

Groupe de travail Réseau

Request for Comments : 5121

Catégorie : Sur la voie de la normalisation

B. Patil, Nokia Siemens Networks

F. Xia, Huawei USA

B. Sarikaya, Huawei USA

JH. Choi, Samsung AIT

S. Madanapalli, Ordyn Technologies

février 2008

Traduction Claude Brière de L'Isle

Transmission de IPv6 via la sous couche de convergence IPv6 sur réseaux IEEE 802.16

Statut du présent mémoire

Le présent document spécifie un protocole de l'Internet sur la voie de la 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.

Résumé

La norme IEEE 802.16 est une spécification d'interface radio pour des systèmes fixes et mobiles d'accès large bande sans fil. Les sous couches de convergence spécifiques de service auxquelles s'interfacent les protocoles de couche supérieure font partie du contrôle d'accès au support (MAC, *Medium Access Control*) de IEEE 802.16. La sous couche de convergence (CS, *convergence sublayer*) de paquet est utilisée pour le transport de tous les protocoles fondés sur le paquet tels que le protocole Internet (IP, *Internet Protocol*) et la méthode d'accès par LAN/MAN CSMA/CD (Ethernet) de IEEE 802.3. Les paquets IPv6 peuvent être envoyés et reçus via la partie spécifique IP de la CS de paquet. Le présent document spécifie l'adressage et le fonctionnement de IPv6 sur la partie spécifique d'IP de la CS de paquet pour les hôtes desservis par un réseau qui utilise l'interface radio de la norme IEEE 802.16. Il recommande l'allocation d'un ou plusieurs préfixes uniques à chaque hôte et permet à l'hôte d'utiliser plusieurs identifiants au sein de ce préfixe, incluant la prise en charge d'identifiants d'interface générés au hasard.

Table des matières

1. Introduction.....	2
2. Terminologie.....	2
3. Conventions utilisées dans ce document.....	2
4. Prise en charge de la sous couche de convergence IEEE 802.16 pour IPv6.....	2
4.1 Encapsulation IPv6 sur la CS IP de MAC.....	4
5. Architecture générique de réseau utilisant l'interface radio 802.16.....	5
6. Liaison IPv6.....	6
6.1 Liaison IPv6 dans 802.16.....	6
6.2 Établissement de liaison IPv6 dans 802.16.....	6
6.3 Unité maximum de transmission dans 802.16.....	7
7. Allocation de préfixe IPv6.....	7
8. Découverte de routeur.....	7
8.1 Sollicitation de routeur.....	7
8.2 Annonce de routeur.....	7
8.3 Durée de vie de routeur et annonces périodiques de routeur.....	7
9. Adressage IPv6 pour les hôtes.....	8
9.1 Identifiant d'interface.....	8
9.2 Détection d'adresse dupliquée.....	8
9.3 Auto configuration d'adresse sans état.....	8
9.4 Auto configuration d'adresse à états pleins.....	8
10. Découverte d'écouter de diffusion groupée.....	8
11. Considérations sur la sécurité.....	8
12. Remerciements.....	9
13. Références.....	9
13.1 Références normatives.....	9
13.2 Références pour information.....	9
Appendice A. Architecture de réseau WiMAX et prise en charge de IPv6.....	10

Appendice B. Liaison IPv6 dans WiMAX.....	11
Appendice C. Établissement de liaison IPv6 dans WiMAX.....	11
Appendice D. Unité maximum de transmission dans WiMAX.....	12
Adresse des auteurs.....	12
Déclaration complète de droits de reproduction.....	12

1. Introduction

La norme IEEE 802.16 est une interface radio pour les systèmes fixes et mobiles d'accès sans fil large bande. La norme IEEE 802.16 [802.16] spécifie l'interface radio, incluant la spécification de la couche de contrôle d'accès au support (MAC, *Medium Access Control*) et de plusieurs couches physiques (PHY). Elle peut être déployée dans le spectre sous licence aussi bien que non licencié. Alors que PHY et MAC sont spécifiées dans IEEE 802.16, les détails du fonctionnement de IPv4 et IPv6 sur l'interface radio n'y sont pas inclus. Le présent document spécifie le fonctionnement de IPv6 sur l'interface radio de IEEE 802.16.

Les paquets IPv6 peuvent être portés sur l'interface radio spécifiée dans la norme IEEE 802.16 via :

1. la partie spécifique de IP de la CS de paquet ou
2. la partie spécifique de [802.3] de la CS de paquet.

La portée de cette spécification est limitée seulement au fonctionnement de IPv6 sur la CS IP.

La spécification IEEE 802.16 inclut les détails des couches PHY et MAC. Les sous couches de convergence font partie du MAC. La sous couche de convergence de paquet inclut la partie spécifique de IP qui est utilisée par la couche IPv6.

La station mobile (MS) / hôte est rattachée à un routeur d'accès (AR, *access router*) via une station de base (BS, *base station*). L'hôte et la BS sont connectés via l'interface radio IEEE 802.16 à la couche de liaison et à la couche physique. La liaison IPv6 provenant de la MS se termine à un routeur d'accès qui peut faire partie de la BS ou d'une entité au delà de la BS. La station de base est une entité de couche 2 (du point de vue de la liaison IPv6 entre la MS et du routeur d'accès) et relaye les paquets IPv6 entre l'AR et l'hôte via une connexion en point à point sur l'interface radio.

2. Terminologie

La terminologie dans ce document se fonde sur les définitions dans la [RFC5154] "Position du problème et buts de IP sur 802.16".

- o CS IP : partie spécifique de IP de la sous couche de convergence de paquet. Les termes CS IPv6 et CS IP sont utilisés de façon interchangeable.
- o Station d'abonné (SS), station mobile (MS), nœud mobile (MN) : les termes de station d'abonné, station mobile, et nœud mobile sont utilisés de façon interchangeable dans ce document et signifient la même chose, c'est-à-dire, un hôte IP.

3. Conventions utilisées dans ce document

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].

4. Prise en charge de la sous couche de convergence IEEE 802.16 pour IPv6

Le MAC IEEE 802.16 spécifie deux sous couches de convergence spécifiques de service principales :

1. la sous couche de convergence ATM,
2. la sous couche de convergence de paquet.

La CS de paquet est utilisée pour le transport de protocoles fondés sur le paquet, qui incluent :

1. la norme IEEE 802.3 (Ethernet)

2. le protocole Internet (IPv4 et IPv6).

