Équipe d'ingénierie de l'Internet (IETF)
Request for Comments : 5692
Catégorie : Sur la voie de la normalisation
ISSN: 2070-1721
Traduction Claude Brière de L'Isle

H. Jeon, ETRI
S. Jeong, ETRI
M. Riegel, NSN
octobre 2009

Transmission de IP sur Ethernet sur réseaux IEEE 802.16

Résumé
Le présent document décrit la transmission de IPv4 ainsi que IPv6 sur Ethernet, dans un réseau d'accès déployant la technologie de transmission radio cellulaire IEEE 802.16. L'Ethernet par dessus IEEE 802.16 est réalisé en pontant les connexions que fournit IEEE 802.16 entre une station de base et ses stations d'abonné associées. Du fait des contraintes de ressource des systèmes de transmission radio et des limitations de la fonction de contrôle de l'accès au support (MAC, *Media Access Control*) de IEEE 802.16 pour la réalisation d'un Ethernet, la transmission de IP sur Ethernet en IEEE 802.16 bénéficiera considérablement de l'ajout de fonctions de prise en charge spécifiques de IP dans l'Ethernet sur IEEE 802.16 tout en maintenant une pleine compatibilité avec le comportement standard de IP sur Ethernet.

Table des matières

1. Introduction

IEEE 802.16 [802.16] spécifie un système d'accès sans fil large bande de fixe à mobile.

La norme IEEE 802.16 définit une sous couche de convergence (CS, *Convergence Sublayer*) de paquet pour l'interface avec des protocoles spécifiques fondés sur le paquet ainsi qu'une sous couche de convergence générique de paquet (GPCS, *Generic Packet Convergence Sublayer*) pour fournir une interface de couche supérieure, indépendante du protocole. Le présent document décrit la transmission de IPv4 et IPv6 sur Ethernet via la partie spécifique d'Ethernet de la CS de paquet ainsi que de la GPCS dans le réseau d'accès fondé sur IEEE 802.16.

Ethernet a été à l'origine architecturé et conçu pour un support partagé tandis que IEEE 802.16 utilise une architecture de point à multipoint comme les autres systèmes de transmission radio cellulaires. Donc, Ethernet par dessus IEEE 802.16 est réalisé en établissant un pont entre les connexions radio IEEE 802.16 qui connectent une station de base (BS, *Base Station*) et ses stations d'abonné (SS, *Subscriber Station*) associées.

Avec les contraintes de ressource des systèmes de transmission radio et les particularités de IEEE 802.16 pour la réalisation d'Ethernet, il y a du sens à ajouter des fonctions de soutien spécifiques de IP dans la couche Ethernet au-dessus de IEEE 802.16 tout en maintenant une pleine compatibilité avec le comportement standard de IP sur Ethernet.

2. 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].

3. Terminologie

La terminologie du présent document est fondée sur les définitions de la [RFC5154] "Position du problème et buts de IP sur réseau IEEE 802.16".

4. Modèle de liaison IEEE 802.16

4.1 Interface radio en mode connexion

Le MAC IEEE 802.16 établit les connexions entre une BS et ses SS associées pour le transfert des données d'utilisateur sur

le réseau. Chacune de ces connexions réalise un flux de service individuel, qui est identifié par un numéro d'identifiant de connexion (CID, *Connection Identifier*) de 16 bits et a un profil de qualité de service (QS) défini.

Plusieurs connexions peuvent être établies entre une BS et une SS, chacune avec sa classe de QS et direction particulières. Bien que la BS et toutes les SS ne soient pas associées à des adresses de MAC de 48 bits uniques, les paquets qui vont sur le réseau sont seulement identifiés dans l'en-tête de MAC IEEE 802.16 par le numéro de CID de la connexion particulière. Les connexions sont établies par des messages de MAC entre la BS et la SS durant l'entrée de réseau ou aussi plus tard à la demande.

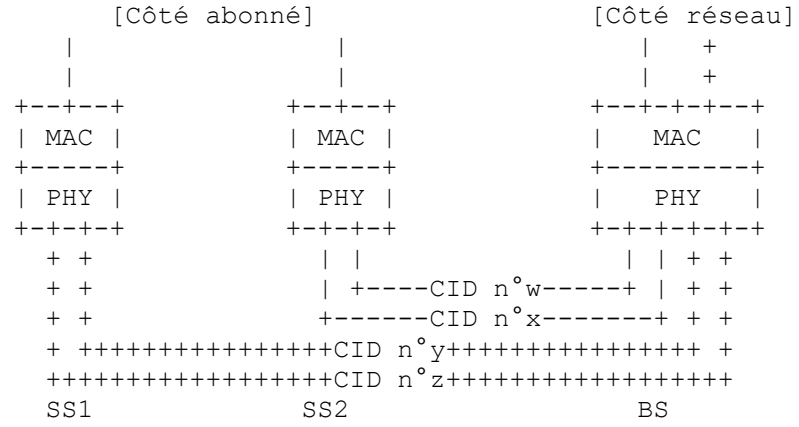

Figure 1 : Modèle de base de liaison IEEE 802.16

4.2 Adressage MAC dans IEEE 802.16

Chaque SS a une adresse de MAC unique de 48 bits ; l'adresse de MAC de 48 bits est utilisée durant le processus initial de repérage pour l'identification de la SS et peut être vérifiée par la phase suivante d'authentification de gestion de clé de confidentialité (PKM, *Privacy Key Management*). En dehors de la réussite de l'authentification, la BS établit et maintient la liste des SS rattachées fondée sur leur adresse de MAC, pour les seuls besoins de la gestion de MAC.

