

Groupe de travail Réseau
Request for Comments : 4145
 Catégorie : En cours de normalisation

D. Yon, Tactical Software, LLC
 G. Camarillo, Ericsson
 septembre 2005
 Traduction Claude Brière de L'Isle

Transport de supports fondé sur TCP dans le protocole de description de session (SDP)

Statut de ce mémoire

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

Notice de copyright

Copyright (C) The Internet Society (2005).

Résumé

Le présent document décrit comment exprimer le transport de supports sur TCP en utilisant le protocole de description de session (SDP, *Session Description Protocol*). Il définit l'identifiant de protocole 'TCP' de SDP, l'attribut SDP 'setup', qui décrit la procédure d'établissement de connexion, et l'attribut SDP 'connection', qui traite le rétablissement de connexion.

Table des Matières

| | |
|--|---|
| 1. Introduction..... | 1 |
| 2. Terminologie..... | 2 |
| 3. Identifiant de protocole..... | 2 |
| 4. Attribut Setup..... | 2 |
| 4.1 Attribut Setup dans le modèle Offre/réponse..... | 2 |
| 5. Attribut Connection..... | 3 |
| 5.1 Comportement de l'offreur..... | 3 |
| 5.2 Comportement du répondeur..... | 4 |
| 6. Gestion de connexion..... | 4 |
| 6.1 Établissement de connexion..... | 4 |
| 6.2 Rétablissement de connexion..... | 5 |
| 6.3 Terminaison de connexion..... | 5 |
| 7. Exemples..... | 5 |
| 7.1 Passif/actif..... | 5 |
| 7.2 Actpass/Passive..... | 5 |
| 7.3 Réutilisation d'une connexion existante..... | 6 |
| 7.4 Refus d'une connexion existante..... | 6 |
| 8. Autres protocoles de transport en mode connexion..... | 6 |
| 9. Considérations pour la sécurité..... | 7 |
| 10. Considérations relatives à l'IANA..... | 7 |
| 11. Remerciements..... | 7 |
| 12. Références..... | 7 |
| 12.1 Références normatives..... | 7 |
| 12.2 Références pour information..... | 8 |
| Adresse des auteurs..... | 8 |
| Déclaration complète de droits de reproduction..... | 8 |

1. Introduction

Le protocole de description de session [RFC2327] fournit un format général pour décrire les sessions multimédia en annonces ou invitations. SDP utilise un format de données entièrement textuel (le sous ensemble US-ASCII de l'UTF-8 [RFC3629]) pour maximiser la portabilité parmi les transports. SDP ne définit pas un protocole ; il définit la syntaxe pour décrire une session multimédia avec des informations suffisantes pour participer à cette session. Les descriptions de session peuvent être envoyées en utilisant des protocoles d'application arbitraires existants pour le transport (par exemple, SAP

[RFC2974], SIP [RFC3261], RTSP [RFC2326], la messagerie électronique, HTTP [RFC2616], etc.).

SDP [RFC2327] définit deux identifiants de protocole : RTP/AVP et UDP, qui représentent tous deux des protocoles non fiables, sans connexion. Bien que ces transports soient des choix appropriés pour les flux multimédia, il y a des applications pour lesquelles TCP est plus approprié. Le présent document définit un nouvel identifiant de protocole, 'TCP', pour décrire les connexions TCP dans SDP.

TCP introduit deux nouveaux facteurs qui décrivent une session : comment et quand les points d'extrémité devraient effectuer la procédure d'établissement de connexion TCP. Le présent document définit deux nouveaux attributs pour décrire l'établissement des connexions TCP : 'setup' et 'connection'.

2. Terminologie

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] et ils indiquent les niveaux d'exigence pour les mises en œuvre conformes.

3. Identifiant de protocole

Voici l'ABNF pour une ligne 'm', comme spécifié par la [RFC2327].

```
media-field = "m=" media space port ["/" integer] space proto 1*(space fmt) CRLF
```

Le présent document définit une nouvelle valeur pour le champ proto : 'TCP'.

