

Équipe d'ingénierie de l'Internet (IETF)
Request for Comments: 5679
Catégorie : Sur la voie de la normalisation
ISSN: 2070-1721

G. Bajko, Nokia
décembre 2009

Traduction Claude Brière de L'Isle

Localisation des services de mobilité IEEE 802.21 avec le DNS

Résumé
Le présent document définit des étiquettes de service d'application qui permettent la localisation de service sans s'appuyer sur des conventions rigides de dénomination de domaine, et les procédures du DNS pour découvrir les serveurs qui fournissent les services de mobilité définis par IEEE 802.21. Ces services de mobilité sont utilisés pour aider un nœud mobile (MN, *Mobile Node*) qui prend en charge IEEE 802.21, dans la préparation du transfert inter-cellulaire (découverte de réseau) et la décision de transfert inter-cellulaire (choix du réseau). Les services visés par le présent document sont les services de transfert inter-cellulaire indépendants du support (MIHS, *Media Independent Handover Services*) définis dans IEEE 802.21.

Statut de ce mémoire
Ceci est un document de l'Internet sur la voie de la normalisation.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Tous les documents approuvés par l'IESG ne sont pas candidats à devenir une norme de l'Internet ; voir la Section 2 de la RFC5741.

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à <http://www.rfc-editor.org/info/rfc5679>

Notice de droits de reproduction
Copyright (c) 2009 IETF Trust et les personnes identifiées comme auteurs du document. Tous droits réservés.

Le présent document est soumis au BCP 78 et aux dispositions légales de l'IETF Trust qui se rapportent aux documents de l'IETF (<http://trustee.ietf.org/license-info>) en vigueur à la date de publication de ce document. Prière de revoir ces documents avec attention, car ils décrivent vos droits et obligations par rapport à ce document. Les composants de code extraits du présent document doivent inclure le texte de licence simplifié de BSD comme décrit au paragraphe 4.e des dispositions légales du Trust et sont fournis sans garantie comme décrit dans la licence de BSD simplifiée.

Table des matières

1. Introduction.....	1
1.1 Conventions utilisées dans ce document.....	2
1.2 Terminologie.....	2
2. Découverte d'un serveur de mobilité.....	3
2.1 Choix d'un service de mobilité.....	3
2.2 Choix du protocole de transport.....	3
2.3 Détermination de l'adresse et accès IP.....	4
3. Considérations relatives à l'IANA.....	4
4. Considérations sur la sécurité.....	5
5. Références normatives.....	6
6. Références pour information.....	6
Adresse de l'auteur.....	6

1. Introduction

[IEEE802.21] définit trois types de services distincts pour faciliter le transfert inter-cellulaire de couche de liaison à travers des technologies hétérogènes :

- a) Le service d'informations de MIH (MIHIS, *MIH Information Service*) : IS fournit un cadre unifié aux entités de couche supérieure à travers un environnement de réseau hétérogène pour faciliter la découverte et le choix de plusieurs types de réseaux existants au sein d'une zone géographique, avec l'objectif d'aider les protocoles de mobilité de couche supérieure à acquérir une vue globale des réseaux hétérogènes et effectuer un transfert inter-cellulaire sans à-coups à travers ces réseaux.
- b) Le service d'événements MIH (MIHES, *MIH Event Service*) : les événements peuvent indiquer des changements dans l'état et le comportement de transmission des couches physique, de liaison des données et de liaison logique, ou prédire des changements d'état de ces couches. Les services d'événements peuvent aussi être utilisés pour indiquer des actions de gestion ou des états de commandes sur la partie de réseau ou sur une entité de gestion.
- c) Le service de commandes MIH (MIHCS, *MIH Command Service*) : le service de commandes permet aux couches supérieures de contrôler les couches physique, de liaison des données, et de liaison logique. Les couches supérieures peuvent contrôler la reconfiguration ou le choix d'une liaison appropriée à travers un ensemble de commande de transfert inter-cellulaire.

Dans la terminologie IEEE, ces services sont appelés des services de transfert inter-cellulaire indépendant du support (MIH, *Media Independent Handover*). Bien que ces services puissent être co-localisés, les différents schémas et types d'informations qu'ils fournissent ne nécessitent pas la co-localisation.