La CS spécifique de service réside au dessus de la sous couche de partie commune de MAC (CPS, *MAC Common Part Sublayer*) comme le montre la Figure 1. La CS spécifique de service est chargé de :

- o accepter les paquets (unités de données de protocole (PDU, *Protocol Data Units*)) provenant de la couche supérieure,
- o effectuer le classement des paquets/PDU sur la base d'un ensemble de critères définis spécifiques du service,
- o livrer la PDU de CS au flux de service et à la connexion de transport appropriés, et
- o recevoir les PDU de l'entité homologue.

La suppression de l'en-tête de charge utile (PHS, *Payload Header Suppression*) est aussi une fonction facultative de la CS.

La figure ci-dessous montre le concept de CS spécifique de service en relation avec le MAC :

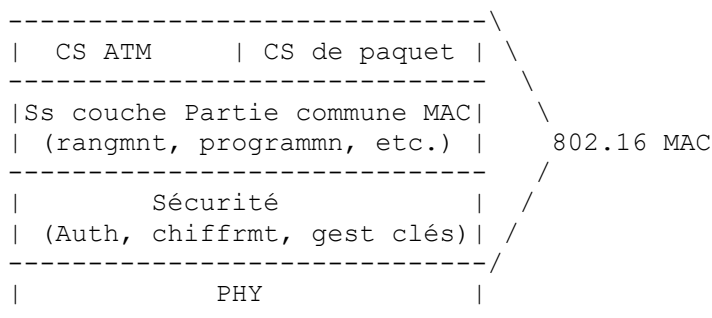
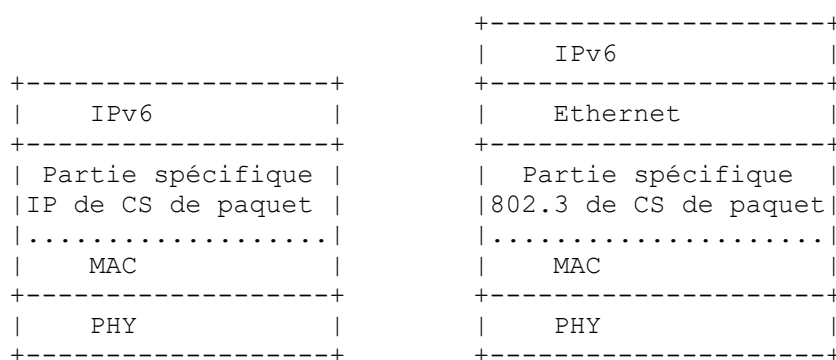


Figure 1 : MAC IEEE 802.16

Les critères de classement pour chaque protocole spécifique de couche supérieure, c'est-à-dire, Ethernet et IP, sont définis dans la spécification IEEE 802.16, qui permet que les paquets provenant de la couche supérieure soient traités par la partie spécifique de service appropriée de la CS de paquet. IPv6 peut être transporté directement sur la partie spécifique de IP de la CS de paquet (CS IP). Les paquets IPv4 sont aussi transportés sur la partie spécifique de IP de la CS de paquet. Les critères de classements utilisés par la CS IP permettent la différenciation des paquets IPv4 et IPv6 et leur transposition en les connexions spécifiques du transport sur l'interface radio.

La figure ci-dessous montre les options pour le transport IPv6 sur la CS de paquet de IEEE 802.16 :



(1) IPv6 sur partie spécifique IP de CS de paquet (2) IPv6 sur partie spécifique 802.3/Ethernet de CS de paquet

Figure 2 : IPv6 sur parties spécifiques de IP et 802.3 de CS de paquet

La figure ci-dessus montre qu'il y a plusieurs méthodes pour transmettre IPv6 sur une interface radio 802.16, mais que le domaine d'application du présent document est limitée au fonctionnement de IPv6 sur la seule CS IP. La transmission de IP sur Ethernet est spécifiée dans la [RFC5692]. La transmission de IPv4 sur la CS IP est spécifiée dans la [RFC5948].

On devrait noter que immédiatement après le classement (procédure d'interface radio 802.16) et l'échange des messages SBC-REQ/RSP (spécifiques de 802.16) la MS et la BS échangent leurs capacités via les messages de MAC 802.16 REG-REQ (demande d'enregistrement) et REG-RSP (réponse d'enregistrement). Ces trames de gestion négocient des paramètres comme la couche de convergence prise en charge par la MS et la BS. Par défaut, Packet, IPv4, et 802.3/Ethernet sont pris en charge. IPv6 via la CS IP n'est pris en charge par la MS et la BS que quand le bit de prise en charge d'IPv6 dans les

messages de négociation de capacités (REG-REQ et REG-RSP) impliquant une telle prise en charge est indiqué dans le paramètre "Options de classification/PHS et prise en charge de l'encapsulation de SDU (*Service Data Unit*)" (voir [802.16]). De plus, durant l'établissement de la connexion de transport des paquets IPv6, les messages demande et réponse de service dynamique (DSA, *Dynamic Service Addition*) entre la BS et la MS indiquent via le TLV CS-Specification la CS que la connexion qui va être établie devra utiliser. Quand le paquet IPv6 est précédé de l'en-tête de MAC IEEE 802.16 de 6 octets, il n'y a pas d'indication spécifique dans l'en-tête de MAC lui-même sur le type de charge utile. Le traitement du paquet est entièrement fondé sur les classificateurs. Sur la base des règles de classement, la couche MAC choisit une connexion de transport appropriée pour la transmission du paquet. Un paquet IPv6 est transporté sur une connexion de transport établie spécifiquement pour porter de tels paquets.

La transmission de IPv6 comme expliquée ci-dessus est possible via plusieurs méthodes, c'est-à-dire, via la CS IP ou via des interfaces Ethernet. Chaque hôte Internet connecté via une liaison 802.16 :

1. DOIT être capable d'envoyer et recevoir des paquets IPv6 via la CS IP quand la MS et la BS indiquent la prise en charge du protocole IPv6 sur la CS IP,
2. DOIT être capable d'envoyer et recevoir des paquets IPv6 sur la partie spécifique d'Ethernet (802.3) de la CS de paquet quand la MS et la BS indiquent la prise en charge du protocole IPv6 sur la CS Ethernet. Cependant, quand la MS et la BS indiquent la prise en charge du protocole IPv6 à la fois sur la CS IP et sur la CS Ethernet, la MS et la BS DOIVENT utiliser la CS IP pour envoyer et recevoir les paquets IPv6.

