Groupe de travail Réseau
Request for Comments : 4174
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

C. Monia, Consultant
J. Tseng, Riverbed Technology
K. Gibbons, McDATA Corporation
septembre 2005

Option Protocole de configuration dynamique d'hôte (DHCP) IPv4 pour le service de noms de mémorisation sur Internet

Résumé
Le présent document décrit l'option Protocole de configuration dynamique d'hôte (DHCP, *Dynamic Host Configuration Protocol*) pour permettre aux clients du service de nom de mémorisation sur Internet (iSNS, *Internet Storage Name Service*) de découvrir automatiquement la localisation du serveur iSNS par l'utilisation de DHCP pour IPv4. iSNS fournit des capacités de découverte et de gestion pour les appareils de mémorisation SCSI sur Internet (iSCSI, *Internet SCSI*) et du protocole de canal fibre Internet (iFCP, *Internet Fibre Channel Protocol*) dans un réseau de mémorisation IP à l'échelle de l'entreprise. iSNS fournit des services de gestion de mémorisation intelligente comparables à ceux qu'on trouve dans les réseaux de canal fibre, permettant à un réseau IP commercial de fonctionner avec une capacité similaire à celle d'un réseau de zone de mémorisation.

Table des matières

1. Introduction

Le protocole de configuration dynamique d'hôte pour IPv4 fournit un cadre pour passer les informations de configuration aux hôtes. Son utilité s'étend aux hôtes et appareils qui utilisent les protocoles iSCSI et iFCP pour se connecter aux infrastructures de mémorisation de niveau bloc sur un réseau TCP/IP.

Le protocole iSNS donne un cadre pour la découverte automatique, la gestion et la configuration d'appareils iSCSI et iFCP sur un réseau TCP/IP. Il fournit des fonctionnalités similaires à celles qu'on trouve sur les réseaux canal fibre, excepté que iSNS fonctionne dans le contexte d'un réseau IP. iSNS fournit par là l'intelligence de mémorisation requise aux réseaux IP standard sur les réseaux canal fibre existants.

Les options DHCP existantes ne peuvent pas être utilisés pour trouver les serveurs iSNS pour les raisons suivantes :
a) La fonction iSNS est notablement différente de celle des autres protocoles qui utilisent des options DHCP. Précisément, iSNS fournit un ensemble de capacités significativement plus grand que celui des protocoles de résolution de noms

normaux comme le DNS. Il est conçu pour prendre en charge un appareil client qui lui permet d'être configuré et géré à partir d'un serveur iSNS central.

b) iSNS exige un format d'option DHCP qui fournisse plus que la localisation du serveur iSNS. L'option DHCP doit spécifier le sous ensemble de services iSNS qui peuvent être activement utilisés par le client iSNS.

Le numéro d'option DHCP pour iSNS est utilisé par les appareils iSCSI et iFCP pour découvrir la localisation et le rôle du serveur iSNS. Le numéro d'option DHCP alloué pour iSNS par l'IANA est 83.

1.1 Conventions utilisées dans le document

iSNS se réfère au cadre de service de noms de mémorisation Internet, qui consiste en le modèle de réseau de mémorisation et les services associés.

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].

Tous les formats de trame sont dans l'ordre gros boutien des octets du réseau. Les champs marqués "réservé" DEVRAIENT être remplis de zéros.

Le présent document utilise les termes suivants :

"Client iSNS" - Les clients iSNS sont des processus résidants dans les appareils iSCSI et iFCP qui initient des transactions avec le serveur iSNS en utilisant le protocole iSNS.

"Serveur iSNS" - Le serveur iSNS répond aux messages d'interrogation et d'enregistrement du protocole iSNS et initie des messages de notification asynchrones. Le serveur iSNS mémorise les informations enregistrées par les clients iSNS.

"iSCSI (SCSI Internet)" - iSCSI est une encapsulation de SCSI pour une nouvelle génération d'appareils de mémorisations interconnectés avec TCP/IP.

