

Groupe de travail Réseau
Request for Comments : 4944
 Catégorie : sur la voie de la normalisation
 Traduction Claude Brière de L'Isle

G. Montenegro, Microsoft Corporation
 N. Kushalnagar, Intel Corp
 J. Hui, Arch Rock Corp
 D. Culler, Arch Rock Corp
 septembre 2007

Transmission des paquets IPv6 sur les réseaux IEEE 802.15.4

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 "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

(La présente traduction incorpore les errata n° 4349 et 6194)

Notice de Copyright

Copyright (C) The Internet Society (2007).

Résumé

Le présent document décrit le format de trame pour la transmission de paquets IPv6 et la méthode de formation des adresses IPv6 de liaison locale et des adresses auto configurées sans état sur les réseaux IEEE 802.15.4. Des spécifications supplémentaires incluent un simple schéma de compression d'en-tête en utilisant un contexte partagé et des dispositions pour la livraison de paquets dans les maillages IEEE 802.15.4.

Table des matières

1. Introduction.....	2
1.1 Notation des exigences.....	2
1.2 Termes utilisés.....	2
2. Mode IEEE 802.15.4 pour IP.....	2
3. Modes d'adressage.....	3
4. Unité maximum de transmission	3
5. Couche d'Adaptation LoWPAN et format de trame.....	4
5.1 Type et en-tête Dispatch.....	5
5.2 Type et en-tête Adressage maillé.....	6
5.3. Type et en-tête Fragmentation.....	6
6. Auto configuration d'adresse sans état.....	8
7. Adresse locale de liaison IPv6.....	8
8. Transposition d'adresse d'envoi individuel.....	9
9. Transposition d'adresse de diffusion groupée.....	9
10 Compression d'en-tête.....	10
10.1 Codage des champs d'en-tête IPv6.....	10
10.2 Codage des champs d'en-tête UDP.....	12
10.3 Champs non compressés.....	12
11. Livraison de trame dans un maillage de couche de liaison.....	13
11.1 Diffusion LoWPAN.....	13
12. Considérations relatives à l'IANA.....	14
13. Considérations sur la sécurité.....	15
14. Remerciements.....	15
15. Références.....	15
15.1 Références normatives.....	15
15.2 Références pour information.....	16
Appendice A. Solutions de remplacement pour la livraison de trames dans un maillage.....	16
Adresse des auteurs.....	17
Déclaration complète de droits de reproduction.....	17

1. Introduction

La norme IEEE 802.15.4 [IEEE802.15.4] a pour cible les réseaux domestiques sans fil à faible puissance (LoWPAN, *low-power personal area network*). Le présent document définit le format de trame pour la transmission des paquets IPv6 [RFC2460] ainsi que la formation des adresses IPv6 de liaison locale et des adresses auto configurées sans état par dessus les réseaux IEEE 802.15.4. Comme IPv6 exige la prise en charge de tailles de paquet beaucoup plus grandes que la plus grande taille de trame IEEE 802.15.4, une couche d'adaptation est définie. Le présent document définit aussi des mécanismes pour la compression d'en-tête nécessaire pour rendre IPv6 praticable sur les réseaux IEEE 802.15.4, et les dispositions requises pour la livraison de paquets dans les maillages IEEE 802.15.4. Cependant, une spécification complète de l'acheminement de maillage (le protocole spécifique utilisé, les interactions avec la découverte de voisin, etc.) sort du domaine d'application du présent document.

1.1 Notation des exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

1.2 Termes utilisés

AES (*Advanced Encryption Standard*) norme de chiffrement évolué

CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*) accès multiple avec surveillance de signal et détection de collision

FFD (*Full Function Device*) appareil à fonctions complètes

GTS (*Guaranteed Time Service*) service à temps garanti

MAC (*Media Access Control*) contrôle d'accès au support

MTU (*Maximum Transmission Unit*) unité de transmission maximum

PAN (*Personal Area Network*) réseau de zone domestique

RFD (*Reduced Function Device*) appareil à fonctions réduites

2. Mode IEEE 802.15.4 pour IP

IEEE 802.15.4 définit quatre types de trames : les trames balises, les trames de commande MAC, les trames d'accusé de réception, et les trames de données. Les paquets IPv6 DOIVENT être portés sur des trames de données. Les trames de données peuvent facultativement demander qu'elles fassent l'objet d'un accusé de réception. Conformément à la [RFC3819], il est recommandé que les paquets IPv6 soient portés dans des trames pour lesquelles des accusés de réception sont demandés afin d'aider à la récupération à la couche de liaison.

Les réseaux IEEE 802.15.4 peuvent être sans capacité de balise ou à capacité de balise [IEEE802.15.4]. Cette dernière est un mode facultatif dans lequel les appareils sont synchronisés par ce qu'on appelle une balise de coordination. Cela permet l'utilisation de supertrames au sein desquelles un service à temps garanti (GTS, *Guaranteed Time Service*) libre de toute concurrence est possible. Le présent document n'exige pas que les réseaux IEEE fonctionnent en mode à capacité de balise. Dans les réseaux sans capacité de balise, les trames de données (incluant celles qui portent des paquets IPv6) sont envoyées via la méthode d'accès par canal fondé sur la concurrence de CSMA/CA sans créneau.

Dans les réseaux sans capacité de balise, les balises ne sont pas utilisées pour la synchronisation. Cependant, elles sont quand même utiles pour la découverte d'appareil de couche de liaison pour aider aux événements d'association et de désassociation. Le présent document recommande que les balises soient configurées de telle façon qu'elles aident ces fonctions. Une autre recommandation est que ces événements soient disponibles à la couche IPv6 pour aider à détecter le rattachement au réseau, un problème sur lequel travaille l'IETF au moment de la rédaction du présent mémoire.

La spécification permet des trames dans lesquelles les adresses de source ou de destination (ou les deux) sont éliminées. Les mécanismes définis dans le présent document exigent que les adresses de source et de destination soient toutes deux incluses dans l'en-tête de trame IEEE 802.15.4. Les champs Identifiant de PAN de source ou destination peuvent aussi être inclus.

3. Modes d'adressage

IEEE 802.15.4 définit plusieurs modes d'adressage : il permet l'utilisation des adresses IEEE étendues de 64 bits ou (après un événement d'association) des adresses de 16 bits uniques dans le PAN [IEEE802.15.4]. Le présent document prend en charge les deux adresses étendues de 64 bits et les adresses courtes de 16 bits. Pour l'utilisation dans les 6LoWPAN, le présent document impose des contraintes supplémentaires (au delà de celles imposées par IEEE 802.15.4) sur le format des adresses courtes de 16 bits, comme spécifié à la Section 12. Les adresses courtes étant transitoires par nature, un mot de précaution est nécessaire : comme elles sont distribuées de façon parcimonieuse par la fonction de coordination de PAN durant un événement d'association, leur validité et leur unicité est limitée par la durée de vie de cette association. Cela peut être terminé par l'expiration de l'association ou simplement par un accident survenant au coordinateur de PAN. À cause des problèmes d'adaptabilité posés par une telle allocation centralisée et un seul point de défaillance au coordinateur de PAN, les déploieurs devraient soupeser avec attention les compromis (et mettre en œuvre les mécanismes nécessaires) de développement de tels réseaux fondés sur des adresses courtes. Bien sûr, les adresses IEEE étendues de 64 bits ne peuvent pas souffrir de tels inconvénients, mais elles subissent les problèmes restants d'adaptabilité concernant l'acheminement, la découverte, la configuration, etc.

Le présent document suppose qu'un PAN se transpose en une liaison IPv6 spécifique. Cela se conforme à la recommandation que les réseaux partagés prennent en charge la diffusion de sous réseau de couche de liaison [RFC3819]. Strictement parlant, c'est la diffusion groupée, et non la diffusion qui existe dans IPv6. Cependant, la diffusion groupée n'est pas prise en charge de façon native dans IEEE 802.15.4. Donc, les paquets de diffusion groupée de niveau IPv6 DOIVENT être portés comme des trames de diffusion de couche de liaison dans les réseaux IEEE 802.15.4. Ceci DOIT être fait de façon telle que les trames en diffusion soient seulement prises en compte par les appareils au sein du PAN spécifique de la liaison en question. Selon le paragraphe 7.5.6.2 de [IEEE802.15.4], ceci est accompli comme suit :

1. un identifiant de PAN de destination est inclus dans la trame, et il DOIT correspondre à l'identifiant de PAN de la liaison en question ;
2. une adresse de destination courte est incluse dans la trame, et elle DOIT correspondre à l'adresse de diffusion (0xffff).