Quand la MS et la BS prennent en charge IPv6 sur la CS IP, elle DOIT être utilisée comme mode par défaut pour transporter les paquets IPv6 sur IEEE 802.16 et les recommandations du présent document qui sont suivies. L'incapacité à négocier une sous couche de convergence commune pour le transport IPv6 entre la MS et la BS va résulter en l'échec de l'établissement d'une connexion de transport et ainsi rendre l'hôte incapable d'envoyer et recevoir les paquets IPv6. Dans le cas d'un hôte qui met en œuvre plus d'une méthode de transport des paquets IPv6, le choix par défaut de la méthode à utiliser (c'est-à-dire, IPv6 sur la CS IP ou IPv6 sur 802.3) est IPv6 sur la CS IP quand la BS prend aussi en charge cette capacité. Dans tous les cas, la MS et la BS DOIVENT négocier au plus une sous couche de convergence pour le transport IPv6 sur une liaison donnée.

De plus, pour assurer l'interopérabilité entre des appareils qui prennent en charge des encapsulations différentes, il est EXIGÉ que les mises en œuvre de BS prennent en charge toutes les encapsulations sur la voie de la normalisation définies pour 802.16 par l'IETF. Au moment de la rédaction de la présente spécification, c'est la seule encapsulation ; des spécifications supplémentaires sont en préparation. Il n'est cependant pas exigé que les mises en œuvre de BS utilisent toutes les encapsulations qu'elles prennent en charge ; certains modes de fonctionnement peuvent être désactivés par configuration.

4.1 Encapsulation IPv6 sur la CS IP de MAC

La charge utile IPv6, quand elle est portée sur la partie spécifique d'IP de la CS de paquet, est encapsulée par l'en-tête de MAC générique de 6 octets IEEE 802.16. Le format du paquet IPv6 encapsulé par l'en-tête de MAC générique est montré dans la figure ci-dessous. Le format de l'en-tête de MAC de 6 octets est décrit dans la spécification [802.16]. Le contrôle de redondance cyclique (CRC, *cyclic redundancy check*) est facultatif. On devrait noter que l'adresse MAC réelle n'est pas incluse dans l'en-tête de MAC.

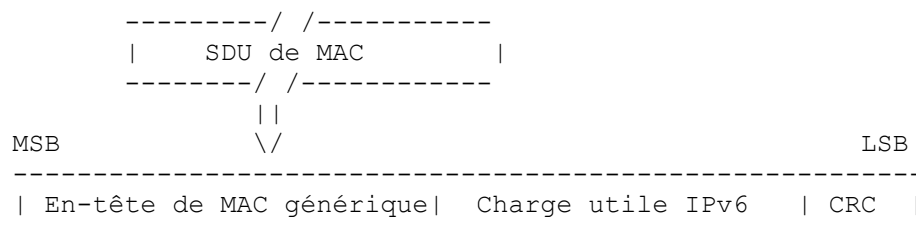


Figure 3 : Encapsulation IPv6

Pour la transmission de paquets IPv6 via la CS IP sur IEEE 802.16, la couche IPv6 s'interface directement avec le MAC 802.16. La couche IPv6 livre le paquet IPv6 à la CS de paquet du MAC IEEE 802.16. La CS de paquet définit un ensemble de classeurs qui sont utilisés pour déterminer comment traiter le paquet. Les classeurs IP qui sont utilisés au MAC opèrent sur les champs de l'en-tête IP et le protocole de transport, et ils incluent la classe de trafic IP, le champ Prochain en-tête, les adresses masquées de source et destination IP, et les gammes d'accès de source et destination de protocole. Le prochain en-tête dans ce cas se réfère au dernier en-tête de la chaîne d'en-têtes IP. En analysant ces classeurs, le MAC transpose un

paquet de couche supérieure en un flux de service et connexion de transport spécifiques à utiliser. Le MAC encapsule le paquet IPv6 dans l'en-tête de MAC (MAC SDU) de 6 octets et le transmet. La figure ci-dessous montre l'opération sur la liaison vers l'aval, c'est-à-dire, la transmission de la BS à l'hôte. L'inverse est applicable pour la transmission en amont.

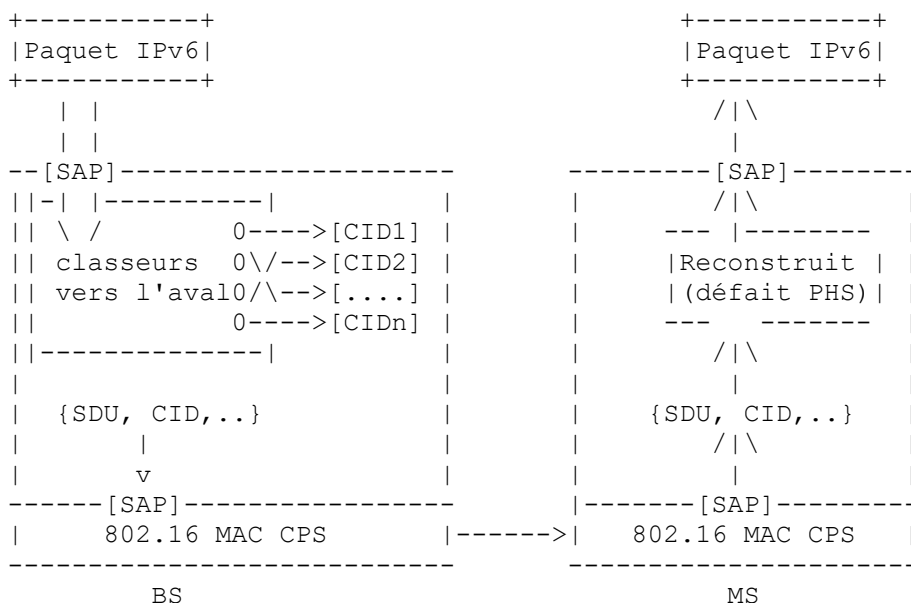


Figure 4 : Transmission de paquet IPv6 : vers l'aval

5. Architecture générique de réseau utilisant l'interface radio 802.16

Dans un réseau qui utilise l'interface radio 802.16, l'hôte/MS est rattaché à un routeur d'accès (AR, *access router*) IPv6 dans le réseau. La BS est seulement une entité de couche 2. L'AR peut être une partie intégrante de la BS, ou il pourrait être une entité au delà de la BS au sein du réseau d'accès. Un AR peut être rattaché à plusieurs BS dans un réseau. Les paquets IPv6 entre la MS et la BS sont portés sur une connexion de transport en point à point qui est identifiée par un identifiant de connexion (CID, *Connection Identifier*) univoque. La connexion de transport est une liaison de couche MAC entre la MS et la BS. Les figures ci-dessous décrivent les architectures de réseau possibles et sont de nature générique. Des architectures plus ésotériques sont possibles mais ne sont pas considérées dans le présent document.

