

Groupe de travail Réseau
Request for Comments : 4173
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

P. Sarkar, IBM
D. Missimer, Hewlett-Packard Company
C. Sapuntzakis, Stanford University
septembre 2005

Clients d'amorçage qui utilisent le protocole d'interface de système de petit ordinateur sur Internet (iSCSI)

Statut de ce mémoire

Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de copyright

Copyright (C) The Internet Society (2005).

Résumé

L'interface de système de petit ordinateur sur Internet (iSCSI, *Internet Small Computer System Interface*) est une proposition de protocole de transport pour l'interface de système de petit ordinateur (SCSI, *Small Computer Systems Interface*) qui fonctionne par dessus TCP. Le présent mémoire décrit un mécanisme standard pour permettre aux clients de s'amorcer en utilisant le protocole iSCSI. Le but de cette norme est de permettre aux clients d'amorcer iSCSI pour obtenir les informations permettant d'ouvrir une session iSCSI avec le serveur d'amorçage iSCSI.

1. Introduction

L'interface de système de petit ordinateur (SCSI) est une famille de protocoles populaire pour communiquer avec des appareils marche/arrêt, en particulier des appareils de mémorisation. SCSI peut être caractérisé comme un protocole de messages de demande/réponse avec une architecture standard et des ensembles de commandes à composants pour les différentes classes d'appareils.

iSCSI est un protocole de transport proposé pour SCSI qui fonctionne par dessus TCP. Le rôle de iSCSI est rendu nécessaire par l'évolution de l'interconnexion des systèmes à partir d'un bus partagé vers un réseau commuté. Les réseaux IP satisfont aux exigences d'architecture et de performances du transport de SCSI, ouvrant la voie au protocole iSCSI.

De nombreux clients sans disque dur s'amorcent parfois à partir d'appareils SCSI distants. De telles entités sans disque dur sont légères, efficaces en espace et en consommation d'énergie et sont de plus en plus populaires dans divers environnements.

Le présent mémoire décrit un mécanisme standard pour permettre aux clients de s'amorcer en utilisant le protocole iSCSI. Le but de cette norme est de permettre aux clients d'amorçage iSCSI d'obtenir les informations pour ouvrir une session iSCSI avec le serveur d'amorçage iSCSI. Il est possible que toutes les informations ne soient pas disponibles à ce moment précis, de sorte que ce mémoire décrit les étapes pour obtenir les informations requises pour que les clients s'amorcent à partir d'un serveur d'amorçage iSCSI.

1.1 Mots-clés

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].

2. Exigences

1. Il ne doit pas y avoir de restrictions à la topologie du réseau entre le client d'amorçage iSCSI et le serveur d'amorçage autres que celles existant pour établir la session iSCSI. Par conséquent, il est possible qu'un client d'amorçage iSCSI

s'amorce auprès d'un serveur d'amorçage iSCSI derrière des passerelles ou pare-feu pour autant qu'il est possible d'établir une session iSCSI entre le client et le serveur.

2. Ce qui suit représente le minimum d'informations requises pour qu'un client d'amorçage iSCSI contacte un serveur d'amorçage iSCSI : (a) l'adresse IP du client (IPv6 ou IPv4) ; (b) le nom de cible iSCSI du serveur; et (c) les capacités obligatoires d'initiateur iSCSI.

Les exigences ci-dessus supposent que le numéro d'unité logique (LUN, *Logical Unit Number*) par défaut pour le processus d'amorçage est 0 et que l'accès par défaut pour le serveur d'amorçage iSCSI est l'accès iSCSI bien connu [RFC3720]. Cependant, tous deux peuvent être écrasés au moment de la configuration.

Des informations supplémentaires peuvent être exigées à chaque étape du processus d'amorçage.

3. Il est possible que le client d'amorçage iSCSI n'ait aucune des informations ou capacités ci-dessus au démarrage.
4. Le client devrait être capable de réaliser l'amorçage sans intervention de l'utilisateur (pour les amorçages qui surviennent durant une mise sous tension inattendue). Cependant, il devrait y avoir un mécanisme pour que l'utilisateur entre des valeurs qui court-circuitent les étapes du protocole d'amorçage.
5. Un logiciel de protocole supplémentaire (par exemple, BOOTP ou DHCP) peut être nécessaire si les informations minimum requises pour une session iSCSI ne sont pas fournies.

