

Groupe de travail Réseau
Request for Comments : 2327
 Catégorie : Sur la voie de la normalisation
 Traduction Claude Brière de L'Isle

M. Handley, ISI/LBNL
 V. Jacobson, ISI/LBNL
 avril 1998

SDP : Protocole de description de session

Statut du présent mémoire

Le présent document spécifie un protocole Internet normalisé pour la communauté Internet. Il appelle à une discussion et à des suggestions pour son amélioration. Prière de se référer à l'édition en cours des "normes officielles de protocoles de l'Internet " (STD 1) pour voir l'état de la normalisation et le statut du présent protocole. La distribution de ce mémo n'est pas limitée.

Notice de copyright

Copyright (C) The Internet Society (1998). Tous droits réservés

Résumé

Le présent document définit le protocole de description de session (SDP, *Protocole de description de session*). SDP est destiné à la description des sessions multimédia pour les annonces de session, l'invitation à une session, et d'autres formes d'initiation de session multimédia.

Le présent document a été produit par le groupe de travail Multiparty Multimedia Session Control (MMUSIC) de l'IETF (*Internet Engineering Task Force*). Des commentaires sont sollicités et devraient être adressés à la liste de diffusion du groupe de travail à confctrl@isi.edu et/ou aux auteurs.

Table des matières

1 Introduction.....	1
2 Généralités.....	2
3 Glossaire des termes utilisés.....	2
3.1 Terminologie.....	2
4 Utilisation de SDP.....	3
4.1 Annonces en diffusion groupée.....	3
4.2 Annonces email et WWW.....	3
5 Prescriptions et recommandations.....	3
5.1 Informations sur le support.....	4
5.2 Informations d'horaire.....	4
5.3 Sessions privées.....	4
5.4 Obtenir d'autres informations sur une session.....	4
5.5 Catégorisation.....	5
5.6 Internationalisation.....	5
6 Spécification de SDP.....	5
6.1 Communication de la politique de contrôle de Conférence.....	17
7 Considérations sur la sécurité.....	17
Appendice A : Grammaire de SDP.....	18
Appendice B : Lignes directrices pour l'enregistrement des noms SDP auprès de l'IANA.....	20
Appendice C : Adresse des auteurs.....	22
Remerciements.....	22
Références.....	22
Déclaration de droits de propriété intellectuelle.....	23

1 Introduction

Sur le réseau dorsal de diffusion groupée de l'Internet (Mbone), un outil de répertoire de sessions est utilisé pour publier les

conférences multimédia et communiquer les adresses de conférence et les informations spécifiques de l'outil pour la conférence nécessaires pour y participer. Le présent document définit un protocole de description de session à cette fin, et pour les besoins de la description générale de session multimédia en temps réel. Le présent mémo ne décrit pas l'allocation des adresses de diffusion groupée ni des détails de la distribution des messages SDP. Elles sont décrites dans d'autres RFC. SDP n'est pas destiné à la négociation des codages de support.

2 Généralités

Le Mbone est la partie de l'Internet qui prend en charge la diffusion groupée IP, et permet donc des communications efficaces de beaucoup à beaucoup. Il est largement utilisé pour tenir des conférences multimédia. De telles conférences ont habituellement pour propriété qu'il n'est pas nécessaire d'avoir une étroite coordination des membres de la conférence ; pour participer à une conférence, un utilisateur d'un site Mbone a juste besoin de savoir l'adresse du groupe de diffusion groupée de la conférence et les accès UDP des flux de données de conférence.

Les répertoires de session aident à la publicité des sessions de conférence et communiquent les informations pertinentes pour l'établissement de la conférence aux participants potentiels. SDP est conçu pour convoier de telles informations aux destinataires. SDP est uniquement un format pour la description de session - il n'incorpore pas de protocole de transport, et est destiné à utiliser différents protocoles de transport selon le besoin, y compris le protocole d'annonce de session [RFC2974], le protocole d'initialisation de session [RFC3261], le protocole de diffusion en temps réel [RFC2326], la messagerie électronique utilisant les extensions MIME, et le protocole de transport Hypertexte.

SDP est destiné à tous usages de sorte qu'il puisse servir dans une plus large gamme d'environnements de réseau et applications que le simple répertoire des sessions en diffusion groupée. Cependant, il n'est pas destiné à prendre en charge la négociation du contenu de session ou des codages de support - ceci est considéré comme en dehors de la portée de la description de session.

3 Glossaire des termes utilisés

Les termes suivants sont utilisés dans le présent document, et ont une signification spécifique dans ce contexte.

Conférence : Une conférence multimédia est un ensemble de deux ou plus utilisateurs en communication ainsi que le logiciel qu'ils utilisent pour communiquer.

Session multimédia : Une session multimédia est un ensemble d'expéditeurs et de receveurs multimédia et les flux de données qui vont des expéditeurs aux receveurs. Une conférence multimédia est un exemple de session multimédia.

Publicité de session : Voir annonce de session.

Annonce de session : C'est le mécanisme par lequel une description de session est envoyée aux utilisateurs d'une façon proactive, c'est-à-dire qu'une description de session n'a pas été explicitement demandée par l'utilisateur.

Description de session : Format bien défini pour convoier des informations suffisantes pour découvrir et participer à une session multimédia.

3.1 Terminologie

Les mots clé "DOIT", "NE DOIT PAS", "EXIGÉ", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans la [RFC2119].

4 Utilisation de SDP

4.1 Annonces en diffusion groupée

SDP est un protocole de description de session pour les sessions multimédia. Un mode d'utilisation courant est celui qui

permet à un client d'annoncer une session de conférence en multi diffusant périodiquement un paquet d'annonce à des adresses et accès de diffusion groupée bien connus en utilisant le protocole d'annonce de session (SAP, *Session Announcement Protocol*).

Les paquets SAP sont des paquets UDP avec le format suivant:

```
|-----|
| En-tête SAP          |
|-----|
| texte de charge utile |
|////////////////////
```

L'en-tête est celui du protocole d'annonce de session. SAP est décrit plus en détail dans un autre mémo [RFC2974].

La charge utile de texte est une description de session SDP, comme décrit dans le présent mémo. La charge utile de texte NE DEVRAIT PAS être supérieure à une longueur de 1 K octet. Si c'est annoncé par SAP, seule une annonce de session est permise dans un seul paquet.

4.2 Annonces email et WWW

D'autres moyens de convoier des descriptions de session incluent la messagerie électronique et la toile mondiale. Aussi bien la distribution de messagerie électronique que la toile mondiale DEVRAIENT utiliser le type de contenu MIME "application/sdp". Ceci permet le lancement automatique des applications pour la participation à la session à partir du client WWW ou du lecteur de messagerie d'une façon standard.

Noter que les annonces de sessions en diffusion groupée faites seulement via email ou par la toile mondiale (WWW) n'ont pas la propriété de faire que le receveur d'une annonce de session reçoive nécessairement la session parce que les sessions de diffusion groupée PEUVENT avoir un domaine d'application limité, et l'accès au serveur WWW ou la réception de courriels n'est pas possible en dehors de ce domaine. Les annonces SAP ne souffrent pas de ce dérangement.

5 Prescriptions et recommandations

L'objet de SDP est de convoier des informations sur les flux de support dans les sessions multimédia pour permettre aux receveurs d'une description de session de participer à la session. SDP est principalement destiné à être utilisé en inter-réseau, bien qu'il soit suffisamment général pour pouvoir décrire des conférences dans d'autres environnements de réseau.

Une session multimédia, est définie à cette fin comme un ensemble de flux de support qui existent pendant une certaine durée. Les flux de support peuvent être beaucoup à beaucoup. La durée pendant laquelle la session est active n'a pas besoin d'être continue.

Jusqu'ici les sessions fondées sur la diffusion groupée sur l'Internet différaient de nombreuses autres formes de conférence en ce que toute personne recevant le trafic pouvait se joindre à la session (sauf si le trafic de la session est crypté). Dans un tel environnement, SDP sert deux objectifs principaux. C'est un moyen de communiquer l'existence d'une session, et c'est un moyen de convoier des informations suffisantes pour permettre de se joindre à la session et d'y participer. Dans un environnement d'envoi individuel, seul le dernier objectif est vraisemblablement pertinent.

Et donc SDP inclut :

- o Le nom et l'objet de la session
- o L'heure ou les heures où la session est active
- o Le support comprenant la session
- o Les informations pour recevoir ces supports (adresses, ports, formats, etc.)

Comme les ressources nécessaires à la participation à une session PEUVENT être limitées, certaines informations supplémentaires PEUVENT être aussi souhaitables :

- o Des informations sur la bande passante à utiliser par les conférences
- o Des informations de contact pour la personne responsable de la session. En général, SDP DOIT convoier des informations suffisantes pour être capable de se joindre à une session (avec l'exception possible des clés de chiffrement)

et pour annoncer les ressources à utiliser que des non participants PEUVENT avoir besoin de connaître.

5.1 Informations sur le support

SDP inclut :

- o Le type de support (vidéo, audio, etc.)
- o Le protocole de transport (RTP/UDP/IP, H.320, etc.)
- o Le format de support (vidéo H.261, vidéo MPEG, etc.)

Pour une session IP en diffusion groupée, sont aussi envoyés ce qui suit :

- o L'adresse de diffusion groupée pour le support
- o L'accès de transport pour le support

Ces adresse et accès sont l'adresse de destination et l'accès de destination du flux de diffusion groupée, qu'il soit envoyé, reçu, ou les deux.

Pour une session IP en envoi individuel, sont envoyés ce qui suit :

- o L'adresse distante pour le support
- o L'accès de transport pour l'adresse de contact.

La sémantique de ces adresse et accès dépend du support et du protocole de transport définis. Par défaut, c'est l'adresse distante et l'accès distant auquel sont envoyées les données, et l'adresse distante et l'accès local sur lesquels recevoir les données. Cependant, certains supports PEUVENT définir de les utiliser pour établir un canal de commande pour le flux de support réel.

5.2 Informations d'horaire

Les sessions PEUVENT être limitées ou non dans le temps. Qu'elles soient ou non limitées, ELLE PEUVENT n'être actives qu'à des horaires spécifiques.

SDP peut convoier :

- o Une liste arbitraire d'heures de début et de fin limitant la session
- o Pour chaque limite, une heure répétitive, du style "chaque mercredi à 10 h pour une heure".

Ces informations d'horaire sont cohérentes au plan mondial, sans considération de la zone horaire locale ou de l'horaire d'été éventuel.