Option A :

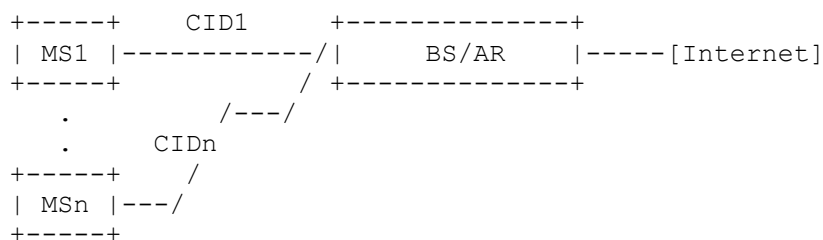


Figure 5 : AR IPv6 comme partie intégrante de la BS

Option B :

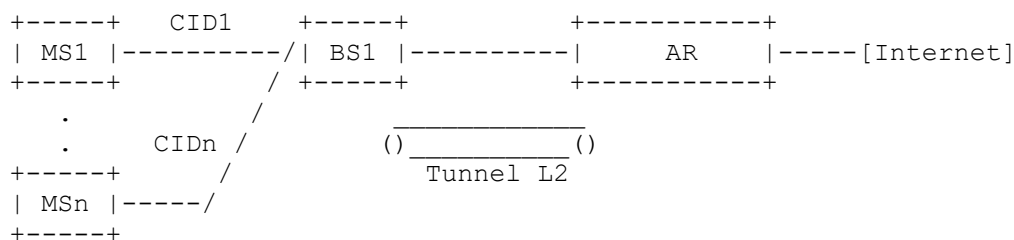


Figure 6 : AR IPv6 séparé de la BS

Les modèles de réseau ci-dessus servent d'exemples et illustrent la liaison point à point entre la MS et l'AR.

6. Liaison IPv6

La [RFC4861] "Découverte de voisin pour IP version 6 (IPv6)" définit une liaison comme une facilité ou support de communication sur lequel les nœuds peuvent communiquer à la couche de liaison, c'est-à-dire, la couche immédiatement en-dessous de IP. Une liaison est liée par des routeurs qui décrémentent le champ Limite de bonds dans l'en-tête IPv6. Quand une MS se déplace au sein d'une liaison, elle peut conserver l'usage de ses adresses IP. C'est une définition de couche 3 et on notera que cette définition n'est pas identique à la définition du terme "liaison de couche 2" dans les normes IEEE 802.

6.1 Liaison IPv6 dans 802.16

Dans 802.16, la connexion de transport entre une MS et une BS est utilisée pour transporter des données d'utilisateur, c'est-à-dire, des paquets IPv6 dans ce cas. Une connexion de transport est représentée par un CID, et plusieurs connexions de transport peuvent exister entre une MS et une BS.

Quand un AR et une BS sont co-localisés, la collection de connexions de transport à une MS est définie comme une seule liaison. Quand un AR et une BS sont séparés, il est recommandé qu'un tunnel soit établi entre l'AR et une BS dont la granularité n'est pas supérieure à "par MS" ou "par flux de service" (une MS peut avoir plusieurs flux de service qui sont identifiés par un identifiant de flux de service). Ensuite, le ou les tunnels pour une MS, combinés avec les connexions de transport de la MS, forment une seule liaison point à point.

La collection des flux de service (tunnels) à une MS est définie comme une seule liaison. Chaque liaison qui utilise le même protocole de couche supérieure a seulement une MS et un AR. Chaque MS appartient à une liaison différente. Un préfixe différent devrait être alloué à chaque liaison unique. Cette liaison est pleinement cohérente avec une liaison IP standard, sans exception, et se conforme à la définition d'une liaison point à point dans la découverte de voisin pour IPv6 [RFC4861]. Donc, le modèle de liaison point à point pour le fonctionnement IPv6 sur la partie spécifique de IP de la CS de paquet dans 802.16 DEVRAIT être utilisé. Un ou des préfixes IPv6 uniques par liaison (MS/hôte) DOIVENT être alloués.

6.2 Établissement de liaison IPv6 dans 802.16

Afin de permettre l'envoi et la réception des paquets IPv6 entre la MS et l'AR, la liaison entre la MS et l'AR via la BS doit être établie. Ce paragraphe illustre la procédure d'établissement de liaison.

La MS passe par la procédure d'entrée de réseau spécifiée par 802.16. La description générale de la procédure d'entrée de réseau est que :

1. La MS effectue le classement initial avec la BS. Le classement est un processus par lequel une MS devient synchronisée avec la BS. La MS est synchronisée avec la BS à l'achèvement réussi du classement et est prête à établir une connexion.
2. La MS et la BS échangent les capacités de base nécessaires pour une communication effective durant l'initialisation en utilisant les messages SBC-REQ/RSP (spécifiques de 802.16).
3. La MS passe à la phase d'authentification. L'authentification est fondée sur la version 2 de gestion de clé de confidentialité (PKMv2, *Privacy Key Management version 2*) définie dans IEEE 802.16.
4. Une fois l'authentification réussie, la MS effectue l'enregistrement 802.16 avec le réseau.
5. La MS et la BS effectuent l'échange de capacités selon les procédures de 802.16. La prise en charge de protocole est indiquée dans cet échange. Le paramètre Capacité de CS indique quelles options de classification/PHS et encapsulation de SDU la MS supporte. Par défaut, Packet, IPv4, et 802.3/Ethernet devront être pris en charge ; donc, l'absence de ce paramètre dans REG-REQ (message 802.16) signifie que les options nommées sont prises en charge par la MS/SS. La prise en charge de IPv6 sur la partie spécifique de IP de la CS de paquet est indiquée par le bit n° 2 du paramètre Capacité de CS (voir [802.16]).
6. La MS DOIT demander l'établissement d'un flux de service pour les paquets IPv6 sur CS IP si la MS et la BS ont

confirmé la capacité de prise en charge de IPv6 sur CS IP. Le flux de service PEUT aussi être déclenché par le réseau par suite de pré-provisionnement. Le flux de service établit une liaison entre la MS et l'AR sur lequel les paquets IPv6 peuvent être envoyés et reçus.