Alors que les adresses de MAC sont allouées à toutes les BS ainsi qu'aux SS, la transmission de paquets sur le réseau est seulement fondée sur la valeur de CID de la connexion particulière dans l'en-tête MAC IEEE 802.16. Ne pas s'appuyer sur les adresses de MAC dans la charge utile pour la réception d'une trame radio permet le transport d'adresses MAC de source et destination arbitraires dans des trames Ethernet entre une SS et sa BS. Ceci est exigé pour le pontage de trames Ethernet vers une SS rattachée à un pont connecté à un autre réseau.

Du fait de la gestion des allocations de flux de service et des valeurs de CID associées aux SS individuelles, la BS est capable de regrouper toutes les connexions d'envoi individuel appartenant à une SS particulière en une seule liaison sur le côté réseau, comme le montre la Figure 1, afin de fournir une seule liaison de couche 2 entre la SS et sa liaison filaire associée sur le côté réseau.

4.3 Prise en charge de la diffusion et de la diffusion groupée unidirectionnelle

La norme IEEE 802.16 actuelle [802.16] ne prend pas en charge la diffusion et la diffusion groupée bidirectionnelle native pour les paquets IP. Alors que les connexions descendantes peuvent être utilisées pour la transmission en diffusion groupée à un groupe de SS ainsi qu'en transmission en envoi individuel de la BS à une seule SS, les connexions montantes des SS à la BS fournissent seulement des capacités de transmission en envoi individuel. De plus, l'utilisation de CID en diffusion groupée pour réaliser des transmissions de diffusion groupée descendante n'est pas nécessairement préférable du fait de l'efficacité de transmission réduite des CID en diffusion groupée pour de petits groupes de diffusion groupée. L'Appendice A donne des informations supplémentaires sur les questions qui se posent avec les CID en diffusion groupée dans les systèmes IEEE 802.16.

Le service de diffusion et diffusion groupée (MBS, *Multicast and Broadcast Service*) comme spécifié dans IEEE 802.16, ne couvre pas non plus les données de diffusion ou diffusion groupée IP parce que MBS est invisible à la couche IP.

4.4 Sous couche de convergence IEEE 802.16 pour IP sur Ethernet

IEEE 802.16 fournit deux solutions pour transférer des trames Ethernet sur des connexions de MAC IEEE 802.16.
La CS de paquet est définie pour traiter les protocoles fondés sur le paquet en classant les paquets de couche supérieure selon la valeur du champ d'en-tête de paquet et en allouant les paquets au flux de service auquel ils se rapportent. La CS de paquet comprend plusieurs parties spécifiques du protocole pour permettre la transmission des différentes sortes de paquets sur IEEE 802.16. La partie spécifique de Ethernet de la CS de paquet prend en charge la transmission de Ethernet en définissant des règles de classification fondées sur les informations d'en-tête Ethernet.
La sous couche générique de convergence de paquet (GPCS, *Generic Packet Convergence Sublayer*) peut être utilisée comme solution de remplacement au transfert de trames Ethernet sur IEEE 802.16. La GPCS ne définit pas de règle de classification pour chaque sorte de charge utile mais s'appuie sur une fonction de couche supérieure qui sort du domaine d'application de IEEE 802.16 pour fournir l'allocation des paquets à des flux de service particuliers.

5. Modèle de réseau Ethernet pour IEEE 802.16

Comme dans les réseaux Ethernet filaires d'aujourd'hui, le pontage est exigé pour mettre en œuvre la connectivité entre plus de deux appareils. Dans IEEE 802.16, les connexions point à point entre les SS et la BS peuvent être pontées afin que Ethernet soit réalisé sur le réseau d'accès IEEE 802.16.

5.1 Modèle de liaison Ethernet IEEE 802.16

Pour réaliser Ethernet par dessus IEEE 802.16, toutes les connexions en point à point qui appartiennent à une SS DOIVENT être connectées à une fonction de pontage côté réseau, comme montré à la Figure 2. Ceci est équivalent à l'Ethernet commuté d'aujourd'hui avec une paire de fils torsadés ou de fibres connectant les hôtes à un pont ("commutateur").
La fonction de pontage côté réseau peut être réalisée par un seul pont centralisé côté réseau ou par plusieurs ponts interconnectés, de préférence arrangés en ordre hiérarchique. Seul le pont centralisé côté réseau permet le meilleur contrôle du comportement de diffusion et de transmission de l'Ethernet sur IEEE 802.16. L'Appendice B explique les problèmes d'une architecture de pontage réparti quand aucune hypothèses ne peut être faite sur la localisation du routeur d'accès.
La BS DOIT transmettre tous les flux de service appartenant à une SS à un accès de la fonction de pontage côté réseau. Pas plus d'une SS ne DOIT être connectée à un accès de la fonction de pontage côté réseau. La méthode de séparation pour plusieurs liaisons sur la connexion entre la BS et la fonction de pontage côté réseau sort du domaine d'application du présent document. Le transport de couche 2 ou le tunnelage de couche 3 peut être utilisé.

