Groupe de travail Réseau
Request for Comments : 3959
Catégorie : En cours de normalisation

G. Camarillo, Ericsson
décembre 2004
Traduction Claude Brière de L'Isle

Type de disposition Session précoce pour le protocole d'initialisation de session (SIP)

Résumé
Le présent document définit un nouveau type de disposition (session précoce) pour le champ d'en-tête Disposition de contenu dans le protocole d'initialisation de session (SIP, *Session Initiation Protocol*). Le traitement des corps "session précoce" est similaire au traitement des corps "session". C'est-à-dire qu'ils suivent le modèle offre/réponse. La seule différence est que les descriptions de session dont le type de disposition est "session précoce" sont utilisés pour établir des sessions de support précoces au sein de dialogues précoces, par opposition aux sessions régulières au sein des dialogues réguliers.

Table des Matières

1. Introduction....1
2. Terminologie....2
3. Questions relatives à l'établissement d'une session de support précoce....2
4. Type de disposition Session précoce....3
5. Préconditions....3
6. Étiquette d'option....3
7. Exemple....3
8. Considérations sur la sécurité....5
9. Considérations relatives à l'IANA....5
10. Remerciements....6
11. Références....6
11.1 Références normatives....6
11.2 Références pour information....6
Adresse de l'auteur....6
Déclaration complète de droits de reproduction....6

1. Introduction

Support précoce se réfère aux supports (par exemple, audio et vidéo) qui sont échangés avant qu'une session particulière soit acceptée par l'usager demandé. Au sein d'un dialogue, le support précoce se produit à partir du moment où l'INVITE initial est envoyé jusqu'à ce que le serveur d'agent d'utilisateur (UAS, *User Agent Server*) génère une réponse finale. Il peut être unidirectionnel ou bidirectionnel, et peut être généré par l'appelant, l'appelé, ou les deux. Des exemples typiques de support précoce généré par l'appelant sont les tonalités et annonces d'appel (par exemple, l'état de mise en file d'attente). Les supports précoces générés par l'appelant consistent normalement en commandes vocales ou en bitonalités multifréquences (DTMF, *dual tone multi-frequency*) pour piloter des systèmes à réponse vocale interactive (IVR, *interactive voice response*).

La spécification SIP de base [RFC3261] ne prend en charge que des mécanismes de support précoce très simples. Ces mécanismes simple posent un certain nombre de problèmes relatifs au fourchement et à la sécurité, et ne satisfont pas aux exigences de la plupart des applications. La [RFC3960] va au delà des mécanismes définis dans la [RFC3261] et décrit

deux modèles de support précoce qui utilisent SIP : le modèle passerelle et le modèle de serveur d'application.

Bien que les deux modèles de support précoce décrits dans la [RFC3960] soient supérieurs à celui spécifié dans la [RFC3261], le modèle passerelle pose quand même une série de problèmes. En particulier, le modèle passerelle ne fonctionne pas bien avec le fourchement. Néanmoins, le modèle passerelle est nécessaire parce que certaines entités SIP (en particulier, certaines passerelles) ne peuvent pas mettre en œuvre le modèle serveur d'application.

Le modèle serveur d'application résout certains des problèmes présents dans le modèle de la passerelle. Ce modèle utilise le type de disposition de session précoce spécifié dans le présent document.

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 la [RFC2119] et indiquent les niveaux d'exigence pour les mises en œuvre conformes.

3. Questions relatives à l'établissement d'une session de support précoce

Traditionnellement, les sessions de support précoce ont été établies de la même façon que les sessions régulières. C'est-à-dire en utilisant un échange offre/réponse où le type de disposition des descriptions de session est "session". Les serveurs d'application effectuent un échange d'offre/réponse avec le client d'agent d'utilisateur (UAC, *User Agent Client*) pour échanger exclusivement des supports précoces, tandis que les UAS utilisent le même échange d'offre/réponse, d'abord pour échanger des supports précoces, et une fois que le dialogue régulier est établi, pour échanger des supports réguliers. La façon d'établir des sessions de support précoce est connue par le modèle de passerelle [RFC3960], qui pose certains problèmes relatifs au fourchement et à la sécurité. Ces problèmes existent lorsque ce modèle est utilisé par un serveur d'application ou par un UAS.

Les serveurs d'application peuvent n'être pas capables de générer une réponse à une offre reçue dans l'INVITE. L'UAC a créé l'offre pour l'UAS, et donc, il peut avoir appliqué un chiffrement de bout en bout ou avoir inclus des informations (par exemple, relatives à la gestion de clé) que le serveur d'application n'est pas supposé utiliser. Donc, les serveurs d'application ont besoin d'un moyen pour effectuer un échange d'offre/réponse avec l'UAC qui soit indépendant de l'échange d'offre/réponse entre les deux UA.