7. L'AR et la MS DEVRAIENT envoyer des annonces et sollicitations de routeur comme spécifié dans la découverte de voisins [RFC4861].

Le flux ci-dessus ne montre pas les messages 802.16 réels qui sont utilisés pour le classement, l'échange de capacités, ou l'établissement de flux de service. Les détails sont dans [802.16].

6.3 Unité maximum de transmission dans 802.16

La valeur de MTU pour les paquets IPv6 sur une liaison 802.16 est configurable. La MTU par défaut pour les paquets IPv6 sur une liaison 802.16 DEVRAIT être 1500 octets.

La PDU de MAC 802.16 est composée d'un en-tête de 6 octets suivi d'une charge utile facultative et d'un CRC facultatif couvrant l'en-tête et la charge utile. La longueur de la PDU est indiquée par le paramètre Longueur dans l'en-tête de MAC générique. Le paramètre Longueur fait 11 bits. Donc, la taille totale de la PDU de MAC est de 2048 octets. La taille de charge utile IPv6 peut varier. Dans certains scénarios de déploiement, la valeur de MTU peut être supérieure à celle par défaut. La découverte de voisin pour IPv6 [RFC4861] définit une option de MTU qu'un AR DOIT annoncer, via une annonce de routeur (RA) si une valeur différente de 1500 est utilisée. La MN traite cette option comme défini dans la [RFC4861]. Les nœuds qui mettent en œuvre la découverte de la MTU de chemin [RFC1981] PEUVENT utiliser le mécanisme pour déterminer la MTU pour les paquets IPv6.

7. Allocation de préfixe IPv6

La MS et l'AR sont connectés via une connexion point à point à la couche IPv6. Donc, chaque MS peut être considérée comme étant sur un sous réseau séparé. Un type d'appareil d'abonné qui dessert plusieurs hôtes IPv6 peut être le point d'extrémité de la connexion. Donc, un ou plusieurs préfixes /64 DEVRAIENT être alloués à une liaison. Les préfixes sont annoncés avec le bit en-liaison (bit L) établi comme spécifié dans la [RFC4861]. La taille et le nombre des préfixes sont une question de configuration. Aussi, la délégation de préfixe fondée sur le protocole de configuration dynamique d'hôte (DHCP, *Dynamic Host Configuration Protocol*) ou l'authentification, autorisation, et comptabilité (AAA) PEUT être utilisée pour fournir un ou plusieurs préfixes à la MS pour un AR connecté sur 802.16. Les autres propriétés des préfixes sont aussi traitées via la configuration.

8. Découverte de routeur

8.1 Sollicitation de routeur

À l'achèvement de l'établissement de la liaison IPv6, la MS peut envoyer un message de sollicitation d'annonce de routeur à l'AR pour acquérir les informations nécessaires conformément à la spécification de découverte de voisins pour IPv6 [RFC4861]. Une MS qui est rattachée au réseau peut aussi envoyer des sollicitations de routeur à tout moment. La détection de mouvement à la couche IP d'une MS est dans de nombreux cas fondée sur la réception périodique d'annonces de routeur. Une MS peut aussi détecter des changements dans son rattachement via des déclencheurs de liaison ou d'autres moyens. La MS peut agir sur de tels déclencheurs en envoyant des sollicitations de routeur. La sollicitation de routeur est envoyée sur la liaison IPv6 établie précédemment. La MS envoie des sollicitations de routeur à l'adresse de diffusion groupée Tous-les-routeurs. Elle est portée à l'AR sur la liaison point à point via la BS. La MS n'a pas besoin de connaître l'adresse de liaison locale de l'AR pour envoyer à tout moment une sollicitation de routeur. L'utilisation des annonces de routeur comme moyen de détection de mouvement n'est pas recommandée pour les MN connectées via des liaisons 802.16 car la fréquence des annonces de routeur périodiques devrait être élevée.

8.2 Annonce de routeur

L'AR DEVRAIT envoyer un certain nombre (configurable) d'annonces de routeur à la MS aussitôt que la liaison IPv6 est établie. L'AR envoie des annonces de routeur non sollicitées périodiquement conformément à la [RFC4861]. L'intervalle entre les annonces périodiques de routeur est cependant supérieur à celui de la spécification de la découverte de voisin pour IPv6, et est discuté au paragraphe suivant.

8.3 Durée de vie de routeur et annonces périodiques de routeur

La durée de vie de routeur DEVRAIT être réglée à une valeur élevée, de préférence en heures. Le présent document se substitue à la spécification de la valeur de la durée de vie de routeur dans la [RFC4861] "Découverte de voisin pour IP version 6 (IPv6)". Le paramètre AdvDefaultLifetime (*durée de vie d'annonce par défaut*) dans l'annonce de routeur DOIT être zéro ou entre MaxRtrAdvInterval (*intervalle maximal de retransmission d'annonce*) et 43200 secondes. La valeur par défaut est $2 * \text{MaxRtrAdvInterval}$.

Les hôtes 802.16 ont la capacité de passer à un mode dormant, auquel cas, la liaison radio entre la BS et la MS est supprimée. La radiolocalisation est nécessaire dans le cas où le réseau a besoin de livrer des paquets à la MS. Pour éviter d'éveiller un mobile qui est en mode dormant et de consommer des ressources sur l'interface radio, l'intervalle entre les annonces de routeur périodiques DEVRAIT être réglé à une valeur assez élevée. La valeur de MaxRtrAdvInterval spécifiée dans le présent document se substitue à la recommandation de la [RFC4861] "Découverte de voisin pour IP version 6 (IPv6)". MaxRtrAdvInterval DOIT être de pas moins de 4 secondes et de pas plus de 21 600 secondes. La valeur par défaut pour MaxRtrAdvInterval est 10 800 secondes.

9. Adressage IPv6 pour les hôtes

Le schéma d'adressage pour les hôtes IPv6 dans les réseaux 802.16 suit la recommandation de l'IETF pour les hôtes spécifiée dans "Exigences pour les nœuds IPv6" [RFC4294]. La [RFC4294] spécifie un ensemble de RFC qui sont applicables à l'adressage, et la même chose est applicable aux hôtes qui utilisent 802.16 comme couche de liaison pour transporter des paquets IPv6.