Si l'Ethernet sur IEEE 802.16 est étendu à plusieurs stations d'extrémité derrière la SS (c'est-à-dire, SSn°4 dans la figure ci-dessous) alors la SS DEVRAIT prendre en charge le pontage d'accès conformément à [802.1D] et son amendement [802.16k], autrement dit, pont côté abonné, entre tous ses accès côté abonné et la liaison radio IEEE 802.16.

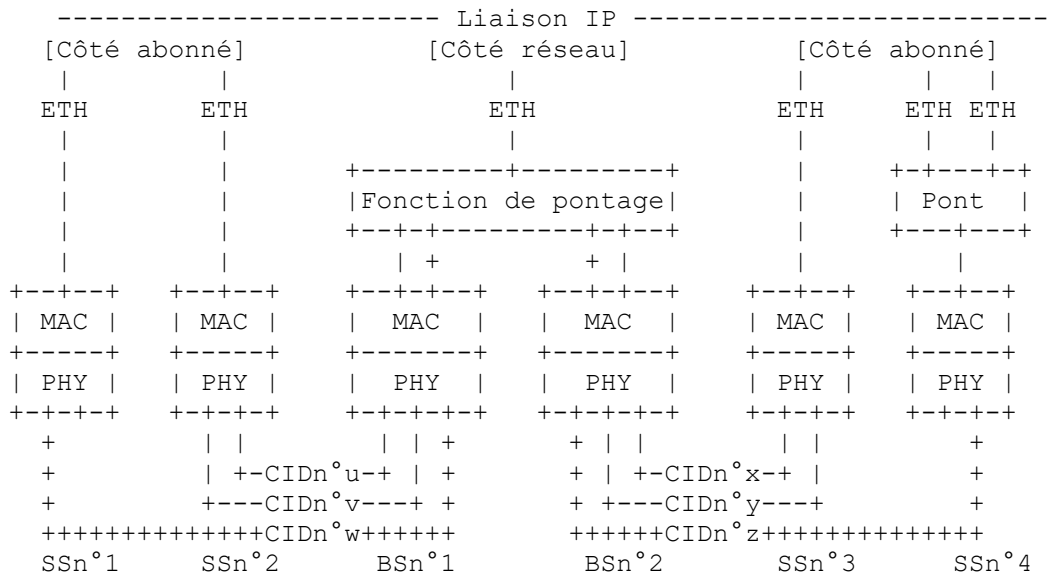

Figure 2 : Modèle de liaison Ethernet IEEE 802.16

5.2 Ethernet sans prise en charge native de diffusion et diffusion groupée

La norme IEEE 802.16 actuelle ne définit pas de diffusion et diffusion groupée de trames Ethernet. Donc, les trames Ethernet qui sont en diffusion ou en diffusion groupée DEVRAIENT être dupliquées et ensuite portées via des connexions de transport en envoi individuel sur la liaison d'accès IEEE 802.16. La fonction de pontage côté réseau effectue la duplication et la transmission pour la diffusion et diffusion groupée Ethernet sur les liaisons radio IEEE 802.16.

5.3 Fonction de pontage côté réseau

La fonction de pontage côté réseau DOIT créer un nouvel accès côté radio chaque fois qu'une nouvelle SS se rattache à une des BS du réseau, ou elle DOIT supprimer un accès côté radio quand une SS associée se détache de la BS. La méthode pour gérer l'accès sur la fonction de pontage côté réseau peut dépendre du protocole utilisé pour établir plusieurs liaisons sur la connexion entre la BS et le pont côté réseau. La méthode de gestion d'accès sort du domaine d'application de ce document.
La fonction de pontage côté réseau DOIT être fondée sur [802.1D] et son amendement [802.16k] pour interconnecter les SS rattachées et passer les trames Ethernet entre les connexions point à point associées aux SS rattachées. Cependant, pour améliorer le modèle de liaison Ethernet IEEE 802.16 en évitant l'inondation de paquets en diffusion ou diffusion groupée, des fonctions supplémentaires spécifiques de IP PEUVENT être fournies par la fonction de pontage côté réseau en plus des fonctions obligatoires, conformément au paragraphe 5.1 de [802.1D].

5.4 Segmentation d'Ethernet en VLAN

Il est possible de restreindre la taille et la couverture du domaine de diffusion en segmentant l'Ethernet sur IEEE 802.16 en VLAN et en groupant des sous ensembles d'hôtes en VLAN particuliers, chaque VLAN représentant une liaison IP. Donc, la fonction de pontage côté réseau PEUT être habilitée à prendre en charge des VLAN conformément à [802.1Q] en allouant des identifiants de VLAN et en les traitant sur les accès de ponts virtuels.
Si une SS est directement connectée à un pont côté abonné qui prend en charge les VLAN, l'accès associé à une telle SS PEUT être habilité comme accès de jonction. Sur les accès de jonction, les trames Ethernet sont transmises dans le format de trame [802.1Q].

6. Transmission de IP sur Ethernet sur une liaison IEEE 802.16

6.1 Scénario générique IP sur réseau Ethernet

Le scénario générique IP sur réseau Ethernet suppose que tous les hôtes résident sur la même liaison. Il permet aux hôtes de communiquer directement les uns avec les autres sans détours. Il peut y avoir plusieurs routeurs d'accès (AR, *Access Router*) sur la liaison, et ils peuvent résider sur le côté abonné ou sur le côté réseau, comme montré à la Figure 3.