De plus, la prise en charge de la transposition des adresses de diffusion groupée IPv6 selon la Section 9 DOIT seulement être utilisée dans une configuration de maillage. La spécification d'une telle fonction sort du domaine d'application du présent document.

Comme d'habitude, les hôtes apprennent les préfixes IPv6 via les annonces de routeur, conformément à la [RFC4861].

4. Unité maximum de transmission

La taille de MTU pour les paquets IPv6 sur IEEE 802.15.4 est de 1280 octets. Cependant, un paquet IPv6 plein ne tient pas dans une trame IEEE 802.15.4. Les unités de données de protocole 802.15.4 ont des tailles différentes selon la quantité de frais généraux présente [IEEE802.15.4]. En commençant par une taille maximum de paquet de couche physique de 127 octets (aMaxPHYPacketSize) et des frais généraux maximum de trame de 25 (aMaxFrameOverhead) la taille maximum de trame résultante à la couche de contrôle d'accès au support est 102 octets. La sécurité de la couche de liaison impose plus de frais généraux, qui dans le cas maximum (21 octets de frais généraux dans le cas de AES-CCM-128, contre 9 et 13 pour AES-CCM-32 et AES-CCM-64, respectivement) laisse seulement 81 octets disponibles. Ceci est évidemment très en dessous de la taille minimum de paquet IPv6 de 1280 octets, et en ligne avec la Section 5 de la spécification IPv6 [RFC2460], une couche d'adaptation de fragmentation et réassemblage doit être fournie à la couche en dessous de IP. Cette couche est définie à la Section 5.

De plus, comme l'en-tête IPv6 est de 40 octets, cela laisse seulement 41 octets pour les protocoles de couche supérieure, comme UDP. Ce dernier utilise 8 octets dans l'en-tête ce qui laisse seulement 33 octets pour les données d'application. Comme on l'a noté plus haut, il y a besoin d'une couche de fragmentation et réassemblage, ce qui va utiliser encore plus d'octets.

Ces considérations conduisent aux deux observations suivantes :

1. La couche d'adaptation doit être fournie pour se conformer aux exigences de IPv6 d'une MTU minimum. Cependant, on s'attend à ce que (a) la plupart des applications de IEEE 802.15.4 n'utilisent pas d'aussi gros paquets, et (b) de petites charges utiles d'application en conjonction avec la compression d'en-tête appropriée vont produire des paquets qui tiennent dans une seule trame IEEE 802.15.4. La justification de cette couche d'adaptation n'est pas juste pour la conformité à IPv6, car il est assez probable que les tailles de paquet produites par certains échanges d'application (par

exemple, la configuration ou le provisionnement) peuvent exiger un petit nombre de fragments.

- Même si le calcul d'espace ci-dessus montre le scénario du pire des cas, il souligne le fait que la compression d'en-tête est une exigence presque inévitable. Comme on s'attend à ce que la plupart (sinon toutes) les applications de IP sur IEEE 802.15.4 utilisent la compression d'en-tête, elle est définie à la Section 10.

5. Couche d'Adaptation LoWPAN et format de trame

Les formats d'encapsulation définis dans cette section (auxquels on se réfère ensuite comme "encapsulation LoWPAN") sont la charge utile dans l'unité de données de protocole (PDU, *protocol data unit*) MAC de IEEE 802.15.4. La charge utile LoWPAN (par exemple, un paquet IPv6) suit cet en-tête d'encapsulation.

Tous les datagrammes encapsulés LoWPAN transportés sur IEEE 802.15.4 sont munis d'un préfixe par une pile d'en-tête d'encapsulation. Chaque en-tête dans la pile d'en-tête contient un type d'en-tête suivi par zéro, un ou plusieurs champs d'en-tête. Tandis que dans un en-tête IPv6 la pile va contenir, dans l'ordre suivant, l'adressage, les options bond par bond, l'acheminement, la fragmentation, les options de destination, et finalement la charge utile [RFC2460], dans un en-tête LoWPAN, la séquence d'en-tête analogue est l'adressage maillé (de couche 2) les options bond par bond (incluant la diffusion/diffusion groupée de couche 2) la fragmentation, et finalement la charge utile. Les exemples qui suivent montrent des piles d'en-têtes typiques qui peuvent être utilisées dans un réseau LoWPAN.

Un datagramme IPv6 encapsulé LoWPAN :

```
+-----+-----+-----+
| Répartiteur IPv6 | En-tête IPv6 | Charge utile |
+-----+-----+-----+
```

Un datagramme IPv6 compressé LOWPAN_HC1 encapsulé LoWPAN :

```
+-----+-----+-----+
| Répartiteur HC1 | En-tête HC1 | Charge utile |
+-----+-----+-----+
```

Un datagramme IPv6 compressé LOWPAN_HC1 encapsulé LoWPAN qui exige un adressage maillé :

```
+-----+-----+-----+-----+-----+
| Type maillage | En-tête maillage | Répartiteur HC1 | En-tête HC1 | Charge utile |
+-----+-----+-----+-----+-----+
```

Un datagramme IPv6 compressé LOWPAN_HC1 encapsulé LoWPAN qui exige une fragmentation :

```
+-----+-----+-----+-----+-----+
| Type frag | En-tête frag | Répartiteur HC1 | En-tête HC1 | Charge utile |
+-----+-----+-----+-----+-----+
```

Un datagramme IPv6 compressé LOWPAN_HC1 encapsulé LoWPAN qui exige à la fois l'adressage de maillage et la fragmentation :

```
+-----+-----+-----+-----+-----+-----+
| Type mg | E-t mg | Type fr | E-t fr | Rép. HC1 | E-t HC1 | Charge utile |
+-----+-----+-----+-----+-----+-----+
```

Un datagramme IPv6 compressé LOWPAN_HC1 encapsulé LoWPAN qui exige à la fois l'adressage de maillage et un en-tête de diffusion pour prendre en charge la diffusion/diffusion groupée maillée :

```
+-----+-----+-----+-----+-----+-----+
| Type mg | E-t mg | Rép dif | E-t dif | Réprt HC1 | E-t HC1 | Charge utile |
+-----+-----+-----+-----+-----+-----+
```

Lorsque plus d'un en-tête LoWPAN est utilisé dans le même paquet, ils DOIVENT apparaître dans l'ordre suivant:

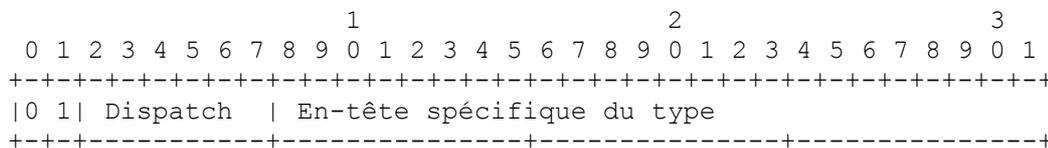
En-tête d'adressage maillé
 En-tête de diffusion
 En-tête de fragmentation

Tous les datagrammes de protocole (par exemple, IPv6, en-têtes IPv6 compressés, etc.) DEVRONT être précédés d'un des en-têtes d'encapsulation LoWPAN valides, dont des exemples sont donnés ci-dessus. Cela permet un traitement de logiciel uniforme sans considération de leur mode de transmission.

La définition des en-têtes LoWPAN, autre que d'adressage maillé et de fragmentation, consiste en la valeur de répartition, la définition des champs d'en-tête qui suivent, et de leurs contraintes d'ordre par rapport à tous les autres en-têtes. Bien que la structure de pile d'en-tête donne un mécanisme pour traiter de futures demandes sur la couche d'adaptation LoWPAN, elle n'est pas destinée à fournir un mécanisme d'extensibilité généraliste. Le présent document de format spécifie un petit ensemble de types d'en-tête en utilisant la pile d'en-têtes dans un souci de clarté, compacité, et orthogonalité.

