Groupe de travail Réseau
Request for Comments : 4168
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

J. Rosenberg, Cisco Systems, Inc.
H. Schulzrinne, Columbia University
G. Camarillo, Ericsson
octobre 2005

Protocole de transmission de contrôle de flux (SCTP) comme transport pour le protocole d'initialisation de flux (SIP)

Résumé
Le présent document spécifie un mécanisme pour utiliser le protocole de transmission de contrôle de flux (SCTP, *Stream Control Transmission Protocol*) comme mécanisme de transport entre les entités du protocole d'initialisation de session (SIP, *Session Initiation Protocol*). SCTP est un nouveau protocole qui fournit plusieurs caractéristiques qui peuvent se révéler avantageuses pour le transport entre des entités SIP qui échangent une grande quantité de messages, incluant des passerelles et des mandataires. Comme SIP est indépendant du transport, la prise en charge de SCTP est un processus relativement direct, presque identique à la prise en charge de TCP.

Table des Matières

1. Introduction

Le protocole de transmission de contrôle de flux (SCTP, *Stream Control Transmission Protocol*) [RFC2960] a été conçu comme un nouveau protocole de transport pour l'Internet (ou les intranets) à la même couche que TCP et UDP. SCTP a été conçu en pensant au transport des messages traditionnels de la signalisation SS7. On a observé que beaucoup des caractéristiques destinées à prendre en charge une telle signalisation sont aussi utiles pour le transport du protocole d'initialisation de session (SIP, *Session Initiation Protocol*) [RFC3261], qui est utilisé pour initier et gérer des sessions interactives sur l'Internet.

SIP lui-même est indépendant du transport, et peut fonctionner sur tout transport de message ou flux fiable ou non fiable. Cependant, les procédures ne sont définies que pour le transport sur UDP et TCP. Le présent document définit le transport de SIP sur SCTP.

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].

3. Avantages potentiels

La [RFC3257] présente certains des avantages clés de SCTP. On les résume ici et on analyse comment ils se rapportent à SIP (une analyse plus détaillée se trouve dans [SIP-ETP]).

3.1 Avantages sur UDP

Tous les avantages qu'a SCTP sur UDP concernant le transport de SIP sont aussi partagés par TCP. Voici une liste des avantages généraux qu'un protocole de transport en mode connexion tel que TCP ou SCTP a sur un protocole de transport sans connexion comme UDP.

Retransmission rapide : SCTP peut rapidement déterminer la perte d'un paquet, à cause de son utilisation du SACK et d'un mécanisme qui envoie les messages SACK plus vite que la normale quand des pertes sont détectées. Il en résulte que les pertes de messages SIP peuvent être détectées plus vite que lorsque SIP fonctionne sur UDP (la détection va prendre au moins 500 ms, sinon plus). Noter que le SACK TCP existe aussi, et TCP a aussi une option retransmission rapide. Sur une connexion existante, il en résulte des temps d'établissement d'appel plus rapides dans des conditions de perte de paquet, ce qui est très souhaitable. C'est probablement l'avantage le plus significatif de SCTP pour le transport de SIP.

Contrôle d'encombrement : SCTP tient le contrôle d'encombrement sur l'association entière. Pour SIP, cela signifie que le taux d'agrégation des messages entre deux entités peut être contrôlé. Lorsque SIP fonctionne sur TCP, les mêmes avantages sont recueillis. Cependant, lorsque il fonctionne sur UDP, SIP fournit un contrôle d'encombrement moins efficace. C'est parce que l'état d'encombrement (mesuré en termes d'intervalle de retransmission UDP) est calculé transaction par transaction, plutôt que sur toutes les transactions. Donc, les performance de contrôle d'encombrement sont similaires à l'ouverture de N connexions TCP parallèles, par opposition à l'envoi de N messages sur une connexion TCP.

Fragmentation de couche transport : SCTP et TCP assurent la fragmentation de la couche transport. Si un message SIP est supérieur à la taille de la MTU, il est fragmenté à la couche transport. Lorsque UDP est utilisé, la fragmentation se produit à la couche IP. La fragmentation IP augmente la probabilité d'avoir des pertes de paquet et rend la traversée des NAT et pare-feu difficile, sinon impossible. Cette caractéristique va devenir importante si la taille des messages SIP augmente beaucoup.

