMA permet le fonctionnement conventionnel côté hôte du protocole de découverte de voisin IPv6, tout en prenant aussi en charge l'établissement de chemins en "raccourci'" de transmission NBMA (lorsque sont disponibles des liaisons NBMA à signalisation dynamique).

La majeure partie de ce document est consacrée à l'utilisation des appels à gestion dynamique en point à point et point à multipoint entre des interfaces sur un réseau NBMA. C'est ce qu'on appelle de façon générique les "SVC" dans la suite du document. L'utilisation d'appels point à point à configuration administrative sera aussi exposée. De tels appels sont désignés comme des "PVC". Selon le contexte, les un et les autres peuvent être abrégés en "VC" *(Virtual Circuit)*.

Certains réseaux NBMA peuvent fournir une forme de service sans connexion (par exemple, SMDS). Dans ces cas, un "appel" ou "VC" devra être considéré comme existant implicitement si l'envoyeur a une adresse de destination NBMA à laquelle il peut transmettre des paquets chaque fois qu'il le désire.

1.1 Découverte de voisin.

Une différence clé entre cette architecture et les protocoles IP sur NBMA précédents est son mécanisme pour la prise en charge de la découverte de voisin IPv6.

Le monde d'IPv4 évoluait dans une approche de la résolution d'adresse qui dépendait du fonctionnement de protocoles auxiliaires à la "couche liaison" – en commençant par l'ARP Ethernet (RFC0826 [14]). Dans le monde des réseaux NBMA (*Non Broadcast, Multiple Access*, multi accès sans diffusion) ARP a été appliqué à IPv4 sur SMDS (RFC1209 [13]) et à IPv4 sur ATM (RFC1577 [3]). Plus récemment, le groupe de travail ION a développé NHRP (*Next Hop Resolution Protocol*, protocole de résolution du prochain bond [8]), un protocole général pour effectuer la résolution d'adresse intra-réseau et inter-réseau applicable à toute une gamme de technologies de réseaux NBMA.

Les développeurs de IPv6 ont choisi de s'éloigner de l'approche spécifique de la couche liaison en combinant un certain nombre de tâches dans un protocole appelé Découverte de voisin [7], destiné à être non spécifique à travers un certain nombre de technologies de couche liaison. Une hypothèse clé faite par le protocole actuel de découverte de voisin est que la technologie de liaison qui sous-tend une interface IP donnée est capable de diffusion groupée par nature. Cela n'est pas particulièrement vrai de la plupart des services réseau NBMA, et requiert normalement des protocoles de convergence pour émuler le service désiré. (Le protocole MARS, RFC2022 [5], est un exemple d'un tel protocole de convergence.) Le présent document augmente et optimise le protocole MARS pour qu'il soit utilisé pour la prise en charge de la découverte de voisin IPv6, en généralisant l'applicabilité de la RFC2022 au-delà des réseaux ATM.

1.2 Raccourcis NBMA

Un raccourci est un appel (VC) de niveau NBMA qui connecte directement deux points d'extrémité IP qui sont séparés logiquement par un ou plusieurs routeurs au niveau IP. Les paquets IPv6 qui traversent ce VC sont dits "raccourcir" les routeurs qui sont dans le chemin IPv6 logique entre les points d'extrémité du VC.

Le raccourci NBMA est un mécanisme pour minimiser la consommation de ressources au sein d'un nuage IP sur NBMA (par exemple, des bonds de routeur et des VC NBMA).

Il est important que les raccourcis NBMA soient pris en charge chaque fois que IP est déployé à travers des réseaux NBMA capables de prendre en charge l'établissement dynamique des appels (SVC ou équivalents fonctionnels). Pour IPv6 sur NBMA, la découverte et la gestion du raccourci sont réalisées par un mélange de découverte de voisin et de NHRP.

1.3 Composants clés de IPv6 sur l'architecture NBMA

1.3.1 Réseaux NBMA qui prennent en charge le mode PVC

Lorsque le réseau NBMA est utilisé en mode PVC, chaque PVC va connecter exactement deux nœuds et l'utilisation de la découverte de voisin et autres dispositifs IPv6 est limitée. Les interfaces IPv6/NBMA ont seulement un voisin sur chaque liaison. Les protocoles MARS et NHRP ne sont PAS nécessaires, car les opérations de diffusion et diffusion groupée se résolvent en une opération d'envoi individuel au niveau NBMA. La découverte dynamique de raccourcis n'est pas prise en charge.

Les détails réels des encapsulations et de la génération de jetons de liaison DEVRONT être traités par les documents d'accompagnement qui couvrent les technologies spécifiques de NBMA. Ils DEVRONT se conformer aux directives suivantes :

- Les paquets IPv6 en envoi individuel et en diffusion groupée DEVRONT tous deux être transmis sur des liaisons PVC utilisant l'encapsulation décrite au paragraphe 4.4.1.

- Les jetons d'interface pour les liaisons PVC DEVRONT être construits comme décrit à la section 5. Les jetons d'interface doivent seulement être uniques entre deux nœuds sur la liaison PVC.

Cette utilisation des liaisons PVC ne rend pas obligatoire, ni n'interdit l'utilisation des extensions au protocole de découverte de voisins qui peuvent être développées pour utilisation générale ou pour utilisation dans les connexions PVC (par exemple, la découverte inverse de voisin).

Les documents d'accompagnement spécifiques de NBMA PEUVENT de plus spécifier l'enchaînement de IPv6 sur PPP et de PPP sur des mécanismes NBMA comme approche FACULTATIVE de IPv6 en point à point.

Sauf comme lorsque noté ci-dessus, le reste du présent document se concentre sur le cas de SVC.

1.3.2 Réseaux NBMA qui prennent en charge le mode SVC

Lorsque le réseau NBMA est utilisé en mode SVC, les composantes clés sont :

- Le modèle de voisin IPv6, où les voisins sont découverts par l'utilisation de la diffusion groupée de messages aux membres de la liaison locale IPv6 d'une interface IPv6.
- Le modèle MARS qui permet l'émulation d'une diffusion groupée générale ulilisant des appels en diffusion groupée fournis par le réseau NBMA sous-jacent.
- Le service NHRP pour rechercher les identités NBMA des interfaces IP qui sont logiquement distantes au sens de la topologie IP.
- La modélisation du trafic IP en flux, et facultativement en utilisant l'existence d'un flux comme base des tentatives d'établissement d'une connexion de niveau liaison en raccourci.

En résumé :

La "liaison" IPv6 est généralisée en "Liaison logique" (LL) dans les environnements NBMA (analogue à la généralisation du sous-réseau IP de IPv4 en sous-réseau logique IP dans la RFC1209 et ensuite dans la RFC1577).

Les interfaces IPv6/NBMA utilisent la RFC2022 (MARS) pour la diffusion groupée générale intra-liaison logique. Le protocole MARS lui-même est utilisé pour répartir de façon optimale les messages de découverte au sein de la liaison logique.

Pour les destinations qui ne sont pas actuellement considérées comme des voisins, un hôte envoie les paquets à un de ses routeurs par défaut.

Lorsque il est configuré de façon appropriée, le routeur de sortie d'une liaison logique est chargé de détecter parmi ceux qui passent à travers lui l'existence d'un flux de paquets qui pourrait bénéficier d'une connexion en raccourci.

Tout en continuant à transmettre les paquets du flux de façon conventionnelle, le routeur initie une interrogation NHRP pour l'adresse IP de destination du flux.

Le dernier routeur/NHS (*Next Hop Server,* serveur du prochain bond) avant la cible de l'interrogation NHRP certifie l'adresse NBMA préférée de l'interface de la cible.

Le routeur à l'origine de l'interrogation produit alors une Redirection à la source IP, identifiant la destination du flux comme voisin transitoire.

Le déclanchement à l'initiative de l'hôte de la découverte de raccourci, sans considération de l'existence d'un flux de paquets, est aussi pris en charge par des sollicitations de voisin spécifiques envoyées au routeur par défaut d'un hôte de source.

Un certain nombre d'avantages clés sont au crédit de cette approche :

- La pile de protocoles IPv6 sur les hôtes ne met pas en œuvre des protocoles de découverte de voisin (ND, *Neighbor Discovery*) séparés pour chaque technologie de couche liaison.

- Lorsque la destination d'un flux est sollicitée comme voisin transitoire, l'adresse NBMA retournée sera celle choisie par la destination lorsque le flux a été à l'origine établi par un traitement bond par bond. Cela prend en charge la capacité de ND existante des destinations IPv6 à effectuer leur propre partage dynamique de charge d'interface.

1.4 Terminologie

Les schémas binaires ou les valeurs numériques utilisées pour identifier une interface NBMA particulière au niveau NBMA seront désignées comme une "adresse NBMA". (Un exemple serait une adresse de système d'extrémité ATM (AESA, *ATM End System Address*) quand on applique cette architecture aux réseaux ATM, ou un numéro E.164 quand on applique cette architecture à des réseaux SMDS.)

L'appel qui, une fois établi, est utilisé pour transférer les paquets IP d'une interface NBMA à une autre sera appelé un SVC ou un PVC selon que l'appel est établi de façon dynamique à travers un mécanisme de signalisation, ou établi administrativement. Les mécanismes spécifiques de signalisation utilisés pour établir ou supprimer un SVC seront définis dans les spécifications d'accompagnement spécifiques de NBMA. Certains réseaux NBMA peuvent fournir une forme de service sans connexion (par exemple, SMDS). Dans ce cas, un "appel" ou un "SVC" devra être considéré comme existant implicitement si l'envoyeur a une adresse de destination NBMA à laquelle il peut transmettre les paquets chaque fois qu'il le désire.

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 [16].

1.5 Structure du document

La suite de ce document est structurée comme suit : la Section 2 explique la généralisation de la liaison IPv6 en "Liaison logique" lorsque utilisée sur des réseaux NBMA, et introduit la notion de voisin transitoire. La Section 3 décrit les modifications au protocole MARS pour une distribution efficace des messages ND au sein d'un liaison logique, et les règles et mécanismes pour découvrir les voisins transitoires. La Section 4 traite des règles de base qui gouvernent l'initialisation de l'interface IPv6/NBMA, l'encapsulation du paquet et du message de contrôle, et les règles de la gestion de SVC. La Section 5 décrit les règles générales de construction des jetons d'interface, l'option d'adresse de couche liaison, et les adresses de liaison locales. La Section 6 conclut les sections normatives de ce document. L'Appendice A donne une description non normative des opérations de la découverte de voisin IPv6. L'Appendice B décrit des solutions sous

optimales pour l'émulation de la diffusion groupée des messages de découverte de voisin autour d'une liaison logique. L'Appendice C discute de la suppression d'un raccourci et revoit brièvement les relations futures entre la détection de flux et la transposition des flux en SVC de qualités de service différentes.

2. Liaison logique et voisin transitoire

IPv6 contient les concepts de "en-liaison" et de "hors-liaison". Les voisins sont les nœuds qui sont considérés comme en liaison et dont les adresses de couche liaison peuvent donc être localisées en utilisant la découverte de voisin. En empruntant à la terminologie des définitions du texte de ND :

En-liaison adresse allouée à une interface d'un voisin sur une liaison partagée. Un hôte considère qu'une adresse est en liaison si :
- elle est couverte par un des préfixe de la liaison, ou
- un routeur voisin spécifie l'adresse comme cible d'un message Redirection, ou
- un message Annonce de voisin est reçu pour l'adresse cible, ou
- un message Découverte de voisin est reçu de l'adresse.

Hors-liaison l'opposé de "en liaison" ; une adresse qui n'est allouée à aucune interfaces rattachée à une liaison partagée. Les nœuds hors liaison sont considérés comme n'étant accessibles qu'à travers un des routeurs directement rattachés à la liaison.

L'environnement NBMA complique le sens du mot "liaison" de façon assez semblable à celle dont il compliquait le sens de "sous-réseau" dans le cas d'IPv4. Pour IPv4, cela exigeait la définition du sous-réseau IP logique (LIS, *Logical IP Subnet*) - un ensemble, construit administrativement, d'hôtes qui partageraient les mêmes préfixes d'acheminement (gabarits de réseau et de sous-réseau).

Le présent document considère son analogue IPv6 comme une liaison logique (LL, *Logical Link*).

