Groupe de travail Réseau
RFC 5505
Catégorie : Information
mai 2009
Traduction Coralie Gauge

B. Aboba
D. Thaler
L. Andersson
S. Cheshire
Internet Architecture Board

Principes de la configuration de l'hôte Internet

Résumé
Ce document décrit les principes de la configuration de l'hôte Internet.
Il traite des problèmes relatifs à la configuration des paramètres de la couche Internet, ainsi que des paramètres concernant les protocoles de la couche supérieure.

Table des matières

1. Introduction

Ce document décrit les principes de la configuration de l'hôte Internet [STD3]. Il traite des problèmes relatifs à la configuration des paramètres de la couche Internet, ainsi que des paramètres concernant les protocoles de la couche supérieure.

Au cours de ces dernières années, de nombreuses questions d'architecture se sont posées, c'est la raison pour laquelle nous fournissons un guide aux développeurs de protocole :

- Les couches de protocole et les approches générales les plus appropriées pour la configuration de divers paramètres.
- La relation entre la configuration de paramètres et la découverte du service.
- La relation entre configuration par interface et configuration par hôte.
- La relation entre l'authentification d'accès réseau et la configuration de l'hôte.
- Les avantages obtenus de la prise en charge de l'auto configuration des paramètres ou d'éviter complètement la configuration des paramètres.
- Le rôle des protocoles de couche liaison et des protocoles de tunnelage dans la configuration d'hôte Internet.

Le rôle des protocoles de couche liaison et de tunnelage est particulièrement important puisqu'il peut affecter les propriétés d'une liaison vue par les couches supérieures (par exemple : si des extensions de confidentialité [RFC 4941] sont disponibles aux applications).

1.1. Terminologie

Liaison
Dispositif ou support de communication par lequel les nœuds peuvent communiquer à la couche liaison, c'est-à-dire la couche immédiatement en dessous de IP. Exemples : des Ethernet (simples ou pontés), des liaisons en protocole point à point (PPP), réseaux X.25, relais de trames ou ATM, ainsi que les "tunnels" Internet ou de couche supérieure, tels que les tunnels sur IPv4 ou IPv6 lui-même.

En liaison
Adresse attribuée à une interface sur une liaison spécifiée.

Hors liaison
Contraire de "en liaison". Adresse qui n'est attribuée à aucune interface sur la liaison spécifiée.

Agent de mobilité
C'est soit un agent de rattachement soit un agent étranger [RFC3344] [RFC3775].

1.2. Configuration de l'hôte Internet

1.2.1. Configuration de la couche Internet

La configuration de la couche Internet est définie comme étant la configuration requise pour prendre en charge le fonctionnement de la couche Internet. Elle inclut la configuration des paramètres par interface et par hôte, y compris les paramètres des adresses IP, des préfixes de sous-réseau, des passerelles par défaut, des agents de mobilité, de configuration du service de démarrage et autres.

Adresses IP
La configuration d'adresse de protocole Internet (IP) comprend la configuration des adresses de portée liaison aussi bien que celle des adresses mondiales.
La configuration des adresses IP est une étape indispensable puisque pratiquement tout le réseautage IP repose sur l'hypothèse que les hôtes ont une ou des adresses IP associées à (chacune de) leurs interfaces réseau actives. Ces adresses IP indiquent l'expéditeur du paquet lorsqu'elles sont utilisées comme adresse de source d'un paquet IP, et le destinataire prévu lorsqu'elles sont utilisées comme adresse de destination d'un paquet IP en envoi individuel.
Le seul exemple courant de protocole fondé sur IP opérant sans adresse IP implique la configuration de l'adresse, telle que l'utilisation du protocole DHCPv4 [RFC 2131] pour obtenir une adresse. Dans ce cas, le protocole DHCPv4 opère, par définition, avant que l'hôte n'ait une adresse IPv4, par conséquent, les concepteurs du protocole DHCP avaient le choix d'utiliser IP sans adresse IP ou de ne pas utiliser IP du tout. L'autonomie de l'IPv4 grâce à la configuration avec ses propres paquets IPv4 plutôt que la dépendance à un autre protocole a des avantages qui l'emportent sur les inconvénients de l'utilisation de IP dans ce mode limité. L'utilisation de IP pour des raisons autres que la configuration de l'adresse peut assurer avec certitude que l'hôte aura une ou plusieurs adresses IP, qui peuvent être des adresses de liaison locale auto configurées [RFC 3927] [RFC 4862] ou d'autres adresses configurées via DHCP ou d'autres moyens.

Préfixe de sous-réseau
Une fois que le préfixe de sous-réseau est configuré sur une interface, les hôtes ayant une adresse IP peuvent échanger directement des paquets IP en envoi individuel avec les hôtes en liaison dans le même préfixe de sous-réseau.

Passerelle par défaut
Une fois que la passerelle par défaut est configurée sur une interface, les hôtes ayant une adresse IP peuvent expédier des paquets IP en envoi individuel à cette passerelle pour les transférer aux hôtes hors liaison.

Agent de mobilité
Bien que IPv4 mobile [RFC 3344] et IPv6 mobile [RFC 3775] incluent leurs propres mécanismes pour la localisation des agents de rattachement, il est également possible aux nœuds mobiles d'utiliser la configuration dynamique de l'agent de rattachement.

Configuration du service de démarrage
La configuration du service de démarrage est définie comme étant la configuration nécessaire pour un hôte afin d'obtenir et également de vérifier une image de démarrage appropriée. Elle convient aux hôtes sans disque qui cherchent à obtenir une image de démarrage via des mécanismes tels que le protocole simple de transfert de fichiers (TFTP) [RFC 1350], le système de fichier réseau (NFS) [RFC 3530] et l'interface SCSI (iSCSI) [RFC 3720] [RFC 4173]. Elle peut également être utile dans

des situations où il est nécessaire de mettre à jour l'image de démarrage d'un hôte qui prend en charge un disque, tels que dans l'environnement d'exécution pré-démarrage (PXE) [RFC 4578]. Bien qu'au sens strict, les services de démarrage opèrent au-dessus de la couche Internet, lorsque le service de démarrage est utilisé pour obtenir le code de la couche Internet il peut être considéré comme faisant partie de la configuration de la couche Internet. Bien que les paramètres du service de démarrage puissent être fournis sur la base de l'interface, le chargement et la vérification de l'image de démarrage affectent le comportement de l'hôte dans son ensemble

Autres paramètres IP
La configuration des paramètres de la couche Internet comprend également la configuration des paramètres de l'hôte (par exemple, nom de l'hôte) et des paramètres par interface (par exemple, durée de vie (TTL) IP à utiliser dans les paquets sortants, activation/désactivation de la transmission IP et de l'acheminement de source, unité de transmission maximale (MTU)).