9.1 Identifiant d'interface

La MS a une adresse MAC de 48 bits unique au monde comme spécifié dans [802.16]. Cette adresse MAC DOIT être utilisée pour générer l'identifiant d'interface de format EUI-64 modifié comme spécifié dans la [RFC4291] "Architecture d'adressage IP version 6". L'identifiant d'interface EUI-64 modifié est utilisé dans l'auto configuration d'adresse sans état. Comme dans d'autres liaisons qui prennent en charge IPv6, les identifiants d'interface fondés sur EUI-64 ne sont pas obligatoires et d'autres mécanismes, comme les identifiants d'interface aléatoires, "Extensions de confidentialité pour l'auto configuration d'adresse sans état dans IPv6" [RFC4941], PEUVENT aussi être utilisés.

9.2 Détection d'adresse dupliquée

La détection d'adresse dupliquée (DAD, *Duplicate Address Detection*) DEVRAIT être effectuée conformément à la [RFC4861] "Découverte de voisin pour IP version 6", et à la [RFC4862] "Auto configuration d'adresse sans état pour IPv6". La liaison IPv6 sur 802.16 est spécifiée dans le présent document comme une liaison en point à point. Sur la base de ce critère, il peut être redondant d'effectuer la DAD sur une adresse mondiale en envoi individuel qui est configurée en utilisant l'EUI-64 ou générée selon la [RFC4941] pour l'interface au titre du protocole d'auto configuration d'adresse IPv6 sans état [RFC4862] tant que les deux conditions suivantes sont satisfaites :

1. les préfixes annoncés par les messages d'annonce de routeur du routeur d'accès terminant la liaison 802.16 IPv6 sont uniques pour cette liaison,
2. le routeur d'accès terminant la liaison 802.16 IPv6 n'auto-configue aucune adresse mondiale IPv6 en envoi individuel à partir du préfixe qu'il annonce.

9.3 Auto configuration d'adresse sans état

Quand l'autoconfiguration d'adresse sans état est effectuée, elle DOIT être effectuée comme spécifié dans les [RFC4861] et [RFC4862].

9.4 Auto configuration d'adresse à états pleins

Quand l'autoconfiguration d'adresse à états pleins est effectuée, elle DOIT l'être comme spécifié dans les [RFC4861] et [RFC3315].

10. Découverte d'écouter de diffusion groupée

La [RFC3810] "Découverte d'écouter de diffusion groupée version 2 (MLDv2) pour IPv6" DEVRAIT être prise en charge comme spécifié par les hôtes et routeurs rattachés les uns aux autres via une liaison 802.16. Le routeur d'accès qui a des hôtes rattachés via une liaison point à point sur un réseau 802.16 NE DEVRAIT PAS envoyer d'interrogations périodiques si l'hôte est en mode repos/dormant. L'AR peut obtenir des informations sur l'état d'un hôte de la part du contrôleur de localisation dans le réseau.

11. Considérations sur la sécurité

Le présent document n'introduit aucune nouvelle vulnérabilité dans les spécifications ou opérations IPv6. La sécurité de l'interface radio 802.16 fait l'objet de [802.16]. On devrait noter que 802.16 fournit la capacité de chiffrer le trafic porté sur les connexions de transport. Une clé de chiffrement de trafic (TEK, *Traffic Encryption Key*) est générée par la MS et la BS à l'achèvement réussi de l'authentification et est utilisée pour sécuriser le trafic sur l'interface radio. Une MS peut encore utiliser les mécanismes de sécurité de IPv6 même en présence de la sécurité sur la liaison 802.16. De plus, les questions de sécurité dans l'architecture de réseau s'étendant au delà des stations de base 802.16 font l'objet des documents qui définissent ces architectures, comme l'architecture de réseau WiMAX [WiMAXArch] dans les paragraphes 7.2 et 7.3 de l'étape 2, partie 2.

12. Remerciements

Les auteurs tiennent à remercier de leurs contributions les présidents du groupe de travail 16NG Soohong Daniel Park et Gabriel Montenegro ainsi que Jari Arkko, Jonne Soininen, Max Riegel, Prakash Iyer, DJ Johnston, Dave Thaler, Bruno Sousa, Alexandru Petrescu, Margaret Wasserman, et Pekka Savola pour leur relecture et commentaires. La révision et les commentaires de Phil Barber ont aussi aidé à améliorer la qualité du document.

13. Références

13.1 Références normatives

- [802.16] "IEEE Std 802.16e: IEEE Standard for Local and metropolitan area networks, Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands", octobre 2005, <<http://standards.ieee.org/getieee802/download/802.16e-2005.pdf>>.
- [RFC1981] J. McCann, S. Deering, J. Mogul, "Découverte de la [MTU de chemin pour IP version 6](#)", août 1996. (D.S. ; Remplacé par [RFC8201], STD87)
- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. DOI 10.17487/RFC2119, (MàJ par [RFC8174](#))
- [RFC3810] R. Vida, L. Costa, éditeurs, "Découverte d'[écouteur de diffusion groupée version 2](#) (MLDv2) pour IPv6", juin 2004.
- [RFC4291] R. Hinden, S. Deering, "[Architecture d'adressage IP version 6](#)", février 2006, DOI 10.17487/RFC4291. (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](#), [RFC9131](#))
- [RFC4862] S. Thomson et autres, "[Auto configuration d'adresse IPv6 sans état](#)", septembre 2007. (Remplace [RFC2462](#)) (D.S.)

13.2 Références pour information

- [802.3] IEEE Std 802.3-2005, "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks--Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications",

décembre 2005, <<http://standards.ieee.org/getieee802/802.3.html>>.