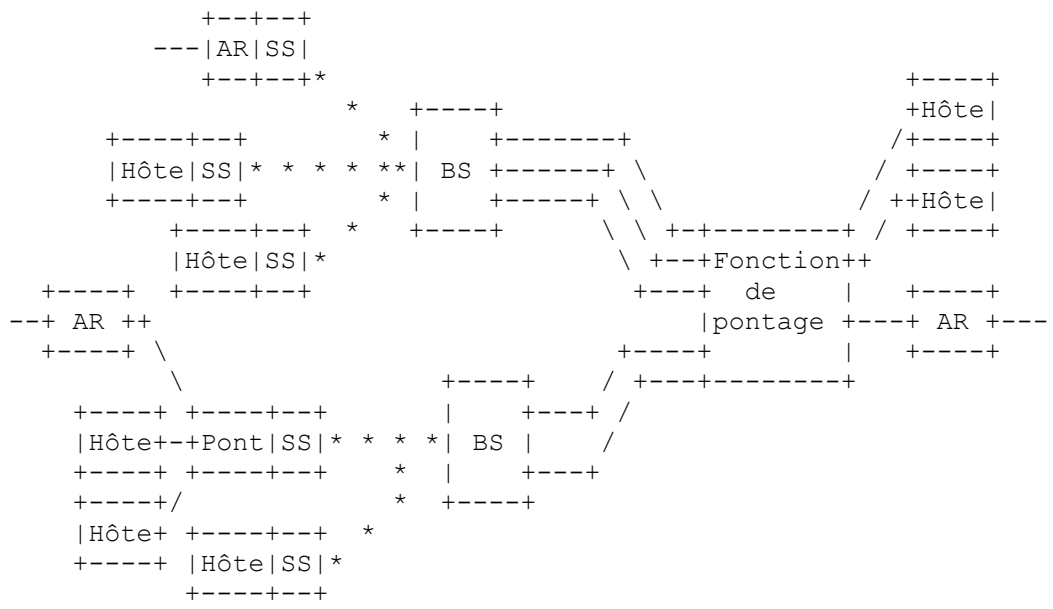

Figure 3 : Scénario générique IP sur réseau Ethernet utilisant IEEE 802.16

6.2 Transmission de IP sur Ethernet

6.2.1 Transmission de paquet IPv4 sur Ethernet

La [RFC0894] définit la transmission de paquets IPv4 sur réseaux Ethernet. Elle contient la spécification de l'encapsulation des paquets IPv4 dans des trames Ethernet ainsi que les règles de transposition des adresses IP en adresses MAC Ethernet. Les hôtes qui transmettent des paquets IPv4 sur Ethernet sur IEEE 802.16 DOIVENT suivre les opérations spécifiées dans la [RFC0894].

6.2.1.1 Configuration d'adresse

Les adresses IPv4 peuvent être configurées manuellement ou allouées dynamiquement à partir des serveurs du protocole de configuration dynamique d'hôte pour IPv4 (DHCPv4, *Dynamic Host Configuration Protocol for IPv4*) [RFC2131].

6.2.1.2 Résolution d'adresse

Le protocole de résolution d'adresse (ARP, *Address Resolution Protocol*) [RFC0826] DOIT être utilisé pour trouver l'adresse de MAC de destination Ethernet.

6.2.2 Transmission de paquet IPv6 sur Ethernet

La [RFC2464] définit la transmission des paquets IPv6 sur réseaux Ethernet, qui inclut une encapsulation de paquets IPv6 dans des trames Ethernet ; le présent document inclut des règles pour la transposition des adresses IPv6 en adresses Ethernet (c'est-à-dire, des adresses de MAC). Les hôtes qui transmettent des paquets IPv6 sur Ethernet sur IEEE 802.16 DOIVENT suivre les opérations spécifiées dans la [RFC2464].

6.2.2.1 Découverte de routeur, de préfixe et de paramètres

Les procédures de découverte de routeur, découverte de préfixe, et découverte de paramètres sont réalisées par la réception de messages d'annonce de routeur. Cependant, les messages périodiques d'annonce de routeur peuvent gaspiller les ressources radio et perturber les SS en mode dormant dans IEEE 802.16. Donc, les paramètres AdvDefaultLifetime et MaxRtrAdvInterval DEVRAIENT être remplacés par les valeurs hautes spécifiées au paragraphe 8.3 de la [RFC5121].

6.2.2.2 Configuration d'adresse

Quand l'auto configuration d'adresse à état plein est exigée, la configuration d'adresse à état plein conforme à la [RFC3315] DOIT être effectuée. Dans ce cas, un routeur d'accès prend en charge une fonction de serveur ou de relais de protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6).

Quand l'autoconfiguration d'adresse sans état est exigée, la configuration d'adresse sans état conforme aux [RFC4862] et [RFC4861] DOIT être effectuée.

6.2.2.3 Résolution d'adresse

Le protocole de découverte de voisin (NDP, *Neighbor Discovery Protocol*) [RFC4861] DOIT être utilisé pour déterminer l'adresse de MAC de destination Ethernet.