3. Travaux connexes

Le protocole de résolution d'adresse inverse (RARP, *Reverse Address Resolution Protocol*) [RFC0903] à travers les extensions définies dans le RARP dynamique (DRARP, *Dynamic RARP*) [RFC1931] traite explicitement le problème de la découverte d'adresse réseau, et inclut un mécanisme automatique d'allocation d'adresse IP. Le protocole trivial de transfert de fichier (TFTP, *Trivial File Transfer Protocol*) [RFC1350] assure le transport d'une image d'amorçage à partir d'un serveur d'amorçage. BOOTP [RFC0951], [RFC1497], [RFC1542] est un mécanisme de transport pour une collection d'informations de configuration. BOOTP est aussi extensible, et des extensions officielles ont été définies pour plusieurs paramètres de configuration. DHCPv4 [RFC2131], [RFC1534] et DHCPv6 [RFC3315] sont des normes par lesquelles les hôtes sont configurés de façon dynamique dans un réseau IP. Le protocole de localisation de service (SLP, *Service Location Protocol*) assure la localisation de services de niveau supérieur [RFC2608].

4. Étape logicielle

Certains clients d'amorçage iSCSI peuvent manquer des ressources pour s'amorcer avec la capacité d'initiateur iSCSI obligatoire. De tels clients d'amorçage peuvent choisir d'obtenir un logiciel d'initiateur iSCSI d'un serveur d'amorçage. Actuellement, de nombreux protocoles établis permettent un tel service afin de permettre aux clients de télécharger des images de logiciel. Par exemple, les serveurs BOOTP et DHCP ont la capacité de fournir les localisations de serveurs qui peuvent servir des images de logiciel à la demande des clients d'amorçage.

Noter que le présent document ne recommande aucun des protocoles ci-dessus, et la décision finale du choix du protocole d'amorçage à utiliser pour charger un logiciel d'initiateur iSCSI est laissée à la discrétion de la mise en œuvre.

5. Étape DHCP

Pour utiliser un serveur d'amorçage iSCSI, les éléments d'information suivants sont requis pour un client d'amorçage iSCSI.

- L'adresse IP du client d'amorçage iSCSI (IPv4 ou IPv6)
- Le point d'extrémité de transport IP pour l'accès de cible iSCSI pour le serveur d'amorçage iSCSI. Si le transport est TCP, par exemple, cela doit se résoudre en une adresse IP et un numéro d'accès TCP. TCP est actuellement le seul transport approuvé pour iSCSI.
- La structure de LUN de huit octets qui identifie l'unité logique au sein du serveur d'amorçage iSCSI.

Au moment de l'amorçage, toutes ces informations, ou aucune, peuvent être mémorisées dans le client d'amorçage iSCSI. Cette section décrit les techniques pour obtenir les informations requises via l'étape DHCP. Autrement, si le client d'amorçage iSCSI a toutes les informations, il procède directement à l'étape d'amorçage.

Un client d'amorçage iSCSI qui ne connaît pas son adresse IP à la mise sous tension peut l'acquérir via BOOTP ou DHCP (v4 ou v6), ou via l'autoconfiguration d'adresse IPv6. Noter que les réglages DHCP (comme les réglages RA dans DHCPv6) peuvent interdire l'utilisation de DHCP pour distribuer les informations d'amorçage iSCSI ; dans ce cas, l'étape DHCP ne peut pas être utilisée.

Sauf spécification contraire, les champs BOOTP ou DHCP comme l'identifiant de client et les informations de passerelle sont utilisées d'une façon identique à celle des applications autres que iSCSI.

Un serveur BOOTP ou DHCP (v4 ou v6) PEUT donner à un client iSCSI les instructions pour atteindre son appareil d'amorçage. Cela se fait en utilisant l'option de longueur variable appelée "Chemin racine" [RFC2132], [RFC1497]. L'utilisation de ce champ d'option est réservée à l'utilisation de l'amorçage iSCSI en faisant précéder la chaîne de "iscsi:". L'option Chemin racine n'est actuellement pas définie pour DHCPv6 ; si à l'avenir l'option est définie pour DHCPv6, l'utilisation de l'option comme défini pour l'amorçage iSCSI s'appliquera.

