

Équipe d'ingénierie de l'Internet (IETF)  
**Request for Comments : 8866**  
 RFC rendue obsolète : 4566  
 Catégorie : Sur la voie de la normalisation  
 ISSN: 2070-1721  
 Traduction Claude Brière de L'Isle

A. Begen, Networked Media  
 P. Kyzivat  
 C. Perkins, University of Glasgow  
 M. Handley, UCL  
 janvier 2021

## 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. Le présent document rend obsolète la RFC 4566.

### Statut de ce mémoire

Ceci est un document de l'Internet sur la voie de la normalisation.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Plus d'informations sur les normes de l'Internet sont disponibles à la Section 2 de la RFC7841.

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à <http://www.rfc-editor.org/info/rfc8866>

### Notice de droits de reproduction

Copyright (c) 2012 IETF Trust et les personnes identifiées comme auteurs du document. Tous droits réservés.

Le présent document est soumis au BCP 78 et aux dispositions légales de l'IETF Trust qui se rapportent aux documents de l'IETF (<http://trustee.ietf.org/license-info>) en vigueur à la date de publication de ce document. Prière de revoir ces documents avec attention, car ils décrivent vos droits et obligations par rapport à ce document. Les composants de code extraits du présent document doivent inclure le texte de licence simplifié de BSD comme décrit au paragraphe 4.e des dispositions légales du Trust et sont fournis sans garantie comme décrit dans la licence de BSD simplifiée.

Le présent document peut contenir des matériaux provenant de documents de l'IETF ou de contributions à l'IETF publiées ou rendues disponibles au public avant le 10 novembre 2008. La ou les personnes qui ont le contrôle des droits de reproduction sur tout ou partie de ces matériaux peuvent n'avoir pas accordé à l'IETF Trust le droit de permettre des modifications de ces matériaux en dehors du processus de normalisation de l'IETF. Sans l'obtention d'une licence adéquate de la part de la ou des personnes qui ont le contrôle des droits de reproduction de ces matériaux, le présent document ne peut pas être modifié en dehors du processus de normalisation de l'IETF, et des travaux dérivés ne peuvent pas être créés en dehors du processus de normalisation de l'IETF, excepté pour le formater en vue de sa publication comme RFC ou pour le traduire dans une autre langue que l'anglais.

## Table des matières

1. Introduction.....	2
2. Glossaire des termes.....	3
3. Exemples d'utilisation de SDP.....	3
3.1 Initialisation de session .....	3
3.2 Support en direct.....	3
3.3 Messagerie électronique et Toile mondiale.....	3
3.4 Annonce de session en diffusion groupée.....	4
4. Exigences et recommandations.....	4
4.1 Informations de support et de transport.....	4
4.2 Informations d'horaire.....	5
4.3 Obtenir plus d'informations sur une session.....	5
4.4 Internationalisation.....	5
5. Spécification de SDP.....	5

5.1	Version du protocole ("v=")	7
5.2	Origine ("o=")	7
5.3	Nom de session ("s=")	8
5.4	Informations de session ("i=")	8
5.5	URI ("u=")	9
5.6	Adresse de messagerie électronique et numéro de téléphone ("e=" et "p=")	9
5.7	Données de connexion ("c=")	9
5.8	Informations de bande passante ("b=")	11
5.9	Heure d'activité ("t=")	11
5.10	Heures de répétition ("r=")	12
5.11	Ajustement de zone horaire ("z=")	12
5.12	Clés de chiffrement ("k=")	13
5.13	Attributs ("a=")	13
5.14	Descriptions de supports ("m=")	14
6.	Attributs SDP	16
6.1	cat (catégorie)	16
6.2	keywds (mots clés)	16
6.3	tool (outil)	16
6.4	ptime (heure de paquet)	17
6.5	maxptime (durée maximum du paquet)	17
6.6	rtpmap (transposition RTP)	17
6.7	Attributs de direction du support	18
6.8	orient (orientation)	20
6.9	type (type de conférence)	20
6.10	charset (jeu de caractères)	21
6.11	sdplang (langage SDP)	21
6.12	lang (langage)	22
6.13	framerate (taux de trame)	22
6.14	quality (qualité)	22
6.15	fntp (paramètres de format)	23
7.	Considérations sur la sécurité	23
8.	Considérations relatives à l'IANA	24
8.1	Type de support "application/sdp"	24
8.2	Enregistrement des paramètres SDP auprès de l'IANA	25
8.3	Méthodes d'accès aux clés de chiffrement (Obsolète)	29
9.	Grammaire de SDP	29
10.	Résumé des changements par rapport à la RFC 4566	33
11.	Références	34
11.1	Références normatives	34
11.2	Références pour information	35
	Remerciements	37
	Adresses des auteurs	37

## 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 (SAP, *Session Announcement Protocol*) [RFC2974], le protocole d'initialisation de session (SIP, *Session Initiation Protocol*) [RFC3261], le protocole de flux directs en temps réel (RTSP, *Real-Time Streaming Protocol*) [RFC7826], la messagerie électronique avec extensions MIME [RFC5322], et le protocole de transport Hypertext (HTTP, *Hypertext Transport Protocol*) [RFC7230].

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 obsolète la [RFC4566]. 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 de son contexte.

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

Description de support : une description de support contient les informations nécessaires à une partie pour établir une connexion de protocole réseau de niveau application avec l'autre partie. Elle commence par une ligne "m=" et se termine par la prochaine ligne "m=" ou par la fin de la description de session.

Section de niveau session : cela se réfère aux parties qui ne sont pas des descriptions de supports, tandis que la description de session se réfère au corps entier qui inclut la section de niveau session et la ou les descriptions de supports.

Les termes "conférence multimédia" et "session multimédia" sont utilisés dans ce document comme défini dans la [RFC7656]. Les termes "session" et "session multimédia" sont utilisés de façon interchangeable dans ce document.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119], [RFC8174] quand, et seulement quand ils apparaissent tout en majuscules, comme montré ci-dessus.

## 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 [RFC6838]. 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*) [RFC7826], 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 descriptions de sessions en diffusion groupée faites seulement via la messagerie électronique ou le WWW n'ont pas la propriété que le receveur d'une description 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 convoier 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 avec les protocoles Internet, 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 convoier 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 passante qui va être utilisée par la session
- o informations de contact pour la personne responsable de la session

En général, SDP doit convoier 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 l'adresse et de l'accès dépend du contexte. Normalement, ce DEVRAIT être l'adresse et l'accès distants auxquels ces données sont envoyées ou reçues. Les détails peuvent différer sur la base du type de réseau, du type d'adresse, du protocole, et du support spécifiés, et de si SDP est distribué comme une annonce ou négocié dans un échange offre/réponse [RFC3264]. (Par exemple, certains types d'adresses ou de protocoles peuvent ne pas avoir une notion d'accès.) S'écarter de ce comportement normal ne devrait être fait qu'avec prudence 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 envoyer :

- 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 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*) [RFC3986] pour donner plus d'informations sur la session. (Noter que l'utilisation d'URI pour indiquer des ressources distantes fait l'objet de considérations sur la sécurité dans la [RFC3986].)

#### 4.4 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 SDP est notée par le type de support "application/sdp" (voir la Section 8).

Une description de session SDP est entièrement textuelle. Les noms de champs et attributs SDP utilisent seulement le sous ensemble US-ASCII de l'UTF-8 [RFC3629], mais les champs textuels et les valeurs d'attribut PEUVENT utiliser le jeu de caractères ISO 10646 complet en codage UTF-8, ou un autre jeu de caractères défini par l'attribut "a=charset:" (paragraphe 6.10). Les valeurs de champs et d'attribut qui utilisent le 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 endommagées par un serveur de mise en antémémoire 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 peut être facilement détectée et éliminée.

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

où <type> est 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 de séparation NE DOIVENT PAS être utilisées d'un côté ou de l'autre du signe "=", cependant, la valeur peut contenir une espace blanche en tête au titre de sa syntaxe, c'est-à-dire, cette espace blanche fait partie de la valeur.

Une description SDP DOIT se conformer à la syntaxe définie à la Section 9. Ce qui suit est une vue générale de la syntaxe.

Une description SDP consiste en une section de niveau session suivie par zéro, une ou plusieurs descriptions de supports. La section de niveau session commence par une ligne "v=" et continue jusqu'à la première description de supports (ou la fin de la description complète, selon ce qui vient en premier). Chaque description de supports commence par une ligne "m=" et se continue jusqu'à la prochaine description de support ou la fin de la description de session complète, selon ce qui vient en premier. 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 lorsque présentes, elles doivent apparaître exactement dans l'ordre donné ici (l'ordre fixe améliore grandement la détection d'erreur et permet un analyseur simple). Dans la présentation qui suit, les éléments facultatifs sont marqués avec 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 "z=" ; voir ci-dessous)

- k=\* (obsolète)
- 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)
- z=\* (ligne facultative d'ajustement de zone horaire)

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=\* (obsolète)
- a=\* (zéro, une ou plusieurs lignes d'attributs du support)

Un analyseur SDP DOIT ignorer tout attribut qu'il ne comprend pas.

L'ensemble de lettres de type est délibérément petit et n'est pas destiné à être extensible -- un analyseur SDP DOIT complètement ignorer ou rejeter toute description de session qui contient une lettre de type qu'il ne comprend pas. Le mécanisme d'attribut ("a=" décrit au paragraphe 5.13) est le principal moyen pour étendre SDP et l'adapter à des applications ou supports particuliers. Certains attributs (ceux mentionnés à la Section 6) ont une signification définie, mais d'autres peuvent être ajoutés sur la base d'un support ou session spécifique. (Des portées d'attribut en plus des portées spécifiques du support et de la session peuvent aussi être définies dans des extensions à ce document, par exemple, la [RFC5576] et la [RFC8864].) 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=") dans la section de niveau session s'appliquent à toutes les descriptions de supports de cette session sauf outrepassées par les informations de connexion dans la description de support. Par exemple, dans l'exemple ci-dessous, chaque description de support audio se comporte comme si elle avait reçu un "c=IN IP4 198.51.100.1".