5.1 Type et en-tête Dispatch

Le type dispatch (*répartiteur*) est défini par un bit à zéro comme premier bit et un bit à 1 comme second bit. Le type et l'en-tête dispatch sont montrés ci-dessous :



Dispatch : sélecteur de 6 bits. Identifie le type de l'en-tête qui suit immédiatement l'en-tête Dispatch.

En-tête spécifique du type : en-tête déterminé par l'en-tête Dispatch.

Figure 1 : Type et en-tête Dispatch

La valeur de dispatch peut être traitée comme un espace de noms non structuré. Seuls quelques symboles sont requis pour représenter la fonction LoWPAN actuelle. Bien que quelques économies supplémentaires pourraient être réalisées par une fonction de codage supplémentaire dans l'octet dispatch, ces mesures tendraient à contraindre la capacité de traiter de futures solutions de remplacement.

Schéma	Type d'en-tête
00 xxxxxx	NALP (<i>Not a LoWPAN frame</i>) pas une trame LoWPAN
01 000001	IPv6 : adresses IPv6 non compressées
01 000010	LOWPAN_HC1 - IPv6 LOWPAN_HC1 compressé
01 000011	réservé - réservé pour une utilisation future
...	réservé - réservé pour une utilisation future
01 001111	réservé - réservé pour une utilisation future
01 010000	LOWPAN_BC0 - diffusion LOWPAN_BC0
01 010001	réservé - réservé pour une utilisation future
...	réservé - réservé pour une utilisation future
01 111110	réservé - réservé pour une utilisation future
01 111111	ESC - des octets Dispatch supplémentaires suivent
10 xxxxxx	MESH - en-tête de maillage
11 000xxx	FRAG1 - en-tête de fragmentation (premier)
11 001000	réservé - réservé pour une utilisation future
...	réservé - réservé pour une utilisation future
11 011111	réservé - réservé pour une utilisation future
11 100xxx	FRAGN - en-tête de fragmentation (suivant)
11 101000	réservé - réservé pour une utilisation future
...	réservé - réservé pour une utilisation future
11 111111	réservé - réservé pour une utilisation future

Figure 2 : Schéma de bit de valeur Dispatch

NALP : spécifie que les bits suivants ne font pas partie de l'encapsulation LoWPAN, et que tout nœud LoWPAN qui rencontre une valeur dispatch de 00xxxxxx devra éliminer le paquet. Les autres protocoles non LoWPAN qui souhaitent coexister avec des nœuds LoWPAN devraient inclure un octet correspondant à ce schéma suivant immédiatement l'en-tête 802.15.4.

IPv6 : spécifie que l'en-tête suivant est un en-tête IPv6 non compressé [RFC2460].

LOWPAN_HC1 : spécifie que l'en-tête suivant est un en-tête IPv6 LOWPAN_HC1 compressé. Ce format d'en-tête est défini dans la Figure 9.

LOWPAN_BC0 : spécifie que l'en-tête suivant est un en-tête LOWPAN_BC0 pour la prise en charge de diffusion/diffusion groupée maillée et est décrit au paragraphe 11.1.

ESC : spécifie que l'en-tête suivant est un seul champ de 8 bits pour la valeur de Dispatch. Il permet la prise en charge des valeurs de Dispatch supérieures à 63.

5.2 Type et en-tête Adressage maillé

Le type Maillé est défini par un bit à 1 et un bit à zéro comme deux premiers bits. Le type et l'en-tête Maillé sont :

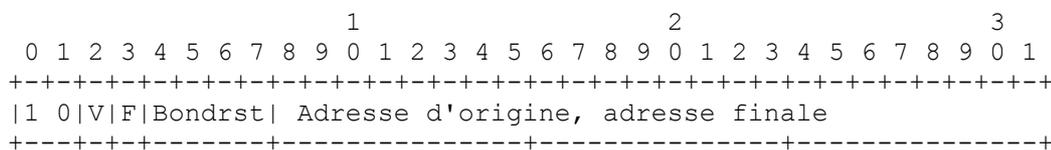


Figure 3 : Type et en-tête d'adressage maillé

La définitions des champs est la suivante :

V : Ce champ de 1 bit DEVRA être à zéro si l'adresse d'origine (ou la "toute première") est une adresse IEEE étendue de 64 bits (EUI-64), ou 1 si c'est une adresse courte de 16 bits.

F : Ce champ de 1 bit DEVRA être à zéro si l'adresse Destination finale est une adresse IEEE étendue de 64 bits (EUI-64), ou 1 si c'est une adresse courte de 16 bits.

Bonds restants : ce champ de 4 bits DEVRA être décrémenté par chaque nœud transmetteur avant l'envoi de ce paquet vers son prochain bond. Le paquet n'est plus transmis si Bonds restants est à zéro. La valeur 0xF est réservée et signifie qu'un champ de 8 bits Bonds restants profonds suit immédiatement, et permet à un nœud source de spécifier une limite de bonds supérieure à 14 bonds.

Adresse d'origine : c'est l'adresse de couche de liaison de l'origine.

Adresse de destination finale : c'est l'adresse de couche de liaison de la destination finale.

Noter que les bits 'V' et 'F' permettent un mélange d'adresses de 16 et de 64 bits. Cela est utile au moins pour permettre la couche de maillage "diffusion", car les adresses de diffusion 802.15.4 sont définies comme des adresses courtes de 16 bits.

Des explications plus détaillées de la livraison de trame au sein d'un maillage sont à la Section 11.

5.3 Type et en-tête Fragmentation

Si une charge utile entière (par exemple, IPv6) de datagramme tient dans une seule trame 802.15.4, elle n'est pas fragmentée et l'encapsulation LoWPAN ne devrait pas contenir d'en-tête de fragmentation. Si le datagramme ne tient pas dans une seule trame IEEE 802.15.4, elle DEVRA être coupée en fragments sur la liaison. Comme le décalage de fragment peut seulement exprimer des multiples de huit octets, tous les fragments de liaison pour un datagramme sauf le dernier DOIVENT être des multiples de huit octets. Le premier fragment de liaison DEVRA contenir l'en-tête de premier fragment comme défini ci-dessous.

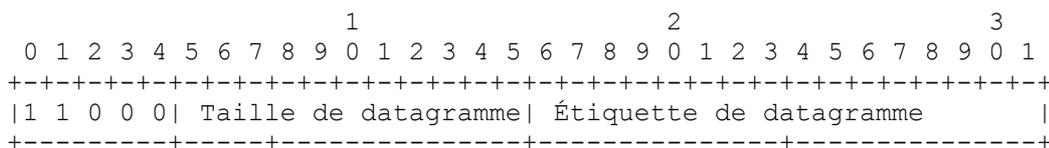


Figure 4 : premier fragment

Le second fragment et les suivants (jusque et y compris le dernier) DEVRONT contenir un en-tête de fragmentation qui se conforme au format ci-dessous.

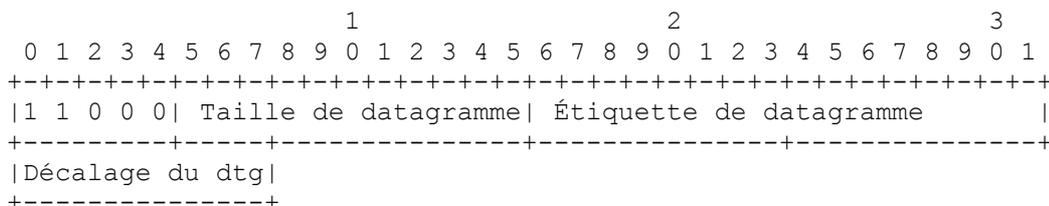


Figure 5 : Fragments suivants

Taille de datagramme : ce champ de 11 bits code la taille du paquet IP entier avant la fragmentation de couche de liaison (mais après la fragmentation de couche IP). La valeur de Taille de datagramme DEVRA être la même pour tous les fragments de couche de liaison d'un paquet IP. Pour IPv6, ce DEVRA être 40 octets (la taille de l'en-tête IPv6 non compressé) plus la valeur de la longueur de charge utile dans l'en-tête IPv6 [RFC2460] du paquet. Noter que ce paquet peut être déjà fragmenté par les hôtes impliqués dans la communication, c'est-à-dire, ce champ doit coder une longueur maximum de 1280 octets (la MTU de liaison IEEE 802.15.4, comme définie dans le présent document).