Les UAS utilisant l'échange d'offre/réponse qui vont porter des supports réguliers pour envoyer et recevoir des supports précoces peuvent causer une mutilation du support, comme décrit au paragraphe 2.1.1 de la [RFC3960]. Certains UAC ne peuvent pas recevoir de supports précoces de différents UAS en même temps. Donc, lorsque un INVITE fourche et que plusieurs UAS commencent à envoyer des supports précoces, l'UAC assourdit tous les UAS sauf un (qui est généralement choisi au hasard). Si l'UAS qui accepte l'INVITE (c'est-à-dire, envoie un 200 OK) a été assourdi, un nouvel échange d'offre/réponse est nécessaire pour le démutiser. Cela cause généralement la mutilation du support. Donc, les UAS ont besoin d'un moyen pour effectuer un échange d'offre/réponse avec l'UAC pour échanger des supports précoces qui soit indépendant de l'échange d'offre/réponse utilisé pour échanger des supports réguliers.

Une solution potentielle à ce besoin serait d'établir un dialogue différent en utilisant un URI acheminable mondialement pour effectuer un échange d'offre/réponse indépendant. Ce dialogue serait étiqueté comme dialogue pour supports précoces et serait en relation avec le dialogue d'origine à l'UAC. Cependant, effectuer tous les échanges d'offre/réponse au sein du dialogue original présente de nombreux avantages :

- c'est plus simple,
- cela ne pose pas de problème de synchronisation, parce que tous les dialogues précoces sont terminés lorsque la session est acceptée,
- cela n'exige pas d'URI acheminable mondialement,
- cela n'introduit pas de problème d'interaction de service par rapport aux services qui peuvent être appliqués à tort au nouveau dialogue,
- cela rend plus facile la gestion de pare-feu.

Cette façon d'effectuer les échanges d'offre/réponse pour les supports précoces est appelé "modèle de serveur d'application" dans la [RFC3960]. Ce modèle utilise le type de disposition Session précoce défini dans la section qui suit.

4. Type de disposition Session précoce

On définit un nouveau type de disposition pour le champ d'en-tête Content-Disposition *(disposition du contenu)* : early-session *(session précoce)*. Les agents d'utilisateur DOIVENT utiliser des corps de session précoce pour établir des sessions de supports précoces de la même façon qu'ils utilisent les corps de session pour établir les sessions régulières, comme décrit dans les [RFC3261] et [RFC3264]. En particulier, les corps de session précoces DOIVENT suivre le modèle d'offre/réponse et PEUVENT apparaître dans les mêmes messages comme le font les corps de session à l'exception des réponses 2xx pour les INVITE et les ACK. Néanmoins, il n'est PAS RECOMMANDÉ que soient incluses des offres précoces dans les INVITE parce que elles peuvent fourcher, et l'UAC pourrait recevoir plusieurs réponses précoces établissant des flux de supports précoces en gros au même moment. Aussi, l'utilisation de la même adresse de transport (adresse IP plus accès) dans un corps de session et dans un cops de session précoce n'est PAS RECOMMANDÉE. L'utilisation d'adresses de transport différentes (par exemple, des accès différents) pour recevoir des supports précoces et des supports réguliers rend plus facile la détection du début du support régulier.

Si un agent d'utilisateur (UA) a besoin de refuser une offre de session précoce, il DOIT le faire en refusant tous les flux de supports qu'elle contient. Lorsque on utilise SDP [RFC2327], ceci se fait en réglant le numéro d'accès de tous les flux de supports à zéro.

Les UAC utilisent le même mécanisme pour refuser les offres régulières qui arrivent en réponse à une INVITE vide.

Une session de supports précoces établie en utilisant un corps de session précoce DOIT se terminer lorsque son dialogue précoce correspondant se termine ou qu'il effectue sa transition en dialogue régulier.

Il est RECOMMANDÉ que les UA qui génèrent des descriptions de session régulière et précoce utilisent, pour autant qu'il soit possible, les mêmes codecs dans les deux. De cette façon, l'UA distant n'a pas besoin de changer de codec lorsque la session précoce se transforme en session régulière.