Un exemple de description SDP est :

```
v=0
o=jdoe 3724394400 3724394405 IN IP4 198.51.100.1
s=Appel à John Smith
i=Offre SDP n° 1
u=http://www.jdoe.example.com/home.html
e=Jane Doe <jane@jdoe.example.com>
p=+1 617 555-6011
c=IN IP4 198.51.100.1
t=0 0
m=audio 49170 RTP/AVP 0
m=audio 49180 RTP/AVP 0
m=video 51372 RTP/AVP 99
c=IN IP6 2001:db8::2
a=rtpmap:99 h263-1998/90000
```

Les champs de texte comme le champ de nom de session et le champ informations sont des chaînes d'octets qui peuvent contenir tout octet à l'exception de 0x00 (Nul), 0x0a (nouvelle ligne ASCII), et 0x0d (retour chariot ASCII). La séquence CRLF (0x0d0a) est utilisée pour terminer une ligne, mais les analyseurs DEVRAIENT être tolérants et aussi accepter les lignes terminées 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. Quand l'attribut "a=charset" est présent, le champ nom de session, le champ informations, et certains champs d'attributs sont interprétés conformément au jeu de caractères choisi.

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] et [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 [RFC5890] et NE DOIVENT PAS être directement représentés en UTF-8 ou tout autre codage (cette exigence est pour la compatibilité avec la [RFC2327] et les autres normes antérieures relatives à SDP, qui précèdent le développement des noms de domaines internationalisés).

## 5.1 Version du protocole ("v=")

```
v=0
```

La ligne "v=" (champ version) 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 mineure.

## 5.2 Origine ("o=")

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

La ligne "o=" (champ origine) 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 tuple <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 un horodatage, en secondes depuis le 1er janvier 1900 UTC est recommandé pour assurer l'unicité.

<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 à la description de session. Ici comme avec <identifiant de session> il est RECOMMANDÉ qu'un horodatage 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 une 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 d'une adresse IPv4 de la machine. Pour un type d'adresse de IP6, c'est soit un nom de domaine pleinement qualifié de la machine, soit l'adresse de la machine représentée comme spécifié à la Section 4 de la [RFC5952]. Pour IP4 et IP6, le nom de domaine pleinement qualifié est la forme qui DEVRAIT être donnée sauf si elle est indisponible, auquel cas une adresse unique au monde PEUT y être substituée.

En général, la ligne "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 la ligne "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>

La ligne "s=" (champ nom de session) est le nom de session textuel. Il DOIT y avoir une et une seule ligne "s=" par description de session. La ligne "s=" NE DOIT PAS être vide. Si une session n'a pas un nom significatif, la valeur "s=" ou "s=-" (c'est-à-dire, une seule espace ou un tiret comme nom de session) est RECOMMANDÉ. Si un attribut "a=charset:" de niveau session est présent, il spécifie le jeu de caractères utilisé dans le champ "s=". Si un attribut "a=charset:" de niveau session n'est pas présent, le champ "s=" DOIT contenir des caractères ISO 10646 en codage UTF-8.

### 5.4 Informations de session ("i=")

i=<informations de session>

La ligne "i=" (champ informations) donne des informations textuelles sur la session. Il ne peut y avoir qu'au plus une ligne "i=" de niveau session par description de session, et au plus une ligne "i=" dans chaque description de support. Sauf si une ligne "i=" de niveau support est fournie, la ligne "i=" de niveau session s'applique à cette description de support. Si l'attribut "a=charset" est présent, il spécifie le jeu de caractères utilisé dans la ligne "i=". Si l'attribut "a=charset" n'est pas présent, la ligne "i=" DOIT contenir des caractères ISO 10646 en codage UTF-8.

Au plus une ligne "i=" peut être utilisée pour chaque description de support. Dans les définitions de supports, les lignes "i=" sont principalement destinés à étiqueter les flux de supports. À ce titre, elles 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.

La ligne "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. Elle ne convient pas pour l'analyse par un automate.

## 5.5 URI ("u=")

u=<uri>

La ligne "u=" (champ uri) donne un identifiant de ressource universel (URI, *Uniform Resource Identifier*) [RFC3986]. L'URI devrait être un pointeur sur des informations supplémentaires lisibles par l'homme sur la session. Cette ligne est FACULTATIVE. 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>

La ligne "e=" (champ messagerie électronique) et la ligne "p=" (champ téléphone) spécifient les informations de contact pour la personne responsable de la session. Ce n'est pas nécessairement la même personne que celle qui a créé la description de session.

L'inclusion d'une adresse de messagerie électronique ou d'un numéro de téléphone est FACULTATIVE.

Si une adresse de messagerie électronique ou un numéro de téléphone est présent, il DOIT être spécifié avant la première description 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 [E164]) 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 [RFC5322] 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>

La ligne "c=" (champ connexion) contient les informations nécessaires pour établir une connexion réseau.

Une description de session DOIT contenir soit au moins une ligne "c=" dans chaque description de support, soit une seule ligne "c=" au niveau session. Elle PEUT contenir une seule ligne "c=" de niveau session et une ou des lignes "c=" supplémentaires de niveau support par description de support, et dans ce cas les valeurs de niveau 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 supplémentaires PEUVENT

être ajoutés après l'adresse de connexion selon la valeur du sous 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 (paragraphe 5.13). 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 "IP4" 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 de cette session 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 "IP6" n'utilise pas la portée par la TTL, et donc, la valeur de TTL NE DOIT PAS être présente pour la diffusion groupée "IP6". Il est prévu que la portée des adresses IPv6 sera utilisée pour limiter la portée des conférences multimédia.

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 233.252.0.1/127/3 déclarerait que les adresses 233.252.0.1, 233.252.0.2, et 233.252.0.3 sont à utiliser avec une TTL de 127. Ceci est sémantiquement identique à inclure plusieurs lignes "c=" dans une description de support :

```
c=IN IP4 233.252.0.1/127
c=IN IP4 233.252.0.2/127
c=IN IP4 233.252.0.3/127
```

De même, un exemple IPv6 pourrait être : c=IN IP6 ff00::db8:0:101/3

qui est sémantiquement équivalent à :

```
c=IN IP6 ff00::db8:0:101
c=IN IP6 ff00::db8:0:102
c=IN IP6 ff00::db8:0:103
```

(on se souvient que le champ TTL n'est pas présent dans la diffusion groupée "IP6").

Plusieurs adresses ou lignes "c=" NE PEUVENT être spécifiées sur la base du support QUE si elles fournissent des adresses de diffusion groupée pour des couches différentes dans un schéma de codage hiérarchique ou en couches. Plusieurs adresses ou lignes "c=" NE DOIVENT PAS être spécifiées au 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 Informations de bande passante ("b=")

b=<bwtype>:<bande passante>

La ligne "b=" (champ bande passante) FACULTATIVE note la bande passante proposée à utiliser par la description de session ou de 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 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"). De même, si la bande passante d'un bouquet de flux de supports [RFC8843] dans une ligne "m=" est différente de la valeur implicite provenant de la portée, une ligne "b=CT:" DEVRAIT être fournie au niveau support. Le principal objet de cela est de donner une idée approximative de si deux sessions (ou bouquet de flux de supports) ou plus peuvent coexister simultanément. Noter qu'une ligne "b=CT:" donne un chiffre de bande passante totale pour tous les supports à tous les points d'extrémité.

La catégorie Mux pour "b=CT:" est NORMAL. Ceci est expliqué dans la [RFC8859].

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, la ligne "b=AS:" donne la "bande passante de session" RTP comme défini au paragraphe 6.2 de la [RFC3550]. Noter que la ligne "b=AS:" donne un chiffre de bande passante pour un seul support et un seul point d'extrémité, bien qu'il puisse y avoir de nombreux points d'extrémité qui envoient simultanément.

La catégorie Mux pour "b=AS:" est SUM. Ceci est expliqué dans la [RFC8859].

La [RFC4566] définissait un préfixe "X-" pour les noms <bwtype>. C'était destiné aux seuls besoins expérimentaux. Par exemple : b=X-YZ:128

L'utilisation du préfixe "X-" N'EST PAS RECOMMANDÉE. À la place, de nouveaux noms de <bwtype> (sans préfixe "X-") DEVRAIENT être définis, et ensuite DOIVENT être enregistrés par l'IANA dans l'espace de noms standard. Les analyseurs SDP DOIVENT ignorer les champ de bande passante avec des noms de <bwtype> inconnus. Les noms de <bwtype> 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 (incluant la redondance de transport et de couche réseau, mais pas de la couche de liaison). 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 Heure d'activité ("t=")

t=<heure de début> <heure de fin>

Une ligne "t=" (champ heure) commence par une description de l'heure qui spécifie l'heure de début et l'heure de fin d'une session. Plusieurs descriptions d'heure PEUVENT être utilisées si une session est active à plusieurs heures espacées de façon irrégulière ; chaque description d'horaire supplémentaire spécifie des périodes de temps supplémentaires pendant lesquelles la session va être active. Si la session est active à des heures répétées régulières, une description de répétition, commençant par une ligne "r=" (voir au paragraphe 5.10) peut être incluse, suivie par un champ horaire, et dans ce cas le champ horaire spécifie les heures de début et de fin de la séquence de répétition entière.

L'exemple suivant spécifie deux intervalles d'activité :

```
t=3724394400 3724398000 ; Mon 8-Jan-2018 10:00-11:00 UTC
t=3724484400 3724488000 ; Tue 9-Jan-2018 11:00-12:00 UTC
```

Le premier et le second sous champs du champ d'horaire donnent les heures respectivement de début et de fin de la session. Ces valeurs sont la représentation en décimal des valeurs horaires en secondes depuis le 1er janvier 1900 UTC. Pour convertir

ces valeurs en heure UNIX, soustraire le décimal 2 208 988 800.