Une LL consiste en nœuds administrativement configurés comme étant "en-liaison" les uns par rapport aux autres.

Les membres d'une LL sont l'ensemble initial de voisins de l'interface IPv6, et chaque adresse de liaison locale de chaque interface n'a besoin d'être unique que parmi cet ensemble.

On notera que tandis que les membres d'une LL sont des voisins IPv6, il est possible à des voisins de n'être pas, administrativement, membres de la même LL.

Des événements de découverte de voisin peuvent résulter en l'expansion de l'ensemble de voisins d'une interface IPv6. Cependant, cela ne change pas l'ensemble des interfaces qui constituent cette LL. Cela conduit à trois relations possibles entre deux interfaces IPv6 quelconques :
- en LL, voisines.
- hors LL, voisines.
- hors LL, non voisines.

Hors LL voisines représente les connexions "raccourcies", où on s'est assuré que la connexité directe au niveau NBMA est possible avec une cible qui n'est pas un membre de la LL de la source.

Les voisins découverts grâce à des messages non sollicités, tels que des Redirections, sont appelés des "voisins transitoires".

3. Découverte intra-LL et inter-LL

Ce document fait une distinction entre la découverte des voisins au sein d'une liaison logique (intra-LL) et celle des voisins au-delà de la LL (inter-LL). Le but est de permettre que la découverte de voisin aussi bien inter- que intra-LL n'implique aucun changement à la pile de protocoles IPv6 côté hôte pour les interfaces NBMA.

Noter que le paragraphe 1.3.1 s'applique lorsque le réseau NBMA est utilisé pour ne fournir qu'un service configuré en point à point (PVC).

3.1 ND intra-LL sur émulation de diffusion groupée

Le modèle de base de ND suppose qu'une interface de couche liaison va faire quelque chose de significatif avec un paquet ICMPv6 envoyé à une adresse de destination IP de diffusion groupée. (IPv6 suppose que la diffusion groupée fait partie intégrante du service Internet.) Le présent document suppose que la prise en charge de la diffusion groupée sera fournie en utilisant le service MARS de la RFC2022 [5] (dont l'utilisation est généralisée sur d'autres technologies NBMA en plus de l'ATM). Une LL IPv6 se transpose directement en grappe MARS IPv6 de la même façon qu'un LIS IPv4 se transpose directement en une grappe MARS IPv4.

Le but de l'opération intra-LL est que la couche IPv6 soit capable de simplement passer les paquets ICMPv6 en diffusion groupée au pilote IPv6/NBMA sans aucun traitement particulier, spécifique de NBMA. Le mécanisme sous-jacent pour distribuer les messages de découverte de voisin et de routeur devrait alors fonctionner comme prévu.

Le paragraphe 3.1.1 décrit les fonctions supplémentaires qui DEVRONT être requises de tout MARS utilisé conformément au présent document. La discussion de fond sur ces ajouts figure à l'Appendice B.

3.1.1 MARS élargi obligatoire et comportement du client MARS

Les interfaces IPv6/NBMA DEVRONT s'enregistrer comme membres de grappe MARS, comme décrit au paragraphe 4.1, et DEVRONT envoyer certaines classes de paquets IPv6 sortants directement à leur MARS local comme décrit au paragraphe 4.4.2.

Le MARS lui-même DEVRA alors retransmettre ces paquets conformément aux règles suivantes :

- Lorsque le MARS reçoit un paquet IPv6, il examine la base de données des adhérents du groupe pour trouver les adresses NBMA des membres du groupe de destination IPv6.

- Le MARS vérifie alors si chaque membre du groupe a actuellement son VC de contrôle point à point ouvert au MARS. S'il en est ainsi, le MARS envoie une copie du paquet de données directement à chaque membre du groupe sur les VC point à point existants.

- Si un ou plusieurs des membres du groupe découverts n'ont pas un VC point à point ouvert avec le MARS, ou si il n'y a pas de membre du groupe répertorié, le paquet est envoyé à la place à ClusterControlVC. Aucune copie du paquet n'est envoyée sur les VC point à point existants (s'il en est).

3.2 Génération des Redirections inter-LL

Les connexions en raccourci se justifient par le fait que les flux demandeurs de paquets IP peuvent exister entre des paires source/destination qui sont séparées par des frontières d'acheminement IP. Les raccourcis sont créés entre des voisins transitoires.

La clé pour créer des voisins transitoires est le message Redirection (à la section 8 de [7]). IPv6 permet à un routeur d'informer les membres d'une LL qu'il y a un meilleur "premier bond" pour une destination donnée (paragraphe 8.2 de [7]). L'annonce elle-même est réalisée par un message Redirection de routeur, qui peut porter l'adresse de couche liaison de ce meilleur bond.

Un hôte émetteur n'écoute les Redirections de routeur que de la part du routeur qui agit actuellement comme routeur par défaut pour la destination IP à laquelle se réfère la redirection. Si une redirection arrive et indique un meilleur premier bond pour une destination donnée, et fournit une adresse (NBMA) de couche liaison à utiliser comme meilleur premier bond, l'entrée d'antémémoire de voisin associée chez l'hôte de source est mise à jour et son accessibilité réglée à PÉRIMÉ. La mise à jour de l'antémémoire dans ce contexte implique de construire un nouveau VC avec la nouvelle adresse NBMA. Si cela réussit, le vieux VC n'est supprimé que si on n'en a plus besoin (car le vieux VC était avec le routeur, il peut être toujours nécessaire pour les autres paquets provenant de l'hôte qui sont adressés au routeur).

Deux mécanismes sont fournis pour le déclanchement de la découverte d'un meilleur premier bond :
- L'identification/détection du flux fondée sur le routeur ;
- La demande de raccourci à l'initiative de l'hôte.

Le paragraphe 3.2.1 expose le déclanchement fondé sur le flux, le paragraphe 3.2.2 discute du déclanchement initié par l'hôte, et le paragraphe 3.2.3 décrit l'utilisation de NHRP pour découvrir les transpositions des cibles IPv6 dans les LL distantes.

3.2.1 Redirection déclanchée par le flux

La modification des chemins de transmission sur la base de la détection dynamique des flux de paquets IP est au cœur de modèles tels que celui du routeur à commutation de cellules [11] et du commutateur IP [12]. La responsabilité de la détection des flux est placée dans les routeurs, où les paquets franchissent les bordures des frontières d'acheminement IP.

Pour les besoins de la conformité au présent document, un routeur PEUT choisir d'initier la découverte d'une meilleur premier bond lorsque il détermine qu'un flux identifiable de paquets IP passe à travers lui.

Un tel routeur :
- DEVRA seulement traquer les flux qui sont générés par un hôte directement rattaché (un hôte qui est au sein de la portée de LL locale d'une des interfaces du routeur).
- NE DEVRA PAS utiliser les paquets IP qui arrivent d'un autre routeur pour déclancher la génération d'une Redirection de routeur.
- DEVRA seulement considérer les paquets IPv6 qui ont un FlowID de zéro pour les besoins de la détection de flux comme définie dans cette section.
- DEVRA utiliser NHRP comme décrit au paragraphe 3.2.3 pour s'assurer d'un meilleur premier bond lorsque un flux convenable est détecté, et annoncer les informations dans une Redirection de routeur.

Les routeurs IPv6 qui prennent en charge le comportement FACULTATIF de détection de flux décrit ci-dessus DEVRONT prendre en charge les mécanismes administratifs pour désactiver la détection de flux. Ils PEUVENT fournir des mécanismes pour ajouter des contraintes supplémentaires aux catégories de paquets IPv6 qui constituent un "flux".

Le ou les algorithmes réels pour la détermination des séquences de paquets IPv6 qui constituent un "flux" sortent du domaine d'application du présent document. L'appendice C expose les raisons de l'utilisation d'un FlowID différent de zéro pour supprimer la détection de flux.

3.2.2 Redirection déclanchée par l'hôte

Un hôte de source PEUT aussi déclancher une redirection vers un voisin transitoire.
Pour prendre en charge les redirections déclanchées par les hôtes,les routeurs conformes au présent document DEVRONT reconnaître les messages Sollicitation de voisin (NS, *Neighbor Solicitation*) spécifiques envoyés par les hôtes comme demandes de résolution d'adresses hors liaison.

Pour effectuer une redirection déclanchée par l'hôte, un hôte de source DEVRA :
- Créer un message Sollicitation de voisin se référant à la destination (cible) hors LL pour laquelle un raccourci est désiré.
- Adresser le message NS au routeur qui serait le prochain bond pour le trafic envoyé vers la cible hors LL (plutôt qu'à l'adresse de diffusion groupée de nœud sollicité de la cible).
- Utiliser la limite de bond ND standard de 255 pour s'assurer que les NS ne seront pas éliminés par le routeur.
- Inclure l'option Limite de raccourci définie à l'Appendice D. La valeur de cette option devrait être égale à la limite de bonds du flux de données pour laquelle ce déclanchement est envoyé. Cela assure que le routeur est capable de restreindre les tentatives de raccourci pour ne pas excéder la portée du flux de données.
- Transmettre le paquet NS au routeur qui serait le prochain bond pour le trafic envoyé vers la cible hors LL.

Les routeurs DEVRONT considérer un NS en envoi individuel avec l'option Limite de raccourci comme une demande de redirection déclanchée par l'hôte. Cependant, la découverte de raccourci est FACULTATIVE pour Ies routeurs IPv6.

Lorsque la découverte de raccourci n'est pas prise en charge, le routeur DEVRA construire un message Redirection qui identifie le routeur lui-même comme le meilleur raccourci, et le retourner à l'hôte solliciteur.

Si la découverte de raccourci doit être prise en charge, la réponse du routeur DEVRA être :

- Une demande NHRP convenable construite et envoyée comme décrit au paragraphe 3.2.3. Le message NS d'origine DEFRAIT être éliminé.

- Une fois que la Réponse NHRP est reçue par le routeur d'origine, le routeur DEVRA construire un message Redirection contenant l'adresse IPv6 du voisin transitoire, et l'adresse NBMA de couche liaison retournée par le processus de résolution NHRP.

- Le message Redirection résultant DEVRA alors être retransmis à l'hôte de source. Lorsque le message Redirection est reçu, l'hôte de source DEVRA mettre à jour ses antémémoires de voisin et de destination.

- La cible hors LL est maintenant considérée comme un voisin transitoire. Le prochain paquet envoyé au voisin transitoire va résulter en la création du VC raccourci direct (pour la cible hors LL elle-même, ou pour le meilleur routeur de sortie vers ce voisin, comme déterminé par NHRP).

- Si un NAK NHRP, ou une indication d'erreur est reçue pour une tentative de raccourci déclanchée par un hôte, le routeur demandeur DEVRA construire un message Redirection identifiant le routeur lui-même comme meilleur "raccourci", et le retourner à l'hôte solliciteur.

3.2.3 Utilisation de NHRP entre routeurs

Une fois qu'est survenue la détection de flux, ou qu'un déclanchement par un hôte a été détecté, les routeurs DEVRONT utiliser NHRP en mode NHS à NHS pour établir la transposition de IPv6 en adresse de niveau liaison d'un meilleur premier bond.

Les routeurs IPv6/NBMA qui prennent en charge la découverte de raccourci devront effectuer certaines ou toutes les fonctions suivantes :
- Construire les demandes et réponses NHRP.
- Analyser les demandes et réponses NHRP entrantes de la part des autres (routeurs) NHS.
- Transmettre les demandes NHRP vers un NHS topologiquement plus proche de la cible IPv6.
- Transmettre les réponses NHRP vers un NHS topologiquement plus proche du demandeur.
- Effectuer la traduction syntaxique entre les sollicitations de voisin et les demandes NHRP externes.
- Effectuer la traduction syntaxique entre les réponses NHRP externes et les redirections.

La destination du flux qui a causé le déclanchement (ou la cible du déclanchement initié par l'hôte) est utilisée comme cible pour la résolution dans une demande NHRP. Le routeur transmet alors cette demande NHRP au prochain plus proche NHS. Le processus continue (comme il l'aurait fait pour un NHRP normal) jusqu'à ce que la demande atteigne un NHS qui pense que la cible IP est dans la portée de liaison locale de l'une de ses interfaces. (Cela peut survenir au sein d'un seul routeur.)