L'identifiant de protocole 'TCP' est similaire à l'identifiant de protocole 'UDP' en ce qu'il décrit seulement le protocole de transport, et non le protocole de couche supérieure. Une ligne 'm' qui spécifie 'TCP' DOIT de plus qualifier le protocole de couche application en utilisant un identifiant fmt. Les supports décrits en utilisant une ligne 'm' qui contient l'identifiant de protocole 'TCP' sont portés avec TCP [RFC0793].

4. Attribut Setup

L'attribut 'setup' indique lequel des points d'extrémité devrait initier l'établissement de la connexion TCP (c'est-à-dire, envoyer le SYN TCP initial). L'attribut 'setup' est indépendant du jeu de caractères et peut être un attribut de niveau session ou de niveau support. Voici l'ABNF de l'attribut 'setup' :

```
setup-attr = "a=setup:" role
role = "active" / "passive" / "actpass" / "holdconn"
'active' : le point d'extrémité va initier une connexion sortante.
```

'passive' : le point d'extrémité va accepter une connexion entrante.

'actpass' : le point d'extrémité veut accepter une connexion entrante ou initier une connexion sortante.

'holdconn' : le point d'extrémité ne veut pas que la connexion soit établie pour l'instant.

4.1 Attribut Setup dans le modèle Offre/réponse

Le modèle d'offre/réponse, défini dans la [RFC3264], donne aux points d'extrémité un moyen d'obtenir une vue partagée d'une session. Certains paramètres de session sont négociés (par exemple, les codecs à utiliser) tandis que d'autres sont simplement communiqués d'un point d'extrémité à l'autre (par exemple, les adresses IP). La valeur de l'attribut 'setup' entre dans la première catégorie. C'est-à-dire que les deux points d'extrémité négocient sa valeur en utilisant le modèle offre/réponse.

La négociation de la valeur de l'attribut 'setup' a lieu comme suit. L'offreur déclare quels rôles il veut jouer, et le répondeur; prenant en compte les volontés de l'offreur, choisit quels rôles les deux points d'extrémité vont en fait jouer durant l'établissement de la connexion. Voici les valeurs que l'attribut 'setup' peut prendre dans un échange offre/réponse :

| Offre | Réponse |
|----------|---------------------------|
| actif | passif / holdconn |
| passif | actif / holdconn |
| actpass | actif / passif / holdconn |
| holdconn | holdconn |

Le point d'extrémité actif DEVRAIT initier une connexion au numéro d'accès sur la ligne 'm' de l'autre point d'extrémité. Le numéro d'accès sur sa propre ligne 'm' n'est pas pertinent, et le point d'extrémité opposé NE DOIT PAS tenter d'initier une connexion au numéro d'accès qui y est spécifié. Néanmoins, comme la ligne 'm' doit contenir un numéro d'accès valide, le point d'extrémité qui utilise la valeur 'active' DEVRAIT spécifier un numéro d'accès de 9 (l'accès d'élimination) sur sa ligne 'm'. Le point d'extrémité NE DOIT PAS spécifier un numéro d'accès de zéro, sauf pour noter une ligne 'm' qui a été ou est en train d'être refusée.

Le point d'extrémité passif DEVRAIT être prêt à accepter une connexion sur le numéro d'accès spécifié dans la ligne 'm'.

Une valeur de 'actpass' indique que l'offreur peut soit initier une connexion au numéro d'accès de la ligne 'm' dans la réponse, soit accepter une connexion sur le numéro d'accès spécifié dans la ligne 'm' de l'offre. C'est à dire que l'offreur n'a pas de préférence quant au fait d'accepter ou d'initier la connexion et donc qu'il laisse le choix à celui qui répond.

Une valeur de 'holdconn' indique que la connexion ne devrait pas être établie pour l'instant.