1.2.2. Configuration de la couche supérieure

La configuration de la couche supérieure est définie comme étant la configuration requise pour prendre en charge le fonctionnement d'autres composants au-dessus de la couche Internet. Elle comprend par exemple :

Configuration du service de noms
C'est la configuration requise pour que l'hôte résolve les noms. Elle inclut la configuration des adresses des serveurs de résolution de noms, y compris les serveurs IEN 116 [IEN116], les serveurs du système des noms de domaine (DNS), les serveurs du service de noms Internet Windows (WINS), les serveurs du service de noms de mémorisation sur Internet (iSNS) [RFC 4171] [RFC 4174] et les serveurs du service d'information réseau (NIS) [RFC 3898], ainsi que le réglage des paramètres de résolution de noms, tels que le domaine DNS et la liste de recherche [RFC 3397], le type de nœud NetBIOS, etc. Elle peut également inclure la transmission ou l'établissement du propre nom de l'hôte. Noter que les services de résolution de noms de liaison locale (tels que NetBIOS [RFC 1001], la résolution de noms en diffusion groupée sur liaison locale (LLMNR) [RFC 4795] et la diffusion groupée DNS (mDNS) [mDNS] ne requièrent normalement aucune configuration.
Une fois que l'hôte a terminé la configuration du service de noms, il est capable de résoudre des noms en utilisant les protocoles de résolution de noms qui requièrent une configuration. Ceci ne permet pas seulement à l'hôte de communiquer avec les hôtes hors liaison dont les adresses IP sont inconnues, mais, dans la mesure où les services de noms exigeant une configuration sont utilisés pour la découverte du service, ceci permet également à l'hôte de découvrir les services disponibles sur le réseau ou ailleurs. Bien que les paramètres du service de noms puissent être fournis sur la base de l'interface, leur configuration affectera généralement le comportement de l'hôte dans son ensemble.

Configuration du service de l'heure
La configuration du service de l'heure comprend la configuration des serveurs pour les protocoles tels que le protocole simple de l'heure du réseau (SNTP) et le protocole de l'heure du réseau (NTP). Étant donné que la détermination précise de l'heure peut être importante pour le fonctionnement des applications en cours d'exécution sur l'hôte (y compris les services de sécurité), la configuration des serveurs de l'heure peut être un pré-requis pour le fonctionnement de la couche supérieure. Cependant, ceci n'est pas, en général, exigé pour la configuration de la couche Internet. Bien que les paramètres du service de l'heure puissent être fournis sur la base de l'interface, leur configuration affectera généralement le comportement de l'hôte dans son ensemble.

Configuration d'autres services
Elle peut comprendre la découverte de serveurs et de périphériques supplémentaires, tels que les imprimantes, mandataires du protocole d'initialisation de session (SIP), etc. Cette configuration s'appliquera généralement à l'ensemble de l'hôte.

2. Principes

Cette section décrit les principes de base de la configuration de l'hôte Internet.

2.1 Réduire la configuration

Tout ce qui peut être configuré peut être mal configuré. La section 3.8 de la RFC 1958 "Principes de l'architecture de l'Internet" indique qu'il faut : « éviter les options et les paramètres lorsque cela est possible. Toutes les options et tous les paramètres doivent être configurés ou négociés dynamiquement plutôt que manuellement. »

C'est-à-dire que, pour minimiser la possibilité d'erreurs de configuration, les paramètres devraient être automatiquement calculés (ou du moins comporter des défauts raisonnables) chaque fois que possible. Par exemple, l'unité maximum de transmission de chemin (PMTU) peut être découverte, comme décrit dans les "Découverte de la MTU de chemin de couche de mise en paquet" [RFC 4821], "Problèmes de TCP avec la découverte de la MTU de chemin" [RFC 2923], "Découverte de la MTU de chemin" [RFC 1191] et "Découverte de la MTU de chemin pour IP version 6" [RFC 1981].

Une conception de protocole avec de nombreux paramètres configurables accroit les possibilités de paramètres mal configurés qui conduisent à des échecs ou à d'autres opérations non-optimales. La suppression ou la diminution des paramètres configurables aide à réduire ce risque. Là où les paramètres configurables sont nécessaires ou souhaitables, les protocoles peuvent réduire le risque d'erreur humaine en rendant ces paramètres auto configurables, comme avec l'utilisation de la négociation de capacité dans le protocole, ou avec la découverte automatique des autres hôtes qui mettent en œuvre le même protocole.

2.2. Moins veut dire plus

La disponibilité de mécanismes simples et standardisés pour la configuration de l'hôte Internet d'usage général est hautement recommandée. La RFC 1958 "Principes de l'architecture de l'Internet" indique que : « la performance et le coût doivent être pris en compte tout comme les fonctionnalités » et qu'il faut « faire simple. Lorsque vous avez un doute au moment de la conception, choisissez la solution la plus simple ».

Afin de permettre la prise en charge du protocole dans de nombreux types d'appareils, il est important de réduire l'exigence d'empreinte. Par exemple, les protocoles fondés sur IP sont utilisés dans une grande variété d'appareils, des superordinateurs aux petits appareils bon marché qui exécutent des systèmes d'exploitation intégrés. Étant donné que les ressources (par exemple, taille de la mémoire et du code) disponibles pour la configuration de l'hôte peuvent être très petites, il est recommandé qu'un hôte soit capable de se configurer lui-même d'une manière aussi simple que possible.

La prise en charge de IP dans les environnements d'exécution pré-démarrage est un exemple intéressant. Étant donné que, par définition, la configuration de démarrage est requise dans les hôtes qui n'ont pas encore été complètement démarrés, il est souvent nécessaire que le code de pré-démarrage soit exécuté à partir de la mémoire morte (ROM), avec une mémoire disponible minimale. De nombreux hôtes n'ont pas un espace suffisant sur cette mémoire ROM même pour une simple mise en œuvre de TCP, par conséquent, dans l'environnement d'exécution pré-démarrage (PXE), la tâche d'obtention d'une image d'amorçage est obtenue en utilisant à la place le protocole de datagramme d'utilisateur sur IP, UDP/IP de la [RFC 768]. C'est une des raisons pour laquelle les mécanismes de lconfiguration de la couche Internet dépendent généralement seulement de IP et de UDP. Après avoir obtenu l'image d'amorçage, l'hôte aura à sa disposition la totalité des dispositifs TCP/IP, y compris la prise en charge des protocoles de transport fiable, la sécurité du protocole Internet (IPsec), etc.

Afin de réduire la complexité, il est recommandé que les mécanismes de configuration de la couche Internet évitent la dépendance aux couches supérieures. Étant donné que les périphériques intégrés peuvent être extrêmement limités sur la quantité de code qu'ils peuvent ajuster dans leur mémoire ROM, la conception d'un mécanisme de configuration, de manière à ce qu'il requière la disponibilité des installations de la couche supérieure, peut rendre le mécanisme de configuration inutilisable dans de tels périphériques. En fait, la disponibilité de toutes les installations de la couche Internet n'est pas garantie. Par exemple, la version minimale de l'IP dans une mémoire ROM de démarrage de l'hôte ne peut pas implémenter la fragmentation et le réassemblage IP.

