Groupe de travail Réseau
Request for Comments : 4571
Catégorie : Sur la voie de la normalisation

J. Lazzaro, UC Berkeley
juillet 2006
Traduction Claude Brière de L'Isle

Mise en trame de paquets du protocole de transport en temps réel (RTP) et du protocole de contrôle de RTP (RTCP) sur transport orienté connexion

Résumé
Le présent mémoire définit une méthode de tramage pour les paquets du protocole de transport en temps réel (RTP, *Real-time Transport Protocol*) et du protocole de commande de RTP (RTCP, *RTP Control Protocol*) sur un transport en mode connexion (comme TCP). Ce mémoire définit aussi comment les descriptions de session peuvent spécifier des flux RTP qui utilisent cette méthode de tramage.

Table des matières

1. Introduction

Le profil audio/vidéo (AVP, *Audio/Video Profile*) [RFC3550] pour le protocole de transport en temps réel (RTP, *Real-time Transport Protocol*) [RFC3551] ne définit pas de méthode pour tramer les paquets RTP et du protocole de contrôle RTP (RTCP, *RTP Control Protocol*) sur des protocoles de transport en mode connexion (comme TCP). Cependant, des versions antérieures de RTP/AVP définissaient une méthode de tramage, et cette méthode est utilisée dans plusieurs mises en œuvre.

Dans le présent mémoire, on documente la méthode de tramage qui a été définie par des versions antérieures de RTP/AVP. De plus, on introduit un mécanisme pour qu'une description de session [RFC4566] signale l'utilisation de la méthode de tramage. Noter que la signalisation de description de session pour la méthode de tramage est nouvelle et n'a pas été définie dans les versions antérieures de RTP/AVP.

1.1 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].

2. Méthode de tramage

La Figure 1 définit la méthode de tramage.

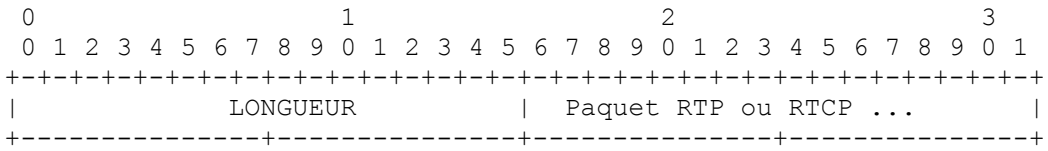

Figure 1 : définition des champs de bits de la méthode de tramage

Un champ LONGUEUR d'entier non signé de 16 bits, codé dans l'ordre des octets du réseau (gros boutien) commence la trame. Si LONGUEUR n'est pas zéro, un paquet RTP ou RTCP suit le champ LONGUEUR. La valeur codée dans le champ LONGUEUR DOIT être égale au nombre d'octets dans le paquet RTP ou RTCP. Zéro est une valeur valide pour LONGUEUR, et code le paquet nul.

Cette méthode de tramage n'utilise pas de marqueur de trame (c'est-à-dire, un octet de valeur constante qui précéderait le champ LONGUEUR). Les marqueurs de trame sont utiles pour détecter les erreurs dans le champ LONGUEUR. Au lieu d'un marqueur de trame, les receveurs DEVRAIENT surveiller les champs d'en-tête RTP et RTCP dont les valeurs sont prévisibles (par exemple, le numéro de version RTP). Voir des lignes directrices supplémentaires dans l'Appendice A.1 de la [RFC3550].

3. Propriétés du flux de paquets

À la plupart des égards, la méthode de tramage ne spécifie pas les propriétés au dessus du niveau d'un seul paquet. En particulier, la Section 2 ne spécifie pas ce qui suit :

Questions de bidirectionnalité
La Section 2 définit une méthode de tramage à utiliser dans une direction sur une connexion. La relation entre les paquets tramés qui s'écoulent dans une direction définie et dans la direction inverse n'est pas spécifiée.

Perte de paquet et changement d'ordre
La nature fiable d'une connexion n'implique pas qu'un flux RTP tramé a un ordre de numéros de séquence contigus. Par exemple, si la connexion est utilisée pour tunneler un flux UDP à travers un boîtier de médiation réseau qui ne passe que TCP, les numéros de séquence dans le flux tramé reflètent toutes les pertes de paquet ou les réarrangements sur la portion UDP du flux de bout en bout.

Sémantique de hors bande
La Section 2 ne définit pas de sémantique RTP ou RTCP pour clore une prise TCP, ou tout autre signal "hors bande" pour la connexion.

Les documents qui incluent normativement la méthode de tramage PEUVENT spécifier ces propriétés. Par exemple, la Section 4 du présent mémoire spécifie ces propriétés pour les sessions RTP/AVP spécifiées dans les descriptions de session.

À un égard, le protocole de tramage spécifie bien une propriété au dessus du niveau d'un seul paquet. Si une direction d'une connexion porte des paquets RTP, les flux portés dans cette direction DOIVENT prendre en charge l'utilisation de plusieurs sources de synchronisation (SSRC, *synchronization source*) dans ces paquets RTP. Si une direction d'une connexion porte des paquets RTCP, les flux portés dans cette direction DOIVENT prendre en charge l'utilisation de plusieurs SSRC dans ces paquets RTCP.