Comme les demandes de résolution NHRP suivent toujours le chemin tracé pour une adresse de protocole d'une cible donnée, la portée d'une demande de raccourci sera automatiquement limitée à la portée de l'adresse IPv6 de la cible. (Par exemple, les demandes de résolution pour des adresses de site local ne seront pas transmises à travers les frontières du site.)

Le routeur du dernier bond DEVRA résoudre la demande NHRP à partir des informations de transposition contenues dans son antémémoire de voisins pour l'interface sur laquelle la cible spécifiée est joignable. Si il n'y a pas d'entrée appropriée dans l'antémémoire de voisins, ou si la destination est actuellement considérée comme injoignable, le routeur du dernier bond DEVRA effectuer une découverte de voisin sur l'interface locale, et construire la réponse NHRP à partir de la réponse résultante. (Noter, dans le cas où la demande NHRP a été générée à la suite d'une détection de flux, qu'il doit déjà y avoir un flux de paquets bond par bond qui passe par le routeur de dernier bond vers la cible. Dans ce cas typique, l'antémémoire de voisins aura déjà les informations désirées.)

La réponse NHRP est propagée en retour vers la source de la demande NHRP, en utilisant un chemin bond par bond comme dans un NHRP normal.

Si le processus de découverte a été déclanché à travers une détection de flux chez le routeur d'origine, le retour de la réponse NHRP a pour résultat les événements suivants :

- Une Redirection est construite en utilisant la transposition IPv6/NBMA portée dans la réponse NHRP.

- La Redirection est en envoi individuel pour la source du flux de paquets IP (en utilisant le VC sur lequel le flux est arrivé chez le routeur, si c'est un VC bidirectionnel point à point).

- Tout message Redirection envoyé par un routeur DOIT se conformer à toutes les règles décrites dans [7] afin que le paquet soit correctement validé par l'hôte qui le reçoit. Précisément, si la cible du raccourci résultant est l'hôte de destination, l'adresse cible ICMP DOIT être la même que l'adresse ICMP de destination dans le message d'origine. Si la cible du raccourci est un routeur de sortie, l'adresse ICMP de cible DOIT être une adresse de liaison locale du routeur de sortie qui soit unique pour le nuage NBMA auquel est rattachée l'interface NBMA du routeur.

- Noter aussi que les routeurs de sortie peuvent ensuite rediriger l'hôte de source. Pour ce faire, l'adresse de source ICMP de liaison locale du message Redirection DOIT être la même que l'adresse cible ICMP de liaison locale du message Redirection d'origine.

Noter que le routeur qui construit la réponse NHRP le fait en utilisant l'adresse NBMA retournée par l'hôte cible lorsque celui-ci a d'abord accepté le flux de trafic IP. Cela conserve une caractéristique utile de la découverte de voisin, le partage de charge des interfaces de destination.

À réception d'une réponse NAK NHRP, ou d'une indication d'erreur pour une tentative de raccourci déclanchée par le flux, aucune indication n'est envoyée à la source du flux.

3.2.3.1 Règles de traduction de paquet NHRP/ND

Les règles de traduction suivantes sont destinées à augmenter la spécification du format de paquet de la section 5 de la spécification NHRP [8], qui couvrent les champs du paquet utilisés spécifiquement par l'architecture IPv6/NBMA.

Les messages NHRP sont construits et envoyés conformément aux règles de [8]. La valeur des champs spécifiques de la technologie NBMA tels que arafn, arpro.type, ar$pro.snap et le format d'adresse de couche liaison est définie dans les documents d'accompagnement spécifiques de NBMA. Les adresses de source, de destination ou de protocole client dans l'en-tête commun ou une entrée d'informations client (CIE, *Client Information Entry*) d'un message NHRP sont toujours des adresses IPv6 de 16 octets.

Pour construire une demande de résolution NHRP déclanchée par l'hôte en réponse à une sollicitation de voisin :

- Le champ ar$hopcnt DOIT être plus petit que la valeur limite du raccourci spécifiée dans l'option Limite de raccourci incluse dans le message NS déclancheur. Cela assure que les hôtes ont le contrôle de la portée de leur demande de raccourci. Noter que la limite de raccourci donnée dans l'option est relative à l'hôte demandeur, et donc l'exigence est que ar$hopcnt soit plus petit que la limite de raccourci donnée.

- Le champ Fanions dans l'en-tête commun de la demande de résolution NHRP DEVRAIT avoir les bits Q et S établis.

- Le bit U DEVRAIT être établi. Les adresses NBMA et de source de protocole sont celles du routeur qui construit la demande.

- L'adresse cible provenant du message NS est utilisée comme adresse NHRP de protocole de destination. Une CIE NE DEVRA PAS être spécifiée.

Pour construire une demande de résolution NHRP par suite d'une détection de flux, le choix des valeurs dépend de la configuration.

Une réponse de résolution NHRP est construite conformément aux règles de [8].

Pour chaque CIE retournée, le temps de garde est de 10 minutes.

La MTU peut être 0 ou une valeur spécifiée dans le document d'accompagnement spécifique de NBMA.

Une réponse réussie de résolution NHRP pour une tentative de raccourci déclanchée par l'hôte est traduite comme suit dans un message Redirection IPv6 :

Champs IP :
Adresse de source : adresse de liaison locale allouée à l'interface du routeur à partir de laquelle ce message est envoyé.
Adresse de destination : adresse IPv6 de source du NS déclencheur.
Limite de bond : 255

Champs ICMP :
Adresse cible : adresse NHRP du protocole client.
Adresse de destination : cible du NS déclencheur (c'est équivalent à l'adresse NHRP du protocole de destination).
Adresse cible de couche liaison : adresse NHRP du client NBMA

Toutes les extensions NHRP actuellement définies dans [8] ont un effet nul sur la traduction NHRP/ND et PEUVENT être utilisées dans les messages NHRP pour IPv6.

3.2.3.2 Règles de purge de NHRP

Les purges sont générées par NHRP lorsque on détecte des changements qui invalident une réponse NHRP précédemment produite (cela peut inclure des changements topologiques, ou la défaillance d'un hôte cible ou un changement d'identité). Tout raccourci IPv6 établi précédemment sur la base d'informations nouvellement purgées DEVRAIT être supprimé.

Les routeurs DEVRONT garder trace des entrées d'antémémoire NHRP pour lesquelles ils ont produit des annonces de voisin ou des redirections de routeur. Si une purge NHRP reçue invalide des informations précédemment produites à l'hôte local, le routeur DEVRA produire une redirection de routeur qui spécifie le routeur lui-même comme étant le nouveau meilleur prochain bond pour la cible IPv6 affectée.

Les routeurs DEVRONT garder trace des entrées d'antémémoire de voisin qui ont été précédemment utilisées pour générer une réponse NHRP. L'expiration d'une telle entrée d'antémémoire de voisin DEVRA résulter en un purge NHRP envoyée au routeur qui a demandé la réponse NHRP à l'origine.

3.3 Détection d'inaccessibilité du voisin

Les sollicitations de voisin envoyées pour les besoins de la détection d'inaccessibilité de voisin (NUD, *Neighbor Unreachability Detection*) sont en envoi individuel au voisin en question, en utilisant le VC qui est déjà ouvert sur ce voisin. Cela suggère que pour autant que NUD est concerné, le voisin transitoire est indistinguable d'un voisin en LL.

3.4 Détection d'adresse dupliquée

La détection d'adresse dupliquée n'est exigée qu'au sein de la portée de liaison locale, qui dans ce cas est la portée de la LL locale. Les voisins transitoires sont en dehors de la portée de la LL. Aucune interaction particulière n'est requise entre le mécanisme d'établissement de raccourcis et le mécanisme de détection d'adresses dupliquées de liaison locales.

4. Concepts du fonctionnement de nœud

Cette section décrit les opérations des nœuds pour effectuer les fonctions de base (telles que l'envoi et la réception des données) sur une liaison logique. L'application de ces fonctions de base aux opérations des divers protocoles IPv6 comme la découverte de voisin est décrite à l'Appendice A.

La majeure partie de cette section ne s'applique qu'aux réseaux NBMA lorsque ils sont utilisés pour fournir des SVC en point à point et point à multipoint. La Section 7 expose le cas où le réseau NBMA est utilisé seulement pour fournir des PVC en point à point.

4.1 Connexion à une liaison logique

Avant qu'un nœud puisse envoyer ou recevoir des datagrammes IPv6, son ou ses interfaces IPv6/NBMA sous-jacentes doivent d'abord joindre une liaison logique.

Un pilote IPv6/NBMA DEVRA établir un VC point à point avec le MARS associé à sa liaison logique, et s'enregistrer comme membre d'une grappe [5]. L'interface IPv6/NBMA du nœud sera alors membre de la LL, aura un identifiant de membre de grappe (CMI, *Cluster Member ID*) alloué, et pourra commencer à prendre en charge IPv6 et des opérations de découverte de voisin IPv6.

Si le nœud est un hôte ou un routeur qui démarre, il DEVRA produire un seul groupe MARS_JOIN pour les groupes suivants :
- Sa ou ses adresses de nœud sollicité déduites avec une portée de liaison locale.
- L'adresse Tous les nœuds avec portée de liaison locale.
- Les autres groupes de diffusion groupée configurés avec au moins une portée de liaison locale.

Si le nœud est un routeur, il DEVRA produire de plus :
- Un seul groupe MARS_JOIN pour l'adresse Tous les routeurs avec une portée de liaison locale.
- Un bloc MARS_JOIN pour la ou les gammes d'adresses de diffusion groupée IPv6 (avec une portée supérieure à la liaison locale) pour lesquelles une réception de proximité est exigée.

Le mécanisme d'encapsulation et les valeurs de champs clés des messages de contrôle de MARS DEVRONT être définis dans les documents d'accompagnement spécifiques des technologies particulières du réseau NBMA.

4.2 Adhésion à un groupe de diffusion groupée

Ce paragraphe décrit le comportement du nœud lorsqu'il reçoit une demande JoinLocalGroup provenant de la couche IPv6. Les détails de la façon dont ce comportement se réalise seront spécifiques de la mise en œuvre.

Si une JoinLocalGroup pour une adresse de nœud local est reçue, le pilote IPv6/NBMA DEVRA retourner une indication de réussite à l'appelant sans autre action. (Les paquets envoyés aux adresses de nœud local n'atteignent jamais le pilote IPv6/NBMA.)

Si une demande JoinLocalGroup est reçue pour une adresse avec une portée supérieure à celle du nœud local, le pilote IPv6/NBMA DEVRA envoyer une demande d'un seul groupe MARS_JOIN approprié pour enregistrer cette adresse auprès du MARS.

4.3 Sortie d'un groupe de diffusion groupée

Ce paragraphe décrit le comportement du nœud lorsque il reçoit une demande LeaveLocalGroup de la couche IPv6. Les détails de la façon dont ce comportement est réalisé relèvent de la mise en œuvre.

Si une demande LeaveLocalGroup pour une adresse de nœud local est reçue, le pilote IPv6/NBMA DEVRA retourner une indication de réussite à l'appelant sans autre action. (Les paquets envoyés aux adresses de nœud local n'atteignent jamais le pilote IPv6/NBMA.)

Si une demande LeaveLocalGroup est reçue pour une adresse qui a une portée supérieure au nœud local, le pilote IPv6/NBMA DEVRA envoyer une demande d'un seul groupe MARS_LEAVE approprié pour désenregistrer cette adresse chez le MARS.

4.4 Envoi des données

Des règles de traitement et d'encapsulation différentes s'appliquent pour les paquets sortants en envoi individuel et en diffusion groupée.

4.4.1 Envoi individuel de données

Le "prochain bond" de niveau IP pour chaque paquet IPv6 sortant en envoi individuel est utilisé pour identifier un VC en point à point destiné à la transmission du paquet.

Pour les réseaux NBMA où l'encapsulation LLC/SNAP est normalement utilisée (par exemple ATM ou SMDS) le paquet IPv6 DEVRA être encapsulé avec l'en-tête LLC/SNAP suivant et envoyé sur le VC.

[0xAA-AA-03]	[0x00-00-00]	[0x86-DD][paquet IPv6]
(LLC)	(OUI)	(PID)

Pour les réseaux NBMA qui n'utilisent pas l'encapsulation LLC/SNAP, une règle de remplacement DEVRA être spécifiée dans le document d'accompagnement spécifique de NBMA.