Le champ option consiste en une chaîne UTF-8 [RFC3629]. La chaîne a la composition suivante :

```
"iscsi:"<nomDeServeur>":"<protocole>":"<accès>":"<LUN>":"<nomDeCible>
```

Les champs "nomDeServeur", "accès", "protocole", et "LUN" sont FACULTATIFS et devraient être laissés en blanc si il n'y a pas de valeur correspondante. Le champ "nomDeCible" n'est pas facultatif et DOIT être fourni.

Le "nomDeServeur" est le nom du serveur iSCSI et contient un nom de domaine valide, une adresse IPv4 littérale, ou une adresse IPv6 littérale. Le nomDeServeur doit suivre les spécifications du paragraphe 3.2.2 de la spécification d'URI [RFC3986], les caractères admis doivent aussi se conformer au paragraphe 2.2 de cette même spécification. La compression de nomDeServeur NE DOIT PAS être utilisée dans ce champ.

Le champ "protocole" est la représentation en décimal de la chaîne approuvée par l'IANA pour le protocole de transport à utiliser pour iSCSI. Si le champ Protocole est laissé en blanc, la valeur par défaut est supposées être "6" pour TCP. Le protocole de transport DOIT avoir été approuvé pour l'usage de iSCSI ; actuellement, le seul protocole approuvé est TCP.

Le champ "accès" est la représentation en décimal de l'accès sur lequel le serveur d'amorçage iSCSI écoute. Si il n'est pas spécifié, l'accès par défaut est l'accès iSCSI bien connu (3260) [RFC3720].

Le champ "LUN" est une représentation hexadécimale du numéro de LU. Si le champ LUN est blanc, LUN 0 est alors supposé. Si le champ LUN n'est pas blanc, la représentation DOIT être divisée en quatre groupes de quatre chiffres hexadécimaux, séparés par "-". Les chiffres au delà de 9 peuvent être en majuscule ou minuscules. Un exemple d'une telle représentation serait 4752-3A4F-6b7e-2F99. Dans un souci de concision, au plus trois zéros ("0") en tête PEUVENT être omis dans tout groupe de chiffres hexadécimaux. Donc, la représentation de "LUN" 6734-9-156f-127 est équivalente à 6734-0009-156f-0127. De plus, les groupes en queue qui contiennent seulement le chiffre "0" PEUVENT être omis ainsi que le "-" précédent. Ainsi, la représentation de "LUN" 4186-9 est équivalente à 4186-0009-0000-0000. D'autres représentations concises du champ LUN NE DOIVENT PAS être utilisées.

Noter qu'il est permis aux cibles SCSI de présenter des numérotations de LU différentes pour des initiateurs SCSI différents, de sorte qu'à notre connaissance rien n'empêche une cible SCSI d'exporter plusieurs LU différents à plusieurs initiateurs SCSI différents comme leur LUN 0 respectifs.

Le champ "nomDeCible" est un nom iSCSI qui est défini par la norme iSCSI [RFC3720] comme identifiant de façon univoque une cible iSCSI. Les caractères approuvés dans le champ Nom de cible sont énoncés dans le document Profil de chaîne iSCSI [RFC3722].

Si le champ "nomDeServeur" est fourni par BOOTP ou DHCP, ce champ est alors utilisé en conjonction avec les autres champs associés pour contacter le serveur d'amorçage dans l'étape Amorçage (Section 7). Cependant, si le champ "nomDeServeur" n'est pas fourni, le champ "nomDeCible" est alors utilisé dans l'étape Service de découverte en conjonction avec les autres champs associés (Section 6).

6. Étape Service de découverte

Cette étape est requise si le serveur BOOTP ou DHCP (v4 ou v6) ne connaît aucun serveur d'amorçage iSCSI ou si le serveur BOOTP ou DHCP est dans l'incapacité de fournir les informations minimales requises pour connecter au serveur d'amorçage iSCSI, à part le nom de la cible.

Le service de découverte peut se fonder sur le protocole SLP [RFC2608], [RFC4018] et est une instanciation du service SLP ou d'agent de répertoire. Autrement, le service de découverte peut se fonder sur le protocole iSNS [RFC4171] et est une instanciation du serveur iSNS.