La valeur par défaut de l'attribut setup dans un échange offre/réponse est 'active' dans l'offre et 'passive' dans la réponse.

5. Attribut Connection

La description précédente de l'attribut 'setup' est placée dans le contexte de l'utilisation de SDP pour initier une session. SDP peut encore être échangé entre les points d'extrémité à diverses étapes d'une session pour accomplir des tâches comme terminer une session, rediriger des supports sur un nouveau point d'extrémité, ou renégocier les paramètres de supports pour une session. Après l'établissement initial de session, il peut être ambigu qu'un échange SDP suivant représente une confirmation que le point d'extrémité veut continuer d'utiliser la connexion TCP courante inchangée, ou si c'est une demande de faire une nouvelle connexion TCP. L'attribut 'connection' de niveau support, qui est indépendant du jeu de caractères, est utilisé pour lever l'ambiguïté entre ces deux scénarios. Voici l'ABNF de l'attribut connection :

```
connection-attr = "a=connection:" conn-valeur
conn-valeur = "new" / "existing"
```

5.1 Comportement de l'offreur

Offreurs et répondeurs utilisent l'attribut 'connection' pour décider si une nouvelle connexion de transport doit être établie ou, d'un autre côté, si la connexion TCP existante devrait encore être utilisée. Lorsque un offreur génère une ligne 'm' qui utilise TCP, il DEVRAIT fournir un attribut de connexion pour la ligne 'm' sauf si l'application qui utilise la ligne 'm' a d'autres moyens de traiter le rétablissement de connexion.

Après l'échange offre/réponse initial, tout point d'extrémité peut générer une nouvelle offre de changer des caractéristiques de la session (par exemple, l'attribut de direction). Si cet offreur veut continuer d'utiliser la connexion de couche transport établie précédemment pour la ligne 'm', l'offreur DOIT utiliser une valeur de connexion de 'existing' pour la ligne 'm'. Si d'un autre côté, l'offreur veut établir une nouvelle connexion de couche transport pour la ligne 'm', il DOIT utiliser une valeur de connexion de 'new'.

Noter que, selon les règles de cette section, une offre qui change l'adresse de transport (adresse IP ou numéro d'accès) d'une ligne 'm' aura une valeur de connexion de 'new'. De même, l'attribut 'connection' dans une offre initiale (c'est-à-dire qu'aucune connexion de transport n'a encore été établie) prend la valeur 'new'.

La valeur 'connection' résultant d'un échange offre/réponse est la valeur 'connection' de la réponse. Si la valeur 'connection' de la réponse est 'new', les points d'extrémité DEVRAIENT établir une nouvelle connexion. Si la valeur de connexion dans la réponse est 'existing', les points d'extrémité DEVRAIENT continuer d'utiliser la connexion existante.

Prenant en considération les règles du paragraphe 5.2, les valeurs que l'attribut 'connection' peut prendre dans un échange offre/réponse sont les suivantes :

| Offre | Réponse |
|--------------|----------------|
| new | new |
| existing | existing / new |

Si la valeur de connexion résultant d'un échange offre/réponse est 'existing', les points d'extrémité continuent d'utiliser la connexion existante. Par conséquent, les numéros d'accès, les adresses IP, et les attributs 'setup' négociés dans l'échange offre/réponse seront ignorés parce que il n'y a pas besoin d'établir une nouvelle connexion.

La règle précédente implique qu'un offreur qui génère une offre d'une valeur de connexion de 'existing' et une valeur d'établissement de 'passive' doit être prêt (c'est-à-dire, il doit allouer des ressources) pour recevoir une demande de connexion provenant du répondeur juste au cas où le répondeur choisirait une valeur de connexion de 'new' pour la réponse. Cependant, si le répondeur utilise une valeur de connexion de 'existing' dans la réponse, l'offreur aura besoin de désallouer les ressources précédemment allouées qui n'auront jamais été utilisées parce que aucune demande de connexion n'aura été reçue.