Les messages de service de "gestion de service", c'est-à-dire, les messages d'enregistrement de MIH, de découverte de capacité MIH et d'abonnement aux événements de MIH, sont considérés comme des MIHES et MIHCS quand ils transportent des messages MIH sur du transport de couche 3.

Un nœud mobile (MN, *Mobile Node*) peut utiliser tout type de service de MIH séparément ou dans toute combinaison.

Il est prévu qu'un serveur de mobilité ne va pas nécessairement héberger ensemble ces trois services de MIH, donc il faut découvrir séparément les types de service de MIH.

Le présent document définit un certain nombre d'étiquettes de service d'application qui permettent la localisation de service sans s'appuyer sur des conventions rigides de désignation de domaine.

1.1 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].

1.2 Terminologie

Services de mobilité : composé d'un ensemble de différents services fournis par le réseau aux nœuds mobiles pour faciliter la préparation et la décision du transfert inter-cellulaire, comme décrit dans [IEEE802.21] et la [RFC5164].

Serveur de mobilité : nœud de réseau fournissant les services de mobilité IEEE 802.21.

Transfert inter-cellulaire indépendant du support (MIH, *Media Independent Handover*) : comme défini dans [IEEE802.21].

Service d'application : terme générique pour certains types d'application, indépendamment du protocole qui peut être utilisé pour l'offrir. Chaque service d'application va être associé à une étiquette enregistrée par l'IANA.

Protocole d'application : utilisé pour mettre en œuvre le service d'application. Il est aussi associé à une étiquette enregistrée par l'IANA.

Domaine de rattachement : suffixe DNS de l'opérateur avec lequel le nœud mobile a un service d'abonnement. Le suffixe est généralement mémorisé dans le nœud mobile au titre de l'abonnement.

2. Découverte d'un serveur de mobilité

Le système de découverte dynamique de délégation (DDDS, *Dynamic Delegation Discovery System*) [RFC3401] est utilisé pour mettre en œuvre des liens lâches des chaînes aux données, afin de prendre en charge les systèmes de délégation configurés dynamiquement. Le DDDS fonctionne en transposant une chaîne unique en données mémorisées dans une base de données DDDS en appliquant itérativement les règles de transformation de chaîne jusqu'à ce qu'une condition terminale soit atteinte. Quand DDDS utilise le DNS comme une base de données distribuée de règles, ces règles sont codées en utilisant l'enregistrement de ressource (RR, *Resource Record*) de pointeur d'autorité de dénomination (NAPTR, *Naming Authority Pointer*). Une de ces règles est la première règle bien connue, qui dit où commence le processus.

Dans les spécifications actuelles, la première règle bien connue dans une application DDDS [RFC3403] est supposée être fixée, c'est-à-dire, le domaine dans l'arborescence où les recherches vont être acheminées, est connue. Le présent document propose que l'entrée à la première règle bien connue soit dynamique, sur la base du chemin de recherche que le résolveur découvre ou avec lequel il est configuré.

Le chemin de recherche du résolveur peut être pré-configuré, découvert en utilisant DHCP, ou appris d'une interrogation précédente des services d'information (IS) MIH [IEEE802.21] comme décrit dans la [RFC5677].

Quand le MN a besoin de découvrir des services de mobilité dans son domaine de rattachement, l'entrée à la première règle bien connue DOIT être le domaine de rattachement du MN, qui est supposé être pré-configuré dans le MN.

Quand le MN a besoin de découvrir des services de mobilité dans un domaine local (visité) il DEVRAIT utiliser DHCP comme décrit dans la [RFC5678] pour découvrir l'adresse IP du serveur hébergeant le service désiré, et le contacter directement. Dans certaines instances, la découverte peut résulter en une liste par protocole/application de noms de domaine qui sont alors utilisés comme points de départ des recherches de NAPTR suivantes. Si ni l'adresse IP ni le nom de domaine ne peuvent être découverts avec la procédure ci-dessus, le MN PEUT demander une liste de recherche de domaine, comme décrit dans les [RFC3397] et [RFC3646], et l'utiliser comme entrée de l'application DDDS.