5.3 Sessions privées

Il est possible de créer à la fois des sessions publiques et des sessions privées. Les sessions privées seront normalement envoyées en cryptant la description de session pour la distribuer. Les détails sur la façon de crypter dépendent du mécanisme utilisé pour convoier SDP - voir [RFC2974] pour la façon dont ceci est fait pour les annonces de sessions.

Si une annonce de session est privée, il est possible d'utiliser cette annonce privée pour convoier les clés de chiffrement nécessaires pour décoder chacun des supports d'une conférence, y compris des informations suffisantes pour savoir quel schéma de chiffrement est utilisé pour chaque support.

5.4 Obtenir d'autres informations sur une session

Une description de session DEVRAIT convoier suffisamment d'informations pour décider de participer ou non à une session. SDP PEUT inclure des pointeurs supplémentaires sous la forme d'identifiants de ressources universels (URI, *Universal Resource Identifier*) pour des informations complémentaires sur la session.

5.5 Catégorisation

Lorsque de nombreuses descriptions de session sont distribuées par SAP ou tout autre mécanisme de publicité, il PEUT être souhaitable de filtrer les annonces intéressantes pour les séparer de celles qui ne le sont pas. SDP prend en charge un

mécanisme de catégorisation pour les sessions, qui peut être automatisé.

5.6 Internationalisation

La spécification SDP recommande l'utilisation de l'ensemble de caractères ISO 10646 dans le codage UTF-8 [RFC2044] pour permettre de représenter de nombreux langages différents. Cependant, pour aider les représentations compactes, SDP admet aussi que soient utilisés si désiré d'autres ensembles de caractères tels que ISO 8859-1. L'internationalisation ne s'applique qu'aux champs de texte libre (nom de session et informations de base), et non à SDP en tant que tel.

6 Spécification de SDP

Les descriptions de session SDP sont entièrement textuelles et utilisent l'ensemble de caractères ISO 10646 en codage UTF-8. Les noms de champ et les noms d'attributs SDP utilisent seulement le sous-ensemble US-ASCII de l'UTF-8, mais les champs textuels et les valeurs d'attribut PEUVENT utiliser l'ensemble complet de caractères ISO 10646. La forme textuelle, par opposition aux codages binaires tels que ASN/1 ou XDR, a été choisie pour améliorer la portabilité, pour permettre d'utiliser divers transports (par exemple, la description de session dans un message électronique MIME) et pour permettre que des boîtes à outils souples, fondées sur le texte (par exemple, Tcl/Tk) soient utilisées pour générer et traiter les description de sessions. Cependant, comme la bande passante totale allouée à toutes les annonces SAP est strictement limitée, le codage est délibérément compact. Aussi, comme les annonces PEUVENT être transportées via des moyens très peu fiables (par exemple, email) ou endommagées par un serveur cache intermédiaire, le codage a été conçu avec des règles strictes d'ordre et de formatage de sorte que la plupart des erreurs résulteraient en annonces mal formées qui pourraient être facilement détectées et éliminées. Cela permet aussi une élimination rapide des annonces cryptées pour lesquelles un récepteur ne dispose pas de la clé correcte.

Une description de session SDP consiste en un certain nombre de lignes de texte de la forme <type>=<valeur>. <type> est toujours exactement de un caractère et est sensible à la casse. <valeur> est une chaîne textuelle structurée dont le format dépend du <type>. Elle sera aussi sensible à la casse, sauf si un champ spécifique la définit autrement. Les espaces blanches ne sont pas permises de part et d'autre du signe "=". En général <valeur> est soit un nombre de champs délimité par un caractère d'espace simple ou une chaîne de format libre.

Une description de session consiste en une description de niveau de session (détails qui s'appliquent à toute la session et à tous les flux de support) et FACULTATIVEMENT en plusieurs descriptions de niveau support (détails qui s'appliquent seulement à un seul flux de supports).

Une annonce consiste en une section de niveau session suivie par zéro ou plus sections de niveau support. La partie niveau session commence par une ligne "v=" et continue jusqu'à la première section de niveau support. La description de support commence par une ligne "m=" et continue jusqu'à la prochaine description de support ou la fin de toute la description de session. En général, les valeurs de niveau de session sont les valeurs par défaut pour tout le support à moins qu'elles ne soient supplantées par une valeur équivalente de niveau support.

Lorsque SDP est convoyé par SAP, seule une description de session est permise par paquet. Lorsque SDP est convoyé par d'autres moyens, de nombreuses descriptions de session SDP PEUVENT être enchaînées ensemble (la ligne "v=" indiquant le début d'une description de session termine la description précédente). Certaines lignes dans chaque description sont EXIGÉES et certaines sont FACULTATIVES mais toutes DOIVENT apparaître exactement dans l'ordre donné ici (l'ordre fixé améliore grandement la détection d'erreur et permet un analyseur simple). Les éléments FACULTATIFS sont marqués par un "*".

Description de session

- v= (version du protocole)
- o= (identifiant de propriétaire/créateur et de session).
- s= (nom de session)
- i=* (informations de session)
- u=* (URI de description)
- e=* (adresse électronique)
- p=* (numéro de téléphone)
- c=* (informations de connexion - non EXIGÉES si incluses dans tous les supports)
- b=* (informations de bande passante)

Une ou plusieurs descriptions d'horaire (voir ci-dessous)

z=* (réglages de zone horaire)

k=* (clés de chiffrement)

a=* (zéro ou plus lignes d'attribut de session)

Zéro ou plus descriptions de support (voir ci-dessous)

Description de l'heure

t= (heure d'activité de la session)

r=* (zéro ou plus heures de répétition)

Description du support

m= (nom du support et adresse de transport)

i=* (titre du support)

c=* (informations de connexion - FACULTATIF si inclus au niveau session)

b=* (informations de bande passante)

k=* (clé de chiffrement)

a=* (zéro ou plus lignes d'attribut de support)

L'ensemble des lettres "type" est délibérément petit et n'est pas destiné à être extensible -- les analyseurs SDP DOIVENT complètement ignorer toute annonce contenant une lettre "type" qu'il ne comprend pas. Le mécanisme "attribut" ("a=" décrit ci-dessous) est le moyen principal d'extension de SDP et de le tailler sur mesure pour des applications ou supports particuliers. Certains attributs (ceux énumérés dans le présent document) ont une signification définie mais d'autres PEUVENT être ajoutés sur une base spécifique de l'application, du support ou de la session. Un répertoire de session DOIT ignorer tout attribut qu'il ne comprend pas.

Les informations de connexion ("c=") et d'attribut ("a=") dans la section de niveau session s'appliquent à tous les supports de cette session à moins qu'elles ne soient supplantées par des informations de connexion ou un attribut de même nom dans la description de support. Dans l'exemple ci-dessous, chaque support se comporte comme si il avait reçu un attribut "recvonly".

Un exemple de description SDP est :

```
v=0
o=mhandley 2890844526 2890842807 IN IP4 126.16.64.4
s=Séminaire SDP
i=Séminaire sur le protocole de description de session
u=http://www.cs.ucl.ac.uk/staff/M.Handley/sdp.03.ps
e=mjh@isi.edu (Mark Handley)
c=IN IP4 224.2.17.12/127
t=2873397496 2873404696
a=recvonly
m=audio 49170 RTP/AVP 0
m=video 51372 RTP/AVP 31
m=application 32416 udp wb
a=orient:portrait
```

Les mentions textuelles comme le nom de session et les informations sont des chaînes d'octets qui PEUVENT contenir tout octet à l'exception de 0x00 (Nul), 0x0a (saut de ligne ASCII) et 0x0d (retour chariot ASCII). La séquence CRLF (0x0d0a) est utilisée pour terminer une mention, bien que les analyseurs DEVRAIENT être tolérants et accepter aussi les mentions terminées par un seul caractère de saut de ligne. Par défaut, ces chaînes d'octets contiennent des caractères ISO-10646 en codage UTF-8, mais cette valeur par défaut PEUT être changée en utilisant l'attribut "jeu de caractères".

Version du protocole

v=0

Le champ "v=" donne la version du protocole de description de session.

Il n'y a pas de numéro de version mineur.

Origine

o=<nom d'utilisateur> <identifiant de session> <version> <type de réseau> <type d'adresse> <adresse>

Le champ "o=" donne l'origine de la session (son nom d'utilisateur et l'adresse de l'hôte de l'utilisateur) plus un id de session et un numéro de version de session.

<nom d'utilisateur> est le nom d'enregistrement de l'utilisateur sur l'hôte d'origine, ou c'est "-" si l'hôte d'origine ne prend pas en charge le concept d'identifiant d'utilisateur. <username> NE DOIT PAS contenir d'espaces. <session id> est une chaîne numérique telle que le tuple <username>, <identifiant de session>, <type de réseau>, <type d'adresse> et <adresse> forme un identifiant mondialement unique pour la session.

La méthode d'allocation de <session id> est à la discrétion de l'outil de création, mais il a été suggéré qu'un horodatage du protocole de l'heure du réseau (NTP, *Network Time Protocol*) soit utilisé pour assurer son unicité [RFC1305].

<version> est un numéro de version pour cette annonce. Il est nécessaire que les annonces de mandataire détectent laquelle des diverses annonces est la plus récente pour la même session. Cette utilisation est elle aussi à la discrétion de l'outil de création, du moment que <version> est augmenté lorsqu'une modification est faite aux données de la session. Il est aussi RECOMMANDÉ (mais pas obligatoire) d'utiliser un horodatage NTP.

<type de réseau> est une chaîne textuelle qui donne le type de réseau. Au départ "IN" est défini comme signifiant "Internet". <type d'adresse> est une chaîne textuelle qui donne le type de l'adresse qui suit. Au départ "IP4" et "IP6" sont définis. <adresse> est l'adresse unique au monde de la machine d'après laquelle la session a été créée. Pour un type d'adresse de IP4, c'est soit le nom de domaine pleinement qualifié de la machine, soit la représentation en décimal séparé par des virgules de la version IPv4 de l'adresse de la machine. Pour un type d'adresse de IPv6, c'est soit le nom de domaine pleinement qualifié de la machine, soit la représentation textuelle compressée de l'adresse IP v6 de la machine. Aussi bien pour IP4 qu'IP6, le nom de domaine pleinement qualifié est la forme qui DEVRAIT être donnée sauf si elle est indisponible, auquel cas l'adresse unique au monde PEUT y être substituée. Une adresse IP locale NE DOIT PAS être utilisée dans un contexte où la description SDP pourrait quitter le domaine d'application dans lequel l'adresse est significative.

