Groupe de travail Réseau
Request for Comments : 4171
Catégorie : Sur la voie de la normalisation

J. Tseng, Riverbed Technology
K. Gibbons, McDATA Corporation
F. Travostino, Nortel
C. Du Laney, Rincon Research Corporation
J. Souza, Microsoft

Traduction Claude Brière de L'Isle
septembre 2005

Service de nom de mémorisation Internet (iSNS)

Résumé
Le présent document spécifie le protocole du service de nom de mémorisation Internet (iSNS, *Internet Storage Name Service*) utilisé pour l'interaction entre les serveurs iSNS et les clients iSNS, qui facilite la découverte automatique, la gestion, et la configuration des appareils iSCSI *(Internet Small Computer System Interface)* et de canal fibre (FC, *Fiber Channel)* (en utilisant des passerelles iFCP *(Internet Fiber Channel Protocol)*) sur un réseau TCP/IP. iSNS fournit des services de découverte et de gestion de mémorisation intelligente comparables à ceux qu'on trouve dans les réseaux de canal fibre, permettant à un réseau IP de fonctionner avec des capacités similaires à celles d'un réseau de zone de mémorisation. iSNS facilite une intégration sans à coups des réseaux IP et canal fibre due à sa capacité à émuler le tissu des services de canal fibre et à gérer les appareils iSCSI et canal fibre. iSNS apporte ainsi sa valeur ajoutée à tout réseau de mémorisation composé d'appareils iSCSI, d'appareils canal fibre (utilisant des passerelles iFCP), ou toute combinaison de ceux-ci.

Table des matières

1. Introduction

1.1 Conventions utilisées dans le document

"iSNS" se réfère au modèle de réseau de mémorisation et aux services associés couverts dans le texte de ce document.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

Tous les formats de trame sont dans l'ordre gros boutien des octets du réseau.

Tous les champs inutilisés et toutes les transpositions binaires, incluant ceux qui sont RÉSERVÉ, DEVRAIENT être réglés à zéro à l'envoi et ignorés à réception.

1.2 Objet du document

Ce document sur la voie de la normalisation contient du texte normatif qui spécifie le protocole iSNS, utilisé par les appareils iSCSI et iFCP pour communiquer avec le serveur iSNS. Ce document se concentre sur l'interaction entre les serveurs iSNS et les clients iSNS ; les interactions entre plusieurs serveurs iSNS principaux d'autorité sont un sujet potentiel pour de futurs travaux.

2. Vue d'ensemble de iSNS

iSNS facilite une configuration et gestion adaptable d'appareils de mémorisation iSCSI et canal fibre (FC) dans un réseau IP en fournissant un ensemble de services comparable à celui disponible dans les réseaux canal fibre. iSNS permet donc à un réseau IP de base de fonctionner à un niveau d'intelligence comparable à celui d'un tissu canal fibre. iSNS permet à l'administrateur d'aller au delà d'un simple modèle de gestion appareil par appareil, où chaque appareil de mémorisation est configuré manuellement et individuellement avec sa propre liste d'initiateurs et cibles connus. En utilisant iSNS, chaque appareil de mémorisation subordonne ses responsabilités de découverte et de gestion au serveur iSNS. Le serveur iSNS sert ainsi de point de configuration consolidé à travers lequel les stations de gestion peuvent configurer et gérer le réseau de mémorisation entier, incluant les appareils iSCSI aussi bien que canal fibre.

iSNS peut être mis en œuvre pour prendre en charge les protocoles iSCSI et/ou iFCP autant que nécessaire ; une mise en œuvre iSNS PEUT fournir la prise en charge d'un de ces protocoles ou des deux comme désiré par la mise en œuvre. Les exigences de mise en œuvre au sein de chacun de ces protocoles sont exposées à la Section 5. L'utilisation de iSNS est FACULTATIVE pour iSCSI et EXIGÉE pour iFCP.

2.1 Composants architecturaux de iSNS

2.1.1 Protocole iSNS (iSNSP)

Le protocole iSNS (iSNSP) est un protocole souple et léger qui spécifie comment clients et serveurs iSNS communiquent. Il convient pour diverses plateformes, incluant des commutateurs et cibles ainsi que des serveurs hôtes.

2.1.2 Client iSNS

Les clients iSNS initient des transactions avec les serveurs iSNS en utilisant iSNSP. Les clients iSNS sont des procès qui sont corésidents dans l'appareil de mémorisation, et qui peuvent enregistrer des informations d'attribut d'appareil, télécharger des informations sur d'autres clients enregistrés dans un domaine de découverte (DD, *Discovery Domain*) commun, et recevoir des notifications asynchrones d'événements qui surviennent dans leurs DD. Les stations de gestion sont un type particulier de client iSNS qui ont accès à tous les DD mémorisés dans l'iSNS.

2.1.3 Serveur iSNS

Les serveurs iSNS répondent aux interrogations et demandes de protocole iSNS, et initient les notifications de changement d'état de protocole iSNS. Les informations authentifiées de façon appropriée soumises par une demande d'enregistrement sont mémorisées dans une base de données iSNS.

2.1.4 Base de données iSNS

La base de données iSNS est le répertoire des informations pour le ou les serveurs iSNS. Elle conserve les informations sur les attributs de client iSNS. Une mise en œuvre de iSNS à capacité de répertoire peut mémoriser les attributs de client dans une infrastructure de répertoire LDAP.

2.1.5 iSCSI

iSCSI (Internet SCSI) est une encapsulation de SCSI pour une nouvelle génération d'appareils de mémorisation interconnectés avec TCP/IP [RFC3720].

2.1.6 iFCP

iFCP (Internet FCP) est un protocole de passerelle à passerelle conçu pour interconnecter les appareils canal fibre et SCSI existants en utilisant TCP/IP. iFCP transpose la norme FCP existante et les services canal fibre associés en TCP/IP [RFC4172].

2.2 Vue fonctionnelle d'ensemble de iSNS

iSNS a quatre fonctions principales :
1) Un service de noms qui assure la découverte des ressources de mémorisation
2) Un domaine de découverte (DD) et un service de contrôle d'établissement

3) Un service de notification de changement d'état
4) Une transposition ouverte des appareils canal fibre et iSCSI

2.2.1 Service d'enregistrement de nom

iSNS fournit une fonction d'enregistrement pour permettre à toutes les entités dans un réseau de mémorisation de s'enregistrer et d'interroger la base de données iSNS. Les cibles et les initiateurs peuvent tous deux s'enregistrer dans la base de données iSNS, ainsi qu'interroger pour des informations sur d'autres initiateurs et cibles. Cela permet, par exemple, à un client initiateur d'obtenir des informations sur les appareils cibles auprès du serveur iSNS. Ce service est modélisé sur le serveur de nom de services génériques canal fibre décrit dans FC-GS-4, avec des extensions, fonctionnant au sein du contexte d'un réseau IP.

Le service d'enregistrement de noms fournit aussi la capacité d'obtenir un identifiant de domaine unique pour le réseau pour les passerelles iFCP quand c'est nécessaire.

2.2.2 Service de découverte de domaine et de contrôle d'enregistrement

Le service de découverte de domaine (DD) facilite la partition des nœuds de mémorisation en des groupements plus gérables pour les besoins de contrôle administratif et d'établissement. Il permet à l'administrateur de limiter le processus d'établissement de chaque hôte au sous ensemble le plus approprié de cibles enregistrées dans l'iSNS. Ceci est particulièrement important pour réduire le nombre d'établissements non nécessaires (établissements iSCSI ou établissements d'accès de canal fibre) et pour limiter la durée que passe l'hôte à initialiser les relations d'établissement lorsque la taille du réseau de mémorisation augmente. Les nœuds de mémorisation doivent être dans au moins un DD activé commun afin d'obtenir des informations les uns sur les autres. Les appareils peuvent être membres de plusieurs DD simultanément.

Le contrôle d'établissement permet aux cibles de déléguer leurs politiques de contrôle/autorisation d'accès au serveur iSNS. Ceci est cohérent avec le but de centralisation de la gestion des appareils de mémorisation qui utilisent le serveur iSNS. Le nœud ou appareil cible télécharge la liste des initiateurs autorisés de l'iSNS. Chaque nœud ou appareil est identifié de façon univoque par un nom iSCSI ou un nom d'accès FC. Seuls les initiateurs qui correspondent à l'identification et autorisation requises fournies par le iSNS auront la permission d'accès à ce nœud cible durant l'établissement de session.

Placer des portails d'une entité réseau dans les domaines de découverte permet aux administrateurs d'indiquer l'interface de portail IP préférée à travers laquelle le trafic de mémorisation devrait accéder aux nœuds de mémorisation spécifiques de cette entité réseau. Si aucun portail d'une entité réseau n'a été placé dans un DD, les interrogations portant sur ce DD DEVRONT alors rapporter tous les portails de cette entité réseau. Si un ou plusieurs portails d'une entité réseau ont été placés dans un DD, les interrogations portant sur ce DD DEVRONT alors rapporter seulement les portails qui ont été explicitement placés dans le DD.

Les DD peuvent être gérés hors ligne avec une station de travail séparée qui utilise iSNSP ou SNMP. Si la cible opte pour l'utilisation du dispositif de contrôle d'établissement de l'iSNS, elle délègue la gestion de la politique de contrôle d'accès (c'est-à-dire, la liste des initiateurs qui ont la permission de se connecter à cette cible) aux stations de travail de gestion qui gèrent la configuration dans la base de données iSNS.

Si elle est autorisée administrativement, une cible peut télécharger sa propre liste de contrôle d'établissement. Cela se fait en utilisant les message DDReg et en faisant la liste des noms iSCSI de chaque initiateur à enregistrer dans le DD de la cible.

Une mise en œuvre PEUT décider que les nouveaux appareils enregistrés qui n'ont pas été explicitement placés dans un DD par la station de gestion seront placés dans un "DD par défaut" contenu dans un "DDS par défaut" dont la valeur initiale d'état d'ensemble de DD est "activé". Cela les rend visibles aux autres appareils dans le DD par défaut. D'autres mises en œuvre PEUVENT décider qu'elles ne sont enregistrées auprès d'aucun DD, les rendant inaccessibles aux messages iSNSP à portée de source.

Le serveur iSNS utilise l'attribut Source de chaque message iSNSP pour déterminer l'origine de la demande et pour délimiter l'opération à un ensemble de domaines de découverte. De plus, le type de nœud (spécifié dans le champ binaire Type de nœud iFCP ou iSCSI) peut aussi être utilisé pour déterminer les autorisations pour l'opération iSNS spécifiée. Par exemple, seuls les nœuds de contrôle sont autorisés à créer ou supprimer des domaines de découverte.

Les domaines de découverte valides et actifs appartiennent à au moins un ensemble de domaines de découverte (DDS, *Discovery Domain Set*) actif. Les domaines de découverte qui n'appartiennent pas à un DDS activé ne sont pas activés. Le serveur iSNS DOIT maintenir l'état de membre de DD pour tous les nœuds de mémorisation, même pour ceux qui ont été

désenregistrés. La qualité de membre de DD persiste sans considération de si un nœud de mémorisation est activement enregistré ou non dans la base de données iSNS.

2.2.3 Service de notification de changement d'état

Le service de notification de changement d'état (SCN, *State Change Notification*) permet au serveur iSNS de produire des notifications sur les événements réseau qui affectent l'état de fonctionnement des nœuds de mémorisation. Le client iSNS peut s'enregistrer à la notification au nom de ses nœuds de mémorisation pour la notification des événements détectés par le serveur iSNS. La SCN notifie aux clients iSNS les changements implicites ou explicites de la base de données iSNS ; elle n'indique pas nécessairement l'état de connexité aux appareils de mémorisation homologues dans le réseau. La réponse d'un appareil de mémorisation à la réception d'une SCN est spécifique de la mise en œuvre ; la politique pour répondre aux SCN sort du domaine d'application du présent document.

Il y a deux types d'enrgistrements à la SCN : les enregistrements réguliers et les enregistrements de gestion. Les enregistrements de gestion résultent en SCN de gestion, tandis que les enregistrements réguliers résultent en SCN régulières. Le type d'enregistrement et de message de SCN est indiqué dans le gabarit binaire de SCN (paragraphes 6.4.4 et 6.6.12).

Un enregistrement pour une SCN régulière indique que le service de domaine de découverte DEVRA être utilisé pour contrôler la distribution des messages de SCN. La réception de SCN régulières se limite aux domaines de découverte dans lesquels l'événement qui déclenche la SCN a lieu. Les SCN régulières ne contiennent pas d'information sur les domaines de découverte.

Un enregistrement de SCN de gestion ne peut être demandé que par des nœuds de gestion. Les SCN de gestion résultant des enregistrements de gestion ne sont pas liées par le service de domaine de découverte. L'autorisation de demander des enregistrements de gestion à la SCN peut être contrôlé administrativement.

Le serveur iSNS DEVRAIT être mis en œuvre avec des ressources de matériel et de logiciel suffisantes pour prendre en charge le nombre attendu de clients iSNS. Cependant, si les ressources sont épuisées de façon inattendue, le serveur iSNS PEUT alors refuser le service de SCN en retournant un message Enregistrement SCN rejeté (Code d'état 17). Le rejet peut se produire dans des situations où la taille du réseau ou le nombre courant d'enregistrements à la SCN a dépassé un seuil spécifique de la mise en œuvre. Un client qui n'a pas la permission de s'enregistrer pour les SCN peut décider de surveiller ses sessions directement avec d'autres appareils de mémorisation.

Le mécanisme spécifique de notification par lequel le serveur iSNS apprend les événements qui déclenchent les SCN est spécifique de la mise en œuvre, mais peut inclure des exemples tels que des messages de notification explicites d'un client iSNS au serveur iSNS, ou une interruption du matériel à un serveur iSNS hébergé par un hôte suite à une défaillance de liaison.

2.2.4 Transposition ouverte entre appareils canal fibre et iSCSI

La base de données iSNS mémorise les informations de dénomination et de découverte sur les appareils canal fibre et iSCSI. Cela permet au serveur iSNS de mémoriser les transpositions d'un appareil canal fibre en un appareil mandataire iSCSI "image" dans le réseau IP. De façon similaire, les transpositions d'un appareil iSCSI en un "mandataire WWN" peuvent être mémorisées sous le champ Jeton WWNN pour cet appareil iSCSI.

De plus, en utilisant des passerelles iSCSI-FC, les stations de gestion à capacité canal fibre peuvent interagir avec le serveur iSNS pour restituer des informations sur les appareils canal fibre, et utiliser ces informations pour gérer les appareils canal fibre et iSCSI. Cela permet que des fonctions de gestion comme les domaines de découverte et les notifications d'état de changement soient appliquées sans interruption aux appareils iSCSI et canal fibre, facilitant l'intégration des réseaux IP avec les appareils canal fibre et leur structure.

Noter que les attributs canal fibre sont mémorisés comme des attributs iFCP, et que la capacité de mémoriser ces informations dans le serveur iSNS est utile même si le protocole iFCP n'est pas mis en œuvre. En particulier, l'étiquette 101 peut être utilisée pour mémoriser un "nom de mandataire iSCSI" pour les appareils canal fibre enregistrés au serveur iSNS. Ce champ est utilisé pour associer l'appareil FC à une entrée d'enregistrement iSCSI qui est utilisée pour que l'appareil canal fibre communique avec les appareils iSCSI dans le réseau IP. À l'inverse, l'étiquette 37 (voir au paragraphe 6.1) contient un champ Jeton WWNN *(World Wide Node Name)*, qui peut être utilisé pour mémoriser une valeur de nom de nœud FC (WWNN) utilisée par les passerelles iSCSI-FC pour représenter un appareil iSCSI dans le domaine canal fibre.

En mémorisant la transposItion entre appareils canal fibre et iSCSI dans le serveur iSNS, ces informations deviennent ouvertes à tout client iSNS autorisé qui souhaite récupérer et utiliser ces informations. Dans de nombreux cas, cela présente

un avantage sur la mémorisation des informations en interne au sein d'une passerelle iSCSI-FC, où la transposition est inaccessible aux autres appareils, sauf par des mécanismes non normalisés.

2.3 Modèle d'usage iSNS

Ce qui suit est une description générale de la façon dont chaque type d'appareil dans un réseau de mémorisation peut utiliser iSNS. Chaque type d'appareil interagit avec le serveur iSNS comme un client iSNS et doit s'enregistrer dans la base de données iSNS afin d'accéder aux services fournis par l'iSNS.

2.3.1 Initiateur iSCSI

Un initiateur iSCSI va interroger le serveur iSNS pour découvrir la présence et la localisation des appareils cibles iSCSI. Il peut aussi demander des notifications de changement d'état (SCN) afin que lui soient notifiées de nouvelles cibles qui apparaissent sur le réseau après l'établissement et la découverte initiale. Les SCN peuvent aussi informer l'initiateur iSCSI des cibles qui ont été retirées ou ne sont plus disponibles dans le réseau de mémorisation, afin que des sessions de mémorisation incomplètes puissent être terminées en douceur et que les ressources pour des cibles non existantes puissent être réallouées.

2.3.2 Cible iSCSI

Une cible iSCSI permet qu'elle soit découverte par les initiateurs iSCSI en enregistrant sa présence dans le serveur iSNS. Elle peut aussi s'enregistrer pour les SCN afin de détecter l'ajout ou la suppression d'initiateurs pour les besoins de l'allocation de ressources. L'appareil cible iSCSI peut aussi s'enregistrer pour les messages d'enquête d'état d'entité (ESI, *Entity Status Inquiry*) qui permettent à l'iSNS de surveiller la disponibilité de l'appareil cible dans le réseau de mémorisation.

2.3.3 Passerelle iSCSI-FC

Une passerelle iSCSI-FC relie les appareils dans un réseau canal fibre à un réseau iSCSI/IP. Elle peut utiliser le serveur iSNS pour mémoriser les attributs d'appareil FC découverts dans le serveur de noms FC, ainsi que les transpositions d'identifiants d'appareil FC en identifiants d'appareil iSCSI. iSNS a la capacité de mémoriser tous les attributs des appareils iSCSI et canal fibre ; les appareils iSCSI sont gérés par des interactions directes utilisant iSNS, tandis que les appareils FC peuvent être gérés indirectement par des interactions iSNS avec la passerelle iSCSI-FC. Cela permet aux deux types d'appareils iSCSI et canal fibre d'être gérés dans un cadre de gestion sans rupture.

2.3.4 Passerelle iFCP

Une passerelle iFCP utilise iSNS pour émuler les services fournis par un serveur de noms canal fibre pour les appareils FC dans sa région de passerelle. iSNS fournit les informations de base de découverte et de configuration de zone à appliquer par la passerelle iFCP. Quand il est interrogé, iSNS retourne les informations sur l'adresse réseau N_Port utilisée pour établir les sessions iFCP entre les appareils FC pris en charge par les passerelles iFCP.

2.3.5 Station de gestion

Une station de gestion utilise iSNS pour surveiller les appareils de mémorisation et pour activer ou désactiver les sessions de mémorisation en configurant les domaines de découverte. Une station de gestion interagit généralement avec le serveur iSNS comme un nœud de gestion doté d'un accès à tous les enregistrements de base de données iSNS et avec des privilèges particuliers pour configurer les domaines de découverte. Par la manipulation des domaines de découverte, la station de gestion contrôle la portée de la découverte d'appareils pour les clients iSNS qui interrogent le serveur iSNS.

2.4 Réglages iSNS contrôlés administrativement

Certains réglages de fonctionnement importants pour le serveur iSNS sont configurés en utilisant des moyens administratifs, comme un fichier de configuration, un accès de console, une méthode SNMP, ou autre, spécifique de la mise en œuvre. Ces réglages contrôlés administrativement ne peuvent pas être configurés en utilisant le protocole iSNS, et donc la mise en œuvre de serveur iSNS DOIT fournir une telle interface de contrôle administratif.

Voici une liste de paramètres qui sont administrativement contrôlés pour le serveur iSNS. En l'absence de réglages de remplacement fournis par l'administrateur, les réglages par défaut suivants DOIVENT être utilisés.

Réglage	**Réglage par défaut**
Seuil de non réponse ESI	3 (voir au § 5.6.5.13)
SCN de gestion (seulement nœuds de gestion)	activé (voir au § 5.6.5.8)
DD/DDS par défaut	désactivé
Modification DD/DDS :	
- nœud de gestion	activé
- type de nœud cible iSCSI	désactivé
- type de nœud initiateur iSCSI	désactivé
- rôle d'accès cible iFCP	désactivé
- rôle d'accès initiateur iFCP	désactivé
nœuds de gestion autorisés	N/A

Le seuil de non réponse ESI détermine le nombre de messages ESI envoyés sans recevoir de réponse avant que l'entité réseau soit désenregistrée de la base de données iSNS.

La SCN de gestion pour les nœuds de gestion détermine si un nœud de gestion enregistré a la permission de s'enregistrer pour recevoir des SCN de gestion.

DD/DDS par défaut détermine si un appareil nouvellement enregistré non explicitement placé dans un domaine de découverte (DD) et un ensemble de domaines de découverte (DDS) est placé dans un DD/DDS par défaut.

Modification DD/DDS détermine si le type de nœud spécifié a la permission d'ajouter, supprimer ou mettre à jour les DD et DDS.

Les nœuds de gestion autorisés sont une liste de nœuds, identifiés par un nom iSCSI ou un nom d'accès FC WWPN, qui sont autorisés à s'enregistrer comme nœuds de gestion.

2.5 Découverte de serveur iSNS

2.5.1 Protocole de localisation de service (SLP)

Le protocole de localisation de service (SLP, *Service Location Protocol*) fournit un cadre souple et adaptable pour fournir aux hôtes l'accès aux informations sur l'existence, la situation, et la configuration des services sur le réseau, incluant le serveur iSNS. SLP peut être utilisé par les clients iSNS pour découvrir l'adresse IP ou le FQDN du serveur iSNS. Pour mettre en œuvre la découverte avec SLP, un agent de service (SA, *Service Agent*) devrait être cohébergé dans le serveur iSNS, et un agent d'utilisateur (UA, *User Agent*) devrait être dans chaque client iSNS. Chaque client envoie en diffusion groupée un message de découverte demandant l'adresse IP du ou des serveurs iSNS. Le SA répond à cette demande. Facultativement, la localisation du serveur iSNS peut être mémorisée dans l'agent de répertoire (DA, *Directory Agent*) SLP.

Noter qu'une description et spécification complète de SLP peut être trouvée dans la [RFC2608], et qu'elle sort du domaine d'application du présent document. Un gabarit de service pour utiliser SLP pour localiser les serveurs iSNS peut être trouvé dans la [RFC4018].

2.5.2 Protocle de configuration dynamique d'hôte (DHCP)

L'adresse IP du serveur iSNS peut être mémorisée dans un serveur DHCP pour être téléchargée par les clients iSNS en utilisant une option DHCP. Le numéro d'option DHCP à utiliser pour distribuer la localisation du serveur iSNS se trouve dans la [RFC4174].

2.5.3 Message Battement de cœur de iSNS

Le message Battement de cœur iSNS est décrit au paragraphe 5.6.5.14. Il permet aux clients iSNS au sein du domaine de diffusion ou diffusion groupée du serveur iSNS de découvrir la localisation du serveur iSNS actif et de tous serveurs de sauvegarde.

2.6 iSNS et les traducteurs d'adresse réseau (NAT)

L'existence de NAT aura un impact sur les informations restituées du serveur iSNS. Si le client iSNS existe dans un domaine d'adressage différent de celui du serveur iSNS, les informations d'adresse IP mémorisées dans le serveur iSNS peuvent n'être pas correctes lorsque interprétées dans le domaine du client iSNS.

Il y a plusieurs approches possibles pour permettre le fonctionnement de iSNS au sein d'un réseau à NAT. La première approche est d'exiger l'utilisation du numéro d'accès TCP canonique par les cibles et les initiateurs quand ils s'adressent à des cibles à travers une frontière de NAT, et pour le client iSNS de ne pas interroger sur des adresses IP nominales. Le client iSNS interrogera plutôt sur le nom de domaine pleinement qualifié du DNS (FQDN, *Fully Qualified Domain Name*) mémorisé dans le champ Identifiant d'entité quand il cherche les informations d'adressage. Une fois restitué, le nom DNS peut être interprété dans chaque domaine d'adresse et transposé en l'adresse IP appropriée par les serveurs DNS locaux.

Une seconde approche est de déployer un réseau réparti de serveurs iSNS. Les serveurs iSNS locaux sont déployés à l'intérieur et à l'extérieur des frontières de NAT, chaque serveur local mémorisant les adresses IP pertinentes pour leur domaines de NAT respectifs. Les mises à jour dans le réseau de serveurs iSNS décentralisés locaux sont traitées en utilisant LDAP et les règles de traduction de NAT appropriées mises en œuvre au sein du mécanisme de mise à jour de chaque serveur.

Finalement, on notera qu'il est possible à un serveur iSNS dans le domaine d'adressage privé derrière une frontière de NAT de prendre en charge exclusivement les clients iSNS qui fonctionnent dans le domaine d'adressage IP mondial. Si c'est le cas, l'administrateur a seulement besoin de s'assurer que les transpositions appropriées sont configurées sur les passerelles de NAT pour permettre aux clients iSNS d'initier des sessions iSNSP avec le serveur iSNS. Toutes les adresses enregistrées contenues dans le serveur iSNS sont donc des adresses IP publiques à utiliser à l'extérieur des frontières du NAT. Il faut veiller à s'assurer qu'il n'y a pas de clients iSNS qui interrogent le serveur de l'intérieur des frontières du NAT.

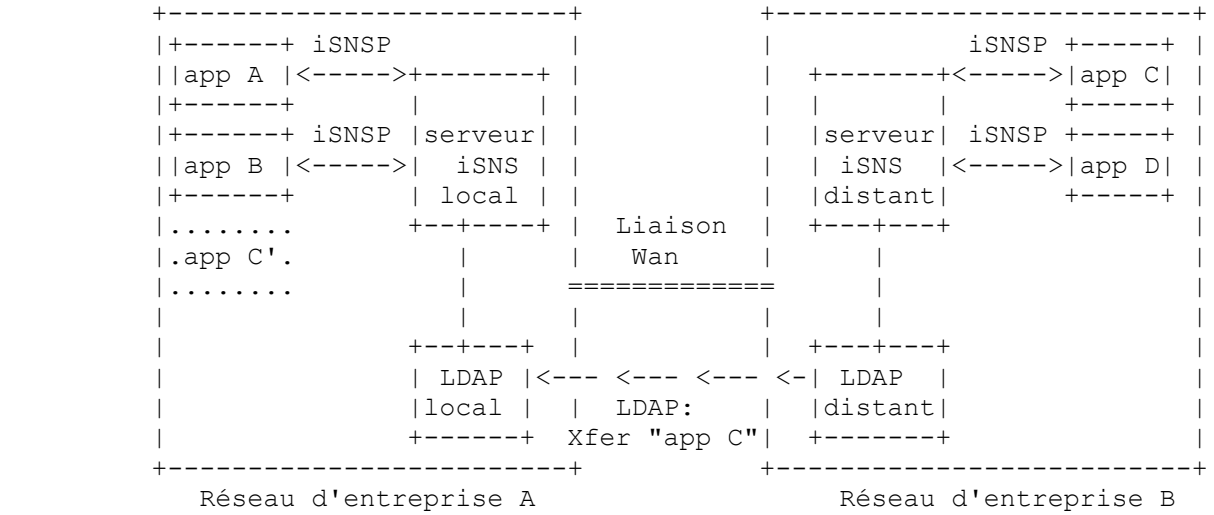
2.7 Transfert des enregistrements de base de données iSNS entre les serveurs iSNS

Le transfert des enregistrements de base de données iSNS entre les serveurs iSNS a des applications importantes, incluant les suivantes :

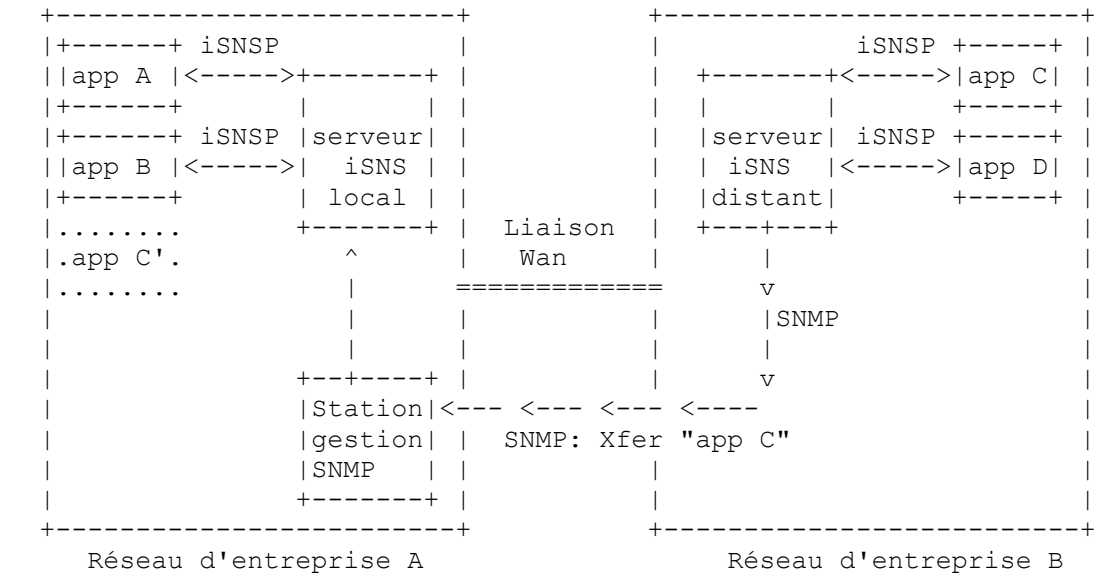
1) Une organisation indépendante a besoin de transférer des informations de mémorisation à une organisation différente. Chaque organisation conserve indépendamment sa propre infrastructure iSNS. Pour faciliter la découverte des bases de mémorisation de l'organisation homologue en utilisant IP, les enregistrements de la base de données iSNS peuvent être transférés entre des serveurs iSNS d'autorité de chaque organisation. Cela permet que des sessions de mémorisation soient établies directement entre les appareils résidant dans l'infrastructure de réseau de mémorisation de chaque organisation sur un réseau IP commun.

2) Plusieurs serveurs iSNS sont désirés pour assurer la redondance. Les serveurs de sauvegarde doivent conserver des copies de la base de données du serveur principal qui changent de façon dynamique.

Pour prendre en charge les applications ci-dessus, les informations d'un serveur iSNS peuvent être distribuées aux autres serveurs iSNS soit en utilisant le protocole iSNS, soit par des mécanismes hors bande utilisant des protocoles non iSNS. Les exemples qui suivent illustrent des méthodes possibles pour transférer des enregistremements de données entre les serveurs iSNS. Dans le premier exemple, une base d'informations LDAP d'arrière plan est utilisée pour prendre en charge le serveur iSNS, et les données sont transférées en utilisant le protocole LDAP. Une fois achevé le transfert d'enregistrements à l'appareil distant, il devient visible et accessible aux appareils locaux en utilisant le serveur iSNS local. Cela permet aux appareils locaux d'établir des sessions avec les appareils distants (pourvu que les fonrtières de pare-feu puissent être négociées).



Dans le diagramme ci-dessus, deux partenaires d'affaires souhaitent partager la mémorisation de "app C". En utilisant LDAP, l'enregistrement pour "app C" peut être transféré du réseau B au réseau A. Une fois accessible au serveur iSNS local dans le réseau A, les appareils locaux A et B peuvent maintenant découvrir et se connecter à "app C".



Le diagramme ci-dessus illustre un second exemple de la façon dont les enregistrements iSNS peuvent être partagés. Cette méthode utilise une station de gestion fondée sur SNMP pour restituer (GET) l'enregistrement désiré pour "app C" manuellement, et ensuite le mémoriser (SET) directement sur le serveur local iSNS. Une fois l'enregistrement transféré au serveur local iSNS dans le réseau A, "app C" devient visible et accessible (pourvu que les limites du pare-feu puissent être négociées) aux autres appareils dans le réseau A.

D'autres méthodes, incluant des protocoles propriétaires, peuvent être utilisées pour transférer des enregistrements d'appareils entre serveurs iSNS. La discussion et l'explication de ces méthodes sort du domaine d'application du document.

2.8 Serveurs iSNS de sauvegarde

Ce paragraphe offre un large cadre pour la mise en œuvre et le déploiement de serveurs iSNS de sauvegarde. La défaillance et la récupération de serveur sont des sujets de recherche continus, et la résolution adéquate des problèmes comme un cerveau partagé et la sélection d'un serveur principal dépendent des exigences spécifiques de mise en œuvre et des besoins de déploiement. Les mécanismes de reprise sur défaillance discutés dans le présent document se concentrent sur l'interaction entre clients iSNS et serveurs iSNS. Précisément, ce qui est couvert dans ce document inclut ce qui suit :

- Le comportement du client iSNS et l'interaction du protocole iSNS entre le client et plusieurs serveurs iSNS, dont certains sont des serveurs de sauvegarde.
- Les comportements de reprise sur défaillance exigés de la collection des serveurs iSNS qui inclut des serveurs actifs et des serveurs de sauvegarde.

Cependant, noter que le présent document ne spécifie pas les exigences complètes de la fonction de reprise sur défaillance de chaque serveur iSNS. En particulier, il ne spécifie pas l'ensemble complet d'interactions de protocole entre les serveurs iSNS qui sont requis de réaliser une opération de récupération stable d'une manière interopérable.

Pour les besoins de cette discussion, les mécanismes de sauvegarde spécifiés relèvent de l'interaction entre différents serveurs logiques iSNS. Noter qu'il est possible de créer plusieurs serveurs iSNS physiques pour former une seule grappe logique de serveurs iSNS, et donc de répartir le traitement des transactions iSNS parmi plusieurs serveurs physiques. Cependant, une discussion plus détaillée des interactions entre serveurs physiques au sein d'une grappe logique de serveurs iSNS sort du domaine d'application du présent document.

Plusieurs serveurs logiques iSNS peuvent être utilisés pour fournir une redondance au cas où le serveur iSNS actif aurait une défaillance ou serait supprimé du réseau. Les méthodes décrites au paragraphe 2.7 ci-dessus peuvent être utilisées pour transférer les enregistrements de serveur de noms à des serveurs iSNS de sauvegarde. Chaque serveur de sauvegarde conserve une copie redondante de la base de données du serveur de noms qui se trouve dans le serveur iSNS principal, et peut répondre aux messages de protocole iSNS de la même façon que le serveur actif. Chaque serveur de sauvegarde DEVRAIT surveiller la santé et l'état du serveur iSNS actif, incluant des vérifications pour s'assurer que sa propre base de données est synchronisée avec celle du serveur actif. Comment chaque serveur de sauvegarde accomplit cela dépend de la

mise en œuvre, et peut (ou non) inclure d'utiliser le protocole iSNS. Si le protocole iSNS est utilisé, le serveur de sauvegarde PEUT alors s'enregistrer dans la base de données iSNS du serveur actif comme nœud de gestion, ce qui lui permet de recevoir les notifications de changement d'état.

Généralement, l'administrateur ou un processus automatique est chargé de la désignation initiale et des désignations suivantes du serveur principal et de chaque serveur de sauvegarde.

Un maximum de un serveur logique de sauvegarde iSNS DEVRA exister à toute adresse IP individuelle, afin d'éviter des conflits provenant de l'écoute de multiples serveurs sur le même numéro d'accès canonique iSNS TCP ou UDP.

