Groupe de travail Réseau
Request for Comments : 2608
RFC mise à jour : 2165
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

E. Guttman
C. Perkins, Sun Microsystems
J. Veizades, @Home Network
M. Day, Vinca Corporation
juin 1999

Protocole de localisation de service, version 2

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

Résumé
Le protocole de localisation de service donne un cadre adaptable pour la découverte et le choix de services réseau. L'utilisation de ce protocole par les ordinateurs qui se servent de l'Internet ne nécessite que peu ou pas du tout de configuration statique des services réseau pour les applications fondées sur le réseau. Cela est particulièrement important alors que les ordinateurs deviennent de plus en plus portables, et que les utilisateurs sont moins tolérants ou moins capables de satisfaire aux demandes de l'administration du système réseau.

Table des matières

1. Introduction

Le protocole de localisation de service (SLP, *Service Location Protocol*) fournit un cadre souple et adaptable pour donner aux hôtes l'accès aux informations sur l'existence, la localisation, et la configuration des services réseau. Traditionnellement, les usagers ont eu à trouver les services en connaissant le nom d'un hôte réseau (une chaîne textuelle lisible par l'homme) qui est un alias pour une adresse réseau. SLP élimine le besoin qu'un usager connaisse le nom d'un hôte réseau qui prend en charge un service. L'usager fournit plutôt le type de service désiré et un ensemble d'attributs qui décrivent le service. Sur la base de cette description, le protocole de localisation de service résout l'adresse réseau du service pour l'usager.

SLP fournit un mécanisme de configuration dynamique pour les applications dans les réseaux de zone locale. Les applications sont modélisées comme des clients qui ont besoin de trouver les serveurs rattachés à un des réseaux disponibles au sein d'une entreprise. Pour les cas où il y a de nombreux clients et/ou services disponibles différents, le protocole est adapté à faire usage d'agents de répertoire du voisinage qui offrent un répertoire centralisé des services annoncés.

Le présent document met à jour SLPv1 [RFC2165] ; il corrige les erreurs du protocole, ajoute quelques améliorations et supprime certaines exigences. La présente spécification comporte deux parties. La première décrit les caractéristiques exigées du protocole. La seconde décrit les caractéristiques étendues du protocole qui sont facultatives, et permettent une plus grande capacité d'adaptation.

1.1 Déclaration d'applicabilité

SLP est destiné à fonctionner au sein de réseaux sous contrôle administratif coopératif. De tels réseaux permettent de mettre en œuvre une politique concernant la sécurité, l'acheminement de diffusion groupée et l'organisation de services et des clients en groupes qui ne sont pas réalisables à l'échelle de l'Internet global.

SLP a été conçu pour servir les réseaux d'entreprise qui partagent des services, et il peut ne pas nécessairement convenir pour la découverte de service sur de larges zones à l'échelle de l'Internet mondial, ou dans des réseaux où il y a des centaines de milliers de clients ou des dizaines de milliers de services.

2. Terminologie

Agent d'utilisateur (UA, *User Agent*)
Un processus qui fonctionne au nom de l'utilisateur pour établir le contact avec un service. L'UA restitue les informations de service à partir des agents de service ou des agents de répertoire.

Agent de service (SA, *Service Agent*)
Un processus qui fonctionne au nom d'un ou plusieurs services pour annoncer les services.

Agent de répertoire (DA, *Directory Agent*)
Un processus qui collecte les annonces de service. Il ne peut y avoir qu'un seul DA présent par hôte.

Type de service
Chaque type de service a une chaîne unique de type de service.

Autorité de dénomination
C'est l'agence ou groupe qui catalogue les types de service et les attributs. L'autorité de dénomination par défaut est l'IANA.

Portée *(Scope)*
Un ensemble de services, constituant normalement un groupe administratif logique.

URL
Localisateur de ressource universel [RFC2396].

2.1 Conventions de notation

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans la [RFC2119].

Syntaxe
La syntaxe pour les chaînes fondées sur le protocole suit les conventions définies pour l'ABNF [RFC2234].

Chaînes
Toutes les chaînes sont codées en utilisant la transformation UTF-8 [RFC2279] du jeu de caractères Unicode [Unicode] et NE SONT PAS terminées par nul lorsque elles sont transmises. Les chaînes sont précédées par un champ Longueur de deux octets.

<liste-de-chaînes>
Liste des chaînes, délimitées par des virgules, avec la syntaxe suivante :

liste-de-chaînes = chaîne / chaîne `,' liste-de-chaînes

Dans les diagrammes de format, tout champ qui se termine par une barre oblique inverse "\" indique un champ de longueur variable, donnée par un champ Longueur antérieur dans le protocole.

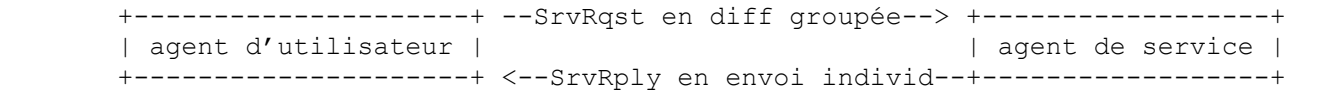
3. Vue d'ensemble du protocole

Le protocole de localisation de service prend en charge un cadre par lequel les applications client sont modélisées comme "Agents d'utilisateur" et les services sont annoncés par les "Agents de service". Une troisième entité, appelée un "Agent de répertoire" fournit la capacité d'adaptation au protocole.

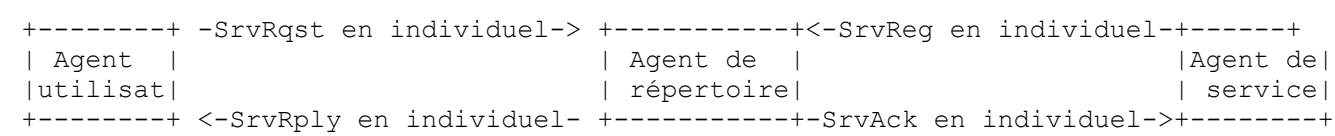
L'agent d'utilisateur produit une "Demande de service" (SrvRqst) au nom de l'application client, spécifiant les caractéristiques du service que demande le client. L'agent d'utilisateur va recevoir une réponse de service (SrvRply) spécifiant la localisation de tous les services dans le réseau qui satisfont la demande.

Le cadre du protocole de localisation de service permet à l'agent d'utilisateur de produire directement les demandes aux agents de service. Dans ce cas, la demande est en diffusion groupée. Les agents de service qui reçoivent une demande pour

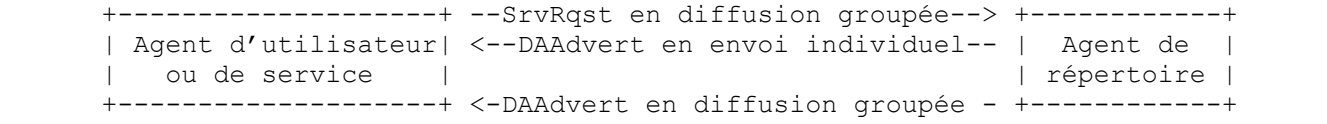
un service qu'ils annoncent envoient une réponse en individuel qui contient la localisation du service.



Dans de plus grands réseaux, on utilise un ou plusieurs agents de répertoire. L'agent de répertoire fonctionne comme une antémémoire. Les agents de service envoient des messages de registre (SrvReg) qui contiennent tous les services qu'ils annoncent aux agents de répertoire et reçoivent des accusés de réception en réponse (SrvAck). Ces annonces doivent être rafraîchies chez les agents de répertoire sinon elles se périment. Les agents d'utilisateur envoient en individuel les demandes aux agents de répertoire au lieu des agents de service si un ou des agents de répertoire sont connus.

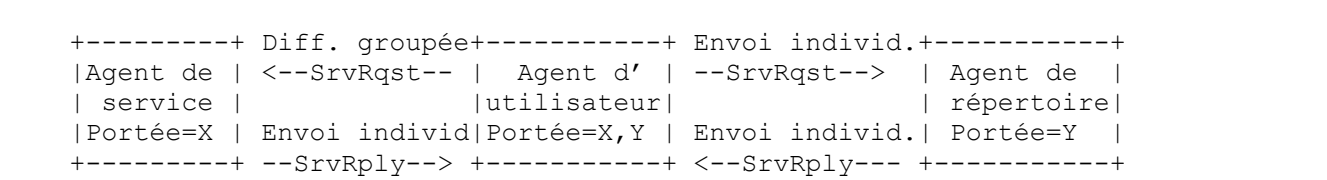


Agents d'utilisateur et de service découvrent de deux façons les agents de répertoire. D'abord, ils produisent une demande de service en diffusion groupée pour le service "agent de répertoire" lorsque ils démarrent. Ensuite, l'agent de répertoire envoie de temps en temps une annonce non sollicitée, pour laquelle les agents d'utilisateur et de service sont à l'écoute. Dans l'un et l'autre cas, les agents reçoivent une annonce de DA (DAAdvert).



Les services sont groupés en utilisant des "portées". Ce sont des chaînes qui identifient les services qui sont identifiés administrativement. Une portée peut indiquer une localisation, un groupement administratif, la proximité dans une topologie de réseau ou quelque autre catégorie. Les agents de service et les agents de répertoire reçoivent toujours une chaîne de portée.

Un agent d'utilisateur reçoit normalement une chaîne de portée (auquel cas l'agent d'utilisateur sera seulement capable de découvrir ce groupement de services particulier). Cela permet à un administrateur de réseau de "provisionner" les services aux usagers. Autrement, l'agent d'utilisateur peut n'être configuré avec aucune portée du tout. Dans ce cas, il va découvrir toutes les portées disponibles et permettre à l'application client de produire des demandes pour tout service disponible sur le réseau.



Dans l'illustration ci-dessus, l'agent d'utilisateur est configuré avec les portées X et Y. Si on recherche un service dans la portée X, la demande est en diffusion groupée. Si elle est recherchée dans la portée Y, la demande est en envoi individuel au DA. Finalement, si la demande doit être faite dans les deux portées, elle doit être à la fois en envoi individuel et en diffusion groupée.

Les agents de service et les agents d'utilisateur peuvent vérifier les signatures numériques fournies avec les DAAdvert. Les agents d'utilisateur et les agents de répertoire peuvent vérifier les informations de service enregistrées par les agents de service. Le matériel de clé à utiliser pour vérifier les signatures numériques est identifié en utilisant un indice de paramètre de sécurité SLP (SLP SPI, *SLP Security Parameter Index*).

Chaque hôte configuré pour générer une signature numérique comporte le SLP SPI utilisé pour la vérifier dans le bloc d'authentification qu'il transmet. Chaque hôte qui peut vérifier une signature numérique doit être configuré avec le matériel de clé et les autres paramètres correspondant au SLP SPI afin qu'il puisse effectuer les calculs de vérification.

Les SA DOIVENT accepter les demandes de service en diffusion groupée et les demandes de service en envoi individuel. Les SA PEUVENT accepter d'autres demandes (demandes d'attribut et de type de service). Les SA DOIVENT être à l'écoute des annonces de DA en diffusion groupée.

Les caractéristiques décrites jusqu'à présent sont de mise en œuvre obligatoire. Une mise en œuvre minimum consiste en

un agent d'utilisateur, un agent de service ou les deux.

Il y a plusieurs caractéristiques facultatives dans le protocole. Noter que les DA DOIVENT prendre en charge tous ces types de message, mais la prise en charge de l'agent de répertoire lui-même est de déploiement facultatif dans les réseaux qui utilisent SLP. Les UA et les SA PEUVENT prendre en charge trois types de message. Ces opérations sont principalement pour une utilisation interactive (en feuilletant ou en mettant à jour de façon sélective les enregistrements de service). Les UA et les SA les prennent ou non en charge selon les exigences et contraintes de l'environnement où ils seront utilisés.

Demande de type de service
C'est une demande pour tous les types de service sur le réseau. Cela permet de construire des feuilleteurs de service génériques.

Réponse de type de service
C'est une réponse à une demande de type de service.

Demande d'attribut
C'est une demande pour des attributs d'un certain type de service ou des attributs d'un certain service.

Réponse d'attribut
C'est une réponse à une demande d'attribut.

Désenregistrement de service
C'est une demande de désenregistrer un service ou des attributs d'un service.

Mise à jour de service
C'est une SrvRqst postérieure à une annonce. Cela permet une mise à jour dynamique d'attributs individuels.

Annonce de SA
En l'absence d'agents de répertoire, un agent d'utilisateur peut demander aux agents de service de découvrir leur configuration de portée. L'agent d'utilisateur peut utiliser ces portées dans les demandes.

En l'absence de prise en charge de la diffusion groupée, la diffusion PEUT être utilisée. La localisation des DA peut être statiquement configurée, découverte en utilisant SLP comme décrit ci-dessus, ou configurée en utilisant DHCP. Si un message est trop grand, il peut être en envoi individuel en utilisant TCP.

Une mise en œuvre SLPv2 DEVRAIT prendre en charge SLPv1 [RFC2165]. Cette prise en charge inclut :

1. Les DA SLPv2 sont déployés, supprimant graduellement les DA SLPv1.

2. Les demandes SLPv1 sans portée sont considérées comme étant de portée par DEFAUT. Les UA SLPv1 DOIVENT être reconfigurés pour avoir une portée, si possible.

3. Il n'y a aucun moyen pour un DA SLPv2 de se comporter comme un DA SLPv1 sans portée. Les SA SLPv1 DOIVENT être reconfigurés pour avoir une portée, si possible.

4. Les DA SLPv2 répondent aux demandes SLPv1 avec des réponses SLPv1 et aux demandes SLPv2 avec des réponses SLPv2.

5. Les DA SLPv2 utilisent de la même façon les enregistrements provenant de SLPv1 et de SLPv2. C'est-à-dire que les demandes entrantes provenant d'agents qui utilisent l'une ou l'autre version du protocole seront confrontées à l'ensemble commun de services enregistrés.

6. Les enregistrements SLPv2 qui utilisent des étiquettes de langage qui font plus de deux caractères seront inaccessibles aux UA SLPv1.

7. Les DA SLPv2 DOIVENT retourner seulement des chaînes de type de service dans les messages SrvTypeRply qui se conforment à la syntaxe de type de service SLPv1, c'est-à-dire qu'ils NE DOIVENT PAS retourner des chaînes de type de service pour des types de service abstraits.

8. Les SrvRqst et AttrRqst SLPv1 par type de service ne correspondent pas aux URL Service avec des types de service abstraits. Ils ne correspondent qu'aux URL Service avec des types de service concrets.

Les UA SLPv1 ne vont pas recevoir de réponses provenant des SA SLPv2 et les UA SLPv2 ne vont pas recevoir de réponses des SA SLPv1. Afin de faire interopérer les UA et SA de différentes versions, il faut que soit présent un DA SLPv2 sur le réseau qui prend en charge les deux protocoles.

L'utilisation de types de service abstrait dans SLPv2 pose un problème de rétro compatibilité pour SLPv1. Il est possible qu'un UA SLPv1 demande un type de service qui soit en fait un type de service abstrait. Sur la base de la règle ci-dessus, l'UA SLPv1 ne va jamais recevoir une réponse d'URL Service abstrait. Par exemple, le type de service "service:x" dans une AttrRqst SLPv1 ne va pas retourner les attributs de "service:x:y://orb". Si la demande était faite avec SLPv2, il retournerait les attributs de ce service.

4. URL utilisés avec la localisation de service

Un URL Service indique la localisation d'un service. Cet URL peut être du schéma service: [RFC2609] (repris au paragraphe 4.1) ou tout autre schéma d'URL qui se conforme à l'URI standard [RFC2396], excepté que les URL sans d'adresse NE DEVRAIENT PAS être annoncés par SLP. Le type de service pou un URL "générique" est son nom de schéma. Par exemple, la chaîne type de service pour "http://www.srvloc.org" serait "http".

Les caractères réservés dans les URL suivent les règles de la [RFC2396].

4.1 URL Service:

La syntaxe et la sémantique de l'URL Service sont définies dans la [RFC2609]. Tout service réseau peut être codé dans un URL Service.

Ce paragraphe donne une introduction aux URL Service et un exemple qui en montre une application simple, représentant des services réseau standard.

Un URL Service peut être de la forme : "service:"<srvtype>"://"<adrspec>

Le type de service (srvtype) de cet URL service: est défini comme étant la chaîne jusqu'au (mais sans l'inclure) ":" final avant <adrspec>, la spécification d'adresse.