4. Descriptions de session pour RTP/AVP sur TCP

Les protocoles de gestion de session qui utilisent le protocole de description de session [RFC4566] en conjonction avec le protocole d'offre/réponse [RFC3264] DOIVENT utiliser les méthodes décrites dans la [RFC4145] pour établir des flux RTP/AVP sur TCP. Dans ce cas, l'utilisation de l'offre/réponse est EXICÉE, car les méthodes d'établissement décrites dans la [RFC4145] reposent sur l'offre/réponse.

En principe, la [RFC4145] est capable d'établir des sessions RTP pour tout profil RTP. En pratique, chaque profil a des problèmes uniques qui doivent être considérés quand la [RFC4145] est appliquée pour établir des flux pour le profil.

Dans le présent mémoire, on restreint l'objectif au profil audio/vidéo [RFC3551]. Ci-dessous, on définit une valeur de jeton "TCP/RTP/AVP" qui signale l'utilisation de RTP/AVP dans une session TCP. On définit aussi les procédures de fonctionnement que DOIT suivre un flux TCP/RTP/AVP.

On s'attend à ce que d'autres mémoires sur la voie de la normalisation apparaissent pour prendre en charge l'utilisation de la méthode de tramage avec d'autres profils RTP. Le document définissant un nouveau profil DOIT définir une valeur de jeton pour le profil, en utilisant le style utilisé pour AVP. Donc, pour le profil xyz, la valeur du jeton DOIT être "TCP/RTP/xyz". Le document DEVRAIT adopter les procédures de fonctionnement définies ci-dessous pour AVP, sauf si ces procédures se trouvaient d'une certaine façon incompatibles avec le profil.

Le reste de cette Section décrit comment établir et utiliser un flux AVP dans une session TCP. La Figure 2 montre la syntaxe d'une ligne de support (m=) [RFC4566] d'une description de session :

"m=" support SP accès ["/" entier] SP proto 1*(SP fmt) CRLF

Figure 2 : Syntaxe d'une ligne de support SDP (m=) (d'après la [RFC4566])

La valeur du jeton <proto> "TCP/RTP/AVP" spécifie un flux RTP/AVP [RFC3550], [RFC3551] qui utilise la méthode de tramage sur TCP.

Le jeton <fmt> qui suit <proto> DOIT être un entier non signé unique dans la gamme de 0 à 127. Les jetons <fmt> spécifient un type de charge utile RTP associé au flux.

À tous les autres égards, la syntaxe de description de session pour la méthode de tramage est identique à celle de la [RFC4145].

Le champ <accès> TCP sur la ligne de supports porte les paquets RTP. Si un flux de supports utilise RTCP, une seconde connexion porte les paquets RTCP. L'accès pour la connexion RTCP est choisi en utilisant les algorithmes définis dans la [RFC4566] ou par le mécanisme défini dans la [RFC3605].

Le connexions TCP PEUVENT porter du trafic bidirectionnel, suivant la sémantique définie dans la [RFC4145]. Les deux directions d'une connexion DOIVENT porter le même type de paquets (RTP ou RTCP). Les paquets DOIVENT exclusivement coder les flux RTP ou RTCP spécifiés sur la ou les lignes de supports associées à la connexion.

Comme noté dans la [RFC3550], l'utilisation de RTP sans RTCP est fortement déconseillée. Cependant, si un envoyeur ne souhaite pas envoyer des paquets RTCP dans une session de supports, il DOIT ajouter les lignes "b=RS:0" ET "b=RR:0" à la description des supports (d'après la [RFC3556]).

Si les descriptions de session de l'offre ET de la réponse contiennent toutes deux les lignes "b=RS:0" ET "b=RR:0", un flux RTCP TCP pour la session de supports NE DOIT PAS être créé par l'un ou l'autre des points d'extrémité de la session. Dans tous les autres cas, les points d'extrémité DOIVENT établir deux connexions TCP pour un flux RTP/AVP, un pour RTP et un pour RTCP.

Comme décrit dans la [RFC3264], l'utilisation de l'attribut "sendonly" ou "sendrecv" dans une offre (ou réponse) indique que l'offreur (ou répondant) a l'intention d'envoyer des paquets RTP sur la connexion RTP TCP. L'utilisation des attributs "recvonly" ou "sendrecv" dans une offre (ou réponse) indique que l'offreur (ou répondant) souhaite recevoir des paquets RTP sur la connexion RTP TCP.