Le MN peut aussi avoir une liste de noms de domaines de fournisseurs de service en antémémoire, apprise d'une interrogation précédente des services d'information de MIH [IEEE802.21]. Si les entrées d'antémémoire ne sont pas expirées, elles peuvent être utilisées comme entrées à l'application de DDDS.

Quand le MN ne trouve pas de nom de domaine valide en utilisant les procédures ci-dessus, il DOIT cesser de tenter de découvrir des services de MIH.

La règle dynamique décrite ci-dessus NE DEVRAIT PAS être utilisée pour découvrir des services autres que MIH décrits dans le présent document, sauf mention contraire dans une future spécification.

Les procédures définies ici résultent en une adresse IP, un accès, et un protocole de transport où le MN peut contacter le serveur de mobilité qui héberge le service que cherche le MN.

2.1 Choix d'un service de mobilité

Le MN devrait connaître les caractéristiques des services de mobilité définis dans [IEEE802.21], et sur cette base, il devrait être capable de choisir le service qu'il veut utiliser pour faciliter son transfert inter-cellulaire. Les services qu'il peut choisir sont :

- les services d'information (MIHIS)
- les services d'événements (MIHES)
- les services de commandes (MIHCS)

Les identifiants de service pour les services sont "MIHIS", "MIHES", et "MIHCS", respectivement. Le serveur qui prend en charge un des services ci-dessus DOIT prendre en charge au moins UDP et TCP comme transport, comme décrit dans la [RFC5677]. SCTP et d'autres protocoles de transport PEUVENT aussi être pris en charge.

2.2 Choix du protocole de transport

Après le choix du service désiré, le client choisit le protocole de transport qu'il préfère utiliser. Noter que le choix du transport peut impacter les performances de transfert inter-cellulaire.

Les services pertinents pour le choix du protocole de transport sont ceux dont les champs de service NAPTR ont la valeur de "ID+M2X", où ID est l'identifiant de service défini au paragraphe précédent, et X est une lettre qui correspond à un protocole de transport pris en charge par le domaine. La présente spécification définit M2U pour UDP, M2T pour TCP et M2S pour SCTP. Le présent document établit aussi un registre de l'IANA pour les transpositions de nom de service NAPTR en protocole de transport.

Ces enregistrements NAPTR [RFC3403] fournissent une transposition d'un domaine en l'enregistrement de SRV [RFC2782] pour contacter un serveur avec le protocole de transport spécifique dans le champ Services NAPTR. L'enregistrement de ressource DOIT contenir une expression régulière vide et une valeur de remplacement, qui indique le nom de domaine où peut être trouvé l'enregistrement SRV pour ce protocole de transport particulier. Si le serveur prend en charge plusieurs protocoles de transport, il va y avoir plusieurs enregistrements NAPTR, chacun avec une valeur de service différente. Conformément à la [RFC3403], le client élimine tout enregistrement dont les champs de services ne sont pas applicables.

Le MN DOIT éliminer tous les champs de service qui identifient un service de résolution dont la valeur n'est pas "M2X", pour les valeurs de X qui indiquent des protocoles de transport supportés par le client. Le traitement de NAPTR décrit dans la RFC 3403 va résulter en la découverte du protocole de transport préféré du serveur qui est pris en charge par le client, ainsi que en un enregistrement SRV pour le serveur.

Par exemple, considérons un client qui souhaite trouver un service de MIHIS dans le domaine exemple.com. Le client fait une interrogation NAPTR pour ce domaine, et les enregistrements NAPTR suivants sont retournés :

	Ordre	Préf.	Fanions	Service	Regexp	Remplacement
IN NAPTR	50	50	"s"	"MIHIS+M2T"	""	_MIHIS._tcp.exemple.com
IN NAPTR	90	50	"s"	"MIHIS+M2U"	""	_MIHIS._udp.exemple.com

Cela indique que le domaine a bien un serveur qui fournit des services MIHIS sur TCP et UDP, dans cet ordre de préférence. Comme le client prend en charge TCP et UDP, TCP va être utilisé, ciblé sur un hôte déterminé par une recherche de SRV de _MIHIS._tcp.exemple.com. Cette recherche va retourner :

;;		Priorité	Pondération	Accès	Cible
	IN SRV	0	1	XXXX	serveur1.exemple.com
	IN SRV	0	2	XXXX	serveur2.exemple.com

où XXXX représente le numéro d'accès auquel le service est accessible.