<adrspec> est un nom d'hôte (qui devrait être utilisé si possible) ou une notation en décimal séparé par des points pour un nom d'hôte, suivi par un ":" facultatif et le numéro d'accès.

Un URL de schéma service: peut être formé avec tout nom de protocole standard en enchaînant "service:" et le nom d'accès réservé [IANA]. Par exemple, "service:tftp://myhost" indiquerait un service tftp. Un service tftp sur un accès non standard pourrait être : "service:tftp://bad.glad.org:8080".

Les types de service DEVRAIENT être définis par un "gabarit de service" [RFC2609], qui fournit les attributs, valeurs et comportement de protocole attendus. Un type de service abstrait (aussi décrit dans la [RFC2609]) a la forme : "service:<type-abstrait>:<type-concret>".

La chaîne de type de service "service:<type-abstrait>" correspond à tous les services de ce type abstrait. Si le type concret est aussi inclus, seuls ces services satisfont la demande. Par exemple, une SrvRqst ou AttrRqst qui spécifie "service:printer" comme type de service va correspondre aux URL service:printer:lpr://hostname et service:printer:http://hostname. Si la demande spécifiait "service:printer:http" elle ne va correspondre qu'au dernier URL.

Une sous-chaîne facultative PEUT suivre le dernier caractère "." dans le <srvtype> (ou <abstract-type> dans le cas d'un URL de type de service abstrait). Cette sous-chaîne est l'autorité de dénomination, comme décrit au paragraphe 9.6. Les types de service avec des autorité de dénomination différentes sont assez distincts. En d'autres termes, service:x.un et service:x.deux sont des types de service différents, comme le sont service:abstrait.un:y et service:abstrait.deux:y.

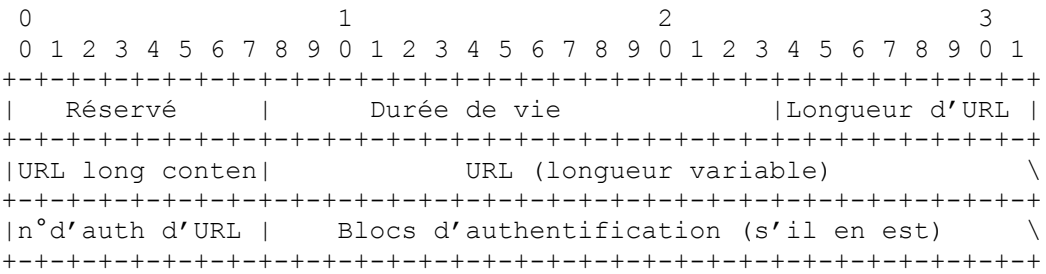
4.2 Autorités de dénomination

Une autorité de dénomination PEUT être facultativement incluse au titre de la chaîne de type de service. L'autorité de dénomination d'un service définit la signification des types et attributs de service enregistrés et fournis avec la localisation du service. L'autorité de dénomination elle-même est normalement une chaîne qui identifie de façon univoque une

organisation. L'IANA est l'autorité de dénomination implicite lorsque aucune chaîne n'est donnée. "IANA" NE DOIT PAS être elle-même incluse explicitement.

Les autorités de dénomination peuvent définir des types de service expérimentaux, propriétaires, ou pour utilisation privée. En utilisant une autorité de dénomination, on peut simplement ignorer des attributs lors de l'enregistrement ou créer un ensemble d'attributs pour utilisation seulement locale pour son site. La procédure à utiliser est de créer une chaîne Autorité de dénomination 'unique' puis de spécifier les définitions d'attribut standard comme décrit ci-dessus. Cette autorité de dénomination va accompagner l'enregistrement et les interrogations, comme décrit aux paragraphes 8.1 et 8.3. Les types de service DEVRAIENT être enregistrés auprès de l'IANA pour permettre l'interopérabilité à l'échelle de l'Internet.

4.3 Entrées d'URL



SLP mémorise les URL dans des éléments de protocole appelés Entrées d'URL, qui associent une longueur, une durée de vie, et éventuellement des informations d'authentification avec l'URL. Les entrées d'URL, définies comme indiqué ci-dessus, sont utilisées dans les réponses de service et les enregistrements de service.

5. Attributs de service

Une annonce de service est souvent accompagnée par des attributs de service. Ces attributs sont utilisés par les UA dans les demandes de service pour choisir les services appropriés.

Les attributs admissibles qui peuvent être utilisés sont normalement spécifiés par un gabarit de service [RFC2609] pour un type de service particulier. Les services qui sont annoncés conformément à un gabarit standard DOIVENT enregistrer tous les attributs de service qu'exige le gabarit standard. Les URL qui ont des schémas autres que "service:" PEUVENT être enregistrés avec des attributs.

Les noms d'attributs non standard DEVRAIENT commencer par "x-", parce que aucun nom d'attribut standard ne va jamais avoir ces caractères initiaux.

Une liste d'attributs est une chaîne codée des attributs d'un service. La grammaire ABNF [RFC2234] suivante définit les listes d'attribut :

```
attr-list = attribut / attribut ',' attr-list
attribut = '(' attr-tag '=' attr-val-list ')' / attr-tag
attr-val-list = attr-val / attr-val ',' attr-val-list
attr-tag = 1*safe-tag
attr-val = intval / strval / boolval / opaque
intval = [-]1*DIGIT
strval = 1*safe-val
boolval = "vrai" / "faux"
opaque = "\FF" 1*escape-val
safe-val =                    ; tout caractère sauf réservé.
safe-tag =                    ; tout caractère sauf réservé, étoile et bad-tag.
réservé = '(' / ')' / ',' / '\' / '!'  / '<' / '=' / '>' / '~' / CTL
escape-val = '\' HEXDIG HEXDIG
bad-tag = CR / LF / HTAB / '_'
étoile = '*'
```

La <attr-list>, si elle est présente, DOIT être examinée avant l'évaluation de toutes occurrences du caractère d'échappement '\'. Les caractères réservés DOIVENT être esquivés (les autres caractères NE DOIVENT PAS être

esquivés). Tous les caractères esquivés doivent être restaurés à leur valeur avant de tenter les correspondances de chaînes. Pour les valeurs opaques, les caractères esquivés ne sont pas convertis – ils sont interprétés comme octets.

Booléen C'est une chaîne qui a la forme "vrai" ou "faux", ne peut prendre qu'une seule valeur et ne peut être comparée qu'avec '='. Les booléens sont insensibles à la casse dans la comparaison.

Entier Les chaînes qui prennent la forme [-] 1*<chiffre> et sont dans la gamme "-2147483648" à "2147483647" sont considérées comme des entiers. Elles sont comparées en utilisant la comparaison d'entiers.

Chaîne Toutes les autres chaînes sont confrontées en utilisant l'ordre lexical strict (voir au paragraphe 6.4).

Opaque Les valeurs opaques sont des séquences d'octets. Elles se distinguent des chaînes en ce qu'elles commencent par la séquence "\FF". Ceci, sans échappement, est un codage UTF-8 illégal, qui indique que ce qui va suivre est une séquence d'octets exprimés en notation échappée qui constituent la valeur binaire. Par exemple, un octet '0' est codé "\FF\00".

Une chaîne qui contient des valeurs esquivées autres que de l'ensemble de caractères réservés est illégale. Si une telle chaîne est incluse dans une <attr-list>, <tag-list> ou filtre de recherche, le SA ou DA qui le reçoit DOIT retourner une PARSE_ERROR au message.

Un mot clé a seulement une <attr-tag> *(étiquette d'attribut)*, et pas de valeur. Les attributs peuvent avoir une ou plusieurs valeurs. Toutes les valeurs sont exprimées comme des chaînes.

Lorsque des valeurs ont été annoncées par un SA ou sont enregistrées dans un DA, elles peuvent suivre des règles de frappe implicites pour satisfaire des demandes entrantes.

Les valeurs mémorisées doivent être cohérentes, c'est-à-dire que x=4,vrai,sue,\ff\00\00 n'est pas permis. Un DA ou SA qui reçoit une telle <attr-list> DOIT retourner une erreur INVALID_REGISTRATION.

6. Caractéristiques exigées

Cette section définit les exigences minimales de mise en œuvre pour les SA et UA ainsi que leur interaction avec les DA. Un DA n'est pas obligé de fonctionner par SLP, mais si il est présent, les UA et SA DOIVENT interagir avec lui de la façon définie ci-dessous.

Une mise en œuvre minimale peut comporter soit un UA, soit un SA, soit les deux. La seule caractéristique exigée d'un UA est qu'il puisse produire des SrvRqst conformément aux règles qui figurent ci-dessous et interpréter les messages DAAdvert, SAAdvert et SrvRply. Le UA DOIT produire des demandes aux DA lorsque ils sont découverts. Un SA DOIT répondre aux SrvRqst appropriées avec des messages SrvRply ou SAAdvert. Le SA DOIT aussi s'enregistrer auprès des DA lorsque ils sont découverts.

Les UA effectuent la découverte en produisant des messages Demande de service. Les messages SrvRqst sont produits en utilisant UDP, selon les règles de priorité suivantes :

1. Un UA produit une demande à un DA pour lequel il a été configuré avec DHCP.

2. Un UA produit des demandes aux DA pour lesquels il a été configuré de façon statique.

3. Un UA utilise des SrvRqst en diffusion groupée/convergence pour découvrir les DA, puis utilise cet ensemble de DA. Un UA qui ne connaît aucun DA DEVRAIT réessayer la découverte de DA, en augmentant de façon exponentielle l'intervalle d'attente entre les tentatives successives (en doublant l'intervalle d'attente à chaque fois). L'intervalle d'attente minimum recommandé est de CONFIG_DA_FIND secondes.

4. Un UA qui ne connaît aucun DA envoie des demandes en utilisant une convergence en diffusion groupée aux SA. Les SA répondent en envoi individuel aux UA, conformément à l'algorithme de convergence de diffusion groupée.

Les UA et les SA sont configurés avec une liste de portées à utiliser conformément aux règles de priorité suivantes :

1. avec DHCP.

2. Avec une configuration statique. La configuration statique peut être établie explicitement à NO SCOPE pour les UA, si

le modèle "Portée choisie par l'utilisateur" est utilisé. Voir au paragraphe 11.2.

3. En l'absence de configuration, la portée de l'agent est "DEFAUT".

Un UA DOIT produire des demandes avec une ou plusieurs des portées qu'il a été configuré à utiliser.

Un UA qui a été configuré de façon statique avec NO SCOPE LIST va utiliser la découverte de DA ou SA pour déterminer de façon dynamique sa liste de portées. Dans ce cas, il utilise une liste de portées vide pour découvrir les DA et éventuellement les SA. Puis, il utilise la liste de portées qu'il obtient à partir des DAAdvert et des éventuels SAAdvert dans les demandes suivantes.

Le SA DOIT enregistrer tous ses services auprès de tous les DA qu'il découvre, si le DA annonce une des portées avec lesquelles il a été configuré. Un SA obtient les informations sur les DA comme le fait un UA. De plus, le SA DOIT être à l'écoute des DAAdvert non sollicités en diffusion groupée. Le SA s'enregistre en envoyant des messages SrvReg aux DA, qui répondent avec des messages SrvReg pour indiquer le succès. Les SA s'enregistrent dans TOUTES les portées qu'ils ont été configurés à utiliser.

6.1 Utilisation des accès, de UDP, et de la diffusion groupée

Les DA DOIVENT accepter les demandes en envoi individuel et les demandes de découverte d'agent de répertoire en diffusion groupée (pour le type de service "service:directory-agent").

Les SA DOIVENT accepter aussi bien les demandes en diffusion groupée que celles en envoi individuel. Le SA peut les distinguer grâce au fanion REQUEST MCAST *(demande en diffusion groupée)* qui est établi ou non dans l'en-tête de message SLP.

Le protocole de localisation de service utilise la diffusion groupée pour découvrir les DA et pour produire des demandes aux SA par défaut.

L'accès d'écoute réservé pour SLP est 427. C'est l'accès de destination pour tous les messages SLP. Les messages SLP PEUVENT être transmis sur un accès éphémère. Les réponses et accusés de réception sont envoyés à l'accès d'où la demande a été envoyée. L'unité maximum de transmission par défaut pour les messages UDP est de 1400 octets en excluant UDP et les autres en-têtes.

Si un message SLP ne tient pas dans un datagramme UDP, il DOIT être tronqué pour tenir, et le fanion Débordement est établi dans le message de réponse. Un UA qui reçoit un message tronqué PEUT ouvrir une connexion TCP (voir au paragraphe 6.2) avec le DA ou le SA et retransmettre la demande, en utilisant le même XID. Il PEUT aussi tenter d'utiliser la réponse tronquée ou reformuler une demande plus restrictive qui va résulter en une réponse plus courte.

Les messages de demande SLP sont en diffusion groupée à l'adresse Diffusion groupée SLP à portée administrative [RFC2365], qui est 239.255.255.253. Le TTL par défaut à utiliser pour la diffusion groupée est 255.

Dans les réseaux isolés, la diffusion va fonctionner à la place de la diffusion groupée. À cette fin, les SA DEVRAIENT et les DA DOIVENT être à l'écoute des messages de localisation de service en diffusion sur l'accès 427. Cela permet aux UA qui ne prennent pas en charge la diffusion groupée d'utiliser la localisation de service sur des réseaux isolés.

Régler le TTL de diffusion groupée à moins de 255 (la valeur par défaut) limite la gamme de découverte SLP dans un réseau, et localise les informations de service dans le réseau.

6.2 Utilisation de TCP

Un SrvReg ou SrvDeReg peut être trop grand pour tenir dans un datagramme. Pour envoyer de tels grands messages SLP, une connexion TCP (en envoi individuel) DOIT être établie.

Pour éviter d'avoir besoin de mettre TCP en œuvre, on DOIT s'assurer que :

- Les UA ne produisent jamais de demande supérieure à la MTU du chemin. Les SA ne peuvent omettre la prise en charge de TCP que si il n'ont jamais à recevoir de demande en envoi individuel supérieure à la PMTU.

- Les UA peuvent accepter les réponses qui ont le fanion "DEBORDEMENT" établi, et faire usage du premier résultat

inclus, ou reformuler la demande.

- Un SA peut envoyer une SrvRply, un SrvReg, ou SrvDeReg dans un seul datagramme. Cela signifie de limiter la taille des URL, le nombre des attributs et le nombre des authentifiants transmis.

Les DA DOIVENT être capables de répondre aux demandes UDP et TCP, ainsi qu'aux SrvRqst de découverte de DA en diffusion groupée. Les SA DOIVENT être capables de répondre à TCP sauf si le SA ne va JAMAIS recevoir de demande ou envoyer de réponse qui excéderait la taille d'un datagramme (par exemple, comme certains systèmes incorporés).

Une connexion TCP PEUT être utilisée pour une seule transaction SLP, ou pour plusieurs transactions. Comme il y a des champs de longueur dans les en-têtes de message, les agents SLP peuvent envoyer plusieurs demandes sur une connexion et lire le flux de retour pour les accusés de réception et les réponses.

L'agent initiateur DEVRAIT fermer la connexion TCP. Le DA DEVRAIT attendre au moins CONFIG_CLOSE_CONN secondes avant de clore une connexion inactive. Les DA et SA DEVRAIENT clore une connexion TCP inactive après CONFIG_CLOSE_CONN secondes pour s'assurer d'un fonctionnement robuste, même lorsque l'agent initiateur néglige de la clore. Voir à la Section 13 les règles de temporisation.

6.3 Retransmission des messages SLP

Les demandes qui échouent à provoquer une réponse sont retransmises. La retransmission initiale survient après une période d'attente de CONFIG_RETRY. Les retransmissions DOIVENT être faites avec une augmentation exponentielle des intervalles d'attente (doublant l'attente à chaque fois). Cela s'applique aux demandes SLP aussi bien en envoi individuel qu'en diffusion groupée.

Les demandes en envoi individuel à un DA ou SA devraient être retransmises jusqu'à ce qu'une réponse (qui peut être une erreur) ait été obtenue, ou que CONFIG_RETRY_MAX secondes se soient écoulées.

Les demandes en diffusion groupée DEVRAIENT être reproduites pendant CONFIG_MC_MAX secondes jusqu'à ce qu'un résultat ait été obtenu. Les UA ont seulement besoin d'attendre jusqu'à la première réponse qui correspond à leur demande. C'est-à-dire que la retransmission n'est pas exigée si l'agent demandeur est prêt à utiliser la "première réponse" au lieu de "autant de réponses que possible pendant un intervalle de temps limité".