En général, le champ "o=" sert d'identifiant mondialement unique pour cette version de cette description de session, et les sous-champs pris tous ensemble identifient la session sans tenir compte des modifications éventuelles.

Nom de session
s=<nom de session>

Le champ "s=" est le nom de session. Il DOIT y avoir un champ "s=" et un seul par description de session, et il DOIT contenir des caractères ISO 10646 (mais voir aussi l'attribut 'jeu de caractères' ci-dessous).

Informations de session et de support
i=<description de session>

Le champ "i=" est d'informations sur la session. Il PEUT y avoir au plus un champ "i=" de niveau session par description de session, et au plus un champ "i=" par support. Bien qu'il PUISSE être omis, c'est déconseillé pour les annonces de session, et les interfaces d'utilisateur pour la composition des sessions DEVRAIENT exiger que du texte soit entré. S'il est présent, il DOIT contenir des caractères ISO 10646 (mais voir aussi l'attribut "jeu de caractères" ci-dessous).

Un seul champ "i=" peut aussi être utilisé pour chaque définition de support. Dans les définitions de support, les champs "i=" sont principalement destinés à l'étiquetage des flux de support. Comme tels, ils seront le plus vraisemblablement utiles lorsqu'une seule session a plus d'un flux de support distinct du même type de support. Ce pourrait, par exemple, être deux tableaux, l'un pour les transparents et l'autre pour les réactions et questions.

URI
u=<URI>

- o Un URI est un identifiant de ressources universel tel qu'utilisé par les clients WWW.
- o L'URI DEVRAIT être un pointeur sur des informations complémentaire sur la conférence.
- o Ce champ est FACULTATIF, mais s'il est présent, il DEVRAIT être spécifié avant le premier champ de support.
- o Pas plus d'un champ URI n'est permis par description de session.

Adresse de messagerie électronique et numéro de téléphone
e=<adresse email>

p=<numéro de téléphone>

- o Ils spécifient les informations de contact pour la personne responsable de la conférence. Ce n'est pas nécessairement la même personne qui a créé l'annonce de la conférence.
- o Un champ email ou un champ téléphone DOIT être spécifié. Des champs email et téléphone supplémentaires sont admis.
- o Si ils sont présents, ils DEVRAIENT être spécifiés avant le premier champ de support.
- o Plus d'un champ email ou téléphone peut être donné pour une description de session.
- o Les numéros de téléphone DEVRAIENT être donnés dans le format international conventionnel - précédé par un "+" et le code international du pays. Il DOIT y avoir une espace ou un trait d'union ("-") entre le code du pays et le reste du numéro de téléphone. Les espaces et traits d'union PEUVENT être utilisés pour partager un champ téléphone pour aider, si c'est souhaité, la lisibilité. Par exemple :
 p=+44-171-380-7777 ou p=+1 617 253 6011
- o Adresses email et numéros de téléphone peuvent tous deux avoir une chaîne FACULTATIVE de texte libre associée, donnant normalement le nom de la personne qui PEUT être contactée. Ceci DEVRAIT être mis entre parenthèses s'il est présent. Par exemple :

e=mjh@isi.edu (Mark Handley)

L'autre convention de citation des noms de la RFC 822 est aussi admise à la fois pour les adresses email et les numéros de téléphone. Par exemple,

e=Mark Handley <mjh@isi.edu>

La chaîne de texte libre DEVRAIT être de l'ensemble de caractères ISO-10646 avec codage UTF-8, ou autrement en ISO-8859-1 ou d'autres codages si l'attribut approprié de jeu de caractères de niveau session est mis.

Données de connexion

c=<type de réseau> <type d'adresse> <adresse de connexion>

Le champ "c=" contient les données de connexion.

Une annonce de session DOIT contenir un champ "c=" dans chaque description de support (voir ci-dessous) ou un champ "c=" au niveau session. Il PEUT contenir un champ "c=" de niveau session et un champ "c=" supplémentaire par description de support, auquel cas les valeurs par support supplantent les réglages de niveau session pour les supports en cause.

Le premier sous champ est le type de réseau, qui est une chaîne textuelle qui donne le type de réseau. Initialement, "IN" est défini comme ayant la signification "Internet".

Le second sous champ est le type d'adresse. Ceci permet d'utiliser SDP pour des sessions qui ne sont pas fondées sur IP. Actuellement, seul IP4 est défini.

Le troisième sous-champ est l'adresse de connexion. Des sous-champs supplémentaires FACULTATIFS PEUVENT être ajoutés après l'adresse de connexion en fonction de la valeur du champ <type d'adresse>.

Pour les adresses IP4, l'adresse de connexion se définit comme suit :

- o Normalement l'adresse de connexion sera une adresse de groupe diffusion groupée IP de classe D. Si la session n'est pas en diffusion groupée, l'adresse de connexion contient alors le nom de domaine pleinement qualifié ou l'adresse IP en envoi individuel de la source de données ou relais de données ou collecteur de données attendu comme déterminé par les champs d'attribut supplémentaires. Il n'est pas prévu que des noms de domaine pleinement qualifié ou des adresses en envoi individuel soient données dans une description de session communiquée par une annonce en diffusion groupée, bien que ce ne soit pas interdit. Si un flux de données en envoi individuel doit passer par un traducteur d'adresses réseau, l'utilisation d'un nom de domaine pleinement qualifié plutôt que d'une adresse IP en envoi individuel est RECOMMANDÉE. Dans les autres cas, l'utilisation d'une adresse IP pour spécifier une interface particulière sur un hôte à rattachements multiples peut être EXIGÉE. Et donc la présente spécification laisse aux applications individuelles la décision sur celle à retenir, mais toutes les applications DOIVENT être capable de recevoir les deux formats.
- o Les conférences utilisant une adresse de connexion IP en diffusion groupée DOIVENT aussi avoir une valeur de durée de vie (TTL, *time to live*) en plus de l'adresse de diffusion groupée. La durée de vie et l'adresse définissent ensemble le domaine d'application dans lequel seront envoyés les paquets en diffusion groupée dans cette conférence. Les valeurs de

durée de vie DOIVENT être dans la gamme 0-255.

La durée de vie pour la session est ajoutée à l'adresse en utilisant une barre oblique comme séparateur. A titre d'exemple :

```
c=IN IP4 224.2.1.1/127
```

Les schémas de codage hiérarchiques ou stratifiés sont des flux de données dans lesquels le codage provenant d'une seule source support est partagé en un certain nombre de couches. Le receveur peut choisir la qualité désirée (et donc la bande passante) en s'abonnant à seulement un sous-ensemble de ces couches. De tels codages stratifiés sont normalement transmis en plusieurs groupes de diffusion groupée pour permettre un élagage de la diffusion groupée. Cette technique écarte le trafic non désiré des sites qui n'exigent que certains niveaux de la hiérarchie. Pour les applications exigeant plusieurs groupes de diffusion groupée, on autorise l'utilisation de la notation suivante pour l'adresse de connexion :

```
<adresse diffusion groupée de base>/<ttl>/<nombre d'adresses>
```

Si le nombre des adresses n'est pas donné, il est supposé être de un. Les adresses de diffusion groupée ainsi allouées le sont de façon contiguë au-dessus de l'adresse de base, de sorte que, par exemple :

```
c=IN IP4 224.2.1.1/127/3
```

établirait que les adresses 224.2.1.1, 224.2.1.2 et 224.2.1.3 sont à utiliser dans une durée de vie de 127. Ce qui est sémantiquement identique à l'inclusion de plusieurs lignes "c=" dans une description de support :

```
c=IN IP4 224.2.1.1/127
c=IN IP4 224.2.1.2/127
c=IN IP4 224.2.1.3/127
```

Plusieurs adresses ou lignes "c=" peuvent seulement être spécifiées support par support, et pas pour un champ "c=" de niveau session.

Il est illégal d'utiliser la notation de barre oblique décrite ci-dessus pour les adresses IP en envoi individuel.

Bande passante

b=<modificateur>:<valeur-de-bande-passante>

- o Cela spécifie la bande passante dont l'utilisation est proposée par la session ou support, et elle est FACULTATIVE.
- o <valeur-de-bande-passante> est en kilo bits par seconde
- o <modificateur> est un seul mot alphanumérique qui donne la signification du chiffre de la bande passante.
- o Deux modificateurs sont définis initialement :

CT (Conference Total) : Une bande passante maximum implicite est associée à chaque durée de vie sur le Mbone ou au sein d'une région de domaine d'application administrative particulière de diffusion groupée (la bande passante du Mbone est donnée par rapport aux limites de durée de vie dans le MBone FAQ). Si la bande passante dans une session ou le support dans une session est différent de la bande passant implicite d'après le domaine d'application, une ligne "b=CT:..." DEVRAIT être fournie pour la session, donnant la limite supérieure proposée pour la bande passante utilisée. Le principal objet de cette disposition est de donner une idée approximative de la possibilité de faire coexister simultanément deux conférences ou plus.

AS (Application-Specific Maximum) : La bande passante est interprétée comme étant spécifique de l'application, c'est-à-dire qu'elle sera le concept de maximum de bande passante de l'application. Normalement, ceci va coïncider avec ce qui est établi sur la commande "maximum de bande passante" de l'application, si applicable.

Noter que CT donne un chiffre total de bande passante pour tous les supports de tous les sites. AS donne un chiffre de bande passante pour un seul support sur un seul site, bien qu'il PUISSE y avoir de nombreux sites émettant simultanément.

- o Mécanisme d'extension : Les rédacteurs d'outils peuvent définir des modificateurs expérimentaux de bande passante en mettant un préfixe "X-" à leur modificateur. Par exemple :

```
b=X-YZ:128
```

Les analyseurs SDP DEVRAIENT ignorer les champs de bande passante ayant des modificateurs inconnus. Le modificateur DEVRAIT être alphanumérique, et, bien qu'aucune limite de longueur ne soit donnée, il est RECOMMANDÉ qu'il soit court.