Si aucun enregistrement NAPTR n'est trouvé, le client construit une interrogation SRV pour les protocoles de transport qu'il prend en charge, et fait une interrogation pour chacun. Les interrogations sont faites en utilisant les identifiants de service "_MIHIS" pour le service d'informations MIH, "_MIHES" pour le service d'événements MIH et "_MIHCS" pour le service de commandes MIH. Un transport particulier est pris en charge si l'interrogation réussit. Le client PEUT utiliser tout protocole de transport qu'il désire et qui est pris en charge par le serveur.

Noter que le champ regexp dans l'exemple de NAPTR ci-dessus est vide. Le champ regexp NE DOIT PAS être utilisé quand on découvre des services de MIH, car son usage peut être complexe et enclin à l'erreur. Aussi, la découverte des services de MIH n'exige pas la souplesse fournie par ce champ sur une cible statique présente dans le champ CIBLE.

Si le client est déjà configuré avec les informations sur le protocole de transport utilisé pour un service de mobilité dans un domaine particulier, il peut effectuer directement une interrogation de SRV pour ce transport spécifique en utilisant l'identifiant de service du service de mobilité. Par exemple, si le client sait qu'il devrait utiliser TCP pour le service MIHIS, il peut effectuer directement une interrogation de SRV pour _MIHIS._tcp.exemple.com.

2.3 Détermination de l'adresse et accès IP

Une fois que le serveur fournissant le service désiré et que le protocole de transport ont été déterminés, l'étape suivante est de déterminer l'adresse et l'accès IP.

La réponse à l'interrogation de SRV du DNS contient le numéro d'accès dans le champ Accès des RDATA du SRV.

Conformément à la spécification des RR SRV dans la [RFC2782], le champ CIBLE est un nom de domaine pleinement qualifié (FQDN) qui DOIT avoir un ou plusieurs enregistrements d'adresse ; le FQDN ne doit pas être un alias, c'est-à-dire,

il NE DOIT PAS y avoir un RR CNAME ou DNAME à ce nom. Sauf si l'interrogation de SRV du DNS a déjà rapporté un nombre suffisant de ces enregistrements d'adresse dans la section des données supplémentaires de la réponse du DNS (comme recommandé par la [RFC2782]) le MN doit effectuer une ou des recherches d'enregistrement A et/ou AAAA du nom de domaine, comme approprié. Le résultat va être une liste d'adresses IP, dont chacune peut être contactée en utilisant le protocole de transport déterminé précédemment.

3. Considérations relatives à l'IANA

L'usage des enregistrements NAPTR décrit ici exige des valeurs bien connues pour les champs de service pour chaque transport supporté par les services de mobilité. Le tableau des transpositions des valeurs de champ de service en protocoles de transport est tenu par l'IANA.

L'enregistrement dans la RFC DOIT inclure les informations suivantes :

Champ Service : le champ de service enregistré.

Protocole : le protocole de transport spécifique associé à ce champ de service. Il DOIT inclure le nom et l'acronyme du protocole, avec une référence au document qui décrit le protocole de transport.

Informations de nom et de contact : nom, adresse, adresse de messagerie, et numéro de téléphone de la personne qui effectue l'enregistrement.

Les valeurs suivantes ont été placées dans le registre :

Champs de service	Protocole
MIHIS+M2T	TCP
MIHIS+M2U	UDP
MIHIS+M2S	SCTP
MIHES+M2T	TCP
MIHES+M2U	UDP
MIHES+M2S	SCTP
MIHCS+M2T	TCP
MIHCS+M2U	UDP
MIHCS+M2S	SCTP

Les nouveaux champs de service sont à ajouter via une action de normalisation, comme défini dans la [RFC5226].