Lorsque des messages SLP SrvRqst, SrvTypeRqst, et AttrRqst sont en diffusion groupée, ils contiennent une <PRList> des sources des réponses précédentes. Au départ, la <PRList> est vide. Lorsque ces demandes sont en envoi individuel, la <PRList> est toujours vide.

Un DA ou SA qui voit son adresse dans la <PRList> NE DOIT PAS répondre à la demande.

Le message DEVRAIT être retransmis jusqu'à ce que la <PRList> ne cause plus d'autre réponse ou que la précédente liste de réponses et la demande ne tienne pas dans un seul datagramme ou jusqu'à ce que CONFIG_MC_MAX secondes s'écoulent.

Les UA qui retransmettent une demande utilisent le même XID. Cela permet à un DA ou SA de mettre en antémémoire sa réponse à la demande d'origine puis de l'envoyer à nouveau, si un duplicata de la demande devait arriver. Ces informations en antémémoire ne devraient être détenues que très brièvement. Les XID DEVRAIENT être choisis au hasard pour éviter des XID dupliqués dans les demandes si les UA redémarrent fréquemment.

6.4 Chaînes dans les messages SLP

Le caractère d'échappement est une barre oblique inverse (UTF-8 0x5c) suivie par deux chiffres en hexadécimal du caractère échappé. Seuls les caractères réservés sont échappés. Par exemple, une virgule (UTF-8 0x29) est esquivée par '\29', et une barre oblique inverse '\' est esquivée par `\5c'. Les listes de chaînes utilisées dans SLP définissent la virgule comme étant le délimiteur entre les éléments d'une liste, de sorte que les virgules dans les chaînes de données doivent être esquivées de cette manière. Les barres obliques inverses sont le caractère d'échappement de sorte qu'ils doivent aussi toujours être esquivés lorsqu'ils sont inclus littéralement dans une chaîne.

La comparaison d'ordre et d'égalité de chaînes dans SLP DOIT être insensible à la casse à l'intérieur de la sous gamme de 0x00 à 0x7F de UTF-8 (qui correspond au codage de caractères ASCII). L'insensibilité à la casse DEVRAIT être prise en charge sur la totalité du jeu de caractères Unicode [Unicode] codé en UTF-8.

La règle de l'insensibilité à la casse s'applique à toutes les correspondances de chaîne dans SLPv2, y compris les chaînes

Scope, les chaînes SLP SPI, de type de service, d'étiquettes et valeurs d'attribut dans le traitement des interrogations, des étiquettes de langue, et des liste de réponses précédentes. La comparaison des chaînes d'URL est cependant sensible à la casse.

Les espaces (SPACE, CR, LF, TAB) internes à une valeur de chaîne sont repliées sur un seul caractère SPACE pour les besoins de la comparaison de chaînes. Les espaces qui précèdent ou suivent une valeur de chaîne sont ignorées pour les besoins de la comparaison de chaînes. Par exemple, " Some String " équivaut à "SOME STRING".

Les comparaisons de chaîne (en utilisant les opérateurs de comparaison tels que '≤' ou '≥') sont faites en utilisant l'ordre lexical des caractères codés en UTF-8, et non en utilisant des règles spécifiques d'une langue.

Le caractère réservé '*' peut précéder, suivre ou être à l'intérieur d'une valeur de chaîne afin d'indiquer une correspondance de sous-chaîne. L'interrogation qui comporte ce caractère correspond à toute séquence de caractères qui se conforme aux lettres qui ne sont pas représentées par le caractère générique.

6.4.1 Listes de portée dans SLP

Les listes de portée dans SLPv2 ont la grammaire suivante :

```
scope-list = scope-val / scope-val ',' scope-list
scope-val = 1*safe
safe =                          ; tout caractère sauf les réservés.
reserved = '(' / ')' / ',' / '\' / '!'  / '<' / '=' / '>' / '~' / CTL / ';' / '*' / '+'
escape-val = '\' HEXDIG HEXDIG
```

Les portées qui comportent des caractères réservés doivent remplacer le caractère esquivé par le format escaped-val.

7. Erreurs

Si le code d'erreur dans un message de réponse SLP est différent de zéro, le reste du message PEUT être tronqué. Aucune données ne sont nécessairement transmises ni ne devraient être attendues après l'en-tête et le code d'erreur, sauf éventuellement certaines extensions facultatives pour préciser l'erreur, par exemple, comme au paragraphe D.1.

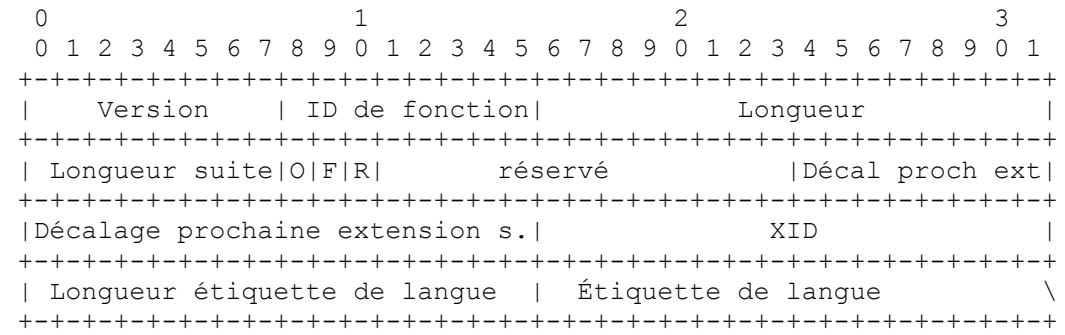
Les erreurs ne sont retournée que pour les demandes en envoi individuel. Les demandes en diffusion groupée sont éliminés en silence si elles résultent en une erreur.

LANGAGE_NON_ACCEPTÉ = 1 : Il y a des données pour le type de service dans la portée de la AttrRqst ou SrvRqst, mais pas dans le langage demandé.
ERREUR_D'ANALYSE = 2 : Le message n'obéit pas à la syntaxe de SLP.
ENREGISTREMENT_INVALIDE = 3 : Le SrvReg pose problème – par exemple, une durée de vie de zéro ou l'omission d'une étiquette de langue.
PORTÉE_NON_ACCEPTÉE = 4 : Le message SLP ne comportait pas de portée dans sa <scope-list> qui soit pris en charge par le SA ou DA.
AUTHENTIFICATION_INCONNUE = 5 : Le DA ou SA reçoit une demande pour un SLP SPI non pris en charge.
AUTHENTIFICATION_ABSENTE = 6 : Le DA attend l'authentification d'URL et d'ATTR dans le SrvReg et ne les a pas reçus.
AUTHENTIFICATION_ÉCHEC = 7 : Le DA a détecté une erreur d'authentification dans un bloc d'authentification.
VERSION_NON_ACCEPTÉE = 9 : Le numéro de version dans un en-tête de message n'est pas accepté.
ERREUR_INTERNE = 10 : Le DA (ou SA) est trop mal en point pour répondre.
DA_OCCUPÉ = 11 : l'UA ou SA DEVRAIT réessayer, en utilisant le retard exponentiel.
OPTION_NON_COMPRISE = 12 : Le DA (ou SA) a reçu une option inconnue de la gamme obligatoire (voir au paragraphe 9.1).
MISE_A_JOUR_INVALIDE = 13 : Le DA a reçu un SrvReg sans FRESH établi, pour un service non enregistré ou avec un type de service non compatible.
MSG_NON_ACCEPTÉ = 14 : Le SA a reçu un AttrRqst ou SrvTypeRqst et ne l'accepte pas.
RAFRAICHISSEMENT_REJETÉ = 15 : Le SA a envoyé un SrvReg ou un SrvDereg partiel à un DA plus fréquemment que l'intervalle min-refresh du DA.

8. Messages SLP exigés

Tous les champs de longueur dans les messages SLP sont dans l'ordre des octets du réseau. Lorsque des tuplets sont définis, ce sont des séquences d'octets, dans l'ordre précis indiqué, dans l'ordre des octets du réseau.

Les messages SLP commencent tous par l'en-tête suivant :



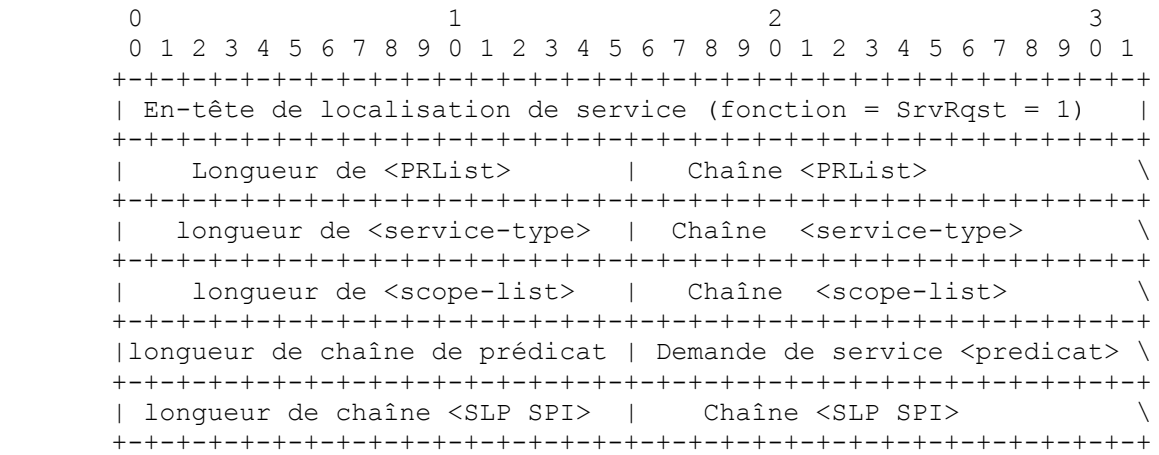
Type de message	Abréviation	Identifiant de fonction
Demande de service	SrvRqst	1
Réponse de service	SrvRply	2
Enregistrement de service	SrvReg	3
Désenregistrement de service	SrvDeReg	4
Accusé de réception de service	SrvAck	5
Demande d'attribut	AttrRqst	6
Réponse d'attribut	AttrRply	7
Annonce de DA	DAAdvert	8
Demande de type de service	SrvTypeRqst	9
Réponse de type de service	SrvTypeRply	10
Annonce de SA	SAAdvert	11

Les SA et les UA DOIVENT prendre en charge les SrvRqst, SrvRply et DAAdvert. Les SA DOIVENT aussi prendre en charge les SrvReg, SAAdvert et SrvAck. Pour les UA et les SA, la prise en charge d'autres messages est FACULTATIVE.

- Longueur est la longueur du message SLP entier, en-tête inclus.
- Les fanions sont : DÉBORDEMENT (0x80) qui est établi si la longueur d'un message dépasse ce qui tient dans un datagramme. FRAIS (0x40) est mis sur tout nouveau SrvReg. DEMANDE EN DIFF (0x20) est mis lors de la diffusion ou diffusion groupée des demandes. Les bits réservés DOIVENT être à 0.
- Décalage de prochaine extension est réglé à 0 sauf si des extensions sont utilisées. La première extension commence à 'offset' octets, à partir du début du message. Il est placé après les données du message SLP. Voir au paragraphe 9.1 comment interpréter les extensions SLP non reconnues.
- XID est réglé à une valeur unique pour chaque demande. Si la demande est retransmise, le même XID est utilisé. Les réponses règlent le XID à la même valeur que le xid de la demande. Seuls les DAAdvert non sollicités sont envoyés avec un XID de 0.
- Longueur d'étiquette de langue est la longueur en octets du champ Étiquette de langue.
- Les étiquettes de langage se conforment à [RFC1766]. L'étiquette de langage dans une réponse DOIT être la même que celle de la demande. Ce champ doit être codé 1*8ALPHA *("-" 1*8ALPHA).

Si une option est spécifiée, et non incluse dans le message, le receveur DOIT répondre avec une ERREUR_D'ANALYSE.

8.1 Demande de service



Pour qu'un service corresponde à une SrvRqst, il doit appartenir au moins à une portée demandée, prendre en charge le type de service demandé, et correspondre au prédicat. Si le prédicat est présent, le langage de la demande (en ignorant la partie dialecte de l'étiquette de langue) doit correspondre au service annoncé.

<PRList> est la liste des répondants précédents. Cette <chaîne-de-listes> contient les adresses IP (v4) en décimal séparé par des points, et est itérativement en diffusion groupée pour obtenir tous les résultats possibles (voir au paragraphe 6.3). Les UA DEVRAIENT mettre en œuvre cet algorithme de découverte. Les SA DOIVENT utiliser cela pour découvrir tous les DA disponibles dans leur portée, si ils ne sont pas déjà configurés par quelque autre moyen avec les adresses des DA.

Un SA abandonne en silence toutes les demandes qui comportent l'adresse du SA dans la <PRList>. Un SA qui a plusieurs interfaces réseau DOIT vérifier si une des entrées dans la <PRList> égale une de ses interfaces. Une entrée dans la PRList qui ne se conforme pas au format d'adresse IPv4 en décimal séparé par des points est ignorée: Le reste de la <PRList> est traité normalement et aucune erreur n'est retournée.

Lorsque une <PRList> plus la demande excède la MTU du chemin, la convergence de diffusion groupée s'arrête. Cet algorithme n'est pas destiné à trouver toutes les instances ; il en trouve "assez" pour donner des résultats utiles.

La <scope-list> est une <liste-de-chaînes> de noms de portée configurées. Les SA et DA qui ont été configurés avec une des portées dans cette liste vont répondre. Les DA et SA DOIVENT répondre aux demandes en envoi individuel avec une erreur PORTÉE_NON_ACCEPTÉE si la <liste-de-portées> est omise ou manque à inclure une portée qu'ils prennent en charge (voir à la Section 11). Les seules exceptions à cela sont décrites au paragraphe 11.2.

La chaîne <service-type> est décrite à la Section 4. Normalement, une SrvRqst entraîne une SrvRply. Il y a deux exceptions: Si le <service-type> est réglé à "service:directory-agent", les DA répondent à la SrvRqst par une DAAdvert (voir au paragraphe 8.5). Si il est réglé à "service:service-agent", les SA répondent par une SAAdvert (voir au paragraphe 8.6). Si ce champ est omis, une ERREUR_D'ANALYSE est retournée – car ce champ est EXIGÉ.

Le <prédicat> est un filtre de recherche LDAPv3 [RFC2254]. Ce champ est FACULTATIF. Les services peuvent être découverts simplement par type et portée. Autrement, les services sont découverts s'ils satisfont au <prédicat>. S'il est présent, il est comparé à chaque service enregistré. Si l'attribut dans le filtre a été enregistrés avec plusieurs valeurs, le filtre est comparé à chaque valeur et les résultats sont traités entre eux par l'opérateur OUX, c'est-à-dire que "(x=3)" correspond à l'enregistrement de (x=1,2,3) ; "(!(Y=0))" correspond à (y=0,1) car Y peut être différent de zéro. Noter que la correspondance est insensible à la casse. Les mots clés (c'est-à-dire, les attributs sans valeurs) sont confrontés à un filtre de "présence", comme dans "(mot-clé=*)".

Un terme de demande entrante DOIT avoir le même type que l'attribut dans un enregistrement afin de correspondre. Donc, "(x=33)" ne va pas correspondre à ' x=vrai', etc. alors que "(y=foo)" va correspondre à 'y=FOO'. "(|(x=33)(y=foo))" sera satisfait, même si "(x=33)" ne peut pas être satisfait, à cause de la '|' (disjonction booléenne).

La correspondance de caractères générique DOIT être faite avec le filtre '='. Dans tout autre cas, une ERREUR_D'ANALYSE est retournée. Les termes d'une demande qui comportent des caractères génériques sont interprétés comme étant des chaînes. C'est-à-dire (x=34*) correspondrait à 'x=34foo', mais pas à 'x=3432' car la première valeur est une chaîne alors que la seconde valeur est un entier ; les chaînes ne correspondent pas à des entiers.

Voici des exemples de prédicats : <t> indique le type de service de la SrvRqst, <s> donne la <scope-list> et <p> est la

chaîne de prédicat.

<t> =service:http <s> =DEFAULT <p> = (chaîne vide)
C'est une chaîne de demande minimale. Elle correspond à tous les services http annoncés avec la portée par défaut.