"iFCP (*Internet Fibre Channel Protocol*, protocole Internet de canal fibre)" - iFCP est un protocole de passerelle à passerelle conçu pour interconnecter les appareils canal fibre existants en utilisant TCP/IP. iFCP transpose les services de transport et de tissu canal fibre dans TCP/IP.

2. Option iSNS pour DHCP

Cette option spécifie la localisation des serveurs principaux et de sauvegarde iSNS et les services iSNS disponibles à un client iSNS.

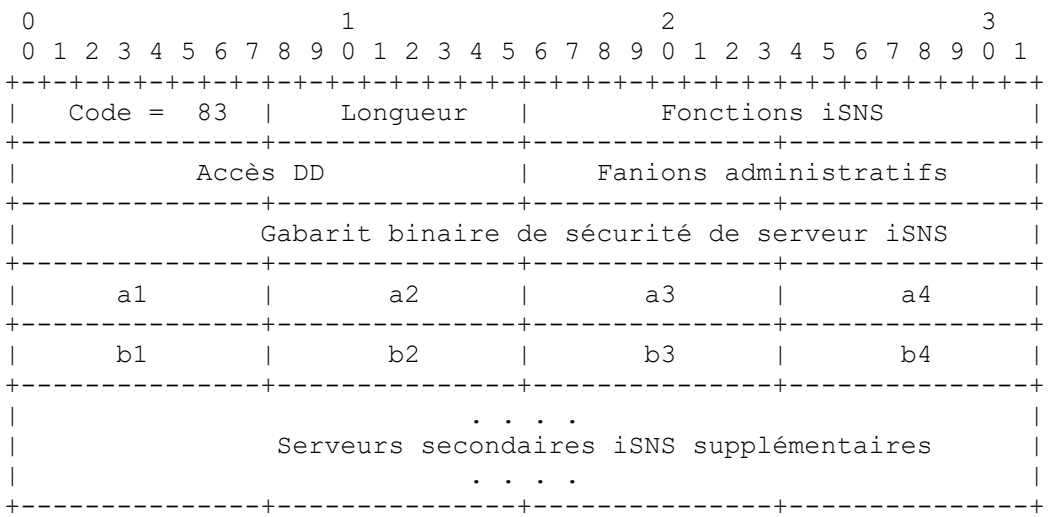

Figure 1. Option Serveur iSNS

L'option iSNS spécifie une liste d'adresses IP utilisées par les serveurs iSNS. L'option contient les paramètres suivants :

Longueur : le nombre d'octets qui suivent le champ Longueur.

Fonctions iSNS : Champ de gabarit binaire qui définit les fonctions prises en charge par les serveurs iSNS. Le format de ce champ est décrit au paragraphe 2.1.

Accès au domaine de découverte : champ binaire qui indique les types de clients iSNS à qui il est permis de modifier les domaines de découverte. Le contenu du champ est décrit au paragraphe 2.2.

Champ Fanions administratifs : contient les réglages administratifs pour les serveurs iSNS découverts par l'interrogation DHCP. Le contenu de ce champ est décrit au paragraphe 2.3.

Gabarit binaire de sécurité de serveur iSNS : Contient les réglages de sécurité du serveur iSNS spécifiés au paragraphe 2.4.

a1...a4 : selon le réglage du bit Battement de cœur dans le champ Fanions administratifs (paragraphe 2.3) ce champ contient soit l'adresse IP d'où le battement de cœur iSNS provient (voir la [RFC4171]) soit l'adresse IP du serveur principal iSNS.

b1...b4 : selon le réglage du bit Battement de cœur dans le champ Fanions administratifs (voir le paragraphe 2.3) ce champ contient soit l'adresse IP du serveur principal iSNS, soit celle d'un serveur secondaire iSNS.

Serveurs secondaires iSNS supplémentaires : chaque ensemble de quatre octets spécifie l'adresse IP d'un serveur secondaire iSNS.

Les champ Code jusqu'au champ Adresse IP a1...a4 DOIVENT être présents dans chaque réponse à l'interrogation iSNS ; donc le champ Longueur a une valeur minimum de 14.