Si il n'existe pas de VC en point à point pour l'adresse du prochain bond pour le paquet, le nœud DEVRA passer un appel pour établir un VC pour la destination du prochain bond. Chaque fois que le pilote IPv6/NBMA reçoit un paquet en envoi individuel à transmettre, la couche IPv6 aura déjà déterminé l'adresse (NBMA) de couche liaison du prochain bond. Donc, les informations nécessaires pour passer l'appel NBMA au prochain bond seront disponibles.

Le nœud envoyeur DEVRAIT mettre en file d'attente le paquet qui a déclanché la demande d'appel, et l'envoyer lorsque l'appel est établi.

Si l'appel au nœud de destination du prochain bond échoue, le nœud envoyeur DEVRA éliminer le paquet qui a déclanché l'établissement de l'appel. Un échec persistant à créer un VC pour la destination du prochain bond sera détecté et traité à la couche Réseau IPv6 par la NUD.

Pour l'instant, aucune règle n'est spécifiée pour transposer les paquets sortants sur les VC en utilisant quelque chose de plus que l'adresse de destination du paquet.

4.4.2 Envoi de données en diffusion groupée

Le "prochain bond" de niveau IP pour chaque paquet IPv6 sortant en diffusion groupée est utilisé pour identifier un VC en point à point ou en point à multipoint sur lequel transmettre le paquet.

Pour les réseaux NBMA où l'encapsulation LLC/SNAP est normalement utilisée (par exemple. ATM ou SMDS), les paquets en diffusion groupée DEVRONT être encapsulés de la façon suivante :

[0xAA-AA-03][0x00-00-5E][0x00-01][pkt$cmi][0x86DD][paquet IPv6]
(LLC) (OUI) (PID) (encapsulation mars)

L'identifiant de membre de grappe du pilote IPv6/NBMA DEVRA être copié dans le champ pkt$cmi de deux octets avant transmission.

Pour les réseaux NBMA qui n'utilisent pas l'encapsulation LLC/SNAP, une règle de remplacement DEVRA être spécifiée dans le document d'accompagnement spécifique de NBMA. Certains mécanismes pour porter l'identifiant de membre de grappe du pilote IPv6/NBMA DEVRONT être fournis.

Si la destination du paquet est une des adresses de diffusion groupée suivantes, elle DEVRA être envoyée sur le VC point à point direct du pilote IPv6/NBMA au MARS :
- Une adresse de nœud sollicité avec portée de liaison locale.
- L'adresse Tous les nœuds avec portée de liaison locale.
- L'adresse Tous les routeurs avec portée de liaison locale.
- Une adresse de diffusion groupée de relais ou serveur DHCPv6.

Le MARS DEVRA alors redistribuer le paquet IPv6 comme décrit au paragraphe 3.1.1. (Si le VC avec le MARS a subi pour une raison ou une autre une fin de temporisation d'inactivité, il DOIT être rétabli avant la transmission du paquet au MARS.)

Si la destination du paquet est toute autre adresse, les mécanismes usuels de client MARS sont alors utilisés par le pilote IPv6/NBMA pour choisir et/ou établir un VC en point à multipoint sur lequel le paquet sera envoyé.

Pour l'instant aucune règle n'est spécifiée pour la transposition des paquets sortants dans les VC en utilisant quelque chose de plus que l'adresse de destination du paquet.

4.5 Réception de données

Les paquets reçus en utilisant l'encapsulation décrite au paragraphe 4.4.1 DEVRONT être désencapsulés et passés à la couche IPv6. La couche IPv6 détermine comment traiter le paquet entrant.

Les paquets reçus en utilisant l'encapsulation spécifiée au paragraphe 4.4.2 DEVRONT avoir leur champ pkt$cmi comparé au CMI propre du pilote IPv6/NBMA local. Si le pkt$cmi dans l'en-tête correspond au CMI local, le paquet DEVRA être éliminé en silence. Autrement, le paquet DEVRA être désencapsulé et passé à la couche IPv6. La couche IPv6 détermine alors comment traiter le paquet entrant.

Pour les réseaux NBMA qui n'utilisent pas l'encapsulation LLC/SNAP, des règles de remplacement DEVRONT être spécifiées dans les documents d'accompagnement spécifiques de NBMA.

Le pilote IPv6/NBMA NE DEVRA PAS tenter de filtrer les paquets IPv6 en diffusion groupées qui arrivent avec l'encapsulation définie pour les paquets en envoi individuel, ni tenter de filtrer les paquets IPv6 en envoi individuel qui arrivent avec l'encapsulation définie pour les paquets en diffusion groupée.

4.6 Établissement et libération de VC pour données en envoi individuel

Les VC en envoi individuel sont maintenus séparément des VC de diffusion groupée. L'établissement et la maintenance des VC en diffusion groupée sont traités par le client MARS dans chaque pilote IPv6/NBMA [5]. Seuls seront décrits ici l'établissement et la maintenance des VC en point à point pour le trafic IPv6 en envoi individuel. Seuls les VC en envoi

individuel au mieux sont considérés. La création de VC pour d'autres classes de service sort du domaine d'application du présent document.

Avant d'envoyer un paquet à une nouvelle destination au sein de la même LL, un nœud va d'abord effectuer une découverte de voisin sur la cible intra LL. Cela est fait pour résoudre l'adresse IPv6 de destination en adresse de couche liaison que l'envoyeur peut alors utiliser pour envoyer des paquets en envoi individuel.

L'Appendice A.1.1 contient un texte descriptif non normatif qui couvre l'échange sollicitation/annonce de voisin et l'éventuel établissement d'un nouveau SVC.

Un message Redirection (une redirection sur un nœud sur la même LL, ou une redirection de raccourci sur un nœud en dehors de la LL) résulte en ce que le nœud envoyeur (redirigé) crée un nouveau VC point à point avec un nouveau nœud de réception. Le message Redirection DEVRA contenir l'adresse (NBMA) de couche liaison de la nouvelle interface IPv6/NBMA receveuse. Le nœud redirigé ne se préoccupe pas de savoir si le nouveau nœud de réception est localisé sur le réseau NBMA. Le nœud redirigé va établir un VC point à point avec le nouveau nœud s'il n'en existe pas déjà un. Le nœud redirigé va alors utiliser le nouveau VC pour envoyer des données plutôt que tout autre VC qu'il utilisait auparavant.

Les redirections sont unidirectionnelles. Même après que la source a réagi à une redirection, la destination va continuer de renvoyer des paquets IPv6 au nœud redirigé sur le vieux chemin. Cela se produit parce que le nœud de destination n'a aucun moyen pour détermine l'adresse IPv6 de l'autre extrémité d'un nouveau VC en l'absence d'une découverte de voisin. Donc, les redirections ne vont pas résulter en ce que les deux extrémités d'une connexion utilisent le nouveau VC. Les redirections IPv6 ne sont pas destinées à fournir une redirection symétrique. Si le nœud non redirigé reçoit finalement une redirection, il PEUT découvrir le VC existant avec le nœud cible et l'utiliser plutôt que de créer un nouveau VC.

Il est souhaitable que les VC soient libérés lorsque ils ne sont plus nécessaires.

Un pilote IPv6/NBMA DEVRA libérer tout VC qui a été inactif pendant 20 minutes.

Cette limite de temps PEUT être réduite par configuration ou comme spécifié dans le document d'accompagnement pour les réseaux NBMA spécifiques.

Si une entrée d'antémémoire de voisin ou de destination est purgée, tout VC associé à l'entrée purgée DEVRAIT être libéré.

Si l'état d'une entrée dans l'antémémoire de voisin est réglé à PÉRIMÉ, tous les VC associés à cette entrée périmée DEVRAIENT être libérés.

4.7 Prise en charge de la signalisation de SVC NBMA et questions de MTU

Les mécanismes de signalisation de l'établissement et de la suppression des SVC en point à point et en point à multipoint pour les différents réseaux NBMA DEVRONT être spécifiés dans les documents d'accompagnement.

Comme un pilote IPv6/NBMA donné ne saura pas si l'extrémité distante d'un VC est dans la même LL, les pilotes DEVRONT mettre en œuvre des mécanismes spécifiques de NBMA pour négocier des MTU acceptables au niveau du VC. Ces mécanismes DEVRONT être spécifiés dans les documents d'accompagnement.

Cependant, les pilotes IPv6/NBMA peuvent supposer qu'ils vont toujours parler à un autre pilote rattaché au même type de réseau NBMA. (Par exemple, un pilote IPv6/NBMA n'a pas besoin de considérer la possibilité d'établir un VC de raccourci directement avec un pilote IPv6/FR.)

5. Jetons d'interface, options d'adresse de couche liaison, adresses de liaison locales

5.1 Jetons d'interface

Chaque interface IPv6 doit avoir un jeton d'interface à partir duquel former des adresses IPv6 autoconfigurées. Ce jeton d'interface doit être unique au sein d'une liaison logique pour empêcher la création d'adresses dupliquées lorsque la configuration d'adresse sans état est utilisée.

Dans les cas où deux nœuds sur la même LL produisent le même jeton d'interface, une des interfaces DOIT choisir un autre jeton d'hôte. Toutes les mises en œuvre DOIVENT prendre en charge la configuration manuelle des jetons d'interface pour

permettre que les opérateurs changent manuellement un jeton d'interface sur la base de la LL. Les opérateurs peuvent choisir de régler manuellement les jetons d'interface pour des raisons autres que l'élimination des adresses dupliquées.

Tous les jetons d'interface DOIVENT être longs de 64 bits et être formatés comme décrit dans les paragraphes suivants. Les jetons d'hôte seront fondés sur le format d'un identifiant EUI-64 [10]. Se reporter à l'Appendice A de [6] pour avoir une description de la création d'identifiants d'interface IPv6 fondés sur EUI-64.

5.1.1 Liaisons logiques uniques sur une seule interface NBMA

Les interfaces NBMA physiques vont généralement avoir un identifiant local qui peut être utilisé pour générer un jeton univoque d'interface IPv6/NBMA. Le mécanisme exact pour générer des jetons d'interface DEVRA être spécifié dans les documents d'accompagnement spécifiques de chaque réseau NBMA.

5.1.2 Liaisons logiques multiples sur une seule interface NBMA

Les interfaces NBMA physiques PEUVENT être utilisées pour fournir plusieurs interfaces NBMA logiques. Comme chaque interface NBMA logique PEUT prendre en charge une interface IPv6 indépendante, deux scénarios distincts sont possibles :

- Un seul hôte avec des interfaces IPv6/NBMA séparées sur un certain nombre de liaisons logiques indépendantes.

- Un ensemble de deux "hôtes virtuels" (vhost) ou plus partageant un pilote NBMA commun. Chaque vhost est libre d'établir des interfaces IPv6/NBMA associées à des LL différentes ou communes. Cependant, les vhosts sont tenus par la même exigence que les hôtes normaux : deux interfaces dans la même LL ne peuvent pas partager le même jeton d'interface.

Dans le premier scénario, comme chaque interface IPv6/NBMA est associée à une LL différente, chaque identité externe d'interface peut être différenciée par le préfixe d'acheminement de la LL. Donc, l'hôte peut réutiliser un seul jeton d'interface unique à travers toutes ses interfaces IPv6/NBMA. (En interne, l'hôte va étiqueter les paquets reçus d'une façon localement spécifique pour identifier sur quelle interface IPv6/NBMA ils sont arrivés. Cependant, c'est un problème générique d'IPv6, qui n'exige pas d'éclaircissements dans le présent document.)

Le second scénario est plus complexe, mais sera vraisemblablement plus rare.

Lorsque elles prennent en charge plusieurs interfaces logiques NBMA sur une seule interface NBMA physique, des identifiants indépendants et univoques DEVRONT être générés pour chaque interface NBMA virtuelle pour permettre la construction de jetons d'interface IPv6/NBMA univoques. Le mécanisme exact pour générer les jetons d'interface DEVRA être spécifié dans les documents d'accompagnement spécifique de chaque réseau NBMA.

5.2 Options d'adresse de couche liaison

La découverte de voisin définit deux champs d'option pour porter les adresses de source et de cible spécifiques de couche liaison.