Le battement de cœur iSNS peut aussi être utilisé pour coordonner la désignation et le choix des serveurs iSNS, principal et de sauvegarde.

Chaque serveur de sauvegarde DOIT noter sa préséance relative dans la liste des serveurs de sauvegarde au serveur actif. Si sa préséance n'est pas encore connue, chaque serveur de sauvegarde PEUT l'apprendre du messages Battement de cœur iSNS, en notant la position de son adresse IP dans la liste ordonnée des adresses IP de serveurs de sauvegarde. Par exemple, si il est la première sauvegarde dans la liste du message Battement de cœur, sa préséance de sauvegarde est 1. Si il est le troisième serveur de sauvegarde de la liste, sa préséance de sauvegarde et alors de 3.

Si un serveur de sauvegarde établit qu'il a perdu la connexité au serveur actif et aux autres serveurs de sauvegarde de préséance supérieure, il DEVRAIT alors supposer qu'il est le serveur actif. La méthode pour déterminer si la connexité a été perdue est spécifique de la mise en œuvre. Une approche possible est de supposer que si le serveur de sauvegarde ne reçoit pas les messages Battement de cœur iSNS depuis un certain temps, la connexité au serveur actif a été perdue. Autrement, le serveur de sauvegarde peut établir des connexions TCP avec le serveur actif et les autres serveurs de sauvegarde, avec la perte de connexité déterminée par la non réponse aux échos périodiques ou aux messages d'interrogation (en utilisant iSNSP, SNMP, ou d'autres protocoles).

Quand un serveur de sauvegarde devient le serveur actif, il DEVRA assumer toutes les responsabilités de serveur actif, incluant (si c'est utilisé) la transmission du message Battement de cœur iSNS. Si il émet le battement de cœur iSNS, le serveur de sauvegarde remplace les entrées d'adresse IP et d'accès TCP/IP du serveur actif par sa propre adresse IP et accès TCP/UDP, et il commence à incrémenter le champ compteur à partir de la dernière valeur connue provenant du serveur actif iSNS précédent. Cependant, il NE DOIT PAS changer la liste ordonnée originale des entrées d'adresse IP et accès TCP/UDP des serveurs de sauvegarde. Si le serveur de sauvegarde principal ou autre serveur de sauvegarde de préséance supérieure revient, alors le serveur actif existant est chargé de s'assurer que la base de données du nouveau serveur actif est à jour avant de se remettre à son état original de sauvegarde.

Comme les serveurs iSNS principal et de sauvegard maintiennent une base de données coordonnée, aucun réenregistrement par un client iSNS n'est requis lorsque un serveur de sauvegarde prend le rôle de serveur actif. De même, aucun réenregistrement par un client iSNS n'est requis quand le précédent serveur principal revient au rôle de serveur actif.

2.9 Protocoles de transport

Le protocole iSNS est neutre à l'égard du transport. Les messages d'interrogation et d'enregistrement sont transportés sur TCP ou UDP. Les messages Battement de cœur iSNS sont transportés en utilisant la diffusion ou diffusion groupée IP.

2.9.1 Utilisation de TCP pour les communications iSNS

Il DOIT être possible d'utiliser TCP pour la communication iSNS. Le serveur iSNS DOIT accepter les connexions TCP pour les enregistrements de client. Pour recevoir les enquêtes d'état d'entité (ESI, *Entity Status Inquiry*) (voir au paragraphe 5.6.5.13) qui surveillent l'utilisation de TCP, le client enregistre l'intervalle d'ESI de portail et le numéro de l'accès TCP qui va être utilisé pour recevoir les messages ESI. Le serveur iSNS initie la connexion TCP utilisée pour livrer le message ESI. Cette connexion TCP n'a pas besoin d'être continuellement ouverte.

Pour recevoir des notifications SCN en utilisant TCP, le client enregistre le gabarit binaire iSCSI ou iFCP de SCN et le numéro de l'accès TCP dans le portail utilisé pour recevoir les SCN. Le serveur iSNS initie la connexion TCP utilisée pour livrer le message de SCN. Cette connexion TCP n'a pas besoin d'être continuellement ouverte.

Il est possible au client iSNS d'utiliser la même connexion TCP pour les interrogations de SCN, d'ESI,et d'iSNS. Autrement, des connexions séparées peuvent être utilisées.

2.9.2 Utilisation de UDP pour les communications iSNS

Le serveur iSNS PEUT accepter des messages UDP pour des enregistrements de client. Le serveur iSNS DOIT accepter les enregistrements provenant de clients qui demandent des messages ESI et SCN fondés sur UDP.

Pour recevoir des messages de surveillance ESI fondés sur UDP, le client enregistre le numéro d'accès UDP dans au moins un portail utilisé pour recevoir et répondre aux messages ESI provenant du serveur iSNS. Si une entité réseau a plusieurs portails avec des accès UDP enregistrés pour ESI, les messages ESI DEVRONT alors être livrés à chaque portail enregistré pour recevoir de tels messages.

Pour recevoir des messages de SCN fondés sur UDP, le client enregistre le numéro d'accès UDP dans au moins un portail utilisé pour recevoir les messages de SCN provenant du serveur iSNS. Si une entité réseau a plusieurs portails avec des accès UDP enregistrés pour les SCN, les messages de SCN DEVRONT alors être livrés à chaque portail enregistré pour recevoir de tels messages.

Lors de l'utilisation de UDP pour transporter les messages iSNS, chaque datagramme UDP DOIT contenir exactement une PDU iSNS (voir la Section 5).

2.9.3 Diffusion groupée iSNS et messages en diffusion

Les messages de diffusion groupée iSNS sont transportés en utilisant la diffusion ou la diffusion groupée IP. Le battement de cœur iSNS est le seul message iSNS en diffusion ou diffusion groupée. Ce message est généré par le serveur iSNS et envoyé à tous les clients iSNS qui écoutent sur l'adresse de diffusion groupée IP allouée par le battement de cœur iSNS.

2.10 Exigences du protocole simple de gestion de réseau (SNMP)

Le serveur iSNS peut être géré via la MIB iSNS [RFC4939] en utilisant un cadre de gestion SNMP [RFC3411]. Prière de se reporter à la Section 7 de la [RFC3410] pour une vue d'ensemble détaillée des documents qui décrivent le cadre actuel de gestion normalisé de l'Internet. La MIB iSNS fournit la capacité de configurer et surveiller un serveur iSNS sans utiliser le protocole iSNS directement. Les cadres de gestion SNMP ont plusieurs exigences pour l'indexation des objets afin que les objets soient ajoutés ou accessibles.

SNMP utilise un identifiant d'objet (OID, *Object Identifier*) pour l'identification d'objet. La taille de chaque OID est restreinte à un maximum de 128 sous identifiants. Les deux protocoles iSCSI et iFCP contiennent des identifiants, comme le nom iSCSI, qui font plus de 128 caractères. Utiliser de tels identifiants comme un indice résulterait en plus de 128 sous identifiants par OID. Afin de prendre en charge les objets qui ont des identifiants de clés dont la longueur maximum est supérieure à la longueur maximum supportée par SNMP, le serveur iSNS fournit des identifiants secondaires d'indice d'entiers non zéro. Ces indices DEVRONT être persistents pendant aussi longtemps que le serveur est actif. De plus, les valeurs d'indice pour les objets récemment désenregistrés NE DEVRAIENT PAS être réutilisées à court terme. Les attributs d'objets, incluant les indices, sont décrits en détail à la Section 6.

Pour que les applications de gestion fondées sur SNMP créent une nouvelle entrée dans un tableau d'objets, un OID valide doit être disponible pour spécifier la rangée du tableau. Le serveur iSNS prend cela en charge en fournissant, pour chaque type d'objet qui peut être ajouté via SNMP, un attribut d'objet qui retourne le prochain indice d'entier non zéro disponible. Cela permet au client SNMP de demander qu'un OID soit utilisé pour enregistrer un nouvel objet dans le serveur. Les attributs d'objets, incluant les prochains attributs d'indice disponible, sont décrits en détail à la Section 6.

3. Modèle d'objet iSNS

iSNS fournit le cadre pour l'enregistrement, la découverte, et la gestion des appareils iSCSI et des appareils fondés sur canal fibre (en utilisant iFCP). Ce cadre architectural fournit les éléments nécessaires pour décrire les divers objets et attributs d'appareil de mémorisation qui peuvent exister dans un réseau de mémorisation IP. Les objets définis dans de cadre architectural incluent des entités réseau, des portails, des nœuds de mémorisation, des appareils FC, des domaines de découverte, et des ensembles de domaines de découverte. Chacun de ces objets est décrit plus en détails dans les paragraphes qui suivent.

3.1 Objet Entité réseau

L'objet Entité réseau est un conteneur d'objets Nœud de mémorisation et d'objets Portail. Il représente l'infrastructure qui prend en charge l'accès à un ensemble unique d'un ou plusieurs nœuds de mémorisation. L'attribut Identifiant d'entité

distingue de façon univoque une entité réseau, et c'est la clé utilisée pour enregistrer un objet Entité réseau dans un serveur iSNS. Tous les nœuds de mémorisation et portails contenus dans un seul objet Entité fonctionnent comme une unité cohésive.

Noter qu'il est possible à un seul appareil physique ou passerelle d'être représenté par plus d'une entité réseau logique dans la base de données iSNS. Par exemple, un des nœuds de mémorisation sur un appareil physique peut être accessible à partir d'un seul sous ensemble des interfaces réseau (c'est-à-dire, des portails) disponibles sur cet appareil. Dans ce cas, une entité réseau logique (c'est-à-dire, une "entité cachée") est créée et utilisée pour contenir les portails et nœuds de mémorisation qui peuvent opérer de façon coopérative. Aucun objet (portails, nœuds de mémorisation, etc.) ne peut être contenu dans plus d'une entité réseau logique.

De même, il est possible qu'une entité réseau logique soit prise en charge par plus d'un appareil physique ou passerelle. Par exemple, plusieurs passerelles FC-iSCSI peuvent être utilisées pour ponter des appareils FC dans un seul réseau canal fibre. Collectivement, les multiples passerelles peuvent être utilisées pour prendre en charge une seule entité réseau logique qui est utilisée pour contenir tous les appareils dans ce réseau canal fibre.

3.2 Objet Portail

L'objet Portail est une interface à travers laquelle l'accès aux nœuds de mémorisation au sein de l'entité réseau peut être obtenu. Les attributs d'adresse IP et de numéro d'accès TCP/UDP distinguent de façon univoque un objet Portail, et les clés utilisées pour enregistrer un objet Portail sont combinées dans un serveur iSNS. Un portail est contenu dans une entité réseau et une seule, et peut être contenu dans un ou plusieurs DD (voir le paragraphe 3.6).

3.3 Objet Nœud de mémorisation

L'objet Nœud de mémorisation est le point d'extrémité logique d'une session iSCSI ou iFCP. Dans iFCP, le point d'extrémité de session est représenté par le nom d'accès mondial (WWPN, *World Wide Port Name*). Dans iSCSI, le point d'extrémité de session est représenté par le nom iSCSI de l'appareil. Pour iSCSI, l'attribut de nom iSCSI distingue de façon univoque un nœud de mémorisation, et est la clé utilisée pour enregistrer un objet Nœud de mémorisation dans un serveur iSNS. Pour iFCP, l'attribut Nom d'accès FC (WWPN) distingue de façon univoque un nœud de mémorisation, et est la clé utilisée pour enregister un objet Nœud de mémorisation dans le serveur iSNS. Le nœud de mémorisation est contenu dans un seul objet Entité réseau et peut être contenu dans un ou plusieurs DD (voir au paragraphe 3.6).

3.4 Objet Groupe portail

L'objet Groupe portail (PG) représente une association entre un portail et un nœud iSCSI. Chaque portail et nœud de mémorisation iSCSI enregistré dans une entité peut être associé en utilisant un objet Groupe portail (PG). L'étiquette PG (PGT, *PG Tag*) si elle est non nulle, indique que le portail associé fournit l'accès au nœud de mémorisation iSCSI associé dans l'entité. Tous les portails qui ont la même valeur de PGT pour un nœud de mémorisation iSCSI spécifique permettent l'accès coordonné à ce nœud.

Un objet PG PEUT être enregistré quand un nœud de mémorisation portail ou iSCSI est enregistré. Chaque portail à une association de nœud iSCSI est représenté par un seul objet PG. Afin qu'un portail fournisse l'accès à un nœud iSCSI, la PGT de l'objet PG DOIT être non nulle. Si la valeur de PGT enregistrée pour un portail et nœud iSCSI spécifié est nulle, ou si aucune valeur de PGT n'est enregistrée, le portail ne fournit pas d'accès à ce nœud iSCSI dans l'entité.

La valeur de PGT indique si l'accès à un nœud iSCSI peut être coordonné à travers plusieurs portails. Tous les portails qui ont la même valeur de PGT pour un nœud iSCSI spécifique peuvent fournir un accès coordonné à ce nœud iSCSI. Conformément à la spécification iSCSI, l'accès coordonné à un nœud iSCSI indique la capacité de coordonner une session iSCSI avec les connexions qui couvrent ces portails [RFC3720].

L'objet PG est dinstingué de façon univoque par les valeurs de nom iSCSI, adresse IP de portail, et accès TCP de portail des objets associés Nœud de mémorisation et Portail. Elles sont représentées dans le serveur iSNS respectivement par les attributs nom iSCSI de PG, adresse IP de portail PG, et accès TCP/UDP de portail PG. L'objet PG est aussi distingué de façon univoque dans le serveur iSNS par la valeur d'indice de PG.

Un nouvel objet PG ne peut être enregistré qu'en faisant référence à son objet associé Nœud de mémorisation iSCSI ou Portail. Un objet PG préexistant peut être modifié ou interrogé en utilisant son indice de groupe portail comme clé de message, ou en faisant référence à son objet associé Nœud de mémorisation iSCSI ou Portail. Une TLV de longueur 0 d'Étiquette, Longueur, Valeur est utilisée pour enregistrer une valeur de PGT NULLE.

L'objet PG n'est désenregistré que si et seulement si ses objets associés Nœud iSCSI et Portail sont tous deux supprimés.

3.5 Objet Appareil

L'appareil FC représente le nœud canal fibre. Cet objet contient des informations qui peuvent être utiles dans la gestion de l'appareil canal fibre. L'attribut Nom de nœud FC (WWNN) distingue de façon univoque un appareil FC, et c'est la clé utilisée pour enregistrer un objet Appareil FC dans le serveur iSNS.

L'appareil FC est contenu dans un ou plusieurs objets Nœud de mémorisation.

3.6 Objet Domaine de découverte

Les domaines de découverte (DD) sont un mécanisme de sécurité et de gestion utilisé pour administrer l'accès et la connexité à des appareils de mémorisation. Pour l'interrogation et l'enregistrement, ils sont considérés comme des conteneurs pour les objets Nœud de mémorisation et Portail. Une interrogation par un client iSNS qui ne provient pas d'un nœud de gestion retourne seulement des informations sur les objets avec lesquels il partage au moins un DD actif. La seule exception à cette règle est avec les portails ; si les nœuds de mémorisation d'une entité réseau sont enregistrés dans le DD sans portails, alors tous les portails de cette entité réseau sont des membres implicites de ce DD. L'attribut Identifiant de domaine de découverte (DD_ID) distingue de façon univoque un objet Domaine de découverte, et c'est la clé utilisée pour enregistrer un objet Domaine de découverte dans le serveur iSNS.

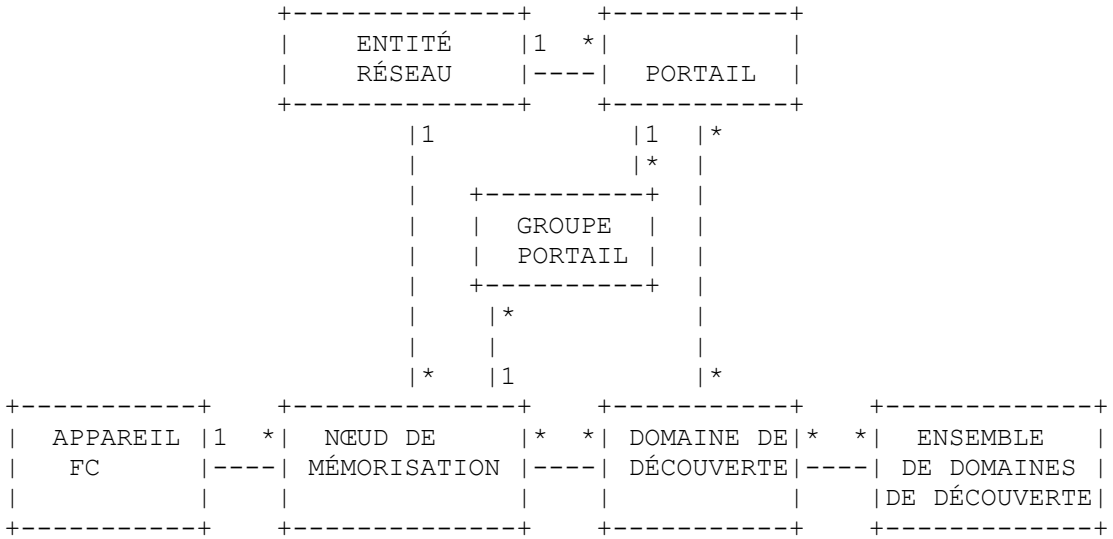
Un DD est considéré comme actif si il est membre d'au moins un ensemble actif de DD. Les DD qui ne sont pas membres d'au moins un DDS activé sont considérés désactivés. Un nœud de mémorisation peut être membre d'un ou plusieurs DD. Un DD activé établit la connexité entre les nœuds de mémorisation dans ce DD.

3.7 Objet Ensemble de domaine de découverte

L'ensemble de domaines de découverte (DDS, *Discovery Domain Set*) est un objet conteneur pour les domaines de découverte (DD). Les DDS peuvent contenir un ou plusieurs DD. De même, chaque DD peut être membre d'un ou plusieurs DDS. Les DDS sont un mécanisme pour mémoriser des ensembles coordonnés de transpositions de DD dans le serveur iSNS. Les DD actifs sont membres d'au moins un ensemble de DD actifs. Plusieurs DDS peuvent être considérés comme actifs au même moment. L'attribut Identifiant d'ensemble de domaines de découverte (DDS_ID) distingue de façon univoque un objet Ensemble de domaines de découverte, et c'est la clé utilisée pour enregistrer un objet Ensemble de domaines de découverte dans le serveur iSNS.

3.8 Modèle de base de données

Comme présenté au client iSNS, chaque objet d'un type spécifique dans la base de données iSNS DOIT avoir un ordre linéaire interne implicite sur la base de la ou des clés pour ce type d'objet. Cet ordre fournit la capacité de répondre aux interrogations DevGetNext (voir le paragraphe 5.6.5.3). L'ordre des objets dans la base de données iSNS NE DEVRAIT PAS être changé par rapport à cet ordre implicite, par suite des insertions et suppressions d'objets. C'est-à-dire que l'ordre relatif des entrées d'objets subsistantes dans la base de données iSNS DEVRAIT être préservé afin que le message DevGetNext rencontre généralement un comportement raisonnable.
Le diagramme suivant montre les divers objets décrits ci-dessus et leurs relation mutuelles.



* représente 0 à plusieurs relations possibles

4. Exigences de mise en œuvre de iSNS

Cette section détaille les exigences spécifiques pour prendre en charge chacun de ces protocoles de mémorisation IP. Les exigences de mise en œuvre pour la sécurité sont décrites à la Section 7.

4.1 Exigences de iSCSI

L'utilisation de iSNS pour la prise en charge de iSCSI est FACULTATIVE. Les appareils iSCSI PEUVENT être configurés manuellement avec le nom iSCSI et l'adresse IP des appareils homologues, sans l'aide ou l'intervention de iSNS. Les appareils iSCSI peuvent aussi utiliser SLP [RFC2608] pour découvrir les appareils iSCSI homologues. Cependant, iSNS est utile pour adapter un réseau de mémorisation à un plus grand nombre d'appareils iSCSI.

4.1.1 Attributs requis pour la prise en charge de iSCSI

Les attributs suivants sont disponibles pour prendre en charge iSCSI. Les attributs indiqués dans la colonne "EXIGÉ pour le serveur" DOIVENT être mis en œuvre par un serveur iSNS utilisé pour prendre en charge iSCSI. Les attributs indiqués dans la colonne "EXIGÉ pour le client" DOIVENT être mis en œuvre par un appareil iSCSI qui choisit d'utiliser iSNS. Les attributs indiqués dans la colonne "Clé" identifient de façon univoque le type d'objet dans le serveur iSNS. On trouvera à la Section 6 une description plus détaillée de chaque attribut.

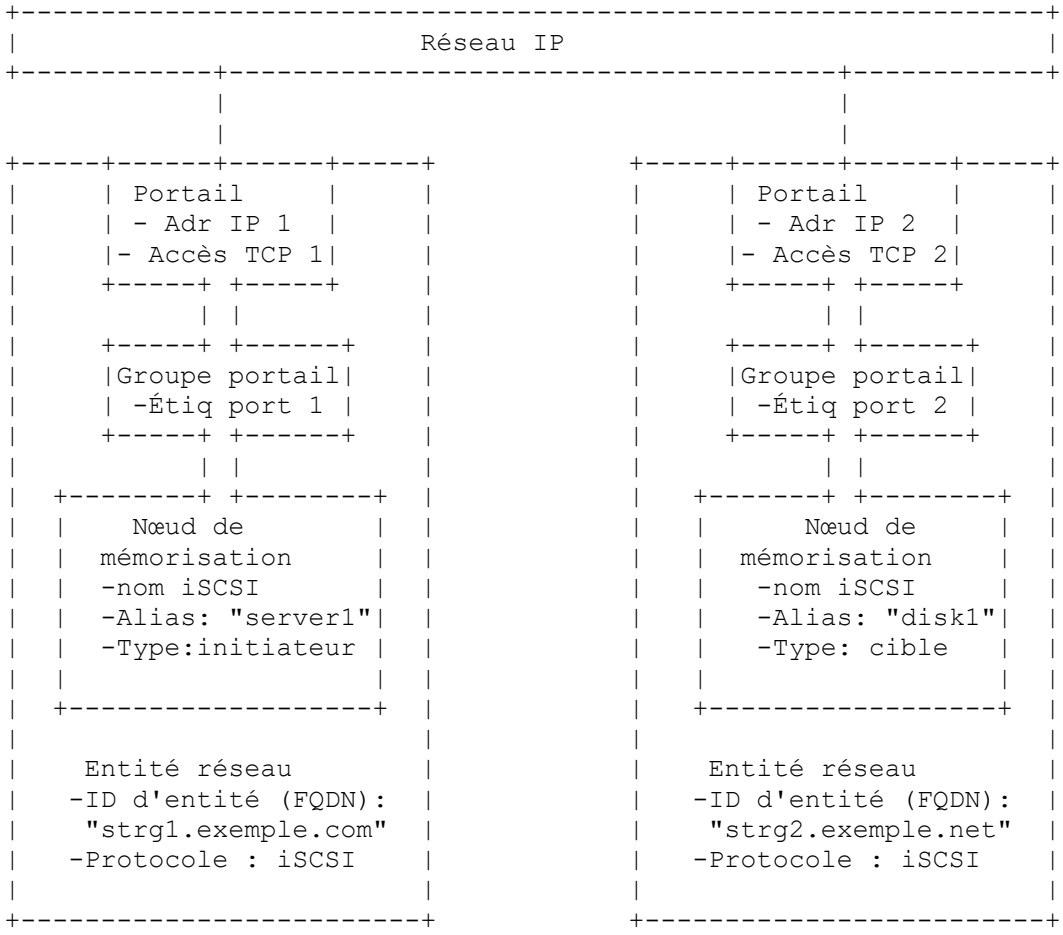
			EXIGÉ pour :	
Objet	**Attribut**	**Clé**	**Serveur**	**Client**
Entité réseau	Identifiant d'entité	*	*	*
	Protocole d'entité		*	*
	Adresse IP de gestion	*		
	Horodatage		*	
	Gamme de version de protocole		*	
	Période d'enregistrement		*	
	Indice d'entité		*	
	Proposition d'entité IKE phase-1			
	Certificat d'entité			
Portail	Adresse IP	*	*	*
	Accès TCP/UDP	*	*	*
	Nom symbolique de portail		*	
	Intervalle d'ESI		*	
	Accès d'ESI		*	
	Indice de portail		*	
	Accès de SCN		*	
	Gabarit binaire de portail de sécurité		*	
	Proposition de portail IKE phase-1			
	Proposition de portail IKE phase-2			
	Certificat de portail			
Groupe portail	Nom iSCSI de PG	*	*	*
	Adresse IP de PG	*	*	*
	Accès TCP/UDP de PG	*	*	*
	Étiquette de PG		*	*
	Indice de PG		*	
Nœud de mémorisation	Nom iSCSI	*	*	*
	Type de nœud iSCSI		*	*
	Alias		*	
	Gabarit binaire de SCN iSCSI		*	
	Indice de nœud iSCSI		*	
	Jeton WWNN			
	Méthode d'authentification iSCSI			
Domaine de découverte	ID de DD	*	*	*
	Nom symbolique de DD		*	
	Indice de nœud iSCSI de membre de DD		*	
	Nom iSCSI de membre de DD		*	
	Indice de portail de membre de DD		*	

	Adresse IP de portail de membre de DD	*	
	Accès TCP/UDP de portail de membre de DD	*	
	Caractéristiques de DD	*	
Ensemble de domaines de découverte	Identifiant de DDS	*	*
	Nom symbolique de DDS	*	
	État de DDS	*	

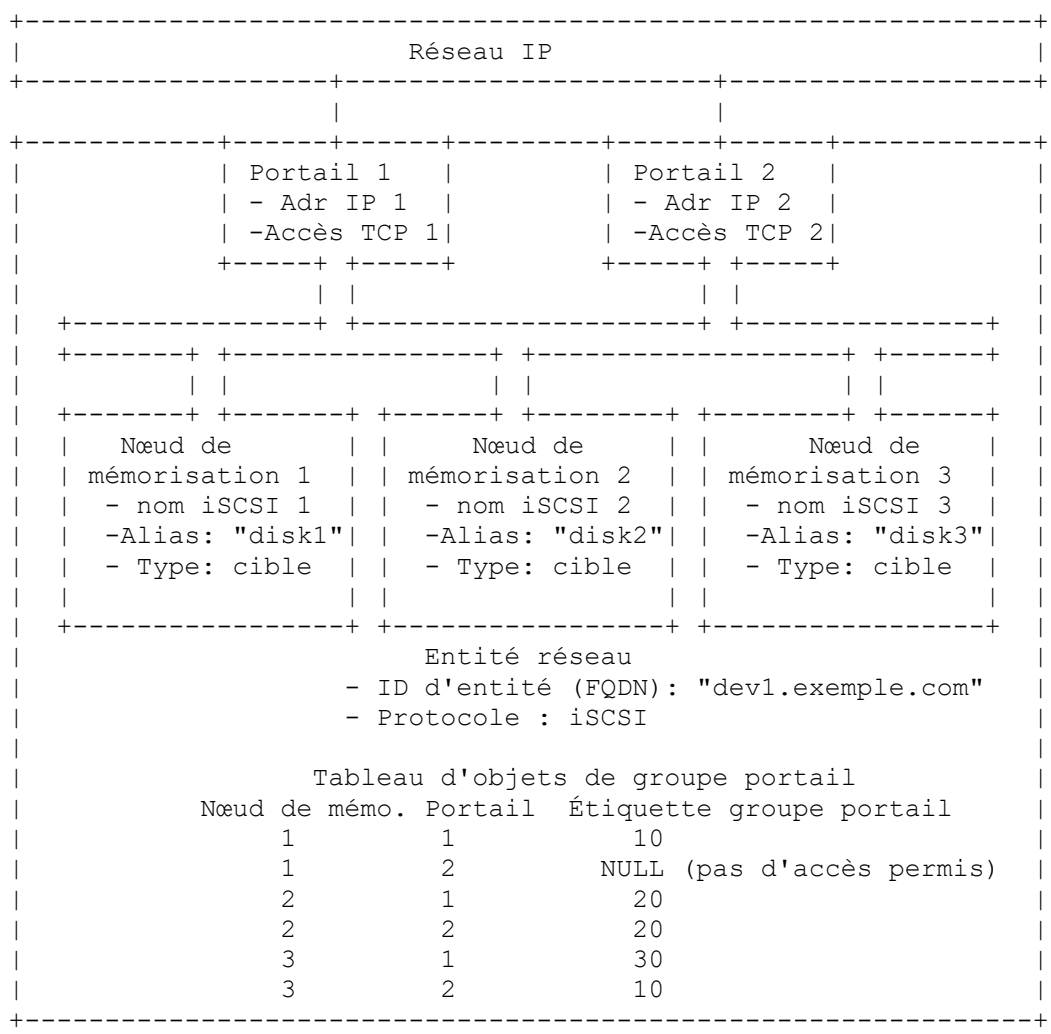
Tous les attributs iSCSI spécifiés par l'usager et spécifiés par le fabricant sont de mise en œuvre et d'utilisation FACULTATIVE.

4.1.2 Exemples : Diagrammes des modèles d'objet iSCSI

Le diagramme suivant modélise comment un simple initiateur et cible fondé sur iSCSI est représenté en utilisant les objets de base de données mémorisés dans le serveur iSNS. Dans cette mise en œuvre, chaque cible et initiateur est rattaché à un seul portail.



Le modèle d'objet peut être étendu pour décrire des appareils plus complexes, comme un appareil iSCSI avec plus d'un contrôleur de mémorisation, dans lequel chaque contrôleur est accessible à travers une des multiples interfaces de portail, utilisant éventuellement plusieurs groupes portails. Les contrôleurs de mémorisation sur cet appareil peuvent être accédés par d'autres interfaces portail si une des interfaces d'origine devait avoir une défaillance. Le diagramme suivant décrit un tel appareil :



Le nœud de mémorisation 1 est accessible via Portail 1 avec une PGT de 10. Il n'y a pas d'étiquette de groupe portail (PGT) allouée pour Portail 2, de sorte que le nœud de mémorisation 1 ne peut pas avoir d'accès via Portail 2.

Le nœud de mémorisation 2 peut être accessible via Portail 1 et Portail 2. Comme le nœud de mémorisation 2 a la même valeur de PGT allouée aux deux Portail 1 et 2, dans ce cas 20, l'accès coordonné via les portails est disponible [RFC3720].

Le nœud de mémorisation 3 peut être accessible via Portail 1 ou Portail 2. Cependant, comme le nœud de mémorisation 3 a des valeurs de PGT différentes allouées à chaque portail, dans les cas 10 et 30, l'accès n'est pas coordonné [RFC3720]. Parce que les PGT sont allouées au sein du contexte d'un nœud de mémorisation, les valeurs de PGT de 10 utilisées pour le nœud de mémorisation 1 et le nœud de mémorisation 3 sont sans relation entre elles.

4.1.3 Messages de commande et réponse requis pour la prise en charge de iSCSI

Les messages et réponses iSNSP suivants sont disponibles pour prendre en charge iSCSI. Les messages indiqués dans la colonne "EXIGÉ pour le serveur" DOIVENT être mis en œuvre dans les serveurs iSNS utilisés pour les appareils iSCSI. Les messages indiqués dans la colonne "EXIGÉ pour le client" DOIVENT être mis en œuvre dans les appareils iSCSI qui choisissent d'utiliser le serveur iSNS.

			EXIGÉ pour :	
Description de message	**Abréviation**	**ID de fonction**	**Serveur**	**Client**
RÉSERVÉ		0x0000		
Demande d'enregistrement d'attribut d'appareil	DevAttrReg	0x0001	*	*
Demande d'interrogation d'attribut d'appareil	DevAttrQry	0x0002	*	*
Demande d'aller au prochain appareil	DevGetNext	0x0003	*	
Demande de désenregistrement d'appareil	DevDereg	0x0004	*	*
Demande d'enregistrement de SCN	SCNReg	0x0005	*	
Demande de désenregistrement de SCN	SCNDereg	0x0006	*	
Événement de SCN	SCNEvent	0x0007	*	

Notification de changement d'état	SCN	0x0008	*	
Enregistrer le DD	DDReg	0x0009	*	*
Désenregistrer le DD	DDDereg	0x000A	*	*
Enregistrer le DDS	DDSReg	0x000B	*	*
Désenregistrer le DDS	DDSDereg	0x000C	*	*
Enquête sur l'état d'entité	ESI	0x000D	*	
Battement de cœur de service de nom	Heartbeat	0x000E		
RÉSERVÉ		0x000F-0x00FF		
Spécifique du fabricant		0x0100-0x01FF		
RÉSERVÉ		0x0200-0x7FFF		

Voici les messages de réponse iSNSP pour la prise en charge de iSCSI :

			EXIGÉ pour :	
Message de réponse	**Abréviation**	**ID de fonction**	**Serveur**	**Client**
RÉSERVÉ		0x8000		
Réponse d'enregistrement d'attribut d'appareil	DevAttrRegRsp	0x8001	*	*
Réponse d'interrogation d'attribut d'appareil	DevAttrQryRsp	0x8002	*	*
Réponse d'aller au prochain appareil	DevGetNextRsp	0x8003	*	
Réponse de désenregistrement d'appareil	DevDeregRsp	0x8004	*	*
Réponse d'enregistrement de SCN	SCNRegRsp	0x8005	*	
Réponse de sésenregistrement de SCN	SCNDeregRsp	0x8006	*	
Réponse d'événement de SCN	SCNEventRsp	0x8007	*	
Réponse de SCN	SCNRsp	0x8008	*	
Réponse d'enregstrement de DD	DDRegRsp	0x8009	*	*
Réponse de désenregistrement de DD	DDDeregRsp	0x800A	*	*
Réponse d'enregstrement de DDS	DDSRegRsp	0x800B	*	*
Réponse de désenregistrement de DDS	DDSDeregRsp	0x800C	*	*
Réponse d'enquête d'état d'entité	ESIRsp	0x800D	*	
RÉSERVÉ		0x800E-0x80FF		
Spécifique de fabricant		0x8100-0x81FF		
RÉSERVÉ		0x8200-0xFFFF		

4.2 Exigences iFCP

Dans iFCP, l'utilisation de iSNS est EXIGÉE. Il n'existe pas de solution de remplacement pour prendre en charge les fonctions iFCP de dénomination et de découverte.

4.2.1 Attributs exigés pour la prise en charge de iFCP

Le tableau suivant affiche les attributs qui sont utilisés par iSNS pour prendre en charge iFCP. Les attributs indiqués dans la colonne "EXIGÉ pour le serveur" DOIVENT être mis en œuvre par le serveur iSNS qui prend en charge iFCP. Les attributs indiqués dans la colonne "EXIGÉ pour le client" DOIVENT être pris en charge par les passerelles iFCP. Les attributs indiqués dans la colonne "Clé" identifient de façon univoque le type d'objet dans le serveur iSNS. Une description plus détaillée de chaque attribut se trouve à la Section 6.