Certaines représentations de l'heure vont revenir à zéro vers l'an 2036. Parce que SDP utilise une représentation décimale de longueur arbitraire, il n'a pas ce problème. Les mises en œuvre de SDP doivent être prêtes à traiter ces plus grandes valeurs.

Si le <stop-time> est réglé à zéro, la session n'est alors pas limitée, mais elle ne deviendra active qu'après le <start-time>. Si le <start-time> 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 la session 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, quelle 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>

Une ligne "r=" (champ répétition) spécifie les heures de répétition pour une session. Si on a besoin d'exprimer des programmations complexes, plusieurs champs répétition peuvent être inclus. 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 la ligne "t=" correspondante va être la représentation 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. La ligne "t=" correspondante d'heure d'arrêt va être la représentation de la fin de la dernière session trois mois plus tard. Par défaut, tous les sous champs sont en secondes, de sorte que les lignes "r=" et "t=" pourraient être les suivantes :

```
t=3724394400 3730536000 ; Mon 8-Jan-2018 10:00-11:00 UTC ; Tues 20-Mar-2018 12:00 UTC
r=604800 3600 0 90000 ; une semaine, une heure, zéro, 25 heures
```

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)

### Tableau 1 : caractères de spécification d'unités de temps

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 Ajustement de zone horaire ("z=")

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

Une ligne "z=" (champ zone) est un modificateur facultatif des champs de répétition qu'elle suit immédiatement. Elle ne s'applique à aucune autre champ.

Pour programmer une session répétée 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 l'hiver et l'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'expéditeur de spécifier l'heure (représentée en secondes depuis le 1er janvier 1900 UTC) où un ajustement de zone horaire se produit et le décalage à partir de l'heure à laquelle la session a été programmée. La ligne "z=" permet à l'expéditeur 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 :

```
t=3724394400 3754123200      ; lundi 8 janvier 2018 10:00 UTC
                             ; mardi 18 décembre 2018 12:00 UTC
r=604800 3600 0 90000       ; 1 semaine, 1 heure, zéro, 25 heures
z=3730928400 -1h 3749680800 0 ; dimanche 25 mars 2018 1:00 UTC,
                             ; décalage 1 heure,
                             ; dimanche 28 octobre 2018 2:00 UTC,
                             ; pas de décalage
```

Cela spécifie qu'à l'heure 3730928400 (dimanche 25 mars 2018 1:00 UTC, le début de l'heure d'été britannique) l'heure de base sur laquelle les heures de répétition de la session sont calculées est reculée d'une heure, et qu'à l'instant 3749680800 (dimanche 28 octobre-2018 2:00 UTC, la fin de l'heure d'été britannique) 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.

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

## 5.12 Clés de chiffrement ("k=")

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

La ligne "k=" (champ clé) est obsolète et NE DOIT PAS être utilisée. Elle est incluse dans ce document pour des raisons historiques. On NE DOIT PAS inclure de ligne "k=" dans un SDP, et on DOIT l'éliminer si elle est reçue dans un SDP.

## 5.13 Attributs ("a=")

```
a=<nom d'attribut>
a=<nom d'attribut>:<valeur d'attribut>
```

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. (Des portées d'attribut en plus des portées de niveau support et des portées de niveau session peuvent aussi être définies dans des extensions à ce document, par exemple, [RFC5576] et [RFC8864].)

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

Les champs d'attribut peuvent être de deux formes :

- o Un attribut de propriété est simplement de forme "a=<nom d'attribut>". 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=<nom d'attribut>:<valeur d'attribut>". 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 des 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 une ligne "m=" (champ support) et est terminée soit par la prochaine ligne "m=", soit par la fin de la description de session. Un champ de support a plusieurs sous champs :

<support> est le type de support. Le présent document définit les valeurs "audio", "vidéo", "texte", "application", et "message". Cette liste est étendue par d'autres textes et pourra être encore étendue à l'avenir par des RFC enregistrant des types de supports (voir la Section 8). Par exemple, la [RFC6466] a défini le type de support "image".

<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 la ligne "c=" pertinente, et du protocole de transport défini dans le sous champ <proto> du champ 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, l'attribut "a=rtp:" 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=rtp:" DOIT être utilisé. Les applications à qui il est demandé d'envoyer des supports à un <accès> qui est impair et où l'attribut "a=rtp:" 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=rtp".

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 la ligne "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 la description de <fmt>).

Le présent document ne comporte pas de mécanisme pour déclarer des flux codés hiérarchiquement en utilisant des accès non contigus. (Il n'y a actuellement pas d'attribut défini qui puisse faire cela. L'attribut "a=rtp:" défini dans la [RFC3605] ne traite pas le codage hiérarchique.) Si il apparaissait un besoin de déclarer des accès non contigus, il serait nécessaire de définir un nouvel attribut pour ce faire.

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

```
m=video 49170/2 RTP/AVP 31
c=IN IP4 233.252.0.1/127/2
```

impliquerait que l'adresse 233.252.0.1 est utilisée avec les accès 49170 et 49171, et que l'adresse 233.252.0.2 est utilisée avec les accès 49172 et 49173.

La transposition est similaire si plusieurs adresses sont spécifiées en utilisant plusieurs lignes "c=". Par exemple :

```
m=video 49170/2 RTP/AVP 31
c=IN IP6 ff00::db8:0:101
c=IN IP6 ff00::db8:0:102
```

impliquerait que l'adresse ff00::db8:0:101 est utilisée avec les accès 49170 et 49171, et que l'adresse ff00::db8:0:102 est utilisée avec les accès 49172 et 49173.

Le présent document ne donne aucune signification à l'allocation de la même adresse de support à plusieurs descriptions de supports. Le faire ne groupe implicitement en aucune façon ces descriptions. Un cadre explicite de groupement (par exemple, la [RFC5888]) devrait plutôt être utilisé pour exprimer la sémantique prévue. Par exemple, voir la [RFC8843].

<proto> est le protocole de transport. La signification du protocole de transport dépend du sous champ type d'adresse dans la ligne "c=" pertinente. Donc une ligne "c=" avec un type d'adresse 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 que les données sont transportées directement sur UDP sans tramage supplémentaire.
- \* 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.
- \* RTP/SAVPF : note SRTP avec le profil SRTP étendu pour retours fondés sur RTCP [RFC5124] 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 peuvent être portés sur des protocoles de transport différents même quand le protocole réseau est le même – un exemple historique est vat (outil audio multimédia populaire de MBone) 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, des 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. Quand plusieurs formats de charge utile sont mentionnés, 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 le paragraphe 6.6) 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 le paragraphe 6.15).

Si le sous-champ <proto> est "udp", les sous champs <fmt> DOIVENT se référer à un type de support qui décrit 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 sous 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).

La Section 3 de la [RFC4855] déclare que les noms de format de charge utile (codage) définis dans le profil RTP sont couramment montrés en majuscules, tandis que les noms de sous type de support sont couramment montrés en minuscules.

Elle déclare aussi que ces deux noms sont insensibles à la casse dans les deux places, comme les noms de paramètres qui sont insensibles à la casse à la fois dans les chaînes de type de support et dans la transposition par défaut en l'attribut "a=fmtp:" SDP.

## 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. La syntaxe est fournie en ABNF [RFC7405] avec quelques règles mieux définies dans la Section 9.

### 6.1 cat (catégorie)

Nom : cat

Valeur : cat-value

Niveau d'utilisation : session

Dépendance au jeu de caractères : non

Syntaxe :

cat-value = category

category = non-ws-string

Exemple : a=cat:foo.bar

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. Cet attribut est obsolète et NE DEVRAIT PAS être utilisé. Il DEVRAIT être ignoré à réception.

### 6.2 keywds (mots clés)

Nom : keywds

Valeur : keywds-value

Niveau d'utilisation : session

Dépendance au jeu de caractères : oui

Syntaxe :

keywds-value = keywords

keywords = text

Exemple : a=keywds:protocole SDP de description de session

Comme l'attribut cat, il était destiné à aider à identifier les sessions voulues chez le receveur et à permettre à un receveur de choisir une session intéressante sur la base des mots clés qui décrivent l'objet de la session ; cependant, il n'y a pas de registre central des mots clés. 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. Cet attribut est obsolète et NE DEVRAIT PAS être utilisé. Il DEVRAIT être ignoré à réception.

### 6.3 tool (outil)

Nom : tool

Valeur : tool-value

Niveau d'utilisation : session

Dépendance au jeu de caractères : non

Syntaxe :

tool-value = tool-name-and-version

tool-name-and-version = text

Exemple : a=tool:foobar V3.2

Cela donne le nom et le numéro de version de l'outil utilisé pour créer la description de session..

#### 6.4 ptime (heure de paquet)

Nom : ptime

Valeur : ptime-value

Niveau d'utilisation : support

Dépendance au jeu de caractères : non

Syntaxe :

ptime-value = non-zero-int-or-real

Exemple : a=ptime:20

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 "a=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.

#### 6.5 maxptime (durée maximum du paquet)

Nom : maxptime

Valeur : maxptime-value

Niveau d'utilisation : support

Dépendance au jeu de caractères : non

Syntaxe :

maxptime-value = non-zero-int-or-real

Exemple : a=maxptime:20

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 que représentent les 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. Noter que cet attribut a été introduit après la RFC 2327, et les mises en œuvre non mises à jour vont ignorer cet attribut.

#### 6.6 rtpmap (transposition RTP)

Nom : rtpmap

Valeur : rtpmap-value

Niveau d'utilisation : support

Dépendance au jeu de caractères : non

Syntaxe :

rtpmap-value = type de charge utile SP nom de codage "/" débit d'horloge [ "/" paramètres de codage ]

type de charge utile = entier de base zéro

nom de codage = jeton

débit d'horloge = entier

paramètres de codage = canaux

canaux = entier

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. Noter que le numéro de type de charge utile est indiqué dans un champ de 7 bits, limitant les valeurs à la gamme 0 à 127

inclus.

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  $\mu$  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 [RFC3551]) est nécessaire, l'attribut "ptime" est utilisé comme montré au paragraphe 6.4.