Note : Ce champ n'a pas besoin d'être dans chaque paquet, car on pourrait l'envoyer dans le premier fragment et l'éliminer ensuite. Cependant, l'inclure dans chaque fragment de liaison facilite la tâche de réassemblage pour le cas où un second (ou suivant) fragment de liaison arriverait avant le premier. Dans ce cas, la garantie d'apprendre la taille de datagramme aussitôt qu'un des fragments arrive dit au receveur combien d'espace de mémoire tampon établir pendant qu'il attend le reste des fragments. Le format ci-dessus fait un compromis entre simplicité et efficacité.

Étiquette de datagramme : la valeur de l'étiquette de datagramme DEVRA être la même pour tous les fragments de liaison d'une charge utile de datagramme (par exemple, IPv6). L'envoyeur DEVRA incrémenter l'étiquette de datagramme pour les datagrammes fragmentés successifs. La valeur incrémentée de Étiquette de datagramme DEVRA revenir de 65535 à zéro. Ce champ est de 16 bits, et sa valeur initiale n'est pas définie.

Décalage du datagramme : ce champ n'est présent que dans le second et les fragments de liaison suivants et DEVRA spécifier le décalage, en incréments de 8 octets, du fragment par rapport au début du datagramme de charge utile. Le premier octet du datagramme (par exemple, le début de l'en-tête IPv6) a un décalage de zéro ; la valeur implicite du décalage du datagramme dans le premier fragment est zéro. Ce champ est long de 8 bits.

Le receveur de fragments de liaison DEVRA utiliser (1) l'adresse de source 802.15.4 de l'envoyeur (ou l'adresse d'origine si un champ Adressage maillé est présent) (2) l'adresse 802.15.4 de la destination (ou l'adresse de destination finale si un champ Adressage maillé est présent) (3) Taille de datagramme, et (4) Étiquette de datagramme pour identifier tous les fragments de liaison qui appartiennent à un certain datagramme.

À réception d'un fragment de liaison, le receveur commence à construire le paquet non fragmenté original dont la taille est Taille de datagramme. Il utilise le champ décalage du datagramme pour déterminer la localisation des fragments individuels au sein du paquet original non fragmenté. Par exemple, il peut placer les données de charge utile (sauf l'en-tête d'encapsulation) au sein d'une mémoire tampon de réassemblage de datagramme de charge utile à l'endroit spécifié par le décalage du datagramme. La taille de la mémoire tampon de réassemblage DEVRA être déterminée à partir de la taille du datagramme.

Si un fragment de liaison qui chevauche un autre fragment est reçu, comme identifié ci-dessus, et diffère soit par la taille soit par le décalage du fragment chevauché, le ou les fragments déjà accumulés dans la mémoire tampon de réassemblage DEVRONT être éliminés. Un nouveau réassemblage peut être commencé avec le fragment de liaison le plus récemment reçu. Le chevauchement de fragments est déterminé par la combinaison du décalage de datagramme provenant de l'en-tête d'encapsulation et de "Longueur de trame" provenant de l'en-tête de paquet Unité de données de protocole de couche

physique (PPDU, *Physical Layer Protocol Data Unit*) 802.15.4.

Sur détection d'un événement Désassociation IEEE 802.15.4, les receveurs de fragment DOIVENT éliminer tous les fragments de tous les datagrammes de charge utile partiellement réassemblés, et les envoyeurs de fragment DOIVENT éliminer tous les fragments de liaison non encore transmis de toute charge utile de datagramme partiellement transmise (par exemple, IPv6). De même, quand un nœud reçoit d'abord un fragment avec une certaine étiquette de datagramme, il lance un temporisateur de réassemblage. Quand ce temporisateur arrive à expiration, si le paquet entier n'a pas été réassemblé, les fragments existants DOIVENT être éliminés et l'état de réassemblage DOIT être purgé. La temporisation de réassemblage DOIT être réglée à un maximum de 60 secondes (c'est aussi la temporisation dans la procédure de réassemblage IPv6 [RFC2460]).

6. Auto configuration d'adresse sans état

Cette Section définit comment obtenir un identifiant d'interface IPv6.

L'identifiant d'interface [RFC4291] pour une interface IEEE 802.15.4 peut être fondé sur l'identifiant EUI-64 [EUI64] alloué à l'appareil IEEE 802.15.4. Dans ce cas, l'identifiant d'interface est formé du EUI-64 en accord avec la spécification "IPv6 sur Ethernet" [RFC2464].

Tous les appareils 802.15.4 ont une adresse IEEE EUI-64, mais des adresses courtes de 16 bits (Section 3 et Section 12) sont aussi possibles. Dans ce cas, une "pseudo adresse de 48 bits" est formée comme suit. D'abord, le 32 bits de gauche sont formés en enchaînant 16 bits de zéros à l'identifiant de PAN de 16 bits (autrement, si aucun identifiant de PAN n'est connu, 16 bits de zéros peuvent être utilisés). Cela produit un champ de 32 bits comme suit :

PAN de 16 bits : 16 bits de zéros

Ensuite, ces 32 bits sont enchaînés avec l'adresse courte de 16 bits. Cela produit une adresse de 48 bits comme suit :

32 bits comme spécifié précédemment : adresse courte de 16 bits

L'identifiant d'interface est formé de cette adresse de 48 bits selon la spécification "IPv6 sur Ethernet" [RFC2464]. Cependant, dans l'identifiant d'interface résultant, le bit "Universel/Local" (U/L) DEVRA être établi à un en sachant que cette valeur n'est pas unique au monde. Pour l'un et l'autre format d'adresse, des adresses toutes de zéros NE DOIVENT PAS être utilisées.

Une adresse MAC différente réglée manuellement ou par le logiciel PEUT être utilisée pour déduire l'identifiant d'interface. Si une telle adresse MAC est utilisée, sa propriété d'unicité mondiale devrait être reflétée dans la valeur du bit U/L.

Un préfixe d'adresse IPv6 utilisé pour l'auto configuration d'adresse sans état [RFC4862] d'une interface IEEE 802.15.4 DOIT avoir une longueur de 64 bits.

7. Adresse locale de liaison IPv6

L'adresse IPv6 de liaison locale [RFC4291] pour une interface IEEE 802.15.4 est formée en ajoutant l'identifiant d'interface, comme défini ci-dessus, au préfixe FE80::/64.

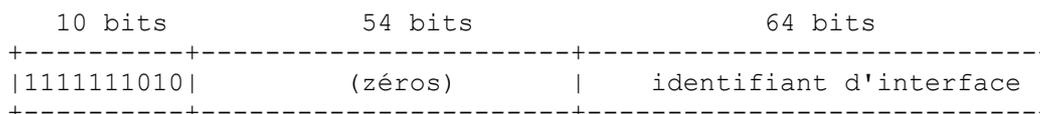


Figure 6

8. Transposition d'adresse d'envoi individuel

La procédure de résolution d'adresse pour transposer les adresses IPv6 non de diffusion groupée en adresses de couche de liaison IEEE 802.15.4 suit la description générale du paragraphe 7.2 de la [RFC4861], sauf mention contraire.

L'option Adresse de source/cible de couche de liaison a les formes suivantes quand la couche de liaison est IEEE 802.15.4 et que les adresses sont respectivement des adresses EUI-64 ou des adresses courtes de 16 bits.

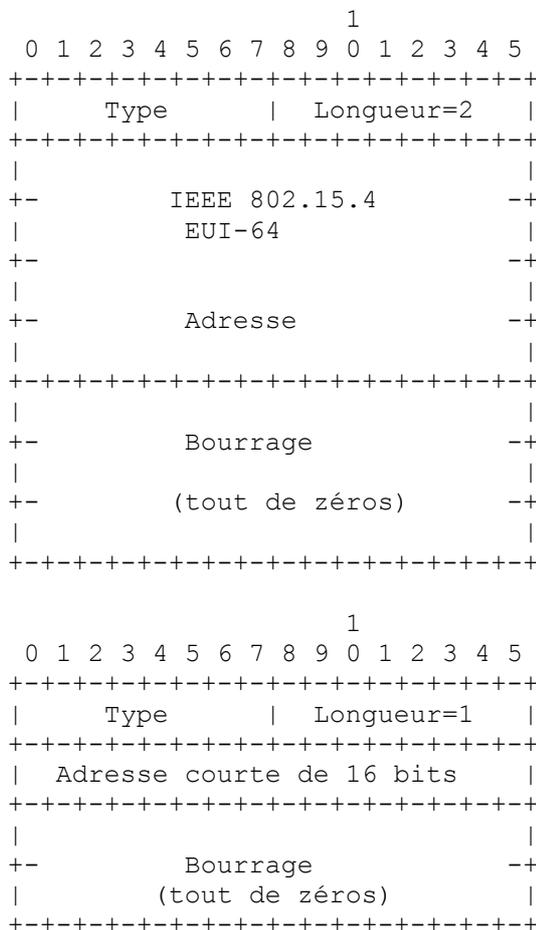


Figure 7

Champs d'option :

Type : 1 pour l'adresse de source de couche de liaison, 2 pour l'adresse cible de couche de liaison.