			EXIGÉ pour :	
Objet	**Attribut**	**Clé**	**Serveur**	**Client**
Entité réseau	Identifiant d'entité	*	*	*
	Protocole d'entité		*	*
	Adresse IP de gestion		*	
	Horodatage		*	
	Gamme de version de protocole		*	
	Période d'enregistrement			
	Indice d'entité			
	Proposition d'entité IKE phase-1			
	Certificat d'entité			
Portail	Adresse IP	*	*	*
	Accès TCP/UDP	*	*	*
	Nom symbolique		*	
	Intervalle d'ESI		*	
	Accès d'ESI		*	

	Accès de SCN		*	
	Proposition de portail IKE phase-1			
	Proposition de portail IKE phase-2			
	Certificat de portail			
	Gabarit binaire de sécurité		*	
Nœud de mémorisation (accès FC)	Nom d'accès FC (WWPN)	*	*	*
	Identifiant d'accès		*	*
	Type d'accès FC		*	*
	Nom symbolique d'accès		*	
	Nom d'accès de tissu (FWWN)		*	
	Adresse de matériel		*	
	Adresse IP d'accès		*	
	Classe de service		*	
	Types FC FC-4		*	
	Descripteurs FC FC-4		*	
	Caractéristiques FC FC-4		*	
	Gabarit binaire de SCN		*	
	Rôle d'accès iFCP		*	
	Nom d'accès permanent		*	
Appareil FC (nœud FC)	Nom de nœud FC (WWNN)	*	*	*
	Nom symbolique de nœud		*	
	Adresse IP de nœud		*	
	Adresse IP de nœud		*	
	Nom de mandataire iSCSI			
Domaine de découverte	Identifiant de DD	*	*	*
	Nom symbolique de DD		*	
	Nom d'accès FC de membre du DD		*	
	Indice de portail de membre du DD		*	
	Adresse IP de portail de membre du DD		*	
	Accès TCP/UDP de portail de membre du DD		*	
Ensemble de domaines de découverte	Identifiant de DDS		*	*
	Nom symbolique de DDS		*	
	État de DDS		*	
Autre	Nom de commutateur			
	Identifiant préféré			
	Identifiant alloué			
	Identifiant de tissu virtuel			

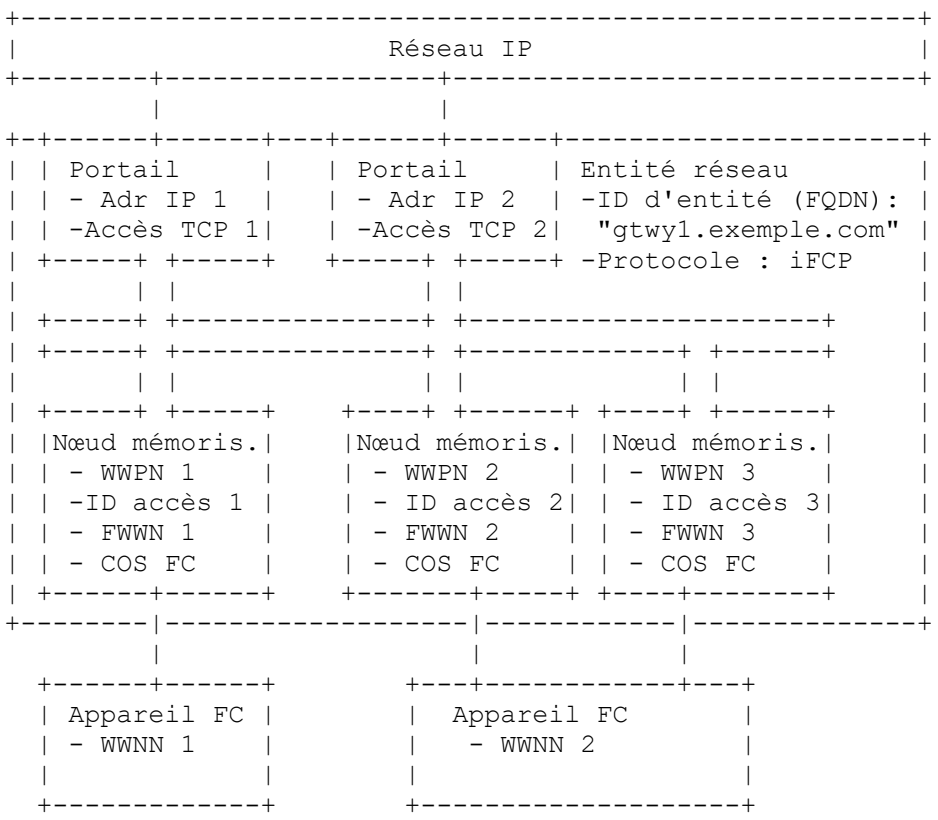
Tous les attributs iFCP spécifié par l'utilisateur et spécifiés par le fabricant sont de mise en œuvre et d'utilisation FACULTATIVE.

4.2.2 Exemple : Diagramme modèle d'objet iFCP

Le protocole iFCP permet aux appareils canal fibre ou tissus canal fibre natifs connectés à une passerelle iFCP d'être directement en réseau en utilisant IP.

Quand il prend en charge iFCP, le serveur iSNS mémorise les attributs d'appareil canal fibre, les attributs de passerelle iFCP, et les attributs de commutateur de tissu canal fibre qui peuvent aussi être mémorisés dans un serveur de noms FC.

Le diagramme qui suit montre la représentation d'une passerelle qui prend en charge plusieurs appareils canal fibre derrière elle. Les deux objets Portail représentent les interfaces IP sur la passerelle iFCP qui peuvent être utilisées pour accéder à un des trois objets Nœud de mémorisation derrière elle. Noter que l'objet Appareil FC n'est pas contenu dans l'objet Entité réseau. Cependant, chaque appareil FC a une relation à un ou plusieurs objets Nœud de mémorisation.



4.2.3 Messages de commandes et réponses exigés pour la prise en charge de iFCP

Les messages et réponses iSNSP affichés dans les tableaux suivants sont disponibles pour prendre en charge des passerelles iFCP. Les messages indiqués dans la colonne "EXIGÉ pour le serveur" DOIVENT être pris en charge par le serveur iSNS utilisé par les passerelles iFCP. Les messages indiqués dans la colonne "EXIGÉ pour le client" DOIVENT être pris en charge par les passerelle iFCP elles-mêmes.

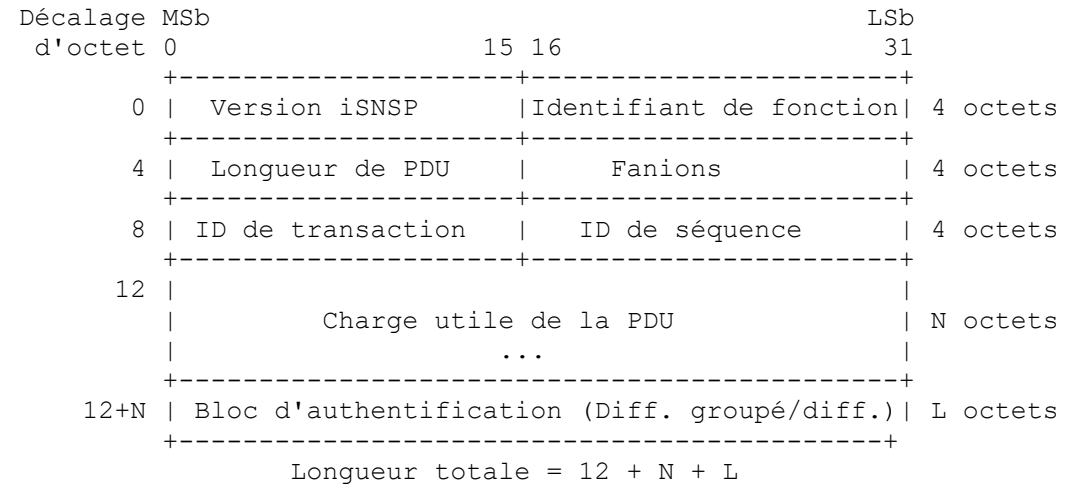
			EXIGÉ pour:	
Message	**Abréviation**	**ID de fonction**	**Serveur**	**Client**
Réservé		0x0000		
Demande d'enregistrement d'attribut d'appareil	DevAttrReg	0x0001	*	*
Demande d'interrogation d'attribut d'appareil	DevAttrQry	0x0002	*	*
Demande d'aller au prochain appareil	DevGetNext	0x0003	*	
Demande de désenregistrement d'appareil	DevDereg	0x0004	*	*
Demande d'enregistrement de SCN	SCNReg	0x0005	*	
Demande de désenregistrement de SCN	SCNDereg	0x0006	*	
Événement de SCN	SCNEvent	0x0007	*	
Notification de changement d'état	SCN	0x0008	*	
Enregistrer le DD	DDReg	0x0009	*	*
Désenregistrer le DD	DDDereg	0x000A	*	*
Enregistrer le DDS	DDSReg	0x000B	*	*
Désenregistrer le DDS	DDSDereg	0x000C	*	*
Enquête sur l'état d'entité	ESI	0x000D	*	
Battement de cœur de service de nom	Heartbeat	0x000E	*	
Réservé		0x000F-0x0010		
Demande de FC_DOMAIN_ID	RqstDomId	0x0011		
Libération de FC_DOMAIN_ID	RlseDomId	0x0012		
Obtenir un FC_DOMAIN_ID	GetDomId	0x0013		
Réservé		0x0014-0x00FF		
Spécifique de fabricant		0x0100-0x01FF		
RÉSERVÉ		0x0200-0x7FFF		

Voici les messages de réponse iSNSP pour la prise en charge de iFCP :

Message	Abréviation	ID de fonction	EXIGÉ pour : Serveur	Client
Réservé		0x8000		
Réponse d'enregistrement d'attribut d'appareil	DevAttrRegRsp	0x8001	*	*
Réponse d'interrogation d'attribut d'appareil	DevAttrQryRsp	0x8002	*	*
Réponse de demande d'aller au prochain appareil	DevGetNextRsp	0x8003	*	
Réponse de désenregistrement d'appareil	DevDeregRsp	0x8004	*	*
Réponse d'enregistrement de SCN	SCNRegRsp	0x8005	*	
Réponse de désenregistrement de SCN	SCNDeregRsp	0x8006	*	
Réponse d'événement de SCN	SCNEventRsp	0x8007	*	
Réponse de SCN	SCNRsp	0x8008	*	
Réponse d'enregistrement de DD	DDRegRsp	0x8009	*	*
Réponse de désenregistrement de DD	DDDeregRsp	0x800A	*	*
Réponse d'enregistrement de DDS	DDSRegRsp	0x800B	*	*
Réponse de désenregistrement de DDS	DDSDeregRsp	0x800C	*	*
Réponse d'enquête d'état d'entité	ESIRsp	0x800D	*	
Non utilisé		0x800E		
Réservé		0x800F-0x8010		
Réponse de demande de FC_DOMAIN_ID	RqstDomIdRsp	0x8011		
Réponse de libération de FC_DOMAIN_ID	RlseDomIdRsp	0x8012		
Obtenir des FC_DOMAIN_ID	GetDomIdRsp	0x0013		
Réservé		0x8014-0x80FF		
Spécifique de fabricant		0x8100-0x81FF		
Réservé		0x8200-0xFFFF		

5. Format de message iSNSP

Le format du message iSNSP est similaire au format des autres protocoles courants comme DHCP, DNS et BOOTP. Un message iSNSP peut être envoyé dans une ou plusieurs unités de données de protocole iSNS (PDU, *Protocol Data Unit*). Chaque PDU est alignée sur quatre octets. Voici la description du format de la PDU iSNSP :



5.1 En-tête de PDU iSNSP

L'en-tête de PDU iSNSP contient les champs Version iSNSP, Identifiant de fonction, Longueur de PDU, Fanions, Identifiant de transaction, et Identifiant de séquence, comme définis ci-dessus.

5.1.1 Version iSNSP

La version iSNSP décrite dans ce document est 0x0001. Toutes les autres valeurs sont RÉSERVÉES. Le serveur iSNS PEUT rejeter les messages pour des numéros de version iSNSP qu'il ne prend pas en charge.

5.1.2 Identifiant de fonction iSNSP

L'identifiant de fonction définit le type de message iSNS et l'opération à exécuter. Les valeurs d'identifiant de fonction dont le bit de tête est à zéro indiquent un message d'interrogation, d'enregistrement, et de notification, tandis que les valeurs d'identifiant de fonction dont le bit de tête est réglé à 1 indiquent des messages de réponse.

Voir à la Section 4 sous le protocole approprié (c'est-à-dire, iSCSI ou iFCP) la transposition de la valeur d'identifiant de fonction en message de commande ou de réponse iSNSP. Toutes les PDU comprenant un message iSNSP doivent avoir la même valeur d'identifiant de fonction.

5.1.3 Longueur de PDU iSNSP

La longueur de la PDU iSNS spécifie la longueur en octets du champ Charge utile de PDU. La charge utile de PDU contient les TLV d'attributs pour l'opération.

De plus, les messages de réponse contiennent un code de succès/échec. La longueur de PDU DOIT être alignée sur quatre octets.

5.1.4 Fanions iSNSP

Le champ Fanions indique des informations supplémentaires sur le message et le type d'entité réseau qui a généré le message. Le tableau suivant donne les fanions valides :

Position du bit	**Signification si établi (1)** :
16	l'envoyeur est le client iSNS
17	l'envoyeur est le serveur iSNS
18	le bloc Authentification est présent
19	fanion de remplacement (pour DevAttrReg)
20	dernière PDU du message iSNS
21	première PDU du message iSNS
22-31	réservé

5.1.5 Identifiant de transaction iSNSP

Identifiant de transaction DOIT être réglé à une valeur unique pour chaque message de demande actuellement en cours. Les réponses DOIVENT utiliser la même valeur d'identifiant de transaction que le message de demande iSNS associé. Si un message est retransmis, la valeur originale d'identifiant de transaction DOIT être utilisée. Toutes les PDU qui comprennent un message iSNSP doivent avoir la même valeur d'identifiant de transaction.

5.1.6 Identifiant de séquence iSNSP

L'identifiant de séquence a une valeur unique pour chaque PDU au sein d'une seule transaction. La valeur d'identifiant de séquence de la première PDU transmise dans un certain message iSNS DOIT être zéro (0), et chaque valeur d'identifiant de séquence dans chaque PDU DOIT être numéroté à la suite dans l'ordre dans lequel les PDU sont transmises. Noter que l'identifiant de séquence de deux octets permet jusqu'à 65 536 PDU par message iSNS.

5.2 Segmentation et réassemblage de message iSNSP

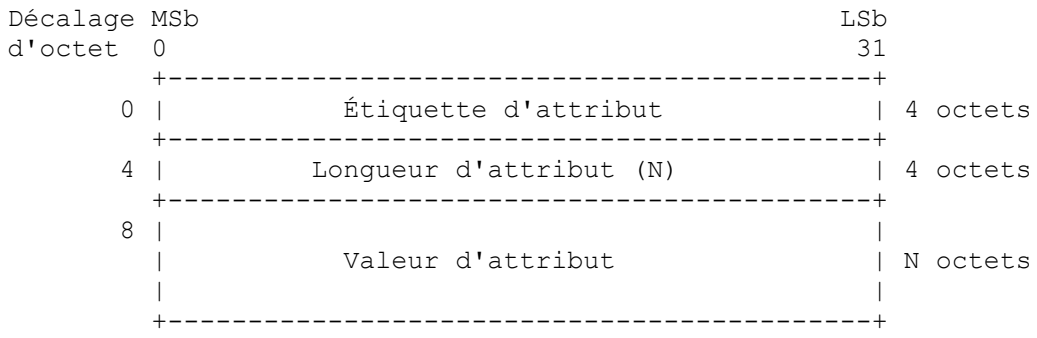
Les messages iSNS peuvent être portés dans une ou plusieurs PDU iSNS. Si une seule PDU iSNS est utilisée pour porter le message iSNS, le bit 21 (première PDU) et le bit 20 dans le champ Fanions (dernière PDU) DEVRONT alors être tous deux établis. Si plusieurs PDU sont utilisées pour porter le message iSNS, le bit 21 DEVRA alors être établi dans la première PDU du message, et le bit 20 DEVRA être établi dans la dernière PDU.

Toutes les PDU composant le même message iSNSP DEVRONT avoir la même valeur d'identifiant de fonction et d'identifiant de transaction. Chaque PDU composant un message iSNSP DEVRA avoir une valeur unique d'identifiant de séquence.

5.3 Charge utile de PDU iSNSP

La charge utile de PDU iSNSP est de longueur variable et contient des attributs utilisés pour les opérations d'enregistrement et d'interrogation. Les éléments de données d'attribut utilisent un format similaire à celui des autres protocoles, comme les

options DHCP [RFC2131]. Chaque attribut iSNS est spécifié dans la charge utile de PDU en utilisant le format de données étiquette-longueur-valeur (TLV, *Tag-Length-Value*) comme indiqué ci-dessous :



Longueur totale = 8 + N

Étiquette d'attribut : champ de 4 octets qui identifie l'attribut comme défini au paragraphe 6.1. Ce champ contient la valeur de l'étiquette provenant du tableau indiqué.

Longueur d'attribut : champ de 4 octets qui indique la longueur, en octets, du champ de valeur qui suit dans la TLV. Pour les attributs de longueur variable, le champ Valeur DOIT contenir des octets de bourrage, si nécessaire, afin de réaliser l'alignement sur 4 octets. Une "TLV de longueur zéro" contient seulement les champs d'étiquette d'attribut et de longueur.

Valeur d'attribut : champ de longueur variable qui contient la valeur d'attribut et les octets de bourrage (si nécessaire).

Le format ci-dessus est utilisé pour identifier chaque attribut dans la charge utile de la PDU. Noter que les limites de TLV n'ont pas besoin d'être alignées sur les limites de PDU ; des PDU peuvent porter une ou plusieurs TLV, ou une fraction de TLV. Le code d'état de réponse, contenu dans les charges utiles de PDU de message de réponse et décrit plus loin, n'est pas en format de TLV. Les charges utiles de PDU pour les messages qui ne contiennent pas d'attribut iSNS, comme le battement de cœur de service de nom *(Name Service Heartbeat)* n'utilisent pas le format de TLV.

5.3.1 Alignement sur quatre octets de valeur d'attribut

Toutes les valeurs d'attribut sont alignées sur des limites de quatre octets. Pour les attributs de longueur variable, si nécessaire, la longueur de TLV DOIT être augmentée jusqu'à la prochaine limite de quatre octets avec un bourrage d'octets contenant des zéros (0). Si une valeur d'attribut est bourrée, une combinaison de l'étiquette et de la valeur d'attribut elle-même est utilisée pour déterminer la valeur réelle de la longueur et du nombre d'octets de bourrage. Il n'y a pas de compte explicite du nombre d'octets de bourrage fournis dans la TLV.

5.4 Codes d'état de réponse iSNSP

Tous les messages de réponse iSNSP contiennent un champ Code d'état de 4 octets comme premier champ dans la charge utile de PDU iSNSP. Si le message de demande iSNSP d'origine a été traité normalement par le serveur iSNS, ou par le client iSNS pour les messages de ESI et de SCN, alors ce champ DEVRA contenir un code d'état de 0 (Succès). Un code d'état non zéro indique le rejet entier du message de demande iSNS du client.

Code d'état	Description d'état
0	Succès
1	Erreur inconnue
2	Erreur de format de message
3	Enregistrement invalide
4	Réservé
5	Interrogation invalide
6	Source inconnue
7	Source absente
8	Source non autorisée
9	Pas de telle entrée
10	Version non prise en charge
11	Erreur interne
12	Occupé
13	Option non comprise

14	Mise à jour invalide
15	Message (Identifiant de fonction) non pris en charge
16	Événement de SCN rejeté
17	Enregistrement de SCN rejeté
18	Attribut non mis en œuvre
19	Identifiant de domaine FC non disponiblle
20	Identifiant de domaine FC non alloué
21	ESI non disponible
22	Désenregistrement invalide
23	Caractéristique d'enregistrement non prise en charge
24 et plus	Réservé

5.5 Authentification des messages iSNS en diffusion et en diffusion groupée

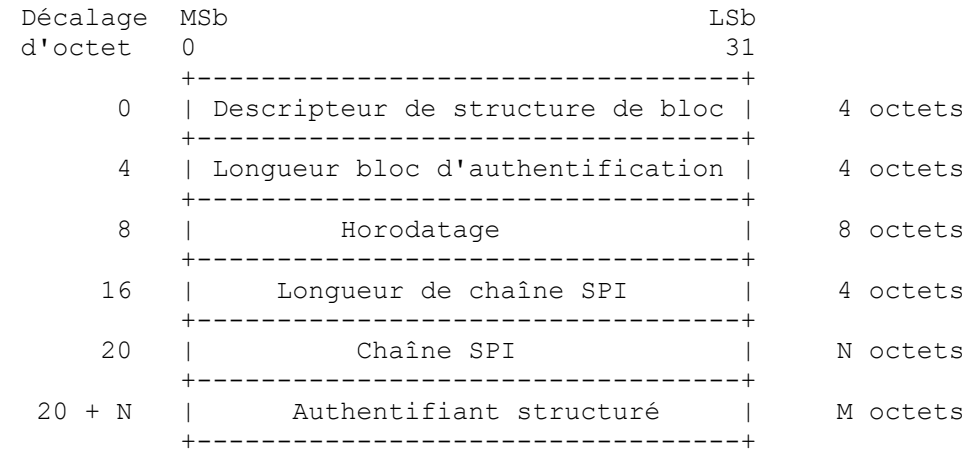
Pour les messages iSNS en diffusion et diffusion groupée (voir au paragraphe 2.9.3) le iSNSP fournit la capacité d'authentification. Ce paragraphe donne les détails du bloc d'authentification iSNS, qui est d'un format identique au bloc d'authentification de SLP [RFC2608]. Les messages iSNS en envoi individuel NE DEVRAIENT PAS inclure de bloc d'authentification, mais devraient plutôt s'appuyer sur les mécanismes de sécurité de IPSec.

Si un message contient un bloc d'authentification, le bit "Bloc d'authentification présent" DEVRA alors être activé dans le champ Fanions de l'en-tête de PDU iSNSP.

Si une PKI est disponible avec une autorité de certification (CA) [X.509] l'authentification de la clé publique du serveur iSNS est alors possible. Le bloc d'authentification renforce le DSA avec l'algorithme SHA-1, qui peut facilement s'intégrer dans une infrastructure de clé publique.

Le bloc d"authentification contient une signature numérique pour le message en diffusion groupée. La signature numérique est calculée PDU par PDU. Le bloc d'authentification contient les informations suivantes :
1. Un horodatage, pour empêcher les attaques en répétition.
2. Un authentifiant structuré contenant une signature calculée sur l'horodatage et le message à sécuriser.
3. Un indicateur de l'algorithme de chiffrement utilisé pour calculer la signature.
4. Un indicateur du matériel de chiffrement et des paramètres d'algorithme utilisés pour calculer la signature.

Le bloc d'authentification est décrit dans la figure qui suit :



Longueur totale = 20 + N + M

Le descripteur de structure de bloc (BSD, *Bloc Structure Descriptor*) définit la structure et l'algorithme à utiliser pour l'authentifiant structuré. Les valeurs de BSD de 0x00000000 à 0x00007FFF sont allouées par l'IANA, tandis que les valeurs de 0x00008000 à 0x00008FFF sont pour utilisation privée.

Longueur de bloc d'authentification définit la longueur du bloc d'authentification, en commençant par le champ BSD et jusqu'au dernier octet de l'authentifiant structuré.

Horodatage : c'est un entier non signé de huit octets à virgule fixe, qui donne le nombre de secondes depuis le 1er janvier 1970 à 00:00:00 GMT.

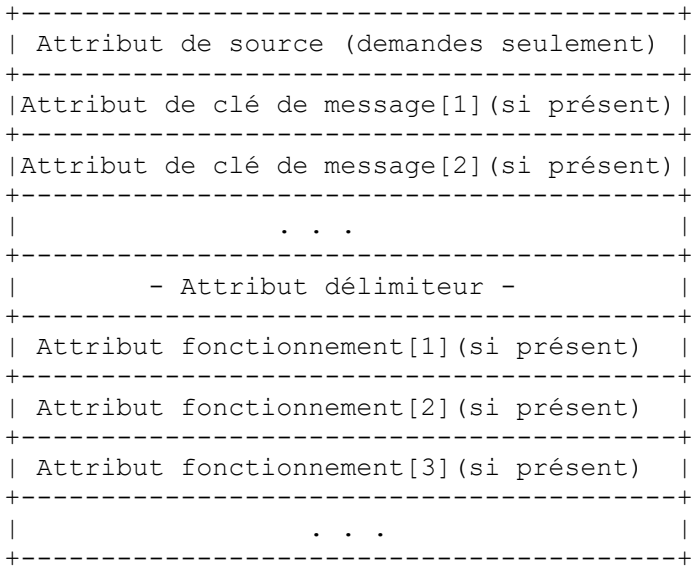
Longueur de chaîne SPI : c'est la longueur du champ Chaîne SPI.

Chaîne SPI *(Security Parameters Index)* : indice de la clé et de l'algorithme utilisés par le receveur du message pour décoder le champ Authentifiant structuré.

Authentifiant structuré : contient la signature numérique. Pour la valeur par défaut de BSD de 0x0002, ce champ DEVRA contenir le codage ASN.1 binaire des valeurs de résultat du calcul de signature DSA avec SHA-1 comme spécifié au paragraphe 2.2.2 de la [RFC3279].

5.6 Messages d'enregistrement et d'interrogation

Les charges utiles de PDU de message iSNSP d'enregistrement et d'interrogation contiennent une liste d'attributs, et ont le format suivant :



Chaque attribut de source, de clé de message, de délimiteur, et de fonctionnement est spécifié dans la charge utile de PDU en utilisant le format de données Étiquette-Longueur-Valeur (TLV). Les messages iSNS d'enregistrement et d'interrogation sont envoyés par les clients iSNS à l'adresse IP du serveur iSNS et à l'accès bien connu TCP/UDP. Les réponses iSNS seront envoyées à l'adresse IP du client iSNS et au numéro d'accès TCP/UDP du message de demande d'origine.

5.6.1 Attribut Source

L'attribut de source est utilisé pour identifier le nœud de mémorisation au serveur iSNS pour les messages d'interrogation et autres qui exigent une identification de la source. L'attribut de source identifie de façon univoque la source du message. Les types d'attributs de source valides sont donnés ci-dessous.

Attributs Source valides :
Nom iSCSI
Nom WWPN d'accès FC

Pour une opération d'interrogation, l'attribut de source est utilisé pour limiter la portée de l'opération spécifiée aux domaines de découverte dont la source est membre. Des nœuds de gestion spéciaux, identifiés par l'attribut de source, peuvent être administrativement configurés pour effectuer l'opération spécifiée sur tous les objets de la base de données iSNS sans viser de domaine de découverte.

Pour les messages qui changent le contenu de la base de données iSNS, le serveur iSNS DOIT vérifier que l'attribut de source identifié est soit un nœud de gestion, soit un nœud de mémorisation qui fait partie de l'entité réseau contenant les objets ajoutés, supprimés, ou modifiés.

5.6.2 Attributs Clé de message

Les attributs de clé de message sont utilisés pour identifier les objets correspondants dans la base de données iSNS pour les messages iSNS d'interrogation et d'enregistrement. Si elle est présente, la clé de message DOIT être une clé

d'enregistrement ou une clé d'interrogation pour un objet comme décrit aux paragraphes 5.6.5 et 6.1. Une clé de message n'est pas requise quand une interrogation s'étend sur l'ensemble entier d'objets disponibles à la source ou si un enregistrement est pour une nouvelle entité.

Les noms iSCSI utilisés dans la clé de message DOIVENT être normalisés conformément au gabarit stringprep [RFC3722]. Les identifiants d'entités (EID) utilisés dans la clé de message DOIVENT être normalisés conformément au gabarit nameprep [RFC3491].

5.6.3 Attributs Délimiteur

L'attribut Délimiteur sépare les attributs de clé de message des attributs de fonctionnement dans une charge utile de PDU. L'attribut Délimiteur a une valeur d'étiquette de 0 et une valeur de longueur de 0. L'attribut Délimiteur a toujours une longueur de 8 octets (un champ d'étiquette de 4 octets et un champ de longueur de 4 octets, contenant tous des zéros). Si une clé de message n'est pas exigée pour un message, l'attribut Délimiteur suit alors immédiatement l'attribut de source.

5.6.4 Attributs de fonctionnement

Les attributs de fonctionnement sont une liste d'un ou plusieurs attributs de clé et de non clé en rapport avec l'opération actuelle d'enregistrement ou d'interrogation iSNS effectuée.

Les attributs de fonctionnement incluent des attributs de clé d'objet et des attributs de non clé. Les attributs de clé d'objet identifient de façon univoque les objets iSNS. Les attributs de clé DOIVENT précéder les attributs non clé de chaque objet dans les attributs de fonctionnement. La valeur d'étiquette distingue l'attribut comme attribut de clé d'objet (c'est-à-dire, étiquette=1, 16 et 17, 32, 64, et 96) ou un attribut non clé. Les noms iSCSI utilisés dans les attributs de fonctionnement DOIVENT être normalisés conformément au gabarit stringprep [RFC3722]. Les identifiants d'entités (EID) utilisés dans les attributs de fonctionnement DOIVENT être normalisés conformément au gabarit nameprep [RFC3491].

L'ordre des attributs de fonctionnement dans le message est important pour déterminer les relations entre les objets et leur possession d'attributs non clé. Les messages de protocole iSNS qui violent ces règles d'ordre DEVRONT être rejetés avec le code d'état de 2 (Erreur de format de message). Voir dans les descriptions de message les exigences d'ordre appropriées des attributs de fonctionnement.

Certains objets sont traités par plus d'une valeur d'attribut de clé d'objet. Par exemple, l'objet Portail a pour clé les étiquettes d'attribut 16 et 17. Lors de la description d'un objet qui a plus d'un attribut de clé, chaque attribut de clé d'objet de cet objet DOIT être rangé à la suite par valeur d'étiquette dans le message avant les attributs non clés de cet objet et les attributs clés de l'objet suivant. Un groupe d'attributs de clé de cette sorte est traité comme un seul attribut de clé logique lors de l'identification d'un objet.

Les attributs non clé qui suivent immédiatement les attributs clés DOIVENT être des attributs de l'objet référencé par les attributs clés. Tous les attributs non clés d'un objet DOIVENT être énumérés avant les attributs clés d'objet qui introduisent le prochain objet.

Les objets DOIVENT être énumérés par ordre d'héritage, conformément à l'ordre de contenance. Les objets Nœud de mémorisation et Portail et leurs attributs respectifs DOIVENT suivre l'objet Entité réseau avec lequel ils sont en relation. De même, les objets Appareil FC DOIVENT suivre l'objet Nœud de mémorisation avec lequel ils sont en relation.

Les objets spécifiques de fabricant sont définis par des valeurs d'étiquette dans la gamme 1537-2048 et ont les mêmes exigences que décrit ci-dessus.

5.6.4.1 Attributs de fonctionnement pour les demandes d'interrogation et passer au suivant

Dans les messages de demande d'interrogation et Get Next *(aller au suivant)*, les attributs de TLV d'une valeur de longueur de 0 sont utilisés pour indiquer quels attributs de fonctionnement sont à retourner dans les valeurs de réponse correspondantes. Les valeurs d'attribut de fonctionnement qui correspondent aux attributs de TLV du message d'origine sont retournées dans le message de réponse.

5.6.5 Types de message d'enregistrement de demande d'interrogation

On décrit dans ce qui suit chaque type d'interrogation et de message.

5.6.5.1 Demande d'enregistrement d'attributs d'appareil (DevAttrReg)

Le type de message DevAttrReg est 0x0001. Le message DevAttrReg fournit aux clients iSNS le moyen de mettre à jour les objets existants ou d'enregistrer de nouveaux objets. La valeur du bit de remplacement dans le champ Fanions détermine si le message DevAttrReg met à jour ou remplace un enregistrement existant.

L'attribut de source identifie le nœud qui initie la demande d'enregistrement.

La clé de message identifie l'objet sur lequel le message DevAttrReg agit. Il DOIT contenir le ou les attributs de clé qui identifient un objet. Cet objet DOIT contenir tous les attributs et les attributs d'objet subordonné qui s'y rapportent qui vont être inclus dans les attributs de fonctionnement de la charge utile de la PDU DevAttrReg. Le ou les attributs de clé qui identifient cet objet DOIVENT aussi être inclus dans les attributs de fonctionnement.

Si la clé de message contient un EID et si aucun objet préexistant ne correspond à la clé de message, le message DevAttrReg DEVRA alors créer une nouvelle entité avec l'EID spécifié et tout nouvel objet spécifié par les attributs de fonctionnement. Le bit de remplacement DEVRA être ignoré.

Si la clé de message ne contient pas d'EID, et si aucun objet préexistant ne correspond à la clé de message, le message DevAttrReg DEVRA alors être rejeté avec un code d'état de 3 (Enregistrement invalide).

Si la clé de message n'est pas présente, le message DevAttrReg enregistre alors implicitement une nouvelle entité réseau. Dans ce cas, le bit de remplacement DEVRA être ignoré ; une nouvelle entité réseau DEVRA être créée. Les entités existantes, leurs objets, et leurs relations, restent inchangées.

Le bit de remplacement détermine la sorte d'opération conduite sur l'objet identifié dans la clé de message DevAttrReg. Le bit de remplacement ne s'applique qu'au message DevAttrReg ; il est ignoré pour tous les autres types de message.

Si le bit de remplacement est établi, les objets, attributs, et relations spécifiés dans les attributs de fonctionnement DEVRONT alors remplacer l'objet identifié par la clé de message. L'objet et tous ses objets subordonnés DEVRONT être désenregistrés, et les SCN appropriées DEVRONT être envoyées par le serveur iSNS pour les objets désenregistrés. Les objets figurant sur la liste des attributs de fonctionnement sont alors utilisés pour remplacer les objets qui viennent d'être désenregistrés. Noter que des SCN supplémentaires DEVRONT être envoyées pour les nouveaux objets enregistrés, si approprié. Les objets et relations existants qui ne sont pas identifiés ou qui sont subordonnés à l'objet identifié par la clé de message NE DOIVENT PAS être affectés ou changés.

Si le bit de remplacement n'est pas établi, le message met alors à jour les attributs de l'objet identifié par la clé de message et ses objets subordonnés. Les relations existantes de contenance d'objet NE DOIVENT PAS être changées. Pour les objets existants, les attributs de clé NE DOIVENT PAS être modifiés, mais de nouveaux objets subordonnés PEUVENT être ajoutés.

Les attributs de fonctionnement représentent les objets, attributs, et relations à enregistrer. Plusieurs objets et attributs en rapports PEUVENT être enregistrés dans un seul message DevAttrReg. L'ordre des objets dans ce message indique la structure et les associations entre les objets à enregistrer. Au moins un objet DOIT figurer sur la liste des attributs de fonctionnement. Des objets supplémentaires (le cas échéant) DOIVENT être subordonnés au premier objet de la liste. Les attributs clés DOIVENT précéder les attributs non clés de chaque objet. Un certain objet ne peut apparaître qu'une seule fois dans les attributs de fonctionnement d'un message. Si le nœud identifié par l'attribut de source n'est pas un nœud de gestion, alors les objets dans les attributs de fonctionnement DOIVENT être membres de la même entité réseau que le nœud de source.

Par exemple, pour établir des relations entre un objet Entité réseau et son portail et des objets Nœud de mémorisation, les attributs de fonctionnement font la liste des attributs clés et non clés de l'objet Entité réseau, suivis par les attributs clés et non clés de chaque objet Portail et Nœud de mémorisation à relier à cette entité réseau. De même, un objet Appareil FC qui suit un objet Nœud de mémorisation est considéré comme un subordonné de ce nœud de mémorisation.