5. Préconditions

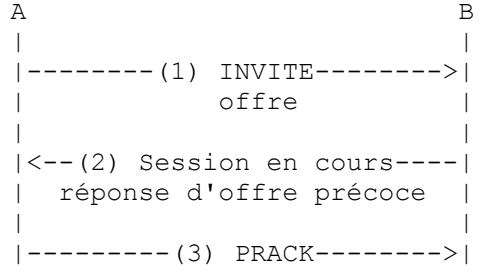
La [RFC3312] définit un cadre pour les préconditions dans SDP. Les sessions précoces PEUVENT contenir des préconditions, qui sont traitées de la même façon que les préconditions dans les sessions régulières. C'est-à-dire que les UA n'échangent pas de supports, et l'usager appelé n'est pas alerté tant que les préconditions ne sont pas satisfaites.

6. Étiquette d'option

On définit une étiquette d'option à utiliser dans les champs d'en-tête Require et Supported : early-session. Un UA qui ajoute l'étiquette d'option "early-session" à un message indique qu'il comprend le type de disposition "Session précoce".

7. Exemple

La Figure 1 montre le flux de messages entre deux UA. INVITE (1) a une étiquette d'option "early-session" dans son champ d'en-tête Supported et son corps montrés dans la Figure 2. L'UAS renvoie une réponse avec deux partie de corps, comme le montre la Figure 3 : une de type de disposition session et l'autre de session précoce. La partie de corps session est la réponse à l'offre dans le INVITE. La partie de corps session précoce est une offre d'établir une session de supports précoces. Quand l'UAC reçoit la réponse 183 (Session en cours) il renvoie la réponse à l'offre de session précoce dans un PRACK, comme le montre la Figure 4. Cette session de supports précoces se termine quand le dialogue précoce se transforme en dialogue régulier. C'est-à-dire quand l'UAS envoie la réponse (5) 200 (OK) à l'INVITE.



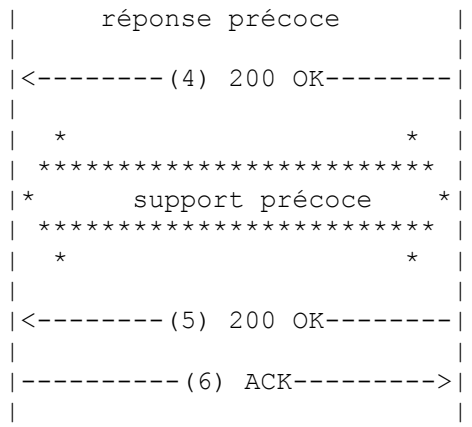


Figure 1 : Flux de message

```
Content-Type: application/sdp
Content-Disposition: session

v=0
o=alice 2890844730 2890844731 IN IP4 host.example.com
s=
c=IN IP4 192.0.2.1
t=0 0
m=audio 20000 RTP/AVP 0
```

Figure 2 : Offre

```
Content-Type: multipart/mixed; boundary="boundary1"
Content-Length: 401

--boundary1
Content-Type: application/sdp
Content-Disposition: session

v=0
o=Bob 2890844725 2890844725 IN IP4 host.example.org
s=
c=IN IP4 192.0.2.2
t=0 0
m=audio 30000 RTP/AVP 0

--boundary1
Content-Type: application/sdp
Content-Disposition: early-session

v=0
o=Bob 2890844714 2890844714 IN IP4 host.example.org
s=
c=IN IP4 192.0.2.2
t=0 0
m=audio 30002 RTP/AVP 0
--boundary1--
```

Figure 3 : Offre précoce et réponse

```
Content-Type: application/sdp
Content-Disposition: early-session

v=0
o=alice 2890844717 2890844717 IN IP4 host.example.com
s=
```

```
c=IN IP4 192.0.2.1
t=0 0
m=audio 20002 RTP/AVP 0
```

Figure 4 : Réponse précoce

8. Considérations sur la sécurité

Les implications de l'utilisation de corps de session précoces pour la sécurité dans SIP sont les mêmes que celles de l'utilisation d'un corps de session ; ils font partie du modèle d'offre/réponse.

SIP utilise le modèle d'offre/réponse [RFC3264] pour établir des sessions précoces dans les deux modèles de la passerelle et du serveur d'application. Les agents d'utilisateur (UA) génèrent une description de session, qui contient l'adresse de transport (c'est-à-dire, l'adresse IP plus l'accès) où ils veulent recevoir les supports, et l'envoient à leur homologue dans un message SIP. Lorsque les paquets de supports arrivent à cette adresse de transport, l'UA suppose qu'ils viennent du receveur du message SIP qui porte la description de session. Néanmoins, des attaquants peuvent tenter d'obtenir l'accès au contenu d'un message SIP et d'envoyer des paquets à l'adresse de transport contenue dans la description de session. Pour empêcher cette situation, les UA DEVRAIENT chiffrer leurs descriptions de session (par exemple, en utilisant S/MIME).