Longueur : c'est la longueur de cette option (incluant les champs de type et de longueur) en unités de 8 octets. La valeur de ce champ est 2 si on utilise des adresses EUI-64, ou 1 si on utilise des adresses courtes de 16 bits.

Adresse IEEE 802.15.4 : adresse IEEE 802.15.4 de 64 bits, ou adresse courte de 16 bits (selon le format de la Section 9) dans l'ordre canonique des bits. C'est l'adresse à laquelle l'interface répond actuellement. Cette adresse peut être différente de l'adresse incorporée utilisée pour déduire l'identifiant d'interface, à cause de considérations de confidentialité ou de sécurité (par exemple, de découverte de voisin).

9. Transposition d'adresse de diffusion groupée

La fonctionnalité de cette section DOIT seulement être utilisée dans un LoWPAN à capacité de maillage. Un paquet IPv6 avec une adresse de destination de diffusion groupée (DST), consistant en les seize octets de DST[1] à DST[16], est transmise à l'adresse de diffusion groupée 802.15.4 de 16 bits suivante :

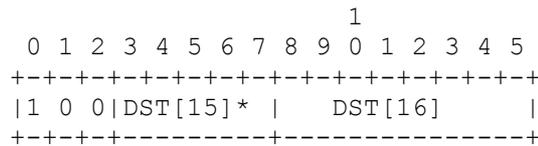


Figure 8

Ici, DST[15]* se réfère aux 5 derniers bits de l'octet DST[15], qui sont les bits 3 à 7 au sein de DST[15]. Le schéma initial de 3 bits de "100" suit le format d'adresse de 16 bits pour les adresses de diffusion groupée (Section 12).

Cela permet la prise en charge de la diffusion groupée au sein des réseaux 6LoWPAN, mais la spécification complète d'une telle prise en charge sort du domaine d'application du présent document. Des exemples du mécanisme sont l'arrosage, l'arrosage contrôlé, l'envoi individuel au coordinateur PAN, etc. Il est prévu que cela soit spécifié par les différents mécanismes d'acheminement maillé.

10 Compression d'en-tête

Il y a beaucoup de travaux de normalisation publiés et en cours sur la compression d'en-tête. Néanmoins, la compression d'en-tête pour IPv6 sur IEEE 802.15.4 a des contraintes différentes résumées comme suit :

Les travaux existants supposent qu'il y a de nombreux flux entre deux appareils. Ici, on suppose une nuance très simple et de peu de contexte pour la compression d'en-tête. Alors que cela fonctionne indépendamment des flux (potentiellement multiples) cela n'utilise aucun contexte spécifique d'un flux. Donc, cela ne peut pas réaliser autant de compression que les schémas qui sont construits sur un contexte séparé pour chaque flux à compresser.

Étant donnée la taille très limitée des paquets, il est souhaitable d'intégrer la compression de couche 2 avec celle de couche 3, chose qui n'est traditionnellement pas faite (bien que cela change maintenant avec le groupe de travail ROHC (compression d'en-tête robuste)).

Il est prévu que les appareils IEEE 802.15.4 seront déployés dans des réseaux multi bonds. Cependant, la compression d'en-tête dans un maillage est différente du scénario usuel de liaisons point à point dans lequel le compresseur et le décompresseur sont en communication directe et exclusive l'un avec l'autre. Dans un réseau IEEE 802.15.4, il est très souhaitable qu'un appareil soit capable d'envoyer des paquets à en-tête compressé via tous ses voisins, avec aussi peu de construction de contexte préliminaire que possible.

Tous les nouveaux formats de paquet requis par la compression d'en-tête réutilisent les formats de paquet de base définis à la Section 5 en utilisant des valeurs de répartiteur différentes.

La compression d'en-tête peut résulter en ce que l'alignement ne tombe pas sur une limite d'octet. Comme les matériels ne peuvent normalement pas transmettre des données dans des unités de moins qu'un octet, du bourrage doit être utilisé. Le bourrage est fait comme suit : d'abord, la série entière d'en-têtes contigus compressés est affichée (le présent document définit seulement des schémas de compression d'en-tête IPv6 et UDP, mais d'autres peuvent être définis ailleurs). Ensuite, des bits zéro DEVRAIENT être ajoutés comme approprié pour s'aligner sur une limite d'octet. Cela contre tout potentiel mauvais alignement causé par la compression d'en-tête, de sorte que les champs suivants (par exemple, des en-têtes non compressés ou des charges utiles de données) commencent sur une limite d'octet et suivent normalement.

10.1 Codage des champs d'en-tête IPv6

Du fait qu'ils se joignent au même réseau 6LoWPAN, les appareils partagent un certain état. Cela rend possible de compresser les en-têtes sans construire explicitement un état de contexte de compression. Donc, la compression d'en-tête 6LoWPAN ne conserve aucun état de flux ; elle s'appuie plutôt sur des informations qui relèvent de la liaison entière. Les valeurs d'en-tête IPv6 suivantes sont supposées être communes sur les réseaux 6LoWPAN, de sorte que l'en-tête HC1 a été construit pour les compresser efficacement d'emblée : la version est IPv6, les adresses IPv6 de source et de destination sont de liaison locale, les identifiants d'interface IPv6 (64 bits du fond) pour les adresses de source ou de destination peuvent être déduits des adresse de source et de destination de couche deux (bien sûr, cela n'est possible que pour les identifiants d'interface déduits d'une adresse MAC 802.15.4 sous-jacente) ; la longueur de paquet peut être déduite de la couche deux

("Longueur de trame" dans la PDU IEEE 802.15.4) ou du champ "taille de datagramme" dans l'en-tête de fragment (si il est présent) ; classe de trafic étiquette de flux sont toutes deux à zéro,; et le prochain en-tête est UDP, ICMP ou TCP. Le seul champ dans l'en-tête IPv6 qui a toujours besoin d'être porté en entier est la limite de bonds (8 bits). Selon la façon dont le paquet suit étroitement ce cas courant, différents champs peuvent ne pas être compressibles, devant donc être portés "en ligne" aussi (paragraphe 10.3.1). Cet en-tête IPv6 commun (comme mentionné ci-dessus) peut être compressé à 2 octets (1 octet pour le codage HC1 et 1 octet pour la limite de bonds) au lieu de 40 octets. Un tel paquet est compressible via le format LOWPAN_HC1 en utilisant une valeur de Dispatch de LOWPAN_HC1 suivie par un champ d'en-tête LOWPAN_HC1 "codage HC1" (8 bits) pour coder les différentes combinaisons montrées ci-dessous. Cet en-tête peut être précédé par un en-tête de fragmentation, qui peut être précédé par un en-tête de maillage.

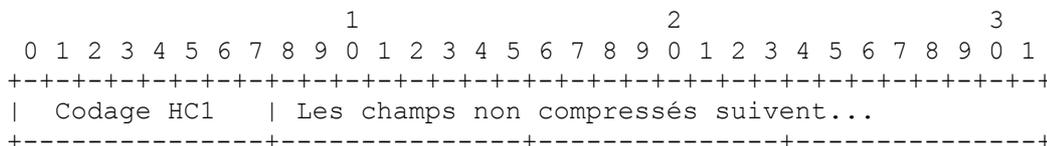


Figure 9 : LOWPAN_HC1 (codage commun d'en-tête compressé)

Comme on peut le voir ci-dessous (bit 7) un codage HC2 peut suivre un octet HC1. Dans ce cas, les champs non compressés suivent le champ de codage HC2 (paragraphe 10.3).