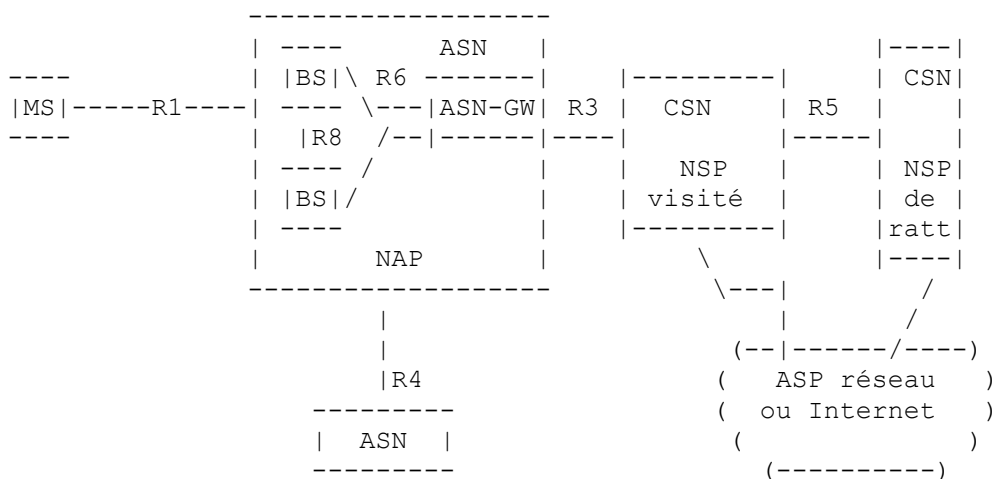
- [RFC3315] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins et M. Carney, "Protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)", juillet 2003. (MàJ par [RFC6422](#) et [RFC6644](#), [RFC7227](#) ; rendue obsolète par [RFC8415](#))
- [RFC4294] J. Loughney, éd., "Exigences pour les nœuds IPv6", avril 2006. (MàJ par [RFC5095](#)) (*Information*)
- [RFC4941] T. Narten et autres, "Extensions de confidentialité pour l'auto configuration d'adresse sans état dans IPv6", septembre 2007, DOI 10.17487/RFC4941. (*D.S. ; remplace [RFC3041](#) ; remplacée par [RFC8981](#)*)
- [RFC5154] J. Jee et autres, "Position du problème et buts de IP sur réseau IEEE 802.16", avril 2008. (*Information*)
- [[RFC5692](#)] H. Jeon, S. Jeong, M. Riegel, "Transmission de IP sur Ethernet dans les réseaux IEEE 802.16", octobre 2009. (*P. S.*)
- [RFC5948] S. Madanapalli, S. Park, S. Chakrabarti, G. Montenegro, "Transmission de paquets IPv4 sur la sous couche de convergence IP de IEEE 802.16", août 2010. (*P.S.*)
- [WMF] "WiMAX Forum", <<http://www.wimaxforum.org>>.
- [WiMAXArch] "WiMAX End-to-End Network Systems Architecture", septembre 2007.

Appendice A. Architecture de réseau WiMAX et prise en charge de IPv6

Le Forum WiMAX (Worldwide Interoperability for Microwave Access) [WMF] a défini une architecture de réseau dans laquelle l'interface radio se fonde sur la norme IEEE 802.16. L'adressage et le fonctionnement de IPv6 décrits dans le présent document sont applicables aussi au réseau WiMAX.

WiMAX est un exemple d'architecture de réseau qui utilise la spécification 802.16 pour l'interface radio. Les réseaux WiMAX sont aussi en cours de déploiement dans diverses parties du monde, et le fonctionnement de IPv6 dans un réseau WiMAX est expliqué dans cet appendice.

L'architecture de réseau WiMAX consiste en le réseau de service d'accès (ASN, *Access Service Network*) et le réseau de service de connexité (CSN, *Connectivity Service Network*). L'ASN est le réseau d'accès qui inclut la BS et l'AR en plus des autres fonctions comme AAA, agent étranger IP mobile, contrôleur de localisation, registre de localisation, etc. L'ASN est défini comme un ensemble complet de fonctions de réseau nécessaires pour fournir l'accès radio à un abonné WiMAX. L'ASN est le réseau d'accès auquel la MS se rattache. Le routeur d'accès IPv6 est une entité au sein de l'ASN. Le terme d'ASN est spécifique de l'architecture de réseau WiMAX. Le CSN est l'entité qui fournit la connexité à l'Internet et inclut des fonctions comme celle d'agent de rattachement IP mobile et d'AAA. La figure ci-dessous montre le modèle de référence WiMAX :



Trois types différents de réalisation d'ASN appelées des profils sont définis par l'architecture. Les ASN de type de profil A et C incluent des BS et des passerelles d'ASN (ASN-GW) qui sont connectées les unes aux autres via une interface R6. Un ASN de profil B est celui dans lequel la fonction de BS et les autres fonctions d'ASN sont fusionnées. Une ASN-GW est spécifiquement définie dans un profil B d'ASN. L'absence de l'interface R6 est aussi caractéristique du profil B. La MS à la couche IPv6 est associée à l'AR dans l'ASN. L'AR peut être une fonction de la ASN-GW dans le cas des profils A et C et est une fonction dans l'ASN dans le cas du profil B. Quand la BS et l'AR sont des entités séparées et reliées via l'interface R6, les paquets IPv6 entre la BS et l'AR sont portés sur un tunnel d'encapsulation d'acheminement générique (GRE, *Generic Routing Encapsulation*). La granularité du tunnel GRE devrait être par MS ou sur la base d'un flux par service (une MS peut avoir plusieurs flux de service, chacun identifié de façon univoque par un identifiant de flux de service). La pile de protocoles dans WiMAX pour IPv6 est montrée ci-dessous :