De nouveaux objets PG sont enregistrés quand un objet associé Portail ou Nœud iSCSI est enregistré. Un enregistrement explicite d'objet PG PEUT suivre l'enregistrement d'un objet Portail ou nœud iSCSI dans un message DevAttrReg.

Quand un portail est enregistré, les attributs de portail PEUVENT être immédiatement suivis par un attribut PGT. L'attribut PGT DEVRA être suivi par l'ensemble des noms iSCSI de PG qui représentent les nœuds qui seront associés au portail en utilisant la valeur de PGT indiquée. Des ensembles supplémentaires de noms iSCSI des PGT et PG à associer au portail enregistré PEUVENT suivre. Les valeurs de PGT indiquées sont allouées à l'objet PG associé au portail nouvellement enregistré et aux nœuds de mémorisation iSCSI référencés immédiatement à la suite de l'attribut de PGT dans les attributs de fonctionnement.

Quand un nœud de mémorisation iSCSI est enregistré, les attributs du nœud de mémorisation PEUVENT être immédiatement suivis par un attribut de PGT. L'attribut de PGT DEVRA être suivi par l'ensemble de paires Adresse IP de portail PG, Accès TCP/UDP de PG représentant les objets Portail qui vont être associés au nœud de mémorisation en utilisant la valeur de PGT indiquée. Des ensembles supplémentaires de paires d'adresse IP de PGT et de portail de PG et d'accès TCP/UDP de PG à associer au nœud de mémorisation enregistré PEUVENT suivre. Les valeurs de PGT indiquées sont allouées à l'objet PG associé au nœud de mémorisation iSCSI nouvellement enregistré et à ou aux objets Portail référencés immédiatement à la suite de l'attribut de PGT dans les attributs de fonctionnement.

Si la valeur de la PGT n'est pas incluse dans l'enregistrement d'objet Nœud de mémorisation ou Portail, et si une valeur de PGT n'a pas été antérieurement enregistrée pour la relation, la PGT pour l'objet PG correspondant DEVRA être enregistrée avec une valeur de 0x00000001. Si l'attribut PGT est inclus dans le message d'enregistrement comme TLV de longueur 0, la valeur de PGT pour l'objet PG correspondant DEVRA alors être enregistrée comme NULLE. Une TLV de longueur 0 pour la PGT dans un message de mise à jour d'enregistrement écrase la valeur de PGT précédente avec NUL, indiquant qu'il n'y a pas de relation entre le nœud de mémorisation et le portail.

Un maximum d'un objet Entité réseau peut être créé ou mis à jour avec un seul message DevAttrReg. Par conséquent, les attributs de fonctionnement NE DOIVENT PAS contenir plus d'un objet Entité réseau. Il n'y a pas de limite au nombre d'objets Portail, Nœud de mémorisation, et Appareil FC qui peuvent figurer sur la liste des attributs de fonctionnement, pourvu qu'ils soient tous subordonnés à l'objet Entité réseau mentionné.

Si la clé de message et les attributs de fonctionnement ne contiennent pas un attribut EID, ou si l'attribut EID a une longueur de 0, un nouvel objet Entité réseau DEVRA alors être créé et le serveur iSNS DEVRA fournir une valeur d'EID unique pour lui. La valeur d'EID fournie DEVRA être incluse dans le message de réponse DevAttrReg. Si la clé de message et les attributs de fonctionnement contiennent un EID qui ne correspond pas à l'EID d'une entité réseau existante dans la base de données iSNS, alors une nouvelle entité réseau DEVRA être créée et recevoir la valeur contenue dans cet attribut EID. Finalement, si la clé de message et les attributs de fonctionnement contiennent un EID qui correspond à l'EID d'un objet existant dans la base de données iSNS, alors les objets, attributs, et relations spécifiés dans les attributs de fonctionnement DEVRONT être ajoutés à l'entité réseau existante identifiée par l'EID.

Un message d'enregistrement qui crée un nouvel objet Entité réseau DOIT contenir au moins un portail ou un nœud de mémorisation. Si le message ne le contient pas, il DEVRA alors être considéré comme invalide et résulter en une réponse avec le code d'état 3 (Enregistrement invalide).

Si un serveur iSNS ne prend pas en charge une caractéristique d'enregistrement, comme l'enregistrement d'un objet PG explicite, le serveur DEVRA alors retourner un code d'état 23 (Caractéristique d'enregistrement non acceptée).

Noter que le serveur iSNS peut modifier ou rejeter l'enregistrement de certains attributs, comme un intervalle d'ESI. De plus, le serveur iSNS peut allouer des valeurs pour des attributs de fonctionnement supplémentaires qui ne sont pas explicitement enregistrés dans le message DevAttrReg d'origine, comme l'EID et le jeton WWNN.

5.6.5.2 Demande d'interrogation d'attribut d'appareil (DevAttrQry)

Le type de message de DevAttrQry est 0x0002. Le message DevAttrQry fournit au client iSNS le moyen d'interroger le serveur iSNS sur les attributs d'objet.

L'attribut Source identifie le nœud qui a initié la demande. Pour les nœuds non de gestion qui initient le message DevAttrQry, l'interrogation a la portée des domaines de découverte dont le nœud initiateur est membre. Le message DevAttrQry DEVRA seulement retourner des informations sur les nœuds de mémorisation et leurs objets parent et subordonnés relatifs, où le nœud de mémorisation a un domaine de découverte commun avec le nœud identifié dans l'attribut Source.

La clé de message peut contenir des attributs de clé et non de clé ou pas d'attribut du tout. Si plusieurs attributs sont utilisés comme clé de message, ils DOIVENT alors tous être du même type d'objet (par exemple, adresse IP et accès TCP/UDP sont des attributs du type d'objet Portail). Une clé de message avec des attributs non clé peut correspondre à plusieurs instances du type d'objet spécifique. Une clé de message avec une ou des TLV de longueur zéro a pour portée chaque objet du type indiqué par la ou les TLV de longueur zéro. Un champ Clé de message vide indique que l'interrogation a pour portée la base de données entière accessible par le nœud Source.

Le message de réponse DevAttrQry retourne les attributs des objets figurant sur la liste des attributs de fonctionnement qui se rapportent à la clé de message du message DevAttrQry d'origine. Les attributs de fonctionnement du message DevAttrQry contiennent des TLV de longueur zéro qui spécifient les attributs qui sont à retourner dans le message

DevAttrQryRsp. Une clé de message contenant des TLV de longueur zéro indique que l'ensemble d'attributs spécifié dans les attributs de fonctionnement est à retourner pour chaque objet correspondant au type indiqué par la clé de message.

Si la clé de message contient des TLV de longueur non zéro, les attributs de fonctionnement pour l'objet correspondant à la clé de message DEVRONT alors être retournés dans le message DevAttrQryRsp. Chaque type d'attribut (c'est-à-dire, TLV de longueur zéro) dans les attributs de fonctionnement indiquant un attribut de l'objet qui correspond à la clé de message, ou d'autres objets dans la même entité qui ont une relation avec l'objet qui correspond à la clé de message, est à retourner dans la réponse. L'ordre des clés d'objet et des attributs associés retournés dans le message de réponse DevAttrQry DEVRA être le même que dans le message d'interrogation d'origine. Si aucun objet ne correspond à la clé de message, le message DevAttrQryRsp NE DEVRA alors PAS retourner d'attributs de fonctionnement. Un tel message et sa réponse correspondante NE DEVRA PAS être considéré comme erreur.

L'objet Groupe portail détermine si une relation existe entre un certain nœud de mémorisation et un objet Portail. Si la PGT du Groupe portail n'est pas NULLE, il existe alors une relation entre le nœud de mémorisation indiqué et le portail ; si la PGT est NUL, il n'existe alors pas de relation. Donc, la valeur (NUL ou non NUL) de l'attribut PGT de chaque objet Groupe portail détermine la structure et l'ordre de la réponse DevAttrQry à une interrogation sur les nœuds de mémorisation et les portails.

Par exemple, une base de données iSNS contient une entité réseau ayant deux portails et deux nœuds. Chaque nœud de mémorisation a deux Groupes portails, un avec une valeur de PGT NUL pour un portail et une autre avec une valeur de PGT non NUL pour l'autre portail. Le message DevAttrQry contient une clé de message qui correspond à un des nœuds, et des attributs de fonctionnement avec des TLV de longueur zéro qui font la liste d'abord des attributs de nœuds, puis des attributs de portail, et ensuite des attributs de PG. Le message de réponse DEVRA donc retourner d'abord l'objet de nœud correspondant, puis les attributs demandés de l'objet Portail qui peuvent être utilisés pour accéder au nœud de mémorisation (comme indiqué par la PGT) et finalement les attributs demandés de l'objet PG utilisés pour accéder à ce nœud de mémorisation. L'ordre dans lequel chaque attribut d'objet est indiqué sur la liste est le même que l'ordre des attributs de l'objet dans les attributs de fonctionnement du message de demande d'origine.

Si l'attribut Clé de message contient des TLV de longueur zéro, l'interrogation retourne alors les attributs demandés pour tous les objets qui correspondent au type de la clé de message (les restrictions de DD DEVRONT s'appliquer pour les nœuds non de gestion). Si plusieurs objets correspondent au type de clé de message, alors les attributs pour chaque objet correspondant à la clé de message DOIVENT figurer sur la liste avant que les attributs pour le prochain objet qui correspond figurent dans la liste dans la réponse à l'interrogation. En d'autres termes, le processus décrit ci-dessus doit être itéré dans le message de réponse pour chaque objet qui correspond au type de la clé de message spécifié par la ou les TLV de longueur zéro.

Par exemple, une base de données iSNS contient seulement une entité réseau ayant deux portails et trois nœuds. Tous les objets PG dans l'entité ont une valeur de PGT de 0x00000001. Dans le message DevAttrQry, la clé de message contient une TLV de longueur zéro qui spécifie un type de nœud, et des attributs de fonctionnement faisant la liste d'abord des attributs du nœud, et ensuite des attributs du portail. Le message de réponse va retourner, dans l'ordre suivant, les attributs pour le premier objet Nœud, le suivant, et le dernier, chacun suivi par les attributs pour les deux portails. Si ce même message DevAttrQry avait à la place contenu une TLV de longueur zéro spécifiant le type d'entité réseau, alors le message de réponse aurait retourné les attributs pour les trois objets Nœud, suivis par les attributs pour les deux portails.

Si il n'y a pas d'attribut Clé de message, l'interrogation retourne alors tous les attributs de la base de données iSNS (là encore, les restrictions de DD DEVRONT s'appliquer pour les nœuds non de gestion). Tous les attributs qui correspondent au type spécifié par chaque TLV de longueur zéro dans les attributs de fonctionnement DEVRONT figurer sur la liste. Tous les attributs de chaque type DEVRONT être sur la liste avant les attributs qui correspondent à la prochaine TLV de longueur zéro.

Par exemple, une base de données iSNS contient deux entités, ayant chacune deux nœuds et deux portails. Le message DevAttrQry ne contient pas d'attribut Clé de message, et les attributs de fonctionnement font apparaître en premier les attributs de portail, et ensuite les attributs du nœud. Les attributs de fonctionnement du message de réponse vont retourner les attributs provenant de chacun des quatre portails, suivis par les attributs provenant de chacun des quatre nœuds.

Si un message DevAttrQry demande un attribut pour lequel le serveur iSNS n'a pas de valeur, le serveur NE DEVRA alors PAS retourner l'attribut demandé dans la réponse à l'interrogation. De tels messages d'interrogation de réponse NE DEVRONT PAS être considérés comme des erreurs.

Les messages d'enregistrement et d'interrogation pour les attributs spécifiques de serveur iSNS (c'est-à-dire, des étiquettes dans la gamme 132 à 384) DEVRONT être formatés en utilisant l'attribut de clé identifiant du nœud de mémorisation qui est à l'origine de l'interrogation (c'est-à-dire, nom iSCSI ou nom d'accès FC WWPN) pour les deux attributs Source et Clé de message. Les attributs de fonctionnement DEVRONT inclure la TLV de l'attribut spécifique du serveur qui est demandé.

La qualité de membre de DD peut être découverte par le message DevAttrQry en incluant soit les attributs de membre du DD (c'est-à-dire, Indice iSCSI de membre de DD, Nœud iSCSI membre du DD, Nœud iFCP membre du DD, Indice de portail de membre du DD, Adresse IP de portail de membre du DD, et Accès TCP/UDP de portail de membre du DD) soit la clé d'objet du nœud de mémorisation ou portail (c'est-à-dire, Nom iSCSI, Indice iSCSI, Adresse IP de portail, Accès TCP/UDP de portail, et Indice de portail) dans les attributs de fonctionnement. Utiliser les attributs de membre du DD DEVRA retourner à la fois les nœuds de mémorisation membres enregistrés et non enregistrés et/ou portails d'un DD. Les messages DevAttrQry qui utilisent la clé d'objet Nœud de mémorisation et/ou Portail DEVRONT retourner seulement les nœuds de mémorisation ou portails membres qui sont actuellement enregistrés dans la base de données iSNS.

Le message DevAttrQry DEVRA prendre en charge l'ensemble minimum suivant d'attributs Clé de message :

Attributs Clé de messages valides pour les interrogations :
- Identifiant d'entité
- Protocole d'entité
- Adresse IP et accès TCP/UDP de portail
- Indice de portail
- Type de nœud iSCSI
- Nom iSCSI
- Indice iSCSI
- Indice PG
- Nom WWPN d'accès FC
- Type d'accès FC
- Type FC-4
- Identifiant de domaine de découverte
- Identifiant d'ensemble de domaine de découverte
- Attribut de source (pour les attributs spécifiques du serveur)
- Nom de commutateur (WWNN d'appareil -- pour les interrogations de Virtual_Fabric_ID)

5.6.5.3 Demande d'aller à l'appareil suivant (DevGetNext)

Le type de message DevGetNext est 0x0003. Ce message fournit au client iSNS le moyen de restituer chaque instance d'un type d'objet exactement une fois.

L'attribut de source identifie le nœud qui initie la demande DevGetNext, et est utilisé pour limiter le processus de restitution aux domaines de découverte dont le nœud initiateur est membre.

L'attribut Clé de message 0x8100-0x81FF peut être un Identifiant d'entité (EID), un Nom iSCSI, un Indice iSCSI, une Adresse IP de portail et un Accès TCP/UDP, un Indice de portail, un Indice de PG, un Nom de nœud WWNN FC ou un Nom d'accès WWPN FC. Si la longueur de TLV de ou des attributs de clé de message est zéro, la première entrée d'objet dans la base de données iSNS correspondant au type de la clé de message DEVRA alors être retournée dans la clé de message du message DevGetNextRsp correspondant. Si aucun attribut TLV de longueur non zéro n'est contenu dans la clé de message, le message de réponse à DevGetNext DEVRA alors retourner le prochain objet mémorisé après l'objet identifié par la clé de message dans le message de demande DevGetNext d'origine.

Si la clé de message fournie correspond à la dernière instance d'objet dans la base de données iSNS, le code d'état 9 (Pas de telle entrée) DEVRA alors être retourné dans la réponse.

Les attributs de fonctionnement peuvent être utilisés pour spécifier la portée de la demande DevGetNext, et pour spécifier les attributs du prochain objet, qui sont à retourner dans le message de réponse DevGetNext. Tous les attributs de fonctionnement DOIVENT être des attributs du type d'objet identifié par la clé de message. Par exemple, si la clé de message est un attribut Entity_ID, les attributs de fonctionnement NE DOIVENT alors PAS contenir des attributs de portails.

Les attributs TLV de longueur non zéro dans les attributs de fonctionnement sont utilisés pour délimiter le message DevGetNext. Seul le prochain objet avec des valeurs d'attribut qui correspondent aux attributs TLV de longueur non zéro DEVRONT être retournés dans le message de réponse DevGetNext.

Les attributs TLV de longueur zéro DOIVENT figurer sur la liste après les attributs de longueur non zéro dans les atributs de fonctionnement du message de demande DevGetNext. Les attributs TLV de longueur zéro spécifient les attributs du prochain objet qui sont à retourner dans le message de réponse DevGetNext.

Noter qu'il n'y a pas d'exigence spécifique concernant l'ordre dans lequel les entrées d'objet sont restituées de la base de données iSNS ; l'ordre de restitution des entrées d'objet en utilisant le message DevGetNext est spécifique de la mise en œuvre.

Le client iSNS est chargé de s'assurer que les informations acquises par l'utiisation du message DevGetNext sont précises et à jour. Il n'est pas garanti que la base de données iSNS ne va pas changer entre des messages successifs de demande DevGetNext. Si la clé de message fournie ne correspond pas à une entrée existante dans la base de données, les attributs pour la prochaine clé d'objet suivant la clé de message fournie DEVRONT alors être retournés. Par exemple, une entrée d'objet peut avoir été supprimée entre les messages DevGetNext successifs. Il peut en résulter une demande DevGetNext dans laquelle la clé de message ne correspond pas à une entrée d'objet existante. Dans ce cas, les attributs pour le prochain objet mémorisé dans la base de données iSNS sont retournés.

5.6.5.4 Demande de désenregistrer l'appareil (DevDereg)

Le type de message DevDereg est 0x0004. Ce message est utilisé pour supprimer des entrées d'objet de la base de données iSNS. Un ou plusieurs objets peuvent être supprimés par un seul message DevDereg. Noter que les objets Nœud de mémorisation désenregistrés vont conserver leur qualité de membre dans leur domaine de découverte jusqu'à un désenregistrement explicite de leur qualité de membre du ou des domaines de découverte.

À réception du DevDereg, le serveur iSNS supprime tous les objets identifiés par les attributs de fonctionnement et tous les objets subordonnés qui ne sont dépendants que de ces objets identifiés. Par exemple, la suppression d'une entité réseau résulte aussi en la suppression de tous les objets Portail, Groupe de portails, Nœud de mémorisation, et Appareil FC associés à cette entité réseau. Les objets Appareil FC NE DEVRONT PAS être désenregistrés de cette manière sauf si tous les nœuds de mémorisation qui leur sont associés ont été désenregistrés.

La charge utile de PDU de demande DevDereg contient un attribut Source et un ou des attributs de fonctionnement ; il n'y a pas d'attribut de clé de message. Si le nœud identifié par l'attribut de source n'est pas un nœud de gestion, il DOIT alors être de la même entité réseau que le ou les objets identifiés pour être supprimés par les attributs de fonctionnement. Les attributs de fonctionnement valides sont énumérés ci-dessous.

Attributs de fonctionnement valides pour DevDereg
- Identifiant d'entité
- Adresse IP et accès TCP/UDP de portail
- Indice de portail
- Nom iSCSI
- Indice iSCSI
- Nom WWPN d'accès FC
- nom WWNN de nœud FC

La supression de l'objet peut résulter en messages de SCN aux clients iSNS appropriés.

La tentative de désenregistrement d'entrées non existantes NE DEVRA PAS être considérée comme une erreur.

Si tous les nœuds et portails associés à une entité réseau sont désenregistrés, l'entité réseau DEVRA alors aussi être supprimée.

Si les deux objets Portail et Nœud de mémorisation iSCSI associés à un objet Groupe de portails sont supprimés, cet objet Groupe de portails DEVRA alors aussi être supprimé. L'objet Groupe de portails DEVRA rester enregistré tant qu'un de ses objets Portail ou Nœud de mémorisation iSCSI associé reste enregistré. Si un objet Nœud de mémorisation ou Portail est ultérieurement réenregistré, une relation entre l'objet réenregistré et un enregistrement existant d'objet Portail ou Nœud de mémorisation, indiquée par l'objet PG, DEVRA alors être restaurée.

5.6.5.5 Demande Enregistrer SCN (SCNReg)

Le type de message SCNReg est 0x0005. Le message Demande d'enregistrement de notification de changement d'état (SCNReg) permet à un client iSNS d'enregistrer un nœud de mémorisation pour recevoir des messages de notification de changement d'état (SCN).

La SCN notifie au nœud de mémorisation les changements à tous les nœuds de mémorisation au sein de tout DD dont il est membre. Si le nœud de mémorisation est un nœud de gestion, il DEVRA recevoir les SCN pour les changements dans le réseau entier. Noter qu'alors que SCNReg établit le champ Gabarit binaire de SCN, le message DevAttrReg enregistre l'accès UDP ou TCP utilisé par chaque portail pour recevoir les messages de SCN. Si aucun champ Accès de SCN d'aucun

portail du nœud de mémorisation n'est enregistré pour recevoir les messages de SCN, le message SCNReg DEVRA alors être rejeté avec le code d'état 17 (Enregistrement de SCN rejeté).

La charge utile de PDU Demande SCNReg contient un attribut de source, un attribut de clé de message, et un attribut de fonctionnement. Les attributs de clé de message valides pour SCNReg sont indiqués ci-dessous :

Nom iSCSI
Nom WWPN d'accès FC

Le nœud avec l'attribut Nom iSCSI ou Nom WWPN d'accès FC qui corrspond à la clé de message dans le message SCNReg est enregistré pour recevoir des SCN en utilisant le gabarit binaire de SCN spécifié. Un maximum de un nœud DEVRA être enregistré pour chaque message SCNReg.

Le gabarit binaire de SCN est le seul attribut de fonctionnement de ce message, et il écrase toujours le contenu précédent de ce champ dans la base de données iSNS. Le gabarit binaire indique les types d'événements de SCN pour lesquels le nœud s'enregistre.

Noter que le réglage de ce gabarit binaire détermine si l'enregistrement de SCN est pour les SCN régulières ou les SCN de gestion. Les nœuds de gestion PEUVENT conduire des enregistrements pour des SCN de gestion ; les clients iSNS qui ne prennent pas en charge les nœuds de gestion NE DOIVENT PAS conduire des enregistrements pour des SCN de gestion. Les nœuds de gestion qui s'enregistrent pour les SCN de gestion reçoivent une copie de chaque message de SCN généré par le serveur iSNS. Il est recommandé que les enregistrements de gestion ne soient utilisés que quand nécessaire afin de conserver les ressources du serveur iSNS. De plus, un nœud de gestion qui conduit de tels enregistrements devrait être prêt à recevoir le volume prévu de trafic de messages de SCN.

5.6.5.6 Demande Désenregistrer SCN (SCNDereg)

Le type du message SCNDereg est 0x0006. Le message SCNDereg permet à un client iSNS d'arrêter de recevoir des messages de SCN.

La charge utile de PDU du message de demande SCNDereg contient un attribut Source et un ou des attributs de clé de message. Les attributs de clé de message valides pour SCNDereg sont :

Nom iSCSI
Nom WWPN d'accès FC

Le nœud avec un attribut Nom iSCSI ou Nom WWPN d'accès FC qui correspond à l'attribut Clé de message dans le message SCNDereg est désenregistré pour les SCN. Le champ Gabarit binaire SCN de tels nœuds est mis à zéro. Un maximum de un nœud DEVRA être désenregistré pour chaque message SCNDereg.

Il n'y a pas d'attribut de fonctionnement dans le message SCNDereg.

5.6.5.7 Événement SCN (SCNEvent)

Le type de message SCNEvent est 0x0007. SCNEvent est un message envoyé par un client iSNS pour demander la génération d'un message de notification de changement d'état (SCN) par le serveur iSNS. La SCN, envoyée par le serveur iSNS, notifie alors aux nœuds iFCP, iSCSI, de gestion au sein du DD affecté les changements indiqués dans le SCNEvent.

La plupartt des SCN sont automatiquement générées par le serveur iSNS quand des nœuds sont enregistrés ou désenregistrés de la base de données. Les SCN sont aussi générées quand une application de gestion de réseau ou un nœud de gestion fait des changements aux membres du DD dans le serveur iSNS. Cependant, un client iSNS peut déclencher une SCN en utilisant SCNEvent.

La charge utile de la PDU de message SCNEvent contient un attribut Source, un attribut Clé de message, et un attribut de fonctionnement. Les attributs de clé valides pour un SCNEvent sont les suivants :

Nom iSCSI
Nom WWPN d'accès FC

La section attributs de fonctionnement DEVRA contenir l'attribut Gabarit binaire d'événement de SCN. Le gabarit binaire indique l'événement qui a causé la génération du SCNEvent.

5.6.5. Notification de changement d'état (SCN)

Le type de message SCN est 0x0008. La SCN est un message généré par le serveur iSNS, qui notifie des changements d'un nœud de mémorisation enregistré. Il y a deux types d'enrgistrements à la SCN : les enregistrements réguliers et les

enregistrements de gestion. Les SCN régulières notifient aux clients iSNS des événements au sein du domaine de découverte. La SCN de gestion notifie aux nœuds de gestion qui sont enregistrés pour les SCN de gestion les événements qui surviennent partout dans le réseau.

Si il n'existe pas de connexion TCP active pour le receveur de SCN, le message SCN DEVRA alors être envoyé à un portail du nœud de mémorisation enregistré qui a une valeur d'accès enregistré TCP ou UDP dans le champ Accès SCN. Si plus d'un portail du nœud de mémorisation a une valeur d'accès SCN enregistré, la SCN DEVRA alors être livrée à un des portails indiqués, pourvu que le portail choisi ne soit pas le sujet de la SCN.

Les types d'événements qui peuvent déclencher un message SCN, et la quantité d'informations contenues dans le message SCN, dépendent du gabarit binaire d'événement de SCN enregistré pour le nœud de mémorisation. Legabarit binaire de SCN du nœud iSCSI est décrit au paragraphe 6.4.4. Le gabarit binaire de SCN iFCP est décrit au paragraphe 6.6.12.

Le format de la charge utile de la PDU iSCN est montré ci-dessous :

Attribut de destination
Horodatage
Gabarit binaire SCN de source 1
Attribut Source [1]
Attribut Source [2] (si present)
Attribut Source [3] (si present)
Attribut Source [n] (si present)
Gabarit binaire SCN de source 2 (si present)
. . .

Tous les attributs Charge utile de PDU sont en format de TLV.

L'attribut Destination est l'identifiant du nœud qui reçoit la SCN. L'attribut Destination peut être un nom iSCSI ou un nom d'accès FC.

Le champ Horodatage, qui utilise le format de TLV Horodatage, décrit au paragraphe 6.2.4, indique l'heure à laquelle la SCN a été générée.

Le champ Gabarit binaire de source de SCN indique le type de SCN (c'est-à-dire, SCN régulière ou de gestion) et le type d'événement qui a causé la génération de la SCN ; il n'est pas nécessairement corrélé avec le gabarit binaire de la SCN d'origine enregistré dans le serveur iSNS.

À la suite de l'horodatage, le message de SCN DEVRA donner le gabarit binaire de la SCN, suivi par l'attribut de clé (c'est-à-dire, Nom iSCSI ou Nom d'accès FC) du nœud de mémorisation affecté par l'événement de SCN. Si la SCN est de gestion, le message SCN DEVRA alors aussi donner l'identifiant de DD et/ou l'identifiant d'ensemble de DD des domaines de découverte et ensembles de domaines de découverte (si il en est) qui ont causé le changement d'état pour ce nœud de mémorisation. Ces attributs supplémentaires (c'est-à-dire, DD_ID et/ou DDS_ID) devront suivre immédiatement le nom iSCSI ou nom d'accès FC et précéder le prochain gabarit binaire de SCN pour le prochain message de notification (si il en est). Le gabarit binaire de SCN est utilisé comme délimiteur pour les messages de SCN qui fournissent plusieurs notifications de changement d'état.

Par exemple, une SCN regulière pour notifier à un client iSNS un nouveau portail disponible pour une certaine cible iSCSI contiendrait le gabarit binaire de SCN suivi par le nom iSCSI de l'appareil cible comme attribut de source. Si la SCN est une SCN de gestion, le nom iSCSI sera alors suivi par le ou les DD_ID des domaines de découverte partagés qui permettent au nœud de mémorisation de destination d'avoir la visibilité sur le nœud de mémorisation affecté. Si un ensemble de domaines de découverte (DDS) a été activé afin de fournir cette visibilité, le DDS_ID approprié sera alors aussi inclus.

Une SCN de gestion est aussi générée pour notifier à un nœud de gestion la création, suppression, ou modification d'un domaine de découverte ou d'un ensemble de domaines de découverte. Dans ce cas, le DD_ID et/ou DDS_ID du domaine de découverte et/ou ensemble de domaines de découverte affecté va suivre le gabarit binaire de SCN.

Par exemple, une SCN de gestion pour notifier à un nœud de gestion un nouveau DD au sein d'un ensemble de domaines de découverte va contenir le DD_ID et le DDS_ID du domaine de découverte et de l'ensemble de domaines de découverte affectés parmi les attributs Source.

Voir aux paragraphes 6.4.4 et 6.6.12 des informations supplémentaires sur le gabarit binaire de SCN.

5.6.5.9 Enregistrer DD (DDReg)

Le type de message DDReg est 0x0009. Ce message est utilisé pour créer un nouveau domaine de découverte (DD), pour metttre à jour un nom symbolique de DD existant et/ou un attribut de caractéristiques de DD, et pour ajouter des membres à un DD.

Les DD sont définis de façon univoque avec les DD_ID. Les attributs d'enregistrement de DD sont décrits au paragraphe 6.11.

La charge utile de PDU de message DDReg contient l'attribut Source et une clé de message facultative et des attributs de fonctionnement.

La clé de message, si elle est utilisée, contient le DD_ID du domaine de découverte à enregistrer. Si la clé de message contient un DD_ID d'une entrée existante de DD dans la base de données iSNS, le message DDReg DEVRA alors tenter de mettre à jour l'entrée existante. Si le DD_ID dans la clé de message (si elle est utilisée) ne correspond pas à une entrée existante de DD, le serveur iSNS DEVRA alors rejeter le message DDReg avec un code d'état de 3 (Enregistrement invalide). Si le DD_ID est inclus dans la clé de message et dans les attributs de fonctionnement, la valeur du DD_ID dans la clé de message DOIT alors être la même que la valeur de DD_ID dans les attributs de fonctionnement.

Un message DDReg sans clé de message DEVRA résulter en la tentative de création d'un nouveau domaine de découverte (DD). Si l'attribut DD_ID (avec une longueur non zéro) est inclus dans les attributs de fonctionnement dans le message DDReg, le nouveau domaine de découverte DEVRA recevoir la valeur contenue dans cet attribut DD_ID. Autrement, si l'attribut DD_ID n'est pas contenu dans les attributs de fonctionnement du message DDReg, ou si le DD_ID est un attribut de fonctionnement avec une longueur de TLV de 0, le serveur iSNS DEVRA alors allouer une valeur de DD_ID. La valeur de DD_ID allouée sera alors retournée dans le message de réponse DDReg. Les attributs de fonctionnement peuvent aussi contenir l'indice de nœud iSCSI membre de DD, le nom iSCSI de membre du DD, le nom d'accès FC de membre du DD, l'adresse IP du portail de membre du DD, le numéro d'accès TCP/UDP de portail du membre du SS, ou l'indice de portail de membre du DD des membres à ajouter au DD. Ils peuvent aussi contenir le DD_Symbolic_Name et/ou les DD_Features du DD.

Ce message DEVRA ajouter tous les membres du DD figurant comme attributs de fonctionnement au domaine de découverte spécifié par le DD_ID. Si l'attribut DD_Features est un attribut de fonctionnement, il DEVRA alors être mémorisé dans le serveur iSNS comme liste des caractéristiques pour le DD spécifié. Si le nom symbolique de DD est un attribut de fonctionnement et si sa valeur est unique (c'est-à-dire, il ne correspond pas à un nom symbolique de DD enregistré pour un autre DD) la valeur DEVRA alors être mémoriséé dans la base de données iSNS comme nom symbolique de DD pour le domaine de découverte spécifié. Si la valeur du nom symbolique de DD n'est pas unique, alors le serveur iSNS DEVRA rejeter la tentative d'enregistrement de DD avec un code d'état de 3 (Enregistrement invalide).

Lors de la création d'un nouveau DD, si le nom symbolique de DD n'est pas inclus dans les attributs de fonctionnement, ou si il est inclus avec une TLV de longueur zéro, le serveur iSNS DEVRA alors fournir une valeur de nom symbolique de DD unique pour le DD créé. La valeur allouée de nom symbolique de DD DEVRA être retournée dans le message DDRegRsp.

Lors de la création d'un nouveau DD, si l'attribut DD_Features n'est pas inclus dans les attributs de fonctionnement, le serveur iSNS DEVRA alors allouer la valeur par défaut. La valeur par défaut pour DD_Features est 0.

Les attributs Nom iSCSI, Nœud iFCP de membre du DD, Adresse IP de portail de membre du DD, et Numéro d'accès TCP/UDP de membre du DD inclus dans les attributs de fonctionnement n'ont pas besoin de correspondre à des entrées existantes de la base de données iSNS. Cela permet, par exemple, qu'un nœud de mémorisation soit ajouté à un DD même si le nœud de mémorisation n'est pas actuellement enregistré dans la base de données iSNS. Un nœud de mémorisation ou portail peut ainsi être ajouté à un DD au moment de la création du DD, même si le nœud de mémorisation ou portail n'est pas actuellement actif dans le réseau de mémorisation.

Si les attributs de fonctionnement contiennent une valeur de Nom iSCSI de membre du DD pour un nœud de mémorisation qui n'est actuellement pas enregistré dans la base de données iSNS, le serveur iSNS DOIT alors allouer un indice de nœud iSCSI non utilisé pour ce nœud de mémorisation. L'indice de nœud iSCSI alloué DEVRA être retourné dans le message DDRegRsp comme indice de nœud iSCSI de membre du DD. La valeur allouée d'indice de nœud iSCSI DEVRA être allouée au nœud de mémorisation si et quand il s'enregistre dans la base de données iSNS.

Si les attributs de fonctionnement contiennent une adresse IP de portail de membre du DD et une valeur TCP/UDP de portail de membre du DD qui ne sont pas actuellement enregistrées dans la base de données iSNS, le serveur iSNS DOIT alors allouer une valeur d'indice de portail inutilisée pour ce portail. La valeur d'indice de portail allouée DEVRA être retournée dans le message DDRegRsp comme l'indice de portail de membre du DD. La valeur de l'indice de portail allouée DEVRA être attribuée au portail si et quand il s'enregistre dans la base de données iSNS.

Les attributs Indice de nœud iSCSI de membre du DD et Indice de portail de membre du DD qui sont fournis dans les attributs de fonctionnement DOIVENT correspondre à l'indice de nœud iSCSI ou indice de portail correspondant d'une entrée de nœud de mémorisation ou de portail existante dans la base de données iSNS. De plus, l'indice de nœud iSCSI de membre du DD et l'indice de portail de membre du DD NE DEVRONT PAS être utilisés pour ajouter des nœuds de mémorisation ou portails à un DD sauf si ces nœuds de mémorisation ou portails sont activement enregistrés dans la base de données iSNS.

5.6.5.10 Désenregistrer DD (DDDereg)

Le type de message DDDereg est 0x000A. Ce message permet à un client iSNS de se désenregistrer d'un domaine de découverte (DD) existant et de retirer des membres d'un DD existant.

Les DD sont identifiés de façon univoque en utilisant les DD_ID. Les attributs d'enregistrement de DD sont décrits au paragraphe 6.11.

La charge utile de PDU de message DDDereg contient un attribut Source, un attribut Clé de message, et des attributs de fonctionnement facultatifs.

L'attribut Clé de message pour un message DDDereg est l'identifiant de DD pour le domaine de découverte à supprimer ou qui a des membres à supprimer. Si l'identifiant de DD correspond à un DD existant et si il n'y a pas d'attributs de fonctionnement, le DD DEVRA alors être supprimé et un code d'état de réussite sera retourné. Tous les membres existants de ce DD DEVRONT rester dans la base de données iSNS sans appartenance au DD qui vient d'être supprimé.