2.3. Réduire la diversité

Le nombre de mécanismes de configuration d'hôte devrait être réduit au minimum. La diversité des mécanismes de configuration d'hôte Internet présente plusieurs problèmes :

Interopérabilité
Lorsque la diversité de configuration s'accroit, il est probable qu'un hôte ne prendra pas en charge le ou les mécanismes de configuration disponibles sur le réseau auquel il est rattaché, ce qui crée des problèmes d'interopérabilité.

Empreinte
Pour une interopérabilité maximale, un hôte aurait besoin d'implémenter tous les mécanismes de configuration utilisés sur toutes les couches liaison qu'il prend en charge. Ceci augmente l'empreinte requise, ce qui est une charge pour les appareils intégré, et mène également à une qualité inférieure, puisque les ressources d'essais (essais formels et utilisation en fonctionnement réel) sont de plus en plus dispersées : plus un périphérique prend en charge de mécanismes de configuration différents, moins il est probable que chacun soit testé.

Redondance
Afin de prendre en charge la diversité dans les mécanismes de configuration, les opérateurs auraient besoin de prendre en charge de multiples services de configuration pour s'assurer que les hôtes connectés à leurs réseaux puissent se configurer eux-mêmes, ce qui représente une dépense supplémentaire pour peu de bénéfice.

Latence
Alors que la diversité de configuration s'accroit, les hôtes prenant en charge de multiples mécanismes de configuration peuvent déployer des efforts croissants pour déterminer quels sont les mécanismes pris en charge. Ceci s'ajoute à la latence de configuration.

Conflits
Chaque fois que plusieurs mécanismes sont disponibles, il est possible que plusieurs configurations soient renvoyées. Pour traiter ce problème, les hôtes auraient besoin de fusionner les configurations potentiellement conflictuelles, ce qui exigerait une logique de résolution de conflit, telle que le classement des sources de configuration potentielles, ce qui augmente la complexité de mise en œuvre.

Trafic supplémentaire
Afin de limiter la latence de configuration, les hôtes peuvent simultanément tenter d'obtenir une configuration par de multiples mécanismes, ce qui pourrait accroître le trafic en ligne, grâce à la fois à l'utilisation de plusieurs mécanismes et aux retransmissions dans les mécanismes de configuration non implantés sur le réseau.

Sécurité
La prise en charge de multiples mécanismes de configuration augmente la surface d'attaque sans aucun bénéfice.

2.4. Indépendance de la couche inférieure

La RFC 1958 "Principes d'architecture de l'Internet" indique que : « la modularité est bonne. Si les choses peuvent rester séparées, qu'elles le soient. »

Il est désormais de plus en plus commun que les hôtes prennent en charge de multiples mécanismes d'accès réseau, y compris le réseau téléphonique, le réseau sans fil, le réseau local câblé, le réseau sans fil métropolitain et le réseau de large zone, Avec la prolifération des mécanismes d'accès réseau, il est recommandé aux hôtes de pouvoir se configurer eux-mêmes sur de multiples réseaux sans ajouter de code de configuration spécifique à chaque nouvelle couche liaison.

Il est par conséquent hautement recommandé que les mécanismes de configuration de l'hôte Internet soient indépendants de la couche inférieure, c'est-à-dire que seul le protocole de couche liaison (liaison physique ou liaison de tunnel virtuelle) doit être explicitement conscient des paramètres de la couche liaison (bien que ces paramètres puissent être configurés par des mécanismes de la couche Internet générale). L'introduction de dépendances de la couche inférieure accroit la probabilité de problèmes d'interopérabilité et ajoute des mécanismes de configuration de la couche Internet que les hôtes doivent implémenter.

Les dépendances de la couche inférieure peuvent être mieux évitées en gardant la configuration de l'hôte Internet au-dessus de la couche liaison, permettant ainsi à la configuration d'être manipulée pour toutes les couches liaison qui prennent l'IP en charge. Afin de fournir l'indépendance au support, les mécanismes de la configuration de l'hôte Internet devraient être indépendants du protocole de la couche liaison.

Bien qu'il y ait des exemples de configuration de la couche Internet au sein de la couche liaison (tels que dans les protocoles PPP IPv4CP [RFC 1332] et dans le document "Spécification de la couche

d'interface radio mobile 3, protocoles de réseau principal, étape 3 (5ème Publication)" [3GPP-24.008]), cette approche a des inconvénients tels que la complexité supplémentaire d'implémentation de différents mécanismes sur différentes couches liaison et la difficulté de l'ajout de nouveaux paramètres de la couche supérieure qui exigeraient la définition d'un mécanisme dans chaque protocole de couche liaison.

Par exemple, la RFC 1877 "Extensions du protocole de contrôle du protocole Internet PPP pour les adresses de serveur de noms" a été développée avant la définition du message DHCPINFORM dans le "Protocole de configuration dynamique d'hôte" [RFC 2131]. À cette époque là, les serveurs du protocole de configuration dynamique d'hôte (DHCP) n'étaient pas largement mis en œuvre sur les appareils d'accès ou développés sur les réseaux des fournisseur d'accès. Bien que la conception de l'IPv4CP fût appropriée en 1992, elle ne doit pas être prise comme un exemple que les nouvelles technologies de la couche liaison devraient suivre. En effet, afin « d'avancer activement les extensions PPP les plus utiles au statut de norme à part entière, tout en se défendant contre les améliorations futures de valeur discutable », les "Considérations de l'IANA sur le protocole PPP" [RFC 3818] ont changé l'allocation des numéros de PPP (y compris des extensions IPv4CP) afin de ne plus être le « premier arrivé, premier servi ».

Dans l'IPv6, là où sont disponibles des mécanismes indépendants de la couche liaison tels que la configuration automatique sans état [RFC 4862] et le DHCPv6 sans état [RFC 3736], le protocole PPP IPv6CP [RFC 5072] configure un identifiant d'interface similaire à l'adresse de contrôle d'accès au support (MAC, *Media Access Control*) ce qui permet au protocole PPP IPv6CP d'éviter la duplication des fonctionnalités DHCPv6.

Cependant, l'échange de clés Internet version 2 (IKEv2) [RFC 4306] utilise la même approche que le protocole PPP IPv4CP en définissant une charge utile de configuration pour la configuration de l'hôte Internet à la fois pour IPv4 et IPv6. Bien que l'approche IKEv2 réduise le nombre d'échanges de paquets, la RFC 3456 "Configuration du protocole de configuration dynamique (DHCPv4) du mode tunnel IPsec" remarque que le fait de tirer parti du DHCP a des avantages en termes d'intégration de gestion d'adresse, de gestion de réservoir d'adresses, de reconfiguration et de reprise sur défaillance.