Pour éviter d'allouer inutilement des ressources, les offreurs qui utilisent une valeur de connexion de 'existing' dans leurs offres peuvent choisir d'utiliser une valeur d'établissement de 'holdconn'. Néanmoins, les offreurs qui utilisent cette tactique devraient avoir conscience que si le répondeur choisit une valeur de connexion de 'new', un nouvel échange offre/réponse (normalement initié par l'offreur précédent) va établir une valeur différente de 'holdconn', et il sera nécessaire d'établir une nouvelle connexion. Cela peut, bien sûr, causer des délais dans l'application qui utilise la connexion TCP.

La valeur par défaut de l'attribut de connexion chez les offreurs et les répondeurs est 'new'.

5.2 Comportement du répondeur

La valeur de connexion pour une ligne 'm' est négociée en utilisant le modèle offre/réponse. La valeur de connexion résultante après un échange offre/réponse est la valeur de connexion dans la réponse. Si la valeur de connexion dans l'offre est 'new', le répondeur DOIT aussi utiliser une valeur de 'new' dans la réponse. Si la valeur de connexion dans l'offre est 'existing', le répondeur utilise une valeur de 'existing' dans la réponse si il souhaite continuer à utiliser la connexion existante et une valeur de 'new' si il veut qu'une nouvelle connexion soit établie.

Dans certains scénarios où est utilisé un contrôle d'appel par un tiers [RFC3725], un point d'extrémité peut recevoir une offre initiale avec une valeur de connexion de 'existing'. Suivant les règles précédentes, un tel répondeur va utiliser une valeur de connexion de 'new' dans la réponse.

Si la valeur de connexion pour une ligne 'm' résultant d'un échange offre/réponse est 'new', les points d'extrémité DEVRAIENT établir une nouvelle connexion TCP comme indiqué par l'attribut 'setup'. Si une connexion TCP antérieure est encore active, les points d'extrémité DEVRAIENT la clore aussitôt que l'échange offre/réponse est achevé. Il appartient à l'application de s'assurer d'une synchronisation appropriée des données entre les deux connexions TCP.

Si la valeur de connexion pour une ligne 'm' résultant d'un échange offre/réponse est 'existing', les points d'extrémité DEVRAIENT continuer d'utiliser la connexion TCP existante.

6. Gestion de connexion

Cette section vise l'établissement de connexion, le rétablissement de connexion, et la terminaison de connexion.

6.1 Établissement de connexion

Un point d'extrémité qui selon un échange offre/réponse est supposé initier une nouvelle connexion TCP DEVRAIT l'initier aussitôt qu'il est capable de le faire, même si le point d'extrémité n'a pas l'intention de commencer immédiatement à envoyer des supports au point d'extrémité distant. Cela permet aux supports de s'écouler à partir du point d'extrémité distant si nécessaire.

Noter que certains points d'extrémité ont besoin d'attendre qu'un événement se produise avant d'être capables d'établir la connexion. Par exemple, un terminal sans fil peut avoir besoin d'établir une porteuse radio avant d'être capable d'initier une connexion TCP.

6.2 Rétablissement de connexion

Si un point d'extrémité détermine que le TCP pour une ligne 'm' a été clos et devrait être rétabli, il DEVRAIT effectuer un nouvel échange offre/réponse en utilisant une valeur de connexion de 'new' pour cette ligne 'm'.

Noter que l'attribut SDP direction (par exemple, 'a=sendonly') traite des supports envoyés sur la connexion TCP, mais n'a pas d'impact sur la connexion TCP elle-même.