Entre les interfaces IPv6/NBMA, le format de ces deux options est adapté des spécifications de MARS [5] et de NHRP [8]. Il DEVRA être :

[Type]	[NTL][STL][..Numéro NBMA..][..Sous-adresse
[Longueur]	NBMA..]
Fixe	Adresse de couche liaison

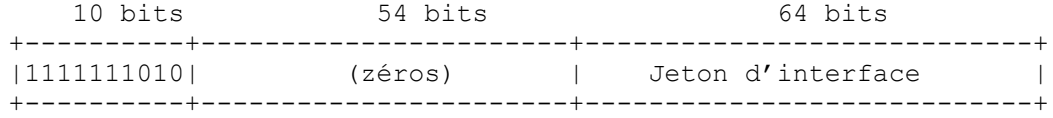
[Type] est un champ d'un octet, 1 pour l'adresse de source de couche liaison ; 2 pour l'adresse cible de couche liaison.
[Longueur] est un champ de un octet. C'est la longueur totale de l'option en multiples de 8 octets. Des octets tout à zéro sont ajoutés à la fin de l'option pour faire coïncider sa longueur avec un multiple de 8 octets.
[NTL] est un champ de un octet "'Type & Longueur de numéro".
[STL] est un champ d'un octet "Type & Longueur de sous-adresse".
[Numéro NBMA] est un champ de longueur variable. Il est toujours présent. Il contient l'adresse NBMA principale.
[Sous-adresse NBMA] est un champ de longueur variable. Il peut être présent ou non. Il contient toute sous-adresse NBMA qui pourrait être nécessaire.

Si la [Sous-adresse NBMA] n'est pas présente, l'option se termine après le champ [Numéro NBMA] (et tout bourrage supplémentaire pour le verrouillage sur 8 octets).

Le contenu et l'interprétation des champs [NTL], [STL], [Numéro NBMA], et [Sous-adresse NBMA] sont spécifiques de chaque réseau NBMA, et DEVRONT être spécifiés dans les documents d'accompagnement.

5.3 Adresses de liaison locales

L'adresse IPv6 de liaison locale est formée par l'ajout du jeton d'interface, comme défini ci-dessus, au préfixe FE80::/64.



6. Conclusion et questions ouvertes

Le présent document décrit une architecture générale pour IPv6 sur les réseaux NBMA. Il forme la base pour des documents d'accompagnement auxiliaires qui fournissent les détails des diverses technologies spécifiques de NBMA (telles que l'ATM ou le relais de trame). L'architecture IPv6 sur NBMA permet le fonctionnement conventionnel côté hôte du protocole de découverte de voisin IPv6, tout en prenant aussi en charge l'établissement de chemins "raccourcis" de transmission NBMA (lorsque des liaisons NBMA à signalisation dynamique sont disponibles).

La "Liaison" IPv6 est généralisée en "Liaison logique" de façon analogue au "sous-réseau logique IP" de IPv4. Le protocole MARS est augmenté et utilisé pour fournir une diffusion groupée relativement efficace intra liaison logique de paquets IPv6, et la distribution de messages de découverte. Les chemins raccourcis de niveau NBMA sont pris en charge par la détection de flux fondée sur le routeur, ou par des demandes explicites générées par l'hôte. La découverte de voisin est utilisée sans modification pour tout le contrôle intra-LL (y compris l'initialisation de la découverte de raccourci NBMA). NHRP de routeur à routeur est utilisé pour obtenir les transpositions d'adresse IPv6/NBMA pour les raccourcis de cibles en dehors de la liaison logique d'une source.

7. Considérations pour la sécurité

La présente architecture n'introduit pas de nouveaux protocoles, mais dépend des protocoles existants (NHRP, IPv6, ND, MARS) et est donc soumise à toutes les menaces contre la sécurité inhérentes à ces protocoles. Cette architecture ne devrait pas être utilisée dans un domaine où un des protocoles de base est considéré comme d'une insécurité inacceptable. Cependant, ce protocole n'introduit par lui-même aucune menace supplémentaire pour la sécurité.

Bien que cette proposition n'introduise aucun nouveau mécanisme de sécurité, tous les mécanismes IPv6 actuels de sécurité fonctionneront sans modification pour NBMA. Cela inclut à la fois l'authentification et le chiffrement pour les deux protocoles de découverte de voisin et l'échange de paquets de données IPv6. Le protocole MARS est modifié d'une manière qui n'affecte pas ni n'augmente la sécurité offerte par la RFC2022.

Remerciements

Eric Nordmark a confirmé l'utilité du message Redirection ND dans un message électronique privé en mars 1996 à l'IETF. Les discussions avec divers membres du groupe de travail ION en juin et décembre 1996 à l'IETF ont aidé à consolider l'architecture décrite ici. Le travail original de Grenville Armitage sur IPv6/NBMA a été fait lorsque il était employé par Bellcore. Des éléments de la section 5 ont été empruntés au mémoire de Matt Crawford sur IPv6 sur Ethernet.

Adresse des auteurs

Grenville Armitage	Peter Schulter
Bell Laboratories, Lucent Technologies	Bright Tiger Technologies
101 Crawfords Corner Road	125 Nagog Park
Holmdel, NJ 07733	Acton, MA 01720

USA	mél : paschulter@acm.org
mél : gja@lucent.com	

Markus Jork
European Applied Research Center
Digital Equipment GmbH
CEC Karlsruhe
Vincenz-Priessnitz-Str. 1
D-76131 Karlsruhe
mél : jork@kar.dec.com

Geraldine Harter
Digital UNIX Networking
Compaq Computer Corporation
110 Spit Brook Road
Nashua, NH 03062
mél : harter@zk3.dec.com

Références

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

[2] ATM Forum, "ATM User Network Interface (UNI) Specification Version 3.1", ISBN 0-13-393828-X, Prentice Hall, Englewood Cliffs, NJ, juin 1995.

[3] M. Crawford, "Méthode de transmission de paquets IPv6 sur réseaux Ethernet", RFC1972, août 1996. (*Obsolète, voir* RFC2464) *(P.S.)*

[4] Juha Heinanen, "Encapsulation multiprotocole sur couche 5 d'adaptation ATM", RFC1483, juillet 1993. *(Obsolète, voir* RFC2684*)*

[5] G. Armitage, "Prise en charge de la diffusion groupée sur réseaux ATM fondés sur UNI 3.0/3.1", RFC2022, novembre 1996. *(P.S.)*

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

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

[8] J. Luciani et autres, "Protocole de résolution du prochain bond NBMA (NHRP)", RFC2332, avril 1998. *(P.S.)*

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

[10] "64-Bit Global Identifier Format Tutorial", http://standards.ieee.org/db/oui/tutorials/EUI64.html.

[11] Y. Katsube, K. Nagami, H. Esaki, "Extensions d'architecture de routeur de Toshiba pour ATM : Généralités", RFC2098, février 1997. *(Information)*

[12] P. Newman, T. Lyon, G. Minshall, "Flow Labeled IP: ATM under IP", Proceedings of INFOCOM'96, San Francisco, mars 1996, pp.1251-1260

[13] D. Piscitello et J. Lawrence, "Transmission de datagrammes IP sur le service SMDS", RFC1209, STD 52, mars 1991.

[14] 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", RFC0826, STD 37, novembre 1982.

[15] J. McCann, S. Deering, J. Mogul, "Découverte de la MTU de chemin pour IP version 6", RFC1981, août 1996. *(D.S.)*

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

[17] G. Armitage, P. Schulter, M. Jork, "IPv6 sur réseaux ATM", RFC2492, janvier 1999. *(P.S.)*

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

Appendice A. Description du fonctionnement du protocole IPv6

Le modèle de IPv6 sur NBMA décrit dans le présent document conserve la sémantique complète des protocoles IPv6. Aucun changement n'est nécessaire à la couche réseau IPv6. Comme le concept d'association de sécurité n'est pas changé pour NBMA, ce cadre conserve la sémantique et les caractéristiques complètes de la sécurité de IPv6. Cela permet aux nœuds IPv6 de choisir leur réponse aux sollicitations sur la base des informations de sécurité comme cela est fait avec les autres liaisons de données, conservant ainsi la sémantique de la découverte de voisin car c'est toujours le nœud sollicité qui choisit de répondre et que répondre à la sollicitation. Donc, NBMA sera transparent à la couche réseau, sauf dans les cas où des services supplémentaires (comme la QS des VC) sont offerts.

La suite de cet Appendice décrit comment les protocoles IPv6 de base fonctionnent au sein du modèle décrit.

A.1 Opérations de la découverte de voisin

Avant d'effectuer aucune opération de découverte de voisin, chaque nœud doit d'abord se joindre au groupe de diffusion groupée Tous-les-nœuds, et à son adresse de diffusion groupée de nœud sollicité (l'utilisation de cette adresse en relation avec la détection d'adresse dupliquée (DAD, *détection d'adresse dupliquée*) est décrite en A.1.4). La description de la façon dont la couche réseau IPv6 va rejoindre ces groupes de diffusion groupée est faite en 4.2.

A.1.1 Effectuer la résolution d'adresse

Un hôte IPv6 effectue la résolution d'adresse en envoyant une Sollicitation de voisin à l'adresse de diffusion groupée de nœud sollicité de l'hôte cible, comme décrit dans [7]. Le message Sollicitation de voisin va contenir une option Adresse de source de couche liaison réglée à l'adresse NBMA sur la LL du nœud solliciteur.

Lorsque le pilote IPv6/NBMA du nœud local reçoit le message Sollicitation de voisin de la couche réseau IPv6, il suit les étapes décrites au paragraphe 4.4.2 "Envoi des données en diffusion groupée".

Un ou plusieurs nœuds vont recevoir le message Sollicitation de voisin. Les nœuds vont traiter les données comme décrit au paragraphe 4.5 et passer les paquets désencapsulés à la couche réseau IPv6.

Si le nœud receveur est la cible de la sollicitation de voisin, il va mettre à jour l'antémémoire de voisin avec l'adresse NBMA du nœud solliciteur, contenue dans l'option Adresse de source de couche liaison du message Sollicitation de voisin, comme décrit dans [7].

L'hôte IPv6 sollicité va répondre à la sollicitation de voisin par un message Annonce de voisin envoyé à l'adresse de diffusion groupée IPv6 du nœud solliciteur. Le message d'annonce de voisin va contenir une option Adresse cible de couche liaison réglée à l'adresse NBMA sur la liaison logique du nœud sollicité.

Le pilote IPv6/NBMA du nœud sollicité va recevoir l'annonce de routeur et l'adresse de couche liaison du nœud solliciteur de la couche réseau IPv6. Il va ensuite suivre les étapes décrites au paragraphe 4.4.1 pour envoyer le message NA au nœud solliciteur. Cela va créer un VC point à point entre le nœud sollicité et le nœud solliciteur si il n'en existait déjà un.

Le nœud solliciteur va alors recevoir le message Annonce de voisin sur le nouveau VC point à point, désencapsuler le message, et le passer à la couche réseau IPv6 pour traitement comme décrit au paragraphe 4.5. Le nœud solliciteur va alors créer les entrées appropriées dans son antémémoire de voisins, en incluant la mise en antémémoire de l'adresse NBMA de couche liaison du nœud sollicité comme décrit dans [7].

À ce point, chaque système a une entrée d'antémémoire de voisin complète pour l'autre système. Ils peuvent échanger des données sur le VC point à point nouvellement créé par le nœud sollicité lorsque il a retourné l'annonce de voisin, ou créé un nouveau VC.

Un hôte IPv6 peut aussi envoyer une annonce de voisin non sollicitée à l'adresse de diffusion groupée Tous-les-nœuds. Lorsque le pilote IPv6/NBMA de nœud local reçoit l'annonce de voisin de la couche réseau IPv6, il suit les étapes décrites au paragraphe 4.4.2 pour envoyer le message Annonce de voisin à l'adresse de diffusion groupée Tous-les-nœuds. Chaque nœud va traiter le paquet entrant comme décrit au paragraphe 4.5, puis passer le paquet à la couche réseau IPv6 où il sera traité comme décrit dans [7].

A.1.2 Effectuer la découverte de routeur

La découverte de routeur (RD) est décrite dans [7]. Pour prendre en charge la découverte de routeur, un routeur IPv6 va joindre l'adresse de groupe de diffusion groupée Tous-routeurs IPv6. Lorsque le pilote IPv6/NBMA obtient la demande JoinLocalGroup de la couche réseau IPv6, il suit le processus décrit au paragraphe 4.2.