Si l'identifiant de DD correspond à un DD existant et si il y a des attributs de fonctionnement qui correspondent à des membres du DD, les membres du DD identifiés par les attributs de fonctionnement DEVRONT être supprimés du DD et un code d'état de réussite sera retourné.

Si un nom iSCSI de membre du DD identifié dans les attributs de fonctionnement contient un nom iSCSI pour un nœud de mémorisation qui n'est pas actuellement enregistré dans la base de données iSNS ou contenu dans un autre DD, l'association entre ce nœud de mémorisation et son indice de nœud iSCSI préalloué DEVRA alors être supprimée. La valeur de l'indice de nœud iSCSI préallouée n'a plus d'association à un nom iSCSI spécifique et peut alors être réallouée.

Si une adresse IP de portail de membre de DD et un accès TCP/UDP de membre de DD identifiés dans les attributs de fonctionnement font référence à un portail qui n'est pas actuellement enregistré dans la base de données iSNS ni contenu dans un autre DD, alors l'association entre ce portail et son indice de portail préalloué DEVRA être supprimée. La valeur d'indice de portail préallouée peut alors être réallouée.

La tentative de désenregistrement d'entrées de DD non existantes NE DEVRA PAS être considérée comme une erreur.

5.6.5.11 Enregistrer DDS (DDSReg)

Le type de message DDSReg est 0x000B. Ce message permet à un client iSNS de créer un nouvel ensemble de domaines de découverte (DDS), de mettre à jour un nom symbolique de DDS existant et/ou d'état de DDS, ou d'ajouter des membres du DDS.

Les DDS sont définis de façon univoque en utilisant les identifiants de DDS. Les attributs d'enregistrement de DDS sont décrits au paragraphe 6.11.1.

La charge utile de PDU de message DDSReg contient l'attribut Source et facultativement la clé de message et les attributs de fonctionnement.

La clé de message, si elle est utilisée, contient l'identifiant de DDS de l'ensemble de domaines de découverte à enregistrer ou modifier. Si la clé de message contient un DDS_ID d'une entrée de DDS existante dans la base de données iSNS, le message DDSReg DEVRA alors tenter de mettre à jour l'entrée existante. Si le DDS_ID dans la clé de message (si elle est utilisée) ne correspond pas à une entrée existante de DDS, le serveur iSNS DEVRA alors rejeter le message DDSReg avec un code d'état de 3 (Enregistrement invalide). Si le DDS_ID est inclus à la fois dans la clé de message et dans les attributs de fonctionnement, alors la valeur de DDS_ID dans la clé de message DOIT être la même que la valeur de DDS_ID dans les attributs de fonctionnement.

Un message DDSReg sans clé de message DEVRA résulter en une tentative de création d'un nouvel ensemble de domaines de découverte (DDS). Si l'attribut DDS_ID (avec une longueur non zéro) est inclus dans les attributs de fonctionnement dans le message DDSReg, le nouvel ensemble de domaines de découverte DEVRA recevoir la valeur contenue dans cet

attribut DDS_ID. Autrement, si l'attribut DDS_ID n'est pas contenu dans les attributs de fonctionnement du message DDSReg, ou si le DDS_ID est un attribut de fonctionnement avec une TLV de longueur 0, alors le serveur iSNS DEVRA allouer une valeur de DDS_ID. La valeur de DDS_ID allouée est alors retournée dans le message de réponse à DDSReg. Les attributs de fonctionnement peuvent aussi contenir le nom symbolique de DDS, l'état de DDS, et les identifiants de DD des domaines de découverte à ajouter au DDS.

Lors de la création d'un nouveau DDS, si le nom symbolique de DDS est inclus dans les attributs de fonctionnement et si sa valeur est unique (c'est-à-dire, si il ne correspond pas au nom symbolique de DDS enregistré pour un autre DDS) alors la valeur DEVRA être mémorisée dans la base de données iSNS comme nom symbolique de DDS pour ce DDS. Si la valeur pour le nom symbolique de DDS n'est pas unique, alors le serveur iSNS DEVRA rejeter la tentative d'enregistrement de DDS avec un code d'état de 3 (Enregistrement invalide).

Lors de la création d'un nouveau DDS, si le nom symbolique de DDS n'est pas inclus dans les attributs de fonctionnement, ou si il est inclus avec une TLV de longueur zéro, le serveur iSNS DEVRA alors fournir une valeur unique de nom symbolique de DDS pour le DDS créé. La valeur de nom symbolique de DDS allouée DEVRA être retournée dans le message DDSRegRsp.

Ce message DEVRA ajouter tous les identifiants de DD figurant sur la liste des attributs de fonctionnement à l'ensemble de domaines de découverte spécifié par l'attribut Clé de message de DDS_ID. De plus, si le nom symbolique de DDS est un attribut de fonctionnement et si sa valeur est unique, alors il DEVRA être mémorisé dans la base de données iSNS comme nom symbolique de DDS pour l'ensemble de domaines de découverte spécifié.

Si un identifiant de DD figurant sur la liste des attributs de fonctionnement ne correspond pas à un DD existant, alors un nouveau DD utilisant le DD_ID DEVRA être créé. Dans ce cas, pour le nouveau DD, le serveur iSNS DEVRA allouer une valeur unique pour le nom symbolique de DD et DEVRA régler l'attribut Caractéristiques de DD à la valeur par défaut de 0. Cette valeur allouée DEVRA être retournée dans le message DDSRegRsp.

5.6.5.12. Désenregistrer DDS (DDSDereg)

Le type de message DDSDereg est 0x000C. Ce message permet à un client iSNS de désenregistrer un ensemble de domaines de découverte (DDS) existant ou de supprimer des DD d'un DDS existant.

La charge utile de PDU de message DDSDereg contient un attribut Source, un attribut Clé de message, et des attributs de fonctionnement facultatifs.

L'attribut Clé de message pour un message DDSDereg est l'identifiant de DDS pour le DDS à supprimer ou qui a des membres à supprimer. Si l'identifiant de DDS correspond à un DDS existant et si il n'y a pas d'attributs de fonctionnement, alors le DDS DEVRA être supprimé et un code d'état de succès sera retourné. Tous les membres existants de ce DDS DEVRONT rester dans la base de données iSNS sans appartenance dans le DDS qui vient d'être supprimé

Si l'identifiant de DDS correspond à un DDS existant, et si il y a des attributs de fonctionnement qui correspondent à des membres du DDS, alors les membres du DDS DEVRONT être retirés du DDS et un code d'état de succès sera retourné.

La tentative de désenregistrement d'entrées de DDS non existantes NE DEVRA PAS être considérée comme une erreur.

5.6.5.13 Enquête sur l'état d'entité (ESI)

Le type de message ESI est 0x000D. Ce message est envoyé par le serveur iSNS, et est utilisé pour vérifier qu'un portail de client iSNS est accessible et disponible. Le message ESI est envoyé à l'accès UDP d'ESI fourni durant l'enregistrement, ou à la connexion TCP utilisée pour l'enregistrement d'ESI, selon le type de communication utilisé.

La charge utile de PDU de message ESI contient les attributs suivant en format de TLV et dans l'ordre donné : l'horadatage iSNS actuel, l'EID, l'adresse IP de portail, et l'accès TCP/UDP du portail. Le format de ce message est montré ci-dessous :

Horodatage
Identifiant d'entité
Adresse IP de portail
Accès TCP/UDP du portail

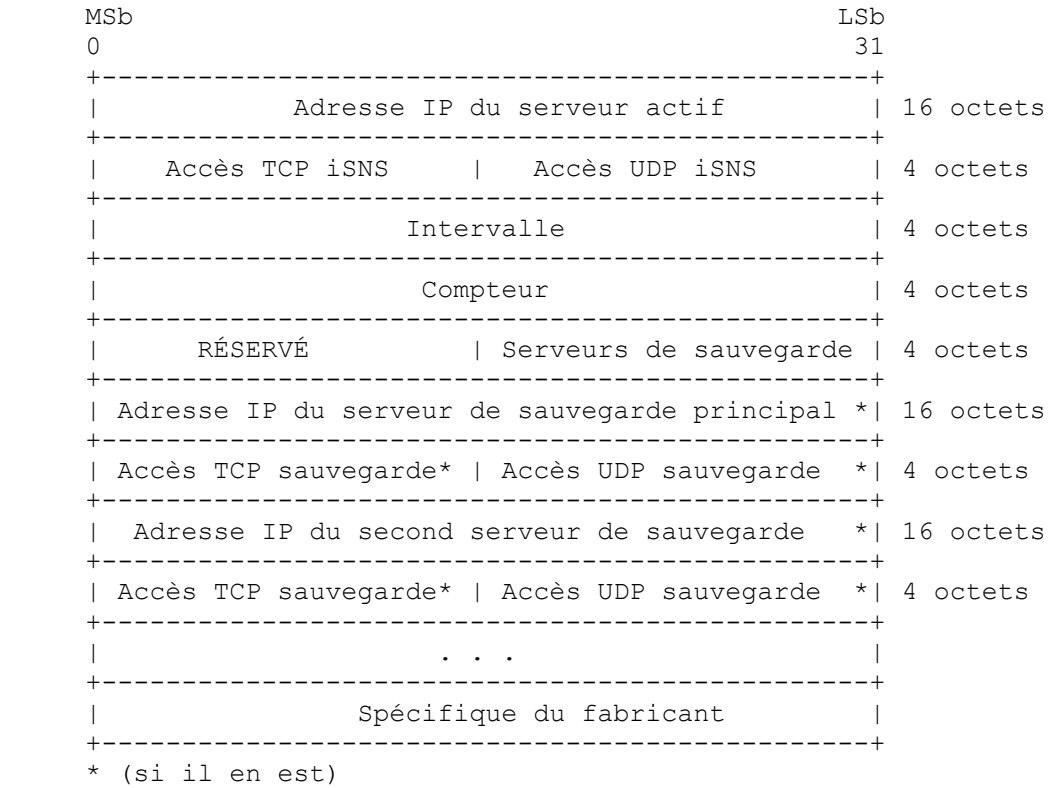
La charge utile de la PDU message de réponse ESI contient un code d'état, suivi par les attributs provenant du message ESI d'origine.

Si le portail échoue à répondre à un nombre déterminé administrativement de messages ESI consécutifs, le serveur iSNS DEVRA alors supprimer ce portail de la base de données iSNS. Si il ne reste pas d'autres portails surveillés par ESI pour l'entité réseau associée, l'entité réseau DEVRA alors aussi être supprimée. Les notifications de changement d'état appropriées, s'il en est, DEVRONT être déclenchées.

5.6.5.14 Battement de cœur de service de nom (Heartbeat)

Ce message, si il est utilisé, n'est envoyés que par le serveur iSNS actif. Il permet aux clients iSNS et aux serveurs de sauvegarde qui écoutent sur une adresse de diffusion ou de diffusion groupée de découvrir l'adresse IP du serveur iSNS principal et des serveurs de sauvegarde. Il permet aussi aux parties concernées de surveiller la santé et l'état du serveur iSNS principal.

Ce message N'EST PAS en format de TLV. IL n'y a pas de message de réponse au battement de cœur de service de nom.



La charge utile de PDU Battement de cœur contient ce qui suit :

Adresse IP du serveur actif : adresse IP du serveur iSNS actif en format IPv6. Quand ce champ contient une valeur IPv4, elle est mémorisée comme une adresse IPv6 transposée en IPv4. C'est-à-dire que les 10 octets de poids fort sont réglés à 0x00, avec les deux octets suivants réglés à 0xFFFF [RFC2373]. Quand ce champ contient une valeur IPv6, le champ entier de 16 octets est utilisé.

Accès TCP act:if : accès TCP pour le serveur actuellement utilisé.

Accès UDP actif : accès UDP du serveur actuellement utilisé, autrement, 0.

Intervalle : l'intervalle, en secondes, du battement de cœur.

Compteur : compteur qui commence à 0 quand ce serveur devient actif. Le compte s'incrémente de un pour chaque battement de cœur envoyé depuis que ce serveur est devenu actif.

Serveurs de sauvegarde : le nombre de serveurs iSNS de sauvegarde. L'adresse IP, l'accès TCP, et l'accès UDP de chaque serveur iSNS de sauvegarde suivent ce champ. Noter que si des serveurs de sauvegarde sont utilisés, le serveur iSNS actif DEVRAIT être dans la liste des serveurs de sauvegarde.

Le contenu du reste de ce message après la liste des serveurs de sauvegarde est spécifique du fabricant. Les fabricants peuvent utiliser des champs supplémentaires pour la coordination entre plusieurs serveurs iSNS, et/ou pour identifier des caractéristiques spécifiques du fabricant.

5.6.5.15 Demande d'identifiant de domaine FC (RqstDomId)

Le type de message RqstDomId est 0x0011. Ce message est utilisé pour le mode iFCP transparent pour allouer des valeurs non chevauchantes d'identifiant de domaine FC entre 1 et 239. Le serveur iSNS devient l'autorité d'allocation d'adresses pour le tissu iFCP entier. Pour obtenir plusieurs valeurs d'identifiant de domaine FC, cette demande doit être répétée plusieurs fois au serveur iSNS. Les clients iSNS qui acquièrent des valeurs d'identifiant de domaine FC d'un serveur iSNS DOIVENT s'enregistrer à la surveillance ESI auprès de ce serveur iSNS.

La charge utile de PDU RqstDomId contient trois attributs de TLV dans l'ordre suivant : Le nom (mondial) de commutateur demandeur comme attribut de source, l'identifiant de tissu virtuel comme attribut de clé de message, et l'identifiant préféré comme attribut de fonctionnement. L'identifiant de tissu virtuel est une chaîne qui identifie l'espace de domaines pour lequel le serveur iSNS DEVRA allouer des valeurs d'entier non chevauchantes d'identifiant de domaine FC entre 1 et 239. L'identifiant préféré est la valeur nominale d'identifiant de domaine FC demandé par le client iSNS. Si la valeur d'identifiant préféré est disponible et n'a pas été dejà allouée pour l'identifiant de tissu virtuel spécifié dans le message, le serveur iSNS DEVRA retourner la valeur d'identifiant préféré demandé comme identifiant alloué au client demandeur.

La réponse de RqstDomId contient un code d'état, et l'identifiant alloué d'attribut de TLV, qui contient la valeur d'entier dans l'espace demandé. Si il n'y a plus de valeurs non allouées disponibles dans cet espace, le serveur iSNS DEVRA répondre avec le code d'état 18 "Identifiant de domaine FC non disponible".

Une fois qu'une valeur d'identifiant de domaine FC a été allouée à un client iSNS par le serveur iSNS pour un certain identifiant de tissu virtuel, cette valeur d'identifiant de domaine FC NE DEVRA PAS être réutilisée jusqu'à ce qu'elle soit désallouée, ou qu'une surveillance d'ESI détecte que le client iSNS n'existe plus sur le réseau et que les objets pour ce client soient retirés de la base de données iSNS.

Le serveur et le client iSNS DEVRONT utiliser TCP pour transmettre et recevoir des messages RqstDomId, RqstDomIdRsp, RlseDomId, et RlseDomIdRsp.

5.6.5.16. Libération de FC_DOMAIN_ID (RlseDomId)

Le type de message RlseDomId est 0x0012. Ce message peut être utilisé par le mode iFCP transparent pour libérer les valeurs d'entier d'identifiant utilisées pour allouer les valeurs de 3 octets d'identifiant d'accès de canal fibre.

Le message RlseDomId contient trois attributs de TLV dans l'ordre suivant : Identifiant d'entité comme attribut de source, identifiant de tissu virtuel comme attribut de clé de message, et identifiant alloué comme attribut de fonctionnement. À réception du message RlseDomId, le serveur iSNS DEVRA désallouer la valeur d'identifiant de domaine FC contenue dans l'attribut Identifiant alloué pour l'attribut Identifiant de tissu virtuel spécifié. À la désallocation, cette valeur d'identifiant de domaine FC peut alors être réutilisée et allouée à un client iSNS différent.

Le serveur et le client iSNS DEVRONT utiliser TCP pour transmettre et recevoir les messages RqstDomId, RqstDomIdRsp, RlseDomId, et RlseDomIdRsp.

5.6.5.17 Obtenir les identifiants de domaine FC (GetDomId)

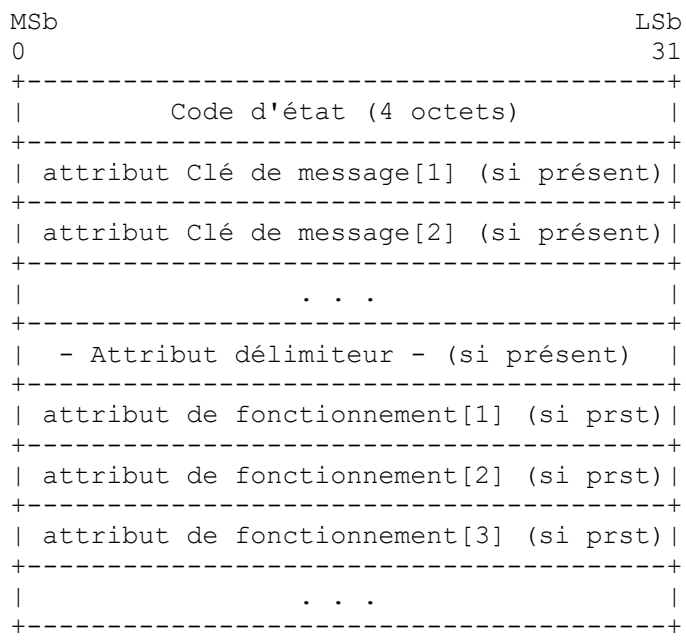
Le type de message GetDomId est 0x0013. Ce message est utilisé pour apprendre les valeurs d'identifiant de domaine FC actuellement allouées pour un certain identifiant de tissu virtuel.

La charge utile de PDU de message GetDomId contient un attribut Source et un attribut Clé de message.

L'attribut Clé de message pour le message GetDomId est l'identifiant de tissu virtuel. La réponse à ce message retourne toutes les valeurs d'identifiant de domaine FC qui ont été allouées pour l'identifiant de tissu virtuel spécifié.

5.7 Messages

Les charges utiles de PDU de message de réponse iSNSP contiennent un code d'état, suivi par une liste d'attributs, et ont le format suivant :



Les messages de réponse iSNSP DEVRONT être envoyés à l'adresse IP du client iSNS et à l'accès TCP/UDP d'origine qui ont éte utilisés pour les messages associés d'enregistrement et d'interrogation.

5.7.1 Code d'état

Le premier champ dans une charge utile de PDU de message de réponse iSNSP est le code d'état pour l'opération qui a été effectuée. Les codages de code d'état sont définis au paragraphe 5.4.

5.7.2 Attributs de clé de message dans la réponse

Selon les spécificités de la demande iSNSP, le message de réponse PEUT contenir des attributs Clé de message. Les attributs Clé de message contiennent généralement les attributs clé intéressants qui sont affectés par l'opération spécifiée dans le message iSNS original d'enregistrement ou d'interrogation.

5.7.3 Attribut délimiteur dans la réponse

L'attribut délimiteur sépare la clé et les attributs de fonctionnement dans un message de réponse, si ils existent. L'attribut délimiteur a une valeur d'étiquette de 0 et une valeur de longueur de 0. L'attribut délimiteur fait huit octets : une étiquette de quatre octets contenant 0x00000000, et un champ Longueur de 4 octets contenant 0x00000000.

5.7.4 Attributs de fonctionnement dans la réponse

Les attributs de fonctionnement dans une réponse sont les résultats qui se rapportent à l'opération d'enregistrement ou d'interrogation iSNS qui est efffectuée. Certains messages de réponse n'ont pas d'attribut de fonctionnement.

5.7.5 Types de message de réponse d'enregistrement et d'interrogation

Les paragraphes qui suivent décrivent chaque type d'interrogation et de message.

5.7.5.1 Réponse d'enregistrement d'attribut d'appareil (DevAttrRegRsp)

Le type de message DevAttrRegRsp est 0x8001. Le message DevAttrRegRsp contient le résultat pour le message DevAttrReg avec le même identifiant de transaction.

La clé de message dans le message DevAttrRegRsp DEVRA retourner la clé de message du message d'enregistrement d'origine. Si le serveur iSNS a alloué l'identifiant d'entité d'une entité réseau, le champ Attribut de clé de message DEVRA alors contenir l'identifiant d'entité alloué.

Les attributs de fonctionnement du message DevAttrRegRsp DEVRONT contenir les attributs clés et non clés des objets affectés qui ont été explicitement modifiés ou créés par le message DevAttrReg d'origine. Parmi les attributs de

fonctionnement, chaque attribut non clé modifié ou ajouté DEVRA figurer sur la liste après son ou ses attributs clés dans le message DevAttrRegRsp. Les attributs enregistrés implicitement NE DOIVENT PAS être retournés dans le message DevAttrRegRsp. Les attributs enregistrés implicitement sont ceux qui ont reçu une valeur fixe par défaut ou une valeur d'indice secondaire par le serveur iSNS.

Les objets PG enregistrés implicitement (c'est-à-dire, les objets PG qui ne sont pas explicitement inclus dans le message d'enregistrement ou de remplacement) NE DOIVENT PAS avoir leurs attributs clés ou non clés retournés dans le message DevAttrRegRsp. Cependant, les objets PG explicitement enregistrés (c'est-à-dire, ceux dont les valeurs de PGT sont explicitement incluses dans le message d'enregistrement ou de remplacement) DEVRONT avoit leur valeur de PGT retournée dans le message DevAttrRegRsp.

Par exemple, trois portails sont enregistrés dans le message de demande original DevAttrReg. Du fait du manque de ressources, le serveur iSNS doit modifier la valeur de l'intervalle d'ESI enregistré d'un de ces portails. Pour ce faire, le serveur iSNS retourne les attributs clés qui identifient le portail, suivis par la valeur d'attribut non clé d'intervalle d'ESI modifié, comme attributs de fonctionnement du message DevAttrRegRsp correspondant.

Si le serveur iSNS rejette un enregistrement à cause de valeurs ou types invalides d'attributs, le code d'état indiqué DEVRA alors être 3 (Enregistrement invalide). Si cela se produit, le serveur iSNS PEUT alors inclure la liste des attributs invalides dans les attributs de fonctionnement du message DevAttrRsp.

Certaines valeurs d'attributs (par exemple, Intervalle d'ESI, Période d'enregistrement) dans le message d'enregistrement d'origine PEUVENT être modifiées par le serveur iSNS. Cela ne peut se produire que pour un ensemble limité de types d'attributs, comme indiqué dans le tableau du paragraphe 6.1. Quand cela se produit, l'enregistrement DEVRA être considéré comme réussi (avec le code d'état 0) et la ou les valeurs changées indiquées dans les attributs de fonctionnement du message DevAttrRsp.

5.7.5.2 Réponse d'interrogation d'attribut d'appareil (DevAttrQryRsp)

Le type de message DevAttrQryRsp est 0x8002. Le message DevAttrQryRsp contient les résultats pour le message DevAttrQry avec le même identifiant de transaction.

La clé de message dans le message DevAttrQryRsp DEVRA retourner la clé de message du message d'interrogation d'origine.

Si aucun attribut de fonctionnement n'est inclus dans l'interrogation d'origine, tous les attributs de fonctionnement DEVRONT alors être retournés dans la réponse.

Pour un résultat d'interrogation réussie, les attributs de fonctionnement de DevAttrQryRsp DEVRONT contenir les résultats du message DevAttrQry d'origine.

5.7.5.3 Réponse Aller à l'appareil suivant (DevGetNextRsp)

Le type de message DevGetNextRsp est 0x8003. Le message DevGetNextRsp contient les résultats pour le message DevGetNext avec le même identifiant de transaction.

Le champ Attribut de clé de message retourne les objets de clé pour le prochain objet après l'attribut Clé de message dans le message DevGetNext d'origine.

Le champ Attribut de fonctionnement retourne les attributs de fonctionnement du prochain objet comme demandé dans le message DevGetNext d'origine. Les valeurs des attributs de fonctionnement sont celles associées à l'objet identifié par le champ Attribut de clé de message du message DevGetNextRsp.

5.7.5.4 Réponse Désenregistrer l'appareil (DevDeregRsp)

Le type de message DevDeregRsp est 0x8004. Ce message est la réponse au message de demande DevDereg.

Ce message de réponse ne contient pas de clé de message, mais PEUT contenir des attributs de fonctionnement.

En cas d'erreur, ce message de réponse contient le code d'état approprié ainsi qu'une liste d'objets provenant du message DevDereg d'origine qui n'ont pas été désenregistrés de la base de données iSNS. Cette liste d'objets est contenue dans les attributs de fonctionnement du message DevDeregRsp. Noter qu'une tentative de désenregistrement d'un objet non existant ne constitue pas une erreur, et des entrées non existantes NE DEVRONT PAS être retournées dans le message DevDeregRsp.

5.7.5.5 Réponse Enregistrer SCN (SCNRegRsp)

Le type de message SCNRegRsp est 0x8005. Ce message est la réponse au message de demande SCNReg.

Le message SCNRegRsp ne contient aucune clé de message ni attribut de fonctionnement.

5.7.5.6 Réponse Désenregistrer SCN (SCNDeregRsp)

Le type de message SCNDeregRsp est 0x8006. Ce message est la réponse au message de demande SCNDereg.

Le message SCNDeregRsp ne contient aucune clé de message ni attribut de fonctionnement.

5.7.5.7 Réponse Événement SCN (SCNEventRsp)

Le type de message SCNEventRsp est 0x8007. Ce message est la réponse au message de demande SCNEvent.

Le message SCNEventRsp ne contient aucune clé de message ni attribut de fonctionnement.

5.7.5.8 Réponse SCN (SCNRsp)

Le type de message SCNRsp est 0x8008. Ce message est envoyé par un client iSNS, et fournit la confirmation que le message SCN a été reçu et traité.

La réponse SCNRsp contient l'attribut Destination de SCN qui représente l'identifiant du nœud qui a réçu la SCN.

5.7.5.9 Réponse Enregistrer DD (DDRegRsp)

Le type de message DDRegRsp est 0x8009. Ce message est la réponse au message de demande DDReg.

La clé de message dans le message DDRegRsp DEVRA retourner la clé de message du message d'interrogation d'origine. Si le message DDReg d'origine n'avait pas de clé de message, alors le message DDRegRsp NE DEVRA PAS avoir de clé de message.

Si l'opération DDReg réussit, l'identifiant de DD du DD créé ou mis à jour DEVRA être retourné comme attribut de fonctionnement du message.

Si l'attribut Nom symbolique de DD ou l'attribut Caractéristiques de DD a été alloué ou mis à jour durant l'opération DDReg, toutes les nouvelles valeurs DEVRONT alors être retournées comme attribut de fonctionnement du message DDRegRsp.

Si le serveur iSNS rejette une DDReg due à des valeurs ou types d'attribut invalides, le code d'état indiqué DEVRA alors être 3 (Enregistrement invalide). Si cela arrive, le serveur iSNS PEUT alors inclure la liste des attributs invalides dans les attributs de fonctionnement du message DDRegRsp.

5.7.5.10 Réponse Désenregistrer DD (DDDeregRsp)

Le type de message DDDeregRsp est 0x800A. Ce message est la réponse au message de demande DDDereg.

Le message DDDeregRsp ne contient aucune clé de message ni attribut de fonctionnement.

5.7.5.11 Réponse Enregistrer DDS (DDSRegRsp)

Le type de message DDSRegRsp est 0x800B. Ce message est la réponse au message de demande DDSReg.

La clé de message dans le message DDSRegRsp DEVRA contenir la clé de message du message DDSReg d'origine. Si le message DDSReg d'origine n'avait pas de clé de message, le message DDSRegRsp NE DEVRA alors PAS avoir de clé de message.

Si l'opération DDSReg est réussie, l'identifiant de DDS du DDS créé ou mis à jour DEVRA être retourné comme attribut de fonctionnement du message.

Si l'attribut Nom symbolique de DDS ou l'attribut État de DDS a été alloué ou mis à jour durant l'opération DDSRegRsp, toutes les nouvelles valeurs DEVRONT alors être retournées comme attributs de fonctionnement du message DDSRegRsp.

Si le serveur iSNS rejette un DDSReg à cause de valeurs ou type d'attributs invalides, le code d'état indiqué DEVRA être 3 (Enregistrement invalide). Si cela arrive, le serveur iSNS PEUT alors inclure la liste des attributs invalides dans les attributs de fonctionnement du message DDSRegRsp.

5.7.5.12 Réponse Désenregistrer DDS (DDSDeregRsp)

Le type de message DDSDeregRsp est 0x800C. Ce message est la réponse au message de demande DDSDereg.

Le message DDSDeregRsp ne contient aucune clé de message ni attribut de fonctionnement.

5.7.5.13. Réponse Enquête sur l'état de l'entite (ESIRsp)

Le type de message ESIRsp est 0x800D. Ce message est envoyé par un client iSNS et fournit la confirmation que le message ESI a été reçu et traité.

La charge utile de PDU de message de réponse ESIRsp contient les attributs provenant du message ESI d'origine. Ces attributs représentent le portail qui répond à l'ESI. Les attributs ESIRsp sont dans l'ordre dans lequel ils étaient fournis dans le message ESI d'origine.

À réception de la ESIRsp du client iSNS, le serveur iSNS DEVRA mettre à jour l'attribut Horodatage pour cette entité réseau et ce portail.

5.7.5.14. Réponse de demande FC_DOMAIN_ID (RqstDomIdRsp)

Le type de message RqstDomIdRsp est 0x8011. Ce message fournit la réponse à RqstDomId.

La réponse à RqstDomId contient un code d'état et la TLV d'attribut Identifiant alloué, qui contient la valeur d'entier dans l'espace demandé. Si aucune autre valeur non allouée n'est disponible dans cet espace, le serveur iSNS DEVRA répondre avec le code d'état 19 "Identifiant de domaine FC non disponible".

Une fois qu'une valeur de FC_DOMAIN_ID a été allouée par le serveur iSNS, elle NE DEVRA PAS être réutilisée jusqu'à ce qu'elle ait été désallouée par le client iSNS auquel la valeur a été allouée, ou jusqu'à ce que le message ESI détecte que le client iSNS n'existe plus sur le réseau.

Le serveur et le client iSNS DEVRONT utiliser TCP pour transmettre et recevoir les messages RqstDomId, RqstDomIdRsp, RlseDomId, et RlseDomIdRsp.

5.7.5.15 Réponse Libérer FC_DOMAIN_ID (RlseDomIdRsp)

Le type de message RlseDomIdRsp est 0x8012. Ce message fournit la réponse à RlseDomId. La réponse contient une erreur qui indique si la demande a réussi. Si la valeur d'identifiant alloué *(Assigned_ID)* dans le message RlseDomId d'origine n'est pas allouée, le serveur iSNS DEVRA alors répondre avec ce message en utilisant le code d'état 20 "Identifiant de domaine FC non alloué".

Le serveur et le client iSNS DEVRONT utiliser TCP pour transmettre et recevoir les messages RqstDomId, RqstDomIdRsp, RlseDomId, et RlseDomIdRsp.

5.7.5.16 Réponse Obtenir les FC_DOMAIN_ID (GetDomIdRsp)

Le type de message GetDomIdRsp est 0x8013. Ce message est utilisé pour déterminer quelles valeurs d'identifiant de domaine FC ont été allouées pour l'identifiant de tissu virtuel spécifié dans le message de demande original GetDomId.

La charge utile de PDU de message de réponse GetDomId contient un code d'état indiquant si la demande a réussi, et une liste des identifiants alloués de l'espace demandé. Les attributs Identifiant alloué sont énumérés en format de TLV.

5.8 Messages spécifiques de fabricant

Les messages iSNSP spécifiques de fabricant ont un identifiant fonctionnel entre 0x0100 et 0x01FF, tandis que les réponses spécifique du fabricant ont un identifiant fonctionnel entre 0x8100 et 0x81FF. Le premier attribut Clé de message dans un message spécifique du fabricant DEVRA être le OUI d'entreprise (étiquette=256) qui identifie le créateur original du message iSNSP propriétaire. Le contenu du reste du message est spécifique du fabricant.

6. Attributs iSNS

Les attributs peuvent être mémorisés dans le serveur iSNS en utilisant des messages d'enregistrement iSNSP, et ils peuvent être restitués en utilisant les messages d'interrogation iSNSP. Sauf indication contraire, ces attributs sont fournis par les clients iSNS en utilisant les messages d'enregistrement iSNSP.

6.1 Résumé des attributs iSNS

Le registre complet des attributs d'iSNS est tenu par l'IANA, et le tableau suivant résume l'ensemble initial des attributs iSNS disponible au moment de la publication du présent document.