Les champs d'adresse codés par le "codage HC1" sont interprétés comme suit :

PI : Préfixe porté en ligne (paragraphe 10.3.1).

PC : Préfixe compressé (préfixe de liaison locale supposé).

II : Identifiant d'interface porté en ligne (paragraphe 10.3.1).

IC : Identifiant d'interface éliminé (déduit de l'adresse de couche de liaison correspondante). Si il est appliqué à l'identifiant d'interface de l'adresse de source ou de destination lors de l'acheminement dans un maillage (Section 11) l'adresse de couche de liaison correspondante est celle trouvée dans le champ "Adressage maillé" (paragraphe 5.2).

Le "codage HC1" est montré ci-dessous (en commençant au bit 0 et en terminant au bit 7) :

Adresse IPv6 de source (bits 0 et 1) :

00 : PI, II
 01 : PI, IC
 10 : PC, II
 11 : PC, IC

Adresse IPv6 de destination (bits 2 et 3) :

00 : PI, II
 01 : PI, IC
 10 : PC, II
 11 : PC, IC

Classe de trafic et étiquette de flux (bit 4) :

0 : non compressé ; 8 bits complets pour la classe de trafic et 20 bits pour l'étiquette de flux sont envoyés.
 1 : classe de trafic et étiquette de flux sont à zéro.

Prochain en-tête (bits 5 et 6) :

00 : non compressé ; 8 bits complets sont envoyés
 01 : UDP
 10 : ICMP
 11 : TCP

Codage HC2 (bit 7) :

0 : Pas d'autre bit de compression d'en-tête.
 1 : Le codage HC1 est suivi immédiatement par plus de bits de compression d'en-tête selon le format de codage HC2. Les bits 5 et 6 déterminent quels codages HC2 possibles s'appliquent (par exemple, les codages UDP, ICMP, ou TCP).

10.2 Codage des champs d'en-tête UDP

Les bits 5 et 6 de LOWPAN_HC1 permettent de compresser le champ Prochain en-tête dans l'en-tête IPv6 (pour UDP, TCP, et ICMP). Plus de compression de chacun de ces en-têtes de protocole est aussi possible. Ce paragraphe explique comment l'en-tête UDP lui-même peut être compressé. Le codage HC2 dans ce paragraphe est le codage HC_UDP, et il s'applique seulement si les bits 5 et 6 dans HC1 indiquent que le protocole qui suit l'en-tête IPv6 est UDP. Le codage HC_UDP (Figure 10) permet la compression des champs suivants dans l'en-tête UDP : accès de source, accès de destination, et longueur. Le champ Somme de contrôle de l'en-tête UDP n'est pas compressé et est donc porté en entier. Le schéma défini ci-dessous permet la compression de l'en-tête UDP à 4 octets au lieu des 8 octets d'origine.

Le seul champ d'en-tête UDP dont la valeur peut être déduite des informations disponibles ailleurs est Longueur. Les autres champs doivent être portés en ligne soit en entier, soit de manière partiellement compressée (paragraphe 10.3.2).

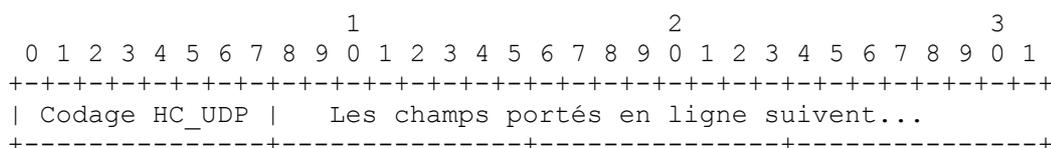


Figure 10 : HC_UDP (codage d'en-tête UDP commun compressé)

Le "codage HC_UDP" pour UDP est montré ci-dessous (en commençant au bit 0 et en terminant au bit 7) :

Accès de source UDP (bit 0) : 0, non compressé, porté "en ligne" (paragraphe 10.3.2) ; 1, compressé à 4 bits. L'accès de source réel de 16 bits est obtenu en calculant : P + valeur d'accès court. La valeur de P est le nombre 61616 (0xF0B0). L'accès court est exprimé par une valeur de 4 bits qui est portée "en ligne" (paragraphe 10.3.2).

Accès de destination UDP (bit 1) : 0, non compressé, porté "en ligne" (paragraphe 10.3.2) ; 1, compressé à 4 bits. L'accès de destination réel de 16 bits est obtenu en calculant : P + valeur d'accès court. La valeur de P est le nombre 61616 (0xF0B0). L'accès court est exprimé par une valeur de 4 bits qui est portée "en ligne" (paragraphe 10.3.2).

Longueur (bit 2) : 0, non compressé, porté "en ligne" (paragraphe 10.3.2) ; 1, compressé, longueur calculée d'après les informations de longueur de l'en-tête IPv6. La valeur du champ Longueur UDP est égale à la longueur de charge utile dans l'en-tête IPv6, moins la longueur de tout en-tête d'extension présent entre l'en-tête IPv6 et l'en-tête UDP.

Réservé (bits 3 à 7)

10.3 Champs non compressés

10.3.1 Champs IPv6 non compressés

Ce schéma permet que l'en-tête IPv6 soit compressé à différents degrés. Donc, au lieu de l'en-tête IPv6 entier (standard) seuls les champs non compressés doivent être envoyés. L'en-tête suivant (comme spécifié par le champ Prochain en-tête dans l'en-tête IPv6 original) suit immédiatement les champs IPv6 non compressés.

L'adressage IPv6 non compressé est décrit par un type Dispatch contenant une valeur de répartiteur IPv6 suivie par l'en-tête IPv6 non compressé. Ce type Dispatch peut être précédé par des en-têtes LoWPAN supplémentaires.

Le champ IPv6 non compressé qui DOIT être toujours présent est la limite de bonds (8 bits). Ce champ DOIT toujours suivre les champs de codage (par exemple, "codage HC1" comme montré dans la Figure 9) incluant peut-être d'autres futurs champs de codage). Les autres champs non compressés DOIVENT suivre la limite de bonds selon ce qui est impliqué par le champ "Codage HC1" exactement dans le même ordre que montré ci-dessus (paragraphe 10.1) : préfixe d'adresse de source (64 bits) et/ou identifiant d'interface (64 bits) préfixe d'adresse de destination (64 bits) et/ou identifiant d'interface (64 bits) classe de trafic (8 bits) étiquette de flux (20 bits) et prochain en-tête (8 bits). Le prochain en-tête réel (par exemple, UDP, TCP, ICMP, etc.) suit les champs non compressés.

10.3.2 Champs UDP non compressés et partiellement compressés

Ce schéma permet que l'en-tête UDP soit compressé à différents degrés. Donc, au lieu de l'en-tête UDP entier (standard) seuls les champs non compressés ou partiellement compressés doivent être envoyés.

Les champs non compressés ou partiellement compressés dans l'en-tête UDP DOIVENT toujours suivre l'en-tête IPv6 et tous ses champs en ligne associés. Tous les champs d'en-tête UDP en ligne présents DOIVENT apparaître dans le même ordre que les champs correspondants dans un en-tête UDP normal [RFC0768], par exemple, accès de source, accès de destination, longueur, et somme de contrôle. Si les accès de source ou de destination sont en notation "accès court" (comme indiqué dans l'en-tête UDP compressé) alors au lieu de prendre 16 bits, les numéros d'accès en ligne prennent 4 bits.

11. Livraison de trame dans un maillage de couche de liaison

Bien que les réseaux 802.15.4 soient supposés utiliser couramment un acheminement maillé, la spécification IEEE 802.15.4-2003 [IEEE802.15.4] ne définit pas une telle capacité. Dans ce cas, les appareils à fonction pleine (FDD, *Full Function Device*) utilisent un protocole d'acheminement ad hoc ou de maillage pour remplir leurs tableaux d'acheminement (qui sort du domaine d'application de ce document). Dans de tels scénarios de maillage, deux appareils n'exigent pas une accessibilité directe pour communiquer. Avec ces appareils, l'expéditeur est appelé "l'origine", et le receveur est appelé la "destination finale". Un appareil d'origine peut utiliser d'autres appareils intermédiaires comme transmetteurs vers la destination finale. Afin de réaliser une telle livraison de trames en utilisant l'envoi individuel, il est nécessaire d'inclure les adresses de couche de liaison de l'origine et de la destination finale, en plus de la source et destination bond par bond.