3.2 Avantages sur TCP

On a montré les avantages de SCTP et TCP sur UDP. On analyse maintenant les avantages de SCTP sur TCP.

Tête de ligne : SCTP est fondé sur le message, par opposition à TCP, qui est fondé sur le flux. Cela permet à SCTP de séparer différents messages de signalisation à la couche transport. TCP ne comprend que les octets. Assembler les octets reçus pour former des messages de signalisation est effectué à la couche application. Donc, TCP délivre toujours un flux ordonné d'octets à l'application. D'un autre côté, SCTP peut délivrer des messages de signalisation à l'application aussitôt qu'ils arrivent (lorsque on utilise le service non ordonné). La perte d'un message de signalisation n'affecte pas la livraison du reste des messages. Cela évite le problème du blocage de tête de ligne dans TCP, qui se produit lorsque plusieurs connexions de couche supérieure sont multiplexées au sein d'une seule connexion TCP. Une transaction SIP peut être considérée comme une connexion de couche application. Il y a plusieurs transactions qui courent entre les mandataires. La perte d'un message dans une transaction NE DEVRAIT PAS affecter la capacité d'une transaction différente d'envoyer un message. Donc, si SIP fonctionne entre des entités avec de nombreuses transactions qui se produisent en parallèle, SCTP peut fournir des performances meilleures que celles de SIP sur TCP (mais pas de SIP sur UDP ; SIP sur UDP n'est pas idéal du point de vue du contrôle d'encombrement ; voir ci-dessus).

Facilité d'analyse : un autre avantage des protocoles fondés sur le message, comme SCTP et UDP, sur les protocoles fondés sur le flux, comme TCP, est qu'il permette une analyse plus facile des messages à la couche application. Il n'est pas nécessaire d'établir de frontières (normalement en utilisant des en-têtes de longueur de contenu) entre les différents messages. Cependant, cet avantage est presque négligeable.

Multi rattachement : une connexion SCTP peut être associée à plusieurs adresses IP sur le même hôte. Les données sont toujours envoyées à une des adresses, mais si elle devient injoignable, les données envoyées à une peuvent migrer sur une adresse différente. Cela améliore la tolérance aux fautes ; les défaillances du réseau rendant une interface du serveur indisponible n'empêchent pas le service de continuer à fonctionner. Les serveurs SIP sont supposés avoir des exigences substantielles de tolérance aux fautes. Il vaut de noter que, parce que SIP est en mode message et non en mode flux, les procédures existantes de sélection de service (SRV, *Service Selection*) définies dans la [RFC3261] peuvent accomplir le même but, même lorsque SIP fonctionne sur TCP. En fait, les enregistrements SRV permettent à la "connexion" de reprendre sur défaillance sur un autre hôte. Comme les mandataires SIP peuvent fonctionner sans état, la reprise sur défaillance peut être réalisée sans synchronisation des données entre le principal et ses sauvegardes. Donc, les capacités de multi rattachement de SCTP fournissent un avantage marginal.

Il est important de noter que la plupart des avantages de SCTP pour SIP se produisent dans des conditions de perte. Donc, dans des conditions de zéro perte, le transport SCTP de SIP DEVRAIT avoir des performances égales avec le transport TCP. Des recherches sont nécessaires pour évaluer dans quelles conditions de pertes les améliorations de temps d'établissement et de débit seront observées.

4. Paramètre Transport

Les champs d'en-tête Via portent un identifiant de protocole de transport. La RFC 3261 définit la valeur "SCTP" pour SCTP, mais ne définit pas la valeur du paramètre de transport pour TLS sur SCTP. Noter que la valeur "TLS", définie par la RFC 3261, est destinée à TLS sur TCP.