5. Exemple

Les descriptions de session des Figures 3 et 4 définissent une session TCP RTP/AVP.

```
v=0
o=first 2520644554 2838152170 IN IP4 first.example.net
s=Example
t=0 0
c=IN IP4 192.0.2.105
m=audio 9 TCP/RTP/AVP 11
a=setup:active
a=connection:new
```

Figure 3 : description de session TCP pour le premier participant

```
v=0
o=second 2520644554 2838152170 IN IP4 second.example.net
s=Example
t=0 0
c=IN IP4 192.0.2.94
m=audio 16112 TCP/RTP/AVP 10 11
a=setup:passive
a=connection:new
```

Figure 4 : description de session TCP pour le second participant

Les descriptions de session définissent deux parties qui participent à une session RTP/AVP en mode connexion. La première partie (Figure 3) est capable de recevoir des flux stéréo L16 (type de charge utile statique 11).

La seconde partie (Figure 4) est capable de recevoir des flux mono (type de charge utile statique 10) ou stéréo L16.

L'attribut "setup" dans la Figure 3 spécifie que la première partie est "active" et initie des connexions, et l'attribut "setup" dans la Figure 4 spécifie que la seconde partie est "passive" et accepte les connexions [RFC4145].

La première partie se connecte à l'adresse réseau (192.0.2.94) et l'accès (16112) de la seconde partie. Une fois la connexion établie, elle est utilisée bidirectionnellement : la première partie envoie des paquets RTP tramés à la seconde partie dans une direction de la connexion, et la seconde partie envoie des paquets RTP tramés à la première partie dans l'autre direction de la connexion.

La première partie initie aussi une connexion RTCP TCP à l'accès 16113 (16112 + 1, comme défini dans la [RFC4566]) de la seconde partie. Une fois la connexion établie, la première partie envoie des paquets RTCP tramés à la seconde partie dans une direction de la connexion, et la seconde partie envoie des paquets RTCP tramés à la première partie dans l'autre direction de la connexion.

6. Contrôle d'encombrement

Les exigences pour le contrôle d'encombrement de RTP sont définies dans la [RFC3550]. Comme noté dans la [RFC3550], tous les protocoles de transport utilisés sur l'Internet doivent traiter d'une façon ou d'une autre du contrôle d'encombrement, et RTP n'y fait pas exception.

De plus, les exigences pour le contrôle d'encombrement pour le profil audio/vidéo sont définies dans la [RFC3551]. L'exigence de contrôle d'encombrement de base définie dans la [RFC3551] est que les sessions RTP devraient concourir équitablement avec les flux TCP qui partagent le réseau. Comme la méthode de tramage utilise TCP, elle concoure par définition équitablement avec les autres flux TCP.

7. Remerciements

Le présent mémoire rend compte en partie de discussions sur la liste de diffusion AVT sur TCP et RTP. Merci à tous les participants à ces discussions.

8. Considérations sur la sécurité

Les développeurs devraient lire attentivement les sections de considérations sur la sécurité des documents RTP [RFC3550] et RTP/AVP [RFC3551] car la plupart des questions discutées dans ces sections s'appliquent directement aux flux RTP tramés sur TCP.

Les descriptions de session qui spécifient des sessions de supports en mode connexion (comme l'exemple de session des Figures 3 et 4 de la Section 5) soulèvent des soucis de sécurité uniques pour les flux de supports. La section Considérations sur la sécurité de la [RFC4145] décrit ces questions en détail.

On discute ci-dessous des questions de sécurité qui sont spécifiques de la méthode de tramage définie à la Section 2.

Des attaquants peuvent envoyer des paquets tramés avec de grosses valeurs de LONGUEUR pour exploiter les trous de la sécurité des applications. Par exemple, une mise en œuvre de langage C peut déclarer un dispositif de 1500 octets comme une variable de pile, et utiliser LONGUEUR comme limite de la boucle qui lit le paquet tramé dans le dispositif. Ce code va bien fonctionner pour les applications amicales qui utilisent des paquets RTP avec des tailles de trame de type Ethernet, mais peut être exploité par un attaquant. Donc, une mise en œuvre a besoin de traiter des paquets de toutes longueurs, depuis un paquet NULL (LONGUEUR == 0) jusqu'à la longueur maximale de paquet contenant 64 K octets (LONGUEUR = 0xFFFF).

9. Considérations relatives à l'IANA

La [RFC4566] définit la syntaxe des lignes de supports de description de session. On reproduit cette définition à la Figure 2 de la Section 4 du présent mémoire. Dans la Section 4, on définit une nouvelle valeur de jeton pour le champ <proto> des lignes de supports : "TCP/RTP/AVP". La Section 4 spécifie la sémantique associée au jeton de champ <proto>, et la Section 5 montre un exemple de son utilisation dans une description de session.

10. Références normatives

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

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

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

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

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

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

[RFC4145] D. Yon, G. Camarillo, "Transport de support fondé sur TCP dan le protocole de description de session (SDP)", septembre 2005. (*MàJ par* RFC4572) *(P.S.)*

[RFC4566] M. Handley, V. Jacobson et C. Perkins, "SDP : Protocole de description de session", juillet 2006. *(P.S. ; remplacée par RFC8866)*

Adresse de l'auteur

John Lazzaro
UC Berkeley
CS Division
315 Soda Hall
Berkeley CA 94720-1776

mél : lazzaro@cs.berkeley.edu

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administatif (IASA) de l'IETF.