<t> =service:pop3 <s> =SALES,DEFAULT <p> =(user=wump)
C'est une demande pour tous les services pop3 disponibles dans les portées SALES ou DEFAULT qui desservent la messagerie pour l'usager 'wump'.

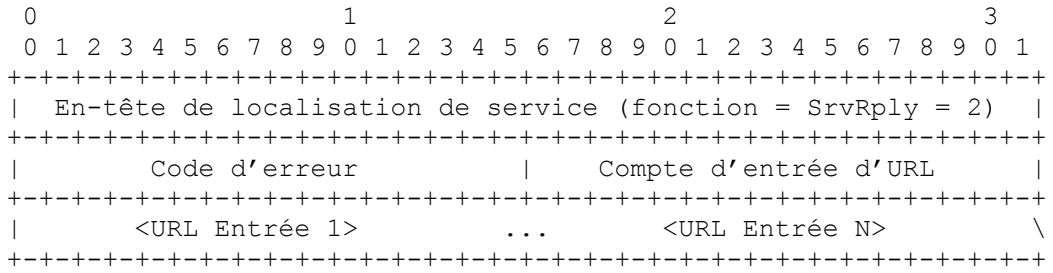
<t> =service:backup <s> =BLDG 32 <p>=(&(q<=3)(speed>=1000))
Ceci retourne le service de sauvegarde qui a une longueur de file d'attente de moins de 3 et une vitesse supérieure à 1000. Il ne va retourner cela que pour les services enregistrés dans la portée BLDG 32.

<t>=service:directory-agent <s>=DEFAULT <p>=
Ceci retourne des DAAdvert pour tous les DA dans la portée DEFAULT.

Les DA sont découverts en envoyant une SrvRqst avec le type de service réglé à "service:directory-agent". Si un prédicat est inclus dans la SrvRqst, le DA DEVRAIT ne répondre que si le prédicat peut être satisfait avec les attributs du DA. La <scope-list> DOIT contenir toutes les portées configurées pour l'UA ou SA qui va à la découverte des DA.

La chaîne <SLP SPI> indique un SLP SPI avec lequel le requérant a été configuré. Si cette chaîne est omise, celui qui répond n'inclut aucun bloc d'authentification dans sa réponse. Si elle est incluse, celui qui répond DOIT retourner une réponse qui a un bloc d'authentification associé au SLP SPI dans la SrvRqst. Si aucune réponse ne peut être retournée parce que le SLP SPI n'est pas pris en charge, celui qui répond retourne une erreur AUTHENTIFICATION_INCONNUE.

8.2 Réponse de service



La réponse de service contient zéro, une, ou plusieurs entrées d'URL (voir au paragraphe 4.3). Une réponse de service avec zéro entrée d'URL DOIT être retournée en réponse à une demande de service en envoi individuel, si aucun URL correspondant n'est présent. Une réponse de service avec zéro entrée d'URL NE DOIT PAS être envoyée en réponse à une demande de service en diffusion ou en diffusion groupée (si aucune correspondance n'est trouvée ou si il y a une erreur dans le traitement de la demande, la réponse de service devrait plutôt ne pas être générée du tout).

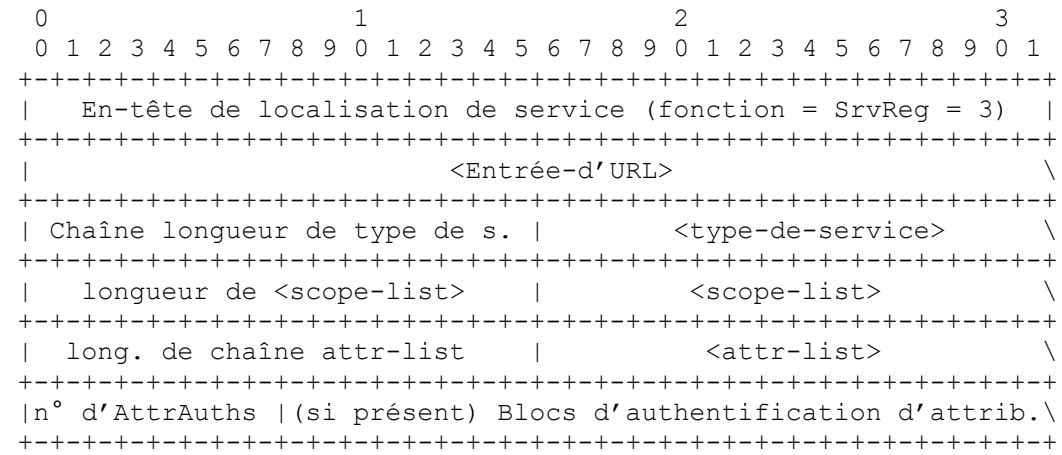
Si la réponse déborde, l'UA PEUT simplement utiliser la première entrée d'URL dans la liste. Un URL obtenu par SLP ne peut pas être mis en antémémoire plus longtemps que le nombre de secondes de sa durée de vie, sauf si un bloc d'authentification d'URL est présent.

Dans ce cas, la durée de vie de l'antémémoire est indiquée par l'horodatage dans l'authentifiant d'URL (voir au paragraphe 9.2).

Un bloc d'authentification est retourné dans les entrées d'URL, incluant le SLP SPI dans la SrvRqst. Si aucun SLP SPI n'était inclus dans la demande, aucun bloc d'authentification n'est retourné dans la réponse. Les blocs d'authentification d'URL sont définis au paragraphe 9.2.1.

Si une SrvRply est envoyée par UDP, une entrée d'URL NE DOIT PAS être incluse, sauf si elle tient entièrement sans fragmentation.

8.3 Enregistrement de service



<Entrée> est une entrée d'URL (voir au paragraphe 4.3). La Durée-de-vie définit pendant combien de temps un DA peut garder l'enregistrement en antémémoire. Les SA DEVRAIENT réenregistrer avant l'arrivée à expiration de cette durée de vie (mais NE DEVRAIENT PAS le faire plus d'une fois par seconde). La durée de vie PEUT être réglée à toute valeur entre 0 et 0xffff (maximum, environ 18 heures). Les enregistrements de longue durée restent périmés plus longtemps si le service échoue et si le SA ne désenregistre pas le service.

Le <type-de-service> définit le type de service de l'URL à enregistrer, sans considération du schéma de l'URL. La <scope-list> DOIT contenir les noms de toutes les portées configurées pour le SA, que le DA enregistre avec la prise en charge. La valeur par défaut pour la <scope-list> est "DEFAULT" (voir à la Section 11).

L'enregistrement du SA auprès de tous les DA DOIT être cohérent. Si un SA est configuré avec les portées X et Y et si il y a trois DA, dont les portées sont respectivement "X", "Y" et "X,Y", le SA va s'enregistrer auprès des trois DA dans leurs portées respectives. Toutes les mises à jour et tous les désenregistrements futurs du service doivent être envoyés au même ensemble de DA dans les mêmes portées dans lesquelles le service était initialement enregistré.

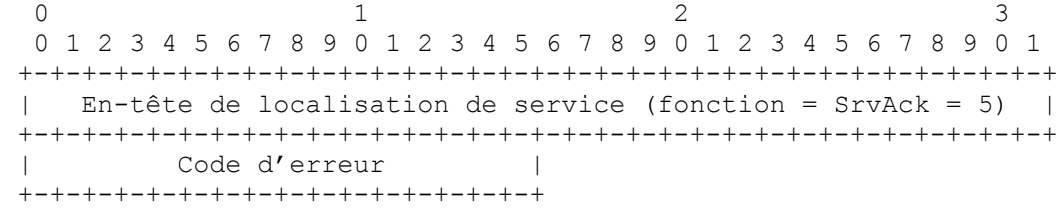
La <attr-list>, si elle est présente, spécifie les attributs et valeurs à associer à l'URL par le DA (voir la Section 5).

Un SA configuré avec la capacité à signer les enregistrements de service DOIT signer chacune des listes d'URL et d'attributs en utilisant chacune des clés qu'il est configuré à utiliser, et que le DA auprès duquel il s'enregistre accepte. (Le SA DOIT acquérir les DAAdvert pour tous les DA auprès desquels il s'enregistre pour obtenir la liste de SLP SPI et d'attributs du DA, comme décrit au paragraphe 8.5). Le SA fournit un SLP SPI dans chaque bloc d'authentification pour indiquer la configuration de SLP SPI exigée pour vérifier la signature numérique. Le format de signatures numériques utilisé est défini au paragraphe 9.2.1.

Les enregistrements ultérieurs de services précédemment enregistrés DOIVENT contenir la même liste de SLP SPI que les précédentes sinon les DA les rejetteront, en répondant avec une erreur AUTHENTIFICATION_ABSENTE.

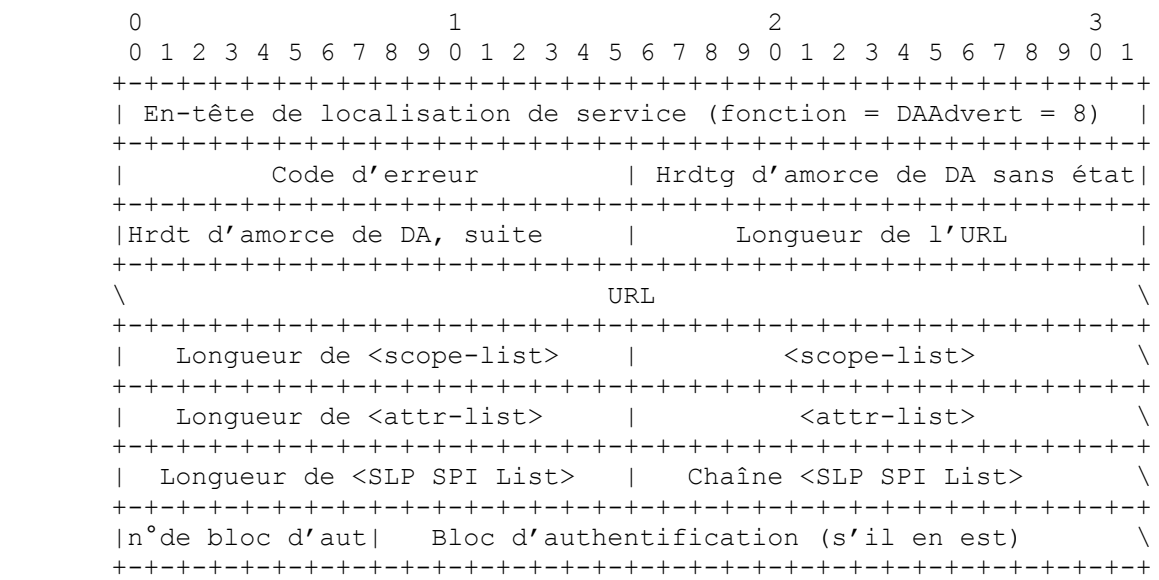
Un enregistrement avec le fanion FRAIS établi va remplacer *entièrement* tout enregistrement précédent pour le même URL dans la même langue. Si le fanion FRAIS n'est pas établi, l'enregistrement est un enregistrement "incrémentaire" (voir au paragraphe 9.3).

8.4 Accusé de réception de Service



Un DA retourne un SrvAck à un SA après un SrvReg. Il ne porte qu'un code d'erreur de deux octets (voir la Section 7).

8.5 Annonce d'agent de répertoire



Le code d'erreur est réglé à 0 lorsque la DAAdvert est en diffusion groupée. Si la DAAdvert est retournée à cause d'une SrvRqst en envoi individuel (c'est-à-dire, une demande sans le fanion REQUEST MCAST établi) le DA retourne les mêmes erreurs que retournerait une SrvRply.

La <scope-list> de la SrvRqst doit être omise ou inclure une portée que prend en charge le DA. L'horodatage d'amorce de DA sans état indique l'état du DA (voir au paragraphe 12.1).

Le DA PEUT inclure une liste de ses attributs dans la DAAdvert. Cette liste DEVRAIT rester courte, car la DAAdvert doit tenir dans un datagramme afin d'être envoyée en diffusion groupée.

Un problème potentiel d'adaptabilité peut survenir dans SLPv2 si les SA choisissent une durée de vie trop faible. Dans ce cas, des réenregistrements coûteux surviennent lorsque plus de services sont déployés. SLPv2 permet aux DA de contrôler la fréquence d'enregistrement des SA. Un DA PEUT produire à nouveau une DAAdvert avec un nouvel ensemble d'attributs à tout moment, pour changer le comportement de réenregistrement des SA. Cela ne s'applique qu'aux enregistrements ultérieurs ; les enregistrements de service existants auprès du DA conservent leur durée de vie enregistrée.

Si la DAAdvert inclut l'attribut "min-refresh-interval", il DOIT être réglé à une seule valeur d'entier indiquant un nombre de secondes. Si cet attribut est présent, les SA NE DOIVENT PAS rafraîchir une annonce de service particulière plus fréquemment que cette valeur. Si une SrvReg avec le fanion FRAIS non établi ou SrvDereg avec une liste d'étiquette non vide mettant à jour un service particulier est reçue plus fréquemment que la valeur de l'attribut annoncé "min-refresh-interval" du DA, celui-ci DEVRAIT rejeter le message et retourner une erreur RAFRAICHISSEMENT_REJETÉ dans le SrvAck.

L'URL est "service:directory-agent://"<addr> du DA, où <addr> est l'adresse numérique en décimal séparé par des points du DA. La <scope-list> du DA NE DOIT PAS être NULL.

La liste SLP SPI est la liste des SPI que le DA est capable de vérifier. Les SA NE DOIVENT PAS enregistrer de services avec les blocs d'authentification pour les SLP SPI qui ne sont pas sur la liste. Les DA vont rejeter les enregistrements de service qu'ils ne peuvent pas vérifier, et retourneront une erreur AUTHENTIFICATION_INCONNUE.

Le format des signatures DAAdvert est défini au paragraphe 9.2.1.

Le SLP SPI qui est utilisé pour vérifier la DAAdvert est inclus dans le bloc d'authentification. Lorsque les DAAdvert sont envoyés en diffusion groupée, ils peuvent avoir à transmettre plusieurs blocs d'authentification de DAAdvert. Si le DA est configuré pour être capable de générer des signatures pour plus d'un SPI, le DA DOIT inclure un bloc d'authentification pour chaque SPI. Si tous ces blocs d'authentification ne tiennent pas dans un seul datagramme (en diffusion ou en diffusion groupée) le DA DOIT envoyer des DAAdvert séparés afin que les blocs d'authentification pour tous les SPI que le DA est capable de générer soient envoyés.

Si la DAAdvert est envoyée en réponse à une SrvRqst, la DAAdvert ne contient que le bloc d'authentification avec la SLP SPI dans la SrvRqst, si le DA est configuré pour être capable de produire des signatures numériques en utilisant ce SLP

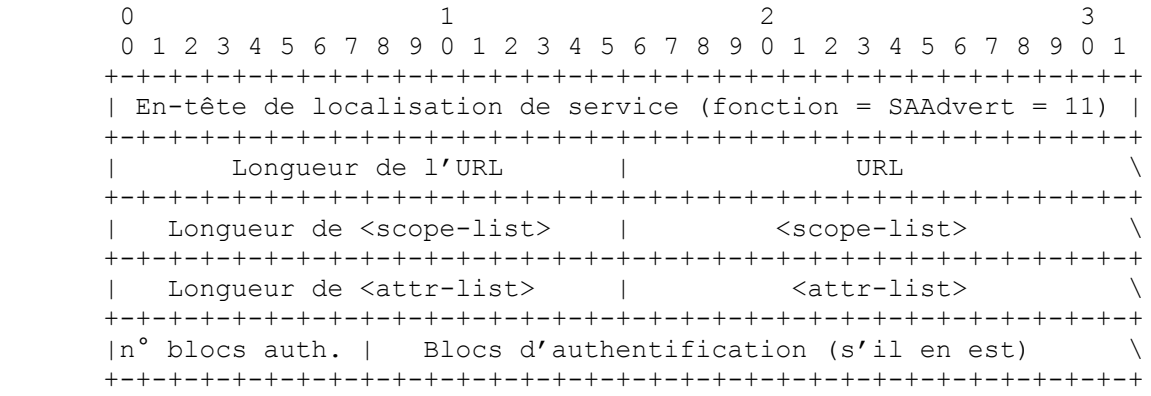
SPI. Si la SrvRqst est en envoi individuel au DA (le fanion REQUEST MCAST n'est pas établi dans l'en-tête) et si un SLP SPI non accepté est inclus, le DA répond avec une DAAdvert qui a le code d'erreur réglé à AUTHENTIFICATION_INCONNUE.