Cette section définit comment effectuer la livraison des trames de couche 2 dans un maillage, connaissant l'adresse de couche de liaison d'une "destination finale" cible.

La livraison de maillage est activée en incluant un en-tête Adressage maillé avant tous les autres en-têtes de l'encapsulation LoWPAN (Section 5) un en-tête non fragmenté et fragmenté, un en-tête IPv6 complet, ou un en-tête IPv6, compressés selon la Section 10 ou tous autres définis ailleurs.

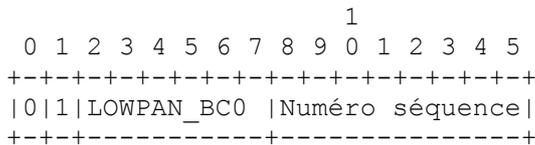
Si un nœud souhaite utiliser un transmetteur de maillage par défaut pour livrer un paquet (c'est-à-dire, parce que il n'a pas d'accessibilité directe à la destination) il DOIT inclure un en-tête Adressage maillé avec l'adresse de couche de liaison de l'origine réglée à son adresse propre, et l'adresse de couche de liaison de la destination finale réglée à la destination ultime du paquet. Il règle l'adresse de source dans l'en-tête 802.15.4 à sa propre adresse de couche de liaison, et met l'adresse de couche de liaison du transmetteur dans le champ Adresse de destination de l'en-tête 802.15.4. Finalement, il transmet le paquet.

De même, si un nœud reçoit une trame avec un en-tête Adressage maillé, il doit chercher le champ "Destination finale" de l'en-tête Adressage maillé pour déterminer la destination réelle. Si le nœud est lui-même la destination finale, il consomme le paquet comme pour une livraison normale. Si il n'est pas la destination finale, l'appareil réduit alors le champ "Bonds restants", et si le résultat est zéro, élimine le paquet. Autrement, le nœud consulte son tableau d'acheminement de couche de liaison, détermine quel devrait être le prochain bond vers la destination finale, et met cette adresse dans le champ Adresse de destination de l'en-tête 802.15.4. Finalement, le nœud change l'adresse de source dans l'en-tête 802.15.4 à sa propre adresse de couche de liaison et transmet le paquet.

Alors qu'un nœud doit participer à un protocole d'acheminement maillé pour être un transmetteur, une telle exigence n'existe pas pour utiliser simplement la transmission maillée. Seuls les "appareils à fonction pleines" (FFD) sont supposés participer comme routeurs dans un maillage. Les "appareils à fonctions réduites" (RFD) se limitent à la découverte des FFD et à les utiliser pour toutes leurs transmissions, d'une manière similaire à celle dont les hôtes IP utilisent normalement les routeurs par défaut pour transmettre tout leur trafic hors liaison. Pour un RFD qui utilise la livraison maillée, le "transmetteur" est toujours le FFD approprié.

11.1 Diffusion LoWPAN

Une fonction d'acheminement maillé supplémentaire est codée en utilisant un en-tête d'acheminement à la suite immédiate de l'en-tête Maillage. En particulier, un en-tête de diffusion consiste en un répartiteur LOWPAN_BC0 suivi par un champ Numéro de séquence. Le numéro de séquence est utilisé pour détecter des paquets dupliqués (et pour essayer de les supprimer).

**Figure 11 : En-tête de diffusion**

La définition des champs est la suivante :

Numéro de séquence : ce champ de 8 bits DEVRA être incrémenté par l'origine chaque fois qu'elle envoie une nouvelle diffusion maillée ou paquet en diffusion groupée. La spécification de la façon de traiter ce champ sort du domaine d'application du présent document.

Les autres implications d'une telle diffusion de couche de maillage, par exemple, si elle se transpose en un mécanisme d'arrosage contrôlé ou son rôle dans, par exemple, la découverte de la topologie, sortent du domaine d'application du présent document.

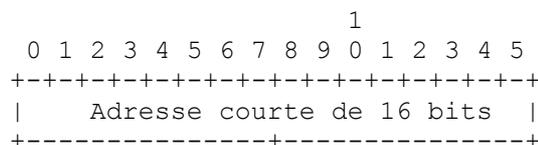
Les capacités supplémentaires d'acheminement maillé, comme de spécifier le protocole d'acheminement maillé, l'acheminement de source, et ainsi de suite, peuvent être exprimées en définissant des en-têtes d'acheminement supplémentaires qui précèdent l'en-tête de fragmentation ou d'adressage dans la pile d'en-têtes. La pleine spécification de telles capacités d'acheminement maillé sort du domaine d'application du présent document.

12. Considérations relatives à l'IANA

Le présent document crée deux nouveaux registres de l'IANA, exposés ci-dessous. Les futures allocations dans ces registres seront coordonnées via l'IANA sous la politique de "spécification exigée" [RFC2434]. Il est attendu de cette politique qu'elle permette que d'autres organisations (non IETF) obtiennent plus facilement des allocations.

Le présent document crée un nouveau registre IANA pour le champ Type de répartiteur montré dans les définitions d'en-tête de la Section 5. Le présent document définit les valeurs IPv6, compression d'en-tête LOWPAN_HC1, diffusion BC0 et deux schémas d'échappement (NALP pour indiquer "pas une trame LOWPAN" et ESC pour permettre des octets de répartiteur supplémentaires). Le présent document définit ce champ comme de 8 bits. Les valeurs 00xxxxxx sont réservées et non utilisées, permettent un total de 192 valeurs différentes, qui devraient être plus que suffisantes. Si des formats de compression d'en-tête en plus de HC1 sont définis ou si des formats en plus de TCP, ICMP HC2 sont définis, il est prévu qu'ils utiliseront les valeurs réservées de répartiteur suivant LOWPAN_HC1. Si des formats supplémentaires de livraison maillée sont définis, ils utiliseront les valeurs réservées qui suivent LOWPAN_BC0.

Le présent document crée un nouveau registre IANA pour les champs d'adresse courte de 16 bits comme utilisés dans les paquets 6LoWPAN.

**Figure 12**

Ce registre DOIT inclure les adresses 0xffff (l'adresse de diffusion de 16 bits acceptée par tous les appareils qui écoutent actuellement sur le canal) et 0xffffe comme défini dans [IEEE802.15.4]. De plus, dans les réseaux 6LoWPAN, les adresses courtes de 16 bits DOIVENT suivre ce format (se référant aux champs de bits dans l'ordre de 0 à 7) où "x" est une notation générique pour une valeur de bit non spécifiée :

Gamme 1, 0xxxxxxxxxxxxxxxx : le premier bit (bit 0) DEVRA être zéro si l'adresse de 16 bits est d'envoi individuel. Cela laisse 15 bits pour l'adresse réelle.

Gamme 2, 100xxxxxxxxxxxxxxxx : les bits 0, 1, et 2 DEVRONT suivre ce schéma si l'adresse de 16 bits est de diffusion groupée (voir la Section 9). Cela laisse 13 bits pour l'adresse de diffusion groupée réelle.

Gamme 3, 101xxxxxxxxxxxx : ce schéma pour les bits 0, 1, et 2 est réservé. Toute allocation future devra suivre la politique mentionnée ci-dessus.

Gamme 4, 110xxxxxxxxxxxx : ce schéma pour les bits 0, 1, et 2 est réservé. Toute allocation future devra suivre la politique mentionnée ci-dessus.

Gamme 5, 111xxxxxxxxxxxx : ce schéma pour les bits 0, 1, et 2 est réservé. Toute allocation future devra suivre la politique mentionnée ci-dessus.

13. Considérations sur la sécurité

La méthode de déduction des identifiants d'interface des adresses MAC EUI-64 est destinée à préserver l'unicité mondiale chaque fois que possible. Cependant, il n'y a pas de protection contre la duplication par accident ou malveillance.

La découverte de voisin dans les liaisons IEEE 802.15.4 peut être susceptible des menaces détaillées dans la [RFC3756]. L'acheminement maillé est supposé être courant dans les réseaux IEEE 802.15.4. Cela implique des menaces supplémentaires dues à l'acheminement ad hoc selon [KW03]. La norme IEEE 802.15.4 fournit des capacités de sécurité à la couche de liaison. Les utilisateurs sont invités à utiliser ces dispositions si cela leur est possible en pratique. Le faire atténuera les menaces mentionnées ci-dessus.