Si le bit Battement de cœur est établi dans le champ Fanions administratifs (voir le paragraphe 2.3) alors b1...b4 DOIT aussi être présent. Dans ce cas, la valeur minimum du champ Longueur est 18.

L'inclusion de serveurs secondaires iSNS supplémentaires dans la réponse DOIT être indiquée en augmentant en conséquence le champ Longueur.

2.1 Champ Fonctions iSNS

Le champ Fonctions iSNS définit le rôle opérationnel du serveur iSNS (c'est-à-dire, comment le serveur iSNS va être utilisé). Le rôle du serveur iSNS peut être aussi simple que de juste fournir les informations de découverte, ou aussi significatif que de fournir les politiques de sécurité IKE/IPsec et les certificats à utiliser par les appareils iSCSI et iFCP. Le format du champ Fonctions iSNS est montré à la Figure 2.

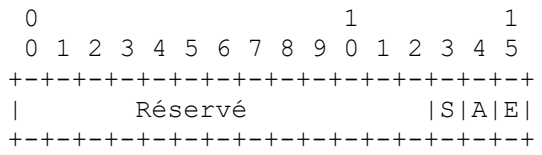

Figure 2. Champ Fonctions iSNS

Bit Fanions	Signification
15	Champs de fonction activés
14	Autorisation fondée sur le domaine de découverte
13	Distribution de politique de sécurité

La définition du champ Fonctions iSNS est la suivante :

Champs de fonction activés : Spécifie la validité des champs Fonction iSNS restants. Réglé à un, il signifie que le contenu de tous les autres champs Fonction iSNS est valide. Réglé à zéro, le contenu de tous les autres champs Fonction iSNS DOIT être ignoré.

Autorisation fondée sur le domaine de découverte : Indique si les appareils dans un domaine de découverte (DD, *Discovery Domain*) commun sont implicitement autorisés à accéder les uns aux autres. Bien que les domaines de découverte contrôlent la portée de la découverte d'appareils, ils n'indiquent pas nécessairement si un membre d'un domaine est

autorisé à accéder aux appareils découverts. Si ce bit est réglé à un, les appareils dans un domaine de découverte ommun sont automatiquement autorisés à accéder les uns aux autres (si leur authentification réussit). Si ce bit est réglé à zéro, l'autorisation d'accès n'est pas impliquée par l'appartenance au domaine et doit être explicitement effectuée par chaque appareil. Dans l'un et l'autre cas, les appareils qui ne sont pas dans un DD commun n'ont pas la permission d'accéder les uns aux autres.

Distribution de politique de sécurité : Indique si le client iSNS va télécharger et utiliser la configuration de politique de sécurité mémorisée dans le serveur iSNS. Si il est réglé à un, la politique est alors mémorisée dans le serveur iSNS et doit être utilisée par le client iSNS pour sa propre politique de sécurité. Si il est réglé à zéro, le client iSNS doit alors obtenir sa configuration de politique de sécurité par d'autres moyens.

2.2 Champ Accès au domaine de découverte

Le format du champ Bit d'accès au DD est montré par la Figure 3.

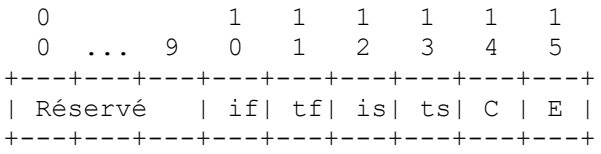

Figure 3. Champ Accès au domaine de découverte

Bit Fanion	Signification
15	E*(nabled)* Activé
14	C*(ontrol Node)* Nœud de contrôle
13	ts : Cible iSCSI
12	is : Initiateur iSCSI
11	tf : Accès iFCP cible
10	if : Accès iFCP initiateur

Voici la définition des champs d'accès au domaine de découverte :

Activé : spécifie la validité du reste du champ Bit d'accès au DD. Si il est réglé à un, le contenu du reste du champ Accès au DD est valide. Si il est réglé à zéro, le contenu du reste de ce champ DOIT être ignoré.