Les routeurs IPv6 envoient périodiquement des annonces de routeur *(RA, Router Advertisment)* non sollicitées qui annoncent leur disponibilité sur la couche liaison. Lorsque un routeur IPv6 envoie une annonce de routeur non sollicitée , il envoie un paquet de données adressé à l'adresse de diffusion groupée Tous-nœuds IPv6. Lorsque le pilote IPv6/NBMA du nœud local obtient le message d'annonce de routeur de la couche réseau IPv6, il transmet le message en suivant les étapes décrites au paragraphe 4.4.2. Le MARS va transmettre le paquet sur le ClusterControlVC de la couche liaison, qui envoie les paquets à tous les nœuds sur la LL. Chaque nœud de la LL va alors traiter le paquet entrant comme décrit au paragraphe 4.5 et passer le paquet reçu à la couche réseau IPv6 pour subir le traitement approprié.

Pour effectuer la découverte de routeur, un hôte IPv6 envoie un message de sollicitation de routeur *(RS)* à l'adresse de diffusion groupée Tous-routeurs. Lorsque le pilote IPv6/NBMA du nœud local reçoit la demande de la couche réseau IPv6 pour l'envoi du paquet, il agit conformément aux étapes décrites au paragraphe 4.4.2. Le message RS va être envoyé aux nœuds qui ont rejoint le groupe de diffusion groupée Tous-routeurs ou à tous les nœuds. Les nœuds qui reçoivent le message RA vont le traiter comme décrit au paragraphe 4.5 et le passer à la couche IPv6 pour traitement. Seuls les nœuds qui sont des routeurs vont traiter le message et y répondre.

Un routeur IPv6 répond à une sollicitation de routeur en envoyant une annonce de routeur adressée à l'adresse de diffusion groupée Tous-nœuds IPv6 si l'adresse de source de la sollicitation de routeur était l'adresse inspécifiée. Si l'adresse de source dans la sollicitation de routeur n'est pas l'adresse inspécifiée, le routeur va envoyer l'annonce de routeur en envoi individuel au nœud solliciteur. Si le routeur envoie l'annonce de routeur à l'adresse de diffusion groupée Tous-les-nœuds, il va suivre alors les étapes décrites ci-dessus pour les annonces de routeur non sollicitées.

Si l'annonce de routeur est en envoi individuel au nœud solliciteur, la couche réseau IPv6 va donner au pilote IPv6/NBMA du nœud l'annonce de routeur et l'adresse de couche liaison du nœud solliciteur (obtenues par la résolution d'adresse si nécessaire) et il va envoyer le paquet conformément aux étapes décrites au paragraphe 4.4.1. Il va en résulter la création d'un nouveau circuit virtuel point à point entre le routeur et le nœud solliciteur s'il n'en existait déjà un.

Le nœud solliciteur va recevoir et traiter l'annonce de routeur comme décrit au paragraphe 4.5 et va passer le message RA à la couche réseau IPv6. La couche réseau IPv6 peut, selon l'état de l'entrée d'antémémoire de voisin, mettre à jour l'antémémoire de voisin avec l'adresse NBMA du routeur, qui est contenue dans l'option Adresse de source de couche liaison du message Annonce de routeur.

Si un circuit virtuel point à point est établi durant la découverte de routeur, les données IPv6 au mieux en envoi individuel suivantes entre le nœud solliciteur et le routeur seront transmises sur le nouveau circuit virtuel en point à point.

A.1.3 Effectuer la détection d'inaccessibilité de voisin

La détection d'inaccessibilité du voisin (NUD, *Neighbor Unreachability Detection*) est le processus par lequel un hôte IPv6 détermine qu'un voisin n'est plus accessible, comme décrit dans [7]. Chaque entrée d'antémémoire de voisin contient des informations utilisées par l'algorithme de NUD pour détecter des défaillances d'accessibilité. La confirmation de l'accessibilité d'un voisin vient soit d'indications d'un protocole de couche supérieure que des données envoyées récemment au voisin ont été reçues, soit de la réception d'un message Annonce de voisin en réponse à une sonde de sollicitation de voisin.

Les défaillance de connexité au pilote IPv6/NBMA du nœud, telles que des libérations de circuits virtuels (voir au paragraphe 4.6) et l'incapacité à créer un circuit virtuel avec un voisin (voir au paragraphe 4.4.1) sont détectées et traitées à la couche réseau IPv6, par la détection d'inaccessibilité du voisin. Le pilote IPv6/NBMA du nœud n'essaye pas de détecter ces conditions ou de s'en relever.

Une défaillance persistante à créer un circuit virtuel de la part de l'hôte IPv6 avec un de ses voisins IPv6 sera détectée et traitée avec la NUD. À chaque tentative d'envoi de données à son voisin de la part d'un hôte IPv6, le pilote IPv6/NBMA du nœud va tenter d'établir un circuit virtuel avec le voisin, et échouant à le faire, il va abandonner le paquet. Les temporisateurs de confirmation d'accessibilité IPv6 vont finalement arriver à expiration, et l'entrée d'antémémoire de voisins du voisin va entrer dans l'état SONDE. L'état SONDE va causer l'envoi par l'hôte IPv6 de sollicitations de voisin en envoi individuel au voisin, qui seront abandonnées par le pilote IPv6/NBMA du nœud local après avoir encore échoué à établir le circuit virtuel. L'hôte IPv6 ne va donc jamais recevoir les annonces de voisin sollicitées nécessaires pour la confirmation d'accessibilité, causant la suppression de l'entrée de voisin de l'antémémoire de voisins. La prochaine fois que l'hôte IPv6 essayera d'envoyer des données à ce voisin, la résolution d'adresse sera effectuée. Selon la raison de la défaillance précédente, la connexité avec le voisin pourrait être rétablie (par exemple, si le précédent échec d'établissement d'un circuit virtuel était causé par une adresse de couche liaison obsolète dans l'antémémoire de voisin).

Dans le cas où un circuit virtuel avec un voisin IPv6 a été libéré, la prochaine fois qu'un paquet est envoyé de l'hôte IPv6 au voisin, le pilote IPv6/NBMA du nœud va reconnaître qu'il n'a plus de VC avec ce voisin et tenter d'établir un nouveau VC avec le voisin. Si, lors de la première transmission et des suivantes, le nœud est incapable de créer un VC avec le voisin, la NUD va détecter la défaillance et la traiter comme décrit plus haut (le traitement d'une défaillance persistante à créer un VC de l'hôte IPv6 à un de ses voisins IPv6). Selon la raison de la défaillance précédente, la connexité avec le voisin peut ou non être restaurée.

A.1.4 Effectuer la détection d'adresse dupliquée

Un hôte IPv6 effectue la détection d'adresse dupliquée (DAD, *détection d'adresse dupliquée*) pour déterminer que l'adresse qu'il souhaite utiliser sur la liaison logique (c'est-à-dire, une tentative d'adresse) n'est pas déjà utilisée, comme décrit dans [9] et [7]. La détection d'adresse dupliquée est effectuée sur toutes les adresses que l'hôte souhaite utiliser, sans considération du mécanisme de configuration utilisé pour obtenir l'adresse.

Avant d'effectuer la détection d'adresse dupliquée, un hôte va joindre l'adresse de diffusion groupée Tous-les-nœuds et l'adresse de diffusion groupée d'hôte sollicité correspondant à la tentative d'adresse de l'hôte (voir au paragraphe 4.2. "Joindre un groupe de diffusion groupée"). L'hôte IPv6 initie la détection d'adresse dupliquée par l'envoi d'une sollicitation de voisin à l'adresse de diffusion groupée d'hôte sollicité correspondant à la tentative d'adresse de l'hôte, avec la tentative d'adresse comme cible. Lorsque le pilote IPv6/NBMA du nœud local obtient le message Sollicitation de voisin de la couche réseau IPv6, il suit les étapes précisées au paragraphe 4.4.2. Le message NS sera envoyé aux nœuds qui se sont joints au groupe de diffusion groupée de nœud sollicité cible ou à Tous-les-nœuds. Le message NS de DAD sera reçu par un ou plusieurs nœuds sur la LL et traité par chacun comme décrit au paragraphe 4.5. Noter que le client MARS du nœud d'envoi va filtrer le message de sorte que la couche réseau IPv6 du nœud d'envoi ne verra pas le message. La couche réseau IPv6 de tout nœud qui n'est pas membre du groupe de diffusion groupée du nœud sollicité cible va supprimer le message Sollicitation de voisin.

Si aucun autre hôte n'a joint l'adresse de diffusion groupée d'hôte sollicité correspondant à la tentative d'adresse, l'hôte ne va alors pas recevoir l'annonce de voisin qui contient la tentative d'adresse comme cible. L'hôte va effectuer la logique de retransmission décrite dans [9], terminer la détection d'adresse dupliquée, et allouer la tentative d'adresse à l'interface NBMA.

Autrement, les autres hôtes de la LL qui se sont joints à l'adresse de diffusion groupée d'hôte sollicité correspondant à la tentative d'adresse vont traiter la sollicitation de voisin. Le traitement va dépendre de ce que l'hôte IPv6 receveur considère l'adresse cible comme une tentative.

Si l'adresse de l'hôte IPv6 receveur n'est pas une tentative, l'hôte va répondre avec une annonce de voisin contenant l'adresse cible. Comme la source de la sollicitation de voisin est l'adresse inspécifiée, l'hôte envoie l'annonce de voisin à l'adresse de diffusion groupée Tous-les-nœuds en suivant les étapes précisées au paragraphe 4.4.2. Le message Annonce de voisin de DAD sera reçu et traité par les clients MARS sur tous les nœuds dans la LL comme décrit au paragraphe 4.5. Noter que le nœud envoyeur va filtrer le message entrant car le CMI dans l'en-tête de message va correspondre à celui du nœud receveur. Tous les autres nœuds vont désencapsuler le message et le passer à la couche réseau IPv6. L'hôte qui effectue la DAD va détecter que sa tentative d'adresse est la cible de l'annonce de voisin, et déterminer que la tentative d'adresse n'est pas unique et ne peut pas être allouée à son interface NBMA.

Si l'adresse de l'hôte IPv6 receveur est une tentative, les deux hôtes effectuent alors la DAD en utilisant la même tentative d'adresse. L'hôte receveur va déterminer que la tentative d'adresse n'est pas unique et ne peut pas être allouée à son interface NBMA.

A.1.5 Traitement des redirections

Un routeur IPv6 utilise un message Redirection pour informer un hôte IPv6 d'un meilleur premier bond pour atteindre une destination particulière, comme décrit dans [7]. Cela peut être utilisé pour diriger les hôtes sur un meilleur routeur de premier bond, sur un autre hôte sur la même LL, ou sur un voisin transitoire sur une autre LL. Le routeur IPv6 va envoyer individuellement la redirection à l'adresse IPv6 de source qui a déclanché la redirection. Le pilote IPv6/NBMA du routeur va transmettre le message Redirection en utilisant la procédure décrite au paragraphe 4.4.1. Cela va créer un circuit virtuel entre le routeur et l'hôte redirigé si il n'en existait pas déjà un.

Le pilote IPv6/NBMA de l'hôte IPv6 qui a déclanché la redirection va recevoir la redirection encapsulée sur un de ses circuits virtuels point à point. Il va désencapsuler le paquet, et passer le message Redirection à la couche réseau IPv6, comme décrit au paragraphe 4.5.

Les données envoyées ensuite de l'hôte IPv6 à la destination le seront à l'adresse de prochain bond spécifiée dans le message Redirection. Pour les réseaux NBMA, le message Redirection devrait contenir l'option d'adresse de couche liaison, comme décrit dans [7] et au paragraphe 5.2, et donc, le nœud redirigé n'aura pas à effectuer une sollicitation de voisin pour apprendre l'adresse de couche liaison du nœud sur lequel il a été redirigé. Donc, la redirection peut être sur tout nœud du réseau NBMA, sans considération de l'adhésion à la LL du nouveau nœud cible. Cela permet aux hôtes NBMA d'être redirigés hors de leur LL pour réaliser des raccourcis en utilisant les protocoles IPv6 standard.