6.2.3 Unité maximum de transmission

La [RFC2460] impose 1280 octets comme taille minimum d'unité de transmission maximum (MTU, *Maximum Transmission Unit*) pour la couche de liaison et recommande au moins 1500 octets pour la transmission IPv6 sur Ethernet. La [RFC0894] spécifie aussi 1500 octets comme longueur maximum de IPv4 sur Ethernet. Donc, la MTU par défaut des paquets IPv6 et IPv4 sur une liaison Ethernet sur IEEE 802.16 DOIT être 1500 octets.

6.2.4 Allocation de préfixe

Comme Ethernet sur IEEE 802.16 peut seulement construire une partie d'un plus grand Ethernet de structure arbitraire, toute sorte d'allocation de préfixe faisable pour Ethernet est applicable aussi pour Ethernet sur IEEE 802.16. Le même préfixe IPv4 et le même ensemble de préfixes IPv6 PEUVENT être alloués à tous les hôtes rattachés à l'Ethernet sur IEEE 802.16 pour faire le meilleur usage du comportement d'Ethernet. Partager le préfixe signifie de localiser tous les hôtes sur le même sous réseau.

7. Améliorations opérationnelles pour IP sur Ethernet en IEEE 802.16

Cette section présente des améliorations opérationnelles afin d'améliorer les performance du réseau et l'efficacité des ressources radio pour la transmission de paquets IP sur les réseaux Ethernet sur IEEE 802.16.

7.1 Traitement du paquet IP en diffusion groupée et en diffusion

Tous les messages de contrôle de diffusion et diffusion groupée peuvent être traités dans la fonction de pontage côté réseau, conformément à la [RFC4541]. Les messages en diffusion à tous les accès côté radio DEVRAIENT être empêchés.

Plus d'informations sur la prévention des messages de diffusion et diffusion groupée à tous les accès côté radio sont données dans les paragraphes qui suivent.

7.1.1 Considérations de transmission en diffusion groupée

Généralement, les ponts dupliquent les paquets IP en diffusion groupée et les transmettent à tous les accès disponibles sauf l'accès entrant. Par suite, les paquets IP en diffusion groupée vont être transmis par radio -- même aux hôtes qui ne se sont du groupe de diffusion groupée correspondant. Pour permettre aux ponts de traiter plus efficacement la diffusion groupée IP, les informations d'adhésion aux groupes de diffusion groupée IP devraient être propagées entre ponts.

Dans le modèle de liaison Ethernet IEEE 802.16 du paragraphe 5.1, la fonction de pontage côté réseau peut traiter toutes les données de diffusion groupée et les messages de contrôle de diffusion groupée conformément à la [RFC4541] afin de tenir les états de membres de groupe de diffusion groupée IP et transmettre les données de diffusion groupée IP seulement aux accès convenables pour le groupe de diffusion groupée IP.

7.1.2 Considérations de transmission en diffusion

Le pont ordinaire écoule les paquets de diffusion IP à partir de tous les accès connectés sauf l'accès sur lequel le paquet a été reçu. Ce comportement n'est pas approprié pour des hôtes aux ressources rares et des hôtes en mode dormant dans un réseau sans fil tel qu'un réseau d'accès fondé sur IEEE 802.16.

La fonction de pontage côté réseau dans le modèle de liaison Ethernet IEEE 802.16 DEVRAIT écouler tous les paquets de diffusion IP sauf le trafic relatif à ARP, DHCPv4, et au protocole de gestion de groupe Internet (IGMP, *Internet Group Management Protocol*).

Les paquets de diffusion relatifs à IGMP peuvent être transmis conformément à la [RFC4541]. Les paquets de diffusion relatifs à ARP DEVRAIENT être traités comme spécifié au paragraphe 7.3.

7.2 Considérations sur DHCP

Dans le cas de IPv4 sur Ethernet, les clients DHCPv4 peuvent envoyer des messages DHCPDISCOVER et DHCPREQUEST avec le bit BROADCAST établi pour demander que le serveur DHCPv4 diffuse ses messages DHCPOFFER et DHCPACK. La fonction de pontage côté réseau DEVRAIT filtrer ces messages de diffusion DHCPOFFER et DHCPACK et transmettre seulement les messages en diffusion à l'hôte défini par l'adresse du matériel client dans l'élément d'information chaddr.

Autrement, l'option DHCP Informations d'agent de relais (option 82) [RFC3046] PEUT être utilisée pour éviter les réponses DHCPv4 en diffusion. L'option 82 consiste en deux types de sous-options : Identifiant de circuit et Identifiant distant. L'agent de relais DHCPv4 est généralement situé sur la fonction de pontage côté réseau comme agent de relais

DHCPv4 de couche 2. Le numéro d'accès de la fonction de pontage côté réseau peut être utilisé comme identifiant de circuit, et l'identifiant distant peut rester non spécifié. Noter qu'utiliser l'option 82 exige des serveurs DHCPv4 qu'ils connaissent l'option 82.

Dans le cas IPv6 sur Ethernet, les clients DHCPv6 utilisent leur adresse de liaison locale et l'adresse de diffusion groupée Tous_les_Agents_de_Relais_et_Serveurs_DHCP pour découvrir et communiquer avec les serveurs DHCPv6 ou agents de relais sur leur liaison. Donc, les paquets relatifs à DHCPv6 sont en envoi individuel ou en diffusion groupée. La fonction de pontage côté réseau DEVRAIT traiter les paquets en envoi individuel relatifs à DHCPv6 sur la base de [802.1D] et DEVRAIT transmettre les paquets en diffusion groupée relatifs à DHCPv6 comme spécifié au paragraphe 7.1.1.