Attributs	Longueur	Étiquette	Clé d'enregistrement	Clé d'interrogation
Délimiteur	0	0	N/A	N/A
Identifiant d'entité (EID)	31/03/56	1	1	1|2|16 & 17|32|64
Protocole d'entité	4	2	1	1|2|16 & 17|32|64
Adresse IP de gestion	16	3	1	1|2|16 & 17|32|64
Horodatage	8	4	--	1|2|16 & 17|32|64
Gamme de version de protocole	4	5	1	1|2|16 & 17|32|64
Période d'enregistrement	4	6	1	1|2|16 & 17|32|64
Indice d'entité	4	7	1	1|2|16 & 17|32|64
Prochain indice d'entité	4	8	--	1|2|16 & 17|32|64
Entité ISAKMP phase 1	var	11	1	1|2|16 & 17|32|64
Certificat d'entité	var	12	1	1|2|16 & 17|32|64
Adresse IP de portail	16	16	1	1|16 & 17|32|64
Accès TCP/UDP de portail	4	17	1	1|16 & 17|32|64
Nom symbolique de portail	31/03/56	18	16 & 17	1|16 & 17|32|64
Intervalle d'ESI	4	19	16 & 17	1|16 & 17|32|64
Accès d'ESI	4	20	16 & 17	1|16 & 17|32|64
Indice de portail	4	22	16 & 17	1|16 & 17|32|64
Accès de SCN	4	23	16 & 17	1|16 & 17|32|64
Prochain indice de portail	4	24	--	1|16 & 17|32|64
Gabarit binaire de sécurité de portail	4	27	16 & 17	1|16 & 17|32|64
ISAKMP phase 1 de portail	var	28	16 & 17	1|16 & 17|32|64
ISAKMP phase 2 de portail	var	29	16 & 17	1|16 & 17|32|64
Certificat de portail	var	31	16 & 17	1|16 & 17|32|64
Nom iSCSI	31/03/24	32	1	1|16 & 17|32|33
Type de nœud iSCSI	4	33	32	1|16 & 17|32
Alias iSCSI	31/03/56	34	32	1|16 & 17|32
Gabarit binaire de SCN iSCSI	4	35	32	1|16 & 17|32
Indice de nœud iSCSI	4	36	32	1|16 & 17|32
Jeton WWNN	8	37	32	1|16 & 17|32
Prochain indice de nœud iSCSI	4	38	--	1|16 & 17|32
Méthode d'autnentification iSCSI	var	42	32	1|16 & 17|32
Nom iSCSI de PG	31/03/24	48	32|16 & 17	1|16 & 17|32|52
Adresse IP de portail de PG	16	49	32|16 & 17	1|16 & 17|32|52
Accès TCP/UDP de portail de PG	4	50	32|16 & 17	1|16 & 17|32|52
Étiquette de PG (PGT)	4	51	32|16 & 17	1|16 & 17|32|52
Indice de PG	4	52	32|16 & 17	1|16 & 17|32|52
Prochain indice de PG	4	53	--	1|16 & 17|32|52
Nom WWPN d'accès FC	8	64	1	1|16 & 17|64|66|96|128
ID d'accès	4	65	64	1|16 & 17|64
Type d'accès FC	4	66	64	1|16 & 17|64
Nom symbolique d'accès	31/03/56	67	64	1|16 & 17|64
Nom d'accès de tissu	8	68	64	1|16 & 17|64
Adresse de matériel	4	69	64	1|16 & 17|64
Adresse IP d'accès	16	70	64	1|16 & 17|64
Classe de service	4	71	64	1|16 & 17|64
Types FC-4	32	72	64	1|16 & 17|64
Descripteur FC-4	31/03/56	73	64	1|16 & 17|64
Caractéristiques FC-4	128	74	64	1|16 & 17|64
Gabarit binaire de SCN iFCP	4	75	64	1|16 & 17|64

Rôle d'accès	4	76	64	1|16 & 17|64
Nom permanent d'accès	8	77	--	1|16 & 17|64
Code de type FC-4	4	95	--	1|16 & 17|64
Nom WWNN de nœud FC	8	96	64	1|16 & 17|64|96
Nom symbolique de nœud	31/03/56	97	96	64|96
Adresse IP de nœud	16	98	96	64|96
Nœud IPA	8	99	96	64|96
Nom de mandataire iSCSI	31/03/56	101	96	64|96
Nom de commutateur	8	128	128	128
Identifiant préféré	4	129	128	128
Identifiant alloué	4	130	128	128
Virtual_Fabric_ID	31/03/56	131	128	128
OUI de fabricant de serveur iSNS	4	256	--	Attribut SOURCE
Serveur iSNS spécifique de fabricant		257-384	--	Attribut SOURCE
Entité spécifique de fabricant		385-512	1	1|2|16 & 17|32|64
Portail spécifique de fabricant		513-640	16&17 1	|16 & 17|32|64
Nœud iSCSI spécifique de fabricant		641-768	32	16 & 17|32
Nom d'accès FC spéc. de fabricant		769-896	64	1|16 & 17|64
Nom de nœud FC spéc. de fabricant		897-1024	96	64|96
DDS spécifique de fabricant		1025-1280	2049	2049
DD spécifique de fabricant		1281-1536	2065	2065
Autre spécifique de fabricant		1537-2048		
Identifiant de DD_Set	4	2049	2049	1|32|64|2049|2065
Nom symbolique de DD_Set	31/03/56	2050	2049	2049
État de DD_Set	4	2051	2049	2049
DD_Set_Next_ID	4	2052	--	2049
DD_ID	4	2065	2049	1|32|64|2049|2065
Nom symbolique de DD	31/03/56	2066	2065	2065
Indice iSCSI de membre de DD	4	2067	2065	2065
Nom iSCSI de membre de DD	31/03/24	2068	2065	2065
Nom d'accès FC de membre de DD	8	2069	2065	2065
Indice de portail de membre de DD	4	2070	2065	2065
Adresse IP portail de membre de DD	16	2071	2065	2065
Accès TCP/UDP portail de membre DD	4	2072	2065	2065
Caractéristiques de DD	4	2078	2065	2065
Prochain identifiant de DD_ID	4	2079	--	2065

Descriptions des colonnes du tableau :

Longueur : indique en octets la longueur de l'attribut utilisé dans le format de TLV. Les identifiants de longueur variable sont terminés par des NUL et alignés sur 4 octets (les nuls sont inclus dans la longueur).

Étiquette : valeur d'entier allouée par l'IANA de l'étiquette utilisée pour identifier l'attribut. Touts les valeurs d'étiquette indéfinies sont réservées.

Clé d'enregistrement : indique les valeurs d'étiquettes pour la clé d'objet dans les messages DevAttrReg pour enregistrer une nouvelle valeur d'attribut dans la base de données. Ces étiquettes représentent les attributs définis comme clés d'objet à la Section 4.

Clé d'interrogation : indique les valeurs d'étiquette possibles pour la clé de message et la clé d'objet qui sont utilisées dans les messages DevAttrQry pour restituer une valeur mémorisée de la base de données iSNS.

Voici un résumé des valeurs d'étiquettes d'attribut iSNS disponibles pour une future allocation par l'IANA au moment de la publication :

Valeurs d'étiquette	**Clé d'enregistrement**	**Clé d'interrogation**
9-10, 13-15	1	1|2|16 & 17|32|64
21, 25-26, 30	16 & 17	1|16 & 17|32|64
39-41, 44-47	32	1|16 & 17|32
54-63	32|16 & 17	1|16 & 17|32|52
78-82, 85-94	64	1|16 & 17|64
102-127	96	64|96
132-255	--	Attribut SOURCE

2053-2064	2049	2049
2073-2077	2065	2065
2080-65535	à allouer	à allouer

Les clés d'enregistrement et d'interrogations pour les attributs dont les étiquettes sont dans la gamme de 2080 à 65535 seront documentées dans les RFC qui introduiront les nouveaux attributs iSNS. L'IANA assurera l'enregistrement de ces valeurs selon les instructions de la nouvelle RFC.

De nouveaux attributs iSNS avec une des valeurs d'étiquette ci-dessus PEUVENT aussi être conçus comme des attributs en"lecture seule". La nouvelle RFC qui introduira ces attributs comme "en lecture seule" DEVRA les documenter comme tels, et l'IANA enregistrera leurs clés d'enregistrement correspondantes comme "--".

6.2 Attributs d'identifiant d'entité à clé

Les attributs suivants sont mémorisés dans le serveur iSNS en utilisant l'attribut Identifiant d'entité comme clé.

6.2.1 Iidentifiant d'entité (EID)

L'identifiant d'entité (EID) est une desciption fondée sur du texte de longueur variable codée en UTF-8 terminé par NULL pour une entité réseau. Cet attribut de clé identifie de manière univoque chaque entité réseau enregistrée dans le serveur iSNS. La longueur de l'attribut varie de 4 à 256 octets (incluant la terminaison NULL) et c'est une valeur unique au sein du serveur iSNS.

Si le client iSNS ne fournit pas un EID durant l'enregistrement, le serveur iSNS DEVRA en générer un qui soit unique au sein de la base de données iSNS. Si un EID doit être généré, la valeur d'attribut EID dans le message d'enregistrement DEVRA alors être vide (longueur 0). L'EID généré DEVRA être retourné dans la réponse d'enregistrement.

Dans les environnements où le serveur iSNS est intégré dans une infrastructure DNS, l'identifiant d'entité peut être utilisé pour mémoriser le nom de domaine pleinement qualifié (FQDN, *Fully Qualified Domain Name*) de l'appareil iSCSI ou iFCP. Les FQDN de plus de 255 octets NE DOIVENT PAS être utilisés.

Si on utilise pas de FQDN, le serveur iSNS peut être utilisé pour générer des EID. Les EID générés par le serveur iSNS DOIVENT commencer par la chaîne "isns:". Les clients iSNS NE DOIVENT PAS générer et enregistrer des EID qui commencent par la chaîne "isns:".

Ce champ DOIT être normalisé conformément au gabarit nameprep [RFC3491] avant d'être mémorisé dans la base de données iSNS.

6.2.2 Protocole d'entité

Le protocole d'entité est un attribut exigé d'entier de 4 octets qui indique le protocole de mémorisation de bloc utilisé par l'entité réseau enregistrée. Les valeurs utilisées pour cet attribut sont allouées et conservées par l'IANA. L'ensemble initial de protocoles pris en charge par iSNS est le suivant :

Valeur	**Type de protocole d'entité**
1	Pas de protocole
2	iSCSI
3	iFCP
Autres	À allouer par l'IANA

"Pas de protocole" est utilisé pour indiquer que l'entité réseau ne prend pas en charge de protocole de mémorisation de bloc IP. Un nœud de gestion ou nœud de surveillance va probablement (mais pas nécessairement) utiliser cette valeur.

Cet attribut est exigé durant l'enregistrement initial de l'entité réseau.

6.2.3 Adresse IP de gestion

Ce champ contient l'adresse IP qui peut être utilisée pour gérer l'entité réseau et tous les nœuds de mémorisation qui y sont contenus via la MIB iSNS [RFC4939]. Certaines mises en œuvre peuvent aussi utiliser cette adresse IP pour prendre en charge des protocoles de gestion propriétaires spécifiques du fabricant. L'adresse IP de gestion est un champ de 16 octets qui peut contenir une adresse IPv4 ou IPv6. Quand ce champ contient une valeur IPv4, il est mémorisé comme une adresse

IPv6 transposée en IPv4. C'est-à-dire que les dix octets de poids fort sont réglés à 0x00, avec les deux octets suivants réglés à 0xFFFF [RFC2373]. Quand ce champ contient une valeur IPv6, le champ entier de 16 octets est utilisé. Si ce champ n'est pas établi, la gestion dans la bande par l'adresse IP d'un des portails de l'entité réseau est supposée.

6.2.4 Horodatage d'enregistrement d'entité

Ce champ indique l'heure la plus récente à laquelle s'est produit l'enregistrement de l'entité réseau ou à laquelle un attribut d'objet associé a été mis à jour ou interrogé par le client iSNS qui a enregistré l'entité réseau. Le format d'heure est, en secondes, la période de mise à jour depuis la base horaire standard de 00:00:00 GMT le 1er janvier 1970. Ce champ ne peut pas être explicitement enregistré. Ce format de TLV d'horodatage est aussi utilisé dans les messages SCN et ESI.

6.2.5 Gamme de version de protocole

Ce champ contient les versions minimum et maximum du protocole de mémorisation de bloc prises en charge par l'entité réseau. Les deux octets de poids fort contiennent la version maximum prise en charge, et les deux octets de moindre poids contiennent la version minimum prise en charge. Si une gamme n'est pas enregistrée, l'entité réseau est alors supposée prendre en charge toutes les versions du protocole. La valeur 0xffff est un caractère générique qui indique qu'il n'y a pas de minimum ni de maximum. Si l'entité réseau ne prend pas en charge un protocole, ce champ DEVRA alors être réglé à 0.

6.2.6 Période d'enregistrement

Ce champ d'entier non signé de quatre octets indique la période maximum, en secondes, pendant laquelle l'enregistrement DEVRA être conservé par le serveur sans recevoir un message iSNS du client iSNS qui a enregistré l'entité réseau. Les entités qui ne sont pas enregistrées pour la surveillance par ESI DOIVENT avoir une période d'enregistrement non à zéro. Si une période d'enregistrement n'est pas demandée par le client iSNS et si les messages d'enquête d'état d'entité (ESI) ne sont pas activés pour ce client, la période d'enregistrement DEVRA alors être réglée à une valeur différente de zéro par le serveur iSNS. Cette valeur spécifique de la mise en œuvre pour la période d'enregistrement DEVRA être retournée dans la réponse d'enregistrement au client iSNS. La période d'enregistrement peut être réglée à zéro, ce qui indique sa non utilisation, seulement si les messages ESI sont activés pour cette entité réseau.

L'enregistrement DEVRA être supprimé de la base de données iSNS si un message de protocole iSNS n'est pas reçu du client iSNS avant l'expitation de la période d'enregistrement. La réception de tout message de protocole iSNS du client iSNS rafraîchit automatiquement la période d'enregistrement de l'entité et l'horodatage d'enregistrement de l'entité. Pour empêcher l'expiration d'un enregistrement, le client iSNS devrait envoyer un message de protocole iSNS au serveur iSNS à des intervalles plus courts que la période d'enregistrement. Un tel message peut être aussi simple qu'une interrogation sur un de ses propres attributs, en utilisant son nom iSCSI associé ou le nom WWPN d'accès FC comme attribut de source.

Pour un client iSNS qui prend en charge une entité réseau avec plusieurs objets Nœud de mémorisation, la réception d'un message iSNS de tout nœud de mémorisation de cette entité réseau est suffisante pour rafraîchir l'enregistrement pour tout les objets Nœud de mémorisation de l'entité réseau.

Si la prise en charge d'ESI est demandée au titre de l'enregistrement de portail, le message de réponse d'ESI reçu du client iSNS par le serveur iSNS DEVRA rafraîchir l'enregistrement.

6.2.7 Indice d'entité

L'indice d'entité est une valeur d'entier non signé non zéro qui identifie de façon univoque chaque entité réseau enregistrée dans le serveur iSNS. À l'enregistrement initial d'une entité réseau, le serveur iSNS alloue une valeur non utilisée pour l'indice d'entité. Chaque entité réseau dans la base de données iSNS DOIT recevoir une valeur pour l'indice d'entité qui n'est pas allouée à une autre entité réseau. De plus, les valeurs d'indice d'entité pour les entités réseau récemment désenregistrées NE DEVRAIENT PAS être réutilisées à court terme.

L'indice d'entité PEUT être utilisé pour représenter l'entité réseau dans des situations où l'identifiant d'entité est trop long ou par ailleurs inapproprié. Un exemple est quand SNMP est utilisé pour la gestion, comme décrit au paragraphe 2.10.

6.2.8 Prochain indice d'entité

C'est un attribut virtuel contenant une valeur d'entier de 4 octets qui indique la prochaine valeur d'indice d'entité disponible (c'est-à-dire, non utilisée). Cet attribut peut seulement être interrogé ; le serveur iSNS DEVRA retourner un code d'erreur de 3 (Enregistrement invalide) à tout client qui tente d'enregistrer une valeur pour cet attribut. Une clé de message n'est pas requise quand on interroge exclusivement sur cet attribut.

L'indice de prochaine entité PEUT être utilisé par un client SNMP pour créer une entrée dans le serveur iSNS. Les exigences de SNMP sont décrites au paragraphe 2.10.

6.2.9 Propositions de phase 1 d'entité ISAKMP

Ce champ contient la proposition de phase 1 d'IKE, qui fait la liste en ordre de préférence décroissante des suites de protection acceptables pour protéger tous les messages IKE phase 2 envoyés et reçus par l'entité réseau. Cela inclut les SA de phase 2 du client iSNS au serveur iSNS ainsi qu'à l'homologue iFCP et/ou aux appareils iSCSI. Cet attribut contient la charge utilie de SA, les charges utiles de proposition, et la ou les charges utiles de transformation dans le format ISAKMP défini dans la [RFC2408].

Ce champ devrait être utilisé si la mise en œuvre souhaite définir une seule configuration de sécurité de SA de phase 1 utilisée pour protéger tout le trafic IKE de phase 2. Si la mise en œuvre désire avoir une configuration de sécurité différente de SA de phase 1 pour protéger chaque interface de portail, la proposition de phase 1 de portail (paragraphe 6.3.10) devrait être utilisée.

6.2.10 Certificat d'entité

Cet attribut contient un ou plusieurs certificats X.509 qui sont liés à l'entité réseau. Ce certificat est téléchargé et enregistré au serveur iSNS par les clients qui souhaitent permettre à d'autres clients de s'authentifier et accéder aux services offerts par cette entité réseau. Le format du certificat X.509 se trouve dans la [RFC3280]. Ce certificat DOIT contenir un nom de sujet avec une séquence vide et DOIT contenir une extension SubjectAltName codée avec le type dNSName. L'identifiant d'entité (paragraphe 6.2.1) de l'entité identifiée DOIT être mémorisé dans le champ SubjectAltName du certificat.

6.3 Attributs de portail à clé

Les attributs de portail suivants sont enregistrés dans la base de données iSNS en utilisant la combinaison de Adresse IP de portail et Accès TCP/UDP de portail comme clé. Chaque portail est associé à une clé d'objet Identifiant d'entité.

6.3.1 Adresse IP de portail

Cet attribut est l'adresse IP du portail à travers lequel un nœud de mémorisation peut transmettre et recevoir des données de mémorisation. L'adresse IP de portail est un champr de 16 octets qui peut contenir une adresse IPv4 ou IPv6. Quand ce champ contient une adresse IPv4, il est mémorisé comme adresse IPv6 transposée en IPv4. C'est-à-dire que les 10 octets de poids fort sont réglés à 0x00, et les deux octets suivants sont réglés à 0xFFFF [RFC2373]. Quand ce champ contient une adresse IPv6, le champ de 16 octets entier est utilisé. L'adresse IP de portail et le numéro d'accès TCP/UDP de portail (voir le paragraphe 6.3.2) sont utilisés comme clé pour identifier de façon univoque un portail. C'est un attribut exigé pour l'enregistrement d'un portail.

6.3.2. Accès TCP/UDP de portail

L'accès TCP/UDP de portail à travers lequel un nœud de mémorisation peut transmettre et recevoir des données de mémorisation. Les bits 16 à 31 représentent le numéro d'accès TCP/UDP. Le bit 15 représente le type d'accès. Si le bit 15 est réglé à 1, le type d'accès est UDP. Autrement, c'est TCP. Les bits 0 à 14 sont réservés.

Si la valeur du champ est 0, le numéro d'accès est alors le numéro d'accès et le type de protocole implicites canoniques indiqués par le type d'entité associé.

L'adresse IP de portail et le numéro d'accès TCP/UDP de portail sont utilisés comme clé pour identifier un portail de façon univoque. C'est un attribut obligé pour l'enregistrement d'un portail.

6.3.3 Nom symbolique de portail

Description fondée sur un texte de longueur variable codé en UTF-8 et terminé par un NULL allant jusqu'à 256 octets. Le nom symbolique de portail est une description lisible par l'utilisateur de l'entrée de portail dans le serveur iSNS.

6.3.4 Intervalle d'enquête d'état d'entité

Ce champ indique le délai exigé, en secondes, entre les messages d'enquête d'état d'entité (ESI) envoyés du serveur iSNS à cette entité réseau. Les messages ESI peuvent être utilisés pour vérifier qu'un enregistrement de portail continue d'être valide. Pour demander la surveillance par le serveur iSNS, un client iSNS enregistre une valeur non zéro pour cet attribut de portail en utilisant un message DevAttrReg. Le client DOIT enregistrer un accès ESI sur au moins un de ses portails pour recevoir la surveillance ESI.

Si le serveur iSNS ne reçoit pas une réponse attendue à un message ESI, il DEVRA tenter un certain nombre, configuré administrativement, de retransmissions du message ESI. La période d'intervalle d'ESI commence avec la réception par le serveur iSNS de la dernière réponse ESI. Toutes les retransmissions DOIVENT être envoyées avant que deux fois la période d'intervalle d'ESI soit écoulée. Si aucune réponse n'est reçue pour un des messages ESI, le portail DEVRA alors être désenregistré. Noter que seuls les portails qui ont enregistré une valeur dans leur champ Accès ESI peuvent être désenregistrés de cette façon.

Si tous les portails associés à une entité réseau qui se sont enregistrés pour les messages ESI sont désenregistrés du fait de la non réponse, et si aucun enregistrement n'a été reçu du client pendant au moins deux périodes d'intervalle d'ESI, l'entité réseau et tous les objets associés (incluant les nœuds de mémorisation) DEVRONT alors être désenregistrés

Si le serveur iSNS est incapable de prendre en charge les messages ESI ou l'intervalle d'ESI demandé, il DEVRA soit rejeter la demande d'ESI en retournant un code d'état "ESI non disponible", soit modifier l'attribut Intervalle d'ESI en choisissant sa propre valeur convenable et en retournant cette valeur dans les attributs de fonctionnement du message de réponse d'enregistrement.

Si à tout moment un client iSNS qui est enregistré pour les messages ESI n'a pas reçu de message ESI sur un de ses portails comme attendu, le client PEUT alors tenter d'interroger le serveur iSNS en utilisant un message DevAttrQry avec son identifiant d'entité comme clé. Si l'interrogation résulte en l'erreur "pas de telle entrée", le client DEVRA alors clore toutes les connexions TCP restantes avec le serveur iSNS et supposer qu'il n'est plus enregistré dans la base de données iSNS. Un tel client PEUT tenter de se réenregistrer.

6.3.5 Accès ESI

Ce champ contient l'accès TCP ou UDP utilisé pour la surveillance d'ESI par le serveur iSNS à l'adresse IP de portail. Les bits 16 à 31 représentent le numéro d'accès. Si le bit 15 est établi, le type d'accès est UDP. Autrement, l'accès est TCP. Les bits 0 à 14 sont réservés.

Si le client iSNS enregistre un numéro d'accès TCP ou UDP valide dans ce champ, le client DEVRA alors permettre que les messages ESI soient reçu à l'accès TCP ou UDP indiqué. Si un accès TCP est enregistré et si une connexion TCP préexistante de cet accès TCP au serveur iSNS n'existe pas déjà, le client iSNS DEVRA alors accepter de nouvelles connexions TCP du serveur iSNS à l'accès TCP indiqué.

Le serveur iSNS DEVRA retourner une erreur si une entité réseau est enregistrée pour la surveillance ESI et si aucun des portails de cette entité réseau n'a une entrée pour le champ Accès d'ESI. Si plusieurs portails ont un accès d'ESI enregistré, le message ESI peut alors être livré à tout portail indiqué.

6.3.6 Indice de portail

L'indice de portail est une valeur d'entier de quatre octets non zéro qui identifie de façon univoque chaque portail enregistré dans la base de données iSNS. Lors de l'enregistrement initial d'un portail, le serveur iSNS alloue une valeur non utilisée pour l'indice de portail de ce portail. Chaque portail dans la base de données iSNS DOIT recevoir une valeur d'indice de portail qui n'est pas allouée à un autre portail. De plus, les valeurs d'indice de portail de portails récemment désenregistrés NE DEVRAIT PAS être réutilisées à court terme.

L'indice de portail PEUT être utilisé pour représenter un portail enregistré dans des situations où l'adresse IP de portail et l'accès TCP/UDP de portail sont d'utilisation incommode. Un exemple est quand SNMP est utilisé pour la gestion, comme décrit au paragraphe 2.10.

6.3.7 Accès SCN

Ce champ contient l'accès TCP ou UDP utilisé par le client iSNS pour recevoir des messages de SCN du serveur iSNS. Quand une valeur est enregistrée pour cet attribut, un message SCN peut être reçu sur l'accès indiqué pour tout nœud de

mémorisation pris en charge par le portail. Les bits 16 à 31 contiennent le numéro d'accès. Si le bit 15 est établi, le type d'accès est UDP. Autrement, le type d'accès est TCP. Les bits 0 à 14 sont réservés.

Si le client iSNS enregistre un numéro d'accès TCP ou UDP valide dans ce champ, le client DEVRA alors permettre que les messages de SCN soient reçus à l'accès TCP ou UDP indiqué. Si un accès TCP est enregistré et si une connexion TCP préexistante de cet accès TCP au serveur iSNS n'existe pas déjà, le client iSNS DEVRA alors accepter de nouvelles connexions TCP du serveur iSNS à l'accès TCP indiqué.

Le serveur iSNS DEVRA retourner une erreur si un message SCN d'enregistrement est reçu et si aucun des portails de l'entité réseau n'a d'entrée pour l'accès de SCN. Si plusieurs portails ont un accès de SCN enregistré, la SCN DEVRA alors être livrée à un des portails indiqués de cette entité réseau.

6.3.8 Indice du prochain portail

C'est un attribut virtuel contenant une valeur d'entier de 4 octets qui indique la prochaine valeur d'indice de portail disponible (c'est-à-dire, non utilisée). Cet attribut ne peut être qu'interrogé ; le serveur iSNS DEVRA retourner un code d'erreur de 3 (Enregistrement invalide) à tout client qui tente d'enregistrer une valeur pour cet attribut. Une clé de message n'est pas exigée pour une interrogation exclusive pour cet attribut.

L'indice de prochain portail PEUT être utilisé par un client SNMP pour créer une entrée dans le serveur iSNS. Les exigences pour SNMP sont décrites au paragraphe 2.10.

6.3.9 Bits de sécurité de portail

Ce champ de 4 octets contient des fanions qui indiquent les réglages d'attribut de sécurité pour le portail. Le bit 31 (LSb) de ce champ doit être 1 (activé) pour que ce champ contienne des informations significatives. Si le bit 31 est activé, cela signifie que le serveur iSNS peut être utilisé pour mémoriser et distribuer des politiques et réglages de sécurité pour les clients iSNS (c'est-à-dire, les appareils iSCSI). Le bit 30 doit être à 1 pour que les bits 25 à 29 contiennent des informations significatives. Tous les autres bits sont réservés pour des mécanismes de sécurité non IKE/IPsec qui seront spécifiés à l'avenir.

Position de bit	Description du fanion
25	1 = Mode tunnel préféré ; 0 = pas de préférence
26	1 = Mode transport préféré ; 0 = pas de préférence
27	1 = Secret parfait vers l'avant (PFS, *Perfect Forward Secrecy*) activé ; 0 = PFS désactivé
28	1 = Mode agressif activé ; 0 = désactivé
29	1 = Mode principal activé ; 0 = désactivé
30	1 = IKE/IPsec activé ; 0 = IKE/IPsec désactivé
31 (LSb)	1 = Gabarit binaire valide ; 0 = Invalide
Autres	Réservé

6.3.10 Propositions de phase 1 de portail ISAKMP

Ce champ contient la proposition IKE phase 1 qui fait la liste en ordre décroissant de préférence des suites de protection acceptables pour protéger tous les messages IKE phase 2 envoyés et reçus par le portail. Cela inclut les SA de phase 2 provenant du client iSNS au serveur iSNS ainsi qu'à l'homologue iFCP et/ou aux appareils iSCSI. Cet attribut contient la charge utile de SA, la ou les charges utiles de proposition, et la ou les charges utiles de transformation dans le format ISAKMP défini dans la [RFC2408].

Ce champ devrait être utilisé si la mise en œuvre souhaite définir une configuration de sécurité de SA de phase 1 sur la base du portail, par opposition à une définition fondée sur l'entité réseau. Si la mise en œuvre désire avoir une seule configuration de sécurité de SA de phase 1 pour protéger tout le trafic de phase2 sans considération de l'interface utilisée, la proposition d'entité de phase 1 (paragraphe 6.2.9) devrait être utilisée.

6.3.11 Propositions de phase 2 de portail ISAKMP

Ce champ contient la proposition de phase 2 IKE, en format ISAKMP [RFC2408], qui fait la liste en ordre décroissant de préférence des propositions de sécurité acceptables pour protéger le trafic envoyé et reçu par le portail. Ce champ est utilisé seulement si les bits 31, 30, et 29 du gabarit binaire de sécurité (voir le paragraphe 6.3.9) sont activés. Cet attribut contient la charge utile de SA, la ou les charges utiles de proposition, et la ou les charges utiles de transformations associées dans le format ISAKMP défini dans la [RFC2408].

6.3.12 Certificat de portail

Cet attribut contient un ou plusieurs certificats X.509 qui sont un accréditif du portail. Ce certificat est utilisé pour identifier et authentifier les communications à l'adresse IP et à l'accès TCP/UDP pris en charge par le portail. Le format du certificat X.509 est spécifié dans la [RFC3280]. Ce certificat DOIT contenir un nom de sujet avec une séquence vide et DOIT contenir une extension SubjectAltName codée avec le type iPAddress. L'adresse IP de portail (paragraphe 6.3.1) du portail identifié DEVRA être mémorisée dans le champ SubjectAltName du certificat.

6.4 Attributs iSCSI de nœud à clé

Les attributs suivants sont mémorisés dans la base de données iSNS en utilisant l'attribut Nom iSCSI comme clé. Chaque ensemble d'attribut à clé de nœud est associé à une clé d'objet Identifiant d'entité.

Bien que la clé Nom iSCSI soit associée à un identifiant d'entité, elle est unique dans toute la base de données iSNS.

6.4.1 Nom iSCSI

C'est une description fondée sur le texte de longueur variable codée en UTF-8 et terminée par NULL de jusqu'à 224 octets. Cet attribut clé est exigé pour les nœuds de mémorisation iSCSI et il est fourni par le client iSNS. Le nom iSCSI enregistré DOIT se conformer au format décrit dans la [RFC3720] pour les noms iSCSI. La taille maximum d'un nom iSCSI est de 223 octets. En incluant le caractère NULL et l'alignement sur quatre octets (voir au paragraphe 5.3.1), la taille maximum du champ Nom iSCSI fait 224 octets.

Si un nom iSCSI est enregistré sans une clé EID, une entité réseau DEVRA alors être créée et un EID alloué. L'EID alloué DEVRA être retourné dans la réponse d'enregistrement comme attribut de fonctionnement.

Ce champ DOIT être normalisé en accord avec le gabarit stringprep [RFC3722] avant d'être mémorisé dans la base de données iSNS.

6.4.2 Type de nœud iSCSI

Ce champ exigé de 32 bits est un gabarit binaire qui indique le type de nœud de mémorisation iSCSI. Les positions des bits sont définies ci-dessous. Un bit établi (1) indique que le nœud a les caractéristiques correspondantes.

Position de bit	Type de nœud
29	Contrôle
30	Initiateur
31 (LSb)	Cible
Autres	Réservé

Si le bit cible est réglé à 1, le nœud représente alors une cible iSCSI. Le bit cible PEUT être établi par les clients iSNS qui utilisent iSNSP.

Si le bit initiateur est réglé à 1, le nœud représente alors un initiateur iSCSI. Le bit initiateur PEUT être établi par les clients iSNS qui utilisent iSNSP.

Si le bit contrôle est réglé à 1, le nœud représente alors une passerelle, une station de gestion, un serveur iSNS de sauvegarde, ou un autre appareil qui n'est ni un initiateur ni une cible, mais exige la capacité d'envoyer et recevoir des messages iSNSP, incluant des notifications de changement d'état. Établir le bit contrôle est une tâche administrative qui DOIT être effectuée sur le serveur iSNS ; les clients iSNS NE DOIVENT PAS changer ce bit en utilisant iSNSP.

Ce champ PEUT être utilisé par le serveur iSNS pour distinguer les permissionsdes différents types de nœuds iSCSI pour accéder aux diverses fonctions iSNS. Plus d'un bit Type de nœud peut être activé simultanément.

6.4.3 Alias de nœud iSCSI

C'est une description fondée sur le texte, de longueur variable, codée en UTF-8, et terminée par un NULL, de jusqu'à 256 octets. L'alias est une description lisible par l'utilisateur de l'entrée de nœud dans la base de données iSNS.

6.4.4 Bits SCN de nœud iSCSI

Le gabarit binaire de SCN de nœud iSCSI indique les événements pour lesquels le client iSNS enregistreur souhaite recevoir un message de notification. Le tableau qui suit présente les événements qui résultent en notifications, et le champ de bits dans le gabarit binaire de SCN qui, quand il est activé, résulte en la notification correspondante.

Noter que ce champ a une double utilisation : il est utilisé dans le processus d'enregistrement de SCN pour définir les événements intéressants qui vont déclencher un message SCN, et il est aussi contenu dans chaque message SCN lui-même, pour indiquer le type d'événement qui a déclenché le message SCN. Un bit établi (1) indique le type de SCN correspondant.

Position de bit	Description du fanion
24	initiateur et auto information seulement
25	cible et auto information seulement
26	enregistrement de gestion/SCN
27	objet supprimé
28	objet ajouté
29	objet mis à jour
30	membre de DD/DDS supprimé (seulement SCN de gestion/enregistrement)
31 (LSb)	membre de DD/DDS ajouté (seulement SCN de gestion/enregistrement)
Autres	réservé

" membre de DD/DDS supprimé" indique qu'un membre existant d'un domaine de découverte et/ou ensemble de domaines de découverte a été supprimé.

"membre de DD/DDS ajouté" indique qu'un nouveau membre a été ajouté à un DD et/ou DDS existant.

"objet supprimé", "objet ajouté", et "objet mis à jour" indiquent qu'un objet Entité réseau, Portail, Nœud de mémorisation, Appareil FC, DD, et/ou DDS, a été retiré de, ajouté à, ou mis à jour dans le domaine de découverte ou dans la base de données iSNS (seulement les nœuds de gestion).

Les SCN régulières fournissent des informations sur les objets qui sont mis à jour dans les domaines de découverte dont le nœud de mémorisation est membre ou leur sont ajoutés ou retirés. Une SCN ou un enregistrement de SCN est considéré comme une SCN régulière ou un enregistrement de SCN régulière si le fanion enregistrement de gestion/SCN est à zéro. Tous les clients iSNS peuvent s'enregistrer pour les SCN régulières.

Les SCN de gestion fournissent des informations sur tous les changements du réseau, sans considération de l'appartenance à un domaine de découverte. L'enregistrement pour les SCN de gestion est indiqué par le réglage du bit 26 à 1. Seuls les nœuds de gestion peuvent s'enregistrer pour les SCN de gestion. Les bits 30 et 31 ne peuvent être activés que si le bit 26 est réglé à 1.

Les SCN "cible et auto information seulement" (bit 25) fournissent seulement des informations sur les changements aux appareils cibles, ou si le nœud de mémorisation iSCSI lui-même a subi un changement. De même, les SCN "initiateur et auto information seulement" (bit 24) ne fournissent des informations que sur les changements aux nœuds initiateurs, ou à la cible elle-même.

6.4.5 Indice de nœud iSCSI

L'indice de nœud iSCSI est une valeur d'entier de quatre octets non zéro utilisée comme clé qui identifie de façon univoque chaque nœud de mémorisation iSCSI enregistré dans la base de données iSNS. À l'enregistrement initial du nœud de mémorisation iSCSI, le serveur iSNS alloue une valeur inutilisée d'indice de nœud iSCSI. Chaque nœud iSCSI DOIT recevoir une valeur d'indice de nœud iSCSI non allouée à un autre nœud de mémorisation iSCSI. De plus, les valeurs d'indice de nœud iSCSI pour les nœuds de mémorisationr iSCSI récemment désenregistrés NE DEVRAIENT PAS être réutilisées à court terme.

L'indice de nœud iSCSI peut être utilisé comme clé pour représenter un nœud enregistré dans des situations où le nom iSCSI est trop long pour être utilisé comme clé. Un exemple est quand SNMP est utilisé pour la gestion, comme décrit au paragraphe 2.10.

La valeur allouée pour l'indice de nœud iSCSI DEVRA persister tant que le nœud de mémorisation iSCSI est enregistré dans la base de données iSNS ou comme membre d'un domaine de découverte. Une valeur d'indice de nœud iSCSI qui est allouée à un nœud de mémorisation NE DEVRA PAS être utilisée pour un autre nœud de mémorisation tant que le nœud d'origine est enregistré dans la base de données iSNS ou comme membre d'un domaine de découverte.

6.4.6 Jeton WWNN

Ce champ contient une valeur d'entier unique au monde de 64 bits qui peut être utilisée pour représenter le nom mondial de nœud de l'appareil iSCSI dans un tissu canal fibre. Cet identifiant est utilisé durant le processus d'enregistrement de l'appareil et DOIT se conformer aux exigences de [FC-FS].

La passerelle FC-iSCSI utilise la valeur qui se trouve dans ce champ pour enregistrer l'appareil iSCSI dans le serveur de noms canal fibre. Elle est mémorisée dans le serveur iSNS pour empêcher des conflits quand des valeurs de WWNN de "mandataire" sont allouées aux initiateurs iSCSI qui établissent des sessions de mémorisation avec des appareils dans le tissu canal fibre.