Les nouvelles entrées au tableau qui spécifient des protocoles de transport supplémentaires pour les champs de service existants peuvent de même être enregistrées par l'IANA par une action de normalisation [RFC5226].

Il est aussi demandé à l'IANA d'enregistrer MIHIS, MIHES, MIHCS comme noms de services dans le registre des noms de protocoles et de services.

4. Considérations sur la sécurité

Une liste des menaces connues sur les services qui utilisent le DNS est documentée dans la [RFC3833]. Pour la plupart de ces menaces identifiées, les extensions de sécurité au DNS [RFC4033] fournissent la protection. Il est donc recommandé d'envisager l'usage de DNSSEC [RFC4033] et des aspects des pratiques de fonctionnement de DNSSEC [RFC4641] quand on déploie les services de mobilité IEEE 802.21.

Dans les déploiements où l'usage de DNSSEC n'est pas faisable, des mesures devraient être prises pour protéger autant que possible contre les réponses falsifiées du DNS et l'empoisonnement de mémoire tampon. Des efforts dans cette direction sont documentés dans la [RFC5452].

Lorsque les entrées à la procédure décrites dans le présent document sont fournies via DHCP, les vulnérabilités de DHCP peuvent aussi causer des problèmes. Par exemple, l'incapacité d'authentifier les résultats de la découverte DHCP peut conduire à ce que les résultats du service de mobilité soient aussi incorrects, même si le processus du DNS était sécurisé.

5. Références normatives

- [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](#))
- [RFC2782] A. Gulbrandsen, P. Vixie et L. Esibov, "Enregistrement de ressource DNS pour la spécification de la [localisation des services](#) (DNS SRV)", février 2000, DOI 10.17487/RFC2782.
- [RFC3397] B. Aboba, S. Cheshire, "Option [Recherche de domaine du protocole de configuration dynamique d'hôte](#) (DHCP)", novembre 2002. (P.S.)
- [RFC3403] M. Mealling, "Système de découverte dynamique de délégation ([DDDS](#)) [Partie III : base de données du système](#) de noms de domaines (DNS)", octobre 2002. (P.S.)
- [RFC3646] R. Droms, éd., "[Options de configuration du DNS](#) pour le protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)", décembre 2003. (P.S.)
- [RFC4033] R. Arends, et autres, "Introduction et [exigences pour la sécurité du DNS](#)", mars 2005, DOI 10.17487/RFC4033
- [RFC5226] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, mai 2008. (Remplace [RFC2434](#) ; remplacée par [RFC8126](#))
- [RFC5677] T. Melia, éd., G. Bajko, S. Das, N. Golmie, JC. Zuniga, "[Conception du cadre des services](#) de mobilité IEEE 802.21 (MSFD)", décembre 2009. (P. S.)
- [RFC5678] G. Bajko, S. Das, "[Options du protocole de configuration](#) dynamique d'hôte (DHCPv4 et DHCPv6) pour la découverte de services de mobilité IEEE 802.21", décembre 2009. (P. S.)

6. Références pour information

- [IEEE80221] "IEEE Standard for Local and Metropolitan Area Networks - Part 21: Media Independent Handover Services", IEEE LAN/MAN Std 802.21-2008, janvier 2009. <http://www.ieee802.org/21/private/Published%20Spec/802.21-2008.pdf> (l'accès au document est réservé aux membres).
- [RFC3401] M. Mealling, "[Système de découverte dynamique de délégation](#) (DDDS) Partie I : DDDS complet", octobre 2002. (Info.)
- [RFC3833] D. Atkins, R. Austein, "[Analyse des menaces contre le système](#) des noms de domaines (DNS)", août 2004. (Info.)
- [RFC4641] O. Kolkman, R. Gieben, "[Fonctionnement pratique de DNSSEC](#)", septembre 2006. (Information)
- [RFC5164] T. Melia, "Transport des services mobiles : position du problème", mars 2008. (Information)
- [RFC5452] A. Hubert, R. van Mook, "[Mesures pour rendre le DNS plus résilient](#) aux fausses réponses", janvier 2009. (MàJ [RFC2181](#)) (P.S.)

Adresse de l'auteur

Gabor Bajko
Nokia
mél : gabor.bajko@nokia.com