Horaires, horaires répétitifs et zones horaires

t=<heure de début> <heure de fin>

- o les champs "t=" spécifient l'heure de début et l'heure de fin d'une session de conférence. Plusieurs champs "t=" PEUVENT être utilisés si une session est active à des horaires espacés de façon irrégulière dans le temps ; chaque champ "t=" supplémentaire spécifie une période de temps additionnelle pendant laquelle la session sera active. Si la session est active à des périodes régulières, un champ "r=" (voir ci-dessous) DEVRAIT être utilisé en plus d'un champ "t=" et à sa suite, auquel cas, le champ "t=" spécifie les heures de début et de fin de la séquence répétitive.
- o Le premier et le second sous-champ donnent respectivement les heures de début et les heures de fin de la conférence. Ces valeurs sont la représentation décimale de la valeur horaire du protocole de l'heure du réseau (NTP) [RFC1305] en secondes. Pour convertir ces valeurs en heure UNIX, soustraire 2 208 988 800 en décimal.
- o Si l'heure de fin est réglée à zéro, la session est alors non limitée, mais elle ne deviendra active qu'après l'heure de début. Si l'heure de début est aussi zéro, la session est considérée comme permanente.

Les interfaces d'utilisateur DEVRAIENT fortement décourager la création de sessions non limitées et permanentes car cela ne donne pas d'informations sur le moment où la session va réellement se terminer, et cela crée des difficultés de programmation.

On PEUT faire l'hypothèse générale, lors de l'affichage de sessions non limitées dont la fin n'a pas été indiquée aux utilisateurs, qu'une session non limitée ne sera active qu'une demie heure après l'heure en cours ou après l'heure de début de la session, selon celui qui est le plus tard. Si un comportement autre que celui-ci est EXIGÉ, une heure de fin DEVRAIT être donnée et modifiée en tant que de besoin lorsque de nouvelles informations deviennent disponibles sur le moment réel ou la session DEVRAIT finir.

Les sessions permanentes PEUVENT apparaître aux utilisateurs comme n'étant jamais actives à moins qu'elles ne soient associées à des horaires répétitifs qui établissent précisément quand la session sera active. En général, les sessions permanentes NE DEVRAIENT PAS être créées pour une session dont on attend qu'elle ait une durée inférieure à deux mois, et DEVRAIENT être déconseillées pour des sessions dont on s'attend à ce qu'elle aient une durée inférieure à 6 mois.

r=<intervalle de répétition> <durée active> <liste des décalages de début>

- o Les champs "r=" spécifient les horaires répétitifs pour une session. Par exemple, si une session est active à 10 h les lundis et à 11 h les mardis pour une heure chaque semaine pendant trois mois, <heure de début> dans le champ "t=" correspondant devra être la représentation NTP de 10 h le premier lundi, <intervalle de répétition> devra être 1 semaine, <durée active> devra être 1 heure, et les décalages devront être zéro et 25 heures. Le champ "t=" correspondant d'heure d'arrêt devra être la représentation NTP de la fin de la dernière session trois mois plus tard. Par défaut, tous les champs sont en secondes, de sorte que les champs "r=" et "t=" pourraient être :

```
t=3034423619 3042462419
r=604800 3600 0 90000
```

Pour compacter un peu plus les annonces, les horaires PEUVENT aussi être donnés en jours, heures, ou minutes. La syntaxe en est un nombre immédiatement suivi par un seul caractère sensible à la casse. Les fractions d'unité ne sont pas autorisées ; on DEVRAIT utiliser à la place des unités plus petites. Les caractères de spécification d'unités suivants sont admis :

```
d - jours (86400 secondes)
h - heures (3600 secondes)
m - minutes (60 secondes)
s - secondes (admis par souci d'exhaustivité, mais pas RECOMMANDÉ)
```

Et donc, l'annonce ci-dessus aurait pu aussi s'écrire :

```
r=7d 1h 0 25h
```

Les répétitions mensuelles et annuelles ne peuvent pas actuellement être directement spécifiées par un seul horaire répétitif SDP - des champs "t=" séparés DEVRAIENT être utilisés à la place pour faire explicitement la liste des horaires de session.

z=<ajustement d'horaire> <décalage> <ajustement d'horaire> <décalage>

- o Pour programmer une session répétitive qui s'étend sur l'horaire d'hiver et l'horaire d'été ou vice-versa, il est nécessaire de spécifier des décalages par rapport à l'horaire répétitif de base. Ceci est exigé parce que différentes zones horaires changent d'horaire à des heures différentes, différents pays changent d'horaire à des dates différentes, et certains pays n'ont pas de changement d'horaire du tout.

Et donc pour programmer une session qui est au même horaire en hiver et en été, il DOIT être possible de spécifier de façon non ambiguë dans quelle zone horaire une session est programmée. Pour simplifier la tâche pour les receveurs, on permet que l'expéditeur spécifie l'heure NTP à laquelle survient un ajustement d'horaire et le décalage par rapport à l'horaire auquel la session a été programmée pour la première fois. Le champ "z" permet à l'expéditeur de spécifier une liste de ces ajustements d'horaire et des décalages par rapport au temps de base.

Un exemple pourrait être :

z=2882844526 -1h 2898848070 0

Ceci spécifie qu'au temps 2882844526, la base de temps par rapport à laquelle l'horaire répétitif de la session est calculé est avancé d'une heure, et qu'au temps 2 898 848 070 la base de temps originale de la session est restaurée. Les ajustements sont toujours par rapport au temps de début spécifié - ils ne sont pas cumulatifs.

- o Si une session doit vraisemblablement durer plusieurs années, il faut s'attendre à ce que l'annonce de session soit modifiée périodiquement plutôt que de transmettre en une seule annonce des ajustements valables sur plusieurs années.

Clés de chiffrement

k=<méthode>

k=<méthode>:<clé de chiffrement>

- o Le protocole de description de session PEUT être utilisé pour convoyer des clés de chiffrement. Un champ de clé est permis avant la première entrée de support (auquel cas il s'applique à tous les supports de la session), ou pour chaque entrée de support en tant que de besoin.
- o Le format des clés et leur utilisation sont en dehors du domaine d'application du présent document, mais voir la [RFC1890].
- o La méthode indique le mécanisme à utiliser pour obtenir une clé utilisable par des moyens externes, ou à partir de la clé de chiffrement codée donnée.

Les méthodes suivantes sont définies :

k=clear:<clé de chiffrement>

La clé de chiffrement (comme décrit en [RFC1890] pour les flux de support RTP sous le profil AV) est incluse non transformée dans ce champ clé.

k=base64:<clé de chiffrement codée>

La clé de chiffrement (comme décrit dans la [RFC1890] pour les flux de support RTP sous le profil AV) est incluse dans ce champ clé mais a été codée en base64 parce qu'elle inclut des caractères qui sont interdits dans SDP.

k=uri:<URI pour obtenir les clés>

Un identifiant de ressources universel tel qu'utilisé par les clients de la toile mondiale est inclus dans ce champ de clé. L'URI se réfère aux données qui contiennent la clé, et PEUT requérir une authentification supplémentaire avant que la clé puisse être retournée. Lorsqu'une demande est faite à un URI donné, le type de contenu MIME de la réponse spécifie le codage pour la clé dans la réponse. La clé NE DEVRAIT PAS être obtenue tant que l'utilisateur ne souhaite pas se joindre à la session pour réduire la synchronisation des demandes pour le ou les serveurs de la toile mondiale.

k=prompt

Aucune clé n'est incluse dans cette description SDP, mais la session ou flux de supports à laquelle se réfère ce champ de clé est chiffré. La clé DEVRAIT être fournie à l'utilisateur lorsqu'il tente de se joindre à la session, et cette clé fournie à l'utilisateur DEVRAIT alors être utilisée pour déchiffrer le flux de supports.

Attributs

a=<attribut>

a=<attribut>:<valeur>

Les attributs sont le principal moyen d'extension de SDP. Les attributs PEUVENT être définis pour être utilisés comme attributs de "niveau session", attributs de "niveau support", ou les deux.

Une description de support PEUT avoir tout nombre d'attributs (champs "a=") qui sont spécifiques du support. On s'y réfère comme à des attributs de "niveau support" et des informations supplémentaires sur le flux de support. Les champs d'attribut peuvent aussi être ajoutés avant le premier champ de supports ; ces attributs de "niveau session" transportent les informations supplémentaires qui s'appliquent à la conférence comme un tout plutôt qu'à un support individuel ; un exemple pourrait être la politique de contrôle des débats de la conférence.

Les champs d'attribut PEUVENT être de deux formes :

- o attributs de propriété. Un attribut de propriété est simplement de la forme "a=<fanion>". Ce sont des attributs binaires, et la présence de l'attribut marque que l'attribut est une propriété de la session. Un exemple pourrait être "a=recvonly" (*réception seule*).
- o attributs de valeur. Un attribut de valeur est de la forme "a=<attribut>:<valeur>". Un exemple pourrait être qu'un tableau blanc pourrait avoir l'attribut de valeur "a=orient:paysage"

L'interprétation des attributs dépend de l'outil de support qui est invoqué. Et donc les receveurs des descriptions de session DEVRAIENT être configurables dans leur interprétation des annonces en général et des attributs en particulier.

Les noms des attributs DOIVENT être dans le sous-ensemble US-ASCII de l'ISO-10646/UTF-8.

Les valeurs d'attribut sont des chaînes d'octets, et PEUVENT utiliser toute valeur d'octet excepté 0x00 (Nul), 0x0A (LF), et 0x0D (CR). Par défaut, les valeurs d'attribut sont à interpréter comme dans l'ensemble de caractères ISO-10646 avec le codage UTF-8. A la différence des autres champs textuels, les valeurs d'attribut ne SONT PAS normalement affectées par l'attribut "jeu de caractères" car cela rendrait problématiques les comparaisons par rapport aux valeurs connues. Cependant, lorsqu'un attribut est défini, il peut être défini comme étant dépendant de jeu de caractères, auquel cas sa valeur DEVRAIT être interprétée dans le jeu de caractères de la session plutôt que dans ISO-10646.

Les attributs qui seront communément utilisés peuvent être enregistrés auprès de l'IANA (voir l'Appendice B). Les attributs non enregistrés DEVRAIENT commencer par "X-" pour empêcher des collisions par inadvertance avec des attributs enregistrés. Dans tous les cas, si un attribut reçu n'est pas compris, il DEVRAIT simplement être ignoré par le receveur.

Annonces de support

m=<support> <accès> <transport> <liste fmt>

Une description de session PEUT contenir un certain nombre de descriptions de supports. Chaque description de support commence par un champ "m=", et se termine par le prochain champ "m=" ou par la fin de la description de session. Un champ de support a aussi plusieurs sous-champs :

- o Le premier sous-champ est le type de support. Les supports couramment définis sont "audio", "vidéo", "application", "données" et "contrôle", bien que cette liste PUISSE être étendue avec l'émergence de nouvelles modalités de communication (par exemple, télé présence). La différence entre "application" et "données" est que cette dernière est un flux de support comme une information de tableau blanc, et que la dernière est du transfert de données en vrac tel que de la diffusion groupée d'exécutables de programmes ce qui n'est normalement pas affiché pour l'utilisateur. "contrôle" est utilisé pour spécifier un canal de contrôle de conférence supplémentaire pour la session.
- o Le second sous-champ est l'accès de transport auquel le flux de support devra être envoyé. La signification de l'accès de transport dépend du réseau utilisé comme spécifié dans le champ "c" pertinent et du protocole de transport défini dans le troisième sous-champ. Les autres accès utilisés par l'application de support (tels que l'accès RTCP, voir [RFC1889]) DEVRAIENT être déduits par un algorithme à partir de l'accès du support de base.

Note : Pour les transports fondés sur UDP, la valeur DEVRAIT être dans la gamme 1024 à 65535 inclus. Pour la conformité à RTP, il DEVRAIT être un nombre pair.

Pour les applications où des flux codés hiérarchiquement sont envoyés à une adresse en envoi individuel, il PEUT être nécessaire de spécifier plusieurs accès de transport. Cela est fait en utilisant une notation similaire à celle utilisée pour les

adresses IP en diffusion groupée dans le champ "c=" :

m=<support> <accès>/<nombre d'accès> <transport> <liste fmt>

Dans un tel cas, les accès utilisés dépendent du protocole de transport. Pour RTP, seuls les accès pairs sont utilisés pour les données et l'accès impair supérieur d'un correspondant est utilisé pour RTCP. Par exemple :

m=video 49170/2 RTP/AVP 31

spécifierait que les accès 49170 et 49171 forment une paire RTP/RTCP et 49172 et 49173 forment la seconde paire RTP/RTCP. RTP/AVP est le protocole de transport et 31 est le format (voir ci-dessous).

Il est illégal à la fois pour les adresses multiples d'être spécifiées dans le champ "c=" et pour les accès multiples d'être spécifiés dans le champ "m=" dans la même description de session.

- o Le troisième sous-champ est le protocole de transport. Les valeurs de protocole de transport dépendent du champ type-d'adresse dans les champs "c=". Et donc un champ "c=" d'IP4 définit que le protocole de transport fonctionne sur IP4. Pour IP4, on s'attend normalement à ce que la plupart du trafic de support soit transporté comme RTP sur UDP. Les protocoles de transport suivants sont prédéfinis, mais PEUVENT être étendus par l'enregistrement de nouveaux protocoles auprès de l'IANA :
 - RTP/AVP : protocole de transport en temps réel de l'IETF utilisant le profil Audio/Vidéo porté sur UDP.
 - udp : protocole de datagrammes d'utilisateur.

Si une application utilise un seul format combiné propriétaire de format de support et de protocole de transport sur UDP, spécifier simplement le protocole de transport comme udp et utiliser le champ format pour distinguer le protocole combiné est RECOMMANDÉ. Si un protocole de transport est utilisé sur UDP pour porter plusieurs types de supports distincts qui ont besoin d'être distingués par un répertoire de session, il est alors nécessaire de spécifier séparément le protocole de transport et le format de support. RTP est un exemple d'un protocole de transport qui porte plusieurs formats de charge utile qui DOIVENT être distingués par le répertoire de sessions pour qu'il sache comment lancer les outils, relais, mixeurs ou enregistreurs appropriés.

La principale raison pour spécifier le protocole de transport en plus du format de support est que les mêmes formats de supports standard PEUVENT être portés sur différents protocoles de transport même lorsque le protocole réseau est le même - un exemple historique est vat PCM audio et RTP PCM audio. De plus les relais et outils de surveillance qui sont spécifiques du protocole de transport mais indépendants du format sont possibles.

Pour les flux de support RTP fonctionnant sous le profil RTP Audio/Vidéo [RFC1890], le champ protocole est "RTP/AVP". Si d'autres profils RTP DEVAIENT être définis à l'avenir, leurs profils devraient être spécifiés de la même façon. Par exemple, le champ protocole "RTP/XYZ" spécifierait RTP fonctionnant sous un profil dont le nom abrégé est "XYZ".

- o Le quatrième sous-champ et les suivants sont des formats de supports. Pour l'audio et la vidéo, ce seront normalement un type de charge utile de support comme défini dans le profil RTP Audio/Vidéo.

Lorsqu'une liste de formats de charge utile est donnée, cela implique que tous ces formats PEUVENT être utilisés dans la session, mais le premier de ces formats est le format par défaut pour la session.

Pour les supports dont le protocole de transport n'est pas RTP ou UDP, le champ format est spécifique du protocole. De tels formats DEVRAIENT être définis dans un document de spécification supplémentaire.

Pour les supports dont le protocole de transport est RTP, SDP peut être utilisé pour fournir un lien dynamique du codage du support au type de charge utile RTP. Les noms de codage dans le profil RTP AV ne spécifient pas de codages audio uniques (en termes de débit d'horloge et de nombre de canaux audio) de sorte qu'ils ne sont pas utilisés directement dans les champs format SDP. Au lieu de cela, le numéro de type de charge utile DEVRAIT être utilisé pour spécifier le format pour les types de charge utile statique et le numéro de type de charge utile avec les informations de codage supplémentaires DEVRAIT être utilisé pour les types de charges utiles allouées de façon dynamique.

Un exemple de type de charge utile statique est le MIC de loi μ codé en un seul canal audio échantillonné à 8 kHz. Ceci est complètement défini dans le profil RTP Audio/Vidéo comme charge utile de type 0, de sorte que le champ support pour un tel flux envoyé à l'accès UDP 49232 est :

```
m=video 49232 RTP/AVP 0
```

Un exemple de type de charge utile dynamique est l'audio stéréo codé linéaire à 16 bits échantillonné à 16 kHz. Si on souhaite utiliser le type de charge utile RTP/AVP dynamique 98 pour un tel flux, des informations supplémentaires sont requises pour le décoder :

```
m=video 49232 RTP/AVP 98
a=rtpmap:98 L16/16000/2
```

La forme générale d'un attribut rtpmap est :

```
a=rtpmap:<type de charge utile> <nom de codage>/<débit d'horloge>[/<paramètres de codage>]
```

Pour les flux audio, <paramètres de codage> PEUT spécifier le nombre de canaux audio. Ce paramètre PEUT être omis si le nombre de canaux est un, pourvu qu'aucun paramètre additionnel ne soit nécessaire. Pour les flux vidéo, aucun paramètre de codage n'est actuellement spécifié.

Des paramètres supplémentaires POURRONT être définis à l'avenir, mais des paramètres spécifiques de codec NE DEVRAIENT PAS être ajoutés. Les paramètres ajoutés à un attribut rtpmap DEVRAIENT seulement être ceux EXIGÉS pour un répertoire de session pour faire le choix du support approprié pour participer à une session. Les paramètres spécifiques de codec DEVRAIENT être ajoutés dans d'autres attributs.

Un attribut rtpmap peut être défini pour chaque format de support spécifié. Et donc on pourrait avoir :

```
m=audio 49230 RTP/AVP 96 97 98
a=rtpmap:96 L8/8000
a=rtpmap:97 L16/8000
a=rtpmap:98 L16/11025/2
```

Les profils RTP qui spécifient l'utilisation de types de charge utile dynamiques DOIVENT définir l'ensemble de noms de codage valides et/ou de moyens d'enregistrer des noms de codage si ce profil doit être utilisé avec SDP.

Des formats de codage expérimentaux peuvent aussi être spécifiés en utilisant rtpmap. Les formats RTP qui ne sont pas enregistrés comme noms de format standard DOIVENT être précédés par "X-". Et donc un nouveau format audio redondant expérimental appelé GSMLPC utilisant le type de charge utile dynamique 99 pourrait être spécifié comme :

```
m=video 49232 RTP/AVP 99
a=rtpmap:99 X-GSMLPC/8000
```

Un tel codage expérimental exige que tout site souhaitant recevoir le flux de support ait l'état configuré pertinent dans son répertoire de session pour savoir quels outils sont appropriés.

Noter que les formats audio RTP n'incluent pas normalement d'informations sur le nombre d'échantillons par paquet. Si une mise en paquet qui n'est pas par défaut (comme défini dans le profil RTP Audio/Vidéo) est exigée, l'attribut "ptime" est utilisé comme donné ci-dessous.

Pour des précisions sur les formats RTP audio et vidéo, voir la [RFC1890].

- o Les formats pour les supports non RTP DEVRAIENT être enregistrés comme types de contenu MIME comme décrit à l'Appendice B. Par exemple, l'application de tableau blanc LBL pourrait être enregistrée comme application/wb de type de contenu MIME avec des considérations sur le codage spécifiant qu'elle fonctionne sur UDP, sans format de fichier approprié. Dans SDP, ceci serait exprimé en utilisant une combinaison du champ "support" et du champ "fmt", comme suit :

```
m=application 32416 udp wb
```

Attributs suggérés

Les attributs suivants sont suggérés. Comme les auteurs d'applications PEUVENT ajouter de nouveaux attributs en tant que de besoin, cette liste n'est pas exhaustive.

```
a=cat:<catégorie>
```

Cet attribut donne la catégorie hiérarchique séparée par un point de la session. Ceci est pour permettre à un receveur de filtrer les sessions non désirées par catégorie. Ce devrait probablement être un champ séparé obligatoire, excepté pour sa nature expérimentale pour l'instant. C'est un attribut de niveau session, et il ne dépend pas du jeu de caractères.

a=keywds:<mots clés>

Comme l'attribut cat, il sert à aider à l'identification des sessions désirées par le receveur. Cela permet à un receveur de choisir les sessions intéressantes sur la base de mots clés qui décrivent l'objet de la session. C'est un attribut de niveau session. C'est un attribut qui dépend du jeu de caractères, qui signifie que sa valeur DEVRAIT être interprétée dans le jeu de caractères spécifié pour la description de session si il en est spécifié un, ou par défaut en ISO 10646/UTF-8.

a=tool:<nom et version d'outil>

Cela donne le nom et le numéro de version de l'outil utilisé pour créer la description de session. C'est un attribut de niveau session, et il ne dépend pas du jeu de caractères.

a=ptime:<durée de paquet>

Cela donne la durée en millisecondes représentée par le support dans un paquet. Cela n'est probablement significatif que pour les données audio. Il NE DEVRAIT PAS être nécessaire de connaître ptime pour décoder RTP ou vat audio, et il est destiné à être une recommandation pour le codage/mise en paquet de l'audio. C'est un attribut de support, et il n'est pas dépendant du jeu de caractères.

a=recvonly

Ceci spécifie que les outils DEVRAIENT être lancés en mode réception-seule, lorsque c'est applicable. Cela peut être un attribut de session ou de support, et ne dépend pas du jeu de caractères.

a=sendrecv

Cela spécifie que les outils DEVRAIENT être lancés en mode émission et réception. Cela est nécessaire pour les conférences interactives avec des outils tels que wb qui reviennent par défaut au mode réception-seule. Cela peut être un attribut de session ou de support, et ne dépend pas du jeu de caractères.

a=sendonly

Cela spécifie que les outils DEVRAIENT être lancés en mode émission-seule. Un exemple peut être lorsqu'une adresse en envoi individuel différente doit être utilisée pour une destination de trafic et pour la source du trafic. Dans un tel cas, deux descriptions de supports PEUVENT être utilisées, une en émission seule et l'autre en réception-seule. Ce peut être un attribut de session ou de support, mais devrait normalement être seulement utilisé comme attribut de support, et n'est pas dépendant du jeu de caractères.

a=orient:<orientation du tableau blanc>

Normalement c'est seulement utilisé dans la spécification d'un support de tableau blanc. Il spécifie l'orientation du tableau blanc sur l'écran. C'est un attribut de support. Les valeurs permises sont "portrait", "paysage" et "bord de mer" (paysage à l'envers). Il ne dépend pas du jeu de caractères

a=type:<type de conférence>

Cela spécifie le type de la conférence. Les valeurs suggérées sont "broadcast", "meeting", "moderated", "test" et "H332". "recvonly" DEVRAIT être la valeur par défaut pour les sessions de "type:broadcast", "type:meeting" DEVRAIT impliquer "sendrecv" et "type:moderated" DEVRAIT indiquer l'utilisation d'un outil de contrôle des interventions et que les outils de support sont lancés de façon à rendre "muets" les nouveaux sites se joignant à la conférence.

Spécifier l'attribut type:H332 indique que cette session à liaisons faibles fait partie d'une session H.332 telle que définie dans la Recommandation UIT-T H.332 [H.332]. Les outils de supports DEVRAIENT être lancés en "recvonly".

Pour spécifier l'attribut type:test il est suggéré comme un conseil que, sauf explicitement demandé autrement, les receveurs puissent éviter en toute sécurité d'afficher cette description de session aux utilisateurs.

L'attribut type est un attribut de niveau session, et il ne dépend pas du jeu de caractères.

a=charset:<jeu de caractères>

Cela spécifie le jeu de caractères qui doit être utilisé pour afficher le nom de session et les données d'information. Par défaut, on utilise le jeu de caractères ISO-10646 en codage UTF-8. Si une représentation plus compacte est nécessaire, d'autres jeux de caractères peuvent être utilisés comme ISO-8859-1 pour les langages du nord de l'Europe. En particulier,

ISO 8859-1 est spécifié avec l'attribut SDP suivant :

a=charset:ISO-8859-1

C'est un attribut de niveau session ; si cet attribut est présent, il DOIT être avant le premier champ de support. Le jeu de caractères spécifié DOIT être un de ceux enregistrés auprès d'IANA, tels que ISO-8859-1. L'identifiant de jeu de caractères est une chaîne US-ASCII et DOIT être comparé aux identifiants IANA en utilisant une comparaison insensible à la casse. Si l'identifiant n'est pas reconnu ou pas pris en charge, toutes les chaînes qui en sont affectées DEVRAIENT être considérées comme chaînes d'octets.

Noter qu'un jeu de caractères spécifié DOIT toujours prohiber l'utilisation des octets 0x00 (Nul), 0x0A (LF) et 0x0d (CR). Les jeux de caractères exigeant l'utilisation de ces caractères DOIVENT définir un mécanisme de citation qui empêche ces octets d'apparaître dans les champs textuels.

a=sdplang:<étiquette de langage>

Ce peut être un attribut de niveau session ou un attribut de niveau support. Comme attribut de niveau session, il spécifie le langage de la description de session. Comme attribut de niveau support, il spécifie le langage de tout champ d'informations SDP de niveau support associé à ce support. Plusieurs attributs sdplang peuvent être fournis au niveau session ou au niveau support si plusieurs langages dans la description de session ou de support utilisent divers langages, auquel cas l'ordre des attributs indique l'ordre d'importance des divers langages dans la session ou le support du plus important au moins important.

En général, l'envoi de descriptions de sessions comportant plusieurs langues DEVRAIT être évité. Plusieurs descriptions devraient être envoyées pour décrire la session, une dans chaque langue. Cependant, ceci n'est pas possible avec tous les mécanismes de transport, et donc plusieurs attributs sdplang sont permis bien que non recommandés.

La valeur de l'attribut sdplang DOIT être une seule étiquette de langage de la RFC 1766 en US-ASCII. Elle ne dépend pas de l'attribut jeu de caractères. Un attribut sdplang DEVRAIT être spécifié lorsqu'une session est d'un domaine d'application suffisant pour franchir des frontières géographiques où on ne peut pas préjuger de la langue des receveurs, ou où la session est dans une langue différente de celle de la langue locale normale.

a=lang:<étiquette de langage>

Ce peut être un attribut de niveau session ou un attribut de niveau support. Comme attribut de niveau session, il spécifie le langage par défaut pour la session décrite. Comme attribut de niveau support, il spécifie la langue pour ce support, supplantant tout langage de niveau session spécifié. Plusieurs attributs lang peuvent être fournis au niveau session ou au niveau support si la description de session ou de support utilise plusieurs langues, auquel cas, l'ordre des attributs indique l'ordre d'importance des diverses langues dans la session ou support du plus important au moins important.

La valeur de l'attribut lang DOIT être une seule étiquette de langage de la RFC 1766 en US-ASCII. Elle ne dépend pas de l'attribut jeu de caractères. Un attribut lang DEVRAIT être spécifié lorsqu'une session est d'une portée suffisante pour franchir des frontières géographiques où la langue des receveurs ne peut être devinée, ou lorsque la session est dans une langue différente de la langue locale normale.

a=framerate:<débit de trame>

Cela donne le débit de trame vidéo maximum en trames/s. C'est une recommandation pour le codage de données vidéo. La représentation décimale de valeurs fractionnelles en utilisant la notation "<entier>.<fraction>" est permise. C'est un attribut de support, il n'est défini que pour les supports vidéo, et il ne dépend pas du jeu de caractères.

a=quality:<qualité>

Il donne une suggestion pour la qualité du codage sous forme d'une valeur d'entier.

L'intention de l'attribut qualité pour la vidéo est de spécifier un compromis qui ne soit pas une valeur par défaut entre le débit de trame et la qualité d'image fixe. Pour la vidéo, la valeur est dans la gamme de 0 à 10, avec la signification proposée suivante :

10 - la meilleure qualité d'image fixe que le schéma de compression peut donner.

5 - le comportement par défaut en l'absence de suggestion de qualité.

0 - la plus mauvaise qualité d'image fixe que le concepteur du codec estime encore utilisable.

C'est un attribut de support, et il ne dépend pas du jeu de caractères.

a=fmtp:<format> <paramètres spécifiques du format>

Cet attribut permet des paramètres qui sont spécifiques d'un format particulier pour être envoyés de telle façon que SDP n'ait pas à les comprendre. Le format doit être un des formats spécifiés pour le support. Les paramètres spécifiques du format peuvent être tout ensemble de paramètres nécessaires pour être envoyés par SDP et donnés sans changement à l'outil de support qui va utiliser ce format.

C'est un attribut de support, et il ne dépend pas du jeu de caractères.

6.1 Communication de la politique de contrôle de Conférence

La façon dont la politique de contrôle de conférence devrait être communiquée fait l'objet d'un débat. En général, les auteurs estiment qu'un style déclaratif implicite est souhaitable si possible pour spécifier le contrôle de la conférence.

Un style déclaratif simple utilise un seul champ d'attribut de conférence avant le premier champ de support, éventuellement accompagné de propriétés telles que "recvonly" pour certains des outils de support. Cet attribut de conférence porte la politique de contrôle de conférence. A titre d'exemple :

```
a=type:moderated
```

Dans certains cas, cependant, il est possible que ceci soit insuffisant pour communiquer le détail d'une politique de contrôle de conférence inhabituelle. Si c'est le cas, un attribut de conférence spécifiant un contrôle externe pourrait alors être établi, et puis un ou plusieurs champs "support" pourraient être utilisés pour spécifier les outils de contrôle de la conférence et les données de configuration pour ces outils. Une session UIT-T H.332 en est un exemple :

```
c=IN IP4 224.5.6.7
a=type:H332
m=audio 49230 RTP/AVP 0
m=video 49232 RTP/AVP 31
m=application 12349 udp wb
m=control 49234 H323 mc
c=IN IP4 134.134.157.81
```

Dans cet exemple, un attribut général de conférence (type:H332) est spécifié, qui établit que le contrôle de la conférence sera fourni par un outil H.332 externe, et il donne des adresses de contact pour le contrôleur multipoint de session H.323 .

Dans ce document, seul le style déclaratif de déclaration de contrôle de conférence est spécifié. D'autres formes de contrôle de conférence devraient spécifier un attribut de type approprié, et devraient définir les implications que cela a pour le support de contrôle.

7 Considérations sur la sécurité

SDP est un format de description de session qui décrit des sessions multimédia. Une description de session ne devrait pas être considérée comme de confiance tant qu'elle n'a pas été obtenue par un protocole de transport authentifié auprès d'une source de confiance. De nombreux protocoles de transport différents peuvent être utilisés pour distribuer des descriptions de session, et la nature de l'authentification va différer d'un transport à l'autre.

Un transport qui va être fréquemment utilisé pour distribuer des description de sessions est le protocole d'annonce de session (SAP). SAP fournit à la fois le chiffrement et les mécanismes d'authentification mais du fait de la nature des annonces de session, il est vraisemblable qu'il y a de nombreuses occasions où l'origine d'une annonce de session ne peut pas être authentifiée parce qu'elle n'est pas connue antérieurement du receveur de l'annonce et parce qu'aucune infrastructure commune de clé publique n'est disponible.

A réception d'une description de session sur un mécanisme de transport non authentifié ou de la part d'une source qui n'est pas de confiance, le logiciel d'analyse de session devrait prendre quelques précautions. La description de session contient des informations exigées pour lancer le logiciel sur les systèmes receveurs. Le logiciel qui analyse une description de session NE DOIT PAS être capable de lancer d'autres logiciels excepté ce qu'il est configuré spécifiquement comme logiciel approprié pour participer à des sessions multimédia. Il est normalement considéré comme INAPPROPRIÉ pour un

logiciel analysant une description de session de lancer, sur un système d'utilisateur, un logiciel approprié pour participer à des sessions multimédia, sans que l'utilisateur ait préalablement été informé qu'un tel logiciel va être lancé et n'ait donné son consentement. Et donc, une description de session arrivant par une annonce de session, courriel, invitation de session, ou page WWW NE DEVRAIT PAS faire entrer l'utilisateur dans une {it interactive} session multimédia sans que l'utilisateur soit au courant de ce qui va se passer. Comme il n'est pas toujours simple de dire si une session est ou non interactive, les applications qui ne sont pas sûres DEVRAIENT supposer que les sessions sont interactives.

Dans la présente spécification, il n'y a pas d'attribut qui permettrait au receveur d'une description de session d'être informé du lancement d'outils multimédia dans un mode où ils n'émettent pas. Dans certaines circonstances, il peut être approprié de définir de tels attributs. Si c'est fait, une application analysant une description de session qui contient de tels attributs DEVRAIT soit les ignorer, soit informer l'utilisateur que se joindre à cette session provoquera une transmission automatique de données multimédia. Le comportement par défaut pour un attribut inconnu est de les ignorer.

Les descriptions de session PEUVENT être analysées à des systèmes intermédiaires tels que des pare-feu pour les besoins de faire une ouverture pour permettre de participer à des sessions multimédia. Il est considéré comme INAPPROPRIÉ pour un pare-feu d'ouvrir de tels trous pour des flux de données en envoi individuel à moins que la description de session ne vienne dans une demande provenant de l'intérieur du pare-feu.

Pour les sessions en diffusion groupée, il est vraisemblable que les administrateurs locaux vont appliquer leurs propres politiques, mais l'utilisation exclusive du domaine d'application administratif "local" ou "site-local" au sein du pare-feu et le refus du pare-feu d'ouvrir un trou pour de tels domaines d'application va provoquer une séparation des sessions en diffusion groupée mondiales et locales.

Appendice A : Grammaire de SDP

Le présent appendice fournit une grammaire BNF augmentée pour SDP. ABNF est défini dans la RFC 2234.

```

annonce =      proto-version
              origin-field
              session-name-field
              information-field
              uri-field
              email-fields
              phone-fields
              connection-field
              bandwidth-fields
              time-fields
              key-field
              attribute-fields
              media-descriptions

proto-version = "v=" 1*DIGIT CRLF           ; ce mémo décrit la version 0
origin-field  = "o=" username space sess-id space sess-version space nettype space addrtype space addr CRLF
session-name-field = "s=" text CRLF
information-field = ["i=" text CRLF]
uri-field     = ["u=" uri CRLF]
email-fields  = *("e=" email-address CRLF)
phone-fields  = *("p=" phone-number CRLF)
connection-field = ["c=" nettype space addrtype space connection-address CRLF]
              ; un champ connexion DOIT être présent dans chaque description de support ou au niveau session
bandwidth-fields = *("b=" bwtype ":" bande passante CRLF)
time-fields     = 1*( "t=" start-time space stop-time
                  *(CRLF repeat-fields) CRLF)
                  [zone-adjustments CRLF]
repeat-fields   = "r=" repeat-interval space typed-time 1*(space typed-time)
zone-adjustments = time space ["-"] typed-time *(space time space ["-"] typed-time)
key-field      = ["k=" key-type CRLF]
key-type       = "prompt" | "clear:" key-data | "base64:" key-data | "uri:" uri
key-data       = email-safe | "~" | "
```

```

attribute-fields = *("a=" attribute CRLF)
media-descriptions = *( media-field
                        information-field
                        *(connection-field)
                        bandwidth-fields
                        key-field
                        attribute-fields )
media-field = "m=" media space port [ "/" integer ] space proto 1*(space fmt) CRLF
media = 1*(alpha-numeric) ; typiquement "audio", "vidéo", "application", ou "data"
fmt = 1*(alpha-numeric) ; typiquement un type de charge utile RTP pour support audio et vidéo
proto = 1*(alpha-numeric) ; typiquement "RTP/AVP" ou "udp" pour IP4
port = 1*(DIGIT) ; DEVRAIT être dans la gamme "1024" à "65535" inclus pour support fondé sur UDP
attribute = (att-field ":" att-value) | att-field
att-field = 1*(alpha-numeric)
att-value = byte-string
sess-id = 1*(DIGIT) ; DEVRAIT être unique pour ce nom-d'utilisateur/hôte d'origine
sess-version = 1*(DIGIT) ; 0 est une nouvelle session
connection-address = multicast-address | addr
multicast-address = 3*(decimal-uchar "." decimal-uchar "/" ttl [ "/" integer ]
; les adresses de diffusion groupée PEUVENT être dans la gamme 224 0 0 0 à 239 255 255 255
ttl = decimal-uchar
start-time = time | "0"
stop-time = time | "0"
time = POS-DIGIT 9*(DIGIT) ; suffisant pour deux siècles supplémentaires
repeat-interval = typed-time
typed-time = 1*(DIGIT) [fixed-len-time-unit]
fixed-len-time-unit = "d" | "h" | "m" | "s"
bwtype = 1*(alpha-numeric)
bandwidth = 1*(DIGIT)
username = safe ; définition très large, mais n'inclut pas d'espace
email-address = email | email "(" email-safe ")" | email-safe "<" email ">"
email = ; défini dans la RFC 822
uri = ; défini dans la RFC 1630
phone-number = phone | phone "(" email-safe ")" | email-safe "<" phone ">"
phone = "+" POS-DIGIT 1*(space | "-" | DIGIT)
; il DOIT y avoir une espace ou trait d'union entre le code international et le reste du numéro.
nettype = "IN" ; liste à étendre
addrtype = "IP4" | "IP6" ; liste à étendre
addr = FQDN | unicast-address
FQDN = 4*(alpha-numeric|"-".") ; nom de domaine pleinement qualifié comme spécifié dans la RFC 1035
unicast-address = IP4-address | IP6-address
IP4-address = b1 "." decimal-uchar "." decimal-uchar "." b4
b1 = decimal-uchar ; moins de "224" ; pas "0" ou "127"
b4 = decimal-uchar ; pas "0"
IP6-address = ; à définir
text = byte-string ; par défaut est à interpréter comme ISO-10646 UTF8
; ISO 8859-1 requiert un "a=charset:ISO-8859-1"
; attribut de niveau session à utiliser
byte-string = 1*(0x01..0x09|0x0b|0x0c|0x0e..0xff) ; tout octet sauf NUL, CR ou LF
decimal-uchar = DIGIT | POS-DIGIT DIGIT | ("1" 2*(DIGIT)) | ("2" ("0"|"1"|"2"|"3"|"4") DIGIT) | ("2" "5"
("0"|"1"|"2"|"3"|"4"|"5"))
integer = POS-DIGIT *(DIGIT)
alpha-numeric = ALPHA | DIGIT
DIGIT = "0" | POS-DIGIT
POS-DIGIT = "1"|"2"|"3"|"4"|"5"|"6"|"7"|"8"|"9"
ALPHA = "a"|"b"|"c"|"d"|"e"|"f"|"g"|"h"|"i"|"j"|"k"|"l"|"m"|"n"|"o"|"p"|"q"|"r"|"s"|"t"|"u"|"v"|"w"|"x"|"y"|"z"
|"A"|"B"|"C"|"D"|"E"|"F"|"G"|"H"|"I"|"J"|"K"|"L"|"M"|"N"|"O"|"P"|"Q"|"R"|"S"|"T"|"U"|"V"|"W"|"X"|"Y"|"Z"
email-safe = safe | space | tab
safe = alpha-numeric | "" | "-" | "." | "/" | ":" | "?" | "" | "#" | "$" | "&" | "*" | ";" | "=" | "@" | "[" | "]" | "^" | "_" | "" | "{" |

```

```
"|" | "}" | "+" | "~" | "
space = %d32
tab = %d9
CRLF = %d13.10
```

Appendice B : Lignes directrices pour l'enregistrement des noms SDP auprès de l'IANA

Il y a sept noms de champs qui PEUVENT être enregistrés auprès d'IANA. En utilisant la terminologie en BNF dans la spécification SPD, ce sont "media", "proto", "fmt", "att-field", "bwtype", "nettype" et "addrtype".

"media" (par exemple audio, vidéo, application, données).

Les types de support mis en paquet, tels que ceux utilisés par RTP, partagent l'espace de nom utilisé par les registres de types de support [RFC 2048] (c'est-à-dire, "types MIME"). La liste des noms de supports valides est l'ensemble des types de contenu MIME de haut niveau. L'ensemble des supports est conçu pour être petit et non pour être étendu excepté dans de rares circonstances. (Le sous-type MIME correspond au paramètre "fmt" ci-dessous).

"proto"

En général ce DEVRAIT être un identifiant de protocole de transport normalisé de l'IETF tel que RTP/AVP (RFC 1889) sous le profil de la RFC 1890).

Cependant, des personnes veulent inventer leurs propres protocoles de transport propriétaires. Certains d'entre eux DEVRAIENT être enregistrés comme un "fmt" en utilisant "udp" comme protocole et certains d'entre eux ne le peuvent pas.

Lorsque le protocole et l'application sont intimement liés, comme le tableau blanc LBL wb qui utilise un protocole propriétaire d'un objet spécial sur UDP, le nom du protocole DEVRAIT être "udp" et le nom de format qui DEVRAIT être enregistré est "wb". Les règles pour les formats (voir ci-dessous) s'appliquent à de tels enregistrements.

Lorsque le protocole de transport propriétaire porte réellement de nombreux formats de données différents, il est possible d'enregistrer un nouveau nom de protocole auprès de l'IANA. Dans de tels cas, une RFC DOIT être produite pour décrire le protocole et le référencer dans l'enregistrement. Une telle RFC PEUT être pour information, bien qu'il soit préférable qu'elle soit normalisée.

"fmt"

L'espace de nom de format dépend du contexte du champ "proto", aussi un format ne peut être enregistré sans spécifier un ou plusieurs des protocoles de transport auquel il s'applique.

Les formats couvrent tous les codages possibles qui peuvent vouloir être transportés dans une session multimédia.

Pour les formats RTP qui ont été alloués à des types de charge utile statiques, le numéro de type de charge utile est utilisé. Pour les formats RTP qui utilisent un numéro de type de charge utile dynamique, le numéro de type de charge utile dynamique est donné comme format et un attribut "rtptime" additionnel spécifie le format et les paramètres.

Pour les formats non RTP, tout nom de format non enregistré PEUT être enregistré par le processus d'enregistrement de type MIME [RFC 2048]. Le type donné ici est seulement le sous-type MIME (le type de contenu MIME de niveau supérieur est spécifié par le paramètre de support). Le type d'enregistrement MIME DEVRAIT faire référence aux RFC normalisées qui décrivent le protocole de transport pour ce type de support. S'il existe un type MIME pour ce format, l'enregistrement MIME DEVRAIT être augmenté de la référence de la spécification de transport pour ce type de support. S'il n'existe pas de type MIME pour ce format, et s'il n'existe pas de format de fichier approprié, ce DEVRAIT être noté dans les considérations sur le codage comme "pas de format de fichier approprié".

"att-field" (noms d'attribut)

Les noms de champ d'attribut PEUVENT être enregistrés auprès de l'IANA, bien que ce ne soit pas obligatoire, et que les attributs inconnus soient simplement ignorés.

Lorsqu'un attribut est enregistré, il DOIT être accompagné d'une brève spécification établissant ce qui suit :

- o nom du contact, adresse de messagerie électronique et numéro de téléphone.
- o nom d'attribut (comme il apparaîtra dans SDP).

- o nom d'attribut de forme longue en anglais.
- o type d'attribut (niveau de session, niveau de support, ou les deux).
- o si la valeur de l'attribut est sujette à l'attribut jeu de caractères.
- o une explication d'un paragraphe sur l'objet de l'attribut.
- o une spécification des valeurs d'attribut appropriées pour cet attribut.

L'IANA ne fait pas de vérification de bonne santé de tels enregistrements d'attribut, sauf pour s'assurer qu'ils n'entrent pas en conflit avec des enregistrements existants.

Bien que les dispositions ci-dessus soient le minimum de ce que l'IANA va accepter, si on s'attend à ce que l'attribut ait une utilisation étendue et que des questions d'interaction soient en cause, les auteurs sont invités à produire des RFC normalisées qui spécifient plus précisément l'attribut.

Ceux qui soumettent des enregistrements DEVRAIENT s'assurer que la spécification est dans l'esprit des attributs de SDP, et en particulier que l'attribut est indépendant de la plate-forme dans le sens où il ne fait pas d'hypothèses implicites sur les systèmes d'exploitation et ne nomme pas des parties spécifiques de logiciel d'une façon qui risque d'inhiber l'interopérabilité.

"bwtype" (spécificateurs de bande passante)

La prolifération des spécificateurs de bande passante est vivement déconseillée.

De nouveaux spécificateurs de bande passante PEUVENT être enregistrés auprès de l'IANA. La soumission DOIT faire référence à une RFC normalisée qui spécifie précisément la sémantique du spécificateur de bande passante, et indique quand il DEVRAIT être utilisé, et pourquoi les spécificateurs de bande passante enregistrés existants ne suffisent pas.

"nettype" (type de réseau)

De nouveaux types de réseau PEUVENT être enregistrés auprès de l'IANA si SDP a besoin d'être utilisé dans le contexte d'environnements non Internet. Bien que ceux-ci soient normalement le domaine réservé de l'IANA, il PEUT y avoir des circonstances où une application Internet a besoin d'inter opérer avec une application non Internet, comme lorsqu'une passerelle assure l'interface entre un appel téléphonique Internet avec le RTPC. Le nombre de types de réseau DEVRAIT être petit et DEVRAIT être rarement étendu. Un nouveau type de réseau ne peut être enregistré sans enregistrer au moins un type d'adresse à utiliser avec ce type de réseau. Un enregistrement de nouveau type de réseau DOIT faire référence à une RFC qui donne les détails du type de réseau et du type d'adresse et spécifie comment et quand ils devraient être utilisés. Une telle RFC PEUT être pour information.

"addrtype" (type d'adresse)

De nouveaux types d'adresses PEUVENT être enregistrés auprès de l'IANA. Un type d'adresse n'est significatif que dans le contexte d'un type de réseau, et tout enregistrement d'un type d'adresse DOIT spécifier un type de réseau enregistré, ou être soumis avec un enregistrement de type de réseau. Un nouvel enregistrement de type d'adresse DOIT faire référence à une RFC qui donne les détails de la syntaxe du type d'adresse. Une telle RFC PEUT être pour information. Les types d'adresse ne sont pas supposés être enregistrés fréquemment.

Procédure d'enregistrement

L'enregistrement d'un nom selon les lignes directrices ci-dessus DEVRAIT du niveau de documentation qui est exigé. L'enregistrement lui-même DEVRAIT être envoyé à l'IANA. Les enregistrements d'attributs DEVRAIENT inclure les informations données ci-dessus. Les autres enregistrements DEVRAIENT inclure les informations supplémentaires suivantes :

- o nom de contact, adresse de messagerie électronique et numéro de téléphone.
- o nom à enregistrer (comme il apparaîtra dans SDP).
- o forme longue du nom en anglais.
- o type de nom ("media", "proto", "fmt", "bwtype", "nettype", ou "addrtype")
- o un paragraphe d'explication sur l'objet du nom enregistré.
- o une référence à la spécification (par exemple le numéro de RFC) du nom enregistré.

L'IANA PEUT se référer pour tout enregistrement à l'IESG ou à tout groupe de travail approprié de l'IETF pour révision, et PEUT demander que des révisions soient faites avant d'effectuer l'enregistrement.

Appendice C : Adresse des auteurs

Mark Handley
Information Sciences Institute
c/o MIT Laboratory for Computer Science
545 Technology Square
Cambridge, MA 02139
United States
electronic mail: mjh@isi.edu

Van Jacobson
MS 46a-1121
Lawrence Berkeley Laboratory
Berkeley, CA 94720
United States
electronic mail: van@ee.lbl.gov

Remerciements

De nombreuses personnes du groupe de travail MMUSIC de l'IETF ont fait des commentaires et suggestions pour contribuer au présent document. En particulier, nous aimerions remercier Eve Schooler, Steve Casner, Bill Fenner, Allison Mankin, Ross Finlayson, Peter Parnes, Joerg Ott, Carsten Bormann, Rob Lanphier et Steve Hanna.

Références

- [H.332] Recommandation UIT-T H.332 (1998): "Terminal multimédia pour la réception de conférences H.323 fondées sur Internet", UIT, Genève.
- [RFC1305] D. Mills, "[Protocole de l'heure du réseau](#), version 3, spécification, mise en œuvre et analyse", STD 12, mars 1992. (*Remplacée par RFC5905*)
- [RFC1641] D. Goldsmith et M. Davis, "Utilisation de Unicode avec MIME", juillet 1994. (*Expérimentale*)
- [RFC1889] H. Schulzrinne, S. Casner, R. Frederick et V. Jacobson, "RTP : protocole de transport pour applications en temps réel", janvier 1996. (*Obsolète, voir RFC3550* STD64)
- [RFC1890] H. Schulzrinne, "Profil RTP pour conférences audio et vidéo avec contrôle minimal", janvier 1996. (*Obsolète, voir RFC3551*) (P.S.)
- [RFC2044] F. Yergeau, "[UTF-8, un format de transformation d'Unicode](#) et d'ISO 10646", octobre 1996. (*Ob., voir RFC2279*) (*Info.*)
- [RFC2326] H. Schulzrinne, A. Rao et R. Lanphier, "Protocole de [flux directs en temps réel](#) (RTSP)", avril 1998. (*Remplacée par RFC7826*)
- [RFC2974] M. Handley, C. Perkins, E. Whelan, "Protocole d'annonce de session (SAP)", octobre 2000. (*Expérimentale*)
- [RFC3261] J. Rosenberg et autres, "SIP : [Protocole d'initialisation de session](#)", juin 2002. (*Mise à jour par 3265, 3853, 4320, 4916, 5393, 6665, 8217, 8760*)
- [UNICODE] The Unicode Consortium, "The Unicode Standard -- Version 2.0", Addison-Wesley, 1996.
- [UTF-8] Norme internationale ISO/CEI 10646-1:1993. "Technologies de l'information -- Ensemble de caractères codé universel pluri-octets (UCS) -- Partie 1 : Architecture et plan de base multilingue". Cinq amendements et un corrigendum technique sont publiés jusqu'à présent. UTF-8 est l'Annexe R, publiée comme amendement 2.
- [VAT] V. Jacobson, S. McCanne, "vat - X11-based audio teleconferencing tool" vat manual page, Lawrence Berkeley Laboratory, 1994.

Déclaration de droits de propriété intellectuelle

Copyright (C) The Internet Society (1998). Tous droits réservés.

Le présent document et ses traductions PEUVENT être copiées et fournis à des tiers et les travaux dérivés qui le commentent ou l'expliquent ou aident à sa mise en œuvre PEUVENT être préparés, copiés, publiés et distribués, en tout ou en partie, sans restrictions d'aucune sorte, pourvu que la déclaration de droits de propriété intellectuelle ci dessus et le présent paragraphe soient inclus dans toute copies et travaux dérivés. Cependant, le présent document lui-même NE PEUT être modifié d'aucune façon, telle qu'en retirant la déclaration de copyright ou les références à la Internet Society ou autres organisations Internet, excepté en tant que de besoin pour le développement des normes Internet, auquel cas les procédures de copyright définies dans le processus de normalisation Internet DOIVENT être suivies, ou comme nécessaire pour le traduire dans des langues autres que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles ne seront pas révoquées par la Internet Society, ses successeurs ou ayants droit.

Le présent document et les informations qu'il contient sont fournis sur une base "EN L'ETAT" et la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toute responsabilité, explicite ou implicite, y compris, mais non limitée à toute garantie que l'utilisation des informations ci-enclosent ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'adaptation à un objet particulier.