6.3 Terminaison de connexion

Normalement, les points d'extrémité ne ferment pas la connexion TCP avant que la session ait expiré, étant alors explicitement terminée, ou une nouvelle valeur de connexion a été fournie pour la ligne 'm'. De plus, des applications spécifiques peuvent en décrire plus des scénarios où un point d'extrémité peut clore une certaine connexion TCP (par exemple, chaque fois qu'une connexion est dans l'état moitié fermé). Aussitôt qu'un point d'extrémité remarque qu'il a besoin de terminer une connexion TCP, il DEVRAIT le faire.

Dans tous les cas, les applications individuelles peuvent s'intéresser de plus près à la façon de réaliser une terminaison de connexion en douceur. Par exemple, une application de fichiers qui utilise TCP pour recevoir un FIN du point d'extrémité distant peut avoir besoin de finir la transmission en cours d'un fichier avant d'envoyer son propre FIN.

7. Exemples

Les exemples qui suivent montre l'usage le plus courant de l'attribut 'setup' combiné aux descriptions de supports fondées sur TCP. Pour faire court, la portion principale de la description de session est omise dans les exemples, avec seulement les lignes 'm' montrées avec leurs attributs (incluant les lignes 'c').

7.1 Passif/actif

Un offreur à 192.0.2.2 signale sa disponibilité pour une session de télécopie T.38 à l'accès 54111 :

```
m=image 54111 TCP t38
c=IN IP4 192.0.2.2
a=setup:passive
a=connection:new
```

Un répondeur à 192.0.2.1 qui reçoit cette offre répond de la façon suivante :

```
m=image 9 TCP t38
c=IN IP4 192.0.2.1
a=setup:active
a=connection:new
```

Le point d'extrémité à 192.0.2.1 initie alors la connexion TCP à l'accès 54111 avec 192.0.2.2.

7.2 Actpass/Passive

Dans un autre exemple, un offreur à 192.0.2.2 signale sa disponibilité pour une session de télécopie T.38 à l'accès TCP 54111. De plus, cet offreur est aussi d'accord pour établir le flux de supports en initiant la connexion TCP:

```
m=image 54111 TCP t38
c=IN IP4 192.0.2.2
a=setup:actpass
a=connection:new
```

Le point d'extrémité à 192.0.2.1 répond par la description suivante :

```
m=image 54321 TCP t38
c=IN IP4 192.0.2.1
a=setup:passive
a=connection:new
```

Cela va amener l'offreur (à 192.0.2.2) à initialiser une connexion à l'accès 54321 avec 192.0.2.1.

7.3 Réutilisation d'une connexion existante

Suite à l'échange du paragraphe 7.2, un autre échange offre/réponse est initié dans la direction opposée. Le point d'extrémité à 192.0.2.1 souhaite continuer d'utiliser la connexion existante :

```
m=image 54321 TCP t38
c=IN IP4 192.0.2.1
a=setup:passive
a=connection:existing
```

Le point d'extrémité à 192.0.2.2 souhaite aussi utiliser la connexion existante et répond par la description suivante :

```
m=image 9 TCP t38
c=IN IP4 192.0.2.2
a=setup:active
a=connection:existing
```

La connexion existante de 192.0.2.2 à 192.0.2.1 sera réutilisée.

Noter que le point d'extrémité à 192.0.2.2 utilise 'setup:active' en réponse à l'offre de 'setup:passive', et utilise l'accès 9 parce qu'il est actif.

7.4 Refus d'une connexion existante

Suite à l'échange du paragraphe 7.3, un autre échange offre/réponse est initié par le point d'extrémité à 192.0.2.2, souhaitant là encore réutiliser la connexion existante :

```
m=image 54111 TCP t38
c=IN IP4 192.0.2.2
a=setup:passive
a=connection:existing
```

Cependant, cette fois le répondeur ne connaît pas l'ancienne connexion et souhaite donc en établir une nouvelle. (Cela pourrait résulter d'un transfert via un contrôle d'appel de tiers.) Il n'est pas capable d'agir dans le mode 'passive' et répond donc comme 'active' :

```
m=image 9 TCP t38
c=IN IP4 192.0.2.3
a=setup:active
a=connection:new
```

Le point d'extrémité à 192.0.2.3 initie alors la connexion TCP à l'accès 54111 à 192.0.2.2, et le point d'extrémité à 192.0.2.2 clôt la vieille connexion.