On définit ici la valeur "TLS-SCTP" pour la partie transport du champ d'en-tête Via à utiliser pour les demandes envoyées sur TLS avec SCTP [RFC3436]. Le format Backus-Naur augmenté (BNF, *Backus-Naur Form*) mis à jour [RFC2234] pour ce paramètre est le suivant (le BNF original pour ce paramètre se trouve dans la RFC 3261):

transport = "UDP" / "TCP" / "TLS" / "SCTP" / "TLS-SCTP" / autre transport

Voici des exemples de champs d'en-tête Via qui utilisent "SCTP" et "TLS-SCTP" :
Via: SIP/2.0/SCTP ws1234.example.com:5060
Via: SIP/2.0/TLS-SCTP ws1234.example.com:5060

5. Usage de SCTP

Les règles pour l'envoi d'une demande avec SCTP sont identiques à celles de TCP. La seule différence est qu'un envoyeur SCTP doit choisir un flux particulier au sein d'une association afin d'envoyer la demande (voir au paragraphe 5.1).

Noter qu'aucun identifiant SCTP n'a besoin d'être défini pour les messages SIP. Donc, l'identifiant de protocole de charge utile dans un tronçon DATA dans SCTP transportant des messages SIP DOIT être réglé à zéro.

La couche de transport SIP des deux homologues est chargée de gérer la connexion SCTP persistante entre eux. Du côté de l'envoyeur, le cœur ou une transaction du client (ou du serveur) génère une demande (ou réponse) et la passe à la couche transport. Le transport envoie la demande à la couche transaction de l'homologue. La couche transaction de l'homologue est chargée de livrer la demande (ou réponse) entrante à la transaction de serveur (ou client) existant appropriée. Si aucune transaction de serveur (ou de client) n'existe pour le message entrant, la couche transport passe la demande (ou réponse) au cœur, qui peut décider de construire une nouvelle transaction de serveur (ou client).

5.1 Transposition des transactions SIP en flux SCTP

Les transactions SIP doivent être transposées en flux SCTP d'une façon qui évite le blocage de tête de ligne (HOL, *Head Of the Line*). Parmi les différentes façons d'effectuer cette transposition qui respectent cette exigence, on a choisi la plus simple ; une entité SIP DEVRAIT envoyer chaque message SIP (demande ou réponse) sur un flux zéro avec le fanion "non ordonné" établi. Du côté receveur, une entité SIP DOIT être prête à recevoir des messages SIP sur tout flux.

Dans le passé, il avait été proposé que les identifiants de flux SCTP soient utilisés comme des identifiant légers de transaction SIP. Cette proposition avait été retirée parce que SIP fournit maintenant (comme défini dans la [RFC3261]) un identifiant de transaction dans le paramètre de branche des entrées Via. Cet identifiant de transaction, qui manquait dans la spécification SIP précédente [RFC2543], rend inutile l'utilisation des identifiants de flux SCTP pour démultiplexer le trafic

SIP.

Dans de nombreuses circonstances, SIP requiert l'utilisation de TLS [RFC2246], par exemple, lors de l'acheminement d'un URI SIPS [RFC3261]. Comme défini dans la [RFC3436], TLS fonctionnant sur SCTP NE DOIT PAS utiliser le service de livraison non ordonnée SCTP. De plus, une utilisation SIP d'une couche supplémentaire entre la couche transport et SIP qui exigerait une livraison ordonnée des messages NE DOIT PAS utiliser le service SCTP de livraison non ordonnée.

Les applications SIP qui exigent la livraison ordonnée des messages provenant de la couche transport (par exemple, TLS) DEVRAIENT envoyer des messages SIP appartenant à la même transaction SIP sur le même flux SCTP. De plus, elles DEVRAIENT envoyer des messages appartenant à des transactions SIP différentes sur des flux SCTP différents, pour autant qu'il y ait assez de flux disponibles.

Un scénario commun où le mécanisme ci-dessus DEVRAIT être utilisé consiste en l'échange par deux mandataires de trafic SIP sur une connexion TLS utilisant SCTP comme protocole de transport. Cela fonctionne parce que toutes les transactions SIP entre les deux mandataires peuvent être établies au sein d'une seule association SCTP.

Noter que si les deux côtés de l'association suivent cette recommandation, lorsque une demande arrive sur un flux particulier, le serveur est libre de retourner les réponses sur un flux différent. De cette façon, les deux côtés gèrent les flux disponibles dans la direction d'envoi, indépendamment des flux choisis par l'autre côté pour envoyer un message SIP particulier. Cela évite des collisions indésirables lors de la saisie d'un flux particulier.