## 6.7 Attributs de direction du support

Au plus une occurrence de "a=recvonly", "a=sendrecv", "a=sendonly", ou "a=inactive" PEUT apparaître au niveau session, et au plus une PEUT apparaître dans chaque description de support.

Si l'un d'eux apparaît dans une description de support, il s'applique alors pour cette description de support. Si aucun n'apparaît dans une description de support, alors celui du niveau session, s'il en est, s'applique à cette description de support.

Si aucun attribut de direction de support n'est présent au niveau session ni au niveau support, "a=sendrecv" DEVRAIT être supposé comme valeur par défaut.

Dans l'exemple SDP qui suit, l'attribut "a=sendrecv" s'applique au premier support audio et l'attribut "a=inactive" s'applique aux autres.

```
v=0
o=joe 3724395000 3724395001 IN IP6 2001:db8::1
s=-
c=IN IP6 2001:db8::1
```

```
t=0 0
a=inactive
m=audio 49170 RTP/AVP 0
a=sendrecv
m=audio 49180 RTP/AVP 0
m=video 51372 RTP/AVP 99
a=rtpmap:99 h263-1998/90000
```

### 6.7.1 **recvonly (réception seule)**

Nom : recvonly  
Valeur :  
Niveau d'usage : session, support  
Dépendance au jeu de caractères : non

Exemple : a=recvonly

Cela spécifie que les outils devraient être commencés en mode réception seule lorsque applicable. Noter que recvonly s'applique seulement au support, et non à un protocole de contrôle associé. Un système fondé sur RTP en mode réception seule **DOIT** quand même envoyer des paquets RTCP comme décrit à la Section 6 de la [RFC3550].

### 6.7.2 **sendrecv (envoi/réception)**

Nom : sendrecv  
Valeur :  
Niveau d'usage : session, support  
Dépendance au jeu de caractères : non

Exemple : a=sendrecv

Cela spécifie que les outils devraient être commencés en mode envoi et réception. Ceci est nécessaire pour les conférences multimédia interactives avec des outils qui prennent par défaut le mode réception seule.

### 6.7.3 **sendonly (envoi seul)**

Nom : sendonly  
Valeur :  
Niveau d'usage : session, support  
Dépendance au jeu de caractères : non

Exemple : a=sendonly

Cela spécifie que les outils devraient être commencés en mode envoi seul. 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 en mode sendonly et une en mode recvonly. Noter que le mode 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.

### 6.7.4 **inactive**

Nom : inactive  
Valeur :  
Niveau d'usage : session, support  
Dépendance au jeu de caractères : non

Exemple : a=inactive

Cela spécifie que les outils devraient être commencés en mode inactif. Ceci est nécessaire pour les conférences multimédia 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 DOIT quand même envoyer RTCP (si RTCP est utilisé) même si il a commencé en mode inactif.

## 6.8 orient (orientation)

Nom : orient

Valeur : orient-value

Niveau d'usage : support

Dépendance au jeu de caractères : non

Syntaxe :

orient-value = portrait / paysage / bord de mer

portrait = %s"portrait"

paysage = %s"paysage"

bord de mer = %s"bord de mer"

Note : ces noms sont sensibles à la casse.

Exemple : a=orient:portrait

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. Les valeurs permises sont "portrait", "paysage", et "bord de mer" (paysage inversé).

## 6.9 type (type de conférence)

Nom : type

Valeur : type-value

Niveau d'usage : session

Dépendance au jeu de caractères : non

Syntaxe :

type-value = type de conférence

type de conférence = diffusion / réunion / modérée / essai / H332

diffusion = %s"diffusion"

réunion = %s"réunion"

modérée = %s"modérée"

essai = %s"essai"

H332 = %s"H332"

Note : ces noms sont sensibles à la casse.

Exemple : a=type:modérée

Cela spécifie le type de la conférence multimédia. Les valeurs permises sont "diffusion", "réunion", "modérée", "essai", et "H332". Ces valeurs ont des implications pour les autres options qui vont probablement être appropriées :

- \* Quand "a=type:diffusion" est spécifié, "a=recvonly" est probablement approprié pour ceux qui se connectent.
- \* Quand "a=type:réunion" est spécifié "a=sendrecv" est probablement approprié.
- \* "a=type:modéré" suggère 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 multimédia.
- \* 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]. Les outils de supports devraient être commencés en "recvonly".
- \* Spécifier l'attribut "type:essai" 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.

## 6.10 charset (jeu de caractères)

Nom : charset

Valeur : charset-value

Niveau d'usage : session

Dépendance au jeu de caractères : non

Syntaxe :

charset-value = <définie dans la [RFC2978]>

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 l'attribut SDP suivant : a=charset:ISO-8859-1

Le jeu de caractères spécifié DOIT être un de ceux enregistrés dans le registre des jeux de caractères de l'IANA (<http://www.iana.org/assignments/character-sets>) comme ISO-8859-1. L'identifiant de jeu de caractères est une chaîne qui DOIT être comparée aux identifiants provenant du champ "Name" ou "Preferred MIME Name" du registre en utilisant une comparaison insensible à la casse. Si l'identifiant n'est pas reconnu ou non pris en charge, toutes les chaînes qui en sont affectées DEVRAIENT être considérées comme des chaînes d'octets.

Les champs qui dépendent du jeu de caractères DOIVENT contenir seulement des séquences d'octets valides en accord avec la définition du jeu de caractères choisi. De plus, les champs qui dépendent du jeu de caractère NE DOIVENT PAS contenir les octets 0x00 (Nul), 0x0A (LF), et 0x0d (CR).

## 6.11 sdplang (langage SDP)

Nom : sdplang

Valeur : sdplang-value

Niveau d'usage : session, support

Dépendance au jeu de caractères : non

Syntaxe :

sdplang-value = Étiquette de langue ; Étiquette de langue est défini dans la RFC 5646

Exemple : a=sdplang:fr

Plusieurs attributs "a=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.

Comme attribut de niveau session, il spécifie le langage de la description de session (pas le langage du support). Comme attribut de niveau support, il spécifie le langage de tout champ d'information SDP de niveau support associé à ce support (là encore, pas la langue du support) outrepassant tout attribut "a=sdplang:" spécifié au niveau session.

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 "a=sdplang:" sont permis bien que NON RECOMMANDÉS.

La valeur de l'attribut "a=sdplang" doit être une seule étiquette de langue de la [RFC5646]. Un attribut "a=sdplang" DEVRAIT être spécifié quand une session est distribuée avec une portée suffisante pour franchir des limites géographiques, lorsque le langage des receveurs ne peut plus être supposé, ou lorsque la session est dans une langue différente de la norme locale supposée.

## 6.12 lang (langage)

Nom : lang

Valeur : lang-value

Niveau d'usage : session, support

Dépendance au jeu de caractères : non

Syntaxe :

lang-value = Étiquette de langue ; Étiquette de langue est défini dans la RFC 5646

Exemple : a=lang:de

Plusieurs attributs sdplang peuvent être fournis au niveau session ou au niveau support si la session ou le support a des capacités dans plusieurs langages, et dans ce cas l'ordre des attributs indique l'ordre de préférence des divers langages dans la session ou support, du plus au moins préféré.

Comme attribut de niveau session, "a=lang:" spécifie une capacité de langage pour la session décrite. Comme attribut de niveau support, il spécifie une capacité de langage pour ce support, outrepassant tout langage de niveau session spécifié.

La valeur de l'attribut "a=lang:" doit être une seule étiquette de langue de la [RFC5646]. Un attribut "a=lang" DEVRAIT être spécifié quand une session est de portée suffisante pour franchir les limites géographiques où le langage des receveurs ne peut être supposé, ou lorsque la session a des capacités dans des langues différentes de la norme locale supposée.

L'attribut "a=lang:" est supposé être utilisé pour régler le ou les langages initiaux utilisés dans la session. Des événements durant la session peuvent influencer la ou les langues utilisées, et les participants ne sont pas strictement liés à la seule utilisation des langages déclarés.

La plupart des cas d'utilisation en temps réel commencent avec un seul langage, tandis que d'autre cas impliquent une gamme de langues, par exemple une session avec interprétation ou sous titres. Quand plus d'un attribut "a=lang:" est spécifié, l'attribut "a=lang:" lui-même ne fournit aucune information sur si il est prévu que plusieurs langues soient utilisées durant la session, ni si l'intention est de choisir seulement une des langues. Si nécessaire, un nouvel attribut peut être défini et utilisé pour indiquer de telles intentions. Sans une telle sémantique, on suppose que pour une session négociée une des langues déclarées sera choisie et utilisée.

### 6.13 framerate (taux de trame)

Nom : framerate

Valeur : framerate-value

Niveau d'utilisation : support

Dépendance au jeu de caractères : non

Syntaxe :

framerate-value = entier ou réel non zéro

Exemple : a=framerate:60

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 sont permises. Il est défini seulement pour les supports vidéo.

### 6.14 quality (qualité)

Nom : quality

Valeur : quality-value

Niveau d'utilisation : support

Dépendance au jeu de caractères : non

Syntaxe :

quality-value = entier de base zéro

Exemple : a=quality:10

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.

## Tableau 2 : valeurs de qualité de codages

### 6.15. fntp (paramètres de format)

Nom : fntp

Valeur : fntp-value

Niveau d'utilisation : support

Dépendance au jeu de caractères : non

Syntaxe :

fntp-value = fnt SP paramètres spécifiques du format

paramètres spécifiques du format = chaîne d'octets

Note : les paramètres de format sont des paramètres de type de support et ils doivent refléter leur syntaxe.

Exemple : a=fntp:96 profile-level-id=42e016;max-mbps=108000;max-fs=3600

Cet attribut permet des paramètres qui sont spécifiques d'un format particulier à convoier d'une façon telle que SDP n'a pas à les comprendre. Le format doit être un des formats spécifiés pour le support. Les paramètres spécifiques du format, séparés par un point virgule, peuvent être tout ensemble de 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.