Les extensions aux protocoles de couche de liaison pour les besoins de la configuration de la couche d'application, de transport ou Internet (y compris la configuration du serveur) devraient être évitées. Ces extensions peuvent affecter négativement les propriétés d'une liaison vues par les couches supérieures. Par exemple, si un protocole de couche liaison (ou un protocole de tunnelage) configure des adresses IPv6 individuelles et exclut l'utilisation d'autres adresses, les applications souhaitant utiliser des extensions de confidentialité [RFC 4941] pourraient alors ne pas fonctionner correctement. Des problèmes similaires peuvent survenir pour d'autres types d'adresses, tels que des adresses générées cryptographiquement [RFC 3972].

Il est recommandé d'éviter les dépendances de la couche inférieures même là où la couche inférieure est indépendante de la liaison . Par exemple, bien que le protocole extensible d'authentification (EAP) puisse être exécuté sur toutes les liaisons satisfaisant à ses exigences (voir section 3.1 de la [RFC 3748]), beaucoup de couches de liaison ne prennent pas en charge le protocole EAP et par conséquent, les mécanismes de la configuration de la couche Internet qui dépendent du protocole EAP ne seront plus utilisables sur les liaisons qui prennent en charge IP et pas EAP.

2.5. La configuration n'est pas un contrôle d'accès

L'authentification et l'autorisation d'accès réseau est un problème distinct de la configuration de l'hôte Internet. Par conséquent, l'authentification et l'autorisation d'accès réseau est mieux traitée indépendamment des mécanismes de configuration de la couche Internet et de la couche supérieure.

Un protocole de couche Internet ou de couche supérieure qui authentifie les clients est approprié pour empêcher l'épuisement d'une ressource rare sur le serveur (tels que les adresses ou préfixes IP), mais ne l'est pas pour empêcher les hôtes d'obtenir un accès à la liaison. Si l'utilisateur peut manuellement configurer l'hôte, l'exigence de l'authentification afin d'obtenir les paramètres de configuration (tels que les adresses IP) n'a que peu de valeur. Les administrateurs de réseau qui souhaitent contrôler l'accès à la liaison peuvent mieux y parvenir en utilisant des technologies comme le contrôleur d'accès réseau fondé sur le port [IEEE-802.1X]. Noter que l'authentification du client n'est pas requise pour le protocole DHCPv6 sans état [RFC 3736] puisqu'il ne résulte pas en l'allocation de ressources limitées sur le serveur.

3. Explications supplémentaires

3.1 Dépendance des mécanismes d'usage général

Les protocoles devraient soit être auto configurés (particulièrement là où le partage de sort est important) soit utiliser des mécanismes de configuration d'usage général (tel que le protocole DHCP ou un protocole de découverte de service, comme noté au paragraphe 3.2). Le choix devrait être fait en prenant en compte les principes d'architecture examinés dans la section 2.

En prenant en compte les mécanismes de configuration d'usage général actuellement disponibles, nous voyons qu'il y a peu de besoin de développement de mécanismes de configuration d'usage général supplémentaires.

Lors de la définition d'un nouveau paramètre d'hôte, les concepteurs de protocole devraient d'abord étudier si la configuration est nécessaire (voir paragraphe 2.1).

Si la configuration est nécessaire, les concepteurs de protocole devraient non seulement examiner le partage de sort (voir paragraphe 3.2.1), mais aussi :

1. Les implications organisationnelles pour les administrateurs. Par exemple, les routeurs et les serveurs sont souvent administrés par des groupes d'individus différents, de sorte que la configuration d'un routeur avec les paramètres du serveur peut exiger une collaboration des groupes.

2. Si le besoin est de configurer un ensemble de serveurs interchangeables ou de sélectionner un serveur particulier qui satisfasse un ensemble de critères. Voir paragraphe 3.2.

3. Si la ou les adresses IP, ou le ou les noms, doivent être configurés. Voir paragraphe 3.3.

4. Si la ou les adresses IP sont configurées, si les adresses IPv4 et l'IPv6 doivent être configurées simultanément ou séparément. Voir paragraphe 3.4.

5. Si le paramètre est par interface ou par hôte. Par exemple, les protocoles de configuration tels que DHCP s'exécutent sur la base de l'interface et sont donc plus appropriés pour les paramètres par interface.

6. Comment la configuration par interface affecte-t-elle le comportement à l'échelle de l'hôte ? Par exemple, si l'hôte doit sélectionner un sous-ensemble des configurations par interface ou si les configurations doivent être fusionnées, et s'il en est ainsi, comment cela est fait. Voir paragraphe 3.5.

3.2. Relation entre la configuration IP et le service de découverte

La configuration de la couche supérieure inclut souvent la configuration des adresses du serveur. La question qui se pose est : comment diffère-t-elle de la "découverte du service" comme fournit par les protocoles de découverte de service tels que le "Protocole d'emplacement du service, version 2 (SLPv2)" [RFC 2608] ou la "Découverte du service DNS (DNS-SD)" [DNS-SD].

Dans les mécanismes de configuration de l'hôte Internet tels que le protocole DHCP, si plusieurs instances de serveur sont fournies, elles sont considérées comme interchangeables. Par exemple, dans une liste de serveurs de l'heure, les serveurs sont considérés comme interchangeables puisqu'ils fournissent tous exactement le même service en vous indiquant l'heure actuelle. Dans une liste de serveurs DNS de mise en antémémoire locale, les serveurs sont considérés comme interchangeables puisqu'ils doivent tous donner la même réponse aux interrogations du DNS. D'autre part, dans les protocoles de découverte de service, un hôte souhaite trouver un serveur qui satisfasse un ensemble particulier de critères pouvant varier selon la demande. Lorsqu'un document est imprimé, ce n'est pas la casse, que toutes les imprimantes vont respecter, mais la vitesse, les capacités et l'emplacement physique de l'imprimante qui ont de l'importance pour l'utilisateur.

Les informations acquises via le protocole DHCP sont généralement acquises une fois, au moment du démarrage, et ensuite, elles peuvent n'être mises à jour que peu fréquemment (par exemple, lors du renouvellement du contrat DHCP) voire pas du tout. Ceci rend le protocole DHCP approprié pour des informations qui sont relativement statiques et constantes sur ces intervalles de temps. La découverte au moment de l'amorçage des adresses de serveur est appropriée pour les types de services où il y a un nombre réduit de serveurs interchangeables qui sont intéressants pour un grand nombre de clients. Par exemple, faire la liste des serveurs de l'heure dans un paquet DHCP est approprié puisqu'une organisation ne peut généralement avoir que deux ou trois serveurs de l'heure et que la plupart des hôtes pourront utiliser ce service. Faire la liste de toutes les imprimantes ou serveurs de fichiers d'une entreprise est beaucoup moins utile puisqu'elle peut contenir des centaines ou des milliers d'entrées, et sur un jour donné, un utilisateur donné peut n'utiliser aucune imprimante de cette liste.