Si le client iSNS n'alloue pas de valeur au jeton WWNN, le serveur iSNS DEVRA alors fournir une valeur à ce champ à l'enregistrement initial de ce nœud de mémorisation iSCSI. Le processus par lequel le jeton WWNN est alloué par le serveur iSNS DOIT se conformer aux exigences suivantes :

1. La valeur du jeton WWNN allouée DOIT être unique parmi toutes les entrées de WWN dans la base de données iSNS existante, et parmi tous les appareils qui peuvent être potentiellement enregistrés dans la base de données iSNS.
2. Une fois la valeur allouée, le serveur iSNS DOIT sauvegarder de façon persistente la transposition entre la valeur du jeton WWNN et le nom iSCSI enregistré. C'est-à-dire que les réenregistrements successifs du nœud de mémorisation iSCSI dont la clé est le même nom iSCSI conservent la transposition originale à la valeur de jeton WWNN associée dans le serveur iSNS. De même, la transposition DEVRA persister à travers les réamorçages du serveur iSNS. Une fois allouée, la transposition ne peut être changée que si un message DevAttrReg provenant d'un client iSNS autorisé fournit explicitement une valeur différente de jeton WWNN.
3. Une fois allouée une valeur de jeton WWNN et transposée en un nom iSCSI, cette valeur de jeton WWNN NE DEVRA PAS être réutilisée ou transposée en en autre nom iSCSI.
4. La valeur de jeton WWNN allouée DOIT se conformer aux exigences de format de [FC-FS] pour les noms mondiaux (WWN).

Un client iSNS, comme une passerelle FC-iSCSI ou l'initiateur iSCSI, PEUT enregistrer sa propre valeur de jeton WWNN ou écraser la valeur de jeton WWNN fournie par le serveur, si il souhaite fournir sa propre transposition de nom iSCSI-FC. Cela se fait en utilisant le message DevAttrReg avec le jeton WWNN (étiquette=37) comme attribut de fonctionnement. Une fois écrasée, la nouvelle valeur de jeton WWNN DOIT être mémorisée et sauvegardée par le serveur iSNS, et toutes les exigences spécifiées ci-dessus continuent de s'appliquer. Si un client iSNS tente d'enregistrer une valeur pour ce champ qui ne soit pas unique dans la base de données iSNS ou qui soit par ailleurs invalide, l'enregistrement DEVRA alors être rejeté avec un code d'état de 3 (Enregistrement invalide).

Il PEUT y avoir des enregistrements correspondants dans la base de données iSNS pour l'appareil canal fibre spécifié par le jeton WWNN. Ces enregistrements peuvent contenir des attributs d'appareil pour cet appareil FC enregistré dans le tissu de serveur de noms canal fibre.

6.4.7 Indice de prochain nœud iSCSI

C'est un attribut virtuel contenant une valeur d'entier de 4 octets qui indique la prochaine valeur d'indice de nœud iSCSI disponible (c'est-à-dire, non utilisée). Cet attribut peut seulement être interrogé ; le serveur iSNS DEVRA retourner un code d'erreur de 3 (Enregistrement invalide) à tout client qui tente d'enregistrer une valeur pour cet attribut. Une clé de message n'est pas exigée lors d'une interrogation exclusive pour cet attribut.

L'indice de prochain nœud iSCSI PEUT être utilisé par un client SNMP pour créer une entrée dans le serveur iSNS. Les exigences de SNMP sont décrites au paragraphe 2.10.

6.4.8 Méthode d'authentification iSCSI

Cet attribut contient une chaîne terminée par un caractère NULL de texte codé en UTF-8 qui fait la liste des méthodes d'authentification iSCSI activées pour ce nœud de mémorisation iSCSI, dans l'ordre des préférences. Les valeurs de texte utilisées pour identifier les méthodes d'authentification iSCSI sont incorporées dans cette chaîne d'attribut et séparées par des virgules. Les valeurs de texte sont identiques à celles qu'on trouve dans le document iSCSI principal [RFC3720] ; des valeurs de texte spécifiques du fabricant sont aussi possibles.

Valeur textuelle	Description	Référence
KB5	Kerberos V5	[RFC1510]
SPKM1	Simple clé publique GSS-API	[RFC2025]
SPKM2	Simple clé publique GSS-API	[RFC2025]
SRP	Mot de passe sûr distant	[RFC2945]
CHAP	Protocole de prise de contact avec défi	[RFC1994]
aucune	pas d'autnentification iSCSI	

6.5 Attributs d'objet Groupe de portails à clé

Les attributs suivants sont utilisés pour associer les objets Portail et Nœud de mémorisation iSCSI. Les objets PG sont mémorisés dans la base de données iSNS en utilisant le nom de PG iSCSI, l'adresse IP de portail de PG, et l'accès TCP/UDP de portail de PG comme clés. De nouveaux objets PG sont implicitement ou explicitement créés au moment où sont enregistrés les objets correspondants Portail et/ou Nœud de mémorisation iSCSI. Le paragraphe 3.4 contient une discussion générale sur l'utilisation des PG. Pour les détails sur l'utilisation des groupes de portails, voir la [RFC3720].

6.5.1 Nom de groupe de portails iSCSI

C'est le nom iSCSI pour le nœud de mémorisation iSCSI qui est associé à l'objet PG. Ce nom PEUT représenter un nœud de mémorisation iSCSI non enregistré actuellement dans le serveur.

6.5.2 Adresse IP de portail PG

C'est l'attribut Adresse IP de portail pour le portail qui est associé à l'objet PG. Cette adresse IP de portail PEUT être celle d'un portail qui n'est pas actuellement enregistré dans le serveur.

6.5.3. Accès TCP/UDP de portail PG

C'est l'attribut Accès TCP/UDP de portail pour le portail qui est associé à l'objet PG. Cet accès TCP/UDP de portail PEUT être celui d'un portail qui n'est pas actuellement enregistré dans le serveur.

6.5.4. Étiquette de groupe portail (PGT)

Ce champ est utilisé pour grouper des portails afin de coordonner les connexions dans une session à travers des portails avec un nœud iSCSI spécifié. La PGT est une valeur dans la gamme de 0 à 65535, ou NUL. Une valeur de PGT NULLE est enregistrée en utilisant 0 pour la longueur dans la TLV durant l'enregistrement. Les deux octets de moindre poids de la valeur contiennent la PGT pour l'objet. Les deux octets de poids fort sont réservés. Si une valeur de PGT n'est pas explicitement enregistrée pour une paire Nœud de mémorisation iSCSI et Portail, la valeur de la PGT DEVRA alors être implicitement enregistrée comme 0x00000001.

6.5.5 Indice de groupe portail

L'indice de PG est une valeur d'entier de quatre octets non zéro utilisée comme clé qui identifie de façon univoque chaque objet PG enregistré dans la base de données iSNS. À l'enregistrement initial d'un objet PG, le serveur iSNS DOIT allouer une valeur non utilisée pour l'indice de PG. De plus, les valeurs d'indice de PG pour les objets PG récemment désenregistrés NE DEVRAIENT PAS être réutilisées à court terme.

L'indice de PG PEUT être utilisé comme clé pour faire référence à un PG enregistré dans des situations où un indice unique pour chaque objet PG est exigé. Il PEUT ausi être utilisé comme clé de message dans un message iSNS pour interroger ou mettre à jour un objet PG préexistant. Un exemple de cela est quand SNMP est utilisé pour la gestion, comme décrit au paragraphe 2.10. La valeur allouée à l'indice de PG DEVRA persister tant que le serveur est actif.

6.5.6 Prochain indice de groupe portail

Le prochain indice de PG est un attribut virtuel contenant une valeur d'entier de 4 octets qui indique la prochaine valeur d'indice de PG disponible (c'est-à-dire, non utilisée). Cet attribut ne peut être qu'interrogé ; le serveur iSNS DEVRA retourner un code d'erreur de 3 (Enregistrement invalide) à tout client qui tente d'enregistrer une valeur pour cet attribut. Une clé de message n'est pas exigée pour une interrogation exclusive pour cet attribut.

L'indice de prochain groupe de portails PEUT être utilisé par un client SNMP pour créer une entrée dans le serveur iSNS. Les exigences pour SNMP sont décrites au paragraphe 2.10.

6.6 Attributs d'accès FC par nom à clé

Les attributs suivants sont enregistrés dans la base de données iSNS en utilisant l'attribut de nom mondial (WWPN) d'accès FC comme clé. Chaque ensemble d'attributs d'accès FC à clés est associé à une clé d'objet Identifiant d'entité.

Bien que le nom mondial d'accès FC soit associé à un identifiant d'entité, il est aussi unique au monde.

6.6.1 Nom d'accès FC (WWPN)

Cet identifiant de 64 bits définit de façon univoque l'accès FC, et il est le nom d'accès mondial (WWPN) de l'appareil canal fibre correspondant. Cet attribut est la clé pour le nœud de mémorisation iFCP. Cet identifiant unique au monde est utilisé durant le processus d'enregistrement de l'appareil, et il utilise une valeur conforme à la norme IEEE EUI-64 [EUI-64].

6.6.2 Identifiant d'accès (FC_ID)

L'identifiant d'accès est un identifiant d'adresse canal fibre allouée à un N_Port ou NL_Port durant l'enregistrement de fabrique. Le format de l'identifiant d'accès est défini dans [FC-FS]. Les trois octets de moindre poids contiennent cet identifiant d'adresse. L'octet de poids fort est réservé.

6.6.3. Type d'accès FC

Indique le type de l'accès FC. La liste des codes de valeurs pour ce champ est donnée dans le tableau suivant :

Type	Description
0x0000	Entrée non identifiée/Nulle
0x0001	canal fibre N_Port
0x0002	canal fibre NL_Port
0x0003	canal fibre F/NL_Port
0x0004-0080	RÉSERVÉ
0x0081	canal fibre F_Port
0x0082	canal fibre FL_Port
0x0083	RÉSERVÉ
0x0084	canal fibre E_Port
0x0085-00FF	RÉSERVÉ
0xFF11	RÉSERVÉ
0xFF12	Accès iFCP
0xFF13-FFFF	RÉSERVÉ

6.6.4 Nom d'accès symbolique

C'est une description fondée sur le texte, de longueur variable, codée en UTF-8, et terminée par un caractère NUL, faisant jusqu'à 256 octets, qui est associée au nom d'accès FC enregistré par iSNS dans le réseau.

6.6.5 Nom d'accès de fabrique (FWWN)

Cet identifiant de 64 bits définit de façon univoque l'accès de fabrique. Si l'accès de l'appareil FC est attaché à un accès de tissu canal fibre avec un nom d'accès enregistré, ce nom d'accès de fabrique DEVRA être indiqué dans ce champ.

6.6.6 Adresse de matériel

Ce champ est l'identifiant d'accès NL de 24 bits de l'adresse de matériel demandée, incluse dans iSNSP pour la compatibilité avec les appareils et topologies d'arbitrage de boucle de canal fibre. Les trois octets de moindre poids de ce champ contiennent l'adresse. L'octet de poids fort est réservé.

6.6.7 Adresse IP de l'accès

C'est l'adresse IP de canal fibre associée à l'accès FC. Quand ce champ contient une valeur IPv4, elle est mémorisée comme un adresse IPv6 transposée en IPv4. C'est-à-dire que les dix octets de poids fort sont réglés à 0x00, avec les deux octets suivants réglés à 0xFFFF [RFC2373]. Quand une valeur IPv6 est contenue dans ce champ, les 16 octets du champ sont utilisés.

6.6.8 Classe de service (COS)

Ce champ de gabarit binaire de 32 bits indique le type de classe de service canal fibre qui est prise en charge par l'accès enregistré. Dans le tableau qui suit, un bit réglé à un (1) indique une classe de service prise en charge.

Position de bit	Description
29	canal fibre de classe 2 prise en charge
28	canal fibre de classe 3 prise en charge

6.6.9 Types FC-4

Ce champ de 32 octets indique les types de protocoles FC-4 pris en charge par l'accès associé. Ce champ peut être utilisé pour prendre en charge des appareils canal fibre et est cohérent avec FC-GS-4.

6.6.10 Descripteur FC-4

C'est une description fondée sur le texte de longueur variable codée en UTF-8 et terminée par un caractère NUL qui fait jusqu'à 256 octets qui est associée à l'accès d'apareil enregistré par iSNS dans le réseau. Ce champ peut être utilisé pour prendre en charge des appareils canal fibre et est cohérent avec FC-GS-4.

6.6.11 Caractéristiques FC-4

C'est un dispositif de 128 octets, de 4 bits par type, pour les types de protocoles FC-4 pris en charge par l'accès associé. Ce champ peut être utilisé pour prendre en charge des appareils canal fibre et est cohérent avec FC-GS-4.

6.6.12 Gabarit binaire de SCN iFCP

Ce champ indique les événements auxquels le client iSNS s'intéresse. Ces événements peuvent causer la génération de SCN. Les SCN fournissent des informations sur les objets qui sont mis à jour, ajoutés ou supprimés des domaines de découverte dont la source et la destination sont membres. Les SCN de gestion fournissent des informations sur tous les changements du réseau. Un bit établi (1) indique le type de SCN pour le gabarit binaire comme suit :

Position de bit	Description de fanion
24	initiateur et auto informations seulement
25	cible et auto informations seulement
26	enregistrement de gestion/SCN
27	objet supprimé
28	objet ajouté
29	objet mis à jour
30	membre de DD/DDS supprimé (seulement SCN de gestion/enregistrement)
31 (LSb)	membre de DD/DDS ajouté (seulement SCN de gestion/enregistrement)
Autres	réservé

D'autres informations sur l'utilisation des positions de bit spécifiée ci-dessus se trouvent au paragraphe 6.4.4.

6.6.13 Rôle d'accès

Ce champ exigé de 32 bits est un gabarit binaire qui indique le type de nœud de mémorisation iFCP. Le champs de bits sont définis ci-dessous. Un bit établi indique que le nœud a les caractéristiques correspondantes.

Position de bit	Type de nœud
29	Contrôle
30	initiateur FCP
31 (LSb)	cible FCP
Autres	réservé

Si le bit "cible" est réglé à 1, l'accès représente alors une cible FC. Établir le bit "cible" PEUT être effectué par les clients iSNS en utilisant iSNSP.

Si le bit "initiateur" est réglé à 1, l'accès représente alors un initiateur FC. Établir le bit "initiateur" PEUT être effectué par les clients iSNS en utilisant iSNSP.

Si le bit "'contrôle" est réglé à 1, l'accès représente alors une passerelle, une station de gestion, un serveur iSNS de sauvegarde, ou un autre appareil.

C'est généralement un appareil spécial qui n'est ni un initiateur ni une cible, qui exige la capacité d'envoyer et recevoir des messages iSNSP, incluant des notifications de changement d'état. Établir le bit "contrôle" est une tâche administrative qui DOIT être configurée administrativement sur le serveur iSNS ; les clients iSNS NE DEVRONT PAS être autorisés à changer ce bit en utilisant iSNSP.

Ce champ PEUT être utilisé par le serveur iSNS pour distinguer parmi les permissions des différents clients iSNS. Par exemple, une mise en œuvre de serveur iSNS peut être administrativement configurée à ne permettre aux cibles que de recevoir les ESI, ou de permettre seulement aux nœuds de gestion d'ajouter, modifier, ou supprimer les domaines de découverte.

6.6.14 Nom d'accès permanent (PPN, *Permanent Port Name*)

Le nom d'accès permanent peut être utilisé pour prendre en charge des appareils canal fibre et est cohérent avec la description de PPN dans FC-GS-4 [FC-GS-4]. Le format du PPN est identique au format de l'attribut Nom WWPN d'accès FC.

6.7. Attributs à clé de nœud

Les attributs suivants sont enregistrés dans la base de données iSNS en utilisant l'attribut Nom de nœud FC (WWNN) comme clé. Chaque ensemble d'attributs à clé de nœud FC représente un seul appareil et peut être associé à plusieurs accès FC.

Le nom de nœud FC est unique sur la base de données iSNS entière.

6.7.1 Nnom de nœud FC (WWNN)

Le nom de nœud FC est un identifiant de 64 bits qui est le nom de nœud mondial (WWNN) de l'appareil canal fibre correspondant. Cet attribut est la clé pour l'appareil FC. Cet identifiant unique au monde est utilisé durant le processus d'enregistrement de l'appareil, et il utilise une valeur conforme à la norme IEEE EUI-64 [EUI-64].

6.7.2 Nom symbolique de nœud

C'est une description fondée sur le texte de longueur variable, codée en UTF-8 et terminée par le caractère NUL, qui fait jusqu'à 256 octets, et est associée à l'appareil FC enregistré par iSNS dans le réseau.

6.7.3 Adresse IP de nœud

Cette adresse IP est associée à l'appareil nœud dans le réseau. Ce champ est inclus pour la compatibilité avec canal fibre. Quand ce champ contient une valeur IPv4, il est mémorisé comme une adresse IPv6 transposée en IPv4. C'est-à-dire que les 10 octets de plus fort poids sont réglés à 0x00, et les deux octets suivants sont réglés à 0xFFFF [RFC2373]. Quand une valeur IPv6 est contenue dans ce champ, les 16 octets du champ sont utilisés.

6.7.4 Nœud IPA

Ce champ de 8 octets est l'associateur de processus initial (IPA, *Initial Process Associator*) de canal fibre associé à l'appareil nœud dans le réseau. L'associateur de processus initial est utilisé pour la communication entre appareils canal fibre.

6.7.5 Nom de mandataire iSCSI

C'est un champ fondé sur le texte de longueur variable codé en UTF-8 et terminé par un caratère NUL qui contient le nom iSCSI utilisé pour représenter le nœud FC dans le réseau IP. Il est utilisé comme pointeur sur l'entrée de nom iSCSI correspondante dans le serveur iSNS. Sa valeur est généralement enregistrée par une passerelle FC-iSCSI connectant le réseau IP au tissu qui contient l'appareil FC.

Noter que si ce champ est utilisé, il DEVRAIT y avoir une entrée correspondante dans la base de données iSNS pour l'appareil iSCSI spécifié par le nom iSCSI. l'entrée de la base de données devrait inclure la gamme complète des attributs iSCSI nécessaires pour la découverte et la gestion de "l'image de mandataire iSCSI" de l'appareil FC.

6.8 Autres attributs

Les attributs qui suivent ne relèvent pas des objets précédemment définis.

6.8.1 Code de type FC-4

C'est un champ de 4 octets utilisés pour fournir un type FC-4 durant une interrogation de type FC-4. Les types FC-4 sont cohérents avec ceux définis dans FC-FS. L'octet 0 contient le type FC-4. Tous les autres octets sont réservés.

6.8.2 Nom de commutateur iFCP

Le nom de commutateur iFCP est un identifiant de nom mondial (WWN, *World Wide Name*) de 64 bits qui identifie de façon univoque une passerelle iFCP dans le réseau. Cet identifiant unique au monde est utilisé durant le processus d'allocation d'enregistrement de commutateur/identifiant de domaine FC. La valeur du nom de commutateur iFCP utilisée DOIT se conformer aux exigences de [FC-FS] pour les noms mondiaux. Le serveur iSNS DEVRA suivre à la trace l'état de toutes les valeurs d'identifiant de domaine FC qui ont été allouées à chaque nom de commutateur iFCP. Si un certain nom de commutateur iFCP est désenregistré de la base de données iSNS, toutes les valeurs d'identifiant de domaine FC allouées à ce nom de commutateur iFCP DEVRONT alors être retournées au réservoir des valeurs non utilisées.

6.8.3 Commandes iFCP en mode transparent

6.8.3.1 Identifiant préferé

C'est un champ d'entier non signé de quatre octets, et c'est la valeur demandée que le client iSNS souhaite utiliser pour l'identifiant de domaine FC. Le serveur iSNS DEVRA accorder au client iSNS l'utilisation de la valeur demandée comme identifiant de domaine FC, si la valeur demandée n'a pas été déjà allouée. Si la valeur demandée n'est pas disponible, le serveur iSNS DEVRA retourner une valeur différente qui n'a pas encore été allouée.

6.8.3.2 Identifiant alloué

C'est un champ d'entier non signé de quatre octets qui est utilisé par une passerelle iFCP pour réserver sa propre valeur unique d'identifiant de domaine FC dans la gamme de 1 à 239. Lorsque un identifiant de domaine FC n'est plus exigé, il DEVRA être libéré par la passerelle iFCP en utilisant le message RlseDomId. Le serveur iSNS DOIT utiliser le message d'enquête d'état d'entité (ESI) pour déterminer si une passerelle iFCP est encore présente sur le réseau.

6.8.3.3 Virtual_Fabric_ID

C'est un champ de longueur variable fondé sur le texte codé en UTF-8 et terminé par le caractère NUL de jusqu'à 256 octets. La chaîne Virtual_Fabric_ID *(identifiant de tissu virtuel)* est utilisée comme attribut clé pour identifier une gamme de valeurs non chevauchantes de FC_DOMAIN_ID à allouer en utilisant RqstDomId. Chaque chaîne Virtual_Fabric_ID soumise par un client iSNS DEVRA avoir sa propre gamme de valeurs FC_DOMAIN_ID non chevauchantes à allouer aux clients iSNS.

6.9 Attributs spécifiques de serveur iSNS

L'accès aux attributs suivants peut être administrativement contrôlé. Ces attributs sont spécifiques de l'instance de serveur iSNS ; la même valeur est retournée pour tous les clients iSNS accédant au serveur iSNS. Seuls les messages d'interrogation peuvent être effectués sur ces attributs. La tentative d'enregistrement de valeurs pour ces attributs DEVRA retourner un code d'état de 3 (Enregistrement invalide).

Une interrogation pour un attribut spécifique de serveur iSNS DOIT contenir l'attribut Identifiant clé (c'est-à-dire, le nom iSCSI ou le nom WWPN d'accès FC) du nœud générateur du message d'enregistrement ou d'interrogation comme attributs de source et de clé de message. Les attributs de fonctionnement sont des attributs spécifiques du serveur qui sont enregistrés ou interrogés.

6.9.1 OUI de fabricant de serveur iSNS

Cet attribut est l'identifiant univoque d'organisation (OUI, *Organizationally Unique Identifier*) [802-1990] qui identifie le fabricant spécifique de la mise en œuvre de serveur iSNS. Cet attribut peut seulement être interrogé ; il NE DEVRA PAS être permis aux clients iSNS d'enregistrer une valeur pour l'OUI de fabricant de serveur iSNS.

6.10 Attributs spécifiques de fabricant

Les mises en œuvre de serveur iSNS PEUVENT définir des attributs spécifiques du fabricant pour utilisation privée. Ces attributs PEUVENT être utilisés pour mémoriser des données facultatives qui sont enregistrées et/ou interrogés par les clients iSNS afin d'obtenir des capacités facultatives. Noter qu'aucune mise en œuvre d'attributs spécifiques du fabricant dans le serveur iSNS NE DEVRA imposer une forme de comportement obligatoire de la part du client iSNS.

Les valeurs d'étiquettes utilisées pour une utilisation spécifique du fabricant et de l'utilisateur sont définies au paragraphe 6.1. Pour éviter de mal interpréter les attributs propriétaires, l'OUI du fabricant DOIT être placé dans les trois octets de poids fort du champ Valeur d'attribut lui-même.

L'OUI est défini dans la norme IEEE 802-1990 et c'est la même constante qu'utilisé pour générer les adresses MAC de LAN universel de 48 bits. La propre mise en œuvre iSNS d'un fabricant sera alors capable de reconnaître le OUI dans le champ d'attribut et sera capable d'exécuter le traitement spécifique du fabricant de l'attribut.

6.10.1 Attributs de serveur spécifiques de fabricant

Les attributs avec des étiquettes dans la gamme de 257 à 384 sont des attributs spécifiques du fabricant ou spécifiques du site du serveur iSNS. Les valeurs pour ces attributs sont réglées administrativement par le fabricant qui fournit la mise en œuvre de serveur iSNS. L'accès en interrogation à ces attributs peut être administrativement contrôlé. Ces attributs sont uniques pour chaque instance logique de serveur iSNS. Les messages d'interrogation pour ces attributs DEVRONT utiliser l'identifiant clé (c'est-à-dire, nom iSCSI ou nom WWPN d'accès FC) pour les deux attributs de source et de clé de message. Ces attributs peuvent seulement être interrogés ; les clients iSNS NE DEVRONT pas être autorisés à enregistrer une valeur pour les attributs de serveur.

6.10.2 Attributs d'entité spécifiques de fabricant

Les attributs dans la gamme de 385 à 512 sont des attributs spécifiques du fabricant ou du site utilisés pour décrire l'objet d'entité réseau. Ces attributs ont pour clé l'attribut Identifiant d'entité (étiquette = 1).

6.10.3 Attributs de portail spécifiques de fabricant

Les attributs dans la gamme de 513 à 640 sont des attributs spécifiques du fabricant ou du site utilisés pour décrire l'objet Portail. Ces attributs ont pour clé l'adresse IP de portail (étiquette = 16) et l'accès TCP/UDP de portail (étiquette = 17).

6.10.4 Attributs de nœud iSCSI spécifiques de fabricant

Les attributs dans la gamme de 641 à 768 sont des attributs spécifiques du fabricant ou du site utilisés pour décrire l'objet Nœud iSCSI. Ces attributs ont pour clé le nom iSCSI (étiquette = 32).

6.10.5 Attributs de nom d'accès FC spécifiques de fabricant

Les attributs dans la gamme de 769 à 896 sont des attributs spécifiques du fabricant ou du site utilisés pour décrire l'objet Nom d'accès N_Port. Ces attributs ont pour clé le nom WWPN d'accès FC (étiquette = 64).

6.10.6 Attributs de nom de nœud FC spécifiques de fabricant

Les attributs dans la gamme de 897 à 1024 sont des attributs spécifiques du fabricant ou du site utilisés pour décrire l'objet Nom de nœud FC. Ces attributs ont pour clé le nom WWNN de nœud FC (étiquette = 96).

6.10.7 Attributs de domaine de découverte spécifiques de fabricant

Les attributs dans la gamme de 1025 à 1280 sont des attributs spécifiques du fabricant ou du site utilisés pour décrire l'objet Domaine de découverte. Ces attributs ont pour clé l'identifiant de domaine de découverte (étiquette = 104).

6.10.8 Attributs Ensemble de domaines de découverte spécifiques de fabricant

Les attributs dans la gamme de 1281 à 1536 sont des attributs spécifiques du fabricant ou du site utilisés pour décrire l'objet Ensemble de domaines de découverte. Ces attributs ont pour clé l'identifiant d'ensemble de domaine de découverte (étiquette = 101)

6.10.9 Autres attributs spécifiques de fabricant

Les attributs dans la gamme de 1537 à 2048 peuvent être utilisés pour des attributs clés et non clés qui décrivent de nouveaux objets spécifiques du fabricant spécifiques de la mise en œuvre de serveur iSNS du fabricant.

6.11 Attributs d'enregistrement de domaine de découverte

6.11.1 Attributs à clé d'identifiant d'ensemble de domaine de découverte

6.11.1.1 Identifiant d'ensemble de domaines de découverte (DDS ID)

L'ID de DDS est un identifiant d'entier non signé non nul utilisé dans la base de données de répertoire iSNS comme clé pour indiquer de façon univoque un ensemble de domaines de découverte. Un DDS est une collection de domaines de découverte qui peut être activée ou désactivée par une station de gestion. Cette valeur est utilisée comme clé pour les interrogations d'attributs de DDS. Quand un domaine de découverte est enregistré, il n'est initialement dans aucun DDS.

Si le client iSNS ne fournit pas de DDS_ID dans un message de demande d'enregistrement de DDS, le serveur iSNS DEVRA générer une valeur de DDS_ID qui soit unique au sein de la base de données iSNS pour ce nouveau DDS. L'ID DDS créé DEVRA être retourné dans le message de réponse. La valeur d'ID de DDS de 0 est réservée, et la valeur d'ID de DDS de 1 est utilisée pour le DDS par défaut (voir au paragraphe 2.2.2).

6.11.1.2 Nom symbolique d'ensemble de domaines de découverte

Champ de longueur variable fondé sur le texte, codé en UTF-8 et teminé par un caractère NUL de jusqu'à 256 octets. C'est un champ lisible par l'utilisateur utilisé pour aider un administrateur de réseau à retracer la fonction de DDS. Quand un client enregistre un nom symbolique de DDS, le serveur iSNS DEVRA vérifier son unicité. Si le nom n'est pas unique, l'enregistrement de DDS DEVRA être rejeté avec un code d'état "Enregistrement invalide". Le ou les attributs invalides, dans ce cas de nom symbolique de DDS, DEVRONT être inclus dans la réponse.

6.11.1.3 État d'ensemble de domaines de découverte

Le champ DDS_Status est un gabarit binaire de 32 bits qui indique l'état du DDS. Le bit 0 du gabarit binaire indique si le DDS est activé (1) ou désactivé (0). La valeur par défaut pour le fanion DDS activé est "désactivé" (0).

Position de bit	**État de DDS**
31 (LSb)	DDS activé (1) / DDS désactivé (0)
Autres	réservé

6.11.1.4 Identifiant du prochain ensemble de domaines de découverte

C'est un attribut virtuel contenant une valeur d'entier de 4 octets qui indique la prochaine valeur d'indice d'ensemble de domaines de découverte disponible (c'est-à-dire, non utilisée). Cet attribut ne peut être qu'interrogé ; le serveur iSNS DEVRA retourner un code d'erreur de 3 (Enregistrement invalide) à toute tentative d'un client d'enregistrer une valeur pour cet attribut. Une clé de message n'est pas exigée pour une interrogation exclusive pour cet attribut.

L'indice de prochain ensemble de domaines de découverte PEUT être utilisé par un client SNMP pour créer une entrée dans le serveur iSNS. Les exigences de SNMP sont décrites au paragraphe 2.10.

6.11.2 Attributs à clé d'identifiant de domaine de découverte

6.11.2.1 Identifiant de domaine de découverte (DD ID)

L'identifiant de domaine de découverte est un identifiant d'entier non signé non nul utilisé dans la base de données de répertoire iSNS comme clé pour identifier de façon univoque un domaine de découverte. Cette valeur est utilisée comme clé pour toute interogation d'atttribut de DD. Si le client iSNS ne fournit pas un DD_ID dans un message de demande d'enregistrement de DD, le serveur iSNS DEVRA générer une valeur de DD_ID unique au sein de la base de données iSNS pour ce nouveau DD (c'est-à-dire, le client iSNS sera enregistré dans un nouveau DD). L'identifiant de domaine de découverte créé DEVRA être retourné dans le message de réponse. La valeur d'identifiant de DD de 0 est réservée, et la valeur 1 est utilisée pour le DD par défaut (voir au paragraphe 2.2.2).

6.11.2.2 Nom symbolique de domaine de découverte

C'est un champ fondé sur le texte, de longueur variable, codé en UTF-8, et terminé par un caractère NUL, qui fait jusqu'à 256 octets. Quand un client enregistre un nom symbolique de DD, le serveur iSNS DEVRA vérifier son unicité. Si le nom

n'est pas unique, l'enregistrement de DD DEVRA être rejeté avec un code d'état "Enregistrement invalide". Le ou les attributs invalides, dans ce cas de nom symbolique de DD, DEVRONT être inclus dans la réponse.

6.11.2.3 Membre de domaine de découverte : indice de nœud iSCSI

C'est l'indice de nœud iSCSI d'un nœud de mémorisation qui est membre du DD. Le DD peut avoir une liste de 0 à n membres. L'indice de nœud iSCSI est une autre représentation des membres d'un domaine de découverte, l'autre solution étant le nom iSCSI. L'indice de nœud iSCSI de domaine de découverte est une valeur d'entier de quatre octets non zéro.

L'indice de nœud iSCSI peut être utilisé pour représenter un membre de DD dans des situations où le nom iSCSI est trop long pour être utilisé. Un exemple est quand SNMP est utilisé pour la gestion, comme décrit au paragraphe 2.10.

L'indice de nœud iSCSI et le nom iSCSI mémorisés comme membre dans un DD DEVRONT être cohérents avec les attributs Indice de nœud iSCSI et Nom iSCSI enregistrés pour l'objet Nœud de mémorisation dans le serveur iSNS.

6.11.2.4 Membre de domaine de découverte : nom iSCSI

Champ fondé sur le texte, de longueur variable, codé en UTF-8 et terminé par un caractère NUL, faisant jusqu'à 224 octets. Il indique l'appartenance au nœud de mémorisation iSCSI spécifié dans le domaine de découverte. Noter que le nœud de mémorisation référencé n'a pas besoin d'être activement enregistré dans la base de données iSNS avant que le client iSNS utilise cet attribut. Il n'y a pas de limite au nombre de membres qui peuvent être dans un DD. L'appartenance est représentée par le nom iSCSI du nœud de mémorisation iSCSI.

6.11.2.5 Membre de domaine de découverte : nom d'accès FC

Cet attribut identifiant de 64 bits indique l'appartenance pour un nœud de mémorisation (accès FC) iFCP dans le domaine de découverte. Noter que le nœud de mémorisation référencé n'a pas besoin d'être activement enregistré dans la base de données iSNS avant que le client iSNS utilise cet attribut. Il n'y a pas de limite au nombre de membres qui peuvent être dans un DD. L'appartenance est représentée par le nom d'accès FC (WWPN) du nœud de mémorisation iSCSI.

6.11.2.6 Membre de domaine de découverte : indice de portail

Cet attribut indique l'appartenance au domaine de découverte pour un portail. C'est une autre représentation pour l'appartenance d'un portail à l'adresse IP de portail et d'accès TCP/UDP de portail. Le portail référencé DOIT être activement enregistré dans la base de données iSNS avant que le client iSNS utilise cet attribut.

6.11.2.7 Membre de domaine de découverte : adresse IP de portail

Cet attribut et l'attribut Accès TCP/UDP de portail indiquent l'appartenance au domaine de découverte pour le portail spécifié. Noter que le portail référencé n'a pas besoin d'être activement enregistré dans la base de données iSNS avant que le client iSNS utilise cet attribut.

6.11.2.8 Membre de domaine de découverte : accès TCP/UDP de portail

Cet attribut et l'attribut Adresse IP de portail indiquent l'appartenance au domaine de découverte pour le portail spécifié. Noter que le portail référencé n'a pas besoin d'être activement enregistré dans la base de données iSNS avant que le client iSNS utilise cet attribut.

6.11.2.9 Caractéristiques de membre de domaine de découverte

Caractéristiques de domaine de découverte est un gabarit binaire qui indique les caractéristiques de ce DD. Les positions de bits sont définies ci-dessous. Un bit réglé à 1 indique que le DD a les caractéristiques correspondantes.

Position de bit	Caractéristique de DD
31 (LSb)	Liste d'amorçage activée (1)/désactivée (0)
Autres	réservé

Liste d'amorçage : cette caractéristique indique que la ou les cibles dans ce DD fournissent les capacités d'amorçage pour les membres initiateurs, comme décrit dans la [RFC4173].

6.11.2.10 Identifiant de prochain indice de domaine de découverte

C'est un attribut virtuel contenant une valeur d'entier de quatre octets qui indique la prochaine valeur d'indice de domaine de découverte disponible (c'est-à-dire, non utilisée). Cet attribut peut seulement être interrogé ; le serveur iSNS DEVRA

retourner un code d'erreur de 3 (Enregistrement invalide) à tout client qui tente d'enregistrer une valeur pour cet attribut. Une clé de message n'est pas exigée quand c'est une interrogation exclusive pour cet attribut.