Les UA DEVRAIENT être configurés avec des SLP SPI qui vont leur permettre de vérifier les annonces de DA. Si l'UA est configuré avec des SLP SPI et s'il reçoit une DAAdvert qui échoue à la vérification en utilisant l'un d'entre eux, l'UA DOIT l'éliminer.

8.6 Annonce d'agent de service

Les agents d'utilisateur NE DOIVENT PAS solliciter d'annonces de SA si ils ont été configurés pour utiliser un DA particulier, si ils ont été configurés avec une <scope-list> ou si des DA ont été découverts. Les UA ne sollicitent d'annonces de SA que lorsque ils sont explicitement configurés pour utiliser des portées choisies par l'utilisateur (voir au paragraphe 11.2) afin de découvrir les portées que prennent en charge les SA. Cela permet aux UA sans configuration de portée d'utiliser les DA ou les SA sans aucune différence fonctionnelle, excepté les performances.

Un SA PEUT être configuré avec des attributs, et DEVRAIT accepter l'attribut 'type de service' dont la valeur est tous les types de service représentés par le SA. Les SA NE DOIVENT PAS répondre si le prédicat de la SrvRqst n'est pas satisfait. Par exemple, seuls les SA qui offrent les services 'nfs' DEVRAIENT répondre avec une SAAdvert à une SrvRqst pour le type de service "service:service-agent" qui inclut un prédicat "(service-type=nfs)".



Le SA ne répond qu'aux demandes de découverte de SA en diffusion groupée qui ne comportent pas de <scope-list> ou une portée qu'ils sont configurés à utiliser.

La SAAdvert PEUT inclure une liste d'attributs que le SA prend en charge. Cette liste d'attributs DEVRAIT rester petite afin que la SAAdvert n'excède pas la taille de la MTU du chemin.

L'URL est "service:service-agent://"<adresse> du SA, où <adresse> est l'adresse numérique en décimal séparé par des points du SA. La <scope-list> du SA NE DOIT PAS être nulle.

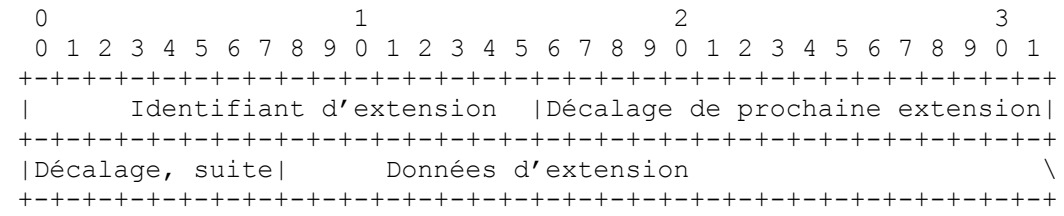
La SAAdvert contient un bloc d'authentification de SAAdvert pour chaque SLP SPI pour lequel le SA peut produire un bloc d'authentification. Si l'UA peut vérifier le bloc d'authentification de la SAAdvert, et si la SAAdvert échoue à la vérification, l'UA DOIT l'éliminer.

9. Caractéristiques facultatives

Les caractéristiques décrites dans cette section ne sont pas obligatoires. Certaines sont utiles pour une utilisation interactive de SLP (lorsque un utilisateur plutôt qu'un programme choisit des services, en utilisant par exemple une interface de navigation) et pour l'adaptabilité de SLP aux plus grands réseaux.

9.1 Extensions au protocole de localisation de service

Le format d'une extension de localisation de service est :



Les identifiants d'extension sont alloués de la façon suivante :

0x0000-0x3FFF normalisé. Mise en œuvre facultative. Ignorée si non reconnue.
0x4000-0x7FFF normalisé. Mise en œuvre obligatoire. Un UA ou SA qui reçoit cette option dans une réponse et ne la comprend pas DOIT éliminer la réponse en silence. Un DA ou SA qui reçoit cette option dans une demande et ne la comprend pas DOIT retourner une erreur OPTION_NON_COMPRISE.
0x8000-0x8FFF pour utilisation privée (non normalisée). Mise en œuvre facultative. Ignorée si non reconnue.
0x9000-0xFFFF Réservé.

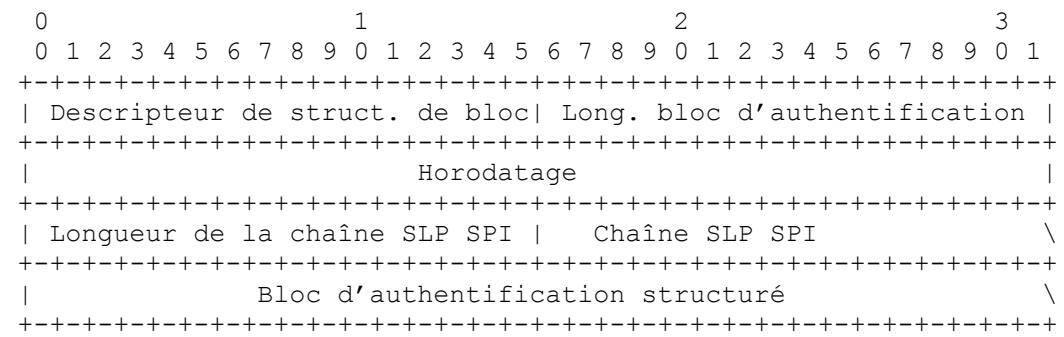
Les trois octets de décalage de la prochaine extension indiquent la position de la prochaine extension comme décalage à partir du début du message SLP.

La valeur du décalage est 0 si il n'y a pas d'extension qui suive l'extension en cours.

Si le décalage est 0, la longueur des données de l'extension en cours est déterminée par soustraction de la longueur totale du message SLP telle que donnée dans l'en-tête du message SLP moins le décalage de l'extension en cours.

Les extensions définies dans le présent document sont dans l'Annexe D. Voir à la Section 15 les procédures qui sont exigées lors de la spécification de nouvelles extensions SLP.

9.2 Blocs d'authentification



Les blocs d'authentification sont retournés avec certains messages SLP pour vérifier que leur contenu n'a pas été modifié, et qu'ils ont été transmis par un agent autorisé. Les données d'authentification (contenues dans le bloc d'authentification structuré) sont normalement insensibles à la casse. Bien que les données d'enregistrement SLP (par exemple, les valeurs d'attribut) ne soient normalement pas sensibles à la casse, la casse des données d'enregistrement doit être préservée par le DA d'enregistrement afin que les UA soient capables de vérifier les données utilisées pour calculer les données des signatures numériques.

Le descripteur de structure de bloc (BSD, *Block Structure Descriptor*) identifie le format de l'authentifiant qui suit. Les BSD de 0x0000 à 0x7FFF seront conservés par l'IANA. Les BSD de 0x8000 à 0x8FFF sont pour utilisation privée.

La longueur de bloc d'authentification est la longueur du bloc entier, en commençant par le BSD.

L'horodatage est l'heure à laquelle expire l'authentificateur (pour empêcher les attaques en répétition). L'horodatage est un nombre non signé de 32 bits à virgule fixe de secondes depuis le 1er janvier 1970 à 0 h. Les SA utilisent cette valeur pour indiquer quand expire la validité de la signature numérique. Cet horodatage va revenir à zéro en 2106. Une fois que la valeur de l'horodatage sera revenue à zéro, l'heure de référence de l'horodatage sera établie à nouveau. Par exemple, après 06 h 28 et 16 secondes le 5 février 2106, toutes les valeurs d'horodatage se rapporteront à cette nouvelle date.

La chaîne d'indice SLP de paramètres de sécurité (SPI, *Security Parameters Index*) identifie la longueur de la clé, les paramètres de l'algorithme et le matériel de clés à utiliser par les agents pour vérifier les données de signature dans le bloc

d'authentification structuré. La chaîne SLP SPI a la même grammaire que la <scope-val> définie au paragraphe 6.4.1.

Les caractères réservés dans les chaînes de SLP SPI doivent être esquivées en utilisant la même convention que celle utilisée partout dans SLPv2.

Les SLP SPI déployés dans un site DOIVENT être univoques. Un SLP SPI utilisé pour BSD = 0x0002 ne doit pas être le même que celui utilisé pour un autre BSD.

Tous les agents SLP DOIVENT mettre en œuvre DSA [FIPS186] (BSD = 0x0002). Les SA DOIVENT enregistrer les services auprès des blocs d'authentification DSA, et ils PEUVENT les enregistrer avec d'autres blocs d'authentification en utilisant d'autres algorithmes. Les SA DOIVENT utiliser les blocs d'authentification DSA dans les messages SrvDeReg et les DA DOIVENT utiliser les blocs d'authentification DSA dans les DAAdvert non sollicitées.

9.2.1 Règles d'authentification du message SLP

Ce paragraphe définit comment calculer la valeur à appliquer à l'algorithme identifié par la valeur de BSD. Les composants énumérés sont utilisés comme si il y avait une mémoire tampon contiguë d'un seul octet alignée dans l'ordre indiqué.

URL
16-bit Longueur de chaîne SLP SPI, chaîne SLP SPI.
16-bit Longueur de l'URL, URL,
32-bit Horodatage.

Liste d'attributs
16-bit Longueur de chaîne SLP SPI, chaîne SLP SPI.
16-bit Longueur de <attr-list>, <attr-list>,
32-bit Horodatage.

DAAdvert
16-bit Longueur de chaîne SLP SPI, chaîne SLP SPI.
32-bit Horodatage de l'amorce du DA sans état ,
16-bit Longueur de l'URL, URL,
16-bit Longueur de <attr-list>, <attr-list>,
16-bit Longueur de la <scope-list> du DA, <scope-list> du DA,
16-bit Longueur de la <SLP SPI List> du DA , <SLP SPI List> du DA,
32-bit Horodatage.

Le premier SLP SPI est le SLP SPI dans le bloc d'authentification. Ce SLP SPI indique le matériel de clé et les autres paramètres à utiliser pour vérifier la DAAdvert. La Liste SLP SPI est la liste des SLP SPI que prend lui-même en charge le DA, et est capable de vérifier.

SAAdvert
16-bit Longueur de la chaîne SLP SPI, chaîne SLP SPI,
16-bit Longueur de l'URL, URL,
16-bit Longueur de <attr-list>, <attr-list>,
16-bit Longueur de <scope-list>, <scope-list>,
32-bit Horodatage.

9.2.2 DSA avec SHA-1 dans les blocs d'authentification

BSD = 0x0002 est défini comme étant DSA avec SHA-1. Le calcul de signature est défini par [FIPS186]. Le format de signature se conforme à celui du certificat X.509 v3 :

1. L'identifiant d'algorithme de signature (un OID)
2. La valeur de la signature (une chaîne d'octets)
3. Le chemin de certificat.

Toutes les données sont représentées en codage ASN.1:

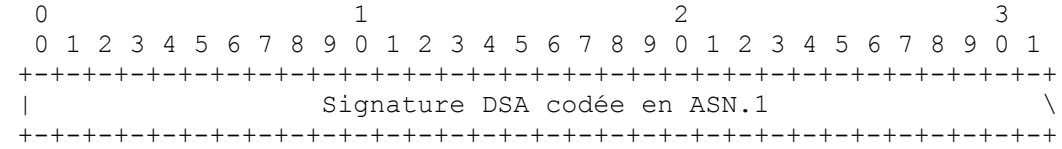
id-dsa-with-sha1 ID ::= { iso(1) member-body(2) us(840) x9-57 (10040) x9cm(4) 3 }

C'est-à-dire, le codage ASN.1 de 1.2.840.10040.4.3 suivi immédiatement par :

```
Dss-Sig-Value  ::=  SEQUENCE  {
            r           ENTIER,
            s           ENTIER  }
```

C'est-à-dire, le codage ASN.1 binaire de r et s calculé en utilisant DSA et SHA-1. Ceci est suivi par un chemin de certificat, comme défini par [X.509], [9594-2], [9594-6], [9594-7], [9594-8].

Les blocs d'authentification pour BSD=0x0002 ont le format suivant. À l'avenir, les BSD pourront être alloués avec des formats différents.



9.3 Enregistrement de service incrémentaire

Les enregistrements incrémentaires mettent à jour les valeurs d'attribut pour un service précédemment enregistré. Les enregistrements incrémentaires de service sont utiles quand, par exemple, un seul attribut a changé. Dans un enregistrement incrémentaire, le fanion FRAIS dans l'en-tête SrvReg N'EST PAS établi.

Les attributs du nouvel enregistrement remplacent ceux de l'enregistrement précédent, mais n'affectent pas les attributs qui étaient inclus précédemment et ne sont pas présents dans la mise à jour.

Par exemple, supposons que le service:x://a.org a été enregistré avec les attributs A=1, B=2, C=3. Si un enregistrement incrémentaire arrive pour le service:x://a.org avec les attributs C=30, D=40, alors les attributs pour le service après la mise à jour sont A=1, B=2, C=30, D=40.

Les enregistrements incrémentaires NE DOIVENT PAS être effectués pour les services enregistrés avec des blocs d'authentification. Ceux-ci doivent être enregistrés avec TOUS les attributs, avec le fanion FRAIS établi dans l'en-tête SrvReg. Les DA qui reçoivent de tels messages d'enregistrement retournent une erreur AUTHENTIFICATION_ÉCHEC.

Si le fanion FRAIS n'est pas établi et si le DA n'a pas un enregistrement antérieur pour le service, l'enregistrement incrémentaire échoue avec le code d'erreur MISE_A_JOUR_INVALIDE.

Le SA DOIT utiliser la même <scope-list> dans un message de mise à jour que celle utilisée dans l'enregistrement antérieur. Si cela n'est pas fait, le DA retourne une erreur PORTÉE_NON_ACCEPTÉE. Pour changer la portée d'une annonce de service il DOIT être d'abord désenregistré et réenregistré avec une nouvelle <scope-list>.

Le SA DOIT utiliser le même <type-de-service> dans un message de mise à jour que celui qui a été utilisé dans un enregistrement antérieur du même URL. Si cela n'est pas fait, le DA retourne une erreur MISE_A_JOUR_INVALIDE.

9.4 Listes d'étiquettes

Les listes d'étiquettes sont utilisées dans les messages SrvDeReg et AttrReq. La syntaxe d'un élément <liste-d'étiquette> est :
filtre-d'étiquette = étiquette-simple / sous-chaîne
étiquette-simple = 1*filt-caract
sous-chaîne = [initial] tout [final]
initial = 1*filt-caract
tout = `*' *(filt-caract `*')
final = 1*filt-caract
filt-caract = Tout caractère à l'exclusion de <réservé> et <bad-tag> (voir la grammaire à la Section 5).

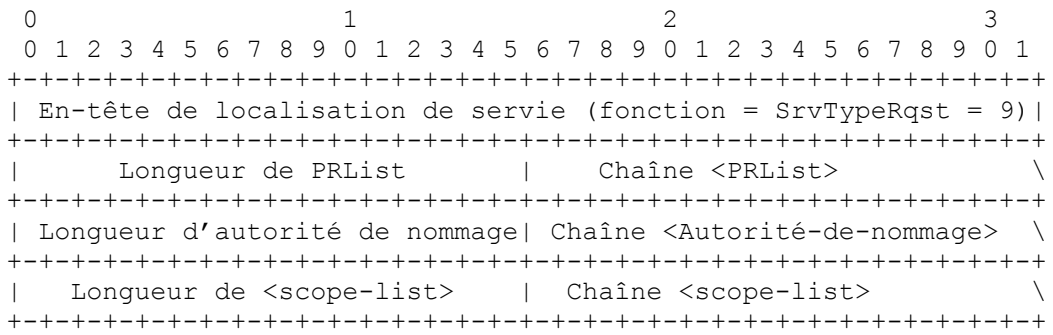
Les caractères génériques dans un élément de <liste-d'étiquette> correspondent à une séquence arbitraire de caractères. Par exemple "*bob*" correspond à "un bob que je connais", "grosbob", "bobby" et "bob".

10. Messages SLP facultatifs

Les demandes supplémentaires fournissent des caractéristiques pour les interactions avec les utilisateurs et pour une mise à jour efficace des annonces de service avec des attributs dynamiques.