Une fois redirigé, la couche réseau IPv6 va donner au pilote IPv6/NBMA du nœud le paquet IPv6 et l'adresse de couche liaison du nœud de prochain bond lorsque il envoie les données à la destination redirigée. Le pilote IPv6/NBMA du nœud va déterminer si il existe un circuit virtuel pour la destination du prochain bond. Si il n'existe pas de circuit virtuel point à point, le pilote IPv6/NBMA va mettre en file d'attente le paquet de données et initier un établissement de circuit virtuel pour la destination. Lorsque le VC est créé, ou si il en existe déjà un, le nœud va alors encapsuler le paquet de données sortant et l'envoyer sur le VC.

Noter que les redirections sont unidirectionnelles. L'hôte redirigé va créer un VC pour la destination de prochain bond, comme spécifié dans le message Redirection, mais le prochain bond ne sera pas redirigé sur l'hôte de source. Comme aucune découverte de voisin n'a lieu, la destination du prochain bond n'a aucun moyen de déterminer l'identité de l'appelant lorsque il reçoit le nouveau VC. Aussi, comme la ND n'a pas lieu sur les redirections, le prochain bond ne reçoit aucun événement qui provoquerait la mise à jour de son antémémoire de voisins ou de destinations. Cependant, il va continuer de retransmettre les données à l'hôte redirigé sur l'ancien chemin pour l'hôte redirigé. Le nœud de prochain bond devrait être capable d'utiliser le nouveau VC à partir de la destination redirigée si il reçoit lui aussi une Redirection qui le redirige sur le nœud redirigé. Ce comportement est cohérent avec [7].

A.2 Configuration d'adresse

Les adresses IPv6 sont autoconfigurées en utilisant les mécanismes d'autoconfiguration d'adresse sans état ou à états pleins, comme décrit dans [9] et [18]. Le processus IPv6 d'autoconfiguration implique la création et la vérification de l'unicité d'une adresse de liaison locale sur une LL, de déterminer s'il faut utiliser les mécanismes de configuration sans état et/ou à états pleins pour obtenir les adresses, et de déterminer si d'autres informations (qui ne sont pas d'adresse) sont à autoconfigurer. Les adresses IPv6 peuvent aussi être configurées manuellement, si par exemple, l'autoconfiguration échoue parce que l'adresse autoconfigurée de liaison locale n'est pas unique. Un administrateur de couche liaison spécifie le type d'autoconfiguration à utiliser ; les hôtes sur une LL reçoivent ces informations d'autoconfiguration par des messages d'annonce de routeur.

Les paragraphes suivants décrivent comment fonctionne la configuration d'adresse sans état, à états pleins, et manuelle dans un environnement IPv6/NBMA.

A.2.1 Configuration d'adresse sans état

La configuration d'adresse IPv6 sans état est le processus par lequel un hôte IPv6 autoconfigure ses interfaces, comme décrit dans [18].

Lorsque un hôte IPv6 démarre pour la première fois, il génère une adresse de liaison locale pour l'interface rattachée à la liaison logique. Il vérifie ensuite l'unicité de l'adresse de liaison locale en utilisant la détection d'adresse dupliquée (DAD). Si l'hôte IPv6 détecte que l'adresse de liaison locale n'est pas unique, le processus d'autoconfiguration se termine. L'hôte IPv6 doit alors être configuré manuellement.

Après que l'hôte IPv6 a déterminé que l'adresse de liaison locale est unique et qu'il l'a allouée à l'interface sur la liaison logique, l'hôte IPv6 va effectuer la découverte de routeur pour obtenir les informations d'autoconfiguration. L'hôte IPv6 va envoyer une sollicitation de routeur et va recevoir une annonce de routeur, ou il va attendre une annonce de routeur non sollicitée. L'hôte IPv6 va traiter les bits M et O de l'annonce de routeur, comme décrit dans [9] et peut ensuite invoquer l'autoconfiguration d'adresse à états pleins.

Si il n'y a pas de routeur sur la liaison logique, l'hôte IPv6 sera capable de communiquer avec les autres hôtes IPv6 sur la liaison logique en utilisant les adresses de liaison locales. L'hôte IPv6 va obtenir l'adresse de couche liaison d'un voisin en utilisant la résolution d'adresse. L'hôte IPv6 va aussi tenter d'invoquer l'autoconfiguration à états pleins, sauf si il a été explicitement configuré pour ne pas le faire.

A.2.2 Configuration (DHCP) d'adresse à états pleins

Les hôtes IPv6 utilisent le protocole de configuration dynamique d'hôte (DHCPv6) pour effectuer l'autoconfiguration d'adresses à états pleins, comme décrit dans [18].

Un serveur DHCPv6 ou un agent de relais est présent sur une liaison logique qui a été configurée avec l'autoconfiguration manuelle ou à états pleins. Le serveur DHCPv6 ou l'agent de relais va se joindre au groupe de diffusion groupée IPv6 DHCPv6 des serveur/agents de relais sur la liaison logique. Lorsque le pilote IPv6/NBMA du nœud obtient la demande JoinLocalGroup de la couche réseau IPv6, il suit le processus décrit au paragraphe 4.2.

Un hôte IPv6 va invoquer l'autoconfiguration à états pleins si les bits M et O de l'annonce de routeur indiquent qu'il devrait le faire, et peut invoquer l'autoconfiguration à états pleins si il détecte qu'aucun routeur n'est présent sur la liaison logique. Un hôte IPv6 qui obtient les informations de configuration par le mécanisme à états pleins est appelé ici un client DHCPv6.

Un client DHCPv6 va envoyer un message DHCPv6 Sollicitation à l'adresse de diffusion groupée Serveurs/Agents de relais DHCPv6 pour localiser un agent DHCPv6. Lorsque le pilote IPv6/NBMA du nœud solliciteur obtient la demande de la couche réseau IPv6 pour envoyer le paquet, il se comporte conformément aux étapes décrites au paragraphe 4.4.2. Il va en résulter qu'un ou plusieurs nœuds sur la LL vont recevoir le message. Chaque nœud qui reçoit le paquet de sollicitation le traite comme décrit au paragraphe 4.5. Seule la couche réseau IPv6 du serveur/agent de relais DHCPv6 va accepter le paquet et le traiter.

Un serveur ou agent de relais DHCPv6 sur la liaison logique va envoyer individuellement une annonce DHCPv6 au client DHCPv6. La couche réseau IPv6 va donner au pilote IPv6/NBMA du nœud le paquet et l'adresse de couche liaison du client DHCPv6 (obtenue si nécessaire par la découverte de voisin). Le pilote IPv6/NBMA du nœud va alors transmettre le paquet comme décrit au paragraphe 4.4.1. Il va en résulter la création d'un nouveau circuit virtuel point à point entre le serveur et le client si il n'en existait pas déjà un.

Le pilote IPv6/NBMA du client DHCP va recevoir le paquet encapsulé du serveur ou agent de relais DHCP, comme décrit au paragraphe 4.5. Le nœud va désencapsuler le paquet de diffusion groupée et le passer ensuite à la couche réseau IPv6 pour traitement. La couche réseau IPv6 va livrer le message DHCPv6 Annonce au client DHCPv6.

Les autres messages DHCPv6 (Demande, Réponse, Libération et Reconfiguration) sont en envoi individuel entre le client DHCPv6 et le serveur DHCPv6. Selon l'accessibilité de l'adresse du client DHCPv6, les messages échangés entre un client DHCPv6 et un serveur DHCPv6 sur une autre LL sont envoyés via un routeur ou agent de relais DHCPv6. Avant d'envoyer le message DHCPv6, la couche réseau IPv6 va effectuer une découverte de voisin (si nécessaire) pour obtenir l'adresse de couche liaison correspondant au prochain bond du paquet. Un circuit virtuel point à point sera établi entre l'envoyeur et le prochain bond, et le paquet encapsulé sera transmis sur lui, comme décrit en 4.4 "Envoi des données".

A.2.3 Configuration manuelle d'adresse

Un hôte IPv6 sera configuré manuellement si il découvre par la DAD que son adresse de liaison locale n'est pas unique. Une fois que l'hôte IPv6 est configuré avec un jeton d'interface unique, le mécanisme d'autoconfiguration peut alors être invoqué.

A.3 Protocole de gestion de groupe Internet (IGMP)

Les routeurs de diffusion groupée IPv6 vont utiliser le protocole IGMPv6 pour déterminer périodiquement les membres d'un groupe d'hôtes locaux. Dans le cadre décrit ici, les protocoles IGMPv6 peuvent être utilisés sans aucune modification particulière pour NBMA. Bien que ces protocoles puissent n'être pas les plus efficaces dans cet environnement, il vont quand même fonctionner comme décrit ci-dessous. Cependant, les routeurs de diffusion groupée IPv6 connectés à une liaison logique NBMA pourraient facultativement optimiser les fonctions IGMP par l'envoi de messages MARS_GROUPLIST_REQUEST au MARS qui dessert la LL et en déterminant les membres du groupe avec les messages MARS_GROUPLIST_REPLY. Interroger le MARS sur les membres d'un groupe de diffusion groupée est une amélioration facultative et n'est pas exigé des routeurs pour déterminer les membres d'un groupe de diffusion groupée IPv6 sur une LL.

Il y a trois types de message ICMPv6 qui portent des informations sur les membres d'un groupe de diffusion groupée : les messages Interrogation d'appartenance de groupe, Rapport d'appartenance de groupe et Réduction d'appartenance de groupe. IGMPv6 va continuer de fonctionner non modifié sur l'architecture IPv6/NBMA décrite dans ce document.

Un routeur de diffusion groupée IPv6 reçoit tous les paquets IPv6 en diffusion groupée sur la LL en se joignant à tous les groupes de diffusion groupée en mode disparate *(promiscuous)* [5]. Le serveur MARS va alors provoquer l'ajout du routeur de diffusion groupée à tous les VC de diffusion groupée existants et futurs. Le routeur de diffusion groupée IPv6 va à partir de là être en réception de tous les paquets IPv6 en diffusion groupée envoyés au sein de la liaison logique.

Un routeur IPv6 de diffusion groupée découvre quels groupes de diffusion groupée ont des membres dans la liaison logique en envoyant périodiquement des messages Interrogation d'appartenance de groupe à l'adresse de diffusion groupée Tous-nœuds-IPv6. Lorsque le pilote IPv6/NBMA du nœud local obtient la demande de la couche réseau IPv6 d'envoi du paquet Interrogation d'appartenance de groupe, il suit les étapes décrites au paragraphe 4.4.2. Le nœud détermine si l'adresse de destination du paquet est l'adresse de diffusion groupée Tous-les-nœuds et passe le paquet au client MARS du nœud où le paquet est encapsulé et directement transmis au MARS. Le MARS relaie alors le paquet à tous les nœuds dans la LL. Chaque pilote IPv6/NBMA du nœud va recevoir le paquet, le désencapsuler, et le passer à la couche réseau IPv6. Si le nœud d'origine reçoit le paquet encapsulé, celui-ci va être filtré par le client MARS car l'identifiant de membre de grappe du nœud receveur va correspondre au CMI dans l'en-tête d'encapsulation MARS du paquet.

Les hôtes IPv6 dans la liaison logique vont répondre à l'interrogation d'appartenance de groupe par un rapport d'appartenance de groupe pour chaque groupe de diffusion groupée IPv6 rejoint par l'hôte. Les hôtes IPv6 peuvent aussi transmettre un rapport d'appartenance de groupe lorsque l'hôte rejoint un nouveau groupe de diffusion groupée IPv6. Le rapport d'appartenance de groupe est envoyé au groupe de diffusion groupée dont l'adresse est rapportée. Lorsque le pilote IPv6/NBMA du nœud local obtient la demande d'envoi du paquet de la couche réseau IPv6, il suit les étapes décrites au paragraphe 4.4.2. Le nœud détermine si le paquet est envoyé à une adresse en diffusion groupée afin de le transmettre au client MARS du nœud pour envoi sur le VC approprié.

Les paquets de Rapport d'appartenance de groupe vont arriver à chaque nœud qui est membre du groupe rapporté par un des VC rattachés à chaque client MARS du nœud. Le client MARS va désencapsuler le paquet entrant et celui-ci va être passé à la couche réseau IPv6 pour traitement. Le client MARS du nœud envoyeur va filtrer le paquet à réception.