Nœud de contrôle : spécifie si le serveur iSNS permet d'ajouter, modifier, ou supprimer des domaines de découverte au moyen des nœuds de contrôle. Si il est réglé à un, les nœuds de contrôle sont autorisés à modifier la configuration de domaine de découverte. Réglé à zéro, les nœuds de contrôle ne sont pas autorisés à modifier les configurations de domaine de découverte.

Cible iSCSI, initiateur iSCSI, accès iFCP cible, accès iFCP d'initiateur : déterminent si le client iSNS enregistré (déterminé par son type de nœud iSCSI ou son rôle d'accès iFCP) a la permission d'ajouter, supprimer ou modifier les DD. Si ils sont réglé à un, la modification par le type de client spécifié est permise. Réglés à zéro, la modification par le type de client spécifié n'est pas permise.

(Un nœud peut mettre en œuvre plusieurs types de nœuds.)

2.3 Champ Fanions administratifs

Le format du champ Fanions administratifs est donné par la Figure 4.

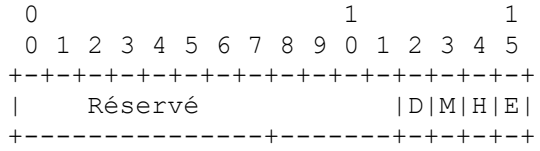

Figure 4. Fanions administratifs

Fanions	Signification
15	E*(nabled)* Activé

14	H*(eartbeat)* Battement de cœur
13	M*(anagement SCN)* SCN de gestion
12	D*(efault Discovery Domain)* Domaine de découverte par défaut

Définition des champs de fanions administratifs :

Activé : Spécifie la validité du reste du champ Fanions administratifs. Réglé à un, le contenu du reste du champ Fanions administratifs est valide. Réglé à zéro, le contenu restant DOIT être ignoré, indiquant que les réglages administratifs iSNS sont obtenus par d'autres moyens que DHCP.

Battement de cœur : Indique si la première adresse IP est l'adresse de diffusion groupée à laquelle le message Battement de cœur est envoyé. Si il est réglé à un, les bits a1 à a4 contiennent alors l'adresse de diffusion groupée de battement de cœur et les bits b1 à b4 contiennent l'adresse IP du serveur iSNS principal, suivie par la ou les adresses IP de tout serveur de sauvegarde (voir la Figure 1). Si il est réglé à zéro, les bits a1 à a4 contiennent alors l'adresse IP du serveur iSNS principal, suivie par la ou les adresses IP de tout serveur de sauvegarde.

SCN de gestion : Indique si les nœuds de contrôle sont autorisés à s'enregistrer pour recevoir des notifications de changement d'état (SCN, *State Change Notification*) de gestion. Les SCN de gestion sont une classe spéciale de notifications de changement d'état dont la portée est la base de données iSNS entière. Si ce bit est réglé à un, les nœuds de contrôle sont alors autorisés à s'enregistrer pour recevoir des SCN de gestion. Si il est réglé à zéro, les nœuds de contrôle ne sont alors pas autorisés à recevoir des SCN de gestion (mais ils peuvent recevoir des SCN normales).

Domaine de découverte par défaut : Indique si un nouvel appareil enregistré qui n'est pas explicitement placé dans un domaine de découverte (DD) et ensemble de domaines de découverte (DDS) devrait être automatiquement placé dans un DD et DDS par défaut. Si il est réglé à un, un DD par défaut devra contenir tous les appareils de la base de données iSNS qui n'ont pas été explicitement placés dans un DD par un client iSNS. Si il est réglé à zéro, les appareils non explicitement placés dans un DD ne sont alors membres d'aucun DD.

2.4 Gabarit binaire de la sécurité de serveur iSNS

Le format du champ Gabarit binaire de sécurité de serveur iSNS est montré à la Figure 5. Si il est valide, ce champ communique au client DHCP les réglages de sécurité qui sont requis pour communiquer avec le serveur iSNS indiqué.