10.1 Demande de type de service

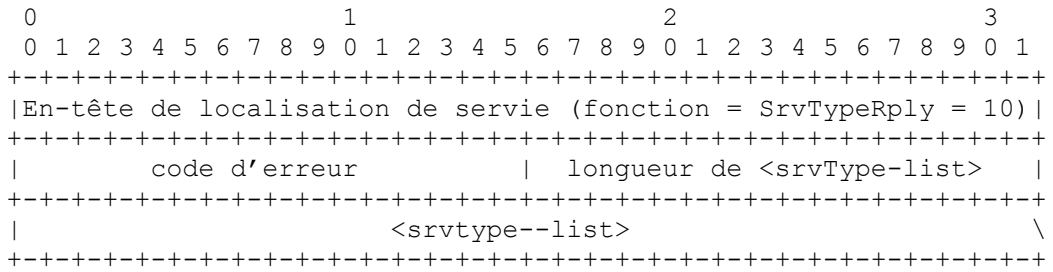
La demande de type de service (SrvTypeRqst) permet à l'UA de découvrir tous les types de service sur un réseau. C'est utile pour les navigateurs génériques.



L'interprétation de la liste <PRList> et de <scope-list> est donnée au paragraphe 8.1.

La chaîne <Autorité de nommage> si elle est présente dans la demande, va limiter la réponse aux chaînes de type de service qui ont l'autorité de nommage spécifiée. Si l'autorité de nommage est absente, les types de service enregistrés auprès de l'IANA seront retournés. Si la longueur de l'autorité de nommage est réglée à 0xFFFF, la chaîne Autorité de nommage est omise et TOUS les types de service sont retournés, sans considération de l'autorité de nommage.

10.2 Réponse de type de service

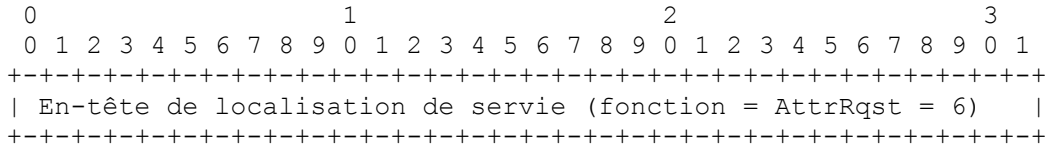


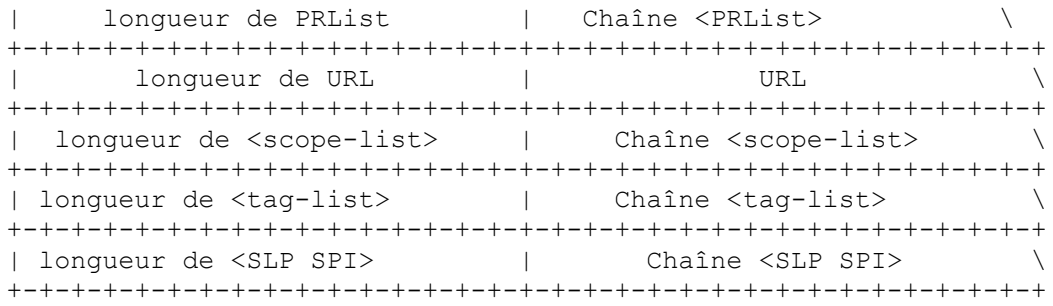
Les chaînes service-type (comme décrit au paragraphe 4.1) sont fournies dans <srvtype-list>, qui est une <liste-de-chaîne>.

Si un type de service a une autorité de nommage autre que l'IANA, il DOIT être retourné à la suite de la chaîne de type de service et d'un caractère '.'. Les types de service qui ont l'IANA comme autorité n'incluent pas de chaîne Autorité de nommage.

10.3 Demande d'attribut

La demande d'attribut (AttrRqst) permet à l'UA de découvrir les attributs d'un certain service (en fournissant son URL) ou un type de service entier. Cette dernière caractéristique permet à l'UA de construire une interrogation des services disponibles en choisissant les caractéristiques désirées. L'UA peut demander que tous les attributs soient retournés , ou seulement un sous-ensemble d'entre eux.





L'interprétation des chaînes <PRList>, <scope-list> et <SLP SPI> est données au paragraphe 8.1.

Le champ URL peut prendre deux formes. Il peut simplement être un type de service (voir au paragraphe 4.1) comme "http" ou "service:tftp". Dans ce cas, tous les attributs et la gamme complète des valeurs de chaque attribut de tous les services de ce type de service sont retournés.

Le champ URL peut autrement être un URL complet, tel que "service:printer:lpr://igore.wco.ftp.com:515/draft" ou "nfs://max.net/znoo". Dans celui-ci, seuls les attributs enregistrés pour l'URL spécifié sont retournés.

Le champ <tag-list> est une <liste de chaînes> des étiquettes d'attribut, comme défini au paragraphe 9.4 qui indique les attributs à retourner dans la AttrRply. Si la <tag-list> est omise, tous les attributs sont retournés. <tag-list> DOIT être omis et un URL complet DOIT être inclus lorsque une chaîne Liste de SLP SPI est incluse, autrement le DA répondra par une erreur AUTHENTIFICATION_ÉCHEC.

10.4 Réponse d'attribut

Le format de la <attr-list> et du bloc d'authentification est spécifié pour SrvReg (voir au paragraphe 9.2.1).

Les réponses d'attribut DEVRAIENT être retournées avec la casse d'origine de l'enregistrement de la chaîne intact, car elles sont probablement destinées à être lisibles par l'homme. Dans le cas où la AttrRqst est par type de service, tous les attributs définis pour le type de service, et toutes leurs valeurs, sont retournés.

Bien que les espaces soient contractées pour les confrontations de chaînes, les étiquettes et valeurs d'attribut DOIVENT être retournées en préservant leurs espaces d'origine.

Une seule copie de chaque étiquette d'attribut ou de valeur de chaîne devrait être retournée, en choisissant arbitrairement une version (par rapport aux majuscules et minuscules et aux espaces internes aux chaînes). Les attributs et valeurs dupliqués DEVRAIENT être retirés. Une version arbitraire de la valeur de la chaîne et du nom de l'étiquette est choisie pour la fusion. Par exemple :"(A=a a,b)" fusionné avec "(a=A A,B)" peut donner "(a=a a,B)".

10.5 Exemples de demande/réponse d'attribut

Supposons que des services d'impression aient été enregistrés comme suit :

Service enregistré :
URL = service:printer:lpr://igore.wco.ftp.com/draft
liste-de-portées = Développement

Étiquette de langue = en
Attributs = (Nom=Igore),(Description=For developers only),
(Protocole=LPR),(description-de-localisation=12th floor),(Opérateur=James Dornan \3cdornan@monster\3e),
(taille-de-support=na-letter),(résolution=res-600),x-OK

URL = service:printer:lpr://igore.wco.ftp.com/draft
liste-de-portées = Développement

Étiquette de langue = de
Attributs = (Nom=Igore),(Description=Nur fuer Entwickler),(Protocol=LPR),(location-description=13te Etage),
(Operator=James Dornan \3cdornan@monster\3e),(media-size=na-letter),(resolution=res-600),x-OK

URL = service:printer:http://not.wco.ftp.com/cgi-bin/pub-prn
liste-de-portées = Développement
Étiquette de langue = en
Attributs = (Nom=Not),(Description=imprimante IPP expérimentale),(Protocole=http),(location-description=QA bench),
(taille-de-support=na-letter),(resolution=autre),x-BUSY

Noter que la première imprimante, "Igore" est enregistrée à la fois en anglais et en allemand. Les caractères '<' et '>' dans la valeur d'attribut Opérateur qui fait partie de l'adresse de messagerie a due être esquivée, car il y a des caractères réservés pour les valeurs.

Les étiquettes d'attribut ne sont pas traduites, bien que les valeurs d'attribut puissent l'être, voir [RFC2609].

La demande d'attribut :
URL = service:printer:lpr://igore.wco.ftp.com/draft
Étiquette de langue = Développement
Étiquette de langue = de
liste-d'étiquettes = resolution,loc*

reçoit la réponse d'attribut :
(description-de-localisation=13te Etage),(resolution=res-600)

La demande d'attribut :
URL = service:printer
Étiquette de langue = Développement
Étiquette de langue = en
liste-d'étiquettes = x-*,resolution,protocol

reçoit une réponse d'attribut qui contient :
(protocols=http,LPR),(resolution=res-600,other),x-OK,x-BUSY

La première demande est par instance de service et retourne les valeurs demandées, en allemand. La seconde demande est le type de service abstrait (voir la Section 4) et retourne les valeurs de "Igore" et de "Not".

Un bloc d'authentification d'attribut est retourné si on peut en retourner un avec le SLP SPI dans la AttrRqst. Noter que la <liste-d'attributs> retournée d'un DA avec un bloc d'authentification DOIT être identique à la <liste-d'attributs> enregistrée par un SA, afin que soient possibles les calculs de vérification d'authentification.

Un SA ou DA ne retourne qu'un bloc d'authentification d'attribut si la AttrRqst incluait un URL complet dans la demande et pas de liste d'étiquettes.

Si un SLP SPI est spécifié dans une demande en envoi individuel (le fanion REQUEST MCAST n'est pas établi dans l'en-tête) et si le SA ou DA ne peut pas retourner un bloc d'authentification avec ce SLP SPI, il est retourné une erreur AUTHENTIFICATION_INCONNUE. Le champ n° d'auth d'attribut est réglé à 0 si aucun bloc d'authentification n'est inclus, ou si aucun bloc d'authentification ne suit.

10.6 Désenregistrement de service

Un DA supprime un enregistrement de service lorsque sa durée de vie est terminée. Les services DEVRAIENT être désenregistrés lorsque ils ne sont plus disponibles, plutôt que de laisser les enregistrements arriver en fin de temporisation.

La <liste-d'étiquette> est une <liste-de-chaîne> (voir au paragraphe 2.1).

Le SA DOIT réessayer si il n'y a pas de réponse de la part du DA, voir au paragraphe 12.3. Le DA accuse réception d'une SrvDeReg avec un SrvAck. Une fois que le SA a reçu un accusé de réception qui indique la réussite, le service et/ou les attributs ne sont plus annoncés par le DA. Le DA désenregistre le service ou les attributs de service de toutes les portées spécifiées dans la SrvDeReg qui avaient été précédemment enregistrées.

Le SA DOIT désenregistrer tous les services qui ont la même liste de portées utilisée pour enregistrer le service auprès d'un DA. Si cela n'est pas fait dans le message SrvDeReg, le DA retourne une erreur PORTÉE_NON_ACCEPTÉE. Le champ Durée de vie dans l'entrée d'URL est ignoré pour les besoins de la SrvDeReg.

La <liste-d'étiquette> est une <liste-de-chaînes> d'étiquettes d'attribut à désenregistrer comme défini au paragraphe 9.4. Si aucune <liste-d'étiquette> n'est présente, la SrvDeReg désenregistre le service dans toutes les langues dans lesquelles elle les a enregistrées. Si la <liste-d'étiquette> est présente, la SrvDeReg désenregistre les attributs dont les étiquettes sont énumérées dans la spécification d'étiquette. Les services enregistrés avec des blocs d'authentification NE DOIVENT PAS inclure de <liste-d'étiquette> dans un message SrvDeReg: Un DA répondra par une erreur AUTHENTICATION_ÉCHEC dans ce cas.

Si le service à désenregistrer a été enregistré avec un ou des blocs d'authentification, un bloc d'authentification d'URL pour chacun des SLP SPI enregistrés doit être inclus dans la SrvDeReg. Autrement, le DA retourne une erreur AUTHENTIFICATION_ABSENTE. Si le message échoue à la vérification par le DA, une erreur AUTHENTICATION_ÉCHED est retournée par le DA.

11. Portées

Les portées sont des ensembles de services. Le principal usage des portées est de fournir la capacité de créer des groupements administratifs de services. Un ensemble de services peut recevoir une portée par les administrateurs du réseau. Un client qui cherche des services est configuré pour utiliser une ou plusieurs portées. L'usager va seulement découvrir les services qui ont été configurés pour son usage. En configurant les UA et les SA avec des portées, les administrateurs peuvent approvisionner des services. Les chaînes de portées sont insensibles à la casse. La chaîne de portée par défaut est "DEFAULT".

Les portées sont le principal moyen qu'a un administrateur pour adapter les déploiements de SLP aux plus grands réseaux. Lorsque des DA avec des portées qui sont NON-DEFAULT sont présents sur le réseau, d'autres avantages peuvent être obtenus en configurant les UA et les SA avec une portée prédéfinie non par défaut. Ces agents peuvent alors effectuer la découverte de DA et faire des demandes qui utilisent leur portée. Cela va limiter le nombre de réponses.

11.1 Règles de portées

Les messages SLP qui échouent à contenir une portée que l'agent receveur est configuré à utiliser sont abandonnés (si la demande était en diffusion groupée) ou une erreur PORTÉE_NON_ACCEPTÉE est retournée (si la demande était en envoi individuel). Chaque message SrvRqst (sauf pour les demandes de découverte de DA et de SA), SrvReg, AttrRqst, SrvTypeRqst, DAAdvert, et SAAdvert DOIT inclure une <liste-de-portées>.

Un UA DOIT envoyer en individuel ses messages SLP à un DA qui accepte la portée désirée, de préférence à l'envoi en diffusion groupée d'une demande aux SA. Un UA PEUT envoyer en diffusion groupée la demande si aucun DA n'est disponible dans la portée qu'il est configuré à utiliser.

11.2 Choix de portées administratif et d'usager

Toutes les demandes et les services sont munis d'une portée. Les deux exceptions sont les SrvRqst pour "service:directory-agent" et "service:service-agent". Elles PEUVENT avoir une <liste-de-portées> de longueur zéro lorsque elles sont utilisées pour permettre à l'usager de faire des choix de portées. Dans ce cas les UA obtiennent leur liste de portées des DAAdvert (ou si les DA ne sont pas disponibles, des SAAdvert.)

Autrement, si les SA et les UA sont décidés à utiliser toute portée autre que celle par défaut (c'est-à-dire, "DEFAULT"), les UA et les SA sont configurés avec des listes de portées à utiliser par les administrateurs du système, peut-être automatiquement au moyen de l'option DHCP 78 ou 79 [RFC2610]. De telles définitions administratives de portées permettent d'approvisionner des services, afin que les utilisateurs ne voient que les services qu'ils sont destinés à voir.

Les portées configurables par l'usager permettent à un utilisateur de découvrir tout service, mais exigent d'eux qu'ils fassent leur propre sélection de portées. Ceci est similaire à la façon dont le réseautage AppleTalk [AppleTalk] et SMB [SMB] permet la sélection par l'utilisateur d'une zone AppleTalk ou de groupes de travail.

Noter que les deux choix de configuration ne sont pas compatibles. Un modèle permet un contrôle des administrateurs sur l'approvisionnement de service. L'autre délègue cela aux usagers (qui peuvent n'être pas préparés à faire des configuration de leur système).

12. Agents de répertoire

Les DA mettent en antémémoire les localisation de service et les informations d'attributs. Cela se fait pour améliorer les performances et l'adaptabilité de SLP. Plusieurs DA fournissent une meilleure adaptabilité et robustesse de fonctionnement, car chacun peut mémoriser les informations sur les services pour les mêmes SA, en cas de défaillance d'un des DA.

Un DA fournit une mémorisation centralisée des informations sur les services. Cela est utile dans un réseau avec plusieurs sous-résaux ou avec de nombreux agents SLP. L'adresse du DA peut être configurée de façon dynamique avec des UA et des SA qui utilisent DHCP, ou bien en utilisant une configuration statique.

Les SA configurés pour utiliser les DA avec DHCP ou par configuration statique DOIVENT envoyer en individuel une SrvRqst au DA, lorsque le SA est initialisé. La SrvRqst omet la liste de portées et règle le type de service de la demande à "service:directory-agent". Le DA va retourner une DAAdvert avec ses attributs, une liste de SLP SPI, et d'autres paramètres qui sont essentiels pour une communication appropriée de SA à DA.

La détection passive des DA par les SA permet que les services soient annoncés de façon cohérente entre les DA de la même portée. Les annonces arrivent à expiration si elles ne sont pas renouvelées, laissant seulement des enregistrements d'état transitoires dans les DA, même dans le cas d'une défaillance d'un SA.

Un seul DA peut prendre en charge de nombreux UA. Les UA envoient les mêmes demandes aux DA que celles qu'ils enverraient aux SA et en attendent les mêmes résultats. Les DA réduisent la charge qui pèse sur les SA, rendant plus simple la mise en œuvre des SA.