Le client d'amorçage iSCSI peut avoir obtenu le nom de la cible du serveur d'amorçage iSCSI dans l'étape DHCP (Section 5). Dans ce cas, le client d'amorçage iSCSI interroge le service de découverte SLP en utilisant la chaîne d'interrogation 1 du gabarit de type de service concret de cible iSCSI, comme spécifié au paragraphe 6.2 du document d'interaction SLP iSCSI [RFC4018], pour résoudre le nom de cible en adresse et numéro d'accès IP. Autrement, le client d'amorçage iSCSI peut interroger le service de découverte iSNS avec une interrogation d'attribut d'appareil en donnant le nom de la cible comme paramètre d'interrogation [RFC4171]. Une fois qu'il est obtenu, le client d'amorçage iSCSI procède à l'étape Amorçage (Section 7).

Il est possible que le numéro d'accès obtenu du service de découverte entre en conflit avec celui obtenu de l'étape DHCP. Dans ce cas, la mise en œuvre a l'option d'essayer les deux numéros d'accès dans l'étape Amorçage.

Si le client d'amorçage iSCSI n'a aucune information sur le nom de la cible, il peut alors interroger le service de découverte SLP avec la chaîne d'interrogation 4 du gabarit de type de service concret de cible iSCSI, comme spécifié au paragraphe 6.2 du document d'interaction SLP iSCSI [RFC4018]. En réponse à cette interrogation, le service de découverte SLP fournit au client d'amorçage une liste des serveurs d'amorçage iSCSI auxquels le client d'amorçage est autorisé à accéder. Autrement, le client d'amorçage iSCSI peut interroger le service de découverte iSNS pour vérifier si les cibles dans un domaine de découverte particulier sont amorçables [RFC4171].

Si la liste des serveurs d'amorçage iSCSI est vide, les actions suivantes sont à la discrétion de la mise en œuvre. Autrement, le client d'amorçage iSCSI peut contacter tout serveur d'amorçage iSCSI de la liste. De plus, l'ordre dans lequel les serveurs d'amorçage iSCSI sont contactés est aussi à la discrétion de la mise en œuvre.

7. Étape d'amorçage

Une fois que le client d'amorçage iSCSI a obtenu les informations minimales pour ouvrir une session iSCSI avec le serveur d'amorçage iSCSI, le processus d'amorçage réel peut commencer.

La séquence réelle de commandes iSCSI qui est nécessaire pour achever le processus d'amorçage est laissée à la discrétion de la mise en œuvre. C'est parce que les exigences diverses des différents fabricants et équipements rendent difficile de spécifier un sous ensemble commun de standard iSCSI acceptable par tous.

La session iSCSI établie pour l'amorçage peut être reprise par le logiciel amorcé dans le client d'amorçage iSCSI.

8. Considérations sur la sécurité

La discussion sur la sécurité est centrée sur la sécurisation de la communication impliquée dans le processus d'amorçage iSCSI.

Cependant, la question de l'application d'accréditifs à une image d'amorçage chargée à travers le mécanisme d'amorçage iSCSI sort du domaine d'application du présent document. Une différence clé entre le mécanisme d'amorçage iSCSI et le chargement d'une image fondée sur BOOTP est le fait que l'identité d'une image d'amorçage peut ne pas être connue quand commence l'étape d'amorçage. L'identité de certaines images d'amorçage et leurs localisations ne sont connues qu'après que le contenu d'un disque d'amorçage exposé par le service d'amorçage iSCSI a été examiné. De plus, les images elles-mêmes peuvent charger de façon récurrente d'autres images fondées sur les configurations de matériel et les entrées de l'utilisateur. Par conséquent, une façon pratique de vérifier les images d'amorçage chargées est de s'assurer que chaque logiciel de chargement d'image vérifie l'image à télécharger en utilisant un mécanisme de son choix.

Les considérations impliquées dans la conception d'une architecture de sécurité pour le processus d'amorçage iSCSI

incluent des considérations de configuration, de déploiement, et de provisionnement en plus des considérations normales de sécurité. Activer l'amorçage iSCSI crée une dépendance fonctionnelle critique à un système externe avec d'évidentes implications de sécurité, et donc la connaissance par l'administrateur de cette activation est extrêmement importante. L'amorçage iSCSI NE DEVRAIT donc PAS être activé ou placé à un rang élevé dans l'ordre d'amorçage sans une action administrative explicite.