Cependant, même si un UA chiffre ses descriptions de session, un attaquant peut essayer de deviner l'adresse de transport utilisée par l'UA et d'envoyer des paquets de supports à cette adresse. Deviner une telle adresse de transport est parfois plus facile qu'il peut sembler parce que de nombreux UA prennent toujours le même accès de supports initial. Pour empêcher cette situation, les UA DEVRAIENT utiliser des mécanismes d'authentification au niveau du support (par exemple, le protocole de transport sécurisé en temps réel (SRTP, *Secure Realtime Transport Protocol*) [RFC3711]). De plus, les UA qui souhaitent garder confidentielles leurs communications DEVRAIENT utiliser des mécanismes de chiffrement de niveau support(par exemple , SRTP [RFC3711]).

Des attaquants peuvent tenter de faire qu'un UA envoie des supports à une victime au titre d'une attaque de DoS. Ceci peut être fait en envoyant une description de session avec l'adresse de transport de la victime à l'UA. Pour empêcher cette attaque, l'UA DEVRAIT engager une prise de contact avec le propriétaire de l'adresse de transport reçue dans une description de session (juste pour vérifier sa volonté de recevoir des supports) avant d'envoyer une grande quantité de données à l'adresse de transport. Cette vérification peut être effectuée en utilisant un protocole de transport en mode connexion, en utilisant STUN [RFC3489] de bout en bout, ou par l'échange de clés dans SRTP [RFC3711].

Dans tous les cas, on notera que les considérations précédentes sur la sécurité ne sont pas spécifiques du support précoce, mais s'appliquent à l'usage du modèle d'offre/réponse dans SIP pour établir des sessions en général.

De plus, un risque spécifique du support précoce (en gros, équivalent aux formes de "fraude au tarif" dans le RTPC) tente d'exploiter les différentes politiques tarifaires que certains opérateurs appliquent aux supports précoces et réguliers. Lorsque il est permis aux UA d'échanger gratuitement des supports précoces, mais doivent payer pour les sessions de support régulières, des UA malveillants peuvent essayer d'établir une session bidirectionnelle de support précoce et ne jamais envoyer de réponse 200 (OK) à l'INVITE.

D'un autre côté, certains serveurs d'applications (par exemple, les systèmes interactifs de réponse vocale) utilisent le support précoce bidirectionnel pour obtenir des informations de la part de l'appelant (par exemple, le code PIN d'une carte d'appel). Donc, on ne recommande pas que les opérateurs interdissent le support précoce bidirectionnel. À la place, les opérateurs devraient envisager comme remède la taxation des échanges de support précoce qui durent trop longtemps, ou de les arrêter au niveau du support (selon la politique de l'opérateur).

9. Considérations relatives à l'IANA

Le présent document définit un nouveau type de disposition de champ d'en-tête Content-Disposition (early-session) à la Section 4. Cette valeur a été enregistrée dans le registre de l'IANA pour Content-Dispositions avec la description suivante :

early-session : ce corps décrit une session de communications précoce, par exemple, un corps SDP de la RFC 2327

Le présent document définit une étiquette d'option SIP (early-session) à la Section 6. Elle a été enregistrée dans le registre des paramètres SIP (http://www.iana.org/assignments/sip-parameters) sous "Option Tags", avec la description suivante :

early-session : un UA qui ajoute une étiquette d'option session précoce à un message indique qu'il comprend la disposition de contenu early-session.

10. Remerciements

Francois Audet, Christer Holmberg, et Allison Mankin ont fourni d'utiles commentaires sur le présent document.

11. Références

11.1 Références normatives

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

[RFC3261] J. Rosenberg et autres, "SIP : Protocole d'initialisation de session", juin 2002. (*Mise à jour par* RFC3265, RFC3853, RFC4320, RFC4916, RFC5393, RFC6665)

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

[RFC3312] G. Camarillo, éd., "Intégration de la gestion de ressource et du protocole d'initialisation de session (SIP)", octobre 2002. (*MàJ par* RFC4032, RFC5027) *(P.S.)*

[RFC3489] J. Rosenberg et autres, "STUN - Simple traversée par le protocole de datagramme d'utilisateur (UDP) des traducteurs d'adresse réseau (NAT)", mars 2003. (*Obsolète, voir* RFC5389) *(P.S.)*

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

11.2 Références pour information

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

[RFC3960] G. Camarillo, H. Schulzrinne, "Support précoce et génération des tonalités d'appel dans le protocole d'initialisation de session (SIP)", décembre 2004. *(Information)*

Adresse de l'auteur

Gonzalo Camarillo
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

mél : Gonzalo.Camarillo@ericsson.com

Déclaration complète de droits de reproduction

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 pourraient 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 le 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 l'Internet Society