Les protocoles de découverte du service peuvent prendre en charge la découverte des serveurs sur Internet et pas seulement ceux dans le domaine administratif local. Par exemple, voir "Découverte du service à distance dans le protocole d'emplacement du service (SLP) via DNS SRV" [RFC 3832] et la découverte du service fondée sur le DNS [DNS-SD]. D'autre part, les mécanismes de configuration de l'hôte Internet tels que le protocole DHCP supposent généralement que le ou les serveurs du domaine administratif local contiennent l'ensemble des informations faisant autorité.

Pour le problème de la découverte du service (c'est-à-dire là où les critères varient sur la base de la requête, même à partir du même hôte), les protocoles devraient être auto découverts (si le partage de sort est critique) ou utiliser un mécanisme de découverte de service d'usage général.

Afin d'éviter une dépendance à l'acheminement en diffusion groupée, il est nécessaire qu'un hôte limite la découverte aux services sur la liaison locale ou découvre l'emplacement d'un agent d'annuaire (DA). Étant donné que le DA peut n'être pas disponible sur la liaison locale, la découverte du service au-delà de la liaison locale est généralement dépendante d'un mécanisme pour la configuration de l'adresse ou du nom du DA. Par conséquent, on ne peut généralement pas se fier aux protocoles de découverte de service pour l'obtention d'une configuration de base de la couche Internet, bien qu'ils puissent être utilisés pour obtenir des paramètres de configuration de la couche supérieure.

3.2.1. Partage de sort

Si un serveur (ou un ensemble de serveurs) est requis pour obtenir un ensemble de paramètres de configuration, "le partage de sort" (paragraphe 2.3 de la [RFC 1958]) est préservé si ces paramètres sont de ceux qui ne peuvent pas être profitablement utilisés sans que ces serveurs soient disponibles. Dans ce cas, réussir à obtenir ces paramètres par d'autres moyens n'a que peu d'avantage s'ils ne peuvent pas être utilisés puisque les serveurs requis ne sont pas disponibles. La possibilité que des informations incorrectes soient configurées est réduite s'il n'y a qu'une machine faisant autorité pour les informations (c'est-à-dire qu'il n'y a aucun besoin de garder synchronisés plusieurs serveurs d'autorité). Par exemple, l'acquisition de passerelle par défaut via des annonces de routeur fournit un parfait partage de sort. C'est-à-dire que les adresses de passerelle peuvent être obtenues si et seulement si elles peuvent être effectivement utilisées. De la même manière, l'obtention de la configuration du serveur DNS à partir d'un serveur DNS fournit un partage de sort puisque la configuration ne peut être obtenue que si le serveur DNS est disponible.

Bien que le partage de sort soit une propriété recommandée du mécanisme de configuration, dans certaines situations, il peut être impossible. Lorsqu'il est utilisé pour découvrir des services sur la liaison locale, les protocoles de découverte du service fournissent généralement le partage de sort, puisque les hôtes qui donnent des informations de service fournissent également les services. Cependant, ce n'est plus le cas lorsque la découverte de service est assistée par un agent d'annuaire (DA). Tout d'abord, la liste des serveurs opérationnels du DA peut ne pas être actuelle, il est donc possible que le DA fournisse aux clients des informations de service qui sont obsolètes. Par exemple, une réponse de DA à une interrogation de découverte de service d'un client peut contenir des informations périmées à propos de serveurs qui ne sont plus opérationnels. De la même manière, des serveurs introduits récemment peuvent ne pas s'être encore enregistrés eux-mêmes auprès du DA. De plus, l'utilisation d'un DA pour la découverte de service introduit également une dépendance selon que le DA est opérationnel ou non, bien qu'il ne soit généralement pas impliqué dans la livraison du service.

Des limitations similaires existent pour d'autres mécanismes de configuration fondés sur le serveur, tel que le protocole DHCP. Les serveurs DHCP ne vérifient généralement pas l'actualité des informations qu'ils fournissent et ne découvrent pas automatiquement de nouvelles informations de configuration. Par conséquent, il n'est pas garanti que les informations de configurations soient actuelles.

Le paragraphe 3.3 de la RFC 4339, "Approches de configuration d'informations de serveur DNS d'hôte IPv6" examine l'utilisation des adresses d'envoi à la cantonade bien connues pour la découverte des

serveurs DNS. L'utilisation des adresses d'envoi à la cantonade permet le partage de sort, même là où l'adresse d'envoi à la cantonade est fournie par un serveur non associé. Cependant, afin d'être universellement utile, cette approche exigerait l'allocation d'une ou plusieurs adresses d'envoi à la cantonade bien connues pour chaque service. La configuration de plus d'une adresse d'envoi à la cantonade est souhaitable pour permettre au client de récupérer plus rapidement qu'il ne serait possible à partir d'une convergence de protocole de routage.

3.3 Découvrir les noms ou bien les adresses

Dans la découverte de serveurs autres que les serveurs de résolution de noms, il est possible de découvrir les adresses IP du ou des serveurs, ou de découvrir les noms, ces deux solutions pouvant se résoudre en une liste d'adresses.

Il est en général plus efficace d'obtenir directement la liste d'adresses puisque cela permet d'éviter les étapes supplémentaires de résolution de noms et la latence qui l'accompagne. D'autre part, là où les serveurs sont mobiles, la liaison nom-adresse peut changer, ce qui requiert l'obtention d'un nouvel ensemble d'adresses. Là où le mécanisme de configuration ne prend pas en charge le partage de sort (par exemple, protocole DHCP) fournir un nom plutôt qu'une adresse peut simplifier le fonctionnement, en supposant que la nouvelle adresse du serveur est mise à jour manuellement ou automatiquement dans le DNS ; dans ce cas, il n'est pas nécessaire de refaire la configuration de paramètre, puisque le nom est toujours valide. Là où le partage de sort est pris en charge (par exemple, dans les protocoles de découverte de service) une nouvelle adresse peut être obtenue en réinitialisant la configuration de paramètre.

Pour fournir les adresses IP pour un ensemble de serveurs, il est recommandé de distinguer à quel serveur appartiennent ces adresses IP. Si l'adresse IP d'un serveur est inaccessible, cela permet à l'hôte d'essayer l'adresse IP d'un autre serveur, plutôt qu'une autre adresse IP du même serveur, au cas où le serveur est en panne. Cela peut être rendu possible en distinguant quelles adresses appartiennent au même serveur.