Dans toutes les phases du processus d'amorçage, un client doit s'assurer qu'un serveur est autorisé à lui envoyer certaines informations. Cela signifie que l'identité authentifiée d'un serveur doit avoir une indication d'autorisation. Une liste de serveurs autorisés peut être pré configurée dans un client, ou la liste peut être téléchargée sous une forme authentifiée dans une étape antérieure au processus d'amorçage.

L'étape logicielle NE DEVRAIT PAS être impliquée dans un processus d'amorçage iSCSI sécurisé, car cela ajouterait la complexité supplémentaire d'essayer de sécuriser le processus de chargement du logiciel nécessaire pour effectuer les étapes ultérieures de l'amorçage iSCSI. L'authentification et la protection de l'intégrité du logiciel d'amorçage téléchargé se sont révélées difficiles et complexes du fait des problèmes administratifs et des limitations de l'environnement de BIOS. Il est donc supposé que tout le logiciel nécessaire est résident sur le client d'amorçage iSCSI.

Si l'étape DHCP est mise en œuvre en utilisant le protocole DHCP, le client d'amorçage iSCSI DEVRAIT mettre en œuvre l'authentification DHCP ([RFC3118], [RFC3315] pour IPv6). Dans ce cas, une interface d'administration DEVRAIT être fournie pour la configuration des accreditifs d'authentification DHCP, à la fois quand l'interface réseau est sur la carte mère et quand elle est amovible. Noter que l'authentification DHCP ([RFC3118],[RFC3315] pour IPv6) se concentre sur l'authentification intra domaine, qui est supposée être suffisante pour les scénarios d'amorçage iSCSI. Dans le contexte du processus d'amorçage iSCSI sécurisé, la réponse du serveur DHCP dans l'étape DHCP DEVRAIT inclure le nomDeServeur en format IPv4 (ou IPv6) pour éviter de s'appuyer sur un serveur DNS (pour la résolution des noms) ou une entité de service de découverte (pour chercher les noms de cibles). Cela réduit le nombre d'entités impliquées dans le processus d'amorçage iSCSI sécurisé.

Si l'étape du service de découverte est mise en œuvre en utilisant SLP, le client d'amorçage iSCSI DEVRAIT prendre en charge IPsec (utilisation FACULTATIVE) pour le protocole SLP, comme défini dans les [RFC4018] et [RFC3723]. Si l'étape du service de découverte n'est pas mise en œuvre en utilisant iSNS, le client d'amorçage iSCSI DEVRAIT fournir la prise en charge de IPsec (utilisation FACULTATIVE) pour le protocole iSNS, comme défini dans les [RFC4171] et [RFC3723]. Lorsque iSNS ou SLP sont utilisés pour distribuer les information de politique de sécurité ou de configuration, l'authentification d'origine des données par paquet, l'intégrité, et la protection contre la répétition DEVRAIENT, au minimum, être utilisées pour protéger le protocole de découverte.

Pour la communication finale entre le client d'amorçage iSCSI et le serveur d'amorçage iSCSI dans l'étape d'amorçage, l'authentification IPsec et dans la bande DEVRAIENT être mises en œuvre conformément aux lignes directrices des [RFC3720] et [RFC3723]. Du fait des contraintes de mémoire, on s'attend à ce que les clients d'amorçage iSCSI ne prennent en charge que l'authentification à clé pré partagée dans IKE. Lorsque l'adresse IP de l'hôte est allouée de façon dynamique, le mode IKE principal NE DEVRAIT PAS être utilisé, comme expliqué dans les [RFC3720] et [RFC3723]. Sans considération de la façon dont les paramètres (DHCP, SLP, iSNS) ont été obtenus dans les étapes précédentes (en toute sécurité ou non) la session d'amorçage iSCSI est vulnérable comme toute session iSCSI (voir les menaces sur la sécurité pour iSCSI dans les [RFC3720] et [RFC3723]). Donc, la sécurité pour cette session DEVRAIT être configurée et utilisée conformément aux lignes directrices des [RFC3720] et [RFC3723].

Noter que si une image d'amorçage est héritée d'une session iSCSI à partir d'une image d'amorçage précédemment chargée, elle hérite aussi des propriétés de sécurité de la session iSCSI.