Les UA DOIVENT être prêts à l'éventualité que les informations de services qu'ils obtiennent des DA soient périmées.

12.1 Règles d'agent de répertoire

Lorsque des DA sont présents, chaque SA DOIT enregistrer ses services auprès des DA qui prennent en charge une ou plusieurs de ses portées.

Les UA DOIVENT envoyer en individuel les demandes directement au DA (lorsque les règles de portée le permettent) en évitant donc d'utiliser un algorithme de convergence de diffusion groupée, pour obtenir les informations des services. Cela diminue l'utilisation du réseau et augmente la vitesse à laquelle les UA peuvent obtenir les informations sur les services.

Les DA DOIVENT purger les annonces de service une fois que leur durée de vie est terminée ou que leur "Horodatage" d'expiration du bloc d'authentification d'URL est passé.

Les DAAdvert DOIVENT inclure un horodatage d'amorce de DA sans état, dans le même format que le bloc d'authentification (voir au paragraphe 9.2). L'horodatage dans le bloc d'authentification indique l'heure à laquelle tous les enregistrements précédents ont été perdus (c'est-à-dire, le dernier réamorçage sans état). L'horodatage est réglé à 0 dans une DAAdvert pour notifier aux UA et aux SA que le DA va fermer. Les DA NE DOIVENT PAS utiliser des horodatages d'amorçage égaux ou inférieurs aux précédents si ils ferment ou redémarrent sans état d'enregistrement de service. Cela induirait faussement les SA à ne pas se réenregistrer auprès du DA.

Les DA qui reçoivent une SrvRqst en diffusion groupée pour le type de service "service:directory-agent" DOIVENT l'éliminer en silence si la <liste-de-portées> est (a) non omise et (b) ne comporte pas une portée qu'ils sont configurés à utiliser. Autrement, le DA DOIT répondre par une DAAdvert.

Les DA DOIVENT répondre aux messages AttrRqst et SrvTypeRqst (cela n'est FACULTATIF que pour les SA, pas pour les DA.)

12.2 Découverte d'agent de répertoire

Les UA peuvent découvrir les DA en utilisant la configuration statique, les options DHCP 78 et 79, ou en envoyant les demandes de service en diffusion ou diffusion groupée en utilisant l'algorithme de convergence du paragraphe 6.3.

Voir la Section 6 en ce qui concerne les DAAdvert non sollicitées. Le paragraphe 12.2.2 décrit comment les SA peuvent réduire le nombre de fois qu'ils doivent se réenregistrer auprès des DA en réponse à des DAAdvert non sollicitées.

Les DA DOIVENT envoyer des DAAdvert non sollicitées une fois par CONFIG_DA_BEAT. Une DAAdvert non sollicitée a un XID de 0. Les SA DOIVENT être à l'écoute des DAAdvert, passivement, comme décrit au paragraphe 8.5. Les UA PEUVENT le faire. Si ils ne sont pas à l'écoute des DAAdvert non sollicitées, ils ne vont pas découvrir les DA qui deviennent disponibles. Les UA DEVRAIENT, dans ce cas, faire périodiquement une découverte active de DA (voir à la Section 6).

Un URL avec le schéma "service:directory-agent" indique la localisation du DA comme défini au paragraphe 8.5. Par exemple : "service:directory-agent://foobawooba.org".

Les paragraphes qui suivent suggèrent des algorithmes de temporisation qui améliorent l'adaptabilité de SLP.

12.2.1 Découverte active de DA

Après le redémarrage d'un UA ou d'un SA, sa demande initiale de découverte de DA DEVRAIT être retardée d'une durée aléatoire à distribution uniforme entre 0 et CONFIG_START_WAIT secondes.

L'UA ou SA envoie la demande de découverte de DA en utilisant une SrvRqst, comme décrit au paragraphe 8.1. Les demandes de découverte de DA DOIVENT inclure une liste des répondants précédents. Les SrvRqst pour la découverte active de DA NE DEVRAIENT PAS être envoyées plus souvent qu'une fois toutes les CONFIG_DA_FIND secondes.

Après la découverte d'un nouveau DA, un SA DOIT attendre un délai aléatoire entre 0 et CONFIG_REG_ACTIVE secondes avant d'enregistrer ses services.

12.2.2 Annonce passive de DA

Un DA DOIT envoyer en diffusion groupée (ou en diffusion) une DAAdvert non sollicitée toutes les CONFIG_DA_BEAT secondes. CONFIG_DA_BEAT DEVRAIT être spécifié pour empêcher les DAAdvert d'utiliser plus de 1 % de la bande passante disponible.

Tous les UA et les SA qui reçoivent la DAAdvert non sollicitée DEVRAIENT examiner son horodatage d'amorce de DA sans état. Si il est réglé à 0, le DA est sur le point de fermer et aucun autre message ne devrait lui être envoyé.

Si un SA détecte un DA qu'il n'a jamais rencontré (avec un horodatage différent de zéro) le SA doit s'enregistrer auprès de lui. Les SA DOIVENT examiner l'horodatage de la DAAdvert pour déterminer si le DA a eu un réamorçage sans état depuis la dernière fois que le SA s'est enregistré auprès de lui. S'il en est ainsi, il s'enregistre auprès du DA. Les SA DOIVENT attendre un intervalle aléatoire entre 0 et CONFIG_REG_PASSIVE secondes avant de commencer l'enregistrement auprès du DA.

12.3 Envoi individuel fiable aux DA et SA

Si un DA ou un SA échoue à répondre à un message UDP en envoi individuel dans les CONFIG_RETRY secondes, le message devrait être réessayé. L'intervalle d'attente pour chaque retransmission successive DOIT augmenter de façon exponentielle, en doublant à chaque fois. Si un DA ou SA échoue à répondre après CONFIG_RETRY_MAX secondes, l'envoyeur devrait considérer que le receveur a fermé. L'UA devrait utiliser un DA différent. Si aucune de ces DA ne répond, la découverte de DA devrait être utilisée pour trouver un nouveau DA. Si aucun DA n'est disponible, on devrait utiliser des demandes en diffusion groupée aux SA.

12.4 Configuration de portée de DA

Par défaut, les DA sont configurés avec la portée "DEFAULT". Les administrateurs peuvent ajouter d'autres portées configurées, afin de prendre en charge les UA et les SA dans des portées qui ne sont pas par défaut. La configuration par défaut NE DOIT PAS être retirée du DA à moins que :
- Il y ait d'autres DA qui prennent en charge la portée "DEFAULT", ou
- que tous les UA et SA aient été configurés avec des portées qui ne sont pas par défaut.

Les portées qui ne sont pas par défaut peuvent être introduites progressivement à mesure de la croissance du déploiement de SLP. Les portées par défaut devraient n'être éliminées progressivement que lorsque les portées qui ne sont pas par défaut seront universellement configurées.

Si un DA et un SA sont corésidents sur un hôte (assez vraisemblablement mis en œuvre dans le même processus) la configuration de l'hôte est considérablement simplifiée si le SA n'accepte que des portées qui sont aussi prises en charge par le DA. C'est à dire que le SA NE DEVRAIT PAS annoncer des services dans des portées qui ne sont pas acceptées par le DA corésident. Cela signifie que les demandes entrantes peuvent être satisfaites par une seule mémorisation de données; et que les enregistrements de SA et de DA n'ont pas besoin d'être tenues séparément.

12.5 DA et blocs d'authentification

Les DA ne sont pas configurés pour signer des enregistrements de service ou des listes d'attributs. Ils mettent simplement en antémémoire les services enregistrés par les agents de service. Les DA NE DOIVENT PAS accepter d'enregistrements comportant des blocs d'authentification pour les SLP SPI avec lesquels ils ne sont pas configurés, voir au paragraphe 8.5.

Un DA protège les enregistrements qui sont faits avec des blocs d'authentification qui utilisent des SLP SPI qu'il est configuré pour utiliser. Si un service S est enregistré, un enregistrement suivant (qui va remplacer l'annonce) ou un désenregistrement (qui va le retirer) DOIT inclure un bloc d'authentification avec le SLP SPI correspondant, voir aux paragraphes 8.3 et 10.6.

Exemple :

Un DA est configuré pour être capable de vérifier les blocs d'authentification avec les SLP SPI "X,Y", c'est-à-dire X et Y.

Un SA enregistre un service avec un bloc d'authentification avec le SPI "Z". Le DA mémorise l'enregistrement, mais élimine le bloc d'authentification. Si un UA demande un service avec une chaîne de SLP SPI "Z", le DA va répondre avec une erreur AUTHENTIFICATION_INCONNUE.

Un SA enregistre un service S avec des blocs d'authentification qui incluent les SLP SPI "X" et "Y". Si un UA demande un service avec une chaîne de SLP SPI "X", le DA va être capable de retourner S (si le type de service, le langage, la portée et le prédicat de la SrvRqst correspondent à S). Le DA va aussi retourner le bloc d'authentification avec le SLP SPI réglé à "X". Si le DA reçoit un SrvDeReg ultérieur pour S (qui va retirer l'annonce) ou un SrvReg ultérieur pour S (qui va le remplacer) le message doit comporter deux blocs d'authentification d'URL, un pour chaque SPI "X" et "Y". Si l'un d'eux est absent, le DA devra retourner une erreur AUTHENTIFICATION_ABSENTE.

13. Temporisations du protocole par défaut

Nom de l'intervalle	§	Valeur par défaut	Signification
CONFIG_MC_MAX	6.3	15 s	Durée maximale d'attente d'une réponse d'interrogation en diffusion groupée complète (toutes les valeurs).
CONFIG_START_WAIT	12.2.1	3 s	Attente pour effectuer la découverte de DA au réamorçage.
CONFIG_RETRY	12.3	2 s	Intervalle d'attente avant la retransmission initiale de demandes en diffusion groupée ou en envoi individuel.
CONFIG_RETRY_MAX	12.3	15 s	Abandon des retransmissions de demande en envoi individuel.
CONFIG_DA_BEAT	12.2.2	3 heures	Battement de cœur de DA, afin que les SA détectent passivement les nouveaux DA.
CONFIG_DA_FIND	12.3	900 s	Intervalle minimum d'attente avant de répéter la découverte active de DA.
CONFIG_REG_PASSIVE	12.2	1-3 s	Attente d'enregistrement des services en découverte passive de DA.
CONFIG_REG_ACTIVE	8.3	1-3 s	Attente d'enregistrement des services en découverte active de DA.
CONFIG_CLOSE_CONN	6.2	5 minutes	Délai après lequel DA et SA closent les connexions inactives.

14. Configuration facultative

Diffusion seule
Tout agent SLP DEVRAIT être configurable à n'utiliser que la diffusion. Voir les paragraphes 6.1 et 12.2.

DA prédéfini DA
Un UA ou SA DEVRAIT être configurable à utiliser un DA prédéfini.

Pas de découverte de DA
L'UA ou SA DEVRAIT être configurable pour utiliser SEULEMENT des DA prédéfinis et configurés avec DHCP et n'effectuer aucune découverte active ou passive de DA.

TTL de diffusion groupée
Le TTL de diffusion groupée par défaut est de 255. Les agents DEVRAIENT être configurables à utiliser d'autres valeurs. Une valeur inférieure se concentrera sur l'algorithme de convergence de diffusion groupée sur les plus petits sous-réseaux, en diminuant le nombre de réponses et en augmentant les performances de la localisation de service. Il peut en résulter que des UA obtiennent des résultats différents pour des demandes identiques, selon l'endroit où ils sont connectés au réseau.

Valeurs de temporisation
Les valeurs de temporisation autres que par défaut PEUVENT être configurables. Voir à la Section 13.

Portées
Un UA PEUT être configurable à prendre en charge les portées sélectionnables par l'usager en omettant toutes les portées prédéfinies. Voir au paragraphe 11.2. Un UA ou SA DOIT être configurable à utiliser des portées spécifiques par défaut. De plus, un UA ou SA DOIT être configurable à utiliser des portées spécifiques pour des demandes et enregistrements de types spécifiques de service. La ou les portées d'un DA DOIVENT être configurables. La valeur par défaut pour un DA est d'avoir la portée "DEFAULT" si elle n'est pas configurée autrement.

Configuration DHCP
Les options DHCP 78 et 79 peuvent être utilisées pour configurer SLP. Si des localisations de DA sont configurées en utilisant DHCP, celles-ci DEVRAIENT être utilisées de préférence aux DA découverts activement ou passivement. Une ou plusieurs des portées configurées en utilisant DHCP DOIVENT être utilisées dans les demandes. La <liste-de-portées> configurée entière DOIT être utilisée dans les messages d'enregistrement et de configuration de DA.

Gabarit de service
Les UA et les SA PEUVENT être configurés en utilisant des gabarits de service. Tout en simplifiant la spécification des valeurs d'attributs, cela leur permet aussi de mettre en application l'inclusion des attributs "exigés" dans les messages SrvRqst, SrvReg et SrvDeReg. Les DA PEUVENT être configurés avec des gabarits pour leur permettre de donner des AVERTISSEMENTS aux UA et SA dans ce cas. Voir au paragraphe 10.4.

SLP SPI pour la découverte de service
Les agents DEVRAIENT être configurables à prendre en charge les SLP SPI en utilisant les paramètres suivants : BSD = 2 (DSA avec SHA-1) et une clé publique identifiée par la chaîne SLP SPI. À l'avenir, lorsque existera une infrastructure de clé publique, les agents SLP pourront être capables d'obtenir des clés publiques et des paramètres cryptographiques correspondant aux noms utilisés dans les chaînes SLP SPI.

Noter que si la chaîne SLP SPI choisie est identique à une chaîne de portée, c'est effectivement la même qu'une portée protégée dans SLPv1. À savoir que chaque SA qui annonce dans cette portée serait configuré avec la même clé privée. Tout DA et UA de cette portée serait configuré avec la clé publique appropriée pour vérifier les signatures produites par ces SA. C'est une façon pratique pour configurer les déploiements de SLP en l'absence d'une infrastructure de clé publique. Actuellement, il serait trop difficile de gérer les clés des UA et des DA si chaque SA avait sa propre clé.

SLP SPI pour la découverte d'agent de répertoire
Les agents DEVRAIENT être configurables à prendre en charge les SLP SPI comme ci-dessus, et les utiliser lors de la découverte des DA. Ce SPI DEVRAIT être envoyé dans les SrvRqst pour découvrir les DA et être utilisé pour vérifier les messages DAAdvert en diffusion groupée.

Clé privée de SA et de DA
Les SA et les DA qui peuvent générer des signatures numériques exigent une clé privée et un identifiant de SLP SPI correspondant à inclure dans le bloc d'authentification. Le SLP SPI identifie la clé publique à utiliser pour vérifier la signature numérique dans le bloc d'authentification.

15. Considérations relatives à l'IANA

SLP comporte quatre ensembles d'identifiants qui peuvent être enregistrés auprès de l'IANA. Les politiques pour ces enregistrements (Voir [RFC2434]) sont notées dans chaque cas.

Le descripteur de structure de bloc (BSD, *Block Structure Descriptor*) identifie le format de l'authentifiant qui suit. Les BSD de 0x8000 à 0x8FFF sont pour utilisation privée.

D'autres valeurs de descripteur de structure de bloc dans la gamme de 0x0003 à 0x7FFF pourront être normalisées à l'avenir par la soumission d'un document qui devra décrire :
- Le format des données du bloc d'authentifiant structuré.
- Quel algorithme de chiffrement utiliser (y compris une référence à la spécification technique de l'algorithme).
- Le format de tout matériel de clé requis pour la pré configuration des UA, des DA et des SA. Cela inclut aussi toutes considérations sur la distribution des clés.
- Les considérations de sécurité pour alerter les autres des forces et faiblesses de l'approche.

L'IANA allouera les numéros de BSD cryptographiques sur la base du consensus de l'IETF.

De nouveaux identifiants de fonctions, dans la gamme de 12 à 255, peuvent être normalisés par la méthode du consensus de l'IETF.

De nouvelles extensions à SLP avec des types dans la gamme de 2 à 65 535 peuvent être enregistrés suite à révision par un expert désigné.

De nouveaux numéros d'erreur dans la gamme de 15 à 65 535 seront alloués sur la base d'une action de normalisation.

Les éléments de protocole utilisés avec le protocole de localisation de service peuvent aussi exiger des actions d'enregistrement de la part de l'IANA. SLP est utilisé en conjonction avec les URL "service:" et les gabarits de service [RFC2609]. Ceux-ci sont normalisés par revue par un expert désigné et une liste de diffusion (voir [RFC2609]).

16. Considérations d'internationalisation

Les messages SLP prennent en charge l'utilisation de plusieurs langages en fournissant un champ Étiquette de langue dans l'en-tête de message commun (voir la Section 8).

Les services PEUVENT être enregistrés dans de multiples langues. Cela fournit des attributs qui permettent aux utilisateurs qui maîtrisent différents langages de choisir les services de façon interactive.

Les étiquettes d'attribut ne sont pas traduites. Les valeurs d'attribut peuvent être traduites sauf si le gabarit de service [RFC2609] définit les valeurs de l'attribut comme 'littérales'.

Un service qui est enregistré dans plusieurs langages peut être interrogé dans plusieurs langues. Le langage de la SrvRqst ou AttrRqst est utilisé pour satisfaire la demande. Si le langage demandé n'est pas pris en charge, une erreur LANGAGE_NON_ACCEPTÉ est retournée. Les messages SrvRply et AttrRply sont toujours dans la même langue que la demande.

Un DA ou SA PEUT être configuré avec des traductions des gabarits de service [RFC2609] pour le même type de service. Cela va permettre au DA ou SA de traduire une demande (disons en italien) dans la langue de l'annonce de service (disons en anglais) et puis de retraduire la réponse en italien. De même, un UA PEUT utiliser les gabarits pour traduire les demandes en cours et les réponses entrantes.

Le champ dialecte dans l'étiquette de langage PEUT être utilisé : les demandes qui peuvent être satisfaites en correspondant à une langue et un dialecte seront préférées à celles qui ne correspondent qu'à la portion langage. Autrement, les dialectes n'ont pas d'effet sur la correspondance aux demandes.

17. Considérations pour la sécurité

SLP fournit l'authentification des URL de service et des attributs de service. Cela permet aux UA et DA de connaître l'intégralité des URL et attributs de service inclus dans les messages SLP. Les seuls systèmes qui peuvent générer des signatures numériques sont ceux qui ont été configurés à l'avance par les administrateurs. Les agents qui vérifient les données signées peuvent supposer qu'elles sont "de confiance" dans la mesure où les administrateurs ont assuré que le chiffrement des SA et DA reflète cette confiance.

La localisation de service n'assure pas la confidentialité. Parce que l'objectif de ce protocole est d'annoncer des services à une communauté d'usagers, la confidentialité pourrait n'être généralement pas nécessaire lorsque ce protocole est utilisé dans des environnements non sensibles. Des schémas spécialisés pourraient être capables de fournir la confidentialité, si elle se révélait nécessaire à l'avenir. Les sites qui exigent la confidentialité devraient mettre en œuvre l'encapsulation de charge utile de sécurité IP (ESP) [9594-6] pour assurer la confidentialité des messages de localisation de service.

Si les agents ne sont pas configurés pour générer des blocs d'authentification et si les agents ne sont pas configurés pour les vérifier, un adversaire peut facilement utiliser ce protocole pour annoncer des services sur des serveurs contrôlés par l'adversaire et par là obtenir l'accès aux informations privées des utilisateurs. De plus, un adversaire qui utilise ce protocole va trouver beaucoup plus facile de lancer des attaques sélectives de déni de service. Les sites qui sont dans des environnements potentiellement hostiles (par exemple, qui sont directement connectés à l'Internet) devraient considérer les avantages d'une distribution de clés associée aux SLP SPI avant de déployer des agents de répertoire ou agents de service sensibles.

SLP est utile comme protocole d'amorçage. Il peut être utilisé dans des environnements dans lesquels aucune pré configuration n'est possible. Dans de telles situations, une certaine quantité de "foi aveugle" est requise : sans aucune configuration préalable, il est impossible d'utiliser un des mécanismes de sécurité décrits ci-dessus. SLP va utiliser les mécanismes fournis par le domaine de sécurité de l'IETF pour la distribution des clés lorsque ils seront disponibles. Pour le moment, il ne sera possible que de tirer parti des avantages associés à l'utilisation des blocs d'authentification si les informations cryptographiques et les SLP SPI peuvent être pré configurés avec les systèmes d'extrémité avant qu'ils utilisent SLP.

SLPv2 permet un certain nombre de politiques de sécurité avec les mécanismes qu'elles comportent. Un UA SLPv2 pourrait, par exemple, rejeter tout message SLP qui ne porte pas de bloc d'authentification qu'il puisse vérifier. Ce n'est pas la seule politique qu'il est possible de mettre en œuvre.

Appendice A Changements au protocole de localisation de service de la v1 à la v2

SLP version 2 (SLPv2) corrige les conditions de concurrence présentes dans SLPv1 [RFC2165]. De plus, l'authentification a été retravaillée pour donner plus de souplesse et de protection (en particulier pour les annonces de DA). SLPv2 change aussi les formats et définitions de nombreux fanions et valeurs et réduit le nombre de caractéristiques exigées. SLPv2 précise et change l'utilisation des portées, éliminant la prise en charge des 'agents de répertoire sans portée' et des 'demandes sans portée'. SLPv2 utilise des codages de chaîne compatibles LDAPv3 pour les attributs et filtres de recherche. D'autres changements (tels que le traitement des langages et des jeux de caractères) adoptent les pratiques recommandées par le groupe de pilotage de l'ingénierie de l'Internet.

Des efforts ont été faits pour que SLPv2 fonctionne de la même façon que des DA soient présents ou non. Pour cette raison, un nouveau message (SAAdvert) a été ajouté. Cela permet aux UA de découvrir les informations de portée en l'absence de configuration administrative et de DA. Cela n'était pas possible dans SLPv1.

SLPv2 est incompatible à certains égards avec SLPv1. Si un DA qui accepte SLPv1 et SLPv2 avec la même portée est présent, les services annoncés par les SA qui utilisent l'une et l'autre version du protocole seront disponibles aussi bien pour les UA SLPv1 que SLPv2. Les DA SLPv1 DEVRAIENT être progressivement éliminés et remplacés par des DA SLPv2 qui acceptent les deux versions du protocole.

SLPv1 permet que les services soient annoncés et demandés sans avoir une portée. De plus, les DA peuvent être configurés sans portée. Cela est incompatible avec SLPv2 et pose des problèmes d'adaptabilité. Pour faciliter cette migration, les agents SLPv1 DOIVENT utiliser les portées pour tous les enregistrements et demandes. Les DA SLPv1 DOIVENT être configurés avec une liste de portées. Cela constitue une révision de la [RFC2165].

Appendice B Découverte de service par type : caractéristiques SLPv2 minimales

Les agents de service peuvent annoncer des services sans attribut. Cela ne permettra que la découverte de services par type. Les types de service découverts de cette façon auront un gabarit de service [RFC2609] défini qui spécifie explicitement qu'aucun attribut n'est associé à l'annonce de service. Les types de service associés aux gabarits de service qui spécifient des attributs NE DOIVENT PAS être annoncés par les SA qui ne prennent pas les attributs en charge.

Bien que la découverte de service par type de service soit un sous-ensemble des caractéristiques possibles, l'utilisation par SLPv2 de cette forme de découverte est cohérente avec la génération actuelle de produits qui permettent un simple feuilletage de tous les services dans une 'zone' ou 'groupe de travail' par type. Dans certains cas, comme celui de la découverte d'attributs, la sécurité et la négociation des caractéristiques est traitée par les protocoles de couche application – tout ce qui est exigé est la découverte de service de base qui prend en charge un certain service.

Les UA qui ne demandent que le service de ce type de service auront seulement besoin de prendre en charge les champs Type de service et Portée de la demande de service. Les UA vont quand même effectuer la découverte de DA et envoyer en individuel les messages SLPv2 SrvRqst au DA qui est dans leur portée une fois qu'ils l'auront découvert au lieu de le faire en diffusion groupée.

Les SA vont aussi effectuer la découverte de DA et utiliser une SrvReg SLPv2 pour enregistrer tous leurs services annoncés aux DA SLPv2 qui sont dans leur portée. Ces annonces ne contiendront bien sûr aucune chaîne d'attribut.

Ces SA minimaux pourraient ignorer l'étiquette de langage dans les demandes car les messages SrvRqst ne vont pas contenir d'attributs, et donc aucune chaîne ne sera internationalisée. De plus, toute chaîne de prédicat non nul va échouer à correspondre à une annonce de service sans attribut, de sorte que ces SA n'auront pas à analyser et interpréter de filtre de recherche. Il n'y aura jamais de débordement de messages SrvRqst, SrvRply ou SrvReg de sorte que le traitement de message TCP n'aura pas à être mis en œuvre. Finalement, tous les messages AttrRqst pourraient être éliminés par le SA, car aucun attribut n'est pris en charge.

Appendice C DAAdvert avec des URL arbitraires

En utilisant la découverte active de DA, la SrvRqst a son champ type de service réglé à "service:directory-agent". Les DA vont répondre par une DAAdvert contenant un URL avec le schéma "service:directory-agent:". C'est la même DAAdvert qu'un tel DA enverrait en diffusion groupée dans une annonce de DA non sollicitée.

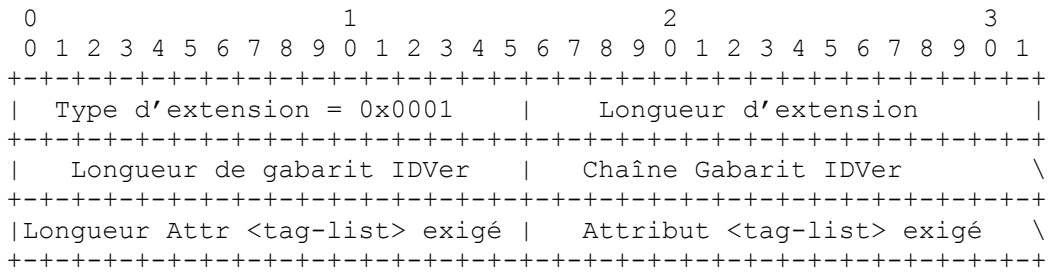
Un UA ou SA qui reçoit une DAAdvert non sollicitée DOIT examiner l'URL pour déterminer si il a un schéma reconnu. Si l'UA ou SA ne reconnaît pas le schéma d'URL de la DAAdvert, celle-ci est éliminée en silence. Le présent document spécifie seulement comment utiliser les URL avec le schéma "service:directory-agent:".

Cela donne la possibilité de compatibilité avec de futures versions de SLP et permet que d'autres services annoncent leur capacité à servir de lieu d'échange des informations de localisation de service.

Par exemple, si LDAPv3 [RFC2251] est utilisé pour l'enregistrement et la découverte de service par un ensemble de systèmes d'extrémité, ceux-ci pourraient interpréter un URL LDAP [RFC2255] pour découvrir passivement le serveur LDAP à utiliser pour cela. Le présent document ne spécifie pas comment cela est fait : les agents SLPv2 sans autre soutien vont simplement éliminer cette DAAdvert.

Appendice D Extensions au protocole SLP

D.1 Option Attribut exigé manquant



Les attributs et le format exigés de la chaîne IDVer sont définis dans [RFC2609].

Si un SA ou DA reçoit une SrvRqst ou un SrvReg qui n'a pas réussi à inclure un attribut exigé pour le type de service exigé (selon le gabarit de service) il PEUT retourner l'extension Attribut exigé en plus de la réponse correspondant au message. L'envoyeur DEVRAIT envoyer le message à nouveau avec un filtre de recherche comportant des attributs énumérés dans l'extension Attribut exigé retournée. De même, l'extension Attribut exigé peut être retournée en réponse à un message SrvDereg qui contient une étiquette d'attribut exigé.

La chaîne Gabarit IDVer est la chaîne de nom et de numéro de version du gabarit de service qui définit l'attribut exigé en question. Il DEVRAIT être inclus, mais peut être omis si un SA ou DA a été individuellement configuré à avoir les "attributs requis".

La <tag-list> Attributs requis NE DOIT PAS inclure de caractères génériques.

Appendice E Remerciements

Le présent document incorpore des idées provenant de travaux sur plusieurs protocoles de découverte, incluant RDP de Perkins et Harjono, et PDS de Michael Day. Nous somme reconnaissants de leurs contributions à Ye Gu et Peter Ford. John Veizades a coopéré à la normalisation du protocole de localisation de service. Les mises en œuvre de Novell, Axis Communications et Sun Microsystems ont contribué de façon significative à rendre ce document plus clair et cohérent.

Appendice F Références

[9594-2] ISO/CEI JTC1/SC 21. "Extensions de certificat". Projet d'amendement DAM 4 à ISO/CEI 9594-2, décembre 1996.

[9594-6] ISO/CEI JTC1/SC 21. "Extensions de certificat". Extensions de certificat DAM 2 à ISO/CEI 9594-6, décembre 1996.

[9594-7] ISO/CEI JTC1/SC 21. "Extensions de certificat". Extensions de certificat DAM 1 à ISO/CEI 9594-7, décembre 1996.

[9594-8] ISO/CEI JTC1/SC 21. "Extensions de certificat". Extensions de certificat DAM 1 à ISO/CEI 9594-8, décembre 1996.

[AppleTalk] S. Gursharan, R. Andrews, et A. Oppenheimer. "Inside AppleTalk". Addison-Wesley, 1990.

[FIPS186] National Institute of Standards et Technology. "Digital signature standard". Technical Report NIST FIPS PUB 186, U.S. Department of Commerce, mai 1994.

[IANA] Numéros d'accès, juillet 1997. ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers.

[RFC1766] H. Alvestrand, "Étiquettes pour l'identification des langues", mars 1995. *(Obsolète, voir* RFC3066, RFC3282)

(P.S.)

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

[RFC2165] J. Veizades et autres, "Protocole de localisation de service", juin 1997. (*MàJ par* RFC2608, RFC2609) *(P.S.)*

[RFC2234] D. Crocker et P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", novembre 1997. (*Obsolète, voir* RFC5234)

[RFC2251] M. Wahl, T. Howes et S. Kille, "Protocole léger d'accès à un répertoire (v3)", décembre 1997.

[RFC2254] T. Howes, "Représentation comme chaîne des filtres de recherche LDAP", décembre 1997. (*Obsolète, voir* RFC4510, RFC4515) *(P.S.)*

[RFC2255] T. Howes, M. Smith, "Format d'URL LDAP", décembre 1997. (*Obsolète, voir* RFC4510, RFC4516) *(P.S.)*

[RFC2279] F. Yergeau, "UTF-8, un format de transformation de la norme ISO 10646", janvier 1998. (*Obsolète, voir* RFC3629) *(D.S.)*

[RFC2365] D. Meyer, "Diffusion groupée sur IP limitée administrativement", juillet 1998. (BCP0023)

[RFC2396] T. Berners-Lee, R. Fielding et L. Masinter, "Identifiants de ressource uniformes (URI) : Syntaxe générique", août 1998. (*Obsolète, voir* RFC3986)

[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 RFC 5226)*

[RFC2609] E. Guttman, C. Perkins, J. Kempf, "Gabarits de service et service : schémas", juin 1999. *(P.S.)*

[RFC2610] C. Perkins, E. Guttman, "Options DHCP pour le protocole de localisation de service", juin 1999. *(P.S.)*

[SMB] Microsoft Networks. SMB File Sharing Protocol Extensions 3.0, Document Version 1.09, novembre 1989.

[Unicode] Unicode Technical Report #8. The Unicode Standard, version 2.1. Technical report, The Unicode Consortium, 1998.

[X.509] CCITT. "L'annuaire : Cadre d'authentification". Recommandation X.509, 1988.

Appendice G. Adresse des auteurs

Erik Guttman
Sun Microsystems
Bahnstr. 2
74915 Waibstadt
Germany
téléphone : +49 7263 911 701
mél : Erik.Guttman@sun.com

Charles Perkins
Sun Microsystems
901 San Antonio Road
Palo Alto, CA 94040
USA
téléphone : +1 650 786 6464
mél : cperkins@sun.com

John Veizades
@Home Network
425 Broadway
Redwood City, CA 94043
USA
téléphone : +1 650 569 5243
mél : veizades@home.net

Michael Day
Vinca Corporation.
1201 North 800 East
Orem, Utah 84097
USA
tél : +1 801 376-5083
mél: mday@vinca.com

Appendice H Déclaration complète de droits de reproduction

Remerciement

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