7. Considérations sur la sécurité

7.1 Analyse des menaces sur la sécurité de iSNS

Quand le protocole iSNS est déployé, l'interaction entre serveur iSNS et clients iSNS est soumise aux menaces pour la sécurité suivantes :

a) Un attaquant peut altérer les messages de protocole iSNS, de façon à conduire les appareils iSCSI et iFCP à établir des connexions avec des appareils homologues non dignes de foi, ou pour affaiblir/éliminer la protection IPsec pour le trafic iSCSI ou iFCP.
b) Un attaquant peut se faire passer pour le serveur iSNS réel en utilisant de faux messages Battement de cœur iSNS. Cela peut amener les appareils iSCSI et iFCP à utiliser des serveurs iSNS non dignes de confiance.
c) Un attaquant peut obtenir des informations sur les appareils iSCSI et iFCP en espionnant les messages de protocole iSNS. De telles informations pourraient aider un attaquant à monter une attaque directe sur les appareils iSCSI et iFCP, comme une attaque de déni de service ou un vol physique caractérisé.

Pour traiter ces menaces,les capacités suivantes sont nécessaires :

a) Les messages de protocole iSNS en envoi individuel peuvent devoir être authentifiés. De plus, pour se protéger contre la menace c), la prise en charge de la confidentialité est souhaitable et est EXIGÉE quand certaines fonctions de serveur iSNS sont utilisées.
b) Les messages de protocole iSNS en diffusion groupée comme le message Battement de cœur iSNS peuvent devoir être authentifiés. Ces messages n'ont pas besoin d'être confidentiels car ils ne contiennent pas d'informations critiques.

7.2 Exigences de mise en œuvre et d'utilisation de la sécurité iSNS

Si le serveur iSNS est utilisé pour distribuer des autorisations pour les communications entre les appareils homologues iFCP et iSCSI, IPsec ESP avec la transformation nulle DOIT être mis en œuvre, et la transformation non nulle PEUT être mise en œuvre. Si une transformation non nulle est mise en œuvre, l'algorithme de chiffrement DES NE DEVRAIT PAS être utilisé.

Si le serveur iSNS est utilisé pour distribuer les politiques de sécurité pour les appareils iFCP et iSCSI, alors l'authentification, l'intégrité des données, et la confidentialité DOIVENT être prises en charge et utilisées. Lorsque la confidentialité est désirée ou exigée, IPsec ESP avec la transformation non nulle DEVRAIT être utilisé, et l'algorithme de chiffrement DES NE DEVRAIT PAS être utilisé.

Si le serveur iSNS est utilisé pour fournir la liste d'amorçage aux clients, comme décrit au paragraphe 6.11.2.9, le client d'amorçage iSCSI DEVRAIT alors mettre en œuvre une connexion iSNS sécurisée.

Afin de protéger contre un attaquant qui se fait passer pour un serveur iSNS, les appareils clients DOIVENT prendre en charge la capacité d'authentifier les messages en diffusion ou en diffusion groupée comme les battements de cœur iSNS. Le bloc d'authentification iSNS (qui est de format identique au bloc d'authentification de SLP) DEVRA être utilisé à cette fin. Les clients iSNS DOIVENT mettre en œuvre le bloc d'authentification iSNS et DOIVENT prendre en charge la valeur de BSD de 0x002. Si le serveur iSNS prend en charge les messages iSNS en diffusion ou en diffusion grouée (c'est-à-dire, le battement de cœur) le serveur DOIT alors mettre en œuvre le bloc d'authentification iSNS et DOIT prendre en charge la valeur de BSD de 0x002. Noter que le bloc d'authentification n'est utilisé que pour les messages iSNS de diffusion ou diffusion groupée et NE DOIT PAS être utilisé dans les messages iSNS en envoi individuel.

Il n'est pas exigé que les identités de communication dans les messages de protocole iSNS restent confidentielles. Précisément, l'identité et la localisation du serveur iSNS ne sont pas considérées comme confidentielles.

Pour protéger les messages de protocole iSNS en envoi individuel, les serveurs iSNS qui prennent en charge la sécurité DOIVENT mettre en œuvre ESP en mode tunnel et PEUVENT mettre en œuvre le mode transport.

Toutes les mises en œuvre iSNS qui prennent en charge la sécurité DOIVENT prendre en charge les mécanismes de protection contre la répétition de IPsec.

Les mises en œuvre de la sécurité de iSNS DOIVENT prendre en charge IKE aussi bien en mode principal que en mode agressif pour l'authentification, la négociation des associations de sécurité, et la gestion de clés, en utilisant le DOI IPsec [RFC2407].

La gestion manuelle des clés NE DEVRAIT PAS être utilisée car elle n'assure pas la prise en charge nécessaire de changement de clés. Les mises en œuvre de sécurité de iSNS conformes DOIVENT prendre en charge l'authentification en utilisant une clé pré partagée, et PEUVENT prendre en charge l'authentification de l'homologue sur la base de certificats en utilisant des signatures numériques. L'authentification de l'homologue en utilisant les méthodes de chiffrement à clé publique décrites aux paragraphes 5.2 et 5.3 de IKE [RFC2409] NE DEVRAIT PAS être prise en charge.

Les mises en œuvre de iSNS conformes DOIVENT prendre en charge IKE aussi bien en mode principal que en mode agressif. Le mode principal IKE avec l'authentification à clés pré partagées NE DEVRAIT PAS être utilisé quand un des homologues utilise des adresses IP allouées de façon dynamique. Bien que l'authentification en mode principal avec des clés pré partagées offre une bonne sécurité dans de nombreux cas, les situations d'utilisation de l'allocation dynamique des adresses force l'utilisation d'une clé prépartagée de groupe, qui est vulnérable à l'attaque par interposition. Le ID_KEY_ID IKE de charge utile d'identité NE DOIT PAS être utilisé.

Quand des signatures numériques sont utilisées pour l'authentification, le mode principal ou le mode agressif d'IKE PEUT être utilisé. Dans tous les cas, l'accès à des informations de secret mémorisées localement (clé prépartagée ou clé privée pour signatures numériques) DOIT être convenablement restreint, car la compromission des informations secrètes annulle les propriétés de sécurité des protocoles IKE/IPsec.

Lorsque des signatures numériques sont utilisées pour réaliser l'authentification, un négociateur IKE DEVRAIT utiliser la ou les charges utiles de demande de certificat IKE pour spécifier la (ou les) autorités de certification qui sont de confiance conformément à sa politique locale. Les négociateurs IKE DEVRAIENT vérifier la liste de révocation de certificats (CRL, *Certificate Revocation List*) pertinente avant d'accepter un certificat de PKI à utiliser dans les procédures d'authentification de IKE.

Quand le serveur iSNS est utilisé sans sécurité, les mises en œuvres de protocole de mémorisation de bloc IP DOIVENT prendre en charge une antémémoire négative pour les échecs d'authentification. Cela permet aux mises en œuvre d'éviter de contacter continuellement les points d'extrémité de découverte qui échouent à l'authentification dans IPsec ou à la couche d'application (dans le cas d'établissement iSCSI). L'antémémoire négative n'a pas besoin d'être maintenue dans la mise en œuvre IPsec, mais plutôt dans la mise en œuvre de protocole de mémorisation de bloc IP.

7.3 Découverte des exigences de sécurité des appareils homologues

Une fois que la communication entre clients iSNS et serveur iSNS a été sécurisée par l'utilisation de IPsec, l'appareil client iSNS a la capacité de découvrir les réglages de sécurité nécessaires pour les utiliser à leurs communications d'homologue à homologue avec les protocoles iSCSI et/ou iFCP. Cela fournit un avantage potentiel d'adaptabilité sur les configurations appareil par appareil de politiques de sécurité individuelles pour chaque appareil iSCSI et iFCP.

Le serveur iSNS mémorise les réglages de sécurité pour chaque interface d'appareil iSCSI et iFCP. Ces réglages de sécurité, qui peuvent être restitués par les hôtes autorisés, incluent l'utilisation ou la non utilisation de IPsec, IKE, mode principal, mode agressif. Par exemple, IKE peut n'être pas activé pour une interface particulière d'un appareil homologue. Si un appareil homologue peut apprendre cela à l'avance en consultant le serveur iSNS, il n'aura pas à perdre de temps et de ressources à tenter d'initier une session IKE phase 1 avec cet interface d'appareil homologue.

Si iSNS est utilisé à cette fin, le minimum d'informations qui devraient être apprises du serveur iSNS est l'utilisation ou non de IKE et IPsec par chaque interface d'appareil homologue iFCP ou iSCSI. Ces informations sont codées dans le champ Gabarit binaire de sécurité de chaque portail de l'appareil homologue, et sont applicables interface par interface pour l'appareil homologue. Les interrogations iSNS pour acquérir les données de configuration de sécurité sur les appareils homologues DOIVENT être protégées par l'authentification IPsec/ESP.

7.4 Configuration des politiques de sécurité des appareils iFCP/iSCSI

L'utilisation de iSNS pour la distribution des politiques de sécurité offre un potentiel de réduction de la charge de configuration manuelle des appareils, et de diminution de la probabilité d'échecs de communications dus à des politiques de sécurité incompatibles. Si iSNS est utilisé pour distribuer les politiques de sécurité, l'authentification IPsec, l'intégrité des données, et la confidentialité DOIVENT alors être utilisées pour protéger tous les messages de protocole iSNS.

La configuration complète de IKE/IPsec sur chaque appareil iFCP et/ou iSCSI peut être mémorisée dans le serveur iSNS, incluant les politiques qui sont utilisées pour les négociations IKE phase 1 et phase 2 entre les appareils clients. Le format de charge utile IKE inclut une série de une ou plusieurs propositions que l'appareil iSCSI ou iFCP va utiliser lors de la négociation de la politique IPsec appropriée à utiliser pour protéger le trafic iSCSI ou iFCP.

De plus, les méthodes d'authentification iSCSI utilisées par chaque appareil iSCSI peuvent aussi être mémorisées dans le serveur iSNS. Le champ iSCSI AuthMethod (étiquette = 42) contient une chaîne terminée par le caractère NUL incorporée dans les valeurs de texte qui indiquent les méthodes d'authentification iSCSI à utiliser par cet appareil iSCSI.

Noter que la distribution des politiques de sécurité iSNS n'est pas nécessaire si les réglages de sécurité peuvent être déterminés par d'autres moyens, comme la configuration manuelle ou la distribution de politique de sécurité IPsec. Si une entité réseau a déjà obtenu sa configuration de sécurité via d'autres mécanismes, elle NE DOIT PAS alors demander sa politique de sécurité via iSNS.

7.5 Questions de ressources

Le protocole iSNS est léger et ne va pas générer une quantité significative de trafic. Le trafic iSNS est caractérisé par des messages occasionnels d'enregistrement, de notification, et de mise à jour qui ne consomment pas de quantités significatives de bande passante. Même les mises en œuvre de IPsec fondées sur le logiciel ne devraient pas avoir de problème à traiter les charges de trafic générées par le protocole iSNS.

Pour satisfaire les exigences de sécurité de iSNS, les seules ressources supplémentaires nécessaires au delà de ce qui est déjà exigé pour iSCSI et iFCP impliquent le serveur iSNS. Parce que les nœuds d'extrémité iSCSI et iFCP sont déjà obligés de mettre en œuvre IKE et IPsec, ces exigences existantes peuvent aussi être utilisées pour satisfaire les exigences de IKE et IPsec pour les clients iSNS.

7.6 Interaction iSNS avec IKE et IPSec

Quand la sécurité IPsec est activée, chaque client iSNS avec au moins un nœud de mémorisation enregistré dans la base de données iSNS DEVRA maintenir au moins une association de sécurité de phase 1 avec le serveur iSNS. Tous les messages de protocole iSNS entre les clients iSNS et le serveur iSNS DEVRONT être protégés par une association de sécurité de phase 2.

Quand une entité réseau est retirée de la base de données iSNS, le serveur iSNS DEVRA envoyer un message de suppression de phase 1 au client iSNS homologue associé IKE, et supprimer toutes les SA de phase 1 et phase 2 associées à ce client iSNS.

8. Considérations relatives à l'IANA

Le numéro d'accès TCP et UDP bien connu pour iSNS est 3205.

Les actions de normalisation de la présente RFC créent deux registres tenus par l'IANA pour prendre en charge iSNSP et allouer les valeurs initiales des deux registres. Le premier registre est celui des protocoles de mémorisation de bloc pris en charge par iSNS. Le second registre détaille les attributs standard iSNS qui peuvent être enregistrés et interrogés dans le serveur iSNS. Noter que la présente RFC utilise le registre créé pour le descripteur de structure de bloc (BSD, *Block Structure Descriptor*) à la Section 15 du protocole de localisation de service, version 2 [RFC2608].

8.1 Registre des protocoles de mémorisation de bloc

Afin de tenir un registre des protocoles de mémorisation de bloc acceptés par iSNSP, l'IANA alloue un nombre entier non signé de 32 bits à chaque protocole de mémorisation de bloc pris en charge par iSNS. Ce nombre est mémorisé dans la base de données iSNS comme protocole d'entité. L'ensemble initial de valeurs à tenir par l'IANA pour les protocoles d'entité est indiqué au tableau du paragraphe 6.2.2. Des valeurs supplémentaires pour de nouveaux protocoles de mémorisation de bloc pris en charge par iSNS DEVRONT être allouées par le président du groupe de travail IPS, ou par un expert désigné [RFC2434] nommé par le directeur de la zone Transport de l'IETF.

8.2 Registre des attributs iSNS standard

L'IANA est chargée de la création et de la tenue du registre des attributs iSNS normalisés. La liste initiale des attributs iSNS est décrite à la Section 6. Pour chaque attribut iSNS, cette information DOIT inclure sa valeur d'étiquette, la longueur de l'attribut, et les valeurs d'étiquette pour l'ensemble des clés d'enregistrement et d'interrogation permises qui peuvent être utilisées pour cet attribut. La liste initiale des attributs iSNS à tenir par l'IANA est indiquée au paragraphe 6.1.

L'ajout de nouveaux attributs standard au registre des attributs iSNS normalisés DEVRA exiger le consensus de l'IETF [RFC2434]. La RFC requise pour ce processus DEVRA spécifier l'utilisation de valeurs d'étiquettes réservées à l'allocation par l'IANA au paragraphe 6.1. La RFC DEVRA spécifier au minimum, la valeur de l'étiquette du nouvel attribut, la longueur de l'attribut, et l'ensemble des clés d'enregistrement et d'interrogations permises qui peuvent être utilisées pour le nouvel attribut.

La RFC DEVRA aussi inclure une discussion des raisons pour le ou les nouveaux attributs et comment ils sont utilisés.

Au titre du processus d'obtention du consensus de l'IETF, la RFC proposée et sa documentation de prise en charge DEVRA être communiquée à la liste de diffusion du groupe de travail IPS, ou si le groupe de travail IPS WG est dissous à ce moment, à une liste de diffusion désignée par le directeur de la zone transport de l'IETF. La période de relecture et commentaires DEVRA durer au moins trois mois avant que le président du groupe de travail IPS ou une personne désignée par le directeur de la zone Transport de l'IETF décide de rejeter la proposition ou de faire passer le projet à l'IESG pour publication comme RFC. Quand la spécification est publiée comme RFC, l'IANA va enregistrer le ou les nouveaux attributs iSNS et rendre l'enregistrement disponible à la communauté.

8.3 Registre des descripteurs de structure de bloc (BSD)

Noter que l'IANA est déjà chargée d'allouer et conserver les valeurs utilisées pour le descripteur de structure de bloc pour le bloc d'authentification iSNS (voir au paragraphe 5.5). La Section 15 de la [RFC2608] décrit le procès d'allocation de nouvelles valeurs de BSD.

9. Références normatives

[802-1990] "IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture", Technical Committee on Computer Communications of the IEEE Computer Society, 31 mai 1990.

[EUI-64] IEEE, "Guidelines for 64-bit Global Identifier (EUI-64) Registration Authority", mai 2001.

[FC-FS] "Fiber Channel Framing and Signaling Interface", NCITS Working Draft Project 1331-D

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par la* RFC8174)

[RFC2407] D. Piper, "Le domaine d'interprétation de sécurité IP de l'Internet pour ISAKMP", novembre 1998. *(Obsolète, voir la RFC*4306)

[RFC2408] D. Maughan, M. Schertler, M. Schneider et J. Turner, "Association de sécurité Internet et protocole de gestion de clés (ISAKMP)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2608] E. Guttman et autres, "Protocole de localisation de service, version 2", juin 1999. (*MàJ par* RFC3224) *(P.S.)*

[RFC3279] L. Bassham, W. Polk et R. Housley, "Algorithmes et identifiants pour le profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", avril 2002.

[RFC3280] R. Housley, W. Polk, W. Ford et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", avril 2002. *(Obsolète, voir* RFC5280)

[RFC3491] P. Hoffman et M. Blanchet, "Nameprep : Profil Stringprep pour les noms de domaine internationalisés (IDN)", mars 2003. (*Remplacée par la* RFC5891, *P.S.*)

[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.)*

[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)

[RFC4172] C. Monia et autres, "iFCP – un protocole pour le réseautage des mises en mémoire des canaux en fibre sur Internet", septembre 2005. *(P.S.)*

[RFC4173] P. Sarkar et autres, "Clients d'amorçage qui utilisent le protocole d'interface de système de petit ordinateur sur Internet (iSCSI)", septembre 2005. *(P.S.)*

[RFC4174] C. Monia et autres, "Option IPv4 du protocole de configuration dynamique d'hôte (DHCP) pour le service de noms de mémorisation sur Internet", septembre 2005. *(P.S.)*

10. Références pour information

[FC-GS-4] "Fiber Channel Generic Services-4" (travail en cours), NCITS Working Draft Project 1505-D

[RFC1510] J. Kohl et C. Neuman, "Service Kerberos d'authentification de réseau (v5)", septembre 1993. *(Obsolète, voir* RFC6649)

[RFC1994] W. Simpson, "Protocole d'authentification par mise en cause de la prise de contact en PPP (CHAP)", août 1996.

[RFC2025] C. Adams, "Mécanisme simple de GSS-API à clé publique (SPKM)", octobre 1996. *(P.S.)*

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

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre 1998. *(Rendue obsolète par la* RFC5226)

[RFC2945] T. Wu, "Système SRP d'authentification et d'échange de clés", septembre 2000. *(P.S.)*

[RFC3410] J. Case et autres, "Introduction et déclarations d'applicabilité pour le cadre de gestion standard de l'Internet", décembre 2002. *(Information)*

[RFC3411] D. Harrington, R. Presuhn, B. Wijnen, "Architecture de description des cadres de gestion du protocole simple de gestion de réseau (SNMP)", décembre 2002. (*MàJ par* RFC5343) (STD0062)

[RFC4939] K. Gibbons et autres, "Définitions des objets gérés pour le service de noms de mémorisation sur Internet (iSNS)", juillet 2007. *(P.S.)*

[X.509] Recommandation UIT-T X.509, "Technologies de l'information - Interconnexion des systèmes ouverts - L'annuaire : cadre d'authentification", juin 1997

Appendice A. Exemples iSNS

A.1 Exemple d'initialisation iSCSI

Cet exemple suppose un agent de service (SA) SLP qui a été mis en œuvre sur l'hôte iSNS, et un agent d'utilisateur SLP (UA) qui a été mis en œuvre chez l'initiateur iSNS. Voir dans la [RFC2608] les détails sur les SA et les UA. Cet exemple suppose aussi que la cible est configurée à utiliser le serveur iSNS, et qu'elle a sa politique de contrôle d'accès subordonnée au serveur iSNS.

A.1.1 Simple enregistrement de cible iSCSI

Dans cet exemple, une simple cible avec un seul nom iSCSI s'enregistre auprès du serveur iSNS. La cible est représentée dans le iSNS par une entité contenant un nœud de mémorisation, un portail, et un groupe de portails implicitement enregistré qui fournit une relation entre le nœud de mémorisation et le portail. L'administrateur n'a pas alloué à la cible de nom de domaine pleinement qualifié (FQDN). Dans cet exemple, comme un objet PG n'est pas explicitement enregistré, un groupe de portails avec une PGT de 1 est implicitement enregistré. Dans cet exemple, SLP est utilisé pour découvrir la

localisation du serveur iSNS. Une solution de remplacement est d'utiliser l'option DHCP iSNS [RFC4174] pour découvrir le serveur iSNS.

Appareil cible iSCSI	**Serveur iSNS**	**Station de gestion**
Découvre iSNS--SLP------->		/*La station de gestion est administrativement
	<--SLP--iSNS ici : 192.0.2.100	autorisée à voir tous les DD. L'appareil NAMEabcd
DevAttrReg--------->		était précédemment placé dans le domaine DDabcd
Source :(tag=32) "NAMEabcd"		avec devpdq et devrst.
Clé : <aucune présente>		
Attributs de fonctionnement :		
tag=1: NULL		
tag=2: "iSCSI"		
tag=16: 192.0.2.5		
tag=17: 5001		
tag=32: "NAMEabcd"		
tag=33: cible		
tag=34: "disk 1"		
	<---DevAttrRegRsp SUCCÈS	
	Clé :(tag=1) "isns:0001"	
	Attributs de fonctionnement :	
	tag=1: "isns:0001"	
	tag=2: "iSCSI"	
	tag=16: 192.0.2.5	
	tag=17: 5001	
	tag=32: "NAMEabcd"	/* précédemment placée dans un DD */
	tag=33: cible	
	tag=34: "disk 1"	
	SCN-------->	
	(ou notification SNMP)	
	dest:(tag=32):"MGMTname1"	
	time:(tag=4): <heure courante>	
	tag=35: "MGT-SCN, OBJ-ADD"	
	tag=32: "NAMEabcd"	
		<-------SCNRsp
DevAttrQry--------->		
Source : (tag=32) "NAMEabcd"		
Clé : (tag=33) "initiateur"		
Attributs de fonctionnement :		
tag=16: NULL		
tag=17: NULL		
tag=32: NULL		
/*L'interrogation demande toutes	<---DevAttrQryRsp SUCCÈS	
les adresses IP d'appareil initiateur,	tag=16:192.0.2.1	
numéro d'accès, et nom*/	tag=17:50000	
	tag=32:"devpdq"	
	tag=16:192.0.2.2	
	tag=17:50000	
	tag=32:"devrst"	
/************************		<-----DevAttrQry
Notre cible "NAMEabcd"		Source : "MGMTname1"
découvre deux initiateurs dans des		Clé : (tag=32)"NAMEabcd"
DD partagés. Elle accepte		Attributs de fonctionnement :
l'établissement iSCSI de ces deux		tag=16: NULL
initiateurs identifiés présentés par		tag=17: NULL
iSNS		tag=32: NULL
************************/	DevAttrQryRsp---> SUCCÈS	
	tag=16: 192.0.2.5	
	tag=17: 5001	
	tag=32: "NAMEabcd"	

A.1.2 Enregistrement de cible et configuration de DD

Dans cet exemple, une cible plus complexe, avec deux nœuds de mémorisation et deux portails utilisant la surveillance par ESI, s'enregistre avec le iSNS. Cette cible a été configurée avec un nom de domaine pleinement qualifié (FQDN) dans les serveurs DNS, et l'utilisateur souhaite utiliser cet identifiant pour l'appareil. La cible enregistre explicitement les groupes de portails pour décrire comment chaque portail fournit l'accès à chaque nœud de mémorisation. Un nœud de mémorisation cible permet l'accès coordonné à travers les deux portails. L'autre nœud de mémorisation permet l'accès, mais pas l'accès coordonné, à travers les deux portails.

Appareil cible iSNS	**Serveur iSNS**	**Station de gestion**
Découvre iSNS--SLP-->		/*La station de gestion est
	<--SLP--iSNS ici : 192.0.2.100	administrativement autorisée à voir tous
DevAttrReg-->		les DD */
Source :		
tag=32: "NAMEabcd"		
Clé de message :		
tag=1: "jbod1.exemple.com"		
Attributs de fonctionnement :		
tag=1: "jbod1.exemple.com"		
tag=2: "iSCSI"		
tag=16: 192.0.2.4		
tag=17: 5001		
tag=19: 5		
tag=20: 5002		
tag=16: 192.0.2.5		
tag=17: 5001		
tag=19: 5		
tag=20: 5002		
tag=32: "NAMEabcd"		
tag=33: "Cible"		
tag=34: "Storage Array 1"		
tag=51: 10		
tag=49: 192.0.2.4		
tag=50: 5001		
tag=49: 192.0.2.5		
tag=50: 5001		
tag=32: "NAMEefgh"		
tag=33: "Cible"		
tag=34: "Storage Array 2"	/**********	
tag=51: 20	jbod1.exemple.com est maintenant	
tag=49: 192.0.2.4	enregistré dans iSNS, mais n'est dans	
tag=50: 5001	aucun DD. Donc aucun autre appareil ne	
tag=51: 30	peut le "voir".	
tag=49: 192.0.2.5	**********/	
tag=50: 5001		
	<--DevAttrRegRsp SUCCÈS	
	Clé de message :	
	tag=1: "jbod1.exemple.com"	
	Attributs de fonctionnement :	
	tag=1: "jbod1.exemple.com"	
	tag=2: "iSCSI"	
	tag=16: 192.0.2.4	
	tag=17: 5001	
	tag=19: 5	
	tag=20: 5002	
	tag=16: 192.0.2.5	
	tag=17: 5001	
	tag=19: 5	
	tag=20: 5002	
	tag=32: "NAMEabcd"	
	tag=33: "Cible"	
	tag=34: "Storage Array 1"	
	tag=48: "NAMEabcd"	

tag=49: 192.0.2.4
tag=50: 5001
tag=51: 10
tag=48: "NAMEabcd"
tag=49: 192.0.2.5
tag=50: 5001
tag=51: 10
tag=32: "NAMEefgh"
tag=33: "Cible"
tag=34: "Storage Array 2"
tag=43: X.509 cert
tag=48: "NAMEefgh"
tag=49: 192.0.2.4
tag=50: 5001
tag=51: 20
tag=48: "NAMEefgh"
tag=49: 192.0.2.5
tag=50: 5001
tag=51: 30
SCN------> (ou notification SNMP)
dest:(tag=32)"mgmt.exemple.com"
time:(tag=4): <heure courante>
tag=35: "MGT-SCN, OBJ-ADD"
tag=32: "NAMEabcd"
tag=35: "MGT-SCN, OBJ-ADD"
tag=32: "NAMEefgh"

<--SCNRsp SUCCÈS
tag=32:"mgmt.exemple.com"
<--DevAttrQry
Source :
tag=32:"mgmt.exemple.com"
Clé de message :
tag=32: "NAMEabcd"
Attributs de fonctionnement :
tag=16: <longueur 0>
tag=17: <ongueur 0>
tag=32: <ongueur 0> |

DevAttrQryRsp--> SUCCÈS
Clé de message :
tag=32: "NAMEabcd"
Attributs de fonctionnement :
tag=16: 192.0.2.4
tag=17: 5001
tag=32:"NAMEabcd"
tag=16: 192.0.2.5
tag=17: 5001
tag=32:"NAMEabcd"

Source :
tag=32:"mgmt.exemple.com"
Clé de message :
tag=32: "NAMEefgh"
Attributs de fonctionnement :
tag=16: <longueur 0>
tag=17: <longueur 0>
tag=32: <longueur 0>

DevAttrQryRsp--> SUCCÈS
Clé de message :
tag=32: "NAMEefgh"
Attributs de fonctionnement :
tag=16: 192.0.2.4
tag=17: 5001
tag=32:"NAMEefgh"
tag=16: 192.0.2.5

/**La station de gestion affiche l'apareil,

	tag=17: 5001 tag=32:"NAMEefgh"	l'opérateur décide de placer "NAMEabcd" dans le domaine "DDxyz"*** *********/
/********* La cible est maintenant enregistrée dans iSNS. Elle est alors placée dans un DD préexistant avec DD_ID 123 par une station de gestion. **********/		<--DDReg Source : tag=32:"mgmt.exemple.com" Clé de message : tag=2065: 123 Attributs de fonctionnement : tag=2068: "NAMEabcd"
	DDRegRsp-----> SUCCÈS Clé de message : tag=2065: 123 Attributs de fonctionnement : tag=2065: 123	

A.1.3 Enregistrement d'initiateur et découverte de cible

L'exemple suivant illustre l'enregistrement d'un nouvel initiateur dans le iSNS, et la découverte de la cible NAMEabcd tirée de l'exemple de A.1.2.

Initiateur iSCSI	**iSNS**	**Station de gestion**
Découvre iSNS--SLP-->		/*La station de gestion est autorisée
	<--SLP--iSNS ; ici : 192.36.53.1	administrativement à voir tous les DD
DevAttrReg-->		********/
Source : tag=32: "NAMEijkl" Clé de message : tag=1: "svr1.exemple.com" Attributs de fonctionnement : tag=1: "svr1.exemple.com" tag=2: "iSCSI" tag=16: 192.20.3.1 tag=17: 5001 tag=19: 5 tag=20: 5002 tag=32: "NAMEijkl" tag=33: "initiateur" tag=34: "Server1" tag=51: 11 tag=49: 192.20.3.1 tag=50: 5001	/********* Appareil dans aucun DD ; il est donc inaccessible aux autres appareils **********/	
	<--DevAttrRegRsp SUCCÈS Clé de message : tag=1: "svr1.exemple.com" Attributs de fonctionnement : tag=1: "svr1.exemple.com" tag=2: "iSCSI" tag=16: 192.20.3.1 tag=17: 5001 tag=19: 5 tag=20: 5002 tag=32: "NAMEijkl" tag=33: "initiateur" tag=34: "Server1" tag=48: "NAMEijkl" tag=49: 192.20.3.1 tag=50: 5001 tag=51: 11	
	SCN------> (ou notification SNMP) dest:(tag=32)"mgmt.exemple.com" time:(tag=4): <heure courante>	

```
                        tag=35: "MGT-SCN, OBJ-ADD"
                        tag=32: "NAMEijkl"
                                                              <------SCNRsp SUCCÈS
                                                              tag=32:"mgmt.exemple.com"
SCNReg-->
Source :
tag=32: "NAMEijkl"
Clé de message :
tag=32: "NAMEijkl"
Attributs de fonctionnement :
tag=35: <TARG&SELF,
OBJ-RMV/ADD/UPD>
                        <--SCNRegRsp SUCCÈS
                                                              <----DevAttrQry
                                                              Source :
                                                              tag=32:"mgmt.exemple.com"
                                                              Clé de message :
                                                              tag=32: "NAMEijkl"
                                                              Attributs de fonctionnement :
                                                              tag=16: <longueur 0>
                                                              tag=17: <longueur 0>
                                                              tag=32: <longueur 0>
                              DevAttrQryRsp---> SUCCÈS
                        Clé de message :
                        tag=32: "NAMEijkl"
                        Attributs de fonctionnement :
                        tag=16:192.20.3.1
                        tag=17: 5001
                        tag=32:"NAMEijkl"                     /***********************************
                                                              La station de gestion affiche l'appareil,
                                                              l'opérateur décide de placer "NAMEijkl"
                                                              dans le domaine préexistant "DDxyz" avec
                                                              l'appareil NAMEabcd
                                                              ***********************************/
                                                              <--DDReg
                                                              Source :
                                                              tag=32:"mgmt.exemple.com"
                                                              Clé de message :
                                                              tag=2065: 123
                                                              Attributs de fonctionnement :
                                                              tag=2068: "NAMEijkl"
                                 DDRegRsp----> SUCCÈS
                        Clé de message :
                        tag=2065: 123
                        Attributs de fonctionnement :
                        tag=2065: 123                         /***********************************
                                                              "NAMEijkl" a été déplace à "DDxyz"
                                                              ************************************/
                                          SCN------>
                        dest:(tag=32)"mgmt.exemple.com"
                        time:(tag=4): <heure actuelle>
                        tag=35: <MGT-SCN, DD/DDS-MBR-ADD>
                        tag=2065: 123
                        tag=2068: "NAMEijkl"
                                                              <------SCNRsp SUCCÈS
                                                              tag=32: "mgmt.exemple.com"
                        <-----SCN
                        dest:(tag=32)"NAMEijkl"
                        time:(tag=4): <heure actuelle>
                        tag=35: <TARG&SELF, OBJ-ADD>
                        tag=32: "NAMEijkl"
SCNRsp------> SUCCÈS
tag=32:"NAMEijkl"
```

```
                                /*******************************
                                Noter que NAMEabcd reçoit aussi une SCN
                                que NAMEijkl est dans le même DD
                                *******************************/
            (à "NAMEabcd")<-----SCN
                                dest:(tag=32)"NAMEabcd"
                                time:(tag=4): <heure actuelle>
                                tag=35: <INIT&SELF, OBJ-ADD>
                                tag=32: "NAMEijkl"
SCNRsp------> SUCCÈS
tag=32:"NAMEabcd"

        DevAttrQry----------->
Source :
tag=32: "NAMEijkl"
Clé de message :
tag=33: "Cible"
Attributs de fonctionnement :
tag=16: <longueur 0>
tag=17: <longueur 0>
tag=32: <longueur 0>
tag=34: <longueur 0>
tag=43: <longueur 0>
tag=48: <longueur 0>
tag=49: <longueur 0>
tag=50: <longueur 0>
tag=51: <longueur 0>
                                <--DevAttrQryRsp SUCCÈS
                                Clé de message :
                                tag=33:"Cible"
                                Attributs de fonctionnement :
                                tag=16: 192.0.2.4
                                tag=17: 5001
                                tag=32: "NAMEabcd"
                                tag=34: "Storage Array 1"
                                tag=16: 192.0.2.5
                                tag=17: 5001
                                tag=32: "NAMEabcd"
                                tag=34: "Storage Array 1"
                                tag=43: X.509 cert
                                tag=48: "NAMEabcd"
                                tag=49: 192.0.2.4
                                tag=50: 5001
                                tag=51: 10
                                tag=48: "NAMEabcd"
                                tag=49: 192.0.2.5
                                tag=50: 5001
                                tag=51: 10
```

/***L'initiateur a découvert la cible, et a tout ce qui est nécessaire pour achever l'établissement iSCSI. Le même processus se produit côté cible ; la SCN invite la cible à télécharger la liste des initiateurs autorisés de iSNS (c'est-à-dire, ceux qui sont dans le même DD que la cible).**********/

Remerciements

De nombreuses personnes ont contribué à la création de ce document grâce à leur relecture attentive et leurs soumissions de commentaires et recommandations. Nous remercions les personnes suivantes de leurs contributions techniques au présent document : Mark Bakke (Cisco), John Hufferd (IBM), Julian Satran (IBM), Kaladhar Voruganti(IBM), Joe Czap (IBM), John Dowdy (IBM), Tom McSweeney (IBM), Jim Hafner (IBM), Chad Gregory (Intel), Yaron Klein (Sanrad), Larry Lamers (Adaptec), Jack Harwood (EMC), David Black (EMC), David Robinson (Sun), Alan Warwick (Microsoft), Bob Snead (Microsoft), Fa Yoeu (Intransa), Joe White (McDATA), Charles Monia (McDATA), Larry Hofer (McDATA), Ken Hirata (Vixel), Howard Hall (Pirus), Malikarjun Chadalapaka (HP), Marjorie Krueger (HP), Siva Vaddepuri (McDATA), et Vinai Singh (American Megatrends).

Adresse des auteurs

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

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

Franco Travostino
Nortel
600 Technology Park Drive
Billerica, MA 01821 USA
téléphone : (978) 288-7708
mél : travos@nortel.com

Curt du Laney
Rincon Research Corporation
101 North Wilmot Road, Suite 101
Tucson AZ 85711
téléphone : (520) 519-4409
mél : cdl@rincon.com

Joe Souza
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399
téléphone : (425) 706-3135
mél : joes@exmsft.com

Déclaration complète de droits de reproduction

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