Groupe de travail Réseau
Request for Comments : 5061
Catégorie : Sur la voie de la normalisation

Traduction Claude Brière de L'Isle

R. Stewart, Cisco Systems, Inc.
Q. Xie, Motorola, Inc.
M. Tuexen, Univ. of Applied Sciences Muenster
S. Maruyama, Kyoto University
M. Kozuka, Kyoto University
septembre 2007

Reconfiguration dynamique d'addresse dans le protocole de transmission de commandes de flux (SCTP)

Résumé
Un hôte local peut avoir plusieurs points de rattachement à l'Internet, lui donnant un certain degré de tolérance aux fautes provenant de défaillances du matériel. Le protocole de transmission de commandes de flux (SCTP, *Stream Control Transmission Protocol*) (RFC 4960) a été développé pour tirer pleinement parti d'un tel hôte multi-rattachement pour fournir une récupération rapide sur défaillance et une survivance d'association en face de telles défaillances de matériel. Le présent document décrit une extension à SCTP qui va permettre à une pile SCTP d'ajouter dynamiquement une adresse IP à une association SCTP, de supprimer dynamiquement une adresse IP d'une association SCTP, et de demander d'établir l'adresse principale que l'homologue va utiliser lors de l'envoi à un point d'extrémité.

Table des Matières

1. Introduction

Un hôte local peut avoir plusieurs points de rattachement à l'Internet, lui donnant un degré de tolérance aux fautes provenant de défaillances matérielles. SCTP a été développé pour tirer pleinement parti d'un tel hôte multi-rattachements pour fournir une récupération rapide des défaillances et une survicance d'association en face de telles défaillances matérielles. Cependant, de nombreux ordinateurs modernes permettent l'ajout et la suppression dynamique des cartes réseau (parfois appelées une interface enfichable à chaud). On complique cela avec la capacilté d'un fournisseur, dans IPv6, de renuméroter dynamiquement un réseau, et il y a encore un trou entre la tolérance complète aux fautes et le protocole SCTP actuellement défini. Peu importe qu'une carte soit ajoutée ou qu'une interface soit renumérotée, afin de tirer parti de cette nouvelle configuration, l'association de transport doit être redémarrée. Pour de nombreuses applications tolérantes aux fautes, ce redémarrage est considéré comme une panne et est indésirable.

Le présent document décrit une extension à SCTP pour tenter de corriger ce problème pour les plus exigeantes des applications tolérantes aux fautes. Cette extension va permettre à une pile SCTP :

- o d'ajouter dynamiquement une adresse IP à une association,
- o de supprimer dynamiquement une adresse IP d'une association.,
- o de demander d'établir l'adresse principale que l'homologue va utiliser quand il envoie à un point d'extrémité.

L'ajout et la suppression dynamique d'adresses IP permet à une association SCTP de continuer de fonctionner à travers les reconfigurations d'hôte et du réseau. Ces changements, effectués par une action du fournisseur ou de l'utilisateur, peuvent signifier que l'homologue va être mieux servi en utilisant la nouvelle adresse ajoutée ; cependant, cette information peut seulement être connue du point d'extrémité chez qui la reconfiguration se produit. Dans ce cas, cette extension permet au point d'extrémité local d'avertir l'homologue de ce qu'il pense être la meilleure adresse principale que l'homologue devrait utiliser.

Une dernière chose que cette extension ajoute est un petit entier de 32 bits appelé une indication d'adaptation qui peut être échangée au démarrage. Cela est utile pour les applications où il y a une ou plusieurs couches spécifiques en-dessous de l'application, mais au-dessus de SCTP. Dans ce cas, l'échange de cette indication peut permettre que la couche appropriée soit activée en dessous de l'application.

2. Conventions

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. Arithmétique des numéros de série

Il est essentiel de se souvenir que l'espace réel de numéros de séquence de tronçon de changement de configuration d'adresse (ASCONF, *Address Configuration Change Chunk*) est fini, bien que très grand. Cet espace va de 0 à 2**32 - 1. Comme l'espace est fini, toute l'arithmétique des numéros de séquence ASCONF DOIT être effectuée modulo 2**32. Cette arithmétique non signée préserve les relations des numéros de séquence lorsque ils parcourent à nouveau le cycle de 2**32 - 1 à 0. Il y a quelques subtilités dans l'arithmétique modulo des ordinateurs, donc un grand soin devrait être apporté à la programmation de la comparaison de ces valeurs. Quand on se réfère aux numéros de séquence ASCONF, le symbole "=<" signifie "inférieur ou égal (modulo 2**32)".

Les comparaisons et l'arithmétique des numéros de séquence ASCONF dans ce document DEVRAIENT utiliser l'arithmétique des numéros de série définie dans la [RFC1982] où SERIAL_BITS = 32.

Les numéros de séquence ASCONF reviennent à zéro quand ils atteignent 2**32 - 1. C'est-à-dire que le prochain numