

Groupe de travail Réseau  
**Request for Comments : 2165**  
 Catégorie : En cours de normalisation  
 Traduction Claude Brière de L'Isle

J. Veizades @Home Network  
 E. Guttman & C. Perkins, Sun Microsystems  
 S. Kaplan  
 juin 1997

## Protocole de localisation de service

### Statut du présent mémoire

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

### Notice de Copyright

Copyright (C) The Internet Society (1997). Tous droits réservés.

### Résumé

Le protocole de localisation de service fournit un cadre adaptable pour la découverte et le choix de services réseau. Avec ce protocole, les ordinateurs qui utilisent l'Internet n'ont plus besoin de beaucoup de configuration statique des services réseau pour les applications fondées sur le réseau. Cela est particulièrement important lorsque les ordinateurs deviennent plus portables, et les utilisateurs moins tolérants ou capables de satisfaire aux demandes de l'administration de système réseau.

## Table des Matières

1. Introduction.....	2
2. Terminologie.....	2
2.1 Conventions de notation.....	3
2.2 Informations de service et représentation de prédicat.....	3
2.3 Langage de spécification .....	4
3. Vue d'ensemble du protocole.....	4
3.1 Transactions du protocole.....	4
3.2 Schémas.....	5
3.3 Définitions d'attribut standard.....	6
3.4 Autorité de désignation.....	6
3.5 Interprétation des réponses de localisation de service.....	6
3.6 Utilisation de TCP, UDP et de la diffusion groupe dans la localisation de service.....	6
3.7 Adaptation de la localisation de service et modes de fonctionnement de diffusion groupée.....	8
4. Format de message général de localisation de service.....	8
4.1 Utilisation des identifiants de transaction (XID).....	9
4.2 Entrées d'URL.....	10
4.3 Blocs d'authentification.....	10
4.4 Durée de vie d'entrée d'URL.....	11
5. Format de message de demande de service.....	12
5.1 Usage de la demande de service.....	13
5.2 Demande de découverte d'agent de répertoire.....	14
5.3 Explication des termes de la grammaire de prédicat.....	14
5.4 Grammaire de prédicat de demande de service.....	15
5.5 Correspondance de chaîne pour les demandes.....	16
6. Format du message de réponse de service.....	16
7. Format du message Demande de type de service.....	17
8. Format du message Réponse de type de service.....	18
9. Format du message d'enregistrement de service.....	19
10. Format du message d'accusé de réception de service.....	21
11. Format du message de désenregistrement de service.....	21
12. Format du message de demande d'attribut.....	22
13. Format du message de réponse d'attribut.....	24
14. Format du message d'annonce d'agent de répertoire.....	25
15. Agents de répertoire.....	25
15.1 Introduction.....	25

15.2 Trouver les agents de répertoire.....	26
16. Découverte et utilisation de la portée.....	27
16.1 Portées protégées.....	27
17. Problèmes de langage et de codage de caractères.....	28
17.1 Problèmes de codage et de chaînes de caractères.....	28
17.2 Chaînes indépendantes du langage.....	29
18. Transactions de localisation de service.....	29
18.1 Connexions de localisation de service.....	29
18.2 Pas d'hypothèse de synchronisme.....	30
18.3 Idempotence.....	30
19. Considérations pour la sécurité.....	30
20. Formats de chaînes utilisés avec les messages de localisation de service.....	30
20.1 Spécification de l'adresse du répondant précédent.....	31
20.2 Définition formelle du schéma "service:".....	31
20.3 Informations d'attribut.....	32
20.4 Spécification d'adresse dans la localisation de service.....	32
20.5 Règles de codage de valeur d'attribut.....	32
21. Exigences du protocole.....	33
21.1 Exigences d'agent d'utilisateur.....	33
21.2 Exigences d'agent de service.....	34
21.3 Exigences pour l'agent de répertoire.....	34
22. Paramètres configurables et valeurs par défaut.....	35
22.1 Agent de service : utilisation d'agent de répertoire prédéfini.....	35
22.2 Intervalles de temporisation.....	36
23. Paramètres non configurables.....	36
24. Remerciements.....	37
Appendice A. Contenu technique de ISO 639:1988 (E/F): "Code pour la représentation des noms de langues".....	37
Appendice B. Certificats SLP.....	37
Appendice C Exemple de déploiement de la sécurité SLP avec MD5 et RSA.....	39
Appendice D. Exemple d'utilisation de certificats SLP par des nœuds mobiles.....	39
Appendice E. Pour approfondir le sujet.....	39
Références.....	39
Adresse des auteurs.....	41

## 1. Introduction

Traditionnellement, les utilisateurs trouvent des services en utilisant le nom d'un hôte du réseau (une chaîne de texte lisible par l'homme) qui est un alias pour une adresse réseau. Le protocole de localisation de service élimine le besoin qu'un usager connaisse le nom d'un hôte réseau qui prend en charge un service. L'usager désigne plutôt le service et fournit un ensemble d'attributs qui décrivent le service. Le protocole de localisation de service permet à l'usager de lier cette description à l'adresse réseau du service.

La localisation de service fournit un mécanisme de configuration dynamique pour les applications dans les réseaux de zone locale. Ce n'est pas un système de résolution mondial pour l'Internet entier ; il est plutôt destiné à servir les réseaux d'entreprise avec des services partagés. Les applications sont modélisées comme des clients qui ont besoin de trouver des serveurs rattachés au réseau d'entreprise à une localisation éventuellement distante. Pour les cas où il y a de nombreux clients et/ou services différents disponibles, le protocole est adapté à l'utilisation des agents de répertoire des environs qui offrent un dépôt centralisé des services annoncés.

## 2. Terminologie

**Agent d'utilisateur (UA)** Processus travaillant au nom de l'utilisateur pour acquérir des attributs et la configuration du service. L'agent d'utilisateur restitue les informations de service des agents de service ou des agents de répertoire.

**Agent de service (SA)** Processus fonctionnant au nom d'un ou plusieurs services pour annoncer les attributs et la configuration du service.

**Information de service** Collection d'attributs et d'informations de configuration associés à un seul service. Les agents de service annoncent les informations de service pour une collection d'instances de service.

- Service** C'est un processus ou système qui fournit une facilité au réseau. L'accès au service lui-même est effectué en utilisant un mécanisme de communication externe au protocole de localisation de service.
- Agent de répertoire (DA)** Processus qui collecte les informations auprès des agents de service pour fournir un seul répertoire des informations de service afin de les centraliser pour un accès efficace par les agents d'utilisateur. Il ne peut y avoir qu'un seul DA présent pour un hôte donné.
- Type de service** Chaque type de service a une chaîne type de service unique. Le type de service définit un gabarit, appelé un "schéma de service", comportant les attributs, les valeurs et le comportement de protocole attendus.
- Autorité de désignation** Agence ou groupe qui catalogue les types de service et attributs donnés. L'autorité de désignation par défaut est l'IANA, l'autorité d'allocation des numéros de l'Internet.
- Mot clé** Chaîne qui décrit une caractéristique d'un service.
- Attribut** Paire de chaînes (classe, liste de valeurs) qui décrit une caractéristique d'un service. La chaîne de valeurs peut être interprétée comme une valeur booléenne, entière ou opaque si elle prend des formes spécifiques (voir le paragraphe 20.5).
- Prédicat** Expression booléenne d'attributs, relations et opérateurs logiques. Le prédicat est utilisé pour trouver des services qui satisfont des exigences particulières. Voir le paragraphe 5.3.
- Alphanumérique** Caractère dans la gamme de 'a' à 'z', 'A' à 'Z', ou '0' à '9'.
- Portée** Collection de services qui constitue un groupe logique. Voir les paragraphes 3.7 et 16.
- Réseau site** Tous les hôtes accessibles au sein du rayon de diffusion groupée de l'agent, qui a par défaut une valeur appropriée pour atteindre tous les hôtes au sein d'un site (voir la section 22). Si le site n'accepte pas la diffusion groupée, le réseau site de l'agent se restreint à un seul sous-réseau.
- URL** Localisateur de ressource universel – voir [6].
- Spécification d'adresse** C'est le mécanisme dépendant du protocole de couche réseau pour spécifier un agent. Pour les systèmes Internet, cela fait partie d'un URL.

## 2.1 Conventions de notation

**CAPS** Les chaînes qui apparaissent en majuscules sont des textes du protocole. Toutes les comparaisons de chaînes sont cependant insensibles à la casse, (voir au paragraphe 5.5). Certaines chaînes sont mises entre guillemets dans le présent document pour indiquer qu'elles devraient être utilisées telles quelles. Les caractères seuls entre des apostrophes sont inclus littéralement.

◇ Les valeurs présentées de cette manière sont décrites à la Section 20. En général, toutes les définitions d'éléments des messages sont décrites à la Section 20 ou immédiatement à la suite de leur première utilisation.

| |, \ \, | | Les messages disposés avec cette notation indiquent un champ de longueur variable.

## 2.2 Informations de service et représentation de prédicat

Les informations de service sont représentées en format texte. L'objectif est que le format soit lisible par l'homme et transmissible via messagerie électronique. La localisation des services réseau est codée comme un localisateur de ressource universel (URL) qui soit lisible par l'homme. Seuls les en-têtes des datagrammes sont codés sous une forme qui n'est pas lisible par l'homme. Les chaînes utilisées dans le protocole de localisation de service ne sont pas terminées par des caractères nuls.

Les prédicats sont exprimés dans une notation booléenne simple en utilisant des mots clés, des attributs, et des connecteurs logiques, comme décrit au paragraphe 5.4.

Les connecteurs et sous-expressions logiques sont présentés dans l'ordre des préfixes, afin que le connecteur vienne en premier et que l'expressions sur laquelle il opère suive.

### 2.3 Langage de spécification

Dans le présent document, plusieurs mots sont utilisés pour signifier les exigences de la spécification [8]. Ces mots sont écrits en majuscules.

**DOIT** Ce mot, ou l'adjectif "exigé", signifie que la définition est une exigence absolue de la spécification.

**NE DOIT PAS** Cette phrase signifie que la définition est une interdiction absolue de la spécification.

**DEVRAIT** Ce mot, ou l'adjectif "recommandé", signifie que, dans certaines circonstances, il peut exister des raisons valables pour ignorer cet élément, mais toutes les implications doivent être comprises et soupesées attentivement avant de choisir un cours différent. Des résultats inattendus peuvent en résulter.

**PEUT** Ce mot, ou l'adjectif "facultatif", signifie que cet élément est un de ceux qui sont admis parmi un ensemble de solutions de remplacement. Une mise en œuvre qui ne comporte pas cette option **DOIT** être prête à interopérer avec une autre mise en œuvre qui comporte cette option.

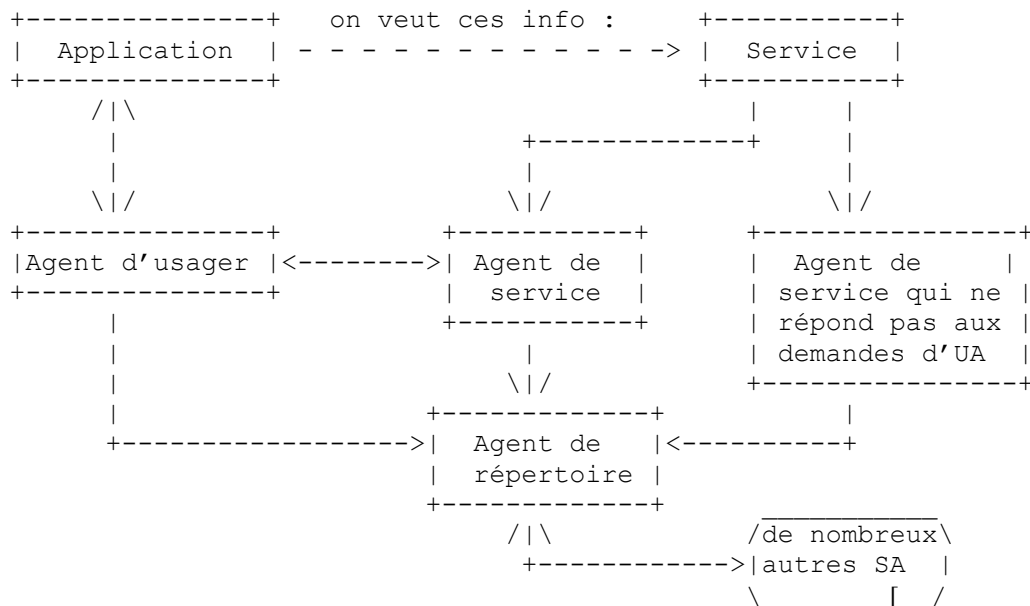
**Éliminer en silence** La mise en œuvre élimine le datagramme sans autre traitement, et sans indiquer d'erreur à l'expéditeur. La mise en œuvre **DEVRAIT** fournir la capacité d'enregistrer l'erreur, incluant le contenu du datagramme éliminé, et, **DEVRAIT** enregistrer l'événement dans un compteur de statistiques.

## 3. Vue d'ensemble du protocole

L'opération de base de la localisation de service est qu'un client tente de découvrir la localisation d'un service. Dans les plus petites installations, chaque service sera configuré de façon à répondre individuellement à chaque client. Dans de plus grandes installations, les services vont enregistrer leurs services auprès d'un ou plusieurs agents de répertoire, et les clients vont contacter l'agent de répertoire pour satisfaire les demandes d'informations de la localisation de service. Les clients peuvent découvrir les tenants et aboutissants d'un agent de répertoire par préconfiguration, DHCP [2], [11], ou en produisant des interrogations à l'adresse de diffusion groupée de découverte de l'agent de répertoire.

### 3.1 Transactions du protocole

Le diagramme ci-dessous illustre les relations qui sont décrites plus loin :



Voici la description des opérations d'un agent d'utilisateur pour trouver des services sur le réseau d'un site. L'agent d'utilisateur n'a pas besoin de configuration pour commencer l'interaction avec le réseau. L'agent d'utilisateur peut acquérir les informations pour construire des prédicats qui décrivent les services qui correspondent aux besoins de l'utilisateur. L'agent d'utilisateur peut bâtir sur la base des informations reçues dans des demandes réseau antérieures pour trouver les informations de service d'annonce des agents de service.

Un agent d'utilisateur va avoir deux façons de fonctionner : si l'agent d'utilisateur a déjà obtenu la localisation d'un agent de

répertoire, l'agent d'utilisateur va lui envoyer une demande en envoi individuel afin de résoudre une demande particulière. L'agent de répertoire va envoyer une réponse en envoi individuel à l'agent d'utilisateur. L'agent d'utilisateur va réessayer une demande à un agent de répertoire jusqu'à ce qu'il obtienne une réponse, de sorte que si l'agent de répertoire ne peut pas servir la demande (disons qu'il n'a pas d'information) il doit retourner une réponse avec des valeurs zéro, éventuellement avec un code d'erreur établi.

Si l'agent d'utilisateur n'a pas connaissance d'un agent de répertoire ou si il n'y a pas d'agent de répertoire disponible sur le réseau de site, un second mode de découverte peut être utilisé. L'agent d'utilisateur envoie en diffusion groupée une demande à l'adresse de diffusion groupée spécifique du service, à laquelle le service qu'il souhaite localiser va répondre. Tous les agents de service qui écoutent sur cette adresse de diffusion groupée vont répondre, pourvu qu'ils puissent satisfaire la demande de l'agent d'utilisateur. Un mécanisme similaire est utilisé pour la découverte d'agent de répertoire ; voir au paragraphe 5.2. Les agents de service qui n'ont pas d'informations pour l'agent d'utilisateur NE DOIVENT PAS répondre.

Lorsque un agent d'utilisateur souhaite obtenir une énumération de TOUS les services qui satisfont à l'interrogation, on utilise une algorithme de retransmission/convergence. L'agent d'utilisateur envoie à nouveau la demande, avec une liste des répondants précédents. Seuls les agents de service qui ne sont pas sur la liste répondent. Une fois qu'il n'y a plus de nouvelle réponse à la demande, l'accumulation des réponses est réputée complète. Selon la longueur de la demande, environ 60 répondants précédents peuvent être énumérés dans un seul datagramme. Si il y a plus de répondants, le mécanisme d'adaptation décrit au paragraphe 3.7 devrait être utilisé.

Bien que le modèle de diffusion groupée/convergence puisse être important pour la découverte de services (tels que les agents de répertoire) il est l'exception plutôt que la règle. Une fois qu'un agent d'utilisateur connaît la localisation d'un agent de répertoire, il va utiliser une transaction de demande/réponse en envoi individuel.

L'agent de service DEVRAIT écouter les demandes en diffusion groupée sur l'adresse de diffusion groupée spécifique du service, et DOIT s'enregistrer auprès d'un agent de répertoire disponible. Cet agent de répertoire va résoudre les demandes provenant des agents d'utilisateur qui sont en envoi individuel en utilisant TCP ou UDP. Cela signifie qu'un agent de répertoire doit d'abord être découvert, en utilisant DHCP, l'adresse de diffusion groupée de découverte de DA, le mécanisme de diffusion groupée décrit ci-dessus, ou la configuration manuelle. Voir au paragraphe 5.2.

Un agent de service qui ne répond pas aux demandes en diffusion groupée ne sera pas utile en l'absence d'agents de répertoire. Certains agents de service peuvent ne pas inclure cette fonctionnalité, si une mise en œuvre très légère est requise.

Si le service devient indisponible, il devrait être désenregistré chez l'agent de répertoire. L'agent de répertoire répond par un accusé de réception à l'enregistrement et au désenregistrement. Les enregistrements de service incluent une durée de vie, et vont finalement arriver à expiration. Les enregistrements de service ont besoin d'être rafraîchis par l'agent de service avant que leur durée de vie ne soit terminée. Si nécessaire, les agents de service peuvent annoncer des URL signés pour prouver qu'ils sont autorisés à fournir le service.

## 3.2 Schémas

Le protocole de localisation de service, conçu comme un moyen pour que les clients accèdent aux ressources qui sont sur le réseau, est une application naturelle pour les localisateurs de ressource universels (URL). Il est prévu qu'en réutilisant la spécification et la technologie d'URL de la Toile mondiale, clients et serveurs soient plus souples et capables d'être écrits en utilisant du code déjà existant. De plus, on espère que les navigateurs seront montés de façon à tirer parti de la similarité du format de localisateur, afin qu'un client puisse formuler de façon dynamique des demandes de services qui sont résolues différemment selon les circonstances.

### 3.2.1 Schéma d'URL "service:"

Le schéma d'URL service: est utilisé par la localisation de service. Il est utilisé pour spécifier une localisation de service. De nombreux types de services seront désignés en incluant un nom de schéma après le nom de schéma "service:". Les types de service sont utilisés par les SA pour enregistrer et désenregistrer les services auprès des DA. Il sont aussi utilisés par les SA et les DA pour retourner des réponses de service aux UA. La définition formelle du schéma d'URL "service:" est au paragraphe 20.2. Le format des informations qui suivent le schéma "service:" devrait suivre d'aussi près que possible la structure et sémantique d'URL telles que formalisées par le processus de normalisation de l'IETF.

Les types de service bien connus sont enregistrés auprès de l'IANA et les gabarits sont disponibles comme RFC. Des types de service privés peuvent aussi être pris en charge.

### 3.3 Définitions d'attribut standard

Les types de service utilisés avec le protocole de localisation de service doivent décrire :

- la chaîne de type de service du service,
- les attributs et les clés,
- les descriptions et interprétations des attributs.

Les types de service non enregistrés auprès de l'IANA utiliseront leur propre chaîne d'autorité de désignation. Le processus d'enregistrement pour les nouveaux types de service est défini dans [13].

Les services qui annoncent un type de service particulier doivent prendre en charge le jeu complet d'attributs normalisés. Ils peuvent prendre en charge des attributs supplémentaires, au delà de l'ensemble normalisé. Les attributs non reconnus DOIVENT être ignorés par les agents d'utilisateur.

Les noms de type de service qui commencent par "x-" sont garantis sans conflit avec tout nom de type de service officiellement enregistré. Il est suggéré que ce préfixe soit utilisé pour les noms de type de service expérimentaux ou privés. De même, les noms d'attribut qui commencent par "x-" sont garantis contre toute utilisation par des noms d'attribut officiellement enregistrés.

Un service d'un certain type de service devrait accepter le protocole de réseautage qui est impliqué par sa définition. Si un type de service peut accepter plusieurs protocoles, les informations de configuration DEVRAIENT être incluses dans les informations d'attribut de type de service. Ces informations de configuration permettront à une application d'utiliser les résultats d'une demande de service et d'une demande d'attribut de se connecter directement à un service.

Voir au paragraphe 20.2.1 le format d'une chaîne de type de service telle qu'utilisée dans le protocole de localisation de service.

### 3.4 Autorité de désignation

L'autorité de désignation d'un service définit la signification du type de service et des attributs enregistrés avec lui et fournis par la localisation de service. L'autorité de désignation elle-même est une chaîne qui identifie une organisation de façon univoque. Si aucune chaîne n'est fournie, l'IANA est désignée par défaut. IANA signifie l'autorité d'allocation des numéros de l'Internet.

Les autorités de désignation peuvent définir des types de service qui sont expérimentaux, propriétaires ou pour utilisation privée. La procédure à utiliser est de créer une chaîne 'unique' d'autorité de désignation et ensuite de spécifier les définitions d'attribut standard comme décrit ci-dessus. Cette autorité de désignation va accompagner l'enregistrement et les interrogations, comme décrit aux sections 5 et 9.

### 3.5 Interprétation des réponses de localisation de service

Les réponses devraient être considérées comme valides au moment de la livraison. Le service peut, cependant, échouer ou changer entre le moment de la réponse et le moment où une application cherche à faire usage du service. L'application qui utilise la localisation de service DOIT être prête à la possibilité que les informations de service fournies soient périmées ou incomplètes. Dans le cas où les informations de service fournies ne permettent pas à l'agent d'utilisateur de se connecter au service comme désiré, la demande de service et/ou la demande d'attribut peut être soumise à nouveau.

Les informations de configuration spécifiques du service (comme le protocole à utiliser) devraient être incluses comme informations d'attribut dans l'enregistrement de service. Ces attributs de configuration seront utilisés par les applications qui interprètent la réponse de localisation de service.

### 3.6 Utilisation de TCP, UDP et de la diffusion groupe dans la localisation de service

Le protocole de localisation de service exige la mise en œuvre des protocoles de transport UDP (sans connexion) et TCP (en mode connexion). Ce dernier est utilisé pour les transferts en vrac, seulement lorsque nécessaire. Les connexions sont toujours initiées par une demande d'un agent ou un enregistrement, et non par un agent de répertoire qui répond. Les agents de service et les agents d'utilisateur utilisent des accès éphémères pour transmettre les informations à l'accès de localisation de service, qui est 427.

Les mécanismes de découverte de localisation de service envoient normalement les messages en diffusion groupée à autant de réseaux d'entreprise que nécessaire pour établir la disponibilité du service. Le protocole va fonctionner dans un environnement de diffusion avec les limitations détaillées au paragraphe 3.6.1.

### 3.6.1 Diffusion groupée ou diffusion

Le protocole de localisation de service a été conçu pour être utilisé dans des réseaux où DHCP est disponible, ou la diffusion groupée est prise en charge à la couche réseau. Pour prendre ce protocole en charge lorsque seule la diffusion est acceptée à la couche réseau, les procédures ci-après peuvent être suivies.

#### 3.6.1.1 Un seul sous-réseau

Si un réseau n'est connecté à aucune couche réseau simple d'autre réseau, la diffusion fonctionnera à la place de la diffusion groupée.

Les agents de service DEVRAIENT et les agents de répertoire DOIVENT écouter les messages de demande de localisation de service en diffusion groupée sur l'accès de localisation de service. Cela permet aux UA qui n'ont pas la capacité de diffusion groupée d'utiliser quand même la localisation de service sur un seul sous-réseau.

#### 3.6.1.2 Plusieurs sous-réseaux

L'agent de répertoire fournit une chambre de compensation centrale des informations pour les agents d'utilisateur. Si le réseau est conçu pour que l'adresse d'un agent de répertoire soit configurée de façon statique avec chaque agent d'utilisateur et agent de service, l'agent de répertoire va agir comme pont pour les informations qui résident sur des sous-réseaux différents. L'adresse de l'agent de répertoire peut être configurée de façon dynamique avec les agents qui utilisent DHCP. L'adresse peut aussi être déterminée par configuration statique.

Une découverte dynamique n'est pas faisable dans un environnement de diffusion avec plusieurs sous-réseaux et la configuration manuelle est difficile ; le déploiement de DA pour servir des entreprises avec plusieurs sous-réseaux va exiger d'utiliser la découverte par diffusion groupée avec plusieurs bonds (c'est-à-dire, un TTL > 1 dans l'en-tête IP).

### 3.6.2 Adresse de diffusion groupée spécifique du service

Ce mécanisme est utilisé de telle sorte que soit minimisé le nombre de datagrammes que reçoit tout agent de service. L'adresse de diffusion groupée générale de localisation de service PEUT être utilisée pour interroger sur tout service, mais on DEVRAIT utiliser l'adresse de diffusion groupée spécifique du service si elle existe.

Si le réseau de site n'accepte pas la diffusion groupée, l'interrogation DEVRAIT alors être diffusée à l'accès de localisation de service. Si, d'un autre côté, le matériel sous-jacent ne prend pas en charge le nombre d'adresses de diffusion groupée nécessaire, l'adresse de diffusion groupée générale de localisation de service PEUT être utilisée. Les agents de service DOIVENT écouter sur cette adresse de diffusion groupée aussi bien que sur les adresses de diffusion groupée spécifiques du service pour les types de service qu'elles annoncent.

Les adresses de diffusion groupées spécifiques d'un service sont calculées par un hachage de chaîne sur la chaîne du type de service. La chaîne de type de service DOIT d'abord être convertie en une chaîne ASCII à partir du jeu de caractère dans lequel elle est représentée, de sorte que le hachage ait un résultat bien défini.

La fonction de hachage de chaîne est modifiée à partir d'un fragment de code attribué à Chris Torek :

```
/* SLPhash retourne une valeur de hachage dans la gamme de 0-1023 pour une chaîne de caractères d'un seul octet, de
longueur spécifiée. */
unsigned long SLPhash (const char *pc, unsigned int length) unsigned long h = 0;
while (length-- != 0) {
    h *= 33;
    h += *pc++;
}
return (0x3FF & h);          /* arrondi à une gamme de 0-1023 */
}
```

Cette valeur est ajoutée à la gamme de base des adresses de découverte spécifiques de service, qui sont allouées par l'IANA. Ce seront 1024 adresses de diffusion groupée contiguës.

### 3.7 Adaptation de la localisation de service et modes de fonctionnement de diffusion groupée

Dans un très petit réseau, avec peu de nœuds, aucun DA n'est requis. Un agent d'utilisateur peut détecter les services par des demandes en diffusion groupée. Les agents de service vont alors leur répondre. De plus, les agents de service qui répondent aux demandes d'utilisateur doivent être utilisés pour rendre disponibles les informations de service. Cela ne s'adapte pas aux environnements où les hôtes et services sont nombreux.

Lorsque on adapte les systèmes de localisation de service aux réseaux de taille intermédiaire, un répertoire central (agent de répertoire) peut être ajouté pour réduire le nombre de messages de localisation de service transmis dans l'infrastructure de réseau. Comme le répertoire central peut répondre à toutes les demandes de service et d'attribut, moins de réponses de service et d'attribut seront nécessaires ; pour la même raison, il n'est pas besoin de différencier les agents de répertoire.

Un site peut aussi atteindre une taille telle qu'il ne soit plus possible d'entretenir un seul répertoire central des informations de service. Dans ce cas, plus d'agents de répertoire sont nécessaires. Les services (et agents de service) annoncés par les divers agents de répertoire sont rassemblés en un groupement logique appelé une "portée".

Tous les enregistrements de service qui ont une portée doivent être enregistrés auprès de tous les DA (au sein du rayon approprié de diffusion groupée) de cette portée qui ont été ou qui seront ultérieurement découverts. Les enregistrements de service qui n'ont pas de portée sont seulement enregistrés auprès des DA sans portée. Les agents d'utilisateur font des demandes de DA dont ils sont configurés à utiliser la portée. Les agents de service DOIVENT s'enregistrer auprès des DA sans portée même si ils sont configurés pour s'enregistrer spécifiquement auprès des DA qui ont une portée ou un ensemble de portées spécifiques. Les agents d'utilisateur PEUVENT interroger les DA sans portée, même si ils sont configurés à utiliser des DA avec une certaine portée. Cela parce que tout DA sans portée aura toutes les informations de service disponibles.

Un agent d'utilisateur avec une portée DEVRAIT toujours utiliser lorsque possible un DA qui prend en charge sa portée configurée plutôt qu'un DA sans portée. Cela va empêcher les DA sans portée d'être sur utilisés et donc de devenir un problème d'adaptation.

Il est possible de configurer spécialement les agents de service pour ne s'enregistrer qu'auprès d'un ensemble spécifique de DA (voir le paragraphe 22.1). Dans ce cas, des services peuvent n'être pas disponibles aux agents d'utilisateurs via tous les agents de répertoire, mais certains administrateurs de réseau peuvent trouver cela approprié.

Il y a donc trois modes de fonctionnement distincts. Le premier n'exige pas d'intervention administrative. Le second requiert seulement que fonctionne un DA. Le dernier demande que tous les DA soient configurés pour avoir une portée et qu'une stratégie cohérente d'allocation des portées aux services soit suivie. Les utilisateurs doivent savoir quelles portées sont appropriées pour leur utilisation. Cet effort administratif va aussi permettre aux utilisateurs et aux applications de découvrir ensuite de façon dynamique les services sans assistance.

Le premier mode (sans DA) est destiné aux LAN. Le second mode (utilisant un ou des DA, mais sans portée) s'adapte bien à un groupe de LAN interconnectés avec un nombre limité d'hôtes. Le troisième mode (avec des DA et des portées) permet au protocole SLP d'être utilisé dans un environnement de campus inter réseaux.

Si des DA avec portées sont utilisés, ils ne vont pas accepter des enregistrements ou demandes sans portée. Les UA qui produisent des demandes sans portée vont découvrir seulement des services sans portée. Ils DEVRAIENT utiliser si possible une portée dans leurs demandes et DEVRAIENT utiliser un DA avec leur portée de préférence à un DA sans portée. Dans un environnement de grand campus, ce serait une mauvaise idée d'avoir des DA sans portée: Ils attirent TOUS les enregistrements et vont donc finalement poser un problème d'adaptation.

Un document de protocole ultérieur décrira les mécanismes de prise en charge d'un protocole de découverte de service pour l'Internet mondial.

## 4. Format de message général de localisation de service

L'en-tête suivant est utilisé dans toutes les descriptions de message ci-dessous et est abrégé en utilisant "en-tête de localisation de service =" suivi par la fonction utilisée.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|  Version  |  Fonction  |                               Longueur  |
+-----+-----+-----+-----+-----+-----+-----+
|O|M|U|A|F| rsvd|  Dialecte  |          Code de langue          |
+-----+-----+-----+-----+-----+-----+-----+
|  Codage de caractères  |                               XID                               |
+-----+-----+-----+-----+-----+-----+-----+

```

Version Ce document de protocole définit la version 1 du protocole de localisation de service.



Fonction Les datagrammes de localisation de service peuvent être identifiés comme leur opération par le champ de fonction. Les valeurs suivantes sont les opérations définies :

Type de message	Abréviation	Valeur de la fonction
Demande de service	SrvReq	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

Longueur Nombre d'octets dans le message, y compris l'en-tête de localisation de service.

O Bit 'Débordement'. Voir à la Section 18 l'utilisation de ce champ.

M Bit 'Monolingue'. Les demandes avec ce bit établi indiquent que l'agent d'utilisateur va seulement accepter des réponses dans le langage (voir la Section 17) qui est indiqué par la demande de service ou d'attribut.

U Bit 'Authentification d'URL présente'. Voir aux paragraphes 4.2, 4.3, 9, et 11 l'utilisation de ce champ.

A Bit 'Authentification d'attribut présente'. Voir aux paragraphes 4.2, 4.3, et 13 l'utilisation de ce champ.

F Si le bit 'F' est établi dans un accusé de réception de service, l'agent de répertoire a enregistré le service comme nouvelle entrée, pas comme une entrée mise à jour.

rsvd DOIT être zéro.

Dialecte Les étiquettes de dialecte seront utilisées pas de futures versions du protocole de localisation de service pour indiquer une variante de vocabulaire utilisée. Ce champ est réservé et DOIT être réglé à 0 pour la compatibilité avec les futures versions du protocole de localisation de service.

Code de langue Les chaînes qui suivent dans le reste du message sont à interpréter dans le langage codé (voir la Section 17 et l'appendice A) dans ce champ.

Codage de caractères Les caractères qui constituent les chaînes dans le reste du message peuvent être codées selon tout codage normalisé (voir au paragraphe 17.1).

Identifiant de transaction (XID) Le champ XID (ID de transaction) permet au demandeur de faire correspondre les réponses aux demandes individuelles (voir au paragraphe 4.1).

Note : Chaque fois qu'il y a un bloc d'authentification d'attribut, il y aura aussi un bloc d'authentification d'URL. Donc, c'est une erreur d'avoir le bit 'A' établi sans avoir aussi le bit 'U' établi.

#### 4.1 Utilisation des identifiants de transaction (XID)

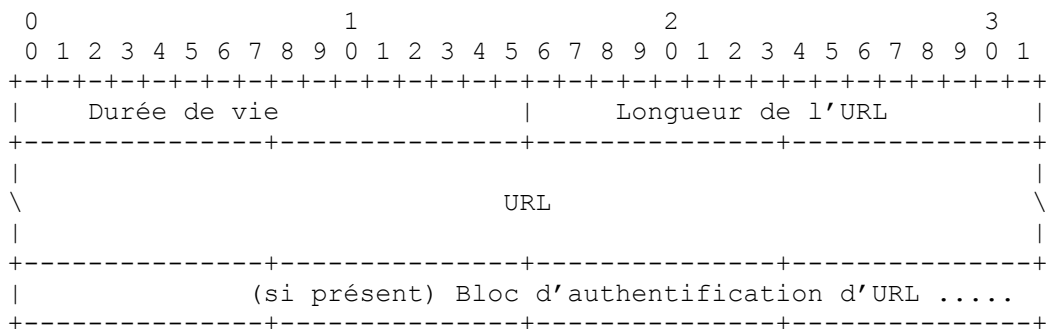
La retransmission est utilisée pour s'assurer de transactions fiables dans le protocole de localisation de service. Si un agent d'utilisateur ou un agent de service envoie un message et ne reçoit pas la réponse attendue, le message sera envoyé à nouveau. La retransmission du même datagramme de localisation de service ne devrait pas contenir un XID mis à jour. Il est assez possible que la demande d'origine ait atteint le DA ou SA, mais que la réponse ait échoué à atteindre le demandeur. Utiliser le même XID permet au DA ou SA de mettre en antémémoire sa réponse à la demande d'origine et de la renvoyer, si une demande dupliquée arrive. Ces informations en antémémoire ne devraient être détenues que très brièvement (CONFIG\_INTERVAL\_0). Tout enregistrement ou désenregistrement auprès d'un agent de répertoire, ou changement des informations de service chez un SA, devrait purger cette antémémoire afin que les informations retournées au client soient toujours valides.

Le demandeur crée le XID à partir d'un germe initial aléatoire et l'incrémente de un pour chaque demande qu'il fait. Les XID reviendront finalement à zéro et continueront de s'incrémenter à partir de là.

Les agents de répertoire utilisent les valeurs de XID dans leurs annonces de DA pour indiquer leur état (voir au paragraphe 15.2).

#### 4.2 Entrées d'URL

Lorsque des URL sont enregistrés, ils ont une durée de vie et une longueur, et peuvent être authentifiés. Ces valeurs sont associées à l'URL pour la durée de l'enregistrement. L'association est appelée une "entrée d'URL", et a le format suivant :



Durée de vie Durée pendant laquelle l'enregistrement est valide, en l'absence d'enregistrements ou désenregistrement ultérieur.

Longueur de l'URL Mesurée en octets et < 32 768.

Bloc d'authentification d'URL (si présent) un authentifiant horodaté (paragraphe 4.3)

L'URL se conforme à la RFC1738 [6]. Si le bit 'U' est établi dans l'en-tête du message, l'URL est suivi d'un bloc d'authentification d'URL. Si le schéma utilisé dans l'URL n'a pas une représentation standard, l'exigence minimale est :

```
service:<srvtype>://<addr-spec>
```

"service" est le schéma d'URL de toute information de localisation de service incluse dans les enregistrements de service et réponses de service. Chaque entrée d'URL contient le nom de schéma service:<srvtype>. Elle peut aussi inclure une <addr-spec> sauf dans le cas d'une réponse à une demande de type de service (voir la Section 7).

### 4.3 Blocs d'authentification

Les blocs d'authentification sont utilisés pour authentifier les enregistrements et désenregistrements de services. Les URL sont enregistrés avec un bloc d'authentification d'URL pour conserver les informations d'authentification dans l'entrée d'URL pour les utilisations ultérieures par les agents d'utilisateur qui reçoivent une réponse de service contenant l'entrée d'URL. Les attributs de service sont enregistrés avec un bloc d'authentification d'attribut. Les deux blocs d'authentification ont le format illustré ci-dessous.

Si un enregistrement de service est accompagné d'une authentification qui peut être validée par le DA, le DA DOIT valider tous les désenregistrements de service suivants, afin que des entités non autorisées ne puissent pas invalider de tels services enregistrés. De même, si un enregistrement de service est accompagné d'un bloc d'authentification d'attribut qui peut être validé par le DA, celui-ci DOIT valider tous les enregistrements d'attribut suivants, afin que des entités non autorisées ne puissent pas invalider de tels attributs enregistrés.

Pour éviter des attaques en répétition qui utilisent des désenregistrements précédemment validés, le message de désenregistrement ou d'enregistrement d'attribut doit contenir un horodatage qui sera utilisé par le DA. Pour éviter des attaques en répétition qui utilisent des enregistrements précédemment validés pour annuler un désenregistrement valide, les enregistrements doivent aussi contenir un horodatage.

Un bloc d'authentification a le format suivant :



Horodatage Valeur de 64 bits formatée comme spécifié par le protocole de l'heure du réseau (NTP) [16].

Descripteur de structure de bloc (BSD) Valeur qui décrit la structure de l'authentifiant. La seule valeur actuellement définie est 1, pour Identifiant d'objet.

Longueur C'est la longueur de l'authentifiant.

Authentifiant structuré Spécification d'algorithme, et données d'authentification produites par l'algorithme. L'authentifiant structuré contient une signature numérique des informations authentifiées. Il contient des informations suffisantes pour déterminer l'algorithme à utiliser et les clés à choisir pour vérifier la signature numérique. La signature numérique est calculée sur le flux de données ordonné suivant :

CODAGE DE CARACTÈRE DE L'URL	(2 octets dans l'ordre des octets du réseau)
DURÉE DE VIE	(2 octets dans l'ordre des octets du réseau)
LONGUEUR DE L'URL	(2 octets dans l'ordre des octets du réseau)
URL	(n octets)
HORODATAGE	(8 octets en format SNTP [16])

Lors de la production d'un bloc d'authentification d'URL, les données d'authentification produites par l'algorithme identifié dans l'authentifiant structuré sont calculées sur le flux de données ordonné suivant :

CODAGE DE CARACTÈRE D'ATTRIBUT	(2 octets dans l'ordre des octets du réseau)
LONGUEUR DES ATTRIBUTS	(2 octets dans l'ordre des octets du réseau)
ATTRIBUTS	(n octets)
HORODATAGE	(8 octets en format SNTP [16])

Chaque entité de protocole de localisation de service (agent d'utilisateur, agent de service, ou agent de répertoire) qui est configuré pour être utilisé avec des portées protégées DEVRAIT mettre en œuvre "md5WithRSAEncryption" [4] et être capable de l'associer avec la valeur de BSD = 1.

Dans le cas où la valeur BSD = 1 et où l'OID "md5WithRSAEncryption" est choisi, l'authentifiant structuré va commencer avec le codage distinctif (DER) ASN.1 [9] pour "md5WithRSAEncryption", qui a comme valeur les octets (MSB en premier en hexadécimal) :

"30 0d 06 09 2a 86 48 86 f7 0d 01 01 04 05 00"

Ceci est alors immédiatement suivi par un codage distinctif ASN.1 (comme une "chaîne binaire") du chiffrement RSA (en utilisant la clé privée de la portée) d'une chaîne binaire consistant en l'OID pour "MD5" enchaîné avec le résumé MD5 [22] du message calculé sur les champs ci-dessus. La construction exacte de l'OID MD5 et du résumé se trouvent dans la RFC1423 [4].

#### 4.4 Durée de vie d'entrée d'URL

Le champ Durée de vie est réglé au nombre de secondes pendant lequel la réponse peut être gardée en antémémoire par tout agent. Une valeur de 0 signifie que les informations ne doivent pas être placées en antémémoire. Les agents d'utilisateur PEUVENT mettre en antémémoire les informations de service, mais si ils le font, ils doivent fournir un moyen pour que les applications purgent ces informations de l'antémémoire et produisent la demande directement sur le réseau.

Les services devraient être enregistrés auprès des DA avec une durée de vie, la valeur suggérée étant CONFIG\_INTERVAL\_1. Le service doit être réenregistré avant que cet intervalle soit écoulé, sinon l'annonce de service ne sera plus disponible. Donc, les services qui disparaissent et manquent à se désenregistrer sont finalement désenregistrés automatiquement.

## 5.

### Format de message de demande de service

La demande de service est utilisée pour obtenir des URL d'un agent de répertoire ou des agents de service.

Le format de la demande de service est comme suit :

```

0          1          2          3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   En-tête de localisation de service (fonction = SrvReq)   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|Long. de chaîne liste rép. préc| <Spéc. adr. rép. précédents> |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                                               |
\   <Spécification d'adresse du répondant précédent>         \
|                                                               |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Longueur de chaîne de prédicat| Demande de service <prédicat> |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                                               |
\                               Demande de service <prédicat>, suite \
|                                                               |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Si un UA produit une demande qui va résulter en une réponse trop longue, le SA ou DA va retourner une réponse abrégée (dans un datagramme dont la taille est celle de la MTU du site) qui a le bit fanion 'Débordement' établi. L'UA doit alors produire à nouveau la demande en utilisant TCP.

La <Spécification d'adresse des répondants précédents> est décrite à la Section 7 et au paragraphe 20.1.

Après le redémarrage de l'agent d'utilisateur (disons, après le réamorçage d'un système, le chargement du noyau réseau) les demandes de service devraient être retardées d'un délai aléatoire à répartition uniforme au sein d'un intervalle d'une seconde centrée sur une valeur de retard configurée (par défaut, CONFIG\_INTERVAL\_4).

La demande de service permet à l'agent d'utilisateur de spécifier le type de service du service et d'un prédicat dans un langage spécifique. La forme générale d'une demande de service est indiquée ci-dessous :

```
<srvtype>[.<na>]/[<portée>]/[<où>]/
```

La ponctuation est nécessaire même lorsque les champs sont omis.

- <srvtype> se réfère au type de service. Pour chaque type de service disponible, il y a une chaîne unique de nom de type de service. Voir au paragraphe 20.2.1.
- <na> est l'autorité de désignation. Cette chaîne détermine l'interprétation sémantique des informations d'attribut dans la partie <où> de la demande de service.
- <portée> est une chaîne utilisée pour resserrer la gamme d'interrogations. Portée est déterminé administrativement, à un certain site. Elle ne se rapporte pas nécessairement à la topologie du réseau (voir la Section 16). Ne pas remplir ce champ signifie que la demande ne peut être satisfaite que par des annonces de service sans portée.
- La chaîne <où> est la clause Où de la demande. Elle contient une interrogation qui permet la sélection des instances de service auxquelles l'agent d'utilisateur est intéressé. L'interrogation inclut des attributs, des opérateurs booléens et des relations. (Voir au paragraphe 5.3.)

Dans le cas d'une demande de service en diffusion groupée, une liste des répondants précédents est envoyée. Cette liste va empêcher ceux qui sont sur la liste de répondre, pour être sûr que les réponses provenant d'autres sources ne sont pas étouffées. La demande est envoyée en diffusion groupée de façon répétée (avec un intervalle d'attente recommandé de CONFIG\_INTERVAL\_2) jusqu'à ce qu'il n'y ait plus de nouvelles réponses, ou que soit écoulé un certain temps (CONFIG\_INTERVAL\_3). Différentes valeurs de temporisation sont appliquées à une demande de service utilisée pour la découverte d'agent de répertoire, voir au paragraphe 5.2.

Afin qu'une demande réussisse à trouver les informations enregistrées correspondantes, les conditions suivantes doivent être remplies :

1. Le résultat doit avoir le même type de service que la demande.
2. Il doit avoir la même autorité de désignation.
3. Il doit avoir la même portée. (Si la portée de la demande est omise, la demande va seulement correspondre aux services qui ont été enregistrés sans portée. Noter qu'une demande avec une portée VA correspondre à tous les services sans portée).
4. Les conditions spécifiées dans la clause Où doivent correspondre aux attributs et mots clés enregistrés pour le service.

### 5.1 Usage de la demande de service

L'agent d'utilisateur peut former des demandes de service en utilisant une connaissance préconfigurée des attributs d'un type de service. Il peut aussi produire des demandes d'attribut pour obtenir les valeurs d'attributs pour un type de service avant de produire des demandes de service (voir la Section 13). Ayant obtenu les attributs qui décrivent une sorte particulière de service à partir d'une demande d'attribut, ou en utilisant la connaissance configurée des attributs d'un service, l'agent d'utilisateur peut construire un prédicat qui décrit les besoins de service de l'utilisateur.

Les demandes de service peuvent être envoyées directement à un agent de répertoire. Supposons qu'une imprimante qui accepte le protocole lpr soit nécessaire au douzième étage avec un accès sans restriction et qu'elle imprime 12 pages à la minute. Supposons de plus qu'une demande d'attribut indique qu'il y a une imprimante au 12<sup>ème</sup> étage, une imprimante qui imprime 12 pages par minute, et une imprimante qui offre un accès illimité. Pour vérifier si il s'agit de la même imprimante, produire la requête suivante :

```
lpr//(& (PAGES PAR MINUTE==12)
      (ACCÈS_ILLIMITÉ)
      (LOCALISATION==12ème ÉTAGE))/
```

Supposons qu'il n'y a pas une telle imprimante. L'agent de répertoire répond par une Réponse de service avec 0 dans le nombre de réponses et pas de valeur de réponse.

L'agent d'utilisateur essaye alors une interrogation moins restrictive pour trouver une imprimante, en utilisant le 12<sup>ème</sup> étage comme critère "où".

```
lpr//(LOCALISATION==12ème ÉTAGE)/
```

Dans ce cas, il y a maintenant une seule réponse :

```
URL retourné : service:lpr://igore.wco.ftp.com:515/draft
```

La spécification d'adresse pour l'imprimante est : igore.wco.ftp.com:515, contenant le nom de l'hôte qui gère l'imprimante demandée. Les fichiers seront imprimés en différé sur cet accès de cet hôte. Le mot 'draft' se réfère au nom de la file d'attente de l'imprimante que le serveur lpr prend en charge.

En l'absence d'un agent de répertoire, la demande ci-dessus pourrait être en diffusion groupée. Dans ce cas, elle serait envoyée à l'adresse de diffusion groupée spécifique du service pour "service:printer" et non à l'agent de répertoire. Les agents de service qui peuvent satisfaire le prédicat vont répondre. Les agents de service qui ne peuvent pas prendre en charge le jeu de caractères de la demande DOIVENT retourner JEU\_DE\_CHARACTERES\_NON\_COMPRIS dans la SrvRply. Dans toutes les autres circonstances, les agents de service qui ne peuvent pas satisfaire la réponse n'envoient pas de réponse du tout.

La seule façon dont l'agent d'utilisateur peut être sûr qu'il n'y a pas de service qui corresponde à l'interrogation est de réessayer la demande (CONFIG\_INTERVAL\_8). Si aucune réponse ne vient, l'agent d'utilisateur abandonne et suppose qu'il n'y a pas de telles imprimantes.

Une autre forme d'interrogation est une plus simple interrogation 'join'. Sa syntaxe n'a pas de parenthèses ou d'opérateur logique. Chaque terme est conjoint (ajoutés ensemble). On en aura un exemple en réécrivant l'interrogation précédente :

```
lpr//PAGES PAR MINUTE==12,
      ACCÈS_ILLIMITÉ,
      LOCALISATION==12ème ÉTAGE/
```

### 5.2 Demande de découverte d'agent de répertoire

Normalement, une demande de service retourne une réponse de service. La seule exception est une demande de service pour le type de service "agent-de-répertoire". Cette demande de service reçoit en réponse une annonce de DA.

Sans connaissance configurée d'un agent de répertoire (DA), un agent d'utilisateur ou de service utilise une demande de service pour découvrir un DA. (Voir au paragraphe 15.1 les mécanismes par lesquels un client peut être configuré pour avoir la connaissance d'un DA). Une telle demande de service utilisée pour la découverte d'agent de répertoire comporte un prédicat de la forme :

```
agent-de-répertoire///
```

Cette interrogation est toujours envoyée à l'adresse de diffusion groupée de découverte d'agent de répertoire. Le type de service d'un agent de répertoire est "agent-de-répertoire", donc, c'est le type de service utilisé dans la demande. Aucune portée n'est incluse dans la demande, de sorte que tous les agents de répertoire vont répondre. C'est la seule demande qui omet une portée à laquelle tous les agents de répertoire DOIVENT répondre. Normalement, un agent de répertoire avec une portée NE répond QU'aux demandes qui ont cette portée. Aucune autorité de désignation n'est incluse, de sorte que "IANA" est supposé. On veut atteindre tous les agents de répertoire disponibles. Si la portée était fournie, seuls les DA qui acceptent cette portée répondraient.

Des réponses aux annonces de DA peuvent arriver de différentes sources, de forme similaire à :

```
URL retourné : service:directory-agent://slp-resolver.catch22.com
Portée retournée : COMPTABILITE
URL retourné : service:directory-agent://204.182.15.66
Portée retournée : CONCIERGERIE
```

Le format d'annonce de DA est défini à la Section 14.

Si le but est simplement de découvrir un agent de répertoire, la première réponse va le faire. Si le but est, cependant, de découvrir tous les DA accessibles, la demande doit être retransmise après un intervalle (la durée recommandée est CONFIG\_INTERVAL\_5). Cette demande retransmise va inclure une liste des DA qui ont déjà répondu. Voir la Section 7 et le paragraphe 20.1. Les agents de répertoire qui reçoivent la demande ne vont répondre que si ils ne sont pas sur cette liste. Après qu'il n'y a plus de nouvelle réponse, tous les DA sont supposés avoir été découverts.

Si un DA manque à répondre après CONFIG\_INTERVAL\_6 secondes, l'agent d'utilisateur ou de service devrait utiliser un DA différent. Les adresses de DA peuvent être mises en antémémoire à partir des tentatives précédentes de découverte, préconfigurées, ou en utilisant DHCP (voir au paragraphe 15.2). Si aucun de ces DA ne répond, la découverte de DA devrait être utilisée pour trouver un nouveau DA. Seulement après CONFIG\_INTERVAL\_7 secondes, on devrait supposer qu'aucun DA n'existe et on devrait utiliser les demandes de service fondées sur la diffusion groupée.

### 5.3 Explication des termes de la grammaire de prédicat

Un prédicat a une structure simple, qui dépend de parenthèses, virgules et barres obliques pour délimiter les éléments. Des exemples de bon usage sont donnés dans le présent document. Les termes utilisés dans la grammaire sont les suivants :

prédicat : Placé dans une demande de service, ceci est interprété par un agent de service ou un agent de répertoire pour déterminer quelles informations retourner.

portée : Si elle est absente dans une demande de service, la demande va correspondre seulement aux services enregistrés sans portée. Si elle est présente, seuls les services enregistrés sous cette portée ou sont sans portée vont satisfaire la demande.

clause où : Cela détermine quels services satisfait la demande. Une clause où vide va satisfaire tous les services. La demande sera limitée aux services qui ont le type de service spécifié, de sorte que la clause où n'est pas le seul facteur pour collecter les services qui satisfont la demande.

liste où : La liste où est une expression logique. Elle peut être une seule expression, une disjonction ou une conjonction. Une seule expression doit s'appliquer pour que la clause où corresponde. Une disjonction correspond si une expression dans la liste OU correspond. Une conjonction ne correspond que si tous les éléments dans la liste ET correspondent.

Note : Il n'y a pas d'opérateur de négation logique: Cela parce que il n'y a pas de notion de retourner "tout sauf" qui corresponde à un critère donné.

Une liste où peut être incorporée et complexe. Par exemple, ce qui suit exige que trois sous expressions doivent être vraies :

```
(& (| <query-item> <query-item>
  <query-item>
  (& <query-item> <query-item> <query-item>)
)
```

Remarquer que les espaces, tabulations ou retours chariot peuvent être ajoutés n'importe où en dehors des éléments

d'interrogation (*query-item*). Chaque liste a deux éléments ou plus en elle, et les listes peuvent être incorporées. Les services qui satisfont l'expression logique entière correspondent à la clause\_où.

Des expressions corrompues devraient être tolérées. Elles sont équivalentes à <query-item>.

query-item : Un élément d'interrogation a la forme :

```
'( <attr-tag> <comp-op> <attr-val> )'
```

ou

```
'( <mot-clé> )'
```

Des exemples de ceci pourraient être :

```
(UN ATTRIBUT == UNE VALEUR)
(RÉSERVÉ)
(LONGUEUR DE FILE D'ATTENTE ≤ 234)
```

query-join : Le query-join est une liste, délimitée par des virgules, de conditions que le service doit satisfaire afin de correspondre à l'interrogation. Les éléments sont considérés comme étant logiquement conjoints. D'où le query-join :

```
ATTR1=VALUE1, KEYWORD1, KEYWORD2, ATTR2>=34
```

est équivalent à la liste\_où :

```
(& (ATTR1=VALUE1) (KEYWORD1) (KEYWORD2) (ATTR2>=34))
```

Le query-join ne peut pas être mélangé avec une liste\_où. Il est donné comme mécanisme pratique pour fournir une déclaration des conditions nécessaires sans construire une expression logique.

#### 5.4 Grammaire de prédicat de demande de service

Les demandes de services peuvent précisément décrire les services dont elles ont besoin en incluant un prédicat au corps de la demande. Ce prédicat doit être construit conformément à la grammaire ci-dessous :

```
<prédicat> ::= <srvtype>['.<na>']/'<portée>'/'<où>/'
```

```
<srvtype> ::= chaîne représentant le type de service. Seuls sont permis les caractères alphanumériques, '+', et '-'.
```

```
<na> ::= chaîne représentant l'autorité de désignation. Seuls sont permis les caractères alphanumériques, '+', et '-'. Si ce champ est omis, "IANA" est alors supposé.
```

```
<portée> ::= chaîne représentant la portée d'agent de répertoire. '/', ',' (virgule) et '!' ne sont pas permis dans cette chaîne. Les portées "LOCAL" et "DISTANT" sont réservées.
```

```
<attr-tag> ::= nom de classe d'un attribut d'un certain type de service. Cette étiquette ne peut pas inclure les caractères suivants : '(', ')', ',', '=', '!', '>', '<', '/', '*', sauf avec un échappement (voir le paragraphe 17.1.)
```

```
<mot-clé> ::= nom de classe d'un attribut qui n'aura pas de valeurs. Cette chaîne a les mêmes limites que le <attr-tag>, sauf que les espaces internes au mot clé sont illégaux.
```

```
<où> ::= <où-tout> | <liste-où> | <query-join>
```

```
<où-tout> ::= C'est RIEN, ou espace.
```

```
<liste-où> ::= '(' '&' <liste-où> <query-list> ')' | '(' '|' <liste-où> <query-list> ')' | '(' <mot-clé> ')' '(' <attr-tag> <comp-op> <attr-val> ')'
```

```
<query-list> ::= <liste-où> | <liste-où> <query-list>
```

```
<query-join> ::= <mot-clé> | <join-item> | <query-join> ',' <mot-clé> | <query-join> ',' <join-item>
```

```
<join-item> ::= <attr-tag> <comp-op> <attr-val>
```

```
<comp-op> ::= "!=" | "==" | "<" | "<=" | ">" | ">="
```

```
<attr-val> ::= toute chaîne (voir au paragraphe 20.5 les façons dont les attr-val sont interprétées). Les chaînes de valeurs ne doivent pas contenir '/', ',', '=', '<', '>', ou '*' sauf avec échappement (voir au paragraphe 17.1.). '(' et ')' peuvent être utilisés dans les valeurs d'attribut pour les besoins du codage des valeurs binaires. Les codages binaires (voir le paragraphe 20.5) peuvent inclure les caractères réservés ci-dessus.
```

#### 5.5 Correspondance de chaîne pour les demandes

Toutes les chaînes sont insensibles à la casse, par rapport à la correspondance de chaînes pour les interrogations. Tous les

blancs précédents ou suivants ne devraient pas être considérés dans une mise en correspondance, mais les blancs internes à une chaîne sont pertinents.

Par exemple, " Certaine Chaîne " correspond à "CERTAINE CHAINE", mais pas "certaine chaîne".

La mise en correspondance de chaîne ne peut être effectuée que sur les mêmes jeux de caractères. Si une demande ne peut pas être satisfaite à cause d'un manque de prise en charge du jeu de caractères de la demande, il est retourné une erreur JEU\_DE\_CARACTÈRES\_NON\_COMPRIS.

Les comparaisons de chaînes (en utilisant des opérateurs de comparaison tels que '<' ou l'enregistrement) n'utilisent aucune règle spécifique de langage. L'ordre suit strictement la valeur de caractère, c'est-à-dire "0" < "A" est vrai lorsque le jeu de caractères est l'US-ASCII, car "0" a la valeur 48 et "A" a la valeur 65.

Le caractère spécial '\*' peut précéder ou suivre une chaîne afin de permettre une correspondance de sous-chaîne. Si '\*' précède une chaîne, il correspond à toute valeur d'attribut qui se termine par la chaîne. Si la chaîne se termine par un '\*', il correspond à toute valeur d'attribut qui commence par la chaîne. Finalement, si une chaîne commence et se termine par le caractère '\*', la chaîne va correspondre à toute valeur d'attribut qui contient la chaîne.

Exemples :

"bob\*" correspond à "bob", "bobcat", et "bob et sue"

"\*bob" correspond à "bob", "bigbob", et "sue et bob"

"\*bob\*" correspond à "bob", "bobcat", "bigbob", et "a bob I know"

La correspondance de chaîne est effectuée après que les séquences d'échappement ont été substituées. Voir la Section 17 et les paragraphes 5.3 et 17.1.

## 6. Format du message de réponse de service

Le message de réponse de service a le format suivant :

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|           En-tête de localisation de service (fonction = SrvRply)           |
+-----+-----+-----+-----+-----+-----+-----+-----+
|           Code d'erreur           |           Compte d'entrées d'URL           |
+-----+-----+-----+-----+-----+-----+-----+
|                                     <Entrée d'URL 1> ...                   |
+-----+-----+-----+-----+-----+-----+-----+
|                                     .                                       |
\                                     .                                       \
|                                     .                                       |
+-----+-----+-----+-----+-----+-----+-----+
|                                     <Entrée d'URL N> ...                   |
+-----+-----+-----+-----+-----+-----+-----+

```

Chaque message Réponse de service est composé d'une liste d'entrées d'URL.

Le code d'erreur peut avoir une des valeurs suivantes :

0 Succès

LANGAGE\_NON\_ACCEPTÉ

Un SA ou DA retourne cette erreur lorsque une demande est reçue d'un UA qui est dans un langage pour lequel il n'y a pas d'informations de service enregistrées et où la demande est arrivée avec le bit Monolingue établi. Voir la Section 17.

ERREUR\_D'ANALYSE\_DE\_PROTOCOLE

Un SA ou DA retourne cette erreur lorsque une SrvRply est reçue qui ne peut pas être analysé ou que les longueurs de chaînes déclarées dépassent le message.

PORTÉE\_NON\_ACCEPTÉE

Un DA va retourner cette erreur si il reçoit une demande qui a une portée non acceptée par le DA. Un SA ne retournera pas cette erreur ; il va simplement ne pas répondre à la demande en diffusion groupée.



**JEU\_DE\_CHARACTERES\_NON\_COMPRIS**

Si le DA ou SA reçoit une demande ou enregistrement dans un jeu de caractères qu'il ne prend pas en charge, il va retourner cette d'erreur.

Chaque <Entrée\_d'URL> dans la liste a la forme définie au paragraphe 4.2. Les entrées d'URL dans la réponse n'ont pas de délimiteurs entre eux, autres que les champs de longueur. Les champs de longueur d'URL indiquent où les chaînes d'URL se terminent. Si la présence d'un bloc d'authentifiant d'URL est signalée par le bit 'U', la longueur du bloc authentifiant est déterminée par les informations au sein du bloc comme exposé au paragraphe 4.3. Un agent d'utilisateur PEUT utiliser le bloc d'authentification pour déterminer si l'agent de service qui annonce l'URL est, en fait, autorisé à offrir le service indiqué. Si, dans une liste d'entrées d'URL, certains des URL indiquent des services qui sont dans des portées protégées (voir au paragraphe 16.1) alors que d'autres URL qui sont dans la liste indiquent des services qui ne sont pas dans des portées protégées, ces derniers doivent quand même avoir des blocs d'authentification, mais la longueur de l'authentifiant est donnée à zéro, et aucune authentification n'a besoin d'être faite.

## 7. Format du message Demande de type de service

La demande de type de service est utilisée pour déterminer tous les types de services acceptés sur un réseau.

La demande devrait être envoyée directement au DA (bien qu'elle puisse aussi être envoyée à l'adresse générale de localisation de service en diffusion groupée) afin de trouver tous les services disponibles sur le réseau de site (qui sont annoncés par les agents de répertoire et les agents de service). Si aucun DA n'est disponible, l'agent d'utilisateur PEUT produire plus d'une demande pour s'assurer que toutes les réponses ont été reçues. Dans chaque demande suivante, l'agent d'utilisateur inclut les types de services dont il a connaissance. Lorsque aucune nouvelle réponse n'arrive dans les CONFIG\_INTERVAL\_3 de la demande, l'agent d'utilisateur peut supposer qu'il a acquis un jeu complet de types de service disponibles.

Le format d'une demande de type de service est :

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
| En-tête de localisation de service (fonction = SrvTypeRqst) |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Longueur de chaîne de rép. préc|<Spec d'adr de répondant préc.>|
+-----+-----+-----+-----+-----+-----+-----+-----+
|                               |                               |
| \   <Spécification des adresses des répondants précédents>   \
|                               |                               |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Longueur d'autorité de désignat| <Chaîne autorité de désign.> |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                               |                               |
| \           <Chaîne d'autorité de désignation>, suite           \
|                               |                               |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Longueur de chaîne Portée   |           <Chaîne Portée>       |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                               |                               |
| \           <Chaîne Portée> suite                               \
|                               |                               |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Noter que <Spécification des adresses des répondants précédents> est une liste délimitée par des virgules. (Voir au paragraphe 20.1.) Le champ 'Longueur de la liste des répondants précédents' indique la longueur de la chaîne de la liste délimitée par des virgules. Une liste des répondants précédents avec 3 éléments prend la forme :

```
<addr-spec>,<addr-spec>,<addr-spec>
```

L'autorité de désignation, si elle est incluse, va limiter les réponses aux demandes de type de service aux types de service qui ont l'autorité de désignation spécifiée. Si ce champ est omis (c'est-à-dire, si le champ Longueur est zéro) l'autorité de désignation par défaut ("IANA") est supposée. Si le champ Longueur est -1, les types de service provenant de toutes les

autorités de désignation sont demandés.

Le champ Chaîne Portée, si il est inclus, va limiter les réponses aux types de service qui ont la portée spécifiée ou sont sans portée. Si ce champ est omis, tous les types de service (provenant de l'autorité de désignation spécifiée) sont retournés.

## 8. Format du message Réponse de type de service

La réponse de type de service a le format suivant :

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   En-tête de localisation de service (fonction = SrvTypeRply) |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|           Code d'erreur           |           Nombre de types de service |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     |                                     |
\                                     <type de service élément 1>          \
|                                     |                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     |                                     |
|                                     . . .                               |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     |                                     |
\                                     <type de service élément N>          \
|                                     |                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Le format d'un élément de type de service est comme suit :

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|Long. de chaîne type de service|   <Chaîne type de service>           |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     |                                     |
\                                     <Chaîne Type de service> suite      \
|                                     |                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

Le code d'erreur peut avoir une des valeurs suivantes :

0 Succès

### ERREUR\_D'ANALYSE\_DU\_PROTOCOLE

Un SA ou DA retourne cette erreur lorsque une SrvTypeRqst est reçue qui ne peut pas être analysée.

### PORTÉE\_NON\_ACCEPTÉE

Un DA qui est configuré pour avoir une portée va retourner cette erreur si il reçoit une SrvTypeRqst qui est réglée pour avoir une portée qu'il ne prend pas en charge. Un SA ne va pas retourner cette erreur, il va simplement éliminer en silence la demande en diffusion groupée.

### JEU\_DE\_CHARACTERES\_NON\_COMPRIS

Si le DA reçoit une SrvTypeRqst dans un jeu de caractères qu'il ne prend pas en charge, il DOIT utiliser cette erreur.

Le nom du type de service est fourni dans la <Chaîne Type de service>. Si le type de service a une autorité de désignation autre que "IANA" elle devrait être retournée à la suite de la chaîne Type de service et un caractère ".". Voir au paragraphe 20.2.1 la définition formelle de ce champ. Les agents d'usager calculent les adresses de diffusion groupée spécifiques du service sur la base d'un hachage du type de service (voir au paragraphe 3.6.2). Cette adresse de diffusion groupée peut alors être utilisée pour produire des demandes de service et d'attribut directement aux SA.

Les exemples de chaîne de type de service suivants peuvent être trouvés dans des réponses de type de service :

```
service:lpr://
```

```
service:http://
service:nfs://
```

## 9. Format du message d'enregistrement de service

Après qu'un agent de service a trouvé un agent de répertoire, il commence à enregistrer un par un ses services annoncés. Un agent de service doit attendre pendant un délai aléatoire à répartition uniforme dans la gamme spécifiée par CONFIG\_INTERVAL\_11 avant d'enregistrer à nouveau. L'enregistrement est fait en utilisant un message d'enregistrement de service qui spécifie tous les attributs pour un service. Si l'enregistrement de service est dans une portée protégée (voir le paragraphe 16.1) le service DOIT alors inclure à la fois un bloc d'authentification d'URL et un bloc d'authentification d'attribut (voir au paragraphe 4.3). Dans ce cas, l'agent de service DOIT établir à la fois le bit 'U' et le bit 'A' (voir la Section 4).

Un agent de répertoire doit accuser réception de chaque demande d'enregistrement de services. Si des blocs d'authentification sont inclus, l'agent de répertoire DOIT vérifier l'authentification avant d'enregistrer le service. Cela exige d'obtenir les informations clés, par préconfiguration, par entretien d'une association de sécurité avec l'agent de service, ou en acquérant le certificat approprié.

Le format d'enregistrement de service est :

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|  En-tête de localisation de service (fonction = SrvReg)  |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                               <Entrée_d'URL>                               |
|                               |                               |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Long. chaîne liste d'attributs|      <liste_d'attributs>      |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                               |                               |
|                               <liste_d'attributs> suite       |
|                               |                               |
+-----+-----+-----+-----+-----+-----+-----+-----+
| (si présent) Bloc d'authentification d'attribut ...      |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

<Entrée\_d'URL> est défini à la fin du paragraphe 4.2. <liste\_d'attributs> est défini au paragraphe 20.3. Le bloc d'authentification d'attribut, qui n'est présent que si le bit 'A' est établi dans l'en-tête de message, est défini au paragraphe 4.3.

L'enregistrement de service peut utiliser un protocole sans connexion (par exemple, UDP) ou un protocole en mode connexion (par exemple, TCP). Si l'opération d'enregistrement peut contenir plus d'informations qu'il n'en peut être envoyé dans un datagramme, l'agent de service DOIT utiliser un protocole en mode connexion pour s'enregistrer auprès du DA. Lorsque un agent de service enregistre la même classe d'attribut plus d'une fois pour une instance de service, l'agent de répertoire réécrit toutes les valeurs associées à cette classe d'attributs pour cette instance de service. Des enregistrements distincts doivent être faits pour chaque langage dans lequel ce service est à annoncer.

Si un SA tente d'enregistrer un service auprès d'un DA et si l'enregistrement est supérieur à la MTU de chemin du site, le DA va alors répondre par un SrvAck, avec le code d'erreur réglé à ENREGISTREMENT\_INVALIDE et le bit 'Débordement' établi.

Exemple d'informations d'enregistrement de service :

```

Durée de vie (secondes) : entier non signé de 16 bits
URL (au moins) :      service:<srvtype>://<addr-spec>
Attributs (s'il en est) : (ATTR1=VALUE),KEYWORD,(ATTR2 = VAL1, VAL2)

```

Pour offrir des services annoncés en continu, les agents de service devraient commencer le processus de réenregistrement avant l'expiration de la durée de vie qu'ils ont utilisée dans l'enregistrement.

Un exemple d'enregistrement de service (valide trois heures) est comme suit :

```
Durée de vie : 10800
URL : service:lpr://igore.wco.ftp.com:515/draft
Attributs : (SCOPE=DEVELOPPEMENT),(PAPIER COULEUR=BLANC),(TAILLE PAPIER =LETTRE),
ACCÈS_ILLIMITÉ,(LANGAGE=POSTSCRIPT, HPGCL),(LOCALISATION=ÉTAGE 12)
```

Le même enregistrement pourrait être fait à nouveau, comme montré ci-dessous, en allemand ; cependant, noter que "lpr", "service", et "SCOPE" sont des termes réservés qui vont rester dans le langage dans lequel ils ont été enregistrés à l'origine (anglais).

```
Durée de vie : 10800
URL : service:lpr://igore.wco.ftp.com:515/draft
Attributs: (SCOPE=ENTWICKLUNG),(PAPIERFARBE=WEISS),(PAPIERFORMAT=BRIEF),
UNBEGRENTZTER_ZUGANG,(DRUECKERSPRACHE=POSTSCRIPT,HPGCL),
(STANDORT=11 ETAGE)
```

Les enregistrements avec portée doivent contenir l'attribut SCOPE. Les enregistrements sans portée doivent être enregistrés auprès de tous les agents de répertoire sans portée.

Les enregistrements d'un service précédemment enregistrés sont considérés comme une mise à jour. Si un tel enregistrement d'attribut est effectué dans une portée protégée (voir au paragraphe 16.1) un nouveau bloc d'authentification d'attribut doit aussi être inclus, et le bit 'A' établi dans l'en-tête du message d'enregistrement.

Les attributs du nouvel enregistrement remplacent ceux du précédent enregistrement, mais n'affectent pas les attributs qui ont été inclus antérieurement 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 nouvel enregistrement vient 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.

Dans l'exemple ci-dessus, SCOPE est réglé à DEVELOPPEMENT (en français) et ENTWICKLUNG (en allemand). On rappelle que toutes les chaînes dans un message doivent être dans un seul langage, qui est spécifié dans l'en-tête. La chaîne SCOPE n'est *\*pas\** traduite, car c'est une des chaînes réservées dans le protocole de localisation de service (voir au paragraphe 17.2.)

L'agent de répertoire peut retourner une erreur de serveur dans l'accusé de réception. Cette erreur est portée dans le champ Code d'erreur de l'en-tête du message de localisation de service. Un agent de répertoire DOIT refuser d'enregistrer un service si il est spécifié avec une portée non acceptée. Dans ce cas, une erreur PORTÉE\_NON\_ACCEPTÉE est retournée dans le SrvAck. Un agent de répertoire NE DOIT PAS accepter des enregistrements de service qui ont une portée non acceptée sauf si c'est un agent de répertoire sans portée, auquel cas, il DOIT accepter tous les enregistrements de service.

Un enregistrement de service sans portée va correspondre à toutes les demandes. Une demande qui spécifie une certaine portée va donc retourner des services qui ont cette portée et des services qui sont sans portée. Il est fortement suggéré d'utiliser des portées dans tous les enregistrements ou dans aucun. Voir les détails à la Section 16 et au paragraphe 3.7.

Lorsque l'entrée d'URL qui accompagne un enregistrement contient aussi un bloc d'authentification (paragraphe 4.3) le DA DOIT effectuer l'authentification indiquée, et ensuite indiquer le résultat dans le message d'accusé de réception de service.

## 10. Format du message d'accusé de réception de service

Un accusé de réception de service est envoyé par suite de la réception et du traitement par un DA d'un enregistrement de service ou d'un désenregistrement de service. Un accusé de réception qui indique un succès doit avoir le code d'erreur réglé à zéro. Une fois qu'un DA a accusé réception d'un enregistrement de service, il rend les informations disponibles aux clients.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|      En-tête de localisation de service (fonction = SrvAck)      |
+-----+-----+-----+-----+-----+-----+-----+-----+
|      Code d'erreur      |
+-----+-----+-----+-----+-----+-----+

```

Le code d'erreur peut avoir une des valeurs suivantes :

0 Succès

#### ERREUR\_D'ANALYSE\_DE\_PROTOCOLE

Un DA retourne cette erreur lorsque un SrvReg ou SrvDereg est reçu qui ne peut pas être analysé ou que les longueurs de chaînes déclarées dépassent le message.

#### ENREGISTREMENT\_INVALIDE

Un DA retourne cette erreur lorsque un SrvReg ou SrvDeReg est invalide. Par exemple, un URL invalide, un attribut inconnu ou mal formé, ou le désenregistrement d'un service non enregistré causent tous le rapport de cette erreur.

**PORTÉE\_NON\_ACCEPTÉE** Un DA qui est configuré pour avoir une portée va retourner cette erreur si il reçoit une SrvReq qui est réglée à avoir une portée qu'il ne prend pas en charge.

#### JEU\_DE\_CARACTERES\_NON\_COMPRIS

Si le DA reçoit un SrvReg ou SrvDereg dans un jeu de caractères qu'il ne prend pas en charge, il va retourner cette erreur.

#### AUTHENTIFICATION\_ABSENTE

Si le DA a été configuré à exiger l'authentification pour tout service enregistré dans la portée demandée, et si il n'y a pas de bloc d'authentification dans l'enregistrement, le DA va retourner cette erreur.

#### ÉCHEC\_D'AUTHENTIFICATION

Si l'enregistrement contient un bloc d'authentification qui ne réussit pas à correspondre au résultat correct tel que calculé (voir au paragraphe 4.3) sur l'URL ou les données d'attribut à authentifier, le DA va retourner cette erreur.

Si l'agent de répertoire accepte un enregistrement de service, et a déjà une entrée existante, il met à jour l'entrée existante avec les nouvelles informations de durée de vie et éventuellement les nouveaux attributs et les nouvelles valeurs d'attributs. Autrement, si l'enregistrement est acceptable (y compris toutes les vérifications d'authentification nécessaires) l'agent de répertoire crée une nouvelle entrée, et établit le bit 'F' dans l'accusé de réception de service retourné à l'agent de service.

## 11. Format du message de désenregistrement de service

Lorsque un service n'est plus disponible à l'utilisation, l'agent de service doit se désenregistrer des agents de répertoire auprès desquels il a été enregistré. Un service utilise la PDU suivante pour se désenregistrer.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      En-tête de localisation de service (fonction = SrvDereg)      |
+-----+-----+-----+-----+-----+-----+-----+-----+
|          Longueur d'URL          |          URL          |
+-----+-----+-----+-----+-----+-----+-----+
|
\          URL de service à désenregistrer, suite          \
|
+-----+-----+-----+-----+-----+-----+-----+
|          (si présent) bloc d'authentification .....          |
+-----+-----+-----+-----+-----+-----+-----+
| Longueur de chaîne <tag spec> |          <tag spec>          |
+-----+-----+-----+-----+-----+-----+-----+
|
\          <tag spec>, suite          \
|
+-----+-----+-----+-----+-----+-----+-----+

```

L'agent de service devrait réessayer cette opération si il n'y a pas de réponse de l'agent de répertoire. L'agent de répertoire accuse réception de cette opération avec un message Accusé de réception de service. Une fois que l'agent de service a reçu un accusé de réception indiquant la réussite, il peut supposer que le service n'est plus annoncé par l'agent de répertoire. Le code d'erreur dans l'accusé de réception de désenregistrement de service peut avoir les mêmes valeurs que celles décrites à la Section 10.

Les informations de désenregistrement de service envoyées à l'agent de répertoire ont la forme suivante :

```
service:<srvtype>://<addr-spec>
Étiquettes d'attribut (s'il en est) : ATTR1,KEYWORD,ATTR2
```

Cela va désenregistrer les attributs spécifiés des informations de service chez l'agent de répertoire. Si aucune étiquette d'attribut n'est incluse, toutes les informations de service sont désenregistrées dans tous les langages et toutes les portées dans lesquelles elles étaient enregistrées. Pour désenregistrer l'imprimante de l'exemple précédent, utiliser :

```
service:lpr://igore.wco.ftp.com:515/draft
```

Si le service était à l'origine enregistré avec une entrée d'URL contenant un bloc d'authentification d'URL, l'en-tête du message de désenregistrement de service DOIT avoir le bit 'U' établi, et l'entrée d'URL est alors suivie par le bloc d'authentification, avec l'authentifiant calculé sur les données de l'URL, l'horodatage, et la longueur de l'authentifiant comme expliqué au paragraphe 4.3. Dans ce calcul, la durée de vie des données d'URL est considérée comme étant zéro, quelle que soit la valeur actuelle de la durée de vie restante de l'URL enregistré.

## 12. Format du message de demande d'attribut

La demande d'attribut est utilisée pour obtenir les informations d'attribut. L'UA produit une demande et les informations d'attribut appropriées sont retournées.

Si l'UA ne fournit qu'un type de service, la réponse comporte alors tous les attributs et toutes les valeurs pour ce type de service. La réponse n'inclut que les attributs pour lesquels existent des services et qui sont annoncés par le DA ou le SA qui a reçu la demande d'attribut. Comme différentes instances d'un certain service peuvent avoir, et très vraisemblablement, auront des valeurs différentes pour les attributs définis par le type de service, l'agent d'utilisateur doit former une union de tous les attributs retournés par tous les agents de service. Les informations d'attribut seront utilisées pour former des demandes de service.

Si l'UA fournit un URL, la réponse va contenir les informations de service qui correspondent à cet URL.

Les demandes d'attribut comportent une 'clause de choix'. Cela peut être utilisé pour limiter la quantité d'informations retournées. Si la clause de choix est vide, toutes les informations sont retournées. Autrement, l'UA fournit une liste, délimitée par des virgules, des étiquettes d'attributs et des mots-clés. Si l'attribut ou mot-clé est défini pour un service, il sera retourné dans la réponse d'attribut, avec toutes les valeurs enregistrées pour cet attribut. Si l'attribut choisi n'a pas été enregistré pour cet URL ou type de service, les informations d'attribut ou mot-clé ne sont simplement pas retournées.

Le message de demande d'attribut a la forme suivante :

```

0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|      En-tête de localisation de service (fonction = AttrRqst)      |
+-----+-----+-----+-----+-----+-----+-----+-----+
|Long. chaîne liste répond. préc|<Spéc. adr. répondants précéd.>|
+-----+-----+-----+-----+-----+-----+-----+-----+
|
\      <Spéc. adr. répondants précéd.> suite                          \
|
+-----+-----+-----+-----+-----+-----+-----+-----+
|      Longueur d'URL          |          URL                          |
+-----+-----+-----+-----+-----+-----+-----+-----+
|
\          URL, suite                                                \
|
+-----+-----+-----+-----+-----+-----+-----+-----+
|      Longueur de <Portée>    |          <Portée>                    |
+-----+-----+-----+-----+-----+-----+-----+-----+
|
\          <Portée>, suite                                            \
|
```

```

+-----+-----+-----+-----+
| Longueur de <select-list> | <select-list> |
+-----+-----+-----+-----+
|
\ <select-list>, suite \
|
+-----+-----+-----+-----+

```

La <Liste des adresses de répondants précédents> fonctionne exactement comme on l'a indiqué à la Section 7. Voir aussi le paragraphe 20.1.

L'URL peut prendre deux formes : soit c'est simplement un type de service, tel que "service:http:", ou cela peut être un URL, comme "service:lpr://igore.wco.ftp.com:515/draft". Dans le premier cas, tous les attributs et la gamme complète des valeurs pour chaque attribut pour le type de service sont retournés. Dans le second cas, seuls sont retournés les attributs pour le service dont l'URL est défini.

La chaîne Portée est fournie afin que les demandes d'attribut pour des types de service puissent être faites de telle sorte que seules les informations d'attribut relevant d'une portée spécifique soient retournées. Ce champ est ignoré dans le cas où un URL complet est envoyé dans la demande d'attribut. Les règles de codage de la chaîne Portée figurent au paragraphe 5.4.

La liste des choix prend la forme :

```
<select-list> ::= <select-item> | <select-item> ',' <select-list>
```

```
<select-item> ::= <keyword> | <attr-tag> | <partial-tag> '*'
```

```
<partial-tag> ::= nom de classe partiel d'un attribut
```

Si il est suivi d'une '\*', il correspond à tous les noms de classe qui commencent par l'étiquette partielle. Si il est précédé par une étiquette partielle, il correspond à tous les noms de classe qui se terminent par l'étiquette partielle. Si est précédé et suivi par une '\*' il correspond à tous les noms de classe qui contiennent l'étiquette partielle.

Pour les définitions de <attr-tag> et <keyword> voir le paragraphe 5.4.

Un exemple de select-list dans l'exemple de l'imprimante serait :

```
PAGES PAR MINUTE, ACCES_SANS_RESTRICTION, LOCALISATION
```

Si il est envoyé à un agent de répertoire, le nombre de répondants précédents est zéro et il n'y a pas de Spécification d'adresse de répondant précédent. Ces champs ne sont utilisés que pour des diffusions groupées répétées, exactement comme pour la demande de service.

### 13. Format du message de réponse d'attribut

Un message de réponse d'attribut prend la forme suivante :

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| En-tête de localisation de service (fonction = AttrRply) |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Code d'erreur | Long. de chaîne <attr-list> |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|
\ <attr-list> \
|
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Le code d'erreur peut avoir les valeurs suivantes :

0 Succès

**LANGAGE\_NON\_ACCEPTÉ**

Un SA ou DA retourne cela lorsque une demande est reçue d'un UA qui est dans un langage pour lequel il n'y a pas d'informations de service enregistrées et que la demande est arrivée avec le bit Monolingue établi. Voir la Section 17.

**ERREUR\_D'ANALYSE\_DU\_PROTOCOLE**

Un DA ou SA retourne cette erreur lorsque une AttrRqst est reçue et qu'elle ne peut pas être analysée ou que les longueurs de chaîne déclarées dépassent le message.

**PORTÉE\_NON\_ACCEPTÉE**

Un DA qui est configuré à avoir une portée va retourner cette erreur si il reçoit une AttrRqst qui est réglée à avoir une portée qu'il n'accepte pas. Les SA vont éliminer en silence les messages AttrRqst en diffusion groupée pour les portées qu'ils ne prennent pas en charge.

**JEU\_DE\_CARACTERES\_NON\_COMPRIS**

Si le DA reçoit une AttrRqst dans un jeu de caractères qu'il ne prend pas en charge, il va retourner cette erreur. Les SA vont éliminer en silence les messages AttrRqst en diffusion groupée qui arrivent en utilisant des jeux de caractères qu'ils ne prennent pas en charge.

La liste d'attributs <attr-list> a la même forme que la liste des attributs dans un enregistrement de service, voir au paragraphe 20.3 la définition formelle de ce champ.

Une demande d'attribut pour "lpr" pourrait choisir la réponse suivante (ACCES\_SANS\_RESTRICTION est un mot-clé) :

```
(COULEUR PAPIER=BLANC,BLEU),
(TAILLE PAPIER=LEGAL,LETTRE,ENVELOPPE,ALIMENTATION TRACTEE),
ACCES_SANS_RESTRICTION,
(PAGES PAR MINUTE=1,3,12),
(LOCALISATION=12e, PRÈS DU BUREAU D'ARUNA),
(QUEUE=LEGAL,LETTRE,ENVELOPPE,TÊTE DE LETTRE)
```

Si l'en-tête du message a le bit 'A' établi, la réponse d'attribut aura un bloc d'authentification d'attribut établi. Dans ce cas, l'authentifiant d'attribut doit être retourné avec la liste entière des attributs, exactement comme il a été enregistré par un SA dans une portée protégée. Dans ce cas, l'URL a été enregistrée dans une portée protégée et l'UA a inclus un URL mais pas une clause de choix. Si la AttrRqst spécifie que seuls certains attributs sont à retourner, le DA ne calcule pas (ne peut normalement pas) un nouvel authentifiant, de sorte qu'il retourne simplement les attributs sans un bloc authentifiant.

Un UA qui souhaite obtenir des attributs authentifiés pour un service dans une portée protégée DOIT donc inclure un URL particulier et pas de liste de choix avec la AttrRqst.

## 14. Format du message d'annonce d'agent de répertoire

Le message d'annonce d'agent de répertoire a le format suivant :

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
| En-tête de localisation de service (fonction = DAAdvert) |
+-----+-----+-----+-----+-----+-----+-----+-----+
|          Code d'erreur          |          Longueur de l'URL          |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                               |                               |
\                               |                               |
|                               |                               |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Longueur de <Scope-list>      |          <Scope-list>          |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                               |                               |
\                               |                               |
|                               |                               |
+-----+-----+-----+-----+-----+-----+-----+-----+

```



Le code d'erreur est réglé lorsque une annonce de DA est retournée par suite d'une demande de service. Il va toujours être réglé à 0 en cas d'annonce de DA non sollicitée. Le code d'erreur peut prendre les valeurs spécifiées à la Section 6.

L'URL correspond à la localisation de l'agent de répertoire. <Scope-list> est une liste, délimitée par des virgules, des portées que le DA prend en charge, dans le format suivant :

```
<Scope-list> ::= <Scope> | <Scope-list> ',' <Scope>
<Scope>      ::= Chaîne représentant une portée.
```

Voir au paragraphe 5.4 les règles lexicales concernant <Scope>.

Les annonces de DA envoyées en réponse à une demande de découverte d'agent de répertoire ont le même format que les annonces de DA non sollicitées, par exemple :

```
URL :      service:directory-agent://SLP-RESOLVER.CATCH22.COM
SCOPE List: ADMIN
```

L'agent de répertoire peut être joint à la spécification d'adresse retournée, et accepte la portée appelée "ADMIN".

## 15. Agents de répertoire

### 15.1 Introduction

Un agent de répertoire agit au nom de nombreux agents de service. Il acquiert d'eux les informations et agit comme un point de contact unique pour fournir ces informations aux agents d'utilisateurs.

Les interrogations que l'agent d'utilisateur envoie en diffusion groupée aux agents de service (dans un environnement sans agent de répertoire) sont les mêmes que les interrogations que l'agent d'utilisateur pourrait envoyer en individuel à un agent de répertoire. Un agent d'utilisateur peut mettre en antémémoire les informations sur la présence d'autres agents de répertoire à utiliser en cas de défaillance de l'agent de répertoire choisi.

En plus de l'amélioration de la capacité d'adaptation du protocole (voir au paragraphe 3.7) fonctionner avec plusieurs DA assure la robustesse du fonctionnement. Les DA peuvent avoir des informations de service dupliquées qui restent accessibles même lorsque un des DA a une défaillance. Les agents de répertoire, à l'avenir, pourront utiliser des mécanismes en dehors du présent protocole pour coordonner la maintenance d'une base de données répartie d'informations de localisation de service, et donc s'adapter aux réseaux d'entreprise ou à de plus grands domaines administratifs.

Chaque agent de service doit s'enregistrer auprès de tous les DA qu'ils sont configurés à utiliser. Les UA peuvent choisir parmi les DA qu'ils sont configurés à utiliser.

En local, la cohérence de l'agent de répertoire est garantie en utilisant des mécanismes du protocole. Il n'y a pas encore de répertoire du protocole des agents de répertoire. C'est plutôt la détection passive des DA par les SA qui assure que finalement les informations de service seront enregistrées de façon cohérente entre les DA. Les données invalides seront périmées chez les agents de répertoire, laissant seulement des enregistrements périmés transitoires même dans le cas d'une défaillance d'un agent de service.

### 15.2 Trouver les agents de répertoire

Un agent d'utilisateur ou de service peut être configuré de façon statique pour utiliser un DA particulier. Ceci est déconseillé sauf si l'application réside sur un réseau où toute forme de diffusion groupée ou de diffusion est impossible.

Autrement, un hôte qui utilise DHCP [2], [11] peut l'utiliser pour obtenir l'adresse d'un agent de répertoire. Les options DHCP 78 et 79 ont été allouées à cette fin [21].

La troisième façon de découvrir les DA est dynamique. Cela se fait en envoyant une demande de découverte d'agent de répertoire (voir au paragraphe 5.2).

Enfin, l'agent peut être informé de façon passive comme suit :

Lorsque un agent de répertoire vient en ligne, il envoie d'abord une annonce de DA non sollicitée à l'adresse de diffusion groupée générale de localisation de service. Si un DA prend en charge une portée particulière ou un ensemble de portées,

celles-ci sont placées dans la réponse. La classe de cet attribut est 'SCOPE'.

Tous les CONFIG\_INTERVAL\_9, un agent de répertoire va envoyer une annonce de DA non sollicitée. Cela va assurer que finalement il sera découvert par toutes les applications qui sont concernées.

Lorsque un agent de répertoire démarre, il commence son XID à 0, et l'incrémente de un chaque fois qu'il envoie une annonce de DA non sollicitée. Lorsque le compteur a fait un tour complet, il devrait aller de 0xFFFF à 0x0100, et non 0.

Si l'agent de répertoire a mémorisé toutes les informations de service dans une mémoire non volatile, il devrait initialement régler le XID à 0x100, car il n'apparaît pas 'sans état'. Si il mémorise les enregistrements de service seulement en mémoire, il va redémarrer sans aucun état. Il devrait indiquer cela en remettant son XID à 0.

Tous les agents de service qui reçoivent l'annonce de DA non sollicitée devraient examiner son XID. Si l'agent de répertoire n'a jamais fait parler de lui auparavant ou si le XID est inférieur à ce qu'il était précédemment et inférieur à 256, l'agent de service devrait supposer que le DA n'a pas son enregistrement de service, même si il l'a fait déjà dans le passé. Si c'est le cas et si le DA a la portée appropriée, le SA devrait enregistrer toutes les informations de service auprès de l'agent de répertoire, après avoir attendu un intervalle aléatoire de CONFIG\_INTERVAL\_10.

Lorsque un agent de service ou un agent d'utilisateur arrive en ligne, il doit produire une demande de découverte d'agent de répertoire sauf si il utilise la configuration statique ou DHCP, comme décrit en 5.2.

Un agent de service enregistre les informations auprès de TOUS les agents de répertoire nouvellement découverts lorsque l'un des deux événements ci-dessus a lieu. Lorsque des portées sont utilisées, un agent de service DEVRAIT choisir un ensemble de portées à annoncer et il a seulement besoin de s'enregistrer auprès des agents de répertoire qui prennent en charge les portées dans lesquelles ils souhaitent être enregistrés. Les services DOIVENT être enregistrés auprès des DA qui prennent en charge leur portée et de ceux qui n'ont pas de portée, sauf s'ils sont spécifiquement configurés pour ne pas le faire (voir au paragraphe 22.1.)

Une fois que l'agent d'utilisateur est au courant d'un agent de répertoire, il va lui envoyer des interrogations en individuel. Dans le cas où plus d'un agent de répertoire serait détecté, il va en choisir un avec qui communiquer. Lorsque des portées sont prises en charge, l'agent d'utilisateur va diriger ses interrogations sur les différents agents de répertoire selon les portées qui sont les domaines appropriés pour les interrogations auxquelles ils doivent répondre.

Le protocole va amener tous les DA (de la même portée) à obtenir finalement des informations cohérentes. Donc, un DA devrait être aussi bon que n'importe quel autre pour obtenir les informations de service. Il peut y avoir des incohérences temporaires entre les DA.

## 16. Découverte et utilisation de la portée

Le mécanisme de portée dans le protocole de localisation de service améliore sa capacité d'adaptation. La principale utilisation des portées est de fournir la capacité à organiser un réseau de site le long des lignes administratives. Un ensemble de services peut être alloué à un certain département d'une organisation, à un certain bâtiment ou zone géographique ou pour certaines fins. Les utilisateurs du système peuvent se présenter à ces éléments organisationnels comme un choix de niveau supérieur, avant que soient recherchés les services au sein de ce domaine.

Un réseau de site qui a crû au delà d'une taille qui peut être raisonnablement desservie par quelques DA peut utiliser le mécanisme de portée. Les DA ont la classe d'attribut "SCOPE". Les valeurs pour cet attribut sont une liste de chaînes qui représentent les zones administratives pour lesquelles cet agent de répertoire est configuré. La sémantique et le langage des chaînes utilisés pour décrire la portée sont presque entièrement le choix de l'entité administrative du domaine particulier dans lequel existent ces portées. Les valeurs de SCOPE devraient être configurables, afin que les administrateurs de système puissent régler sa valeur. Les portées "LOCAL" et "REMOTE" sont réservées et NE DEVRAIENT PAS être utilisées. L'utilisation de ces valeurs réservées sera définie dans un futur document de protocole.

Les services qui ont l'attribut SCOPE devraient seulement être enregistrés auprès de DA qui prennent en charge la même portée ou de DA qui n'ont pas de portée.

Les agents de répertoire annoncent leurs portées disponibles. Un agent de service peut alors choisir une portée dans laquelle s'enregistrer, et DEVRAIT s'enregistrer auprès de tous les agents de répertoire dans cette portée, ainsi qu'auprès de tous les DA qui n'ont pas de portée. Manquer à pratiquer des enregistrements complets conformément à cette règle signifierait que l'annonce de service peut n'être pas disponible pour tous les agents d'utilisateur.

Un agent de répertoire qui a une portée va retourner des annonces en réponse aux demandes de découverte d'agent de répertoire avec les informations de portée incluses. Noter que le schéma "service:directory-agent" est enregistré auprès de l'autorité de désignation IANA (qui est automatiquement choisie en laissant vide le champ d'autorité de désignation).

L'interrogation : `directory-agent/MATH DEPT//` pourrait recevoir l'annonce de DA suivante :

URL retournée : `service:directory-agent://diragent.blah.edu`  
 PORTÉE retournée : MATH DEPT

Le même agent de répertoire répondrait, si il n'a pas de valeur de portée :

URL retournée : `service:directory-agent://diragent.void.com`  
 URL retournée :

Si un agent de répertoire prend en charge plus d'une portée, il va répondre :

URL retournée : `service:directory-agent://srv.domain.org`  
 URL retournée : MATH DEPT,ENGLISH DEPT,CS DEPT

Un DA qui n'a pas de portée va répondre à toute demande de découverte d'agent de répertoire.

Être membre d'une portée signifie qu'un agent DEVRAIT utiliser les agents de répertoire qui prennent en charge sa portée. Les agents d'utilisateur envoient toutes les demandes aux DA qui prennent en charge la portée indiquée. Les services sont enregistrés auprès du ou des DA dans leur portée. Pour qu'un UA trouve un service qui est enregistré dans une portée particulière, il doit envoyer les demandes à un DA qui accepte la portée indiquée. Il n'y a pas de limitation à l'adhésion à une portée incorporée au protocole ; c'est-à-dire que l'agent d'utilisateur ou l'agent de service peut être membre de plus d'une portée. L'adhésion est ouverte à tous, sauf si un mécanisme d'autorisation externe est ajouté pour limiter l'accès.

### 16.1 Portées protégées

L'adhésion à une portée PEUT aussi définir la sécurité d'accès et l'autorisation des services dans la portée ; de telles portées sont appelées des portées protégées. Si l'agent d'utilisateur souhaite être sûr que les agents de service sont autorisés à fournir le service qu'ils annoncent, l'agent d'utilisateur devrait alors demander les services à partir d'une portée protégée qui a été configurée pour avoir le mécanisme d'authentification nécessaire et des clés distribuées aux agents de service au sein de la portée. Un agent de répertoire qui distribue des URL aux services dans une portée protégée va rejeter tous les enregistrements ou désenregistrements pour les agents de service qui ne peuvent pas fournir d'authentification cryptographiquement forte pour prouver leur autorisation de fournir les services.

Par exemple, si le registraire d'un campus souhaite trouver une imprimante pour produire les informations des partiels des étudiants pour un courrier, il va demander à l'agent d'utilisateur de l'imprimante de transmettre le produit imprimable seulement aux agents de service d'impression qui ont été enregistrés dans la portée protégée appropriée. Remarquer que chaque agent de service est, dans des circonstances normales, validé deux fois : une fois lorsque il s'enregistre auprès de l'agent de répertoire, et une fois lorsque l'agent d'utilisateur valide l'URL reçu avec la réponse de service. Cela protège contre la possibilité d'agents de répertoire malveillants aussi bien que d'agents de service malveillants.

Noter que les services dans les portées protégées fournissent une authentification distincte pour leur entrée d'URL, et pour leurs attributs. Cela découle naturellement des besoins du fonctionnement du protocole. Les agents d'utilisateurs qui spécifient un type de service et les attributs nécessaires pour le service dans ce type de service ne vont pas recevoir d'informations d'attribut de l'agent de répertoire ; ils vont seulement recevoir les entrées d'URL appropriées. Seules les informations retournées ont besoin d'être authentifiées.

Les agents d'utilisateur qui reçoivent les informations d'attribut pour un URL particulier (voir la Section 12) ont par ailleurs besoin d'authentifier les attributs lorsque ils sont retournés (voir la Section 13). Dans ce cas, il peut y avoir beaucoup plus de données à authentifier, mais cette opération est aussi effectuée beaucoup moins souvent, normalement seulement lorsque l'utilisateur brasse les ressources réseau disponibles.

## 17. Problèmes de langage et de codage de caractères

Tous les enregistrements de service déclarent le langage dans lequel sont écrites les chaînes dans les attributs de service en spécifiant le code approprié dans l'en-tête du message. Pour chaque langage, le service annonce un enregistrement distinct. Chacun de ces enregistrements utilise le même URL pour indiquer qu'il se réfère au même service.

Si un service est complètement désenregistré (l'URL est donné dans la demande de désenregistrement de service, sans aucune information d'attribut) le service a alors seulement besoin d'être désenregistré une seule fois. Cela va effectivement désenregistrer le service dans toutes les langues dans lesquelles il a été enregistré.

Si par ailleurs des informations d'attribut sont incluses dans la demande de désenregistrement de service, un désenregistrement de service distinct des attributs choisis doit être entrepris dans chaque langage dans lequel des informations de service ont été fournies au DA par un agent de service. Les enregistrements de service dans des langages différents sont mutuellement inintelligibles. Ils ne partagent aucune information sauf leur type de service et l'URL avec lequel ils ont été enregistrés. Aucune tentative n'est faite pour faire correspondre les interrogations avec "indépendance de langage". Les interrogations sont plutôt traitées en utilisant la correspondance de chaîne par rapport aux enregistrements dans la même langue que l'interrogation.

Les types de service qui sont normalisés auront des définitions pour tous les attributs et chaînes de valeur. Des traductions officielles en d'autres langues des étiquettes et valeurs d'attributs peuvent être créées et soumises au titre de la norme ; ceci n'est pas faisable pour toutes les langues. Pour les langues qui ne sont pas définies au titre du type de service, une traduction au mieux des définitions standard des chaînes d'attribut de type de service PEUT être utilisée.

Toutes les demandes de service spécifient le langage demandé dans l'en-tête du message. L'agent de répertoire ou l'agent de service va répondre dans la même langue que la demande, si il a un enregistrement dans la même langue que la demande. Si ce langage n'est pas pris en charge, et si le bit Monolingue n'est pas spécifié, une réponse peut être envoyée dans la langue par défaut (qui est l'anglais). Si le fanion 'bit monolingue' est établi dans l'en-tête et si la langue demandée n'est pas prise en charge, une SrvRply est retournée avec le champ d'erreur réglé à LANGAGE\_NON\_ACCEPTÉ.

Si une interrogation est dans un langage accepté sur un SA ou DA, mais si c'est un dialecte différent de celui des informations de service disponibles, l'interrogation DOIT être servie au mieux. Si possible, l'interrogation devrait être confrontée au même dialecte. Si cela n'est pas possible, elle PEUT être mise en correspondance avec tout autre dialecte de la même langue.

## 17.1 Problèmes de codage et de chaînes de caractères

Les valeurs de codage de caractères se trouvent dans la base de données de l'IANA à <http://www.isi.edu/in-notes/iana/assignments/character-sets> et ont les valeurs référencées par la valeur MIBEnum.

Le codage va déterminer l'interprétation de toutes les données de caractères qui suivent l'en-tête du protocole de localisation de service. Il n'y a aucun moyen de mélanger, par exemple, l'ASCII et l'UNICODE. Toutes les réponses doivent être dans le jeu de caractères de la demande, ou utiliser l'US-ASCII. Si une demande est envoyée à un DA ou SA ou si un enregistrement est envoyé à un DA, et qu'il est incapable de manipuler ou mémoriser le jeu de caractères du message entrant, la demande va échouer. Le SA ou DA retourne une erreur JEU\_DE\_CARACTERES\_NON\_COMPRIS dans ce cas dans un message SrvAck. Les demandes qui utilisent l'US-ASCII ne vont jamais échouer pour cette raison, car tous les SA et DA doivent être capables d'accepter ce jeu de caractères.

Certains caractères sont illégaux dans certains contextes du protocole. Comme le protocole est largement fondé sur la chaîne de caractères, dans certains contextes, des caractères sont utilisés comme délimiteurs du protocole. Dans ces cas, le caractère délimiteur ne doit pas être utilisé comme 'texte de données'.

### 17.1.1 Substitution de séquences d'échappement de caractères

Le protocole de localisation de service a un 'mécanisme d'échappement' qui est cohérent avec HTTP 2.0 [5] et SGML [15]. Si la séquence de caractères "&#" est suivie par un ou plusieurs chiffres, suivis par deux-points ';', la séquence entière est interprétée comme un seul caractère. Les chiffres sont interprétés comme une valeur décimale dans le jeu de caractères de la demande, comme spécifié par l'en-tête. Donc, en US-ASCII &#44; serait interprété comme une virgule. La substitution de ces chaînes d'échappement doit être faite dans toutes les <attr-list> et chaînes présentes dans les messages SrvReq et AttrRqst. Seules les références de caractères numériques sont acceptées, pas les 'références d'entité', comme définies dans HTML. Ces valeurs d'échappement ne devraient être utilisées que pour fournir un mécanisme pour inclure les caractères réservés dans les étiquettes d'attribut et les chaînes de valeurs.

L'interprétation de ces valeurs d'échappement est différente de celle d'HTML sous un aspect : dans HTML, les valeurs d'échappement sont considérées comme étant dans le jeu de caractères ISO Latin-1. Dans la localisation de service, elles sont interprétées dans le jeu de caractères défini dans l'en-tête du message.

Ce mécanisme d'échappement permet d'inclure des caractères comme les virgules dans les étiquettes et les valeurs

d'attribut, qui autrement seraient illégales car la virgule est un délimiteur du protocole.

Les étiquettes et valeurs d'attributs de langages différents sont considérées comme mutuellement inintelligibles. Une interrogation dans une langue DEVRAIT utiliser les informations de service enregistrées dans cette langue.

## 17.2 Chaînes indépendantes du langage

Certaines chaînes, comme des noms de type de service, ont des définitions standard. Ces chaînes devraient être considérées comme des jetons et non comme des mots dans un langage à traduire.

Chaîne réservée	Section	Définition
SCOPE	3, 15	Utilisé pour limiter la mise en correspondance des demandes.
SERVICE	6, 9	Schéma d'URL de toutes les informations de localisation de service enregistrées auprès d'un DA ou retournées d'une demande de service.
<srvtype>	20.2.1	Utilisé dans tous les enregistrements et réponses de service.
domain names	20.4	Nom de domaine pleinement qualifié, utilisé dans les enregistrements et réponses.
IANA	3.3	Autorité de désignation par défaut.
LOCAL	16	Réservé.
REMOTE	16	Réservé.
TRUE	20.5	Booléen vrai.
FALSE	20.5	Booléen faux.

## 18. Transactions de localisation de service

### 18.1 Connexions de localisation de service

Lorsque une demande de localisation de service ou une demande d'attribut résulte en une réponse UDP d'un agent de service ou d'un agent de répertoire qui va faire déborder un datagramme, l'agent d'utilisateur peut ouvrir une connexion avec l'agent et produire à nouveau la demande sur la connexion. La réponse sera retournée avec le bit débordement établi (voir la Section 4). La réponse va contenir autant de données que ce qui va tenir dans un seul datagramme. Si aucune information de MTU n'est disponible pour le chemin, on supposera que la MTU est de 1400 ; cette valeur est configurable (voir la Section 22).

Lorsque une demande résulte en un débordement de données qui ne peuvent pas être correctement analysées (disons, à cause de datagrammes IP dupliqués ou abandonnés) l'agent d'utilisateur qui souhaite obtenir fiablement les données en débordement doit établir une connexion TCP avec l'agent de répertoire ou l'agent de service avec les données. Lorsque la demande est envoyée à nouveau avec un nouvel XID, la réponse est retournée sur la connexion.

Lorsque les données d'enregistrement excèdent la longueur d'un datagramme, l'enregistrement de service devrait être fait en établissant une connexion avec un agent de répertoire et en envoyant l'enregistrement sur le flux de la connexion.

Les agents de répertoire et les agents de service doivent répondre aux demandes de connexion ; les services dont les données d'enregistrement peuvent déborder d'un datagramme doivent être capables d'utiliser TCP pour envoyer l'enregistrement. Les agents d'utilisateur devraient être capables de faire des demandes de service et d'attribut en utilisant TCP. Si ils ne réussissent pas à mettre en œuvre cela, ils doivent être capables d'interpréter les réponses partielles et/ou de produire à nouveau les demandes avec des critères plus sélectifs pour réduire la taille de la réponse.

Une connexion initiée par un agent peut être utilisée pour une seule transaction. Elle peut aussi être utilisée pour plusieurs transactions. Comme il y a des champs de longueur dans les en-têtes de message, les agents peuvent envoyer de multiples demandes sur une connexion et lire le flux de retour pour les accusés de réception et les réponses.

L'agent initiateur est responsable de la fermeture de la connexion TCP. Le DA devrait attendre au moins CONFIG\_INTERVAL\_12 avant de clore une connexion inactive. Les DA et les SA DEVRAIENT éventuellement clore les connexions inactives pour assurer un fonctionnement robuste, même lorsque l'agent qui a ouvert une connexion néglige de la clore

### 18.2 Pas d'hypothèse de synchronisme

Il n'est pas exigé qu'une transaction s'achève avant qu'un hôte en commence une autre. Un agent peut avoir plusieurs transactions en cours, initiées en utilisant UDP ou TCP.

### 18.3 Idempotence

Toutes les actions de localisation de service sont idempotentes. Bien sûr, l'enregistrement et le désenregistrement vont changer l'état d'un DA, mais répéter ces actions avec le même XID aura exactement le même effet chaque fois. Répéter un enregistrement avec un nouvel XID a pour effet d'étendre la durée de vie de l'enregistrement.

## 19. Considérations pour la sécurité

Le protocole de localisation de service assure l'authentification des agents de service au titre du mécanisme de portée, et par conséquent, l'intégrité des données reçues au titre de ces enregistrements. La localisation de service n'assure pas la confidentialité. Comme l'objectif de ce protocole est d'annoncer les services à une communauté d'utilisateurs, la confidentialité pourrait n'être pas généralement nécessaire lorsque ce protocole est utilisé dans des environnements non sensibles. Des schémas spécialisés pourraient être capables de fournir la confidentialité, si nécessaire à l'avenir. Les sites qui requièrent la confidentialité devraient mettre en œuvre l'encapsulation de charge utile de sécurité IP (ESP) [3] pour assurer la confidentialité des messages de localisation de service.

En utilisant des portées protégées, 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 confidentielles des utilisateurs. De plus, un adversaire qui utilise ce protocole va trouver plus facile d'engager des attaques de déni de service sélectives. Les sites qui sont dans des environnements potentiellement hostiles (par exemple, qui sont directement connectés à l'Internet) devraient examiner les avantages de distribuer des clés associées aux portées protégées avant de déployer les agents de répertoire ou agents de service sensibles.

La localisation de service est utile comme protocole d'amorçage. Elle peut être utilisée dans des environnements dans lesquels aucune préconfiguration n'est possible. Dans de telles situations, une certaine quantité de "foi aveugle" est requise: Sans aucune configuration a priori, il est impossible d'utiliser aucun des mécanismes de sécurité décrits ci-dessus. La localisation de service fera usage des mécanismes fournis par la zone de sécurité de l'IETF pour la distribution des clés lorsque elle deviendra disponible. Pour l'instant, il sera seulement possible d'obtenir les bénéfices associés à l'utilisation des portées protégées si des informations cryptographiques peuvent être préconfigurées avec les systèmes d'extrémité avant qu'ils utilisent la localisation de service. Pour les agents d'usager, cela pourrait être aussi simple que de fournir la clé publique d'une autorité de certificat. Voir l'appendice B.

## 20. Formats de chaînes utilisés avec les messages de localisation de service

La présente section fournit les définitions formelles des champs et des éléments de protocole introduits dans les sections indiquées.

Élément de protocole	Défini dans	Utilisé dans
<Spécification d'adresse des répondants précédents>	20.1	SrvReq
Demande de service <predicate>	5.4	SrvReq
URL	20.2	SrvReg, SrvDereg, SrvRply
<attr-list>	20.3	SrvReg, SrvRply, AttrRply
<Informations d'enregistrement de service>	9	SrvReg
<Informations de désenregistrement de service>	11	SrvDereg
<Chaîne de type de service>	20.2.1	AttrRqst

### 20.1 Spécification de l'adresse du répondant précédent

La spécification d'adresse des répondants précédents est spécifiée par

<Spécification d'adresse des répondants précédents> ::=  
 <addr-spec> | <addr-spec>, <Spécification d'adresse des répondants précédents>

c'est-à-dire, une liste séparée par des virgules sans espace intercalée. La spécification d'adresse est l'adresse de l'agent de répertoire ou de l'agent de service qui a fourni la réponse précédente. Le format des spécifications d'adresse dans la localisation de service est définie au paragraphe 20.4. La virgule de délimitation est exigée entre chaque <addr-spec>. L'utilisation de la notation d'adresse IP en décimal séparé par des points ne devrait être faite que dans les environnements qui n'ont pas de service de nom de domaine.

Exemple : RESOLVO.NEATO.ORG,128.127.203.63

## 20.2 Définition formelle du schéma "service:"

Un URL avec un schéma "service:" est utilisé dans les messages SrvReg, SrvDereg, SrvRply et AttrRqst dans la localisation de service. Les URL sont définis dans la RFC1738 [6]. Un URL avec le schéma "service:" doit contenir au moins :

`<url> ::= service:<srvtype>://<addr-spec>`

où :

service est le schéma d'URL pour que la localisation de service retourne les réponses.

`<srvtype>` est une chaîne ; le type de services peut être normalisé en développant une spécification pour la partie spécifique de "type de service" et en l'enregistrant auprès de l'IANA. Voir aux paragraphes 20.2.1 et 3.3.

`<addr-spec>` est le point d'accès au service du service. C'est l'adresse réseau ou le nom de domaine où on peut accéder au service. Voir au paragraphe 20.4.

Le schéma "service:" peut être suivi par tout URL légal. Le protocole utilisé pour accéder au service à l'accès de service `<addr-spec>` peut être implicite dans le nom de type de service. Si ce n'est pas le cas, le type de service DOIT être défini de telle façon que les informations d'attribut incluent toutes les informations nécessaires de configuration et de protocole. Un agent d'utilisateur DOIT donc être capable d'utiliser soit un URL "service:" seul, soit un URL "service:" en conjonction avec des attributs de service pour utiliser un service.

### 20.2.1 Chaîne de type de service

Le type de service est une chaîne qui décrit le type de service. Ces chaînes ne peuvent comprendre que des caractères alphanumériques, '+', et des noms de type.

Si le nom du type de service est suivi par un '.' et une chaîne (qui a les mêmes limitations) le 'suffixe' est considéré comme étant l'autorité de désignation du service. Si l'autorité de désignation est omise, l'IANA est supposée être l'autorité de désignation.

Les types de service développés pour un usage interne ou expérimental peuvent avoir toute sémantique de nom et d'attribut pourvu qu'elle n'entre pas en conflit avec les types de service normalisés.

## 20.3 Informations d'attribut

La `<attr-list>` est retournée dans la réponse d'attribut si la demande d'attribut ne donne pas un résultat vide.

`<attr-list> ::= <attribute> | <attribute>, <attr-list>`  
`<attribute> ::= (<attr-tag>=<attr-val-list>) | <mot-clé>`  
`<attr-val-list> ::= <attr-val> | <attr-val>, <attr-val-list>`

Une `<attr-list>` doit être examinée avant l'évaluation de toutes les occurrences de la chaîne "&#" suivie par un ou plusieurs chiffres suivis par '!'. Voir au paragraphe 17.1.1.

Un mot-clé a seulement une `<attr-tag>`, et pas de valeurs.

Une virgule ne doit pas apparaître dans une `<attr-val>`, car la virgule est utilisée comme délimiteur de plusieurs valeurs. Voici des exemples d'une `<attr-list>` :

(SCOPE=ADMINISTRATION)  
(COLOR=RED, WHITE, BLUE)  
(DELAY=10 MINS),BUSY,(LATEST BUILD=10-5-95),(PRIORITY=L,M,H)

Le troisième exemple a trois attributs dans la liste. Color peut prendre les valeurs red, white et blue. Il y a plusieurs autres exemples de réponses dans le présent document.

## 20.4 Spécification d'adresse dans la localisation de service

La spécification d'adresse utilisée dans la localisation de service est :

```
<addr-spec> ::= [<usager>:<mot-de-passe>@]<hôte>[:<accès>]
<hôte> ::= Nom de domaine pleinement qualifié | adresse IP en notation décimale séparée par des points
```

Lorsque aucun serveur de nom de domaine n'est disponible, les SA et DA doivent utiliser les conventions du décimal séparé par des points pour les adresses IP. Autrement, il est préférable d'utiliser un nom de domaine pleinement qualifié chaque fois que possible car la dénumérotation des adresses des hôtes va à la longue rendre invalides les adresses IP.

En général, seul le nom de domaine de l'hôte (ou l'adresse) est retourné. Lorsque il y a un accès non standard pour le protocole, il devrait être retourné aussi. Certaines applications peuvent faire usage de la syntaxe <usager>:<mot-de-passe>@ syntaxe, mais son utilisation n'est pas conseillée dans ce contexte jusqu'à ce que des mécanismes soient établis pour protéger la confidentialité.

La spécification d'adresse dans la localisation de service est cohérente avec le format d'URL standard [6].

## 20.5 Règles de codage de valeur d'attribut

Les valeurs d'attributs, et les étiquettes d'attributs sont INSENSIBLES A LA CASSE pour le besoins de la comparaison lexicale.

Les valeurs d'attributs sont des chaînes qui contiennent tous caractères à l'exception de '(', ')', '=', '>', '<', '/', '\*', et ',' (la virgule) sauf dans le cas décrit ci-dessous où les valeurs opaques sont codées. Ces caractères peuvent être inclus en utilisant le mécanisme d'échappement de valeur de caractère décrit au paragraphe 17.1.1.

Bien qu'un attribut puisse prendre n'importe quelle valeur, il y a trois types de valeurs qui se différencient des chaînes générales : les booléens, les entiers et les valeurs opaques.

- Les valeurs booléennes sont soit "VRAI" soit "FAUX". Ceci est le cas sans considération du langage (c'est-à-dire en français ou en Telugu, le booléen VRAI est "VRAI", aussi bien qu'en anglais). Les attributs booléens ne peuvent prendre qu'une seule valeur.
- Les valeurs d'entier sont exprimées comme une séquence de nombres. La gamme des valeurs admises pour les entiers est de "-2 147 483 648" à "2 147 483 647". Aucune autre forme de représentation numérique n'est interprétée comme telle que les entiers. Par exemple, les nombres hexadécimaux tels que "0x342" ne sont pas interprétés comme des entiers, mais comme des chaînes.
- Les valeurs opaques (c'est-à-dire les valeurs binaires) sont exprimées en notation radix-64. Leurs syntaxe est :
 

```
<opaque-val> ::= (<long>:<données-en-radix-64>)
<long> ::= nombre d'octets des données d'origine
<données-en-radix-64> ::= codage en radix-64 des données d'origine
```

<long> est un nombre binaire de 16 bits. Le radix-64 code tous les 3 octets de données binaires en 4 octets de données ASCII qui sont dans la gamme de caractères qui sont pleinement imprimables et transférables par messagerie. Pour une définition formelle du format radix-64, voir la RFC1521 [7], MIME Partie une, paragraphe 5.2 "Codage en base64 de transfert de contenu", page 21.

## 21. Exigences du protocole

Dans cette section sont énumérées diverses exigences du protocole pour les agents d'utilisateur, les agents de service, et les agents de répertoire.

### 21.1 Exigences d'agent d'utilisateur

Un agent d'utilisateur PEUT :

- Fournir un moyen pour que l'application configure le DA par défaut, afin qu'il puisse être utilisé sans besoin de le chercher à chaque initialisation.
- Être capable de demander l'adresse d'un DA à partir de DHCP, si il est configuré pour le faire.
- Ignorer toute réponse de service non authentifiée.



- Être capable de produire des demandes dans tout langage ou jeu de caractères pourvu qu'il puisse passer au langage et jeu de caractères par défaut si la demande ne peut pas être servie par les DA et SA sur ce site.
- Exiger un bloc d'authentification dans toute entrée d'URL retournée au titre de la demande de service, avant de faire usage du service annoncé.

Un agent d'utilisateur DEVRAIT :

- Essayer de contacter DHCP pour obtenir l'adresse d'un DA.
- Utiliser une portée dans toutes les demandes, si possible.
- Produire des demandes aux DA avec portée si l'UA a été configuré avec une portée.
- Écouter sur l'adresse de diffusion groupée générale de localisation de service les annonces de DA non sollicitées. Cela va augmenter l'ensemble d'agents de répertoire disponibles à qui faire des demandes. Voir au paragraphe 15.2.
- Être capable d'être configuré à exiger un bloc d'authentification dans toute entrée d'URL reçue annoncée comme appartenant à une portée protégée, avant de faire usage du service.

Si l'UA n'écoute pas les annonces de DA, les nouveaux DA ne seront pas détectés passivement. Un UA qui n'a pas un DA configuré et n'en a pas encore découvert un et qui n'écoute pas les annonces de DA non sollicitées va rester dans l'ignorance de ces DA. Il peut alors faire une découverte de DA avant chaque interrogation effectuée ou il peut simplement utiliser des interrogations en diffusion aux agents de service.

Un agent d'utilisateur DOIT :

- Être capable d'envoyer les demandes en individuel et de recevoir les réponses d'un DA. Les transactions devraient être rendues fiables en utilisant la retransmission de la demande si la réponse n'arrive pas dans un intervalle de temporisation.
- Être capable de détecter les DA en utilisant une demande de découverte d'agent de répertoire produite lorsque l'UA démarre.
- Être capable d'envoyer des demandes à une adresse de diffusion groupée. Les adresses de diffusion groupée spécifiques des services sont calculées sur la base d'un hachage du type de service. Voir au paragraphe 3.6.2.
- Être capable de traiter de nombreuses réponses après une demande en diffusion groupée. La mise en œuvre peut être configurable afin qu'elle retourne la première réponse, toutes les réponses jusqu'à une fin de temporisation, ou de continuer d'essayer jusqu'à ce que les résultats convergent.
- Ignorer toute réponse de service ou réponse d'attribut non authentifiée lorsque il existe une association de sécurité IPsec appropriée pour cette réponse.
- Chaque fois qu'il obtient son adresse IP de DHCP en premier, il doit aussi tenter d'obtenir les informations de portée, et l'adresse d'un DA, de DHCP.
- Utiliser l'en-tête d'authentification IP ou l'encapsulation de charge utile IP dans tous les messages de localisation de service, chaque fois qu'il existe une association de sécurité IPsec appropriée.
- Être capable de produire des demandes en utilisant le jeu de caractères US-ASCII.
- Si il est configuré à utiliser une portée protégée, être capable d'utiliser "md5WithRSAEncryption" [4] pour vérifier les données signées.

## 21.2 Exigences d'agent de service

Un agent de service PEUT être capable de :

- Obtenir l'adresse d'un agent de répertoire local au moyen de DHCP.
- Accepter des demandes dans des codages de caractères non US-ASCII. Ceci est recommandé, en particulier pour les codages UNICODE [1] et UTF-8 [24].
- Enregistrer les services auprès d'un DA dans des codages de caractères non US-ASCII. Ceci est recommandé, en particulier pour les codages UNICODE [1] et UTF-8 [24].

Un agent de service DEVRAIT être capable de :

- Écouter l'adresse de diffusion groupée spécifique du service du service qu'il annonce. Les demandes entrantes devraient être filtrées : si la spécification d'adresse du SA est dans la liste de spécification d'adresse des répondants précédents, le SA NE DEVRAIT PAS répondre. Autrement, une réponse à l'interrogation en diffusion groupée DEVRAIT être en envoi individuel à l'UA qui a envoyé la demande.
- Écouter et répondre aux demandes en diffusion et aux demandes de connexion TCP, sur l'accès de localisation de service.
- Être configurable à calculer les blocs d'authentification et par là être capable de s'enregistrer dans les portées protégées. Cela exige que l'agent de service soit configuré pour posséder les clés nécessaires pour calculer l'authentifiant.

Un agent de service DOIT être capable de :

- Écouter les interrogations sur l'adresse générale de diffusion groupée de la localisation de service (par exemple, les demandes de type de service). Si l'interrogation peut être satisfaite par l'agent de service, il DOIT le faire. Il DOIT

d'abord vérifier qu'il n'est pas sur la liste des répondants précédents.

- Écouter les annonces non sollicitées de DA sur l'adresse générale de diffusion groupée de la localisation de service. Si il en est détectée une, et si le DA a la bonne portée (ou n'a pas de portée) tous les services qui sont actuellement annoncés DOIVENT être enregistrés auprès du DA (sauf si ils sont configurés pour n'utiliser qu'un seul DA (voir au paragraphe 22.1) ou si le DA a déjà été détecté, sous réserve de certaines règles (voir au paragraphe 15.2)).
- Chaque fois qu'il obtient son adresse IP de DHCP en premier, de tenter aussi d'obtenir de DHCP les informations de portée, et l'adresse d'un DA.
- S'enregistrer et désenregistrer en envoi individuel auprès d'un DA. Les transactions devraient être rendues fiables en utilisant la retransmission de la demande si la réponse n'arrive pas dans l'intervalle de temporisation.
- Être capable de détecter les DA en utilisant une demande de découverte d'agent de répertoire produite au démarrage du SA (sauf si il est configuré à n'utiliser qu'un seul DA, voir au paragraphe 22.1).
- Utiliser l'en-tête d'authentification IP ou l'encapsulation de charge utile IP dans tous les messages de localisation de service, chaque fois qu'il existe une association de sécurité IPsec appropriée.
- Être capable d'enregistrer les informations de service auprès d'un DA en utilisant le codage de caractères US-ASCII. Il doit aussi être capable de répondre aux demandes provenant des UA qui utilisent le codage de caractères US-ASCII.
- Se réenregistrer auprès d'un DA avant l'expiration de la durée de vie des informations de service enregistrées.
- Si il est configuré pour utiliser une portée protégée, être capable d'utiliser "md5WithRSAEncryption" [4] pour produire les données signées.

### 21.3 Exigences pour l'agent de répertoire

Un agent de répertoire PEUT :

- Accepter les enregistrements et les demandes dans des codages de caractères non US-ASCII. Cela est conseillé, en particulier pour les codages UNICODE [1] et UTF-8 [24].

Un agent de répertoire DEVRAIT :

- Être capable de configurer certaines portées comme portées protégées, afin que ces enregistrements au sein de ces portées exigent le calcul d'authentifiants cryptographiquement forts. Cela exige que le DA soit capable de posséder les clés nécessaires pour l'authentification, ou que le DA soit capable d'acquérir un certificat généré par une autorité de certificat de confiance [23], avant d'achever les enregistrements de service pour des portées protégées.

Un agent de répertoire DOIT être capable de :

- Envoyer des annonces de DA non sollicitées à l'adresse de diffusion groupée générale de localisation de service au démarrage et de les répéter périodiquement. Cette réponse a un XID qui est incrémenté de un à chaque fois. Si le DA démarre avec un état, il initialise le XID à 0x0100. Si il démarre sans état, il initialise le XID à 0x0000.
- Ignorer tout enregistrement de service ou désenregistrement de service non authentifié provenant d'une entité avec laquelle il entretient une association de sécurité.
- Écouter sur l'adresse de diffusion groupée de découverte d'agent de répertoire les demandes de découverte d'agent de répertoire. Filtrer ces demandes si la liste des spécifications d'adresse des répondants précédents comporte la spécification d'adresse du DA.
- Écouter les demandes en diffusion sur l'accès de localisation de service.
- Écouter sur les accès TCP et UDP de localisation de service les demandes en envoi individuel, les enregistrements et désenregistrements et les servir.
- Fournir un moyen par lequel les informations de portée puissent être utilisées pour configurer l'agent de répertoire.
- Terminer les enregistrements lorsque la durée de vie de l'enregistrement de service arrive à expiration.
- Lorsque un agent de répertoire a été configuré avec une portée, il DOIT refuser toutes demandes et tous enregistrements qui n'ont pas cette portée. Le DA répond par une erreur PORTÉE\_NON\_ACCEPTÉE. Il y a une exception : tous les DA DOIVENT répondre aux demandes de découverte de DA qui n'ont pas de portée.
- Lorsque un agent de répertoire a été configuré sans portée, il DOIT accepter TOUS les enregistrements et demandes.
- Ignorer tout messages de localisation de service non authentifié lorsque une association de sécurité IPsec appropriée existe pour cette demande.
- Utiliser l'authentification et l'encapsulation de charge utile de sécurité IP dans les messages de localisation de service chaque fois qu'existe une association de sécurité IPsec appropriée.
- Accepter les demandes et enregistrements en US-ASCII.
- Si il est configuré avec une portée protégée, être capable d'authentifier les services d'annonce d'enregistrements de service (au moins en utilisant "md5WithRSAEncryption" [4]) relevant de telles portées protégées configurées.

## 22. Paramètres configurables et valeurs par défaut

Il y a plusieurs paramètres de configuration pour la localisation de service. Les valeurs par défaut sont choisies pour permettre le fonctionnement du protocole sans qu'il soit besoin de faire une sélection de ces paramètres de configuration,

mais d'autres valeurs peuvent être choisies par l'administrateur du site. Les paramètres configurables vont permettre à une mise en œuvre de localisation de service d'être plus utile dans divers scénarios.

#### Diffusion groupée ou diffusion

Toutes les entités de localisation de service doivent utiliser la diffusion groupée par défaut. La capacité à utiliser la diffusion des messages doit être configurable pour les UA et les SA. La diffusion des messages est à utiliser dans des environnements où toutes les entités de localisation de service n'ont pas des matériels ou logiciels qui acceptent la diffusion groupée.

#### Rayon de diffusion groupée

Les demandes en diffusion groupée devraient être envoyées à tous les sous-réseaux d'un site. Le rayon de diffusion groupée par défaut pour un site est 32. Cette valeur doit être configurable. La valeur du TTL de la diffusion groupée du site peut être obtenue de DHCP en utilisant une option qui est actuellement non allouée.

#### Adresse d'agent de répertoire

Le mécanisme de découverte de l'adresse de l'agent de répertoire doit être configurable. Il y a trois possibilités pour cette configuration : une adresse par défaut, pas d'adresse par défaut, et l'utilisation de DHCP pour localiser un DA comme décrit au paragraphe 15.2. La valeur par défaut devrait être l'utilisation de DHCP, avec "pas d'adresse par défaut" si DHCP ne répond pas. Dans ce cas, l'UA ou le SA doit faire une interrogation de découverte d'agent de répertoire.

#### Allocation de portée d'agent de répertoire

La ou les portées d'un DA doivent être configurables. La valeur par défaut pour un DA est de n'avoir pas de portée si il n'est pas configuré autrement.

#### MTU du chemin

La MTU par défaut du chemin est supposée être 1400. Cette valeur peut être trop grande pour l'infrastructure de certains sites. Pour cette raison, cette valeur DOIT être configurable pour tous les SA et DA.

#### Clés pour les portées protégées

Si l'administration locale désigne certaines portées comme des "portées protégées", les agents qui font usage de ces portées doivent être capables d'acquérir les clés pour authentifier les données envoyées par les services ainsi que leurs URL annoncés pour les services au sein de la portée protégée. Par exemple, les agents de service vont utiliser une clé privée pour produire les données d'authentification. Par défaut, les agents de service utilisent "md5WithRSAEncryption" [4] pour produire les données signées, pour être incluses avec les enregistrements et désenregistrements de service (voir l'Appendice B, 4.3). Ces données d'authentification pourront être vérifiées par les agents d'utilisateur et les agents de répertoire qui possèdent la clé publique correspondante.

### 22.1 Agent de service : utilisation d'agent de répertoire prédéfini

La configuration par défaut d'un agent de service est de faire la découverte passive et active de DA et de s'enregistrer auprès de tous les DA qui ont une portée appropriée.

Un agent de service DEVRAIT être configurable pour permettre un mode de fonctionnement spécial : il utilisera seulement les DA préconfigurés. Cela signifie qu'ils \*NE VONT PAS\* détecter les DA activement ou passivement.

Si un agent de service est configuré de cette façon, la connaissance des DA doit venir par un autre canal, soit la configuration statique, soit par l'utilisation de DHCP.

La disponibilité des informations de service ne sera pas cohérente entre les DA. Les mécanismes qui réalisent une éventuelle cohérence entre les DA sont ignorés par le SA, de sorte que leurs informations de service ne seront pas distribuées. Cela laisse le SA ouvert à la défaillance si le DA qu'il est configuré à utiliser a une défaillance.

### 22.2 Intervalles de temporisation

Ces valeurs devraient être configurables au cas où le site qui déploie la localisation de service a des exigences particulières (comme des liaisons très lentes.)

Nom d'intervalle	Section	Valeur par défaut	Signification
CONFIG_INTERVAL_0	4.1	1 minute	Antémémoire des réponses par XID.
CONFIG_INTERVAL_1	4.4	10800 s	Durée de vie d'enregistrement (3 heures) après quoi il expire.
CONFIG_INTERVAL_2	5	chaque	Sauvegarde des réessais d'interrogation en diffusion groupée

CONFIG_INTERVAL_3	5	seconde 15 s	jusqu'à ce que il n'arrive graduellement plus de nouvelles valeurs. Temps d'attente maximum pour une réponse complète à une interrogation en diffusion groupée (toutes valeurs.)
CONFIG_INTERVAL_4	9	3 s	Attente d'enregistrement sur réamorçage.
CONFIG_INTERVAL_5	5.2	3 s	Retransmission de découverte de DA, l'essayer 3 fois.
CONFIG_INTERVAL_6	5.2	5 s	Abandon des demandes envoyées à un DA.
CONFIG_INTERVAL_7	5.2	15 s	Abandon de la découverte de DA.
CONFIG_INTERVAL_8	5.1	15 s	Abandon des demandes envoyées aux SA.
CONFIG_INTERVAL_9	15.2	3 heures	Battement de cœur de DA, afin que les SA détectent passivement les nouveaux DA.
CONFIG_INTERVAL_10	15.2	1-3 s	Attente d'enregistrement des services sur découverte passive de DA
CONFIG_INTERVAL_11	9	1-3 s	Attente d'enregistrement des services sur découverte active de DA.
CONFIG_INTERVAL_12	18.1	5 minutes	Les DA et SA ferment les connexions inactives.

Note sur CONFIG\_INTERVAL\_9 : Bien qu'il puisse sembler avantageux d'avoir un battement de cœur fréquent, cela présente un risque significatif de générer beaucoup de trafic redondant. Cette valeur devrait être gardée élevée pour empêcher les opérations de routine de protocole d'utiliser une bande passante significative.

### 23. Paramètres non configurables

Numéro d'accès IP pour les demandes en envoi individuel aux agents de répertoire :

Numéro d'accès UDP et TCP : 427

Adresses de diffusion groupée

Adresse générale de diffusion groupée de localisation de service : 224.0.1.22

Adresse de diffusion groupée de découverte d'agent de répertoire : 224.0.1.35

Une gamme de 1024 adresses de diffusion groupée contiguës à utiliser comme adresses de diffusion groupée spécifiques de la découverte de service sera allouée par l'IANA.

Codes d'erreur :

Pas d'erreur	0
LANGAGE_NON_ACCEPTÉ	1
ERREUR_D'ANALYSE_DE_PROTOCOLE	2
ENREGISTREMENT_INVALIDE	3
PORTÉE_NON_ACCEPTÉE	4
JEU_DE_CARACTERES_NON_COMPRIS	5
AUTHENTIFICATION_ABSENTE	6
ÉCHEC_D'AUTHENTIFICATION	7

### 24. Remerciements

Le présent protocole doit certaines de ses idées d'origine aux autres protocoles de localisation de service trouvées dans de nombreux autres protocoles de réseautage. Leo McLaughlin et Mike Ritter (Metricom) ont fourni de nombreux apports à la première version de ce document. Merci aussi à Steve Deering (Xerox) qui a apporté son expérience des protocoles de diffusion groupée répartis. Harry Harjono et Charlie Perkins ont fourni les bases du protocole réseau fondées sur l'URL dans leur protocole de découverte de ressources. Merci aussi à Peerlogic, Inc. qui a soutenu ce travail. Enfin, merci à Jeff Schiller pour son aide pour structurer l'architecture de sécurité spécifiée dans ce document.

### Appendice A. Contenu technique de ISO 639:1988 (E/F): "Code pour la représentation des noms de langues"

Des symboles de deux lettres minuscules sont utilisés. L'autorité d'enregistrement pour ISO 639 [14] est Infoterm, Osterreichs Normungsinstitut (ON), Postfach 130, A-1021 Vienna, Autriche. Il contient les ajouts de ISO 639/RA Newsletter n 1/1989, consulter aussi la RFC1766.

aa Afari	ga Irlandais	mg Malagasy	sa Sanskri	ug Ouïgour
ab Abkhazien	gd Gaélique	mi Maori	sd Sindhi	uk Ukrainien

af Afrikaans	gl Galicien	mk Macédonien	sg Sangro	ur Ourdu
am Amharique	gn Guarani	ml Malayalam	sh Serbo-Croate	uz Ouzbek
ar Arabe	gu Goujarati	mn Mongol	si Cinghalais	
as Assamais		mo Moldave	sk Slovaque	vi Vietnamien
ay Aymarais	ha Hausa	mr Marathi	sl Slovène	vo Volapuk
az Azéri	he Hébreu	ms Malais	sm Samoan	
	hi Hindi	mt Maltais	sn Shona	wo Ouolof
ba Bashkir	hr Croate	my Birman	so Somali	
be Biélorusse	hu Hongrois		sq Albanais	xh Xhosa
bg Bulgare	hy Arménien	na Nauru	sr Serbe	
bh Bihari		ne Népalais	ss Siswati	yi Yiddish
bi Bislamais	ia Interlingua	nl Néerlandais	st Sesotho	yo Yoruba
bn Bengali ; Bangla	in Indonésien	no Norvégien	su Soudanais	
bo Tibétain	ie Interlingue		sv Suédois	za Zhuang
br Breton	ik Inupiak	oc Occitan	sw Swahili	zh Chinois
	is Icelandais	om (Afan) Oromo		zu Zoulou
ca Catalan	it Italien	ou Oriya	ta Tamoul	
co Corse	ja Japonais		te Telugu	
cs Tchèque	jw Javanais	pa Penjabi	tg Tadjik	
cy Gallois		pl Polonais	th Thaï	
	ka Géorgien	ps Pashton, Pushto	ti Tigrinya	
da Danois	kk Kazak	pt Portugais	tk Turkmène	
de Allemand	kl Groenlandais		tl Tagalog	
dz Bhoutani	km Cambodgien	qu Quechua	tn Setswana	
	rw Kinyarwanda		to Tonga	
el Grec	kn Kannada	rm Rhéto-romanche	tr Turc	
en Anglais	ko Coréen	rn Kirundi	ts Tsonga	
eo Esperanto	ks Kashmiri	ro Roumain	tt Tatar	
es Espaniol	ku Kurde	ru Russe	tw Twi	
et Estonien	ky Kirghize			
eu Basque				
	la Latin			
fa Perse	ln Lingala			
fi Finois	lo Laotien			
fj Fidjien	lt Lithuanien			
fo Féroen	lv Letton			
fr Français				
fy Frisien				

## Appendice B. Certificats SLP

Des certificats peuvent être utilisés dans SLP afin de distribuer les clés publiques des portées protégées de confiance. En supposant des clés publiques, le présent appendice expose l'utilisation de tels certificats dans le protocole de localisation de service.

Posséder la clé privée d'une portée protégée est équivalent à être un SA de confiance. Le caractère de confiance de la portée protégée dépend de ce que ces clés privées sont détenues par des hôtes de confiance, et utilisées seulement pour des enregistrements et désenregistrements de service légitimes.

Avec l'accès à l'autorité de certificat (CA, *Certificate Authority*) appropriée, les DA et UA n'ont pas besoin de détenir (à l'avance) des clés publiques qui correspondent à ces portées protégées. Ils n'exigent pas la clé publique de la CA. La CA produit des certificats en utilisant son unique clé privée. Cette clé privée n'est pas partagée par un autre système, et doit rester sûre. Les certificats déclarent qu'une certaine portée protégée a une certaine clé publique, ainsi que la date d'expiration du certificat.

Le format de la chaîne ASCII (sûr dans les messages électroniques) pour le certificat est la liste d'étiquettes et de paires de valeurs suivante :

```
"certificate-alg="      1*ASN1CHAR   CRLF
"scope-charset="      1*CHIFFRE    CRLF
"scope="              1*RADIX-64-CHAR CRLF
```

"timestamp="	16CHIFFREHEX CRLF
"public-key="	1*RADIX-64-CHAR CRLF
"cert-digest="	1*RADIX-64-CHAR CRLF
ASN1CHAR	= CHIFFRE   '.'
HEXDIGIT	= CHIFFRE   'a'..'f'   'A'..'F'
RADIX-64-CHAR	= CHIFFRE   'a'..'z'   'A'..'Z'   '+'   '/'   '='

La notation radix-64 est décrite dans la RFC1521 [7]. Les espaces sont ignorées dans le calcul de la valeur binaire correspondant à une chaîne radix-64. Si la valeur pour scope, public-key ou cert-digest est supérieure à 72 caractères, la notation Radix-64 peut être cassée pour séparer les lignes. Les lignes de continuation doivent être précédées par une ou plusieurs espaces. Seules les étiquettes dont la liste figure ci-dessus peuvent commencer dans la première colonne de la chaîne de certificat. Cela supprime les ambiguïtés dans l'analyse des valeurs radix-64 (car les étiquettes consistent en valeurs légales de radix-64).

Le certificate-alg est la chaîne ASN.1 pour la valeur d'identifiant d'objet de l'algorithme utilisé pour produire le "cert-digest". Le scope-charset est une représentation décimale de la valeurs de MIBEnum pour le jeu de caractères dans lequel la portée est représentée.

Le codage radix-64 de la chaîne de portée va permettre le rendu en ASCII de la chaîne de chaîne de portée dans tout jeu de caractères.

Les huit octets de l'horodatage en format NTP sont représentés par 16 chiffres hexadécimaux. Cet horodatage est l'heure à laquelle le certificat va arriver à expiration.

Le format de la clé publique va dépendre du type de système de chiffrement utilisé, qui est identifié par le certificat d'algorithme. Lorsque le CA a généré le certificat qui détient la clé publique obtenue, il a utilisé l'algorithme de résumé de message identifié par le certificate-alg pour calculer un résumé D sur la chaîne qui code le certificat, excepté le cert-digest. Le CA a alors chiffré cette valeur en utilisant la clé privée du CA pour produire le cert-digest, qui est inclus dans le certificat.

Le CA génère le certificat hors ligne. Le mécanisme pour distribuer les certificats n'est pas spécifié dans le protocole de localisation de service, mais pourra l'être à l'avenir. Le CA spécifie les algorithmes à utiliser pour le résumé de message et le déchiffrement de la clé publique. Le DA ou SA a seulement besoin d'obtenir le certificat, d'avoir une clé publique préconfigurée pour le CA et de prendre en charge l'algorithme spécifié dans le certificate-alg afin d'obtenir de nouvelles clés publiques pour les portées protégées.

Le DA ou l'UA peut confirmer le certificat en calculant le résumé de message D, en utilisant l'algorithme de résumé de message identifié par le certificate-alg. L'entrée à l'algorithme de résumé de message est la chaîne qui code le certificat, excepté le cert-digest. Le cert-digest est déchiffré en utilisant la clé publique du CA pour produire D'. Si D est le même que D', le certificat est légitime. La clé publique pour la portée protégée peut être utilisée jusqu'à la date d'expiration indiquée par l'horodatage du certificat.

Le certificat peut être distribué sur des canaux qui ne sont pas de confiance, comme de messagerie électronique, ou à travers un transfert de fichiers, car il doit de toutes façons être vérifié. La clé publique du CA doit être livrée en utilisant un canal de confiance.

## Appendice C Exemple de déploiement de la sécurité SLP avec MD5 et RSA

Dans notre site, nous avons un site protégé "CONTROLE". On génère une paire de clé privée – clé publique pour la portée, en utilisant RSA. La clé privée est conservée sur un anneau de clé secret par tous les SA dans la portée protégée. La clé publique est disponible pour tous les DA qui prennent en charge la portée protégée et tous les UA qui vont l'utiliser.

Pour enregistrer ou désenregistrer un URL, les données qui doivent être authentifiées (comme décrit au paragraphe 4.3) sont résumées en utilisant MD5 [22] pour créer une signature numérique, puis chiffrées par RSA avec la clé privée de la portée protégée. Le résultat de RSA est utilisé dans le champ d'authentifiant de données du bloc d'authentifiant.

Le DA ou UA découvre la méthode appropriée pour vérifier l'authentification en regardant à l'intérieur du bloc d'authentification. Supposons que l'algorithme "md5WithRSAEncryption" [4] soit utilisé pour vérifier les données signées. Le DA ou UA calcule le résumé de message de l'entrée d'URL en utilisant md5, exactement comme l'a fait le SA. Le bloc d'authentifiant est déchiffré en utilisant la clé publique pour la portée "CONTROLE", qui est mémorisée dans l'anneau de

clé publique de l'UA ou du DA sous le nom "CONTROLE". Si le résumé calculé par l'UA ou DA correspond à celui du SA, l'entrée d'URL a été validée.

## Appendice D. Exemple d'utilisation de certificats SLP par des nœuds mobiles

Disons qu'un nœud mobile a besoin d'utiliser des portées protégées. Le nœud mobile est d'abord préconfiguré en ajoutant une seule clé publique à son anneau de clés publiques : on va l'appeler CA-Clé. Cette clé sera utilisée pour obtenir des certificats SLP dans le format décrit à l'Appendice B. La clé privée correspondante sera utilisée par le CA pour créer les certificats dans le format nécessaire.

Le CA peut être actionné par un administrateur de système qui utilise un ordinateur qui n'est connecté à aucun réseau. La durée du certificat va dépendre de la politique du site. La durée, la portée, et la clé publique pour la portée protégée, sont utilisées comme entrée à 'md5sum'. Cette somme est alors chiffrée avec RSA en utilisant la clé privée du CA. Le codage radix 64 de cela est ajouté à la chaîne de messagerie sûre sur la base du codage de certificat défini à l'Appendice B.

Le certificat, pour la portée protégée "CONTROLE" pourrait être disponible pour le nœud mobile. Par exemple, il pourrait être sur une page de la Toile. Le nœud mobile pourrait alors traiter le certificat afin d'obtenir la clé publique pour la portée CONTROLE. Il n'y a encore aucune raison \*d'avoir confiance\* que cette clé soit réellement celle à utiliser (comme dans l'Appendice C). Pour lui faire confiance, calculer la somme de contrôle md5 du certificat codé en ASCII, en excluant le cert-digest. Ensuite, déchiffrer le cert-digest en utilisant la clé publique du CA et RSA. Si le cert-digest correspond au résultat de MD5, on peut faire confiance au certificat (jusqu'à ce qu'il arrive à expiration).

Le nœud mobile exige seulement une clé (CA-Clé) pour obtenir les autres de façon dynamique et faire usage des portées protégées. Remarquer qu'on ne définit aucune méthode de contrôle d'accès par des UA et SA arbitraires dans les portées protégées.

## Appendice E. Pour approfondir le sujet

Trois protocoles de découverte de ressource proches sont NBP et ZIP qui font partie de la famille des protocoles AppleTalk [12], la plate-forme d'administration de ressource Legato [25], et le système de chambre de compensation Xerox [20]. Les noms de domaines et la représentation des adresses sont largement utilisées dans le protocole de localisation de service. Les références pour cela sont les RFC 1034 et 1035 [17], [18]. Des exemples de protocole de découverte pour les routeurs sont la découverte de routeur [10] et la découverte de voisin [19].

## Références

- [1] Unicode Technical Report #4. "The unicode standard, version 1.1 (volumes 1 et 2)". Rapport technique (ISBN 0-201-56788-1) et (ISBN 0-201-60845-6), Unicode Consortium, 1994.
- [2] [RFC2131] R. Droms, "Protocole de [configuration dynamique d'hôte](#)", mars 1997. (*MàJ par RFC 3396 et 4361*)
- [3] [RFC1827] R. Atkinson, "Encapsulation dans IP de charge utile de sécurité (ESP)", août 1995. (*Obs., voir RFC2406*)
- [4] [RFC1423] D. Balenson, D., "Amélioration de la confidentialité pour la messagerie électronique Internet : Partie III -- Algorithmes, modes et identifiants", février 1993. (*Historique*)
- [5] [RFC1866] T. Berners-Lee, D. Connolly, "[Langage de balisage Hypertext](#) - 2.0", novembre 1995. (*Obsolète, voir RFC2854*) (*His.*)
- [6] [RFC1738] T. Berners-Lee et autres, "[Localisateurs uniformes de ressource](#) (URL)", décembre 1994. (*P.S., Obsolète, voir les RFC4248 et 4266*)
- [7] [RFC1521] N. Borenstien et N. Freed, "MIME (Extensions [multi-usages de messagerie Internet](#)) Partie 1 : Mécanismes pour spécifier et décrire le format des corps de message Internet", septembre 1993. (*Obsolète voir RFC2045 à 2049*)
- [8] [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

- [9] CCITT. "Spécification de la notation de syntaxe abstraite numéro un (ASN.1)". Recommendation X.208, 1988.
- [10] [RFC1256] S. Deering, éditeur, "Messages ICMP de [découverte de routeur](#)", septembre 1991.
- [11] [RFC2131] R. Droms, "Protocole de [configuration dynamique d'hôte](#)", mars 1997. (*MàJ par RFC 3396 et 4361*)
- [12] Gursharan, S., R. Andrews, et A. Oppenheimer. "Inside AppleTalk". Addison-Wesley, 1990.
- [13] [RFC2609] E. Guttman, C. Perkins, J. Kempf, "Schémas service: et gabarits de service", juin 1999. (*P.S.*)
- [14] Geneva ISO. "Code pour la représentation des noms de langues". ISO 639:1988 (E/F), 1988.
- [15] ISO 8879, Genève. "Information Processing -- Text et Office Systems - Standard Generalized Markup Language (SGML)". <URL:<http://www.iso.ch/cate/d16387.html>>, 1986.
- [16] [RFC2030] D. Mills, "Protocole simple de l'heure du réseau (SNTP) version 4 pour IPv4, IPv6 et OSI", octobre 1996. (*Rendue obsolète par la RFC 4330*)
- [17] [RFC1034] P. Mockapetris, "Noms de domaines - [Concepts et facilités](#)", STD 13, novembre 1987.
- [18] [RFC1035] P. Mockapetris, "Noms de domaines – [Mise en œuvre](#) et spécification", STD 13, novembre 1987. (*MàJ par la RFC6604*)
- [19] [RFC1970] T. Narten, E. Nordmark, W. Simpson, "Découverte du voisinage pour IP version 6 (IPv6)", août 1996. (*Obsolète, voir RFC2461*) (*P.S.*)
- [20] Oppen, D. et Y. Dalal. "The clearinghouse: A decentralized agent for locating named objects in a distributed environment". Technical Report Tech. Rep. OPD-78103, Xerox Office Products Division, 1981.
- [21] [RFC2610] C. Perkins, E. Guttman, "Options DHCP pour le protocole de localisation de service", juin 1999. (*P.S.*)
- [22] [RFC1321] R. Rivest, "Algorithme de [résumé de message MD5](#)", avril 1992. (*Information*)
- [23] Schneier, Bruce. "Applied Cryptography: Protocols, Algorithms, et Source Code in C". John Wiley, New York, NY, USA, 1994.
- [24] X/Open Preliminary Specification. "File System Safe UCS Transformation Format (FSS\_UTF)". Technical Report Document Number: P316, X/Open Company Ltd., 1994.
- [25] Legato Systems. "The Legato Resource Administration Platform". Legato Systems, 1991.

## Adresse des auteurs

Les questions sur le présent mémoire peuvent être adressées à :

John Veizades  
@Home Network  
385 Ravendale Dr.  
Mountain View, CA 94043  
tél. : +1 415 944 7332  
mél : [veizades@home.com](mailto:veizades@home.com)

Erik Guttman  
Sun Microsystems  
Gaisbergstr. 6  
69115 Heidelberg Germany  
tél. : +1 415 336 6697  
mél : [Erik.Guttman@eng.sun.com](mailto:Erik.Guttman@eng.sun.com)

Charles E. Perkins  
Sun Microsystems  
2550 Garcia Avenue  
Mountain View, CA 94043  
tél. : +1 415 336 7153  
mél : [cperkins@Corp.sun.com](mailto:cperkins@Corp.sun.com)

Scott Kaplan  
346 Fair Oaks St.  
San Francisco, CA 94110  
tél. : +1 415 285 4526  
mél : [scott@catch22.com](mailto:scott@catch22.com)