Noter que le point d'extrémité à 192.0.2.2, tout en utilisant une valeur de connexion de 'existing', a utilisé une valeur d'établissement de 'passive'. S'il n'avait pas fait cela et avait plutôt utilisé une valeur d'établissement de 'holdconn' (probablement pour éviter d'allouer des ressources comme décrit au paragraphe 5.1) un nouvel échange offre/réponse aurait été nécessaire afin d'établir la nouvelle connexion.

8. Autres protocoles de transport en mode connexion

Le présent document spécifie comment décrire des flux de supports fondés sur TCP en utilisant SDP. Il reste néanmoins que certains des attributs définis ici pourraient être utilisés pour décrire aussi des flux de supports fondés sur d'autres protocoles de transport en mode connexion. Cette Section donne des avis aux auteurs de spécifications d'extensions à SDP qui traitent de protocoles de transport en mode connexion autres que TCP.

Il est recommandé que les documents qui définissent de nouveaux identifiants de protocole SDP qui impliquent des

couches de protocole supplémentaires entre TCP et le support lui-même (par exemple, TLS [RFC2246] sur TCP) les fassent commencer par la chaîne 'TCP/' (par exemple, 'TCP/TLS').

Les attributs 'setup' et 'connection' sont spécifiés respectivement à la Section 4 et à la Section 5. Bien que les deux attributs soient applicables aux lignes 'm' qui utilisent l'identifiant de protocole 'TCP', ils sont assez généraux pour être réutilisés dans les lignes 'm' avec d'autres protocoles de transport en mode connexion. Donc, il est recommandé que les attributs 'setup' et 'connection' soient réutilisés, autant qu'il est possible, pour les nouvelles valeurs 'proto' associées aux protocoles de transport en mode connexion.

La Section 6 traite de la gestion des connexions TCP. On devrait noter qu'alors que dans TCP les deux points d'extrémité doivent clore une connexion, d'autres protocoles de transport en mode connexion peuvent n'avoir pas le concept de connexion à moitié close. Dans ce cas, une connexion serait terminée aussitôt que les points d'extrémité la ferment, rendant inutile que l'autre point d'extrémité effectue d'autre action pour terminer la connexion. Ainsi, les spécifications qui traitent de tels protocoles de transport peuvent devoir spécifier des procédures légèrement différentes en ce qui concerne la terminaison de connexion.

9. Considérations pour la sécurité

Voir la [RFC2327] pour les considérations sur la sécurité et autres spécifiques du protocole de description de session en général.

Un attaquant peut tenter de modifier les valeurs des attributs 'connection' et 'setup' afin que les points d'extrémité rétablissent inutilement des connexions ou pour les empêcher d'établir une connexion. Donc, il est fortement RECOMMANDÉ que la protection d'intégrité soit appliquée aux descriptions de session SDP. Pour les descriptions de session portées dans SIP [RFC3261], S/MIME est le choix naturel pour fournir une telle protection d'intégrité de bout en bout, comme décrit dans la [RFC3261]. D'autres applications PEUVENT utiliser une forme différente de protection de l'intégrité.

10. Considérations relatives à l'IANA

Le présent document définit deux attributs SDP de niveau session et de niveau support : setup et connection. Leur format est défini respectivement à la Section 4 et à la Section 5. Ces deux attributs devraient être enregistrés par l'IANA sous "Paramètres du protocole de description de session (SDP)" à "att-field (aux deux niveaux session et media)".

Le présent document définit une valeur proto : TCP. Son format est défini à la Section 3. Cette valeur proto devrait être enregistrée par l'IANA sous "Paramètres du protocole de description de session (SDP)" à "proto".