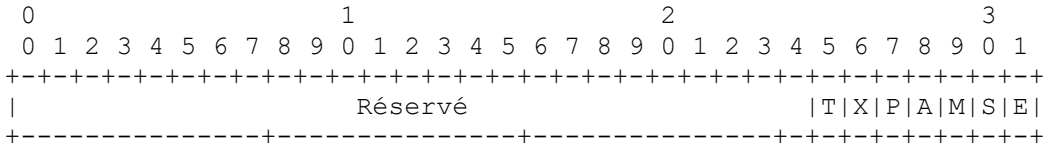

Figure 5. Gabarit binaire de la sécurité de serveur iSNS

Bits Fanions	**Signification**
31	(E) Activé
30	(S) IKE/IPsec
29	(M) Mode principal
28	(A) Mode agressif
27	(P) Secret parfait vers l'avant (PFS, *Perfect Forward Secrecy*)
26	(X) Mode transport
25	(T) Mode tunnel

Voici les définitions du gabarit binaire de sécurité de serveur iSNS :

Activé : Spécifie la validité du reste du gabarit binaire de sécurité de serveur iSNS. Réglé à un, le contenu du reste du champ est valide. Réglé à zéro, le contenu du reste du champ est indéfini et DOIT être ignoré.

IKE/IPsec : 1 = IKE/IPsec activé ; 0 = IKE/IPsec désactivé.

Mode principal : 1 = Mode principal activé ; 0 = Mode principal désactivé.

Mode agressif : 1 = Mode agressif activé ; 0 = Mode agressif désactivé.

PFS : 1 = PFS activé ; 0 = PFS désactivé.

Mode transport : 1 = Mode transport préféré ; 0 = pas de préférence.

Mode tunnel : 1 = Mode tunnel préféré ; 0 = pas de préférence.

Si IKE/IPsec est désactivé, cela indique que le protocole d'échange de clés Internet (IKE) n'est pas disponible pour configurer les clés IPsec pour les sessions iSNS à ce serveur iSNS. Cela n'empêche pas nécessairement d'autres méthodes d'échange de clés (par exemple, changement de clés manuel) pour établir une association de sécurité IPsec pour la session iSNS.

Si IKE/IPsec est activé, alors pour chaque paire de bits <Mode principal, Mode agressif> et <Mode transport, Mode tunnel>, un des deux bits DOIT être réglé à 1, et l'autre DOIT être réglé à 0.

3. Considérations sur la sécurité

Pour protéger l'option iSNS, l'option de sécurité Authentification DHCP telle que spécifiée dans la [RFC3118] peut présenter un problème dû à la mise en œuvre et au déploiement limités de l'option d'authentification DHCP. Le mécanisme de sécurité IPsec pour iSNS est lui-même spécifié dans la [RFC4171] pour fournir la confidentialité quand des informations sensibles sont distribuées via iSNS. Voir à la Section "Considérations sur la sécurité" de la [RFC4171] les détails et les exigences spécifiques pour la mise en œuvre de IPsec.

De plus, la [RFC4171] décrit un bloc d'authentification qui assure l'intégrité des messages pour la diffusion groupée ou la diffusion des messages iSNS (c'est-à-dire, seulement pour les messages de battement de cœur et de découverte). Voir dans la [RFC3723] une discussion plus poussée de la sécurité pour ces protocoles.

Si aucune information sensible, comme décrit dans la [RFC4171], n'est distribuée via iSNS, et si une entité est découverte via iSNS, l'authentification et l'autorisation sont traitées par les protocoles de mémorisation IP dont les points d'extrémité sont découverts via iSNS ; précisément, iFCP [RFC4172] et iSCSI [RFC3720]. Il est de la responsabilité des fournisseurs de ces services d'assurer qu'un service annoncé ou découvert de façon inappropriée ne compromet pas leur sécurité.