6. Localisation d'un serveur SIP

La question principale lors de l'envoi d'une demande est de déterminer si le serveur du prochain bond supporte SCTP afin qu'une association puisse être ouverte. Les entités SIP suivent les procédures SIP normales [RFC3263] pour découvrir un serveur qui prenne en charge SCTP.

Cependant, afin d'utiliser TLS par dessus SCTP, une définition supplémentaire est nécessaire. La RFC 3263 définit la valeur de service de pointeur d'autorité de désignation (NAPTR, *Naming Authority Pointer*) [RFC3403] de "SIP+D2S" pour SCTP, mais ne définit pas de valeur pour TLS sur SCTP. On définit ici la valeur de service NAPTR de "SIPS+D2S" pour les serveurs qui prennent en charge TLS sur SCTP [RFC3436].

7. Considérations sur la sécurité

SCTP n'aggrave pas les problèmes de sécurité soulevés dans la [RFC3261] si on suit l'avis donné au paragraphe 5.1 et si TLS sur SCTP [RFC3436] est utilisé lorsque TLS serait exigé par la [RFC3261] ou la [RFC3263]. Donc, les mécanismes décrits dans la [RFC3436] DOIVENT être utilisés lorsque SIP fonctionne par dessus TLS [RFC2246] et SCTP.

8. Considérations relatives à l'IANA

Le présent document définit une nouvelle valeur de champ de service NAPTR (SIPS+ D2S). L'IANA a enregistré cette valeur dans le registre pour le champ des services d'enregistrement de ressource SRV de SIP. L'entrée résultante est comme suit :

Champ Services	**Protocole**	**Référence**
SIPS+D2S	SCTP	RFC4168

9. Références

9.1 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)

[RFC2234] D. Crocker et P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", novembre 1997.

(*Obsolète, voir* RFC5234)

[RFC2246] T. Dierks et C. Allen, "Protocole TLS version 1.0", janvier 1999. *(P.S. ; MàJ par* RFC7919)

[RFC2960] R. Stewart et autres, "Protocole de transmission de commandes de flux", octobre 2000. (*Obsolète, voir* RFC4960) *(P.S.)*

[RFC3261] J. Rosenberg et autres, "SIP : Protocole d'initialisation de session", juin 2002. (*Mise à jour par* RFC3265, RFC3853, RFC4320, RFC4916, RFC5393, RFC6665, RFC8217)

[RFC3263] J. Rosenberg, H. Schulzrinne, "Protocole d'initialisation de session (SIP) : Localisation des serveurs SIP", juin 2002. (*Remplace* RFC2543) *(P.S. ; MàJ par* RFC7984)

[RFC3403] M. Mealling, "Système de découverte dynamique de délégation (DDDS) Partie III : base de données du système de noms de domaines (DNS)", octobre 2002. *(P.S.)*

[RFC3436] A. Jungmaier, E. Rescorla, M. Tuexen, "Sécurité de la couche Transport sur le protocole de transmission de contrôle de flux", décembre 2002. *(P.S.)*

9.2 Références pour information

[RFC2543] M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg, "SIP : protocole d'initialisation de session", mars 1999. (*Obsolète, voir* RFC3261, RFC3262, RFC3263, RFC3264, RFC3265) *(P.S.)*

[RFC3257] L. Coene, "Déclaration d'applicabilité du protocole de transmission de contrôle de flux", avril 2002. *(Information)*

[RFC3969] G. Camarillo, "Registre des paramètres d'identifiant de ressource uniforme (URI) de l'IANA pour le protocole d'initialisation de session (SIP)", décembre 2004. (BCP0099)

[SIP-ETP] Camarillo, G., Schulrinne, H., and R. Kantola, "Evaluation of Transport Protocols for the Session Initiation Protocol", IEEE, Network vol. 17, no. 5, 2003.

Adresse des auteurs

Jonathan Rosenberg
Cisco Systems
600 Lanidex Plaza
Parsippany, NJ 07054
US
téléphone : +1 973 952-5000
mél : jdrosen@cisco.com
URI : http://www.jdrosen.net

Henning Schulzrinne
Columbia University
M/S 0401
1214 Amsterdam Ave.
New York, NY 10027-7003
US
mél : schulzrinne@cs.columbia.edu

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

Déclaration complète de droits de reproduction

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 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.