3.4. Problèmes de double pile

Une raison en faveur de l'acquisition d'une liste d'adresses de serveur interchangeables est la tolérance de panne, au cas où un ou plusieurs serveurs ne répondent pas. Les hôtes essaieront normalement les adresses à tour de rôle, en ne tentant d'utiliser la seconde adresse et les suivantes dans la liste que si la première ne parvient pas à répondre assez rapidement. Dans de tels cas, une liste organisée selon la probabilité de succès attendue aidera les clients à avoir des résultats plus rapidement. Pour les hôtes qui prennent en charge IPv4 et IPv6, il est recommandé d'obtenir les adresses des serveurs IPv4 et IPv6 dans une unique liste. L'obtention des adresses IPv4 et IPv6 dans des listes séparées, sans indication des serveurs auxquels elles correspondent exige que l'hôte utilise une heuristique pour fusionner les listes.

Par exemple, supposons qu'il y a deux serveurs, A et B, chacun avec une adresse IPv4 et une adresse IPv6. Si la première adresse que l'hôte essaye est l'adresse IPv6 du serveur A, la seconde adresse que l'hôte essaye si la première échoue sera généralement l'adresse IPv4 du serveur B. Ceci puisque l'échec de la première adresse peut être dû au serveur A qui est en panne ou à un certain problème

avec l'adresse IPv6 de l'hôte ou encore un problème de connectivité au serveur A. La tentative de l'adresse IPv4 suivante est préférable puisque l'accessibilité de l'adresse IPv4 est indépendante de toutes ces causes d'échec éventuelles.

Si la liste des adresses de serveurs IPv4 devait être obtenue séparément de la liste des adresses de serveurd IPv6, un hôte essayant de fusionner les listes ne saurait pas quelles adresses IPv4 appartiennent au même serveur que l'adresse IPv6 qu'il vient juste d'essayer. Ceci peut être résolu en distinguant explicitement à quel serveur appartiennent ces adresses ou, plus simplement, en configurant l'hôte avec une liste combinée des adresses IPv4 et IPv6. Noter qu'un problème identique peut être soulevé avec tous les mécanismes (par exemple, DHCP, DNS, etc.) pour obtenir les adresses de serveur IP.

La configuration d'une liste combinée des adresses IPv4 et IPv6 donne au mécanisme de configuration le contrôle de l'ordre des adresses, plutôt que de configurer on de noms et permet au résolveur de l'hôte de déterminer le classement de la liste d'adresse. Voir "Protocole de configuration dynamique de l'hôte (DHCP): problèmes de double pile IPv4 et IPv6" [RFC4477] pour plus d'explication sur les problèmes de double pile dans le contexte du protocole DHCP.

3.5. Relation entre la pré-interface et la pré-configuration de l'hôte

Les paramètres qui sont configurés ou acquis sur la base d'une pré-interface peuvent affecter le comportement de l'hôte dans son ensemble. Là où seule une configuration peut être appliquée à l'hôte, l'hôte peut avoir besoin de prioriser les informations de la configuration de la pré-interface d'une certaine manière (par exemple, de la plus fiable à la moins fiable). Si l'hôte a besoin de fusionner la configuration de la pré-interface pour produire une large configuration d'hôte, il peut avoir besoin de prendre l'union des paramètres de la pré-configuration de l'hôte et de les classer d'une certaine manière (par exemple, de l'interface la plus rapide à la moins rapide). La procédure à appliquer et la manière dont elle est accomplie peuvent varier selon le paramètre configuré. Les exemples sont les suivants :

Configuration du service de démarrage
Bien que la configuration du service de démarrage soit fournie sur de multiples interfaces, un hôte donné peut être limité dans le nombre de charges de démarrage qu'il peut manipuler simultanément. Par exemple, un hôte qui ne prend pas en charge la virtualisation ne peut traiter qu'une seule charge de démarrage à la fois ou un hôte qui prend en charge N machines virtuelles ne peut manipuler que N charges de démarrages simultanément. Par conséquent, un hôte peut avoir besoin de sélectionner les charges de démarrage sur lesquelles il va agir, hors celles qui sont configurées sur la base d'une pré-interface. Il est nécessaire pour cela que l'hôte les priorisent (par exemple, de la plus fiable à la moins fiable).

Configuration du service de noms
Bien que la configuration du service de noms soit fournie sur la base d'une pré-interface, la configuration de résolution de noms affectera généralement le comportement de l'hôte dans son ensemble. Par exemple, étant donné la configuration des adresses du serveur DNS et les paramètres de la liste de recherche sur chaque interface, l'hôte détermine quelle séquence de demandes de service de noms est à envoyer sur ces interfaces.

Étant donné que les algorithmes utilisés pour déterminer le pré-comportement de l'hôte sur la base d'une configuration de pré-interface peuvent affecter l'interopérabilité, il est important que ces algorithmes soient compris par les programmateurs. Par conséquent, nous recommandons que les documents définissant les mécanismes de la pré-interface pour l'acquisition d'une pré-configuration de l'hôte (par exemple, options de l'annonce de routage DHCP ou IPv6) incluent un guide sur la manière de traiter de multiples interfaces. Il peut inclure des analyses des éléments suivants :

1. Fusion. Comment les configurations de pré-interface sont-elles combinées pour produire une pré-configuration de l'hôte ? Une seule configuration est-elle sélectionnée ou est-ce que l'union des configurations est choisie ?

2. Priorisation. Les configurations de pré-interface sont-elles priorisées dans le processus de fusion ? Si oui, quelles sont les considérations à prendre en compte en priorisation ?

4. Considérations de sécurité

La configuration sécurisée de l'IP présente de nombreux défis. En plus des attaques par déni de service et de l'intercepteur, les attaques sur les mécanismes de configuration peuvent cibler des paramètres particuliers. Par exemple, les personnes malveillantes peuvent cibler la configuration du serveur DNS afin de prendre en charge les attaques d'hameçonnage ou de pharming ultérieures telles que celles décrites dans "Nouveau cheval de Troie dans le détournement de masse du DNS" [DNSTrojan]. De nombreux problèmes existent avec plusieurs types de paramètres, comme examiné dans la section 2.6 et 4.2.7 de la RFC 3756 "Modèles fiables et menaces de la découverte du voisin IPv6 (ND)", la section 1.1 de la RFC 3118 "Authentification pour messages DHCP" et la section 23 de la RFC 3315 "Protocole de configuration dynamique de l'hôte pour IPv6 (DHCPv6)". Étant donné les éventuelles vulnérabilités, les hôtes limitent souvent leur prise en charge pour les options DHCP au minimum requis pour fournir une configuration TCP/IP de base.