7.3 Considérations de résolution d'adresse

Dans le cas de IPv4 sur Ethernet, les demandes ARP sont généralement diffusées à tous les hôtes sur la même liaison afin de résoudre une adresse de MAC Ethernet, ce qui va perturber tous les hôtes sur la même liaison. Le mandataire ARP fournit une fonction dans laquelle un appareil sur la même liaison que les hôtes répond aux demandes ARP à la place de l'hôte distant. Quand il transmet des paquets IPv4 sur la liaison Ethernet IEEE 802.16, le mécanisme de mandataire ARP est utilisé par la fonction de pontage côté réseau pour éviter de diffuser les demandes ARP sur le réseau radio.

La fonction de pontage côté réseau DEVRAIT tenir une antémémoire d'ARP assez grande pour traiter les entrées d'ARP pour toutes les SS qu'elle dessert. L'antémémoire d'ARP DEVRAIT être mise à jour par tout paquet qui inclut des demandes ARP provenant de SS de la même façon que l'appareil normal de pontage de couche 2 met à jour sa base de données de filtrage conformément à [802.1D].

À réception d'une demande ARP provenant d'une SS, la fonction de pontage côté réseau DEVRAIT renvoyer en envoi individuel une réponse ARP à la SS avec l'adresse Ethernet de l'hôte cible, pourvu que l'adresse cible corresponde à une entrée dans l'antémémoire d'ARP. Cependant, dans le cas de la réception d'une demande ARP provenant d'un hôte derrière un pont côté abonné, la fonction de pontage côté réseau DEVRAIT éliminer la demande si l'hôte cible est aussi derrière le même pont côté abonné, c'est-à-dire, sur le même accès du pont côté réseau. Autrement, la demande ARP PEUT être écoulée. La fonction de pontage côté réseau DEVRAIT éliminer en silence toute auto demande ARP reçue.

Dans le cas de IPv6 sur Ethernet, les messages de sollicitation de voisin sont en diffusion groupée à l'adresse de diffusion groupée du nœud sollicité pour la résolution d'adresse, y compris une détection d'adresse dupliquée. L'adresse de diffusion groupée du nœud sollicité facilite l'efficacité de l'interrogation des hôtes sans perturber tous les hôtes sur la même liaison. La fonction de pontage côté réseau DEVRAIT transmettre les messages de sollicitation de voisin spécifiés au paragraphe 7.1.1.

8. Recommandations d'accès public

Dans le scénario d'accès public, la communication directe entre nœuds est restreinte à cause de problèmes de sécurité et de comptabilité. La Figure 4 décrit le scénario d'accès public.

Dans ce scénario, l'AR est connecté à un pont côté réseau. L'AR PEUT effectuer un filtrage de sécurité, une régulation, et la comptabilité de tout le trafic provenant des hôtes, par exemple, comme un serveur d'acccès réseau (NAS, *Network Access Server*).

Si l'AR fonctionne comme NAS, tout le trafic provenant des SS DEVRAIT être transmis à l'AR, et non ponté à la fonction de pontage côté réseau -- même dans le cas de trafic entre des SS desservies par le même AR. Le pont DEVRAIT transmettre le trafic en amont provenant des hôtes vers l'AR mais DOIT effectuer une opération de pontage normal pour le trafic vers l'aval provenant de l'AR et il DOIT ponter les messages de découverte sûre de voisin (SEND, *SEcure Neighbor Discovery*) [RFC3971] pour permettre l'application des schémas de sécurité.

Dans le cas IPv4 sur Ethernet, la transmission de MAC forcée (MAC-FF, *MAC-Forced Forwarding*) [RFC4562] peut être utilisée pour que le réseau d'accès public s'assure que le trafic provenant de tous les hôtes est toujours dirigé sur l'AR. La MAC-FF est effectuée dans la fonction de pontage côté réseau ; donc, le pont filtre les demandes de diffusion ARP provenant de tous les hôtes et répond aux demandes ARP avec une adresse de MAC Ethernet de l'AR.

Dans le cas de IPv6 sur Ethernet, les préfixes IPv6 uniques par SS peuvent être alloués parce que le faire force le transfert de tous les paquets IPv6 provenant des SS à l'AR et donc résulte en une séparation de couche 3 entre les SS. Autrement, des

préfixes IPv6 communs peuvent être alloués à toutes les SS desservies par le même AR afin d'exploiter la prise en charge efficace de la diffusion groupée par les liaisons Ethernet du côté réseau. Dans ce cas, une option Informations de préfixe (PIO, *Prefix Information Option*) [RFC4861] portant les préfixes IPv6 communs DEVRAIT être annoncée avec le fanion en-liaison (fanion L) rétabli afin qu'il ne soit pas supposé que les adresses qui correspondent aux préfixes sont disponibles en-liaison.

L'AR devrait relayer les paquets entre les SS au sein du même AR.