L'attribut "a=fntp:" peut être utilisé pour spécifier des paramètres pour tout protocole et format qui définissent l'utilisation de tels paramètres.

## 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 et protégé en intégrité provenant d'une source connue et de confiance. De nombreux protocoles de transport différents peuvent être utilisés pour distribuer les descriptions de session, et la nature de l'authentification et de la protection d'intégrité 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 ; le point d'extrémité peut décider de demander à l'utilisateur si il accepte ou non la session.

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. Des soucis similaires s'appliquent si la protection de l'intégrité n'est pas en place. Les descriptions de session contiennent les 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 devraient

supposer que les sessions sont interactives. Les URL de traitement de logiciel contenus dans les descriptions de session devraient aussi prendre garde aux considérations sur la sécurité identifiées dans la [RFC3986].

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'utilisateur 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 envoyée 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 de certaines procédures et extensions à SDP (par exemple, l'établissement de connectivité interactive (ICE, *Interactive Connectivity Establishment*) [RFC8445] et ICE-SIP-SDP [RFC8839]) peut éviter le besoin que des intermédiaires modifient SDP.

SDP NE DOIT PAS être utilisé pour convoyer du matériel de chiffrement (par exemple, en utilisant l'attribut "a=crypto:" [RFC4568]) sauf si il peut être garanti que le canal sur lequel le SDP est livré est à la fois protégé quant à la confidentialité et authentifié.

## 8. Considérations relatives à l'IANA

### 8.1 Type de support "application/sdp"

Un enregistrement de type de support de la [RFC4566] est mis à jour, comme défini ci-dessous.

Nom du type : application

Nom du sous type : sdp

Paramètres exigés : aucun.

Paramètres facultatifs : aucun.

Considérations de codage : texte en 8 bits. 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 8866). Un contenu binaire arbitraire ne peut pas être directement représenté dans SDP.

Considérations de sécurité : voir la Section 7 de la RFC 8866

Considérations d'interopérabilité : voir la RFC 8866

Spécification publiée : voir la RFC 8866

Applications qui utilisent ce type de support : voix sur IP, téléconférences vidéo, support de flux directs, messagerie instantanée, entre autres. Voir aussi la Section 3 de la RFC 8866.

Considérations d'identifiant de fragment : aucune

Information supplémentaires :

Noms d'alias déconseillés pour ce type : N/A

Numéro magique : aucun

Extension de fichier : l'extension ".sdp" est d'utilisation courante

Code de type de fichier Macintosh : "sdp"

Adresse de la personne & de messagerie à contacter pour plus d'informations : groupe de travail IETF MMUSIC <mmusic@ietf.org>

Usage prévu : COMMUN

Restrictions à l'usage : aucune

Auteur/contrôleur des changements : auteurs de la RFC 8866 ; groupe de travail IETF MMUSIC sur délégation de l'IESG.

## 8.2 Enregistrement des paramètres SDP auprès de l'IANA

Le présent document spécifie les registres IANA de paramètres pour six sous champs nommés de SDP. En utilisant la terminologie du format Bachus-Naur augmenté (ABNF) de la spécification de SDP ce sont <media>, <proto>, <attribute-name>, <bwtype>, <nettype>, et <addrtype>.

Le présent document remplace et met à jour aussi les définitions de tous les paramètres antérieurement définis par la [RFC4566].

L'IANA a changé toutes les références à la RFC 4566 dans ces registres en références au présent document.

Le nom de contact et l'adresse de messagerie électronique pour tous les paramètres enregistrés dans ce document est le groupe de travail IETF MMUSIC <mmusic@ietf.org> ou son successeur comme désigné par l'IESG.

Tous ces registres ont un format commun :

Type	Nom SDP	[autres champs]	référence
------	---------	-----------------	-----------

**Tableau 3 : Format commun des registres SDP**

### 8.2.1 Procédure d'enregistrement

Un document de spécification qui définit des valeurs pour les paramètres SDP <media>, <proto>, <attribute-name>, <bwtype>, <nettype>, et <addrtype> DOIT inclure les informations suivantes :

- \* Nom du contact
- \* adresse électronique du contact
- \* Nom défini (comme il apparaîtra dans SDP)
- \* Type de nom (<media>, <proto>, <attribute-name>, <bwtype>, <nettype>, ou <addrtype>)
- \* Description de l'objet du nom défini
- \* Référence stable au document qui contient ces informations et la définition de la valeur (normalement un numéro de RFC).

Les paragraphes qui suivent spécifient quelles autres informations (s'il en est) doivent être spécifiées pour des paramètres particuliers, et quels autres champs sont à inclure dans le registre.

### 8.2.2 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 [RFC8126]).

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 une 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). Noter aussi que la [RFC6466] a défini le type de support "image".

### 8.2.3 Protocoles de transport (<proto>)

Le sous champ <proto> décrit le protocole de transport utilisé. La procédure d'enregistrement pour ce registre est "RFC exigée".

Le présent document enregistre deux valeurs :

- \* "RTP/AVP" est une référence à la [RFC3550] utilisée sous le profil RTP pour les conférences audio et vidéo avec contrôle minimal [RFC3551] fonctionnant sur UDP/IP.
- \* "udp" indique l'utilisation directe de UDP.

De nouveaux protocoles de transport PEUVENT être définis et DOIVENT 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. La RFC définissant un nouveau protocole DOIT définir les règles de gestion de leur espace de nom <fmt> (voir ci-dessous).

Des noms de <proto> commençant par "RTP/\*" DOIVENT seulement être utilisés pour définir des protocoles de transport qui sont des profils de RTP. Par exemple, un profil dont le nom abrégé est "XYZ" devrait être noté par un sous champ <proto> de "RTP/XYZ".

Chaque protocole de transport, défini par le sous 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 être transportés dans une session multimédia.

Les formats de charge utile RTP sous les profils "RTP/AVP" et autres profils "RTP/\*" DOIVENT utiliser le numéro de type de charge utile comme leur 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 valeurs de <fmt> permises sont des sous types de supports du registre des types de supports de l'IANA. La combinaison du type et sous type de support <media>/<fmt> spécifie le format du corps des paquets UDP. L'utilisation d'un sous type de support existant pour le format est encouragé. Si aucun sous type de support convenable n'existe, il est RECOMMANDÉ qu'il en soit enregistré un nouveau 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 enregistrements de nouveaux formats DOIVENT spécifier à quels protocoles de transport ils s'appliquent.

#### 8.2.4 Noms d'attributs (<attribute-name>)

Les noms des champs d'attributs (<attribute-name>) DOIVENT être enregistrés par l'IANA et documentés, pour éviter tout problème dû à des définitions d'attributs en conflit sous le même nom. (Bien que les attributs inconnus dans SDP soient simplement ignorés, ceux en conflit qui fragmentent le protocole sont un problème sérieux.)

Le format du registre <attribute-name> est :

Type	Nom SDP	Niveau d'usage	Catégorie Mux	Référence
------	---------	----------------	---------------	-----------

**Tableau 4 : Format du registre <attribute-name>**

Par exemple, l'attribut "a=lang:", qui est défini pour les deux niveaux session et support, sera mentionné dans le nouveau registre comme suit :

Type	Nom SDP	Niveau d'usage	Catégorie Mux	Référence
attribut	lang	session, media	TRANSPORT	[RFC8866] [RFC8859]

**Tableau 5 : Exemple de registre <attribute-name>**

Ce registre de un <attribute-name> combine tous les registres antérieurs spécifiques du niveau d'usage de "att-field", incluant les mises à jour faites par la [RFC8859], change le nom du registre "att-field" en registre "attribute-name (anciennement "att-field")". L'IANA a effectué le reformatage nécessaire.

La Section 6 du présent document remplace le jeu initial de définitions d'attributs fait par la [RFC4566]. L'IANA a mis le registre à jour en conséquence.

Des documents peuvent définir de nouveaux attributs et peuvent aussi étendre les définitions d'attributs définis précédemment.

#### 8.2.4.1 Nouveaux attributs

Les enregistrements de nouveaux attributs sont acceptés selon la politique "Spécification exigée" de la [RFC8126], pourvu que la spécification inclue les informations suivantes :

- \* Nom du contact.
- \* Adresse de messagerie électronique du contact.
- \* Nom de l'attribut : nom d'attribut qui va apparaître dans SDP. Il DOIT se conformer à la définition de <attribute-name>.
- \* Syntaxe d'attribut : pour un attribut de valeur (voir au paragraphe 5.13) une définition en ABNF de la syntaxe de la valeur de l'attribut <attribute-value> (Section 9) DOIT être fournie. La syntaxe DOIT suivre la forme de règle selon le paragraphe 2.2 de la [RFC5234] et la [RFC7405]. Ceci DEVRA définir les valeurs admissibles pour l'attribut. Elle PEUT aussi définir une méthode d'extension pour l'ajout de futures valeurs. Pour un attribut de propriété, La définition en ABNF est omise car l'attribut de propriété ne prend pas de valeurs.
- \* Sémantique de l'attribut : pour un attribut de valeur, une description de la sémantique des valeurs que l'attribut peut prendre DOIT être fournie. L'usage d'un attribut de propriété est décrit dans son objet (ci-dessous).
- \* Valeur d'attribut : nom d'une règle de syntaxe ABNF définissant la syntaxe de la valeur. L'absence d'un nom de règle indique que l'attribut ne prend pas de valeurs. Enclore le nom de la règle entre "[" et "]" indique qu'une valeur est facultative.
- \* Niveau d'usage : le ou les niveaux d'usage de l'attribut. Ce DOIT être un ou plusieurs de : session, media, source, dcsa, et dcsa(sous protocole). Pour une définition d'attributs de niveau source, voir la [RFC5576]. Pour une définition d'attributs dcsa, voir la [RFC8864].
- \* Dépendance au jeu de caractères : ce DOIT être "Oui" ou "Non" selon que la valeur de l'attribut est soumise ou non à l'attribut "a=charset:".
- \* Objet : explication de l'objet et de l'usage de l'attribut.
- \* Procédures O/A : procédures d'offre/réponse comme expliqué dans la [RFC3264].
- \* Catégorie Mux : cela DOIT indiquer une des catégories suivantes : NORMAL, NON RECOMMANDÉE, IDENTIQUE, SOMME, TRANSPORT, HÉRITAGE, IDENTIQUE-PAR-PT, SPÉCIAL, ou TBD comme défini par la [RFC8859].
- \* Référence : une référence à la spécification qui définit l'attribut.