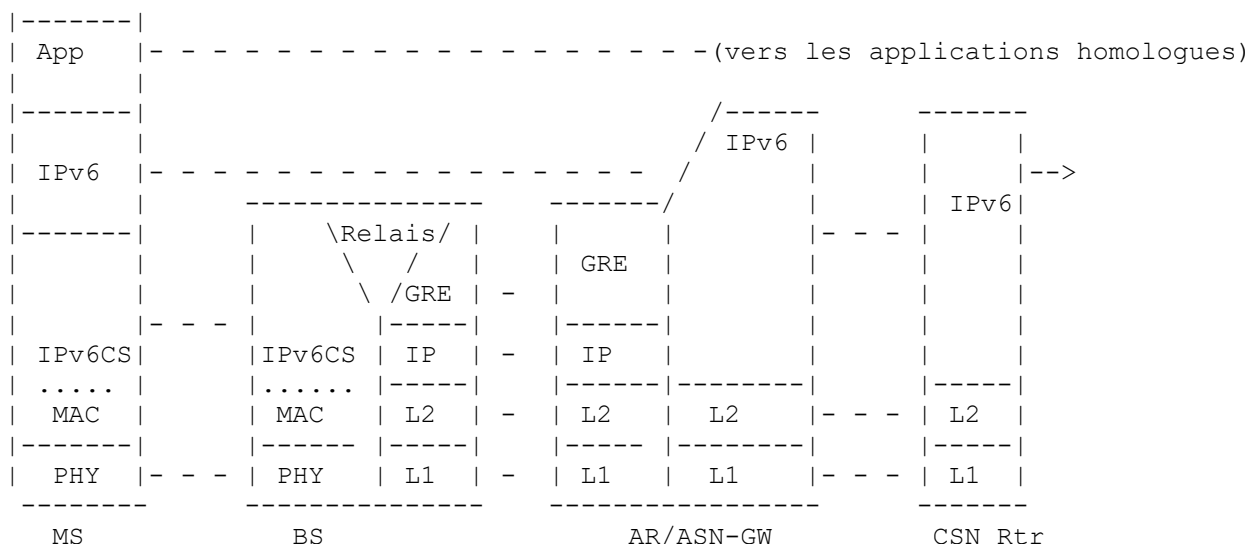


Figure 8 : Pile de protocoles WiMAX

Comme on peut le voir de la description de la pile de protocoles, les points d'extrémité IPv6 sont constitués dans la MS et l'AR. La BS fournit la connectivité de couche inférieure pour la liaison IPv6.

Appendice B. Liaison IPv6 dans WiMAX

WiMAX est un exemple de réseau fondé sur l'interface radio de IEEE 802.16. Cette section décrit la liaison IPv6 dans le contexte d'un réseau WiMAX. La MS et l'AR sont connectés via une combinaison de :

1. la connexion de transport identifiée par un identifiant de connexion (CID) sur l'interface radio, c'est-à-dire, la MS et la BS, et
2. un tunnel GRE entre la BS et l'AR qui transporte les paquets IPv6.

Du point de vue de IPv6, la MS et l'AR sont connectés par une liaison point à point. La combinaison de connexion de transport sur l'interface radio et le tunnel GRE entre la BS et l'AR crée un tunnel (point à point) à la couche en-dessous de IPv6.

La collection de flux de service (tunnels) à une MS est définie comme une seule liaison. Chaque liaison a seulement une MS et un AR. Chaque MS appartient à une liaison différente. Deux MS n'appartiennent pas à la même liaison. Un préfixe différent devrait être alloué à chaque liaison unique. Cette liaison est pleinement cohérente avec une liaison IP standard, sans exception, et se conforme à la définition d'une liaison point à point de la [RFC4861].

Appendice C. Établissement de liaison IPv6 dans WiMAX

La station mobile effectue l'entrée initiale de réseau comme spécifié dans 802.16. À l'achèvement réussi de la procédure d'entrée de réseau, la passerelle/AR d'ASN déclenche l'établissement d'un flux de service initial (ISF, *initial service flow*) pour IPv6 vers la MS. L'ISF est un tunnel GRE entre la ASN-GW/AR et la BS. La BS à son tour demande à la MS d'établir

une connexion de transport sur l'interface radio. Le résultat est une connexion de transport sur l'interface radio pour porter les paquets IPv6 et un tunnel GRE entre la BS et l'AR pour relayer les paquets IPv6. À l'achèvement réussi de l'établissement de l'ISF, les paquets IPv6 peuvent être envoyés et reçus entre la MS et l'AR. L'ISF permet à la MS de communiquer avec l'AR pour les procédures de configuration d'hôte. Après l'établissement de l'ISF, l'AR peut envoyer une annonce de routeur à la MS. Une MS peut établir plusieurs flux de service avec des caractéristiques différentes de qualité de service. L'ISF peut être considéré comme le principal flux de service. La ASN-GW/AR traite chaque ISF, ainsi que les autres flux de service pour la même MS, comme une liaison unique gérée comme une interface (virtuelle).

Appendice D. Unité maximum de transmission dans WiMAX

Le Forum WiMAX [WMF] a spécifié la taille maximum de SDU comme 1522 octets. Donc, la MTU de chemin IPv6 peut être de 1500 octets. Cependant, à cause des frais généraux du tunnel GRE utilisé pour transporter les paquets IPv6 entre la BS et l'AR et l'en-tête de MAC de 6 octets sur l'interface radio, utiliser une valeur de 1500 résulterait en la fragmentation de paquets. Il est recommandé que la MTU pour IPv6 soit réglée à 1400 octets dans les réseaux WiMAX, et que cette valeur (différente de celle par défaut) soit communiquée à la MS. Noter que la spécification de 1522 octets est une spécification du forum WiMAX et non la taille de la SDU qui peut être transmise sur 802.16, qui a une limite supérieure.

Adresse des auteurs

Basavaraj Patil
Nokia Siemens Networks
6000 Connection Drive
Irving, TX 75039
USA
mél : basavaraj.patil@nsn.com

Frank Xia
Huawei USA
1700 Alma Dr. Suite 500
Plano, TX 75075
USA
mél : xiayangsong@huawei.com

Behcet Sarikaya
Huawei USA
1700 Alma Dr. Suite 500
Plano, TX 75075
USA
mél : sarikaya@ieee.org

JinHyeock Choi
Samsung AIT
Networking Technology Lab
P.O.Box 111
Suwon, Korea 440-600
mél : jinchoc@samsung.com

Syam Madanapalli
Ordyn Technologies
1st Floor, Creator Building, ITPL.
Off Airport Road
Bangalore, India 560066
mél : smadanapalli@gmail.com

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2008). Tous droits réservés.

Le présent document et ses traductions peuvent être copiés et fournis aux tiers, et les travaux dérivés qui les commentent ou les expliquent ou aident à leur mise en œuvre peuvent être préparés, copiés, publiés et distribués, en tout ou partie, sans restriction d'aucune sorte, pourvu que la déclaration de droits de reproduction ci-dessus et le présent paragraphe soient inclus dans toutes copies et travaux dérivés. Cependant, le présent document lui-même ne peut être modifié d'aucune façon, en particulier en retirant la notice de droits de reproduction ou les références à la Internet Society ou aux autres organisations Internet, excepté autant qu'il est nécessaire pour les besoins du développement des normes Internet, auquel cas les procédures de droits de reproduction définies dans les procédures des normes Internet doivent être suivies, ou pour les besoins de la traduction dans d'autres langues que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Internet Society ou ses successeurs ou ayant 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 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.