Quand on n'utilise pas la sécurité DHCP, il y a un risque de distribution de fausses informations de découverte (par exemple, via l'option DHCP de iSNS identifiant un faux serveur iSNS qui distribue les fausses informations de découverte). La principale contre mesure pour ce risque est l'authentification par les protocoles de mémorisation IP découverts par iSNS. Quand ce risque est un souci significatif, les SA IPsec DEVRAIENT être utilisées (comme spécifié dans la RFC 3723). Par exemple, si un attaquant utilise DHCP et iSNS pour distribuer des informations de découverte qui identifient faussement un point d'extrémité iSCSI, ce point d'extrémité va manquer des accréditifs nécessaires pour achever avec succès l'authentification IKE, et donc sera empêché d'envoyer ou recevoir du trafic iSCSI falsifié. Quand ce risque de fausses informations de découverte est un souci significatif et que IPsec est mis en œuvre pour iSNS, les SA IPsec DEVRAIENT aussi être utilisées pour le trafic iSNS afin d'empêcher l'utilisation d'un faux serveur iSNS ; ceci est plus robuste que de se reposer seulement sur les protocoles de mémorisation IP pour détecter les fausses informations de découverte.

Lorsque IPsec est mis en œuvre pour iSNS, il y a un risque d'attaque de déni de service fondée sur l'utilisation répétée de fausses informations de découverte qui vont causer l'initiation d'une négociation IKE. Les contre mesures pour cela sont la configuration administrative de chaque entité iSNS pour limiter les homologues avec lesquels elle accepte de communiquer (c'est-à-dire, par gamme d'adresses IP et/ou domaine du DNS) et la maintenance d'une antémémoire d'authentification négative pour éviter de contacter de façon répétée une entité iSNS qui échoue à s'authentifier. Ces trois mesures (c'est-à-dire, les limites de gamme d'adresse IP, les limites de domaine DNS et l'antémémoire d'authentification négative) DOIVENT être mises en œuvre pour les entités iSNS lorsque cette option DHCP est utilisée. Un argument analogue s'applique aux protocoles de mémorisation IP qui peuvent être découverts via iSNS comme discuté dans la RFC 3723.

De plus, l'utilisation des techniques décrites dans la [RFC2827] et la [RFC3833] peut aussi être pertinente pour réduire les attaques de déni de service.

4. Considérations relatives à l'IANA

Conformément à la politique définie dans la [RFC2131], l'IANA a alloué la valeur de 83 à cette option.

Il n'y a pas d'autre valeur allouée par l'IANA qui soit définie dans la présente spécification.

5. Références normatives

[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)

[RFC3118] R. Droms et W. Arbaugh, "Authentification des messages DHCP", juin 2001. *(P.S.)*

[RFC3720] J. Satran et autres, "Interface Internet des systèmes de petits ordinateurs (iSCSI)", avril 2004. *(Remplacée par* RFC7143)

[RFC3723] B. Aboba et autres, "Protocoles de sécurisation de mémorisation de blocs sur IP", avril 2004. *(P.S.)*

[RFC4171] J. Tseng et autres, "Service de noms de mémorisation sur Internet (iSNS)", septembre 2005. *(P.S.)*

6. Références pour information

[RFC2827] P. Ferguson, D. Senie, "Filtrage d'entrée de réseau : Combattre les attaques de déni de service qui utilisent l'usurpation d'adresse de source IP", mai 2000. (*MàJ par* RFC3704) (BCP0038)

[RFC3833] D. Atkins, R. Austein, "Analyse des menaces contre le système des noms de domaines (DNS)", août 2004. *(Information)*

[RFC4172] C. Monia et autres, "iFCP – protocole de réseautage de mémorisation de canal fibre Internet", septembre 2005. *(P.S.)*

Adresse des auteurs

Kevin Gibbons
McDATA Corporation
4555 Great America Parkway
Santa Clara, CA 95054-1208
téléphone : (408) 567-5765
mél : kevin.gibbons@mcdata.com

Charles Monia
7553 Morevern Circle
San Jose, CA 95135
mél : charles_monia@yahoo.com

Josh Tseng
Riverbed Technology
501 2nd Street, Suite 410
San Francisco, CA 94107
téléphone : (650)274-2109
mél : joshtseng@yahoo.com

Déclaration complète de droits de reproduction

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