Remerciements

Nous tenons à remercier John Hufferd de son initiative de former l'équipe d'amorçage iSCSI. Merci aussi à Doug Otis, Julian Satran, Bernard Aboba, David Robinson, Mark Bakke, Ofer Biran, et Mallikarjun Chadalapaka de leurs utiles suggestions et remarques concernant le projet de ce document.

Références normatives

[RFC0951] B. Croft et J. Gilmore, "[Protocole BOOTSTRAP](#) (BOOTP)", septembre 1985.

[RFC1497] J. Reynolds, "Extensions Informations de fabricant BOOTP", août 1993. (*Obsolète, voir RFC1533*)

- [RFC1534] R. Droms, "Interfonctionnement entre DHCP et BOOTP", octobre 1993. (D.S.)
- [RFC1542] W. Wimer, "Précisions et extensions au protocole Bootstrap", octobre 1993. (D.S.)
- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. (MàJ par [RFC8174](#))
- [RFC2131] R. Droms, "Protocole de [configuration dynamique d'hôte](#)", mars 1997. (DS) (Mà J par [RFC3396](#), [RFC4361](#), [RFC5494](#), et [RFC6849](#))
- [RFC2132] S. Alexander et R. Droms, "Options DHCP et [Extensions de fabricant BOOTP](#)", mars 1997.
- [RFC2396] T. Berners-Lee, R. Fielding et L. Masinter, "Identifiants de ressource uniformes (URI) : Syntaxe générique", août 1998. (Obsolète, voir [RFC3986](#))
- [RFC2608] E. Guttman et autres, "[Protocole de localisation de service](#), version 2", juin 1999. (MàJ par [RFC3224](#)) (P.S.)
- [RFC2732] R. Hinden, B. Carpenter et L. Masinter, "Format pour les adresses littérales IPv6 dans les URL", décembre 1999. (Obsolète, voir [RFC3986](#)) (P.S.)
- [RFC3118] R. Droms et W. Arbaugh, "[Authentification des messages](#) DHCP", juin 2001. (P.S.)
- [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](#))
- [RFC3629] F. Yergeau, "[UTF-8, un format de transformation](#) de la norme ISO 10646", STD 63, novembre 2003.
- [RFC3720] J. Satran et autres, "Interface Internet des systèmes de petits ordinateurs (iSCSI)", avril 2004. (Remplacée par [RFC7143](#))
- [RFC3722] M. Bakke, "[Profil de chaîne pour les noms d'interface](#) Internet de systèmes de petits ordinateurs (iSCSI)", avril 2004. (P.S.)
- [RFC3723] B. Aboba et autres, "Protocoles de [sécurisation de mémorisation de blocs](#) sur IP", avril 2004. (P.S.)
- [RFC3986] T. Berners-Lee, R. Fielding et L. Masinter, "[Identifiant de ressource uniforme](#) (URI) : Syntaxe générique", STD 66, janvier 2005.
- [RFC4018] M. Bakke et autres, "[Découverte de cibles et des serveurs de noms](#) des interfaces systèmes de petits ordinateurs (iSCSI) en utilisant le protocole de localisation de service version 2 (SLPv2)", avril 2005. (P.S.) (MàJ par [RFC7146](#))
- [RFC4171] J. Tseng et autres, "[Service de noms de mémorisation sur Internet](#) (iSNS)", septembre 2005. (P.S.)

Références pour information

- [RFC0903] R. Finlayson, T. Mann, J. Mogul et M. Theimer, "Protocole de [résolution inverse d'adresse](#)", STD 38, juin 1984.
- [RFC1350] K. Sollins, "[Protocole TFTP](#) (révision 2)", STD 33, juin 1992. (MàJ par 1782-85, 2347_49)
- [RFC1931] D. Brownell, "Extensions RARP dynamiques pour l'acquisition automatique d'adresse réseau", avril 1996. (Information)

Adresse des auteurs

Prasenjit Sarkar
IBM Almaden Research Center
650 Harry Road
San Jose, CA 95120, USA
téléphone : +1 408 927 1417
mél : psarkar@almaden.ibm.com

Duncan Missimer
Hewlett-Packard Company
10955 Tantau Ave
Cupertino, CA 95014, USA
mél : duncan.missimer@ieee.org

Constantine Sapuntzakis
Stanford University
353 Serra Hall #407
Stanford, CA 94305, USA
mél : csapuntz@alum.mit.edu

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2005).

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

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

Propriété intellectuelle

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

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

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

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.