Ceci est le minimum que l'IANA va accepter. Les attributs qui sont supposés avoir une large utilisation et interopérabilité DEVRAIENT être documentés 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.

Les soumissions d'enregistrement devraient aussi choisir avec soin le niveau d'usage de l'attribut. Elles ne devraient pas choisir seulement "session" quand l'attribut peut avoir des valeurs différentes quand le support est "désagrégé", c'est-à-dire, quand chaque section "m=" a sa propre adresse IP sur des points d'extrémité différents. Dans ce cas, le type d'attribut choisi devrait être "session, support" ou "support" (selon la sémantique désirée). La règle par défaut est que pour tous les nouveaux attributs SDP qui peuvent apparaître au niveau à la fois session et support, le niveau support outrepassé le niveau session. Quand ce n'est pas le cas pour un nouvel attribut SDP, cela DOIT être déclaré explicitement.

L'IANA a enregistré le jeu initial des noms d'attributs (valeurs <attribute-name>) avec les définitions de la Section 6 du présent document (ces définitions remplacent celles de la [RFC4566]).

#### 8.2.4.2 Mises à jour des attributs existants

Les enregistrements de mises à jour d'attribut sont acceptés selon la politique de "spécification exigée" de la [RFC8126].

L'expert désigné qui revoit la mise à jour doit évaluer si la mise à jour est compatible avec l'intention et l'utilisation antérieures de l'attribut, et si le nouveau document est de maturité et autorité suffisantes par rapport au document antérieur.

La spécification qui met à jour l'attribut (par exemple, en ajoutant une nouvelle valeur) DOIT mettre à jour les éléments d'informations d'enregistrement mentionnés au paragraphe 8.2.4.1 en accord avec les contraintes suivantes :

- \* Nom du contact : le nom de l'entité responsable de la mise à jour DOIT être fourni.
- \* Adresse de messagerie électronique du contact : une adresse de messagerie électronique de l'entité responsable de la mise à jour DOIT être fournie.
- \* Nom de l'attribut : DOIT être fourni et NE DOIT PAS être changé. Autrement, c'est un nouvel attribut.
- \* Syntaxe d'attribut : la syntaxe de règle existante avec les extensions de syntaxe DOIT être fournie si il y a un changement de la syntaxe. Une révision de l'usage d'un attribut existant PEUT étendre la syntaxe d'un attribut, mais DOIT être rétro compatible.
- \* Sémantique de l'attribut : une description sémantique des nouvelles valeurs supplémentaires de l'attribut ou une extension de la sémantique de valeurs existantes. La sémantique des valeurs existantes des attributs DOIT n'être étendue que de façon rétro compatible.
- \* Niveau d'usage : les mises à jour PEUVENT seulement ajouter des niveaux supplémentaires.
- \* Dépendance au jeu de caractères : elle NE DOIT PAS être changée.
- \* Objet : il PEUT être étendu en accord avec la mise à jour de l'usage
- \* Procédures O/A : elles PEUVENT être mises à jour de façon rétro compatible et/ou elles s'appliquent seulement à un nouveau niveau d'usage.
- \* Catégorie Mux : aucun changement sauf de "TBD" à une autre valeur (voir la [RFC8859]. Elle PEUT aussi changer si le niveau support est ajouté à la définition d'un attribut qui ne l'incluait précédemment pas.
- \* Référence : une nouvelle référence (supplémentaire ou de remplacement) DOIT être fournie.

Les éléments DEVRAIENT être omis si la mise à jour de l'attribut n'a pas d'impact sur eux.

### 8.2.5 Spécificateurs de bande passante ("bwtype")

La prolifération des spécificateurs de bande passante est fortement déconseillée.

Les nouveaux spécificateurs de bande passante (valeurs de sous 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.

La RFC DOIT spécifier la catégorie Mux pour cette valeur comme défini dans la [RFC8859].

Le format du registre <bwtype> est :

Type	Nom SDP	Catégorie Mux	Référence
------	---------	---------------	-----------

**Tableau 6 : Format du registre <bwtype>**

L'IANA a mis à jour les entrées du registre <bwtype> pour les spécificateurs de bande passante "CT" et "AS" avec les définitions du paragraphe 5.8 du présent mémoire (ces définitions remplacent celles de la [RFC4566]).

### 8.2.6 Types de réseau ("nettype")

Le type de réseau "IN", qui représente l'Internet, est défini aux paragraphes 5.2 et 5.7 (cette définition remplace celle de la [RFC4566]).

Pour permettre à SDP de faire référence à un nouvel environnement non Internet, une nouvelle valeur de sous champ de type de réseau (valeur de sous champ <nettype>) DOIT être enregistrée par l'IANA. L'enregistrement est soumis à la politique de "RFC exigée" de la [RFC8126]. Bien que les environnements non Internet 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 d'enregistrement de réseau DOIT faire référence à une RFC qui donne les détails du type de réseau et du ou des types d'adresse qui peuvent être utilisés avec lui.

Le format du registre <nettype> est :

Type	Nom SDP	Valeurs de type d'adresse utilisables	Référence
------	---------	---------------------------------------	-----------

**Tableau 7 : Format du registre <nettype>**

L'IANA a mis à jour le registre <nettype> à ce nouveau format. Voici le contenu mis à jour du registre :

Type	Nom SDP	Valeurs de type d'adresse utilisables	Référence
nettype	IN	IP4, IP6	[RFC8866]
nettype	TN	RFC2543	[RFC2848]
nettype	ATM	NSAP, GWID, E164	[RFC3108]
nettype	RTPC	E164	[RFC7195]

**Tableau 8 : Contenu du registre <nettype>**

Noter que les deux [RFC7195] et [RFC3108] ont enregistré "E164" comme type d'adresse, bien que la [RFC7195] mentionne que le type d'adresse "E164" a un contexte différent pour les réseaux ATM et RTPC.

### 8.2.7 Types d'adresse ("addrtype")

De nouveaux types d'adresses (<addrtype>) DOIVENT être enregistrés par l'IANA. L'enregistrement est soumis à la politique de "RFC exigée" de la [RFC8126]. Un enregistrement de nouveau type d'enregistrement 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.

Le paragraphe 5.7 du présent document donne les nouvelles définitions des types d'adresses "IP4" et "IP6".

### 8.3 Méthodes d'accès aux clés de chiffrement (Obsolète)

L'IANA tenait précédemment un tableau des noms de méthodes d'accès de clé d'enregistrement 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 les [RFC5234] et [RFC7405].

; Syntaxe SDP

```

session-description = version-field
                    origin-field
                    session-name-field
                    [information-field]
                    [uri-field]
                    *email-field
                    *phone-field
                    [connection-field]
                    *bandwidth-field
                    1*time-description
                    [key-field]
                    *attribute-field
                    *media-description

```

version-field = %s"v" "=" 1\*DIGIT CRLF ; le présent mémoire décrit la version 0

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

session-name-field = %s"s" "=" text CRLF

information-field = %s"i" "=" text CRLF

uri-field = %s"u" "=" uri CRLF

email-field = %s"e" "=" email-address CRLF

phone-field = %s"p" "=" phone-number CRLF

connection-field = %s"c" "=" nettype SP addrtype SP connection-address CRLF

; un champ "connection" doit être présent dans toutes les description de support ou au niveau ;session.

bandwidth-field = %s"b" "=" bwtype ":" bandwidth CRLF

time-description = time-field [repeat-description]

repeat-description = 1\*repeat-field [zone-field]

time-field = %s"t" "=" start-time SP stop-time CRLF

repeat-field = %s"r" "=" repeat-interval SP typed-time 1\*(SP typed-time) CRLF

zone-field = %s"z" "=" time SP ["-"] typed-time \*(SP time SP ["-"] typed-time) CRLF

key-field = %s"k" "=" key-type CRLF

attribute-field = %s"a" "=" attribute CRLF

media-description = media-field  
                           [information-field]  
                           \*connection-field  
                           \*bandwidth-field  
                           [key-field]  
                           \*attribute-field

media-field = %s"m" "=" media SP port ["/" integer] SP proto 1\*(SP fmt) CRLF

; sous règles de 'o='

username = non-ws-string ; définition très large, mais exclut les espaces.

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

sess-version = 1\*DIGIT

nettype = token ; normalement "IN"

addrtype = token ; normalement "IP4" ou "IP6"

; sous règles de 'u='

uri = URI-reference ; voir la RFC 3986

; sous règles de 'e=', ; voir les définitions dans la RFC 5322.

email-address = address-and-comment / dispname-and-address / addr-spec

address-and-comment = addr-spec 1\*SP "(" 1\*email-safe ")"

dispname-and-address = 1\*email-safe 1\*SP "<" addr-spec ">"

; sous règles de 'p='

phone-number = phone \*SP "(" 1\*email-safe ")" / 1\*email-safe "<" phone ">" / phone

phone = ["+"] DIGIT 1\*(SP / "-" / DIGIT)

; sous règles de 'c='

connection-address = multicast-address / unicast-address

; sous règles de 'b='

bwtype = token

bandwidth = 1\*DIGIT

; sous règles de 't='

start-time = time / "0"

stop-time = time / "0"

time = POS-DIGIT 9\*DIGIT

; représentation décimale de l'heure en secondes depuis le 1er janvier 1900 UTC. La représentation est un champ de longueur non limitée contenant au moins 10 chiffres. À la différence de certaines représentations utilisées ailleurs, l'heure dans SDP ne revient pas à zéro en l'an 2036.