La spécification de SDP, RFC2327, déclare que les spécifications qui définissent de nouvelles valeurs de protocoles, comme la valeur TCP 'proto' définie dans la présente RFC, doivent définir les règles selon lesquelles leur espace de noms de format de support (fmt) est géré. Pour le protocole TCP, les nouveaux formats DEVRAIENT avoir un enregistrement MIME associé. L'utilisation d'un sous type MIME existant pour le format est encouragée. Si aucun sous type MIME n'existe, il est RECOMMANDÉ qu'il en soit enregistré un convenable par le processus de l'IETF [RFC2048] par production, ou référence à, une RFC sur la voie de la normalisation qui définisse le protocole de transport pour ce format.

11 Remerciements

Jonathan Rosenberg, Rohan Mahy, Anders Kristensen, Joerg Ott, Paul Kyzivat, Robert Fairlie-Cuninghame, Colin Perkins, et Christer Holmberg ont fourni de précieux apports et contributions.

12. Références

12.1 Références normatives

[RFC0793] J. Postel (éd.), "Protocole de [commande de transmission](#) – Spécification du protocole du programme Internet DARPA", STD 7, septembre 1981.

- [RFC2048] N. Freed, J. Klensin et J. Postel, "Extensions multi-objets de la messagerie Internet (MIME) Partie 4 : Procédures d'enregistrement", BCP 13, novembre 1996. (*Rendue obsolète par les RFC [4288-4289](#)*)
- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. (*MàJ par [RFC8174](#)*)
- [RFC2327] M. Handley et V. Jacobson, "SDP : [Protocole de description de session](#)", avril 1998. (*Obsolète; voir [RFC4566](#)*)
- [RFC3264] J. Rosenberg et H. Schulzrinne, "[Modèle d'offre/réponse](#) avec le protocole de description de session (SDP)", juin 2002.

12.2 Références pour information

- [RFC2246] T. Dierks et C. Allen, "[Protocole TLS version 1.0](#)", janvier 1999. (*P.S. ; MàJ par [RFC7919](#)*)
- [RFC2326] H. Schulzrinne, A. Rao et R. Lanphier, "Protocole de [flux directs en temps réel](#) (RTSP)", avril 1998. (*Remplacée par [RFC7826](#)*)
- [RFC2616] R. Fielding et autres, "[Protocole de transfert hypertexte](#) -- HTTP/1.1", juin 1999. (*D.S., MàJ par [2817](#), [6585](#)*)
- [RFC2974] M. Handley, C. Perkins, E. Whelan, "Protocole d'annonce de session (SAP)", octobre 2000. (*Expérimentale*)
- [RFC3261] J. Rosenberg et autres, "SIP : [Protocole d'initialisation de session](#)", juin 2002. (*Mise à jour par [RFC3265](#), [RFC3853](#), [RFC4320](#), [RFC4916](#), [RFC5393](#), [RFC6665](#), [RFC8217](#)*)
- [RFC3629] F. Yergeau, "[UTF-8, un format de transformation](#) de la norme ISO 10646", STD 63, novembre 2003.
- [RFC3725] J. Rosenberg et autres, "Bonne pratiques actuelles [pour la commande d'appel de tiers \(3pcc\)](#) dans le protocole d'initialisation de session (SIP)", avril 2004. ([BCP0085](#))

Adresse des auteurs

David Yon
Tactical Software, LLC
1750 Elm St., Suite 803
Manchester, NH 03104
USA
mél : yon-comedia@rfdsoftware.com

Gonzalo Camarillo
Ericsson
Hirsalantie 11
Jorvas 02420
Finland
mél : Gonzalo.Camarillo@ericsson.com

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2005).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations y contenues sont fournies sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci-encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourrait être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à <http://www.ietf.org/ipr>.

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

Remerciement

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