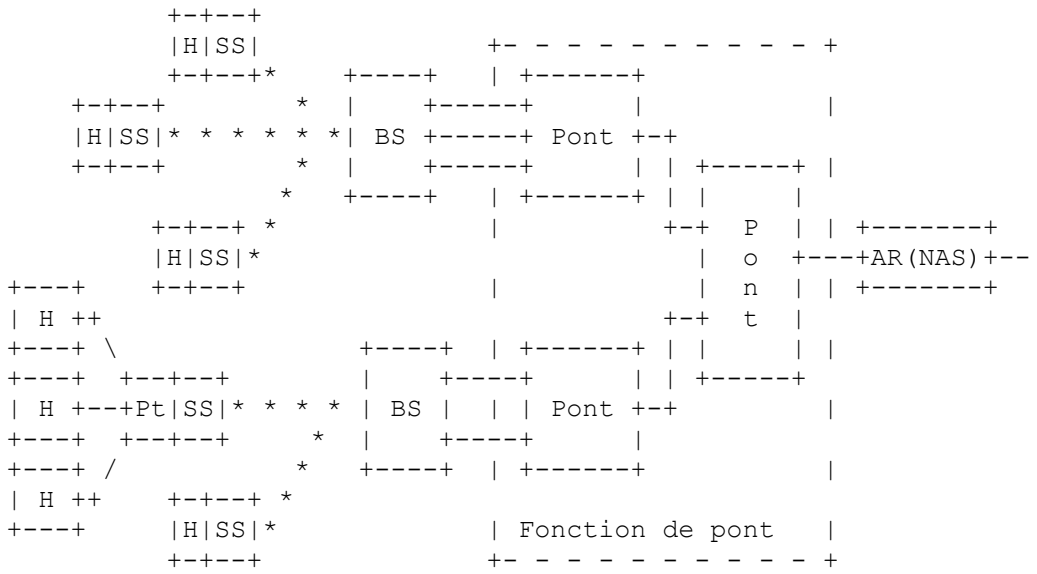

Figure 4 : Réseau d'accès public avec IEEE 802.16

9. Considérations sur la sécurité

La présente recommandation n'introduit pas de nouvelles vulnérabilités dans les spécifications ou opérations IPv4 et IPv6. La sécurité de l'interface radio IEEE 802.16 entre les SS et la BS est le sujet de [802.16], qui fournit les capacités de contrôle d'admission et de chiffrement du trafic porté sur l'interface radio. Une clé de chiffrement de trafic (TEK, *Traffic Encryption Key*) est générée par la SS et la BS à l'achèvement réussi de l'authentification mutuelle et est utilisée pour sécuriser l'interface radio.

Le modèle de liaison Ethernet IEEE 802.16 décrit au paragraphe 5.1 représente une architecture Ethernet pontée (commutée) avec des liaisons en point à point entre la SS et son accès ponté. Bien que le modèle Ethernet ponté empêche l'échange de messages entre les SS sur la même liaison sans passer à travers le pont, il est quand même vulnérable, par exemple, par une reconfiguration malveillante du tableau des adresses du pont dans le processus d'acquisition. Le présent document ne cause pas de nouveau problème de sécurité au delà de ceux déjà connus pour l'architecture d'Ethernet ponté. Par exemple, les mécanismes de sécurité de liaison conforme à [802.1AE] peuvent être utilisés par dessus la présente recommandation pour résoudre les questions de sécurité de l'Ethernet ponté.

Comme le réseau générique IP sur Ethernet utilisant IEEE 802.16 émule une liaison Ethernet standard, les mécanismes existants de sécurité IPv4 et IPv6 sur Ethernet peuvent être utilisés. Le réseau d'accès public utilisant IEEE 802.16 peut sécuriser l'isolation de chaque liaison en amont entre les hôtes et l'AR en adoptant SEND [RFC3971] pour sécuriser les processus de découverte de voisin.

10. Remerciements

Les auteurs tiennent à remercier David Johnston, Dave Thaler, Jari Arkko, et d'autres de leurs apports à ce travail.

11. Références

11.1 Références normatives

[802.16] IEEE Std 802.16-2009, "IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems", mai 2009.

[802.16k] IEEE Std 802.16k-2007, "IEEE Standard for Local and metropolitan area networks, Media Access Control (MAC) Bridges, Amendment 5: Bridging of IEEE 802.16", mars 2007.

[802.1D] IEEE Std 802.1D-2004, "IEEE Standard for Local and metropolitan area networks, Media Access Control (MAC) Bridges", juin 2004.

[802.1Q] IEEE Std 802.1Q-2005, "IEEE Standard for Local and metropolitan area networks, Virtual Bridged Local Area Networks", mai 2005.

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

[RFC0894] C. Hornig, "Norme pour la transmission des datagrammes IP sur les réseaux Ethernet", STD 41, avril 1984.

[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)

[RFC2131] R. Droms, "Protocole de configuration dynamique d'hôte", mars 1997. *(DS) (MàJ par* RFC3396, RFC4361, RFC5494, et RFC6849)

[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)

[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)

[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.)*

[RFC5121] B. Patil et autres, "Transmission de IPv6 via la sous-couche de convergence IPv6 sur réseaux IEEE 802.16", février 2008. *(P.S. ; MàJ par* RFC8064)

11.2 Références pour information

[802.1AE] IEEE Std 802.1AE-2006, "IEEE Standard for Local and metropolitan area networks Media Access Control (MAC) Security", août 2006.