; sous règles de 'r=' and 'z='

repeat-interval = POS-DIGIT \*DIGIT [fixed-len-time-unit]

typed-time = 1\*DIGIT [fixed-len-time-unit]

fixed-len-time-unit = %s"d" / %s"h" / %s"m" / %s"s" ; Note : ces unités sont sensibles à la casse.

; sous règles de 'k='

key-type = %s"prompt" / %s"clear:" text / %s"base64:" base64 / %s"uri:" uri ; Note : ces unités sont sensibles à la casse.

base64 = \*base64-unit [base64-pad]

base64-unit = 4base64-char

base64-pad = 2base64-char "==" / 3base64-char "==="

base64-char = ALPHA / DIGIT / "+" / "/"

; sous règles de 'a='

attribute = (attribute-name ":" attribute-value) / attribute-name

attribute-name = token

attribute-value = byte-string

att-field = attribute-name ; pour la rétro compatibilité.

; sous règles de 'm='

media = token ; normalement "audio", "video", "text", "image" ou "application"

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

proto = token \*("/" token) ; normalement "RTP/AVP", "RTP/SAVP", "udp", ou "RTP/SAVPF".

port = 1\*DIGIT

; sous règles génériques : adressage

unicast-address = IP4-address / IP6-address / FQDN / extn-addr

multicast-address = IP4-multicast / IP6-multicast / FQDN / extn-addr

IP4-multicast = m1 3( "." decimal-uchar ) "/" ttl [ "/" numaddr ]

; les adresses de diffusion groupée IP4 peuvent être dans la gamme 224.0.0.0 à 239.255.255.255

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

IP6-multicast = IP6-address [ "/" numaddr ] ; adresse IP6 commençant par FF.

numaddr = integer

ttl = (POS-DIGIT \*2DIGIT) / "0"

FQDN = 4\*(alpha-numeric / "-" / ".")

; nom de domaine pleinement qualifié comme spécifié dans la RFC 1035 (et ses mises à jour).

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

b1 = decimal-uchar ; moins de "224".

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

; Génériques pour autres familles d'adresses

extn-addr = non-ws-string

; sous règles génériques : types de données

text = byte-string

; est interprété par défaut comme texte UTF8. ISO 8859-1 exige d'utiliser l'attribut de niveau session "a=charset:ISO-8859-1" .

byte-string = 1\*(%x01-09/%x0B-0C/%x0E-FF) ; tout octet sauf NUL, CR, ou LF.

non-ws-string = 1\*(VCHAR/%x80-FF) ; chaîne de caractères visibles

token-char = ALPHA / DIGIT / "!" / "#" / "\$" / "%" / "&" / "'" ; (single quote) / "\*" / "+" / "-" / "." / "^" / "\_"  
 / " " ; (accent grave) / "{" / "|" / "}" / "~"

token = 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 (<>).

integer = POS-DIGIT \*DIGIT

zero-based-integer = "0" / integer

non-zero-int-or-real = integer / non-zero-real

non-zero-real = zero-based-integer "." \*DIGIT POS-DIGIT

; sousrègles génériques : primitives  
alpha-numeric = ALPHA / DIGIT

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

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

; références externes :

ALPHA = <définition ALPHA de la RFC 5234>

DIGIT = <définition DIGIT de la RFC 5234>

CRLF = <définition CRLF de la RFC 5234>

HEXDIG = <définition HEXDIG de la RFC 5234>

SP = <définition SP de la RFC 5234>

VCHAR = <définition VCHAR de la RFC 5234>

URI-reference = <définition URI-reference de la RFC 3986>

addr-spec = <définition addr-spec de la RFC 5322>

## 10. Résumé des changements par rapport à la RFC 4566

- \* La terminologie a généralement été précisée et clarifiée. Les termes utilisés dans le texte ont été alignés sur l'ABNF. Les termes <attribute>, <att-field>, et "att-field" sont maintenant <attribute-name>. Les termes <value> et <att-value> sont maintenant <attribute-value>. Le terme "media" est maintenant <media>.
- \* Les éléments obsolètes ont été identifiés : "a=cat:" (paragraphe 6.1), "a=keywds:" (paragraphe 6.2), et "k=" (paragraphe 5.12).
- \* Mise à jour des références normatives et informatives, et ajout des références aux RFC pertinentes supplémentaires.
- \* Reformatage de la Section 6 Attributs SDP pour sa lisibilité. La syntaxe des valeurs d'attribut est maintenant donnée en ABNF.
- \* L'envoi de RTPC avec des flux de supports inactifs est rendue obligatoire (paragraphe 6.7.4).
- \* Suppression du paragraphe "Sessions privées". Ce paragraphe datait d'une époque où la principale utilisation de SDP était avec SAP (protocole d'annonce de session), qui n'est plus utilisé. La vaste majorité des utilisations de SDP est maintenant pour l'établissement de sessions privées. Les considérations sur cette question sont couvertes dans la Section 7.
- \* Expansion et clarification de la spécification des attributs "a=lang:" (paragraphe 6.12) et "a=sdplang:" (paragraphe 6.11).
- \* Suppression de quelques références à SAP parce qu'il n'est plus très utilisé.
- \* Changement de la façon dont les valeurs de <fmt> pour le transport UDP sont enregistrées (paragraphe 8.2.3).
- \* Changement du mécanisme et de la documentation requis pour l'enregistrement de nouveaux attributs (paragraphe 8.2.4.1).
- \* Précision des procédures d'enregistrement de l'IANA pour les extensions. Suppression des numéros de téléphone et des formes longues de nom (paragraphe 8.2).
- \* Expansion du registre IANA <nettype> pour identifier les sous champs valides <addrtype> (paragraphe 8.2.6).
- \* Réorganisation de plusieurs registres "att-field" de l'IANA en un seul registre <attribute-name> (paragraphe 8.2.4).
- \* Révision de la syntaxe ABNF (Section 9) pour la préciser et l'aligner sur le texte. La rétro compatibilité est conservée à quelques exceptions près. On note en particulier :
  - Révision de la syntaxe des descriptions d'heure ("t=", "r=", "z=") pour supprimer les ambiguïtés. Précisé que "z=" modifie seulement les lignes "r=" immédiatement précédentes. On fait de "z=" sans une "r=" précédente une erreur de

- syntaxe (paragraphe 5.11). (C'est incompatible avec certains usages aberrants.)
- Mise à jour des règles "IP6-address" et "IP6-multicast", en cohérence avec la syntaxe de la [RFC3986], reflétant une correction d'erreur de la [RFC3261] par la [RFC5954]. Suppression des règles non utilisées par suite de ce changement.
  - La règle "att-field" a été renommée "attribute-name" parce qu'ailleurs "\*-field" se réfère toujours à une liste complète. Cependant, le nom de règle "att-field" reste défini comme synonyme pour la rétro compatibilité avec les références d'autres RFC.
  - La règle "att-value" a été renommées "attribute-value".
- \* Révision des déclarations normatives redondantes avec la syntaxe ABNF, rendant ce texte non normatif.
  - \* Révision des adresses IPv4 en envoi individuel et en diffusion groupée dans les exemples de descriptions SDP selon les [RFC5735] et [RFC5771].
  - \* Changement de certains exemples pour utiliser des adresses IPv6, et ajout d'exemples supplémentaires utilisant IPv6.
  - \* Incorporation des règles d'insensibilité à la casse de la [RFC4855].
  - \* Révision des sections qui faisaient une référence incorrecte à NTP (paragraphe 5.2, 5.9, 5.10, et 5.11).
  - \* Précisé l'explication de l'impact et utilisation de l'attribut "a=charset:" (paragraphe 6.10).
  - \* Révision de la description de l'attribut "a=type:" pour supprimer l'implication qu'il change parfois la direction par défaut du support en quelque chose d'autre que "a=sendrecv" (paragraphe 6.9).

## 11. Références

### 11.1 Références normatives

- [E164] Recommandation UIT-T E.164, "Plan de numérotation des télécommunications publiques internationales", Union Internationale des Télécommunications, novembre 2010, <<https://www.itu.int/rec/T-REC-E.164-201011-I/fr>>.
- [ISO.8859-1] International Organization for Standardization, "Information technology - 8-bit single byte coded graphic - character sets - Part 1: Latin alphabet No. 1", JTC1/SC2, ISO/IEC Standard 8859-1, 1998.
- [RFC1034] P. Mockapetris, "Noms de domaines - [Concepts et facilités](#)", STD 13, novembre 1987. DOI 10.17487/RFC1034, (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. DOI 10.17487/RFC1035, (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, DOI 10.17487/RFC2119, mars 1997. (MàJ par [RFC8174](#))
- [RFC2848] S. Petrack, L. Conroy, "[Protocole de service PINT](#) : extensions à SIP et SDP pour l'accès IP aux services de téléphone", juin 2000. DOI 10.17487/RFC2848, (P.S.)
- [RFC2978] N. Freed et J. Postel, "Procédures d'enregistrement des jeux de caractère par l'IANA", BCP 19, DOI 10.17487/RFC2978, octobre 2000.
- [RFC3108] R. Kumar et M. Mostafa, "[Conventions pour l'utilisation du protocole](#) de description de session (SDP) sur les connexions à porteur ATM", mai 2001. DOI 10.17487/RFC3108. (P.S.)
- [RFC3629] F. Yergeau, "[UTF-8, un format de transformation](#) de la norme ISO 10646", STD 63, novembre 2003. DOI 10.17487/RFC3629.
- [RFC3986] T. Berners-Lee, R. Fielding et L. Masinter, "[Identifiant de ressource uniforme](#) (URI) : Syntaxe générique", STD

66, janvier 2005. DOI 10.17487/RFC3986. (P.S. ; MàJ par RFC8820)