Un hôte IPv6 envoie un message Réduction d'appartenance de groupe lorsque l'hôte quitte un groupe de diffusion groupée IPv6. La Réduction d'appartenance de groupe est envoyée au groupe de diffusion groupée que quitte l'hôte IPv6. La transmission et la réception des messages Réduction d'appartenance de groupe est traitée de la même façon que les rapports d'appartenance de groupe.

Appendice B Autres modèles de prise en charge de MARS pour ND intra-LL

B.1 Approche simpliste – Utiliser MARS "tel quel"

Le pilote IPv6/NBMA utilise le protocole MARS standard pour établir en sortie de l'interface un chemin de transmission par circuit virtuel sur lequel il puisse transmettre tous les paquets IPv6 en diffusion groupée, y compris les paquets ICMPv6. Les paquets IPv6 sont alors transmis et reçus par l'ensemble des destinations prévues, en utilisant des VC point à multipoint distincts par groupe de destination.

Dans cette approche, tous les éléments du protocole décrits dans [5] sont utilisés 'tels quels'. Cependant, la consommation des ressources de SVC doit être prise en compte. Malheureusement, la découverte de voisin suppose que les ressources de diffusion du niveau liaison sont mieux conservées en générant un ensemble épars d'adresses de diffusion groupée de nœuds sollicités (auxquelles les interrogations de découverte sont initialement envoyées). Le but original était de minimiser le nombre de nœuds innocents qui reçoivent simultanément les messages de découverte destinés en réalité à quelqu'un d'autre.

Cependant, dans les environnements NBMA orientés connexion, il devient aussi (sinon plus) important de minimiser le nombre de VC indépendants qu'une interface NBMA donnée est obligée de générer ou recevoir. Si nous traitons le service MARS comme une "boîte noire", l'espace épars d'adresses de nœud sollicité peut conduire à un grand nombre de circuits virtuels en point à multi point de courte utilisation, mais d'une durée de vie plus longue (générés chaque fois que le nœud transmet des sollicitations de voisins). Encore plus ennuyeux, ces circuits virtuels ne sont utiles que pour l'envoi de paquets supplémentaires à leur adresse associée de diffusion groupée de nœud sollicité. Un nouveau circuit virtuel point à point est nécessaire pour porter réellement le trafic IPv6 en envoi individuel qui a déclanché la sollicitation de voisin.

L'axe d'inefficacité apporté par l'espace épars d'adresses de nœud sollicité est orthogonal au compromis maillage de circuit virtuel contre serveur de diffusion groupée. Normalement, le serveur de diffusion groupée agrège les flux de trafic pour un groupe de diffusion groupée commun sur un seul VC. Pour réduire la consommation de VC pour la découverte de voisin, on a besoin d'agréger sur l'espace d'adresses de nœud sollicité - effectuant l'agrégation sur la base de la fonction du paquet plutôt que sur sa destination IPv6 explicite. Ici, le compromis est que l'agrégation retire la valeur originale de

l'éparpillement des nœuds à travers l'espace des nœuds sollicités. C'est le prix de la discordance entre la découverte de voisin et les réseaux orientés connexion.

B.2 MARS comme serveur (en diffusion groupée) de liaison

Un mécanisme d'agrégation possible est que chaque pilote IPv6/NBMA de nœud capture les paquets de diffusion groupée ICMPv6 qui portent des messages en diffusion groupée de découverte de voisin ou de routeur, et retranspose logiquement leur destination en groupe Tous-les-nœuds (portée de liaison locale). En s'assurant que le groupe Tous-les-nœuds est pris en charge par un serveur de diffusion groupée, la charge en circuits virtuels résultante au sein de la LL sera significativement réduite.

Une autre optimisation consiste pour le pilote IPv6/NBMA de chaque nœud à capturer les paquets ICMPv6 en diffusion groupée qui portent des messages en diffusion groupée de découverte de voisin ou de routeur, et à les envoyer au MARS lui-même pour retransmission sur ClusterControlVC (ce qui implique une extension triviale au MARS lui-même). Cette approche suppose que dans toute liaison logique qui prend en charge la diffusion groupée IPv6 :
- les nœuds ont déjà un circuit virtuel point à point avec leur MARS,
- le MARS a un circuit virtuel en point à multi point (ClusterControlVC) pour tous les membres de la grappe (les membres de la liaison logique enregistrés comme prenant en charge la diffusion groupée).

Comme les circuits virtuels entre un MARS et son client MARS portent des paquets encapsulés LLC/SNAP, les paquets ICMP peuvent être multiplexés avec les messages de contrôle MARS normaux. Par nature, le MARS se comporte comme un serveur de diffusion groupée pour les paquets non MARS qu'il reçoit des alentours de la LL.

Comme il n'y a pas d'exigence qu'un client MARS n'accepte que les messages de contrôle MARS sur ClusterControlVC, les paquets ICMP reçus de cette façon peuvent être passés à la couche IP de tout nœud sans autre commentaire. Au sein de la couche IP, le filtrage va survenir sur la base de l'adresse IP de destination réelle du paquet, et seul le nœud ciblé va finalement répondre.

Il est regrettable que cette approche fasse que tous les membres de la grappe doivent recevoir divers messages ICMPv6 qu'ils vont toujours devoir éliminer.

Appendice C Détection de flux

Les relations entre les flux de paquets IPv6, les garanties de qualité de service, et l'utilisation facultative des ressources sous-jacentes de réseau IP et NBMA font encore l'objet de recherches actuellement dans l'IETF (précisément dans les groupes de travail ISSLL, RSVP, IPNG, et ION). Le présent document ne décrit que l'utilisation de la détection de flux comme moyen d'optimiser l'usage des ressources d'un réseau NBMA à travers l'établissement de raccourcis inter-LL.

C.1 Utilisation d'identifiant de flux différent de zéro pour supprimer la détection de flux

Pour les besoins de cette architecture IPv6/NBMA, un flux est une séquence ordonnée de paquets IPv6 sur laquelle le routeur de premier bond est autorisé à effectuer la détection de flux afin de déclancher la découverte de raccourci.

La relation entre ces paquets (par exemple, par des champs d'en-têtes communs tels que les adresses de destination IPv6) est une question de configuration locale.

La règle de la détection de flux spécifie que seuls les paquets avec un identifiant de flux de zéro peuvent être considérés comme des flux pour lesquels la découverte de raccourci peut être déclanchée. La raison de cette décision est que :
- les raccourcis NBMA sont destinés à l'optimisation de la transmission par le réseau des paquets IPv6 en l'absence de toute autre indication de la part de l'hôte ;
- il est souhaitable qu'un hôte IPv6/NBMA ait un mécanisme pour surmonter les tentatives 'du réseau' d'optimiser son chemin de transmission interne ;
- un FlowID de zéro a une sémantique IPv6 de "la source permet au réseau d'utiliser à sa discrétion la fourniture du service de transmission au mieux pour les paquets qui ont un FlowID de zéro" ;
- la sémantique IPv6 du FlowID de zéro est cohérente avec la règle de détection de flux du présent document que "si le FlowID est zéro, on est libre d'optimiser le chemin de transmission en utilisant des raccourcis" ;
- un FlowID différent de zéro a la sémantique IPv6 de "la source a précédemment établi un comportement préféré de transmission de bout en bout pour les paquets avec ce FlowID" ;

- la sémantique IPv6 d'un FlowID différent de zéro est cohérente avec la règle de détection de flux du présent document que "si le FlowID est différent de zéro, ne pas essayer d'imposer un raccourci".

Un FlowID différent de zéro peut être alloué par l'hôte de source après la négociation d'un mécanisme préféré de transmission avec "le réseau" (par exemple, par des moyens dynamiques tels que RSVP, ou des moyens administratifs). Autrement, il peut être simplement alloué par l'hôte de source, et le réseau va fournir par défaut une transmission au mieux (un routeur IPv6 revient par défaut à la fourniture de la transmission au mieux pour les paquets dont la paire FlowID/adresse de source n'est pas reconnue).

Donc, les modes de fonctionnement pris en charge par le présent document deviennent :

FlowID de zéro : Transmission au mieux, avec la découverte de raccourci facultative déclanchée au moyen de la détection de flux.

FlowID différent de zéro :

Transmission au mieux si les routeurs le long du chemin n'ont pas été configurés autrement avec des règles de traitement de remplacement pour cette paire FlowID/adresse de source. La détection de flux relative à la découverte de raccourci est suspendue.

Si les routeurs le long du chemin ont été configurés avec des règles de traitement particulières pour cette paire FlowID/adresse de source, le flux est traité conformément à ces règles. La détection de flux relative à la découverte de raccourci est suspendue.

Les mécanismes pour établir des règles particulières de traitement par bond pour les paquets qui ont un identifiant de flux différent de zéro ne sont ni visés ni impliqués par le présent document.

C.2 Futures directions de la détection de flux

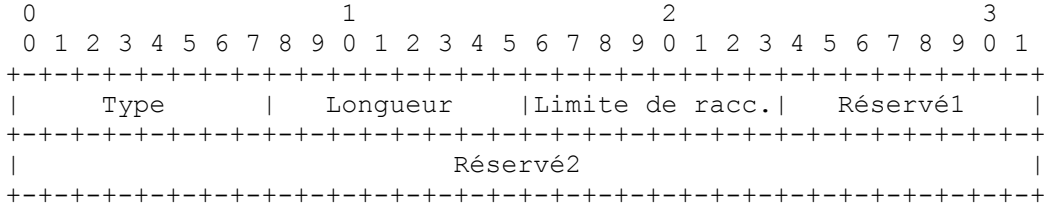
À l'avenir, une transposition précise des flux IPv6 en circuits virtuels NBMA pourrait exiger que plus d'informations soient échangées durant le processus de découverte de voisin qu'il n'en est actuellement disponible dans les paquets de découverte de voisin. Dans ce cas, le protocole de découverte de voisin IPv6 peut être étendu par l'inclusion de nouvelles options de TLV (voir au paragraphe 4.6 de la RFC1970 [7]). Cependant, si de nouvelles options sont nécessaires, la spécification de ces options doit être coordonnée avec le groupe de travail IPNG. Comme la RFC1970 spécifie que les nœuds doivent ignorer en silence les options qu'ils ne comprennent pas, de nouvelles options peuvent être ajoutées à tout moment sans rompre la rétro compatibilité avec les mises en œuvre existantes.

NHRP fournit aussi des mécanismes pour l'ajout de TLV facultatifs aux demandes et réponses NHRP. De futurs développements de l'architecture du présent document exigeront des extensions de qualité de service cohérentes à la fois à la découverte de voisin et à NHRP afin de s'assurer qu'elles sont sémantiquement équivalentes (les différences syntaxiques sont indésirables, mais peuvent être tolérées).

La prise en charge de la qualité de service sur les flux IPv6 en envoi individuel n'exige pas d'autres extensions au protocole MARS existant. Cependant, la future prise en charge de la QS sur les flux IPv6 en diffusion groupée pourra exiger des extensions. Les messages de contrôle MARS partagent le même mécanisme d'extension des TLV que NHRP, permettant aux extensions pour la qualité de service d'être développées en tant que de besoin.

Appendice D Option Limite de raccourci

Pour les messages NS envoyés comme déclencheur de raccourci, un nouveau type d'option ND est nécessaire pour passer les informations sur la limite de bonds du flux de données de l'hôte au routeur. L'utilisation de cette option ND est définie au paragraphe 3.2.2 de cette spécification. Sa représentation binaire suit les règles du paragraphe 4.6 de la RFC4861 :



Champs :
Type : 6
Longueur : 1
Limite de raccourci : Entier non signé de 8 bits. Limite du nombre de bonds pour la tentative de raccourci.
Réservéd1 : Champ inutilisé. Il DOIT être initialisé à zéro par l'envoyeur et ignoré par le receveur.
Réservéd2 : Champ inutilisé. Il DOIT être initialisé à zéro par l'envoyeur et ignoré par le receveur.

Description
L'option Limite de raccourci est utilisée par un hôte dans un message Sollicitation de voisin envoyé comme déclencheur de raccourci à un routeur par défaut. Elle restreint l'interrogation de raccourci du routeur aux cibles accessibles via le nombre de bonds spécifié. La limite de raccourci est donnée par rapport à l'hôte qui demande le raccourci. Les messages NS avec des valeurs de limite de raccourci de 0 ou 1 DOIVENT être ignorées en silence.

Déclaration complète de droits de reproduction