Une portion notable des appareils IEEE 802.15.4 sont supposés toujours communiquer au sein de leur PAN (c'est-à-dire, au sein de leur liaison, en termes IPv6). En réponse aux considérations de coût et de consommation d'énergie, et en restant dans le modèle IEEE 802.15.4 des "appareils à fonctions réduites" (RFD) ces appareils vont normalement mettre en œuvre l'ensemble minimum de caractéristiques nécessaires. En conséquence, la sécurité de ces appareils peut s'appuyer assez fortement sur les mécanismes définis à la couche de liaison par IEEE 802.15.4. Celle-ci ne définit cependant que les modes de la norme de chiffrement avancé (AES) pour l'authentification ou le chiffrement des trames IEEE 802.15.4, et en particulier ne spécifie pas de gestion de clés (en principe en mode groupe). Les autres problèmes à considérer dans les déploiements réels se rapportent à la sécurisation de la configuration et de la gestion. Bien qu'un tableau complet sorte du domaine d'application du présent document, il est impératif que les réseaux IEEE 802.15.4 soient déployés en prenant ces aspects en compte. Bien sûr, il est aussi attendu de certains appareils IEEE 802.15.4 (ceux qu'on appelle des "appareils à fonctions complètes", ou "FFD") qu'ils mettent en œuvre des fonctions de coordination ou d'intégration. Ils peuvent communiquer régulièrement avec des homologues IPv6 hors liaison (en plus des échanges en liaison plus courants). Ces appareils IPv6 sont supposés sécuriser leurs communications de bout en bout avec les mécanismes usuels (par exemple, IPsec, TLS, etc).

14. Remerciements

Merci aux auteurs des RFC 2464 et RFC 2734, car des parties de ce document sont structurées d'après elles. Merci aussi à Geoff Mulligan pour les utiles discussions qui ont aidé à donner forme à ce document. Les suggestions de Erik Nordmark ont été capitales pour la section sur la compression d'en-tête. Merci aussi à Shoichi Sakane, Samita Chakrabarti, Vipul Gupta, Carsten Bormann, Ki-Hyung Kim, Mario Mao, Phil Levis, Magnus Westerlund, et Jari Arkko.

15. Références

15.1 Références normatives

[IEEE802.15.4] IEEE Computer Society, "IEEE Std. 802.15.4-2003", octobre 2003.

[RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. (MàJ par [RFC8174](#))

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

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

[5095](#), [6564](#) ; D.S. ; Remplacée par [RFC8200](#), STD 86)

- [RFC2464] M. Crawford, "Transmission de [paquets IPv6 sur réseaux Ethernet](#)", décembre 1998. (P.S. ; MàJ par [RFC8064](#))
- [RFC4291] R. Hinden, S. Deering, "[Architecture d'adressage IP version 6](#)", février 2006. (MàJ par [5952](#) et [6052](#), [8064](#)) (D.S.)
- [RFC4861] T. Narten et autres, "[Découverte du voisin pour IP version 6 \(IPv6\)](#)", septembre 2007. (Remplace [RFC2461](#)) (D.S. ; MàJ par [RFC8028](#), [RFC8319](#), [RFC8425](#))
- [RFC4862] S. Thomson et autres, "[Auto configuration d'adresse IPv6 sans état](#)", septembre 2007. (Remplace [RFC2462](#)) (D.S.)

15.2 Références pour information

- [EUI64] "Guidelines for 64-bit global identifier (EUI-64) registration authority", IEEE <http://standards.ieee.org/regauth/oui/tutorials/EUI64.html>.
- [KW03] Chris Karlof et David Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures", Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols vol 1, issues 2-3, septembre 2003.
- [RFC0768] J. Postel, "Protocole de [datagramme d'utilisateur](#) (UDP)", (STD 6), 28 août 1980.
- [RFC3756] P. Nikander, éd., "[Modèles de confiance et menaces](#) pour la découverte de voisin IPv6 (ND)", mai 2004. (Information)
- [RFC3819] P. Karn et autres, "Conseils aux concepteurs de sous-réseaux Internet", juillet 2004. ([BCP0089](#))

Appendice A. Solutions de remplacement pour la livraison de trames dans un maillage

Avant de fixer le mécanisme finalement adopté pour la livraison dans un maillage (Section 11) plusieurs solutions de remplacement ont été considérées. En plus des adresses de couche de liaison bond par bond de source et de destination, la livraison d'un paquet dans un maillage LoWPAN exige les adresses de l'origine et de la destination de bout en bout. Cela pourrait être exprimé en adresses de couche 2 ou de couche 3 (c'est-à-dire, IP). Dans ce dernier cas, il ne serait pas besoin de fournir de prise en charge d'en-tête supplémentaire dans ce document (c'est-à-dire, au sein de l'en-tête LoWPAN lui-même). L'adresse de destination de couche de liaison pointerait sur l'adresse de destination du prochain bond tandis que l'en-tête IP de l'adresse de destination pointerait sur l'adresse (IP) de la destination finale (éventuellement à plusieurs bonds de la source) et de même pour les adresses de source. Donc, lors de la transmission des données, les adresses de source et destination d'un seul bond changeraient à chaque bond (pointant toujours, respectivement, sur le nœud qui fait la transmission et sur le "meilleur" prochain bond de couche de liaison) tandis que les adresses IP de source et destination resteraient inchangées. On remarquera que si un paquet IP est fragmenté, les fragments individuels peuvent arriver déclassés à tout nœud. Si le fragment initial (qui contient l'en-tête IP) est retardé pour une raison quelconque, un nœud qui reçoit un fragment suivant manquera des informations nécessaires. Il serait forcé d'attendre de recevoir l'en-tête IP (dans le premier fragment) avant d'être capable de transmettre le fragment plus loin. Cela impose des exigences supplémentaires de mémoire tampon aux nœuds intermédiaires. De plus, une telle spécification ne fonctionnerait que pour un seul type de charge utile LoWPAN : IPv6. En général, elle devrait être adaptée pour chaque autre charge utile, et exigerait que la charge utile fournisse ses propres informations d'adressage de bout en bout.

Par ailleurs, l'approche finalement retenue (Section 11) crée un maillage à la couche LoWPAN (en dessous de la couche 3). En conséquence, l'adresse de couche de liaison de l'origine et de la destination finale sont incluses dans l'en-tête LoWPAN. Cela permet la livraison maillée pour tout protocole ou application mis en couches sur la couche d'adaptation LoWPAN (Section 5). Pour IPv6 tel que pris en charge dans ce document, un autre avantage d'exprimer l'origine et la destination finale comme des adresses de couche 2 est que les adresses IPv6 peuvent être compressées selon la compression d'en-tête spécifiée à la Section 10. De plus, le nombre d'octets nécessaire pour tenir les tableaux d'acheminement est réduit à cause de la plus petite taille des adresses 802.15.4 (64 bits ou 16 bits) par rapport aux adresses IPv6 (128 bits). Un inconvénient est

que les applications par dessus IP n'adressent pas les paquets aux adresses de destination de couche de liaison, mais aux adresses de destination IP (couche 3). Donc, avec une adresse IP, il est nécessaire de résoudre l'adresse de couche de liaison correspondante. En conséquence, une spécification d'acheminement maillé doit préciser les implications de découverte de voisin, bien que dans certains cas particuliers, il soit possible de déduire une adresse d'un appareil à la couche 2 de son adresse à la couche 3 (et vice versa). Une telle spécification sort du domaine d'application de ce document.

Adresse des auteurs

Gabriel Montenegro
Microsoft Corporation
mél : gabriel.montenegro@microsoft.com

Nandakishore Kushalnagar
Intel Corp
mél : nandakishore.kushalnagar@intel.com

Jonathan W. Hui
Arch Rock Corp
mél : jhui@archrock.com

David E. Culler
Arch Rock Corp
mél : dculler@archrock.com

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2007)

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations contenues sont fournis sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY, le IETF TRUST et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations encloses ne viole aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à <http://www.ietf.org/ipr>.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

Remerciement

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