Étant donné que la configuration de démarrage détermine l'image de démarrage que l'hôte doit exécuter, une attaque réussie sur la configuration de démarrage pourrait provoquer l'acquisition complète du contrôle d'un hôte par une personne malveillante. Par conséquent, il est particulièrement important que la configuration de démarrage soit sécurisée. Les approches de sécurité de la configuration de démarrage sont décrites dans la RFC 4173 "Amorçage des clients utilisant le protocole de l'interface SCSI" et "Spécification de l'environnement d'exécution pré-démarrage (PXE)" [PXE].

4.1. Authentification de configuration

Les techniques disponibles pour sécuriser la configuration de la couche Internet sont limitées. Bien qu'il soit techniquement possible d'exécuter un sous-ensemble très limité d'opérations de mise en réseau IP sans adresse IP, les capacités sont sérieusement limitées. Un hôte sans adresse IP ne peut pas recevoir de paquets IP en envoi individuel conventionnels, seulement des paquets IP envoyés à l'adresse de diffusion ou de diffusion groupée. La configuration de l'adresse IP permet l'utilisation de la fragmentation IP. Les paquets envoyés à partir d'une adresse inconnue ne peuvent pas être rassemblés de manière fiable puisque les fragments d'hôtes multiples utilisant l'adresse inconnue peuvent être rassemblés dans un seul paquet IP. Sans adresse IP, il est impossible de bénéficier des

installations de sécurité tel que IPsec, défini dans la RFC 4301 "Architecture de sécurité pour le protocole Internet" ou la RFC 5246 "Protocole de sécurité de la couche transport (TLS)".

Par conséquent, la sécurité de la configuration est généralement implémentée dans les protocoles de configuration eux-mêmes.

Le PPP [RFC 1661] ne prend pas en charge la négociation sécurisée dans l'IPv4CP [RFC 1332] ou l'IPv6CP [RFC 5072], permettant à la personne malveillante avec accès à la liaison de faire échouer la négociation. Par contre, l'IKEv2 [RFC 4306] fournit un chiffrement, une intégrité et une protection de relecture pour les échanges de configuration.

Là où l'on s'attend à ce que les paquets de configurations soient uniquement formés sur des liaisons particulières ou à partir d'hôtes particuliers, le filtrage peut aider à contrôler l'usurpation de configuration. Par exemple, un point d'accès sans fil n'a habituellement aucune raison d'envoyer des paquets DHCP DISCOVER en diffusion à ses clients sans fil, et doit habituellement supprimer tout paquet DHCP OFFER reçu de ces clients sans fil puisqu'en général, on doit demander aux clients sans fil des adresses à partir du réseau, sans les offrir. Afin d'éviter l'usurpation, la communication entre l'agent de relais DHCP et les serveurs doit être authentifiée et l'intégrité doit être protégée en utilisant un mécanisme tel que IPsec.

Les mécanismes de configuration sécurisée de la couche Internet incluent la découverte sécurisée du voisin (SEND) [RFC 3971] pour la configuration de l'adresse IPv6 sans état [RFC 4862] ou l'authentification DHCP pour la configuration de l'adresse avec état. Le protocole DHCPv4 [RFC 2131] n'incluait pas au départ la prise en charge de la sécurité, elle a été ajoutée dans la RFC 3118 "Authentification pour les messages DHCP" [RFC 3118]. Le protocole DHCPv6 [RFC 3315] comprend la prise en charge de la sécurité, cependant, l'authentification n'est pas largement implémentée pour le DHCPv4 ou le DHCPv6.

La configuration de la couche supérieure peut faire usage d'une grande variété de techniques de sécurité. Lorsque l'authentification DHCP est prise en charge, les paramètres de configuration de la couche supérieure fournis par le protocole DHCP peuvent être sécurisés. Cependant, même si un hôte ne prend pas en charge l'authentification DHCPv6, la configuration de la couche supérieure via DHCPv6 avec état [RFC3736] peut encore être sécurisée avec IPsec.

D'éventuelles exceptions peuvent exister là où les installations de sécurité ne sont pas disponibles dans le processus de démarrage. Il peut être difficile de sécuriser une configuration de démarrage même une fois que la couche Internet a été configurée, si les fonctionnalités de sécurité ne sont pas disponibles après que la configuration de démarrage est terminée. Par exemple, il est possible que Kerberos, IPsec ou TLS ne soient plus disponibles d'ici là dans le processus de démarrage, voir la RFC 4173 "Amorçage des clients utilisant le protocole de l'interface ISCSI") pour plus d'explications.

Là où le chiffrement par clé publique est utilisé pour authentifier et protéger l'intégrité de la configuration, les hôtes doivent être configurés avec des ancrages fiables afin de valider les messages de configuration reçus. Pour un nœud qui visite de multiples domaines administratifs, l'acquisition d'ancrages fiables peut s'avérer difficile.

5. Références pour information

[3GPP-24.008] 3GPP TS 24.008 V5.8.0, "Spécification de la couche d'interface radio mobile 3, protocoles de réseau principal, étape 3 (5ème Publication)", juin 2003.

[DNSTrojan] Goodin, D., "Nouveau cheval de Troie dans le détournement de masse du DNS" The Register, 5 décembre 2008, http://www.theregister.co.uk/2008/12/05/ new_dnschanger_hijacks/

[IEN116] J. Postel, "Serveur de noms Internet", IEN 116, août 1979, http://www.ietf.org/rfc/ien/ien116.txt

[IEEE-802.1X] Institut des ingénieurs électriciens et électroniciens, "Réseaux local et métropolitain : contrôleur d'accès réseau par port", IEEE Standard 802.1X-2004, décembre 2004.

[DNS-SD] Cheshire, S. et M. Krochmal, "Découverte du service fondée sur le DNS", travail en cours, septembre 2008.

[mDNS] Cheshire, S. et M. Krochmal, "DNS en diffusion groupée", travail en cours, septembre 2008.

[PXE] Henry, M. et M. Johnston, "Spécification de l'environnement d'exécution pré-démarrage(PXE)", septembre 1999, http://www.pix.net/software/pxeboot/archive/pxespec.pdf

[RFC 768] Postel, J., "Protocole UDP/IP", STD 6, août 1980.

[RFC 1001] Groupe de travail NetBIOS de l'Agence des Projets de Recherche Avancée de Défense, Internet Activities Board et End- to-End Services Task Force, "Protocole standard pour un service NetBIOS sur un transport TCP/UDP : concepts et méthodes", STD 19, mars 1987.

[RFC 1191] Mogul, J.et S. Deering, "Découverte de la MTU de chemin", novembre 1990.

[RFC 1332] McGregor, G., "Le protocole de contrôle d'IP de PPP", mai 1992.

[RFC 1350] Sollins, K., "Le protocole TFTP (Révision 2)", STD 33, juillet 1992.

[RFC 1661] Simpson, W., éd., "Le protocole point à point (PPP)", STD 51, juillet 1994.