[RFC3046] M. Patrick, "Option DHCP Information d'agent de relais", janvier 2001. (*MàJ par* RFC6607)

[RFC3971] J. Arkko et autres, "Découverte de voisin sûre (SEND)", mars 2005. (*MàJ par* RFC6494) *(P.S.)*

[RFC4541] M. Christensen et autres, "Considérations sur les commutateurs d'observation du protocole de gestion de groupe Internet (IGMP) et de découverte d'écoutant de diffusion groupée (MLD)", mai 2006. *(Information)*

[RFC4562] T. Melsen, S. Blake, "Transmission forcée à la couche MAC : une méthode de séparation d'abonné sur un réseau d'accès Ethernet", juin 2006. *(Information)*

[RFC5154] J. Jee et autres, "Position du problème et buts de IP sur réseau IEEE 802.16", avril 2008. *(Information)*

Appendice A. Considérations de déploiement de CID en diffusion groupée

Les CID en diffusion groupée sont un moyen très efficace de distribuer les mêmes informations à plusieurs SS sous la même BS. Cependant, le déploiement de CID en diffusion groupée pour des services de données en diffusion ou en diffusion groupée souffre des inconvénients suivants.

Un inconvénient des CID en diffusion groupée pour Ethernet sur IEEE 802.16 est la nature unidirectionnelle des CID en diffusion groupée. Alors qu'il est possible de faire une diffusion groupée vers l'aval des informations à un certain nombre de SS en parallèle, il n'y a pas de connexions de diffusion groupée en amont. Dans la direction amont, des CID en envoi individuel doivent être utilisés pour envoyer des messages en diffusion groupée sur le réseau radio à la BS, exigeant une fonction de transmission de diffusion groupée spéciale pour renvoyer les informations aux autres SS sur un CID en diffusion groupée. Bien que de nature similaire à une fonction de pontage, il n'y a pas de modèle de transmission approprié disponible. [802.1D] ne peut pas tirer parti des CID en diffusion groupée parce que il repose sur des connexions d'envoi individuel ou des connexions de diffusion bidirectionnelles.

Un autre inconvénient du déploiement de CID en diffusion groupée pour distribuer les messages de contrôle en diffusion, comme les demandes ARP, est l'incapacité d'empêcher l'éveil des SS en mode dormant par les messages qui ne leurs sont pas destinés. Chaque fois qu'un message est envoyé sur un CID en diffusion groupée, toutes les stations associées doivent se mettre sous tension et recevoir et traiter le message. Alors que ce comportement est désirable pour le trafic en diffusion et en diffusion groupée, il est dommageable pour les messages de contrôle de couche de liaison en diffusion visant une seule SS, comme une demande ARP. Toutes les autres SS gaspillent de rares ressources de batterie pour recevoir, décoder, et éliminer le message. Une faible consommation d'énergie est un aspect extrêmement important dans les communications sans fil.

De plus, on devrait garder présent à l'esprit que les CID en diffusion groupée sont seulement efficaces pour un grand nombre de SS abonnées dans une cellule. Du fait de l'incompatibilité avec les algorithmes avancés de couche radio fondés sur les informations de rétroaction du côté receveur, les connexions de diffusion groupée exigent plus de ressources radio pour transférer les mêmes informations que les connexions d'envoi individuel.

Appendice B. Pontage centralisé contre pontage réparti

La présente spécification introduit une fonction de pontage côté réseau, qui peut être réalisée par un appareil centralisé ou par plusieurs ponts interconnectés de manière répartie. Une mise en œuvre courante du modèle réparti est le scénario où un pont est directement rattaché à la station de base, de telle façon que l'interface entre BS et fonction de pontage devienne une interface logicielle dans le système de fonctionnement de l'appareil BS/pont.

Les améliorations opérationnelles décrites dans la Section 7 du présent document sont fondées sur la disponibilité des informations supplémentaires sur tous les hôtes rattachés à l'Ethernet. Arroser tous les accès du pont peut être évité quand des informations a priori sont disponibles pour déterminer l'accès auquel une trame Ethernet doit être livré.

Les meilleures performances peuvent être obtenues par une base de données centralisée contenant toutes les informations sur les hôtes rattachés à l'Ethernet. Une base de données centralisée peut être établie par un appareil de pont centralisé ou une structure de pontage hiérarchique avec des accès entrants et sortants dédiés comme dans le cas de l'accès public, où le pont supérieur est capable de restituer et conserver toutes les informations.

Comme le cas générique du modèle de liaison IP sur Ethernet sur IEEE 802.16 ne fait aucune hypothèse sur la localisation de l'AR (un AR peut même être rattaché à une SS) un système de pontage centralisé est recommandé pour le cas générique. Dans le système centralisé, chaque connexion sur le réseau radio d'une liaison devrait être rattachée à un seul pont centralisé.

Un modèle de pontage réparti est approprié, en particulier, pour le mode d'accès public, où les trames Ethernet, qui n'ont pas d'entrée dans le pont derrière la BS, sont envoyées en amont jusqu'à finalement atteindre un pont qui a une entrée pour

l'adresse de MAC de destination.

Adresse des auteurs

Hongseok Jeon
ETRI
161 Gajeong-dong, Yuseong-gu
Daejeon, 305-350
KOREA
mél : hongseok.jeon@gmail.com

Sangjin Jeong
ETRI
161 Gajeong-dong, Yuseong-gu
Daejeon, 305-350
KOREA
mél : sjjeong@etri.re.kr

Max Riegel
Nokia Siemens Networks
St-Martin-Str 76
Munich, 81541
Germany
mél : maximilian.riegel@nsn.com