- [RFC4566] M. Handley, V. Jacobson et C. Perkins, "SDP : [Protocole de description de session](#)", juillet 2006, DOI 10.17487/RFC4566. (P.S. ; remplacée par RFC8866)
- [RFC5234] D. Crocker, éd., P. Overell, "[BNF augmenté pour les spécifications de syntaxe](#) : ABNF", janvier 2008, DOI 10.17487/RFC5234. ([STD0068](#))
- [RFC5576] J. Lennox, J. Ott, T. Schierl, "Attributs de support spécifiques de source dans le protocole de description de session (SDP)", juin 2009, DOI 10.17487/RFC5576. (P. S.)
- [RFC5646] A. Phillips, M. Davis, "Étiquettes d'identification des langages", [BCP0047](#), septembre 2009, DOI 10.17487/RFC5646. (Remplace [RFC4646](#))
- [RFC5890] J. Klensin, "[Noms de domaine internationalisés pour les applications](#) (IDNA) : Définitions et cadre documentaire", août 2010, DOI 10.17487/RFC5890. (Remplace [RFC3490](#)) (P.S.)
- [RFC5952] S. Kawamura, M. Kawashima, "Recommandation pour la représentation textuelle d'adresse IPv6", août 2010, DOI 10.17487/RFC5952. (MàJ [RFC4291](#)) (P.S.)
- [[RFC7195](#)] M. Garcia-Martin, S. Veikkolainen, "Extension au protocole de description de session (SDP) pour établir des flux de support audio et vidéo sur des porteuses à commutation de circuit dans le réseau téléphonique public commuté (RTPC)", mai 2014, DOI 10.17487/RFC7195. (P.S.)
- [[RFC8126](#)] M. Cotton, B. Leiba, T. Narten, "Lignes directrices pour la rédaction d'une section de considérations relatives à l'IANA dans les RFC", juin 2017, DOI 10.17487/RFC8126. BCP 26. (Remplace [RFC5226](#))
- [[RFC8174](#)] B. Leiba, "Ambiguïté des mots clés en majuscules ou minuscules dans la RFC2119", mai 2017., DOI 10.17487/RFC8174 BCP14. (MàJ 2119)
- [RFC8859] S. Nandakumar, "Cadre pour les attributs du protocole de description de session (SDP) pour le multiplexage", janvier 2021. (P.S.) (DOI : 10.17487/RFC8859)
- [RFC8864] K. Drage, et autres, "Négociation de canaux de données avec le protocole de description de session (SDP)", janvier 2021. (P.S.) (DOI : 10.17487/RFC8864)

## 11.2 Références pour information

- [H332] Recommandation UIT-T H.332, "H.323 étendu pour conférences à couplage lâche", Union Internationale des Télécommunications, septembre 1998, <<https://www.itu.int/rec/T-REC-H.332-199809-1/fr>>.
- [RFC2045] N. Freed et N. Borenstein, "[Extensions de messagerie Internet](#) multi-objets (MIME) Partie 1 : Format des corps de message Internet", novembre 1996, DOI 10.17487/RFC2045. (D. S., MàJ par [2184](#), [2231](#), [5335](#).)
- [RFC2327] M. Handley et V. Jacobson, "SDP : [Protocole de description de session](#)", avril 1998, DOI 10.17487/RFC2327. (*Obsolète; voir [RFC4566](#)*)
- [RFC2974] M. Handley, C. Perkins, E. Whelan, "Protocole d'annonce de session (SAP)", octobre 2000, DOI 10.17487/RFC2974. (*Expérimentale*)
- [RFC3261] J. Rosenberg et autres, "SIP : [Protocole d'initialisation de session](#)", juin 2002, DOI 10.17487/RFC3261. (*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, DOI 10.17487/RFC3264. (P.S. ; MàJ par [RFC8843](#))
- [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, DOI 10.17487/RFC3550. (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, DOI 10.17487/RFC3551. (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, DOI 10.17487/RFC3556. (P.S.)
- [RFC3605] C. Huitema, "Attribut du protocole de contrôle en temps réel (RTCP) dans le protocole de description de session (SDP)", octobre 2003, DOI 10.17487/RFC3605. (P.S.)
- [RFC3711] M. Baugher et autres, "Protocole de [transport sécurisé en temps réel](#) (SRTP)", mars 2004, DOI 10.17487/RFC3711. (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, DOI 10.17487/RFC3840.
- [RFC3890] M. Westerlund, "[Modificateur de bande passante indépendant du transport](#) pour le protocole de description de session (SDP)", septembre 2004, DOI 10.17487/RFC3890. (P.S.)
- [RFC4568] F. Andreassen et autres, "[Définition d'attributs de sécurité](#) dans le protocole de description de session (SDP) pour les flux de support", juillet 2006 DOI 10.17487/RFC4568. (P.S.)
- [RFC4855] S. Casner, "Enregistrement du type de support des formats de charge utile RTP", février 2007, DOI 10.17487/RFC4855. (P.S.)
- [RFC5124] J. Ott, E. Carrara, "Profil étendu de RTP sécurisé pour les rétroactions fondées sur le protocole de contrôle du transport en temps réel (RTCP)", février 2008, DOI 10.17487/RFC5124. (P.S.)
- [RFC5322] P. Resnick, éd., "[Format du message Internet](#)", octobre 2008, DOI 10.17487/RFC5322. (Remplace [RFC2822](#)) (MàJ [RFC4021](#)) (D.S.)
- [RFC5735] M. Cotton, L. Vegoda, "Adresses IPv4 d'utilisation particulière", janvier 2010, DOI 10.17487/RFC5735. (Remplace [RFC3330](#)) ([BCP0153](#)) (MàJ par la [RFC6598](#)) (Remplacée par [RFC6890](#))
- [RFC5771] M. Cotton, L. Vegoda, D. Meyer, "Lignes directrices de l'IANA pour l'allocation des adresses de diffusion groupée IPv4", ([BCP0051](#)), mars 2010, DOI 10.17487/RFC5771. (Remplace [RFC3138](#), [RFC3171](#)) (MàJ [RFC2780](#))
- [RFC5888] G. Camarillo, H. Schulzrinne, "Cadre de groupage du protocole de description de session (SDP)", juin 2010, DOI 10.17487/RFC5888. (Remplace [RFC3388](#)). (P. S. ; MàJ par [RFC8843](#))
- [RFC5954] V. Gurbani, B. Carpenter, B. Tate, "Correction essentielle pour la comparaison d'ABNF et d'URI IPv6 dans la RFC3261", août 2010, DOI 10.17487/RFC5954. (MàJ [RFC3261](#)) (P.S.)
- [RFC6466] G. Salgueiro, "Enregistrement par l'IANA du type de support "image" pour le protocole de description de session (SDP)", décembre 2011, DOI 10.17487/RFC6466. (P.S.)
- [[RFC6838](#)] N. Freed, J. Klensin et T. Hansen, "Spécifications de type de support et procédures d'enregistrement", BCP 13, janvier 2013, DOI 10.17487/RFC6838.
- [[RFC7230](#)] R. Fielding, et J. Reschke, "Protocole de transfert Hypertexte (HTTP/1.1) : syntaxe et acheminement de message", juin 2014, DOI 10.17487/RFC7230. (Remplace RFC 2145, 2616, MàJ RFC 2617, 2618) (P.S. ; MàJ par [RFC8615](#))
- [[RFC7405](#)] P. Kyzivat, "Prise en charge de chaînes sensibles à la casse en ABNF", décembre 2014, DOI 10.17487/RFC7405. (P.S., MàJ [RFC5234](#))
- [[RFC7656](#)] J. Lennox, et autres, "Taxonomie de la sémantique et des mécanismes pour les sources de RTP", novembre 2015,

DOI 10.17487/RFC7656. (*Info*)

- [[RFC7826](#)] H. Schulzrinne, et autres, "Protocole de flux en temps réel version 2.0", décembre 2015, DOI 10.17487/RFC7826. (*P.S. ; Remplace 2326*)
- [[RFC8445](#)] A. Keranen, et autres, "Établissement de connexité interactive (ICE) : un protocole pour la traversée de NAT", juillet 2018, DOI 10.17487/RFC8445. (*P.S. ; remplace la RFC 5245 ; MàJ par RFC8863*)
- [[RFC8839](#)] M. Petit-Huguenin, et autres, "Procédure d'offre/réponse du protocole de description de session pour ICE", janvier 2021. (*P.S. ; remplace RFC5245, et RFC 6336*) (DOI : 10.17487/RFC8839)
- [[RFC8843](#)] C. Holmberg, H. Alvestrand, C. Jennings, "Négociation de multiplexage de support avec le protocole de description de session (SDP)", janvier 2021. (*P.S. ; MàJ RFC 3264, 5888, 7941*) (DOI : 10.17487/RFC8843)

## Remerciements

De nombreuses personnes du groupe de travail IETF Multiparty Multimedia Session Control (MMUSIC) ont fait des commentaires et suggestions qui ont contribué au présent document.

Nous tenons en particulier à remercier les personnes suivantes qui ont contribué à la création de ce document ou d'un de ses prédécesseurs : Adam Roach, Allison Mankin, Bernie Hoeneisen, Bill Fenner, Carsten Bormann, Eve Schooler, Flemming Andreassen, Gonzalo Camarillo, Jörg Ott, John Elwell, Jon Peterson, Jonathan Lennox, Jonathan Rosenberg, Keith Drage, Peter Parnes, Rob Lanphier, Ross Finlayson, Sean Olson, Spencer Dawkins, Steve Casner, Steve Hanna, Van Jacobson.

## Adresses des auteurs

Ali Begen  
Networked Media  
Turkey  
mél : [ali.begen@networked.media](mailto:ali.begen@networked.media)

Paul Kyzivat  
United States of America  
mél : [pkyzivat@alum.mit.edu](mailto:pkyzivat@alum.mit.edu)

Colin Perkins  
University of Glasgow  
School of Computing Science  
Glasgow G12 8QQ  
United Kingdom  
mél : [csp@csperskins.org](mailto:csp@csperskins.org)

Mark Handley  
University College London  
Department of Computer Science  
London WC1E 6BT  
United Kingdom  
mél : [M.Handley@cs.ucl.ac.uk](mailto:M.Handley@cs.ucl.ac.uk)