[RFC 1877] Cobb, S., "Extensions du protocole du contrôle du protocole Internet PPP pour les adresses de serveur de noms", décembre 1995.

[RFC 1958] Carpenter, B., éd., "Principes de l'architecture de l'Internet", juin 1996.

[RFC 1981] McCann, J., Deering, S. et J. Mogul, "Découverte de la MTU de chemin pour IP version 6", août 1996.

[RFC 2131] Droms, R., "Protocole de configuration dynamique du serveur", mars 1997.

[RFC 2608] Guttman, E., Perkins, C., Veizades, J. et M. Day, "Protocole d'emplacement du service, version2", juin 1999.

[RFC 2923] Lahey, K., "Problèmes TCP avec découverte de la MTU de chemin", septembre 2000.

[RFC 3118] Droms, R., éd. et W. Arbaugh, Ed., "Authentification pour messages DHCP", juin 2001.

[RFC 3315] Droms, R., éd., Bound, J., Volz, B., Lemon, T., Perkins, C. et M. Carney, "Protocole de configuration dynamique de l'hôte pour IPv6 (DHCPv6)", juillet 2003.

[RFC 3344] Perkins, C., éd., "Prise en charge de la mobilité IP pour IPv4", août 2002.

[RFC 3397] Aboba, B.et S. Cheshire, "Option de recherché du domaine du protocole DHCP", novembre 2002.

[RFC3456] Patel, B., Aboba, B., Kelly, S. et V. Gupta, "Protocole de configuration dynamique (DHCPv4) Configuration du mode tunnel IPsec", janvier 2003.

[RFC3530] Shepler, S., Callaghan, B., Robinson, D., Thurlow, R., Beame, C., Eisler, M. et D. Noveck, "Protocole de système de fichier réseau (NFS) version 4", avril 2003.

[RFC3720] Satran, J., Meth, K., Sapuntzakis, C., Chadalapaka, M. et E. Zeidner, "Interface SCSI ", avril 2004.

[RFC 3736] Droms, R., "Service pour IPv6 du protocole DHCP sans état", avril 2004.

[RFC 3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J.et H. Levkowetz, Ed., "Protocole extensible d'authentification", juin 2004.

[RFC 3756] Nikander, P., Ed., Kempf, J.et E. Nordmark, "Modèles fiables et menaces de la découverte du voisin IPv6 (ND)", mai2004.

[RFC 3775] Johnson, D., Perkins, C. et J. Arkko, "Prise en charge de la mobilité IPv6", juin 2004.

[RFC 3818] Schryver, V., "Considérations IANA pour le protocole PPP", BCP 88, juin 2004.

[RFC 3832] Zhao, W., Schulzrinne, H., Guttman, E., Bisdikian, C. et W. Jerome, "Découverte du service à distance dans le protocole d'emplacement du service via DNS SRV", juillet 2004.

[RFC 3898] Kalusivalingam, V., "Options de configuration du service d'information réseau (NIS) pour le protocole DHCP pour IPv6 (DHCPv6)", octobre 2004.

[RFC 3927] Cheshire, S., Aboba, B. et E. Guttman, "Configuration dynamique des adresses locales de liaison d'IPv4", mai 2005.

[RFC 3971] Arkko, J., Ed., Kempf, J., Zill, B. et P. Nikander, « Découverte sécurisée du voisin (SEND) », RFC 3971, mars 2005.

[RFC 3972] Aura, T., "Adresses générées cryptographiquement (CGA)", mars 2005.

[RFC 4171] Tseng, J., Gibbons, K., Travostino, F., Du Laney, C. et J. Souza, « Service de noms de mémorisation sur Internet (iSNS)", septembre 2005.

[RFC 4173] Sarkar, P., Missimer, D. et C. Sapuntzakis, "Amorçage des clients utilisant le protocole de l'interface SCSI", septembre 2005.

[RFC 4174] Monia, C., Tseng, J. et K. Gibbons, "Option de protocole DHCP IPv4 pour le service de noms de mémorisation sur Internet", septembre 2005.

[RFC 4301] Kent, S. et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005.

[RFC 4306] Kaufman, C., éd., "Protocole d'échange de clés Internet version 2 (IKEv2)", décembre 2005.

[RFC 4339] Jeong, J., éd., "Approches de la Configuration IPv6 des informations du serveur DNS", février 2006.

[RFC 4477] Chown, T., Venaas, S. et C. Strauf, "Protocole de configuration dynamique de l'hôte (DHCP): problèmes de double pile IPv4 et IPv6", mai 2006.

[RFC 4578] Johnston, M. et S. Venaas, éd., "Options du protocole DHCP pour l'environnement d'exécution de pré-démarrage Intel (PXE)", novembre 2006.

[RFC 4795] Aboba, B., Thaler, D. et L. Esibov, "Résolution de noms multidiffusion de liaison locale (LLMNR)", janvier 2007.

[RFC 4821] Mathis, M.et J. Heffner, "Découverte de la MTU de chemin de la couche de dépaquetage", mars 2007.

[RFC 4862] Thomson, S., Narten, T. et T. Jinmei, "Configuration automatique de l'adresse IPv6 sans état", septembre 2007.

[RFC 4941] Narten, T., Draves, R. et S. Krishnan, "Extensions de confidentialité pour la configuration automatique de l'adresse IPv6 sans état", septembre 2007.

[RFC 5072] Varada, S., Ed., Haskins, D. et E. Allen, "IP Version 6 sur PPP", septembre 2007.

[RFC 5246] Dierks, T.et E. Rescorla, "Protocole sécurité de la couche transport (TLS) version 1.2". août 2008.

[STD3] Braden, R., éd., "Exigences pour les hôtes Internet-couches de communication", STD 3, RFC 1122, octobre 1989.
Braden, R., éd., "Exigences pour les hôtes Internet-application et prise en charge", STD 3, RFC 1123, octobre 1989.

Annexe A. Remerciements

Elwyn Davies, Bob Hinden, Pasi Eronen, Jari Arkko, Pekka Savola, James Kempf, Ted Hardie, et Alfred Hoenes ont fourni des données de valeur pour ce document.

Annexe B. Membres de l'IAB au moment de la rédaction

Loa Andersson
Gonzalo Camarillo
Stuart Cheshire
Russ Housley
Olaf Kolkman
Gregory Lebovitz
Barry Leiba
Kurtis Lindqvist
Andrew Malis
Danny McPherson
David Oran
Dave Thaler
Lixia Zhang

Adresse des auteurs

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
Email : bernarda@microsoft.com

Dave Thaler
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
Email : dthaler@microsoft.com

Loa Andersson
Ericsson AB
Email : loa.andersson@ericsson.com

Stuart Cheshire
Apple Computer, Inc.
1 Infinite Loop
Cupertino, CA 95014
Email : cheshire@apple.com