Groupe de travail Réseau
Request for Comments : 4566
RFC rendues obsolètes : 2327, 3266
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

M. Handley, UCL
V. Jacobson, Packet Design
C. Perkins, University of Glasgow
juillet 2006

SDP : Protocole de description de session

Résumé
Le présent mémoire définit le protocole de description de session (SDP, *Session Description Protocol*). SDP est destiné à décrire les sessions multimédia pour les besoins d'annonce de session, d'invitation aux sessions, et autres formes d'initiation de session multimédia.

Table des matières

1. Introduction

Lors de l'initiation de téléconférences multimédia, d'appels en voix sur IP, de flux vidéo, ou autres sessions, il y a une exigence que soient portés aux participants les détails des supports, les adresses de transport, et autres métadonnées de la description de session.

SDP fournit une représentation normalisée de telles informations, sans considération de la façon dont ces informations sont transportées. SDP est purement un format pour la description de session – il n'incorpore pas de protocole de transport, et il est destiné à utiliser comme approprié les différents protocoles de transport, incluant le protocole d'annonce de session [RFC2974], le protocole d'initialisation de session [RFC3261], le protocole de flux directs en temps réel [RFC2326], la messagerie électronique avec extensions MIME, et le protocole de transport Hypertext.

SDP est destiné à être d'utilisation générale afin qu'il puisse être utilisé dans une large gamme d'environnements de réseau et applications. Cependant, il n'est pas destiné à prendre en charge la négociation du contenu de session ni les codages des supports : ceci sort du domaine d'application de la description de session.

Le présent mémoire rend obsolètes les [RFC2327] et [RFC3266]. La Section 10 mentionne les changements introduits dans le présent mémoire.

2. Glossaire des termes

Les termes qui suivent sont utilisés dans ce document avec une signification spécifique dans son contexte.

Conférence : une conférence multimédia est un ensemble de deux ou plus usagers communicants ainsi que le logiciel qu'ils utilisent pour communiquer.

Session : une session multimédia est un ensemble d'envoyeurs et receveurs multimédia et les flux de données qui s'écoulent des envoyeurs aux receveurs. Une conférence multimédia est un exemple de session multimédia.

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

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

3. Exemples d'utilisation de SDP

3.1 Initialisation de session

Le protocole d'initialisation de session (SIP, *Session Initiation Protocol*) [RFC3261] est un protocole de commande de niveau application pour créer, modifier et terminer des sessions comme des conférences Internet multimédia, des appels téléphoniques Internet, et la distribution multimédia. Les messages SIP utilisés pour créer des sessions portent des descriptions de session qui permettent aux participants de s'accorder sur un ensemble de types de prises en charge compatibles. Ces descriptions de session sont généralement formatées en utilisant SDP. Quand il est utilisé avec SIP, le modèle offre/réponse [RFC3264] fournit un cadre limité pour une négociation avec SDP.

3.2 Support en direct

Le protocole de flux en temps réel (RTSP, *Real Time Streaming Protocol*) [RFC2326], est un protocole de niveau application pour des commandes sur la livraison des données avec des propriétés de temps réel. RTSP fournit un cadre

extensible pour permettre une livraison contrôlée, à la demande, de données en temps réel, comme de l'audio et de la vidéo. Un client et un serveur RTSP négocient un ensemble approprié de paramètres pour la livraison des supports, en utilisant partiellement la syntaxe de SDP pour décrire ces paramètres.

3.3 Messagerie électronique et Toile mondiale

Les autres moyens de transporter les descriptions de session incluent la messagerie électronique et la Toile mondiale (WWW, *World Wide Web*). Pour la distribution par messagerie électronique et WWW, le type de support "application/sdp" est utilisé. Cela permet le lancement automatique d'une manière standard des applications pour la participation à la session à partir du client WWW ou du lecteur de messagerie.

Noter que les annonces de sessions en diffusion groupée faites seulement via la messagerie électronique ou le WWW n'ont pas la propriété que le receveur d'une annonce de session peut nécessairement recevoir la session parce que les sessions en diffusion groupée peuvent avoir une portée restreinte, et l'accès au serveur WWW ou la réception de messages électroniques n'est pas possible hors de cette portée.

3.4 Annonce de session en diffusion groupée

Afin d'aider aux annonces de conférences multimédia en diffusion groupée et autres sessions en diffusion groupée, et pour communiquer les informations pertinentes d'établissement de session aux postulants à la participation, un répertoire de session réparti peut être utilisé. Une instance d'un tel répertoire de session envoie périodiquement des paquets contenant une description de la session à un groupe de diffusion groupée bien connu. Ces annonces sont reçues par les autres répertoires de session de telle façon que les participants distants potentiels peuvent utiliser la description de session pour lancer les outils nécessaires pour participer à la session.

Un protocole utilisé pour mettre en œuvre un tel répertoire réparti est le protocole d'annonce de session (SAP, *Session Announcement Protocol*) [RFC2974]. SDP fournit le format de description de session recommandé pour de telles annonces de session.

4. Exigences et recommandations

L'objet de SDP est de convoyer des informations sur les flux de supports 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 dans l'interréseautage, bien qu'il soit suffisamment général pour pouvoir décrire des conférences dans d'autres environnements de réseau. Les flux de supports peuvent être de beaucoup à beaucoup. Les sessions ne sont pas nécessairement continuellement actives.

Jusqu'à présent les sessions fondées sur la diffusion groupée dans l'Internet ont différé de beaucoup des autres formes de conférence en ce que quiconque reçoit le trafic peut se joindre à la session (sauf si le trafic de session est chiffré). Dans un tel environnement, SDP sert deux objectifs principaux. Il est un moyen pour communiquer l'existence d'une session, et il est un moyen pour convoyer des informations suffisantes pour permettre de se joindre à la session et d'y participer. Dans un environnement d'envoi individuel, seul le premier objet est probablement pertinent.

Une description de session SDP inclut ce qui suit :
o le nom et l'objet de la session
o l'heure ou les heures auxquelles la session est active
o les supports constituant la session
o les informations nécessaires pour recevoir ces supports (adresses, accès, formats, etc.)

Comme les ressources nécessaires pour participer à une session peuvent être limitées, certaines informations supplémentaires peuvent aussi être souhaitables :
o informations sur la bande passants qui va être utilisée par la session
o informations de contact pour la personne responsable de la session

En général, SDP doit convoyer des informations suffisantes pour permettre aux applications de se joindre à une session (à l'exception possible des clés de chiffrement) et d'annoncer les ressources à utiliser à tout non participant qui peut avoir besoin de le savoir. (Cette dernière caractéristique est principalement utile quand SDP est utilisé avec un protocole d'annonce de session en diffusion groupée.)

4.1 Informations de support et de transport

Une description de session SDP inclut les informations de support suivantes :
- o le type de support (vidéo, audio, etc.)
- o le protocole de transport (RTP/UDP/IP, H.320, etc.)
- o le format du support (vidéo H.261, vidéo MPEG, etc.)

En plus du format du support et du protocole de transport, SDP porte les détails d'adresse et d'accès. Pour une session en diffusion groupée IP, cela comprend :
- o l'adresse de groupe de diffusion groupée pour le support,
- o l'accès de transport pour le support.

Cette adresse et cet 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 les sessions en envoi individuel IP, sont convoyés :
- o l'adresse distante pour le support,
- o l'accès de transport distant pour le support.

La sémantique de cette adresse et accès dépend du support et du protocole de transport définis. Par défaut, ce DEVRAIT être l'adresse et l'accès distants auxquels ces données sont envoyées. Certains types de supports peuvent redéfinir ce comportement, mais ceci N'EST PAS RECOMMANDÉ car cela complique la mise en œuvre (incluant celle des boîtiers de médiation qui doivent analyser les adresses pour ouvrir les barrières des traducteurs d'adresse réseau (NAT, *Network Address Translation*) ou pare-feu).

4.2 Informations d'horaire

Les sessions peuvent être limitées ou non dans le temps. Qu'elles soient ou non limitées, elles peuvent n'être actives qu'à des heures spécifiques. SDP peut convoyer :
- o une liste arbitraire d'heures de début et d'arrêt limitant la session,
- o pour chaque limite, répéter les heures, comme "chaque mercredi de 10 h à 13 h".

Ces informations d'horaire sont globalement cohérentes, sans considération de la zone horaire locale ou de l'heure d'hiver (voir le paragraphe 5.9).

4.3 Sessions privées

Il est possible de créer des sessions publiques et des sessions privées. SDP lui-même ne distingue pas entre les deux ; les sessions privées sont normalement convoyées en chiffrant la description de session durant la distribution. Les détails de la façon dont le chiffrement est effectué dépendent du mécanisme utilisé pour convoyer SDP ; des mécanismes sont actuellement définis pour SDP transporté en utilisant SAP [RFC2974] et SIP [RFC3261], et d'autres pourront être définis à l'avenir.

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

4.4 Obtenir plus d'informations sur une session

Une description de session devrait porter assez d'informations pour décider de participer ou non à une session. SDP peut inclure des pointeurs supplémentaires sous la forme d'identifiants de ressource universels (URI, *Uniform Resource Identifier*) pour donner plus d'informations sur la session.

4.5 Catégorisation

Quand de nombreuses descriptions de session sont distribuées par SAP, ou tout autre mécanisme d'annonces, il peut être désirable de filtrer les annonces de session qui sont intéressantes et celles qui ne le sont pas. SDP prend en charge un mécanisme de catégorisation pour les sessions qui sont capables d'automatisation (attribut "a=cat:" ; voir la Section 6).

4.6 Internationalisation

La spécification de SDP recommande l'utilisation des jeux de caractères de la norme ISO 10646 dans le codage UTF-8 [RFC3629] pour permettre que de nombreux langages différents soient représentés. Cependant, pour favoriser les représentations compactes, SDP permet aussi que d'autres jeux de caractères tels que ISO 8859-1 soient utilisés quand désiré. L'internationalisation ne s'applique qu'aux champs de texte libre (nom de session et informations sur les fondements) et non à SDP comme un tout.

5. Spécification de SDP

Une description de session SDP est notée par le type de support "application/sdp" (voir la Section 8).

Une description de session SDP est entièrement textuelle en utilisant le jeu de caractères ISO 10646 en codage UTF-8. Les noms de champs et attributs SDP utilisent seulement le sous ensemble US-ASCII de l'UTF-8, mais les champs textuels et les valeurs d'attribut PEUVENT utiliser le jeu de caractères ISO 10646 complet. Les valeurs de champs et d'attribut qui utilisent les jeu complet de caractères UTF-8 ne sont jamais comparées directement, donc il n'est pas exigé de normalisation UTF-8. La forme textuelle, par opposition à un codage binaire comme ASN.1 ou XDR, a été choisie pour améliorer la portabilité, pour permettre l'utilisation de divers transports, et pour permettre que des outils flexibles, fondés sur le texte soient utilisés pour générer et traiter les descriptions de session. Cependant, comme SDP peut être utilisé dans des environnements où la taille maximum admissible d'une description de session est limitée, le codage est délibérément compact. Aussi, comme les annonces peuvent être transportées via des moyens très peu fiables ou endommagés par un serveur intermédiaire, le codage a été conçu avec des règles strictes d'ordre et de format afin que la plupart des erreurs résultent en annonces de session mal formée qui peuvent être facilement détectées et éliminées. Cela permet aussi une élimination rapide des annonces de session chiffrées pour lesquelles un receveur n'a pas la clé correcte.

Une description de session SDP consiste en un certain nombre de lignes de texte de forme : <type>=<valeur>

où <type> DOIT être exactement un caractère dont la casse est significative et <valeur> est un texte structuré dont le format dépend du <type>. En général, <valeur> est soit un certain nombre de champs délimités par un seul caractère espace soit une chaîne de format libre, et dont la casse est significative sauf si un champ spécifique la définit autrement. Des espaces blanches NE DOIVENT PAS être utilisées d'un côté ou de l'autre du signe "=".

Une description de session SDP consiste en une section de niveau session suivie par zéro, une ou plusieurs sections de niveau support. La partie de niveau session commence par une ligne "v=" et continue jusqu'à la première section de niveau support. Chaque section de niveau support commence par une ligne "m=" et continue jusqu'à la prochaine section de niveau support ou la fin de la description de session. En général, les valeurs de niveau session sont les valeurs par défaut pour tous les supports sauf outrepassées par une valeur de niveau support équivalente.

Certaines lignes dans chaque description sont EXIGÉES et certaines sont FACULTATIVES, mais toutes DOIVENT apparaître exactement dans l'ordre donné ici (l'ordre fixe améliore grandement la détection d'erreur et permet un analyseur simple). Les éléments FACULTATIFS sont marqué d'un "*".

Description de session
  v= (version du protocole)
  o= (identifiant d'origine et de session)
  s= (nom de la session)
  i=* (informations sur la session)
  u=* (URI de description)
  e=* (adresse de messagerie électronique)
  p=* (numéro de téléphone)
  c=* (informations de connexion – non exigé si elles sont incluses dans toutes les descriptions de supports)
  b=* (zéro, une ou plusieurs lignes d'informations de bande passante)
Une ou plusieurs descriptions de l'heure (lignes "t=" et "r=" l; voir ci-dessous)
  z=* (ajustements de zone horaire)
  k=* (clé de chiffrement)
  a=* (zéro, une ou plusieurs lignes d'attributs de session)
Zéro, une ou plusieurs descriptions de supports

Description de l'heure
  t= (heure où la session est active)
  r=* (zéro, une ou plusieurs heures de répétition)

Description de support, si il en est de présent :
  m= (nom du support et adresse de transport)
  i=* (titre du support)
  c=* (informations de connexion – facultatives si elles sont incluses au niveau session)
  b=* (zéro, une ou plusieurs lignes d'informations de bande passante)
  k=* (clé de chiffrement)
  a=* (zéro, une ou plusieurs lignes d'attributs du support)

L'ensemble de lettres de type est délibérément petit et n'est pas destiné à être extensible -- un analyseur SDP DOIT complètement ignorer toute description de session qui contient une lettre de type qu'il ne comprend pas. Le mécanisme d'attribut ("a=" décrit plus loin) est le principal moyen pour étendre SDP et l'adapter à des applications ou supports particuliers. Certains attributs (ceux mentionnés à la Section 6 du présent mémoire) ont une signification définie, mais d'autres peuvent être ajoutés sur la base d'une application, support, ou session spécifique. Un analyseur SDP DOIT ignorer tout attribut qu'il ne comprend pas.

Une description de session SDP peut contenir des URI qui font référence à un contenu externe dans les lignes "u=", "k=", et "a=" . Ces URI peuvent être déréférencés dans certains cas, rendant la description de session non auto contenue.

Les informations de connexion ("c=") et d'attribut ("a=") dans la section de niveau session s'appliquent à tous les supports de cette session sauf outrepassées par les informations de connexion ou par un attribut de même nom dans la description de support. Par exemple, 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=jdoe 2890844526 2890842807 IN IP4 10.47.16.5
s=Séminaire SDP
i=Séminaire sur le protocole de description de session
u=http://www.exemple.com/seminars/sdp.pdf
e=j.doe@exemple.com (Jane Doe)
c=IN IP4 224.2.17.12/127
t=2873397496 2873404696
a=recvonly
m=audio 49170 RTP/AVP 0
m=video 51372 RTP/AVP 99
a=rtpmap:99 h263-1998/90000
```

Les champs de texte comme le nom de session et les informations sont des chaînes d'octets qui peuvent contenir tout octet à l'exceptions de 0x00 (Nul), 0x0a (nouvelle ligne ASCII), et 0x0d (retour chariot ASCII). La séquence CRLF (0x0d0a) est utilisée pour terminer un enregistrement, mais les analyseurs DEVRAIENT être tolérants et aussi accepter les enregistrements terminés par un seul caractère de nouvelle ligne. Si l'attribut "a=charset" n'est pas présent, ces chaînes d'octets DOIVENT être interprétées comme contenant des caractères ISO-10646 en codage UTF-8 (la présence de l'attribut "a=charset" peut forcer certains champs à être interprétés différemment).

Une description de session peut contenir un nom de domaine dans les lignes "o=", "u=", "e=", "c=", et "a=". Tout nom de domaine utilisé dans SDP DOIT se conformer aux [RFC1034], [RFC1035]. Les noms de domaines internationalisés (IDN, *Internationalised domain name*) DOIVENT être représentés en utilisant la forme de codage compatible ASCII (ACE, *ASCII Compatible Encoding*) définie dans la [RFC3490] et NE DOIVENT PAS être directement représentés en UTF-8 ou tout autre codage (cette exigence est pour la compatibilité avec la RFC 2327 et les autres normes relatives à SDP, qui précèdent le développement des noms de domaines internationalisés).

5.1 Version du protocole ("v=")

v=0

Le champ "v=" donne la version du protocole de description de session. Le présent mémoire définit la version 0. Il n'y a pas de numéro de version mineur.

5.2 Origine ("o=")

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

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

<nom d'utilisateur> est le nom utilisé pour la connexion sur l'hôte de l'origine, ou c'est "-" si l'hôte d'origine ne prend pas en charge le concept d'identifiant d'utilisateur. Le <nom d'utilisateur> NE DOIT PAS contenir d'espaces.

<identifiant de session> est une chaîne numérique telle que le tuplet <nom d'utilisateur> <identifiant de session> <type de réseau> <type d'adresse>, et <adresse d'envoi individuel> forme un identifiant unique au monde de la session. La méthode d'allocation de <identifiant de session> est au gré de l'outil de création, mais il a été suggéré qu'un horodatage au format du protocole de l'heure du réseau (NTP, *Network Time Protocol*) soit utilisé pour assurer l'unicité [RFC1305].

<version de session> est un numéro de version pour cette description de session. Son usage est au gré de l'outil de création, pour autant que <version de session> soit augmenté quand une modification est faite aux données de la session. Ici aussi, il est RECOMMANDÉ qu'un horodatage au format NTP soit utilisé.

<type de réseau> est une chaîne de texte qui donne le type de réseau. Initialement "IN" est défini comme signifiant "Internet", mais d'autres valeurs POURRONT être enregistrées à l'avenir (voir la Section 8).

<type d'adresse> est une chaîne de texte qui donne le type de l'adresse qui suit. Initialement, "IP4" et "IP6" sont définis, mais d'autres valeurs POURRONT être enregistrées à l'avenir (voir la Section 8).

<adresse d'envoi individuel> est l'adresse de la machine à partir de 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 points de l'adresse IPv4 de la machine. Pour un type d'adresse de IP6, c'est soit le nom de domaine pleinement qualifié de la machine, soit la représentation textuelle compressée de l'adresse IPv6 de la machine. Pour IP4 et 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 être utilisée dans aucun contexte où la description SDP pourrait sortir de la portée où l'adresse a une signification (par exemple, une adresse locale NE DOIT PAS être incluse dans un référentiel de niveau application qui pourrait sortir de la portée).

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

Pour des raisons de confidentialité, il est parfois souhaitable de masquer le nom d'utilisateur et l'adresse IP de l'origine de la session. Si cela pose problème, un <nom d'utilisateur> arbitraire et une <adresse d'envoi individuel> privée PEUVENT être choisis pour remplir le champ "o=", pourvu qu'ils soient choisis d'une manière qui n'affecte pas l'unicité mondiale du champ.

5.3 Nom de session ("s=")

s=<nom de session>

Le champ "s=" est le nom de session textuel. Il DOIT y avoir un et un seul champ "s=" par description de session. Le champ "s=" NE DOIT PAS être vide et DEVRAIT contenir des caractères ISO 10646 (mais voir aussi l'attribut "a=charset"). Si une session n'a pas un nom significatif, la valeur "s= " DEVRAIT être utilisée (c'est-à-dire, une seule espace comme nom de session).

5.4 Informations de session ("i=")

i=<description de session>

Le champ "i=" donne des informations textuelles sur la session. Il DOIT y avoir au plus un champ "i=" de niveau session par description de session, et au plus un champ "i=" par support. Si l'attribut "a=charset" est présent, il spécifie le jeu de caractères utilisé dans le champ "i=". Si l'attribut "a=charset" n'est pas présent, le champ "i=" DOIT contenir des caractères ISO 10646 en codage UTF-8.

Un seul champ "i=" PEUT aussi être utilisé pour chaque définition de support. Dans les définitions de supports, les champs "i=" sont principalement destinés à étiqueter les flux de supports. À ce titre, il vont très probablement être utiles quand une seule session a plus d'un flux de supports distincts du même type de supports. Un exemple serait deux écrans différents, un pour des transparents et un pour les réactions et questions.

Le champ "i=" est destiné à fournir une description de forme libre lisible par l'homme de la session ou de l'objet d'un flux de supports. Il ne convient pas pour l'analyse par un automate.

5.5 URI ("u=")

u=<uri>

Un URI est un identifiant de ressource universel comme utilisé par les clients de la Toile mondiale [RFC3986]. L'URI devrait être un pointeur sur des informations supplémentaires sur la session. Ce champ est FACULTATIF, mais si il est présent, il DOIT être spécifié avant le premier champ de supports. Pas plus d'un champ URI n'est permis par description de session.

5.6 Adresse de messagerie électronique et numéro de téléphone ("e=" et "p=")

e=<adresse de messagerie électronique>
p=<numéro de téléphone>

Les lignes "e=" et "p=" spécifient les informations de contact pour la personne responsable de la conférence. Ce n'est pas nécessairement la même personne que celle qui a créé l'annonce de la conférence.

L'inclusion d'une adresse de messagerie électronique ou d'un numéro de téléphone est FACULTATIVE. Noter que la précédente version de SDP spécifiait qu'un champ d'adresse de messagerie électronique ou de numéro de téléphone DOIT être spécifié, mais cela a été largement ignoré. Ce changement met la spécification en ligne avec l'usage courant.

Si une adresse de messagerie électronique ou un numéro de téléphone est présent, il DOIT être spécifié avant le premier champ de supports. Plus d'un champ d'adresse de messagerie électronique ou de numéro de téléphone peut être donné pour une description de session.

Les numéros de téléphone DEVRAIENT être donnés sous la forme d'un numéro de téléphone international public (voir la Recommandation UIT-T E.164) précédé d'un "+". Des espaces et tirets peuvent être utilisés pour partager un champ de téléphone pour faciliter sa lecture, si désiré. Par exemple : p=+1 617 555-6011

Les adresses de messagerie électronique et les numéros de téléphone peuvent tous deux avoir une chaîne de texte libre FACULTATIVE associée, donnant normalement le nom de la personne qui peut être contactée. Ceci DOIT être enclos entre des parenthèses si c'est présent. Par exemple : e=j.doe@exemple.com (Jane Doe)

L'autre convention de citation de nom de la [RFC2822] est aussi admise pour les adresses de messagerie électronique et les numéros de téléphone. Par exemple : e=Jane Doe <j.doe@exemple.com>

La chaîne de texte libre DEVRAIT être dans le jeu de caractères ISO-10646 avec le codage UTF-8, ou autrement en ISO-8859-1 ou un autre codage si l'attribut approprié de niveau session "a=charset" est établi.

5.7 Données de connexion ("c=")

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

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

Une description de session DOIT contenir soit au moins un champ "c=" dans chaque description de support, soit un seul champ "c=" au niveau session. Elle PEUT contenir un seul champ "c=" de niveau session et un ou des champs "c=" supplémentaires par description de support, et dans ce cas les valeurs par support outrepassent les réglages de niveau session pour les supports respectifs.

Le premier sous champ ("<type de réseau>") est le type de réseau, qui est une chaîne de texte donnant le type du réseau. Initialement, "IN" est défini comme ayant la signification "Internet", mais d'autres valeurs POURRONT être enregistrées à l'avenir (voir la Section 8).

Le second sous champ ("<type d'adresse>") est le type d'adresse. Cela permet à SDP d'être utilisé pour des sessions qui ne sont pas fondées sur IP. Le présent mémoire définit seulement IP4 et IP6, mais d'autres valeurs POURRONT être enregistrées à l'avenir (voir la Section 8)..

Le troisième sous champ ("<adresse de connexion>") est l'adresse de connexion. Des sous champs FACULTATIFS PEUVENT être ajoutés après l'adresse de connexion selon la valeur du champ <type d'adresse>.

Quand le <type d'adresse> est IP4 et IP6, l'adresse de connexion est définie comme suit :

- Si la session est en diffusion groupée, l'adresse de connexion va être une adresse IP de groupe de diffusion groupée. Si la session n'est pas en diffusion groupée, l'adresse de connexion contient alors l'adresse IP d'envoi individuel de la source attendue des données ou du relais de données ou du collecteur de données comme déterminé par les champs d'attribut supplémentaires. Il n'est pas prévu que des adresses d'envoi individuel soient données dans une description de session qui est communiquée par une annonce en diffusion groupée, bien que ce ne soit pas interdit.

- Les sessions qui utilisent une adresse de connexion IPv4 en diffusion groupée DOIVENT aussi avoir une valeur de durée de vie (TTL) présente en plus de l'adresse de diffusion groupée. La TTL et l'adresse définissent ensemble la portée avec laquelle les paquets en diffusion groupée envoyés dans cette conférence vont être envoyés. Les valeurs de TTL DOIVENT être dans la gamme de 0 à 255. Bien que la TTL DOIVE être spécifiée, son utilisation pour déterminer la portée du trafic en diffusion groupée est déconseillée ; les applications DEVRAIENT utiliser à la place une portée d'adresse déterminée administrativement.

La TTL pour la session est ajoutée à l'adresse en utilisant une barre oblique comme séparateur. Un exemple est :

c=IN IP4 224.2.36.42/127

La diffusion groupée IPv6 n'utilise pas la portée par la TTL, et donc, la valeur de TTL NE DOIT PAS être présente pour la diffusion groupée IPv6. Il est prévu que la portée des adresses IPv6 sera utilisée pour limiter la portée des conférences.

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

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

Si le nombre d' adresses n'est pas donné, il est supposé être un. Les adresses de diffusion groupée ainsi allouées sont contiguës au dessus de l'adresse de base, de sorte que, par exemple : c=IN IP4 224.2.1.1/127/3 déclarerait que les adresses 224.2.1.1, 224.2.1.2, et 224.2.1.3 sont à utiliser au TTL de 127. Ceci est sémantiquement identique à inclure 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

De même, un exemple IPv6 pourrait être : c=IN IP6 FF15::101/3

qui est sémantiquement équivalent à :

c=IN IP6 FF15::101
c=IN IP6 FF15::102
c=IN IP6 FF15::103
(on se souvient que le champ TTL n'est pas présent dans la diffusion groupée IPv6).

Plusieurs adresses ou lignes "c=" PEUVENT être spécifiées sur la base du support si elles fournissent des adresses de diffusion groupée pour des couches différentes dans un schéma de codage hiérarchique ou en couches. Elles NE DOIVENT PAS être spécifiées pour un champ "c=" de niveau session.

La notation barre oblique pour plusieurs adresses décrite ci-dessus NE DOIT PAS être utilisée pour les adresses IP en envoi individuel.

5.8 Bande passante ("b=")

b=<bwtype>:<bande passante>

Ce champ FACULTATIF note la bande passante proposée à utiliser par la session ou le support. Le <bwtype> est un modificateur alphanumérique qui donne la signification du chiffre de <bande passante>. Deux valeurs sont définies dans la présente spécification, mais d'autres valeurs POURRONT être enregistrée à l'avenir (voir la Section 8 et les [RFC3556], [RFC3890]):

CT. Si la bande passante d'une session ou d'un support dans une session est différente de la bande passante implicite provenant de la portée, une ligne "b=CT:..." DEVRAIT être fournie pour la session donnant la limite supérieure proposée pour la bande passante utilisée (la bande passante de la "conférence totale"). Le principal objet de cela est de donner une idée approximative de si deux sessions ou plus peuvent coexister simultanément. Quand on utilise le modificateur CT avec RTP, si plusieurs sessions RTP font partie de la conférence, la conférence totale se réfère à la bande passante totale de toutes les sessions RTP.

AS. La bande passante est interprétée comme spécifique de l'application (cela va être le concept de bande passante maximum de l'application). Normalement, cela va coïncider avec ce qui est réglé dans la commande "bande passante maximum" de l'application, si applicable. Pour les applications fondées sur RTP, AS donne la "bande passante de session" RTP comme défini au paragraphe 6.2 de la [RFC3550].

Noter que CT donne un chiffre de bande passante totale pour tous les supports à 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 qui envoient simultanément.

Un préfixe "X-" est défini pour les noms de <bwtype>. Il est destiné seulement aux utilisations expérimentales. Par exemple : b=X-YZ:128

L'utilisation du préfixe "X-" N'EST PAS RECOMMANDÉE. De nouveaux modificateur DEVRAIENT plutôt être enregistrés auprès de l'IANA dans l'espace de noms standard. Les analyseurs SDP DOIVENT ignorer les champ de bande passante avec des modificateurs inconnus. Les modificateurs DOIVENT être alphanumériques et, bien qu'aucune limite de longueur ne soit donnée, il est recommandé qu'ils soient courts.

La <bande passante> est interprétée comme des kilobits par seconde par défaut. La définition d'un nouveau modificateur <bwtype> PEUT spécifier que la bande passante est à interpréter dans une autre unité (les modificateurs "CT" et "AS" définis dans le présent mémoire utilisent les unités par défaut).

5.9 Heures ("t=")

t=<heure de début> <heure de fin>

Les lignes "t=" spécifient les heures de début et de fin d'une session. Plusieurs lignes "t=" PEUVENT être utilisées si une session est active à plusieurs heures espacées de façon irrégulière ; chaque ligne "t=" supplémentaire spécifie une période supplémentaire pendant laquelle la session va être active. Si la session est active à des heures régulières, une ligne "r=" (voir ci-dessous) devrait être utilisée en plus de, et à la suite, d'une ligne "t=" -- dans ce cas la ligne "t=" spécifie les heures de début et de fin de la séquence répétée.

Le premier et le second sous champs donnent les heures respectivement de début et de fin de la session. Ces valeurs sont la représentation en décimal des valeurs horaires du protocole de l'heure du réseau (NTP) en secondes depuis 1900 [RFC1305]. Pour convertir ces valeurs en heure UNIX, soustraire le décimal 2 208 988 800.

Les horodatages NTP sont représentés par des valeurs de 64 bits, qui reviennent à zéro quelque part en 2036. Comme SDP utilise une représentation décimale de longueur arbitraire, ceci ne devrait pas causer de problème (les horodatages SDP DOIVENT continuer de compter en secondes depuis 1900, NTP va utiliser la valeur modulo la limite de 64 bits).

Si <heure d'arrêt> est réglé à zéro, la session n'est alors pas limitée, bien qu'elle ne devienne pas active avant <heure de début>. Si <heure de début> est aussi zéro, la session est considérée comme permanente.

Les interfaces d'utilisateur DEVRAIENT fortement déconseiller la création de sessions non limitées et permanentes car cela ne donne pas d'informations sur le moment où elle va réellement se terminer, et rend donc la programmation difficile.

Une hypothèse générale peut être faite, quand on affiche des sessions non limitées qui ne sont pas arrivées en fin de temporisation chez l'utilisateur, qu'une session non limitée ne sera active que pour une demie heure à partir de l'heure actuelle ou de l'heure de début de la session, quel que soit la dernière. Si un comportement différent est exigé, une heure de fin DEVRAIT être donnée et modifiée comme approprié quand de nouvelles informations deviennent disponibles sur le moment où la session devrait réellement prendre fin.

Les sessions permanentes peuvent être présentées à l'utilisateur comme n'étant jamais actives sauf si elles sont associées à des heures de répétition qui déclarent précisément quand la session va être active.

5.10 Heures de répétition ("r=")

r=<intervalle de répétition> <durée active> <décalages par rapport à l'heure de début>

Les champs "r=" spécifient les heures de répétition pour une session. Par exemple, si une session est active à 10 h le lundi et 11 h le mardi pendant une heure chaque semaine pendant trois mois, alors <heure de début> dans le champ "t=" correspondant va être la représentation NTP de 10 h le premier lundi, <intervalle de répétition> va être une semaine, <durée active> va être une heure, et les décalages vont être zéro et 25 heures. Le champ "t=" correspondant d'heure d'arrêt va 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 les suivants :

t=3034423619 3042462419
r=604800 3600 0 90000

Pour rendre la description plus compacte, les heures peuvent aussi être données en unités de jours, heures, ou minutes. La syntaxe pour cela est un nombre immédiatement suivi par un seul caractère sensible à la casse. Les unités fractionnelles ne sont pas permises – une plus petite unité devrait plutôt être utilisée. Les caractères de spécification d'unités suivants sont permis :

d - jours (86400 secondes)
h - heures (3600 secondes)
m - minutes (60 secondes)
s - secondes (permis pour être complet)

Donc, l'annonce de session ci-dessus pourrait aussi avoir été écrite : r=7d 1h 0 25h

Les répétitions mensuelles et annuelles ne peuvent pas être directement spécifiées avec une seule heure de répétition SDP ; des champs "t=" séparés devraient plutôt être utilisés pour faire explicitement la liste des heures de session.

5.11 Zones horaires ("z=")

z=<heure d'ajustement> <décalage> <heure d'ajustement> <décalage> ....

Pour programmer une session répétés qui englobe un changement de l'heure d'été/hiver, il est nécessaire de spécifier les décalages à l'heure de base. Ceci est nécessaire parce que des zones horaires différentes changent d'heure à des moments différents, des pays différents passent à l'heure d'été/hiver à des dates différentes, et certains pays n'ont pas du tout de changement d'heure.

Donc, afin de programmer une session qui est à la même heure d'hiver et d'été, il doit être possible de spécifier sans ambiguïté dans quelle zone horaire une session est programmée. Pour simplifier cette tâche pour les receveurs, on permet à l'envoyeur de spécifier l'heure NTP où un ajustement de zone horaire se produit et le décalage à partir de l'heure à laquelle la session a été programmée. Le champ "z=" permet à l'envoyeur de spécifier une liste de ces heures d'ajustement et des décalages par rapport à cette heure de base.

Un exemple pourrait être le suivant : z=2882844526 -1h 2898848070 0

Cela spécifie qu'à l'heure 2882844526, l'heure de base par laquelle les heures de répétition de la session sont calculées est reculée d'une heure, et qu'à l'heure 2898848070, l'heure de base originale de la session est restaurée. Les ajustements sont toujours par rapport à l'heure de début spécifiée – ils ne sont pas cumulatifs. Les ajustements s'appliquent à toutes les lignes "t=" et "r=" d'une description de session.

Si une session va probablement durer plusieurs années, il est supposé que l'annonce de session va être modifiée périodiquement plutôt que de transmettre des ajustements valables sur plusieurs années dans une annonce de session.

5.12 Clés de chiffrement ("k=")

k=<méthode>
k=<méthode>:<clé de chiffrement>

Si il est transporté sur un canal sûr et de confiance, le protocole de description de session PEUT être utilisé pour convoyer les clés de chiffrement. Un mécanisme simple pour l'échange de clés est fourni par le champ ("k=") bien que ceci soit principalement pris en charge pour la compatibilité avec les anciennes mises en œuvre et son utilisation est NON RECOMMANDÉE. Un travail est en cours pour définir de nouveaux mécanismes d'échange de clés à utiliser avec SDP [RFC4567], [RFC4568], et il est prévu que les nouvelles applications vont utiliser ces mécanismes.

Un champ clé est permis avant la première entrée de supports (et dans ce cas, elle s'applique à tous les supports de la session) ou pour chaque entrée de supports comme nécessaire. Le format de clés et leur usage sort du domaine d'application du présent document, et le champ clé ne fournit pas de moyen d'indiquer l'algorithme de chiffrement à utiliser, le type de clé, ou d'autres informations sur la clé : cela est supposé fourni par le protocole de niveau supérieur en utilisant SDP. Si il est nécessaire de porter ces informations dans SDP, les extensions mentionnées précédemment DEVRAIENT être utilisées. De nombreux protocoles de sécurité exigent deux clés : une pour la confidentialité, une autre pour l'intégrité. La présente spécification ne prend pas en charge le transfert de deux clés.

La méthode indique le mécanisme à utiliser pour obtenir une clé utilisable par des moyens externes, ou par la clé de chiffrement codée donnée. Les méthodes suivantes sont définies :

k=clear:<clé de chiffrement>
: La clé de chiffrement est incluse non transformée dans ce champ clé. Cette méthode NE DOIT PAS être utilisée si il ne peut être garanti que SDP est convoyé sur un canal sûr. La clé de chiffrement est interprétée comme du texte conformément à l'attribut de jeu de caractères ; on utilise la méthode "k=base64:" pour convoyer les caractères qui sont par ailleurs interdits dans SDP.

k=base64:<clé de chiffrement codée>
: La clé de chiffrement est incluse dans ce champ clé mais a été codée en base64 [RFC3548] parce qu'elle comporte des caractères qui sont interdits dans SDP. Cette méthode NE DOIT PAS être utilisée si il ne peut être garanti que SDP est convoyé sur un canal sûr.

k=uri:<URI pour obtenir la clé>
: Un identifiant de ressource universel est inclus dans le champ clé. L'URI se réfère aux données contenant la clé, et peut exiger une authentification supplémentaire avant que la clé puisse être retournée. Quand une demande est faite à cet URI, la réponse devrait spécifier le codage de la clé. L'URI est souvent un URI HTTP protégé par la couche de connexion sécurisée/sécurité de la couche transport (SSL/TLS, *Secure Socket Layer/Transport Layer Security*) ("https:") bien que ce ne soit pas exigé.

k=prompt
: Aucune clé n'est incluse dans cette description SDP, mais la session ou le flux de supports auquel se réfère le champ clé est chiffré. L'utilisateur devrait être invité à aller chercher la clé quand il tente de se joindre à la session, et cette clé fournie par l'utilisateur devrait alors être utilisée pour déchiffrer les flux de supports. L'utilisation de clés spécifiées par l'utilisateur n'est PAS RECOMMANDÉE, car de telles clés tendent à avoir des propriétés de sécurité faibles.

Le champ clé NE DOIT PAS être utilisé si il ne peut être garanti que SDP est convoyé sur un canal sûr et de confiance. Un exemple d'un tel canal pourrait être SDP incorporé dans un message S/MIME ou une session HTTP protégée par TLS. Il est important de s'assurer que le canal sûr est avec la partie qui est autorisée à se joindre à la session, et non avec un intermédiaire : si un serveur mandataire de mise en antémémoire est utilisé, il est important de s'assurer que le mandataire est soit de confiance, soit incapable d'accéder à SDP.

5.13 Attributs ("a=")

a=<attribut>
a=<attribut>:<valeur>

Les attributs sont le principal moyen pour étendre SDP. Les attributs peuvent être définis comme étant utilisés comme attributs de "niveau session", de "niveau support", ou les deux.

Une description de support peut avoir un nombre quelconque d'attributs (champs "a=") qui sont spécifiques du support. On les appelle des attributs "de niveau support" et ils ajoutent des informations sur le flux des supports. Des champs d'attribut peuvent aussi être ajoutés avant le premier champ de supports ; ces attributs "de niveau session" portent des informations supplémentaires qui s'appliquent à la conférence comme un tout plutôt qu'aux supports individuels.

Les champs d'attribut peuvent être de deux formes :
- o Un attribut de propriété est simplement de forme "a=<fanion>". Ce sont des attributs binaires, et la présence de l'attribut porte l'idée que l'attribut est une propriété de la session. Un exemple serait "a=recvonly".
- o Un attribut de valeur est de forme "a=<attribut>:<valeur>". Par exemple, un tableau pourrait avoir l'attribut de valeur "a=orient: paysage".

L'interprétation de l'attribut dépend de l'outil support invoqué. Les receveurs de descriptions de session devraient donc être configurables dans leur interprétation des descriptions de session en général et des attributs en particulier.

Les noms d'attribut DOIVENT utiliser le sous ensemble US-ASCII de ISO-10646/UTF-8.

Les valeurs d'attribut sont des chaînes d'octet, et PEUVENT utiliser toute valeur d'octet sauf 0x00 (Nul), 0x0A (LF), et 0x0D (CR). Par défaut, les valeurs d'attribut sont à interpréter comme étant dans le jeu de caractères ISO-10646 avec codage UTF-8. À la différence des autres champs de texte, les valeurs d'attribut NE sont normalement PAS affectées par l'attribut "charset" car cela rendraient problématiques les comparaisons entre deux valeurs connues. Cependant, quand un attribut est défini, il peut l'être comme dépendant du 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 DOIVENT être enregistrés auprès de l'IANA (voir la Section 8). Si un attribut reçu n'est pas compris, il DOIT être ignoré par le receveur.

5.14 Descriptions de supports ("m=")

m=<support> <accès> <proto> <fmt> ...

Une description de session peut contenir un certain nombre de descriptions de supports. Chaque description de support commence par un champ "m=" et est terminée soit par le prochain champ "m=", soit par la fin de la description de session. Un champ de support a plusieurs sous champs:

<support> est le type de support. Les supports actuellement définis sont "audio", "vidéo", "texte", "application", et "message", mais cette liste pourra être étendue à l'avenir (voir la Section 8).

<accès> est l'accès de transport auquel le flux de supports est 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 sous champ <proto> du champ de support. D'autres accès utilisés par l'application de supports (comme l'accès du protocole de contrôle RTP (RTCP) [RFC3550]) PEUVENT être déduits algorithmiquement de l'accès de base du support ou PEUVENT être spécifiés dans un attribut séparé (par exemple, "a=rtcp:" comme défini dans la [RFC3605]).

Si des accès non contigus sont utilisés ou si ils ne suivent pas la règle de parité des accès RTP pairs et des accès RTCP impairs, l'attribut "a=rtcp:" DOIT être utilisé. Les applications à qui il est demandé d'envoyer des supports à un <accès> qui est impair et où le "a=rtcp:" est présent NE DOIVENT PAS soustraire 1 de l'accès RTP : c'est-à-dire, elles DOIVENT envoyer le RTP à l'accès indiqué dans <accès> et envoyer le RTCP à l'accès indiqué dans l'attribut "a=rtcp".

Pour les applications où des flux codés hiérarchiquement sont envoyés à une adresse d'envoi individuel, il peut être nécessaire de spécifier plusieurs accès de transport. Ceci est fait en utilisant une notation similaire à celle utilisée pour les adresses de diffusion groupée IP dans le champ "c=" :

m=<support> <accès>/<nombre d'accès> <proto> <fmt> ...

Dans ce cas, les accès utilisés dépendent du protocole de transport. Pour RTP, ce sont par défaut les seuls accès de numéro pair qui sont utilisés pour les données avec les accès impairs supérieurs de un correspondants utilisés pour le RTCP appartenant à la session RTP, et le <nombre d'accès> note le nombre des sessions RTP. Par exemple :

m=video 49170/2 RTP/AVP 31

va spécifier 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). Si des accès non contigus sont requis, ils doivent être signalés en utilisant un attribut distinct (par exemple, "a=rtcp:" comme défini dans la [RFC3605]).

Si plusieurs adresses sont spécifiées dans le champ "c=" et si plusieurs accès sont spécifiés dans le champ "m=", Une transposition biunivoque de l'accès à l'adresse correspondante est impliquée. Par exemple :

c=IN IP4 224.2.1.1/127/2
m=video 49170/2 RTP/AVP 31

impliquerait que l'adresse 224.2.1.1 est utilisée avec les accès 49170 et 49171, et que l'adresse 224.2.1.2 est utilisée avec les accès 49172 et 49173.

La sémantique de plusieurs lignes "m=" utilisant la même adresse de transport est indéfinie. Cela implique que, à la différence de la pratique limitée du passé, il n'y a pas de groupement implicite défini par ce moyen et qu'un cadre de groupement explicite (par exemple, de la [RFC3388]) devrait plutôt être utilisé pour exprimer la sémantique prévue.

<proto> est le protocole de transport. La signification du protocole de transport dépend du champ type d'adresse dans le champ "c=" pertinent. Donc un champ "c=" de IP4 indique que le protocole de transport fonctionne sur IPv4. Les protocoles de transport suivants sont définis, mais peuvent être étendus par l'enregistrement de nouveaux protocoles auprès de l'IANA (voir la Section 8) :

* udp : note un protocole non spécifié fonctionnant sur UDP,
* RTP/AVP : note RTP [RFC3550] utilisé sous le profil RTP pour les conférences audio et vidéo avec contrôle minimal [RFC3551] fonctionnant sur UDP,
* RTP/SAVP : note le protocole sûr de transport en temps réel [RFC3711] fonctionnant sur UDP.

La principale raison pour spécifier le protocole de transport en plus du format du support est que les mêmes formats de supports standard peut être portés sur des protocoles de transport différents même quand le protocole réseau est le même – un exemple historique est l'audio en modulation par impulsions codées (MIC) et l'audio en MIC RTP ; un autre exemple serait l'audio en MIC TCP/RTP. De plus, les outils de relais et de surveillance qui sont spécifiques du protocole de transport mais indépendants du format sont possibles.

<fmt> est une description du format de support. Le quatrième sous champ et tous les suivants décrivent le format du support. L'interprétation du format du support dépend de la valeur du sous champ <proto>. Si le sous champ <proto> est "RTP/AVP" ou "RTP/SAVP" les sous champs <fmt> contiennent les numéros de type de charge utile RTP. Quand une liste de numéros de type de charge utile est donnée, cela implique que tous ces formats de charge utile PEUVENT être utilisés dans la session, et ces formats de charge utile sont mentionnés dans l'ordre de préférence, le premier format de la liste étant le préféré ; dans ce cas, le premier format de charge utile acceptable depuis le début de la liste DEVRAIT être utilisé pour la session. Pour les allocations dynamiques de type de charge utile, l'attribut "a=rtpmap:" (voir la Section 6) DEVRAIT être utilisé pour transposer d'un numéro de type de charge utile RTP en un nom de codage de support qui identifie le format de charge utile. L'attribut "a=fmtp:" PEUT être utilisé pour spécifier des paramètres de format (voir la Section 6).

Si le sous-champ <proto> est "udp", les sous champs <fmt> DOIVENT se référer à un type de support qui décrive le format sous les types de support de niveau supérieur "audio", "video", "text", "application", ou "message". L'enregistrement du type de support DEVRAIT définir le format de paquet à utiliser avec le transport UDP

Pour les supports qui utilisent d'autres protocoles de transport, le champ <fmt> est spécifique du protocole. Les règles pour l'interprétation du sous champ <fmt> DOIVENT être définies à l'enregistrement des nouveaux protocoles (voir au paragraphe 8.2.2).

6. Attributs SDP

Les attributs suivants sont définis. Comme les rédacteurs d'applications peuvent ajouter de nouveaux attributs lorsque nécessaire, cette liste n'est pas exhaustive. Les procédures d'enregistrement pour les nouveaux attributs sont définies au paragraphe 8.2.4.

a=cat:<catégorie>
Cet attribut donne la catégorie hiérarchique séparée par des points de la session. C'est pour permettre à un receveur de filtrer par catégorie les sessions non voulues. Il n'y a pas de registre central des catégories. C'est un attribut de niveau session, et il ne dépend pas du jeu de caractères.

a=keywds:<mots clés>
Comme l'attribut cat, c'est pour aider à identifier les sessions voulues chez le receveur. Cela permet à un receveur de choisir une session intéressante sur la base des mots clés qui décrivent l'objet de la session ; il n'y a pas de registre central des mots clés. C'est un attribut de niveau session. C'est un attribut qui dépend du jeu de caractères, ce qui signifie que sa valeur devrait être interprétée dans le jeu de caractères spécifié pour la description de session si il en est spécifié une, ou par défaut en ISO 10646/UTF-8.

a=tool:<nom et version de l'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 du paquet>
Cela donne la durée en millisecondes représentée par le support dans un paquet. Ceci n'est probablement significatif que pour les données audio, mais peut être utilisé avec d'autres types de supports si cela a un sens. Il ne devrait pas être nécessaire de connaître ptime pour décoder de l'audio RTP ou vat, et il est entendu comme une recommandation pour le codage/mise en paquet de l'audio. C'est un attribut de niveau support, et ne dépend pas du jeu de caractères.

a=maxptime:<durée maximum du paquet>
Cela donne la quantité maximum de support qui peut être encapsulée dans chaque paquet, exprimée comme un temps en millisecondes. Le temps DEVRA être calculé comme la somme des durées des supports présents dans le paquet. Pour les codecs fondés sur la trame, le temps DEVRAIT être un multiple entier de la taille de trame. Cet attribut n'est probablement significatif que pour les données audio, mais peut être utilisé avec d'autres types de supports si cela a un sens. C'est un attribut de niveau support, et il ne dépend pas du jeu de caractères. Noter que cet attribut a été introduit après la RFC 2327, et les mises en œuvre non mises à jour vont ignorer cet attribut.

a=rtpmap:<type de charge utile> <nom du codage>/<débit d'horloge> [/<paramètres de codage>]
Cet attribut transpose d'un numéro de type de charge utile RTP (comme utilisé dans une ligne "m=") en un nom de codage notant le format de charge utile à utiliser. Il fournit aussi des informations sur le débit d'horloge et les paramètres de codage. C'est un attribut de niveau support qui ne dépend pas du jeu de caractères. Bien qu'un profil RTP puisse faire des allocations statiques de numéros de type de charge utile aux formats de charge utile, il est plus courant qu'une allocation soit faite dynamiquement en utilisant des attributs "a=rtpmap:". Comme exemple de type de charge utile statique, considérons un MIC en loi µ codé sur un seul canal audio échantillonné à 8 kHz. Ceci est complètement défini dans le profil RTP Audio/Vidéo comme type de charge utile 0, de sorte qu'il n'y a pas besoin d'un attribut "a=rtpmap:", et le support pour un tel flux envoyé à l'accès UDP 49232 peut être spécifié comme : m=audio 49232 RTP/AVP 0

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

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

Un seul attribut rtpmap peut être défini pour chaque format de support spécifié. 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 des noms de codage valides et/ou un moyen d'enregistrer les noms de codage si ce profil est utilisé avec SDP.

Les profils "RTP/AVP" et "RTP/SAVP" utilisent des sous types de support pour les noms de codages, sous le type de support de niveau supérieur noté dans la ligne "m=". Dans l'exemple ci-dessus, les types de supports sont "audio/l8" et "audio/l16".

Pour les flux audio, <paramètres de codage> indique le nombre de canaux audio. Ce paramètre est FACULTATIF et peut être omis si le nombre de canaux est un, pourvu qu'aucun paramètre supplémentaire ne soit nécessaire.

Pour les flux vidéo, aucun paramètre de codage n'est actuellement spécifié.

Des paramètres de codage supplémentaires POURRONT être définis à l'avenir, mais des paramètres spécifiques du codec NE DEVRAIENT PAS être ajoutés. Les paramètres ajoutés à un attribut "a=rtpmap:" DEVRAIENT être seulement ceux nécessaires pour qu'un répertoire de sessions fasse le choix des supports appropriés pour participer à une session. Les paramètres spécifiques du codec devraient être ajoutés dans d'autres attributs (par exemple, "a=fmtp:").

Note : les formats audio RTP ne comportent normalement pas d'information sur le nombre d'échantillons par paquet. Si une mise en paquet non par défaut (comme défini dans le profil RTP Audio/Vidéo) est nécessaire, l'attribut "ptime" est utilisé comme montré précédemment.

a=recvonly *(réception seule)*
Cela spécifie que les outils devrait être commencés en mode réception seule lorsque applicable. Ce peut être un attribut de niveau session ou de niveau support, et il ne dépend pas du jeu de caractères. Noter que recvonly s'applique seulement au support, et non à un protocole de contrôle associé (par exemple, un système fondé sur RTP en mode recvonly DEVRAIT quand même envoyer des paquets RTCP).

a=sendrecv *(envoi et réception)*
Cela spécifie que les outils devraient être commencés en mode envoi et réception. Ceci est nécessaire pour les conférences interactives avec des outils qui prennent par défaut le mode réception seule. Il peut être un attribut de niveau session ou de niveau support, et il ne dépend pas du jeu de caractères. Si aucun des attributs "sendonly", "recvonly", "inactive", et "sendrecv" n'est présent, "sendrecv" DEVRAIT être supposé par défaut pour les sessions qui ne sont pas du type de conférence "broadcast" ou "H332" (voir ci-dessous).

a=sendonly *(réception seule)*
Cela spécifie que les outils devraient être commencés en mode envoi seulement. Un exemple peut être lorsque une adresse d'envoi individuel différente est à utiliser pour une destination de trafic et pour la source de trafic. Dans ce cas, deux descriptions de supports peuvent être utilisées, une sendonly et une recvonly. Ce peut être un attribut de niveau session ou de niveau support, mais il ne va normalement être utilisé que comme attribut de support. Il ne dépend pas du jeu de caractères. Noter que sendonly ne s'applique qu'au support, et tout protocole de contrôle associé (par exemple, RTCP) DEVRAIT quand même être reçu et traité comme d'ordinaire.

a=inactive
Cela spécifie que les outils devraient être commencés en mode inactif. Ceci est nécessaire pour les conférences interactives où les utilisateurs peuvent mettre d'autres utilisateurs en garde. Aucun support n'est envoyé sur un flux de supports inactif. Noter qu'un système fondé sur RTP DEVRAIT quand même envoyer RTCP, même si il a connencé comme inactif. Il peut être un attribut de niveau session ou support, et il ne dépend pas du jeu de caractères.

a=orient:<orientation>
Normalement ce n'est utilisé que pour un tableau ou outil de présentation. Cela spécifie l'orientation d'un espace de travail sur l'écran. C'est un attribut de niveau support. Les valeurs permises sont "portrait", "paysage", et "bord de mer" (paysage inversé). 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 le type par défaut pour les sessions "type:broadcast", "type:meeting" devrait impliquer "sendrecv", et "type:moderated" devrait indiquer l'utilisation d'un outil de contrôle de la prise de parole et que les outils du support démarrent en ne donnant pas la parole aux nouveaux sites qui se joignent à la conférence.
Spécifier l'attribut "type:H332" indique que cette session à couplage lâche fait partie d'une session H.332 comme défini dans la Recommandation UIT-T H.332 [H.332]. Les outils de supports devraient être commencés en "recvonly".
Spécifier l'attribut "type:test" est suggéré comme un conseil que, sauf demandé explicitement autrement, les receveurs peuvent en toute sécurité éviter d'afficher cette description de session aux utilisateurs.
L'attribut type est de niveau session, et il ne dépend pas du jeu de caractères.

a=charset:<jeu de caractères>
Cela spécifie le jeu de caractères à utiliser pour afficher le nom de session et les données d'information. Par défaut, le jeu de caractères ISO-10646 en codage UTF-8 est utilisé. Si une représentation plus compacte est exigée, d'autres jeux de caractères peuvent être utilisés. Par exemple, ISO 8859-1 est spécifié avec les attributs SDP suivants :

a=charset:ISO-8859-1
C'est un attribut de niveau session qui ne dépend pas du jeu de caractères. Le jeu de caractères spécifié DOIT être un de ceux enregistrés auprès de l'IANA, comme ISO-8859-1. L'identifiant de jeu de caractères est une chaîne US-ASCII et DOIT être comparée aux identifiant de l'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 sont affectées par lui DEVRAIENT être considérées comme des chaînes d'octets.

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

a=sdplang:<étiquette de langue>
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'information SDP de niveau support associé à ce support. Plusieurs attributs sdplang peuvent être fournis au niveau session ou au niveau support si plusieurs langues dans la description de session ou de support utilisent plusieurs langages, et dans ce cas l'ordre des attributs indique l'ordre d'importance des divers langages dans la session ou support du plus important au moins important. En général, l'envoi de descriptions de session consistant en plusieurs langages est déconseillé. Plusieurs descriptions DEVRAIENT plutôt 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 langue de la [RFC3066] en US-ASCII. Il ne dépend pas de l'attribut de jeu de caractère. Un attribut "sdplang" DEVRAIT être spécifié quand une session est de portée suffisante pour franchir les limites géographiques où le langage des receveurs ne peut plus être supposé, ou lorsque la session est dans une langue différente de la norme locale supposée.

a=lang:<étiquette de langue>
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 le langage pour ce support, outrepassant tout langage de niveau session spécifié. Plusieurs attributs lang peuvent être fournis soit au niveau session, soit au niveau support si la description de session ou le support utilise plusieurs langages, et dans ce cas l'ordre des attributs indique l'ordre d'importance des divers langages dans la session ou support du plus important au moins important. La valeur de l'attribut "lang" doit être une seule étiquette de langue de la [RFC3066] en US-ASCII. Il ne dépend pas de l'attribut charset. Un attribut "lang" DEVRAIT être spécifié quand une session est de portée suffisante pour franchir les limites géographique où le langage des receveurs ne peut être supposé, ou lorsque la session est dans une langue différente de la norme locale supposée.

a=framerate:<taux de trame>
Cela donne le taux de trame vidéo maximum en trames/s. Il est destiné à être une recommandation de codage des données vidéo. Les représentations décimales des valeurs fractionnaires utilisant la notation "<entier>.<fraction>" sont permises. C'est un attribut de niveau support, défini seulement pour les supports vidéo, et il ne dépend pas du jeu de caractères.

a=quality:<qualité>
Cela fait une suggestion sur la qualité du codage par une valeur d'entier. L'intention de l'attribut de qualité pour la vidéo est de spécifier un compromis non 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 les significations suggérées suivantes :
10 - meilleure qualité d'image fixe que peut donner le schéma de compression.
5 – comportement par défaut ne donnant pas de suggestion de qualité.
0 – plus mauvaise qualité d'image fixe dont le concepteur du codec pense qu'elle est encore utilisable.
C'est un attribut de niveau 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 à convoyer d'une façon telle que SDP n' pas à les comprendre. Le format doit être un des formats spécifiés pour le support. Les paramètres spécifiques du format peuvent être tout ensemble des paramètres requis pour être convoyés par SDP et donnés inchangés à l'outil de support qui va utiliser ce format. Au plus une instance de cet attribut est permise pour chaque format. C'est un attribut de niveau support, et il ne dépend pas du jeu de caractères.

7. Considérations sur la sécurité

SDP est fréquemment utilisé avec le protocole d'initialisation de session [RFC3261] en utilisant le modèle offre/réponse de la [RFC3264] pour s'accorder sur les paramètres des sessions en envoi individuel. Lorsque utilisé de cette manière, les considérations sur la sécurité de ces protocoles s'appliquent.

SDP est un format de description de session qui décrit des sessions multimédia. Les entités qui reçoivent et agissent sur un message SDP DEVRAIENT être conscientes qu'une description de session ne peut être de confiance sauf si elle a été obtenue par un protocole de transport authentifié provenant d'une source connue et de confiance. De nombreux protocoles de transport différents peuvent être utilisés pour distribuer la description de session, et la nature de l'authentification va

différer d'un transport à l'autre. Pour certains transports, les caractéristiques de sécurité ne sont souvent pas déployées. En cas d'une description de session qui n'a pas été obtenue en confiance, le point d'extrémité DEVRAIT faire attention parce que, entre autres attaques, les supports de sessions reçus peuvent n'être pas ceux attendus, la destination où les supports sont envoyés peut n'être pas celle attendue, tout paramètre de la session peut être incorrect, ou la sécurité du support peut être compromise. Il appartient au point d'extrémité de prendre une décision raisonnable prenant en compte les risques pour la sécurité de l'application et les préférences de l'utilisateur et il peut décider de demander à l'utilisateur si il accepte ou non la session.

Un transport qui peut être utilisé pour distribuer les descriptions de session est le protocole d'annonce de session (SAP, *Session Announcement Protocol*). SAP fournit des mécanismes à la fois de chiffrement et d'authentification, mais du fait de la nature des annonces de session, il est probable qu'en de nombreuses occasions le générateur d'une annonce de session ne peut pas être authentifié parce qu'il n'est pas connu auparavant du receveur de l'annonce et parce qu 'aucune infrastructure de clé publique commune n'est disponible.

À la réception d'une description de session sur un mécanisme de transport non authentifié ou d'une source qui n'est pas de confiance, le logiciel qui analyse la session devrait prendre quelques précautions. Les descriptions de session contiennent des informations nécessaires pour lancer le logiciel sur le système receveur. Le logiciel qui analyse une description de session NE DOIT PAS être capable de lancer un autre logiciel sauf celui qui est spécifiquement configuré comme logiciel approprié pour participer aux sessions multimédia. Il est normalement considéré comme inapproprié qu'un logiciel qui analyse une description de session lance, sur le système d'un utilisateur, le logiciel qui est approprié pour participer aux sessions multimédia, sans que l'utilisateur soit préalablement informé qu'un tel logiciel va être lancé et que l'utilisateur donne son consentement. Donc, une description de session arrivant par une annonce de session, un message électronique, une invitation à la session, ou une page de la Toile mondiale NE DOIT PAS engager l'usager dans une session multimédia interactive sans que l'usager ait explicitement pré-autorisé une telle action. Comme il n'est pas toujours simple de dire si une session est ou non interactive, les applications qui ne sont pas sûres devrait supposer que les sessions sont interactives.

Dans la présente spécification, il n'y a pas d'attribut qui permette au receveur d'une description de session d'être informé de lancer des outils multimédia dans un mode où ils transmettraient pas défaut. Dans certaines circonstances, il pourrait être approprié de définir de tels attributs. Si cela est fait, une application qui analyse une description de session contenant de tels attributs DEVRAIT soit les ignorer, soit informer l'usager que se joindre à cette session va résulter en la transmission automatique de données multimédia. Le comportement par défaut pour un attribut inconnu est de l'ignorer.

Dans certains environnements, il est devenu courant que les systèmes intermédiaires interceptent et analysent les descriptions de session contenues dans d'autres protocoles de signalisation. Ceci est fait pour toute une série de raisons, incluant, mais sans s'y limiter, pour ouvrir des trous dans les pare-feu pour permettre aux flux de supports de passer, ou pour marquer, attribuer des priorités, ou bloquer sélectivement du trafic. Dans certains cas, de tels systèmes intermédiaires peuvent modifier la description de session, par exemple, pour que le contenu de la description de session corresponde aux liens de NAT créés de façon dynamique. Ces comportements NE SONT PAS RECOMMANDÉS sauf si la description de session est convoyée d'une manière telle qu'elle permette au système intermédiaire de faire les vérifications appropriées pour établir l'authenticité de la description de session, et l'autorité de sa source pour établir de telles sessions de communication. SDP par lui-même n'inclut pas des informations suffisantes pour permettre ces vérifications : elles dépendent du protocole encapsulant (par exemple, SIP ou RTSP).

L'utilisation du champ "k=" pose un problème de sécurité significatif, car il porte les clés de chiffrement de session en clair. SDP NE DOIT PAS être utilisé pour porter du matériel de chiffrement, sauf si il peut être garanti que le canal sur lequel SDP est livré est à la fois privé et authentifié. De plus, la ligne "k=" ne donne aucun moyen pour indiquer ou négocier les algorithmes de clé de chiffrement. Comme elle ne vise qu'une seule clé symétrique, plutôt que des clés séparées pour la confidentialité et l'intégrité, son utilité est très limitée. L'utilisation de la ligne "k=" N'EST PAS RECOMMANDÉE, comme expliqué au paragraphe 5.12.

8. Considérations relatives à l'IANA

8.1 Type de support "application/sdp"

Un enregistrement de type de support de la RFC 2327 est à mettre à jour, comme défini ci-dessous.

Pour : ietf-types@iana.org
Sujet : enregistrement du type de support "application/sdp"
Nom du type : application
Nom du sous type : sdp
Paramètres exigés : aucun.
Paramètres facultatifs : aucun.

Considérations de codage : les fichiers SDP sont principalement du texte en format UTF-8. L'attribut "a=charset:" peut être utilisé pour signaler la présence d'autres jeux de caractères dans certaines parties d'un fichier SDP (voir la Section 6 de la RFC 4566). Un contenu binaire arbitraire ne peut pas être directement représenté dans SDP.
Considérations de sécurité : voir la Section 7 de la RFC 4566
Considérations d'interopérabilité : voir la RFC 4566
Spécification publiée : voir la RFC 4566
Applications qui utilisent ce type de support : voix sur IP, téléconférences vidée, support de flux directs, messagerie instantanée, entre autres. Voir aussi la Section 3 de la RFC 4566.
Informations supplémentaires :
Numéros magiques : aucun.
Extensions de fichier : l'extension ".sdp" est couramment utilisée.
Code de type de fichier Macintosh : "sdp "
Adresse personnel & de messagerie à contacter pour plus d'informations :
Mark Handley <M.Handley@cs.ucl.ac.uk>
Colin Perkins <csp@csperkins.org>
Groupe de travail IETF MMUSIC <mmusic@ietf.org>
Usage prévu : COMMUN
Auteur/contrôleur des changements : auteurs de la RFC 4566 ; groupe de travail IETF MMUSIC sur délégation de l'IESG.

8.2 Enregistrement des paramètres

Il y a sept noms de champs qui peuvent être enregistrés par l'IANA. En utilisant la terminologie de forme Backus-Naur (BNF) de la spécification SDP, ce sont "media", "proto", "fmt", "att-field", "bwtype", "nettype", et "addrtype".

8.2.1 Type de support ("media")

Le jeu de types de supports est destiné à être petit et NE DEVRAIT PAS être étendu sauf dans de rares circonstances. Les mêmes règles devraient s'appliquer pour les noms de supports que pour les types de contenu de support de niveau supérieur, et lorsque possible le même nom que pour MIME devrait être enregistré pour SDP. Pour les supports autres que les types de contenu de support de niveau supérieur existants, une RFC sur la voie de la normalisation DOIT être produite pour enregistrer un nouveau type de contenu de niveau supérieur, et l'enregistrement DOIT fournir une bonne justification de la raison pour laquelle aucun nom de support existant n'est approprié (politique "Action de normalisation" de la [RFC2434].

Le présent mémoire enregistre les types de supports "audio", "video", "text", "application", et "message".

Note : les types de supports "control" et "data" étaient mentionnés comme valides dans la précédente version de cette spécification [RFC2327] ; cependant, leur sémantique n'a jamais été spécifiée pleinement et ils ne sont pas largement utilisés. Ces types de supports ont été retirés de cette spécification, bien qu'ils restent toujours des capacités valides de type de support pour un agent d'utilisateur SIP comme défini dans la [RFC3840]. Si ces types de supports sont considérés comme utiles à l'avenir, une RFC sur la voie de la normalisation DOIT être produite pour documenter leur usage. Jusqu'à ce moment, les applications NE DEVRAIENT PAS utiliser ces types et NE DEVRAIENT PAS déclarer leur prise en charge dans les déclarations de capacités SDP (même si ils existent dans le registre créé par la RFC 3840).

8.2.2 Protocoles de transport ("proto")

Le champ "proto" décrit le protocole de transport utilisé. Il DEVRAIT faire référence à une RFC de protocole sur la voie de la normalisation. Le présent mémoire enregistre trois valeurs : "RTP/AVP" est une référence à RTP [RFC3550] utilisé sous le profil RTP pour les conférences audio et vidéo avec contrôle minimal [RFC3551] fonctionnant sur UDP/IP, "RTP/SAVP" est une référence au protocole sûr de transport en temps réel [RFC3711], et "udp" indique un protocole non spécifié sur UDP. Si d'autres profils RTP sont définis à l'avenir, leur nom "proto" DEVRAIT être spécifié de la même manière. Par exemple, un profil RTP dont le nom abrégé est "XYZ" devrait être noté par un champ "proto" de "RTP/XYZ".

Les nouveaux protocoles de transport DEVRAIENT être enregistrés par l'IANA. Les enregistrements DOIVENT faire référence à une RFC décrivant le protocole. Une telle RFC PEUT être expérimentale ou pour information, bien qu'il soit préférable qu'elle soit sur la voie de la normalisation. Les enregistrements DOIVENT aussi définir les règles de gestion de leur espace de nom "fmt" (voir ci-dessous).

8.2.3 Formats de supports ("fmt")

Chaque protocole de transport, défini par le champ "proto", a un espace de noms "fmt" associé qui décrit les formats de supports qui peuvent être convoyés par ce protocole. Les formats couvrent tous les codages possibles qui pourraient vouloir être transportés dans une session multimédia.
Les formats de charge utile RTP sous les profils "RTP/AVP" et "RTP/SAVP" DOIVENT utiliser le numéro de type de charge utile comme valeur de "fmt". Si le numéro de type de charge utile est alloué de façon dynamique par cette description de session, un attribut "rtpmap" supplémentaire DOIT être inclus pour spécifier le nom du format et les paramètres comme définis par l'enregistrement de type de support pour le format de charge utile. Il est RECOMMANDÉ que les autres profils RTP enregistrés (en combinaison avec RTP) comme protocoles de transport SDP spécifient les mêmes règles pour l'espace de noms "fmt".
Pour le protocole "udp", les nouveaux formats DEVRAIENT être enregistrés. L'utilisation d'un sous type de support existant pour le format est encouragé. Si aucun sous type de support n'existe, il est RECOMMANDÉ qu'il en soit enregistré un convenable selon le processus de l'IETF [RFC4288] par la production, ou la référence, d'une RFC sur la voie de la normalisation qui définisse le protocole de transport pour le format. Pour les autres protocoles, les formats PEUVENT être enregistrés selon les règles de la spécification "proto" associée. Les enregistrement de nouveaux formats DOIVENT spécifier à quels protocoles de transport ils s'appliquent.

8.2.4 Noms d'attributs ("att-field")

Les noms des champs d'attributs ("att-field") DOIVENT être enregistrés par l'IANA et documentés, à cause de problèmes notables dus à des conflits d'attributs portant le même nom. Les attributs inconnus dans SDP sont simplement ignorés, mais ceux en conflit qui fragmentent le protocole sont un problème sérieux.

Les enregistrements de nouveaux attributs sont acceptés selon la politique "Spécification exigée" de la RFC 2434, pourvu que la spécification inclue les informations suivantes :
o nom de contact, adresse de messagerie, et numéro de téléphone
o nom d'attribut (comme il va apparaître dans SDP)
o nom d'attribut en forme longue en anglais
o type de l'attribut (niveau session, niveau support, ou les deux)
o si la valeur de l'attribut est soumise à l'attribut charset
o une explication d'un paragraphe sur l'objet de l'attribut
o une spécification des valeurs appropriées de l'attribut
Ceci est le minimum que l'IANA va accepter. Les attributs sont supposés avoir une large utilisation et l'interopérabilité DEVRAIT être documentée avec une RFC sur la voie de la normalisation qui spécifie plus précisément l'attribut.

Ceux qui soumettent des enregistrements devraient s'assurer que la spécification est dans l'esprit des attributs SDP, en particulier que l'attribut est indépendant de la plate-forme au sens où il ne fait pas d'hypothèse implicite sur les systèmes d'exploitation et ne désigne pas des parties spécifiques de logiciel d'une manière qui puisse gêner l'interopérabilité.

L'IANA a enregistré l'ensemble initial suivant de noms d' attributs (valeurs du champ "att-field") dont les définitions sont à la Section 6 du présent mémoire (ces définitions mettent à jour celles de la RFC 2327):

Nom	Niveau session ou support	Dépendance au jeu de caractères
cat	Session	Non
keywds	Session	Oui
tool	Session	Non
ptime	Support	Non
maxptime	Support	Non
rtpmap	Support	Non
recvonly	l'un et l'autre	Non
sendrecv	l'un et l'autre	Non
sendonly	l'un et l'autre	Non
inactive	l'un et l'autre	Non
orient	Support	Non
type	Session	Non
charset	Session	Non
sdplang	l'un et l'autre	Non
lang	l'un et l'autre	Non
framerate	Support	Non
quality	Support	Non
fmtp	Support	Non

8.2.5 Spécificateurs de bande passante ("bwtype")

La prolifération des spécificateurs de bande passante est fortement déconseillée.

Les nouveaux spécificateurs de bande passante (champs "bwtype") DOIVENT être enregistrés par l'IANA. La soumission DOIT faire référence à une RFC sur la voie de la normalisation spécifiant précisément la sémantique du spécificateur de bande passante, et indiquant quand il devrait être utilisé, et pourquoi les spécificateurs de bande passante enregistrés existants ne suffisent pas.

L'IANA a enregistré les spécificateurs de bande passante"CT" et "AS" dont les définitions sont au paragraphe 5.8 du présent mémoire (ces définitions mettent à jour celles de la RFC 2327).

8.2.6 Types de réseau ("nettype")

De nouveaux types de réseau (champ "nettype") peuvent être enregistrés par l'IANA si SDP doit être utilisé dans un contexte d'environnements non Internet. Bien que ce ne soit normalement pas la chasse gardée de l'IANA, il peut y avoir des circonstances où une application Internet doit inter opérer avec une application non Internet, comme quand il s'agit de faire une passerelle entre un appel téléphonique Internet et le réseau téléphonique public commuté (RTPC). Le nombre de types de réseaux devrait être petit et rarement étendu. Un nouveau type de réseau ne peut être enregistré sans l'enregistrement d'au moins un type d'adresse à utiliser sur 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 vont être utilisés.

L'IANA a enregistré le type de réseau "IN" pour représenter l'Internet, avec la définition des paragraphes 5.2 et 5.7 du présent mémoire (ces définitions mettent à jour celles de la RFC 2327).

8.2.7 Types d'adresse ("addrtype")

De nouveaux types d'adresses ("addrtype") peuvent être enregistrés par l'IANA. Un type d'adresse n'a de signification 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 l'enregistrement d'un type de réseau. Un enregistrement de nouveau type d'adresse DOIT faire référence à une RFC qui donne les détails de la syntaxe du type d'adresse. Les types d'adresses ne sont pas supposés être enregistrés fréquemment.

L'IANA a enregistré les types d'adresses "IP4" et "IP6" dont les définitions sont aux paragraphes 5.2 et 5.7 du présent mémoire (ces définitions mettent à jour celles de la RFC 2327).

8.2.8 Procédure d'enregistrement

Dans la RFC de documentation qui enregistre les champs SDP "media", "proto", "fmt", "bwtype", "nettype", et "addrtype", les auteurs DOIVENT inclure les informations suivantes pour que l' IANA les place dans le registre approprié :
o nom de contact, adresse de messagerie, et numéro de téléphone
o nom enregistre (comme il va apparaître dans SDP)
o nom en forme longue en anglais
o type de nom ("media", "proto", "fmt", "bwtype", "nettype", ou "addrtype")
o une explication d'un paragraphe sur l'objet du nom enregistré
o une référence à la spécification du nom enregistré (ce sera normalement un numéro de RFC).

L'IANA peut renvoyer toute demande d'enregistrement à l'IESG pour révision, et peut demander que les révisions soient faites avant que l'enregistrement soit effectué.

8.3 Méthodes d'accès aux clés de chiffrement

L'IANA tenait précédemment un tableau des noms de méthodes d'accès aux clés de chiffrement SDP ("enckey"). Ce tableau est obsolète, car la ligne "k=" n'est pas extensible. De nouveaux enregistrements NE DOIVENT PAS être acceptés.

9. Grammaire de SDP

Cette Section donne la grammaire en BNF augmenté pour SDP. L'ABNF est défini dans la [RFC4234].

```
; Syntaxe de SDP
session-description = 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 =  %x76 "=" 1*CHIFFRE CRLF                    ; ce mémoire décrit la version 0

origin-field =  %x6f "=" username SP sess-id SP sess-version SP nettype SP addrtype SP unicast-address CRLF

session-name-field = %x73 "=" texte CRLF

information-field = [%x69 "=" texte CRLF]

uri-field = [%x75 "=" uri CRLF]

email-fields = *(%x65 "=" adresse de messagerie électronique CRLF)

phone-fields = *(%x70 "=" numéro de téléphone CRLF)

connection-field =  [%x63 "=" nettype SP addrtype SP connection-address CRLF]
; un champ “connection” doit être présent dans chaque description de support ou au niveau session.

bandwidth-fields = *(%x62 "=" bwtype ":" bande passante CRLF)

time-fields = 1*( %x74 "=" start-time SP stop-time *(CRLF repeat-fields) CRLF) [ajustements de zone CRLF]

repeat-fields = %x72 "=" repeat-interval SP typed-time 1*(SP typed-time)

ajustements de zone = %x7a "=" time SP ["-"] typed-time *(SP time SP ["-"] typed-time)

key-field =  [%x6b "=" key-type CRLF]

attribute-fields = *(%x61 "=" attribut CRLF)

media-descriptions = *( media-field
                        information-field
                        *connection-field
                        bandwidth-fields
                        key-field
                        attribute-fields )

media-field = %x6d "=" media SP accès ["/" entir] SP proto 1*(SP fmt) CRLF

; sous-règles de 'o='
username = chaîne sans espace                               ; définition très large, mais n'inclut pas d'espace

sess-id = 1*CHIFFRE                                         ; devrait être unique pour ce nom d'utilisateur/hôte

sess-version = 1*CHIFFRE

nettype = jeton                                 ; normalement "IN"

addrtype = jeton                                ; normalement "IP4" ou "IP6"
```

```
; sous règles de 'u='
uri =  référence d'URI                          ; voir la RFC 3986

; sous règles de 'e='                           ; voir les définitions dans la RFC 2822.
email-address = adresse et commentaires / dispname-and-address / addr-spec
adresse et commentaires  = addr-spec 1*SP "(" 1*email-safe ")"
dispname-and-address = 1*email-safe 1*SP "<" addr-spec ">"

; sous règles de 'p='
numéro de téléphone =  téléphone *SP "(" 1*email-safe ")" / 1*email-safe "<" téléphone ">" /téléphone

téléphone = ["+"] CHIFFRE 1*(SP / "-" / CHIFFRE)

; sous règles de 'c='
connection-address = multicast-address / unicast-address

; sous règles de 'b='
bwtype = jeton

bandwidth =  1*CHIFFRE

; sous règles de 't='
start-time = heure / "0"

stop-time =  heure / "0"

heure = POS-CHIFFRE 9*DCHIFFRE
; représentation décimale de l'heure NTP en secondes depuis 1900. La représentation de l'heure NTP est un champ de
longueur non limitée contenant au moins 10 chiffres. À la différence de la représentation sur 64 bits utilisée ailleurs, l'heure
dans SDP ne revient pas à zéro en 2036.

; sous règles de 'r=' et 'z='
repeat-interval = POS-CHIFFRE *CHIFFRE [fixed-len-time-unit]

typed-time = 1* CHIFFRE [unité de temps de longueur fixe]

unité de temps de longueur fixe = %x64 / %x68 / %x6d / %x73

; sous règles de 'k='
key-type = %x70 %x72 %x6f %x6d %x70 %x74 /          ; "prompt"
           %x63 %x6c %x65 %x61 %x72 ":" text /      ; "clear:"
           %x62 %x61 %x73 %x65 "64:" base64 /       ; "base64:"
           %x75 %x72 %x69 ":" uri                   ; "uri:"

base64  =  *base64-unit [base64-pad]
base64-unit = 4base64-char
base64-pad = 2base64-char "==" / 3base64-char "="
base64-char = ALPHA / CHIFFRE / "+" / "/"

; sous règles de 'a='
attribute =  (att-field ":" att-value) / att-field

att-field = jeton

att-value = chaîne d'octets

; sous règles de 'm='
media = jeton                   ; normalement "audio", "video", "text", ou application"

fmt = jeton                     ; normalement un type de charge utile RTP pour les supports audio et vidéo

proto  =  jeton *("/" jeton)    ; normalement "RTP/AVP" ou "udp"
```

```
accès =  1*CHIFFRE

; sous règles génériques : adressage
adresse d'envoi individuel = adresse IP4 / adresse IP6 / FQDN / extn-addr

adresse de diffusion groupée = IP4-multicast / IP6-multicast / FQDN / extn-addr

IP4-multicast =  m1 3( "." decimal-uchar ) "/" ttl [ "/" entier ]
; les adresses de diffusion groupée IPv4 peuvent être dans la gamme 224.0.0.0 à 239.255.255.255

m1 = ("22" ("4"/"5"/"6"/"7"/"8"/"9")) / ("23" CHIFFRE )

IP6-multicast = hexpart [ "/" entier ]            ; adresse IPv6 commençant par FF

ttl = (POS- CHIFFRE *2CHIFFRE ) / "0"

FQDN = 4*(alpha-numérique / "-" / ".")
; nom de domaine pleinement qualifié comme spécifié dans la RFC 1035 (et ses mise à jour)

adresse IP4 =  b1 3("." decimal-uchar)

b1 = decimal-uchar                                ; moins que "224"

; Ce qui suit est cohérent avec la [RFC2373], Appendice B.
IP6-multicast = IP6-address [ "/" entier ]

IP6-address =  6( h16 ":" ) ls32
                        /                    "::" 5( h16 ":" ) ls32
                        / [              h16 ] "::" 4( h16 ":" ) ls32
                        / [ *1( h16 ":" ) h16 ] "::" 3( h16 ":" ) ls32
                        / [ *2( h16 ":" ) h16 ] "::" 2( h16 ":" ) ls32
                        / [ *3( h16 ":" ) h16 ] "::"    h16 ":"   ls32
                        / [ *4( h16 ":" ) h16 ] "::"              ls32
                        / [ *5( h16 ":" ) h16 ] "::"              h16
                        / [ *6( h16 ":" ) h16 ] "::"

h16 =  1*4HEXDIG

ls32 = ( h16 ":" h16 ) / IP4-address

; Éléments génériques pour les autres familles d'adresses
extn-addr = chaîne sans espace

; sous règles génériques : datatypes
texte = chaîne d'octets
; par défaut est à interpréter comme texte UTF8. ISO 8859-1 exige d'utiliser l'attribut de niveau session "a=charset:ISO-
8859-1".

chaîne d'octets = 1*(%x01-09/%x0B-0C/%x0E-FF)      ; tout octet sauf NUL, CR, ou LF.

chaîne sans espace = 1*(VCHAR/%x80-FF)            ; chaîne de caractères visibles.

token-char = %x21 / %x23-27 / %x2A-2B / %x2D-2E / %x30-39 / %x41-5A / %x5E-7E

jeton = 1*(token-char)

email-safe = %x01-09/%x0B-0C/%x0E-27/%x2A-3B/%x3D/%x3F-FF
; tout octet sauf NUL, CR, LF, ou les caractères de citation ()<>

entier = POS-CHIFFRE * CHIFFRE

; sous règles génériques : primitives
```

alpha-numeric = ALPHA / CHIFFRE

POS-CHIFFRE = %x31-39 ; 1 - 9

decimal-uchar = CHIFFRE / POS- CHIFFRE CHIFFRE / ("1" 2(CHIFFRE)) / ("2" ("0"/"1"/"2"/"3"/"4") CHIFFRE) / ("2" "5" ("0"/"1"/"2"/"3"/"4"/"5"))

; références externes : ; ALPHA, CHIFFRE, CRLF, SP, VCHAR : de la RFC 4234
; URI-reference : de la RFC 3986
; addr-spec : de la RFC 2822

10. Résumé des changements par rapport à la RFC 2327

Le présent mémoire a été significativement restructuré, incorporant un grand nombre d'éclaircissements à la spécification à la lumière de l'usage. À l'exception des éléments notés ci-dessous, les changements du mémoire sont destinés à être des éclaircissements rétro compatibles. Cependant, du fait d'incohérences et de définitions non claires dans la RFC 2327, il est probable que certaines mises en œuvre aient interprété cette RFC d'une manière différente de cette version de SDP.

La grammaire ABNF de la Section 9 a été largement révisée et mise à jour, corrigeant un certain nombre de fautes et incorporant les extensions IPv6 de la RFC 3266. Les incohérences connues entre la grammaire et le texte de la spécification ont été résolues.

Un enregistrement de type de support pour SDP est inclus. Les exigences pour l'enregistrement des attributs et autres paramètres par l'IANA ont été précisées et resserrées (Section 8). Il est noté que "text" et "message" sont des types de supports valides pour l'usage avec SDP, mais que "control" et "data" sont sous spécifiés et déconseillés.

Les termes de la RFC 2119 sont maintenant utilisés dans tout le document pour spécifier les niveaux d'exigences. Certaines de ces exigences, en particulier en relation avec l'enregistrement de paramètres, sont plus strictes que dans la RFC 2327.

Le profil RTP "RTP/SAVP" et son espace de noms "fmt" sont enregistrés.

Les attributs "a=inactive" et "a=maxptime" ont été ajoutés.

La RFC 2327 rendait obligatoire que soit "e=", soit "p=" soit exigé. Les deux sont maintenant facultatifs, pour refléter l'usage actuel.

Les limitations significatives du champ "k=" sont notées, et son utilisation est déconseillée.

La plupart des utilisations de la notation de préfixe "x-" pour des paramètres expérimentaux sont interdites et les autres utilisations sont déconseillées.

11. Remerciements

De nombreuses personnes du groupe de travail de l'IETF Commande de session multi parties multimédia (MMUSIC) ont fait des commentaires et suggestions qui ont contribué au présent document. En particulier, nous tenons à remercier Eve Schooler, Steve Casner, Bill Fenner, Allison Mankin, Ross Finlayson, Peter Parnes, Joerg Ott, Carsten Bormann, Steve Hanna, Jonathan Lennox, Keith Drage, Sean Olson, Bernie Hoeneisen, Jonathan Rosenberg, John Elwell, Flemming Andreasen, Jon Peterson, et Spencer Dawkins.

12. Références

12.1 Références normatives

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936, 8020, 8482, 8767)

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2673, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604, 7766, 8482, 8767)

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

[RFC2327] M. Handley et V. Jacobson, "SDP : Protocole de description de session", avril 1998. *(Obsolète; voir* RFC4566)

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

[RFC3066] H. Alvestrand, "Étiquettes pour l'identification des langues", BCP 47, janvier 2001. *(Obsolète, voir la* RFC4646.)

[RFC3266] S. Olson, G. Camarillo, A. B. Roach, "Prise en charge de IPv6 dans le protocole de description de session (SDP)", juin 2002. (*Obsolète, voir* RFC4566) *(P.S.)*

[RFC3490] P. Faltstrom et autres, "Internationalisation des noms de domaine dans les applications (IDNA)", mars 2003. (*Remplacée par les* RFC5890 et 5891, *P.S.*)

[RFC3548] S. Josefsson, "Codages de données Base16, Base32, et Base64", juillet 2003. *(Obsolète, voir* 4648) *(Info)*

[RFC3629] F. Yergeau, "UTF-8, un format de transformation de la norme ISO 10646", STD 63, novembre 2003.

[RFC3986] T. Berners-Lee, R. Fielding et L. Masinter, "Identifiant de ressource uniforme (URI) : Syntaxe générique", STD 66, janvier 2005. *(P.S. ; MàJ par* RFC8820)

[RFC4234] D. Crocker et P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", octobre 2005. *(Remplace* RFC2234, *remplacée par* RFC5234)

12.2 Références pour information

[H.332] Recommandation UIT-T H.332, "H.323 étendu pour conférences à couplage lâche", Union Internationale des Télécommunication, septembre 1998.

[RFC1305] D. Mills, "Protocole de l'heure du réseau, version 3, spécification, mise en œuvre et analyse", STD 12, mars 1992. *(Remplacée par* RFC5905)

[RFC2326] H. Schulzrinne, A. Rao et R. Lanphier, "Protocole de flux directs en temps réel (RTSP)", avril 1998. *(Remplacée par* RFC7826)

[RFC2373] R. Hinden, S. Deering, "Architecture d'adressage IP version 6", juillet 1998. (*Obsolète, voir* RFC4291) *(PS)*

[RFC2822] P. Resnick, "Format de message Internet", avril 2001. *(Remplace la* RFC0822, STD 11, *Remplacée par* RFC5322)

[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)

[RFC3264] J. Rosenberg et H. Schulzrinne, "Modèle d'offre/réponse avec le protocole de description de session (SDP)", juin 2002. *(P.S. ; MàJ par* RFC8843)

[RFC3388] G. Camarillo, G. Eriksson, J. Holler et H. Schulzrinne, "Groupage des lignes de support dans le protocole de description de session (SDP)", décembre 2002. *(Remplacée par* RFC5888)

[RFC3550] H. Schulzrinne, S. Casner, R. Frederick et V. Jacobson, "RTP : un protocole de transport pour les applications en temps réel", STD 64, juillet 2003. *(MàJ par* RFC7164, RFC7160, RFC8083, RFC8108, RFC8860)

[RFC3551] H. Schulzrinne et S. Casner, "Profil RTP pour conférences audio et vidéo avec contrôle minimal", STD 65, juillet 2003. *(MàJ par* RFC8860)

[RFC3556] S. Casner, "Modificateurs de bande passante du protocole de description de session (SDP) pour la bande passante du protocole de contrôle de RTP (RTCP)", juillet 2003. *(P.S.)*

[RFC3605] C. Huitema, "Attribut du protocole de contrôle en temps réel (RTCP) dans le protocole de description de session (SDP)", octobre 2003. *(P.S.)*

[RFC3711] M. Baugher et autres, "Protocole de transport sécurisé en temps réel (SRTP)", mars 2004. *(P.S.)*

[RFC3840] J. Rosenberg, H. Schulzrinne et P. Kyzivat, "Indication des capacités d'agent d'utilisateur dans le protocole d'initialisation de session (SIP)", août 2004

[RFC3890] M. Westerlund, "Modificateur de bande passante indépendant du transport pour le protocole de description de session (SDP)", septembre 2004. *(P.S.)*

[RFC4288] N. Freed et J. Klensin, "Spécifications du type de support et procédures d'enregistrement", BCP 13, décembre 2005.

[RFC4567] J. Arkko et autres, "Extensions de gestion de clés pour le protocole de description de session (SDP) et le protocole d'écoulement en temps réel (RTSP)", juillet 2006. *(P.S.)*

[RFC4568] F. Andreasen et autres, "Définition d'attributs de sécurité dans le protocole de description de session (SDP) pour les flux de support", juillet 2006. *(P.S.)*

Adresse des auteurs

Mark Handley
University College London
Department of Computer Science
Gower Street
London WC1E 6BT
UK
mél : M.Handley@cs.ucl.ac.uk

Van Jacobson
Packet Design
2465 Latham Street
Mountain View, CA 94040
USA
mél : van@packetdesign.com

Colin Perkins
University of Glasgow
Department of Computing Science
17 Lilybank Gardens
Glasgow G12 8QQ
UK
mél : csp@csperkins.org

Déclaration complète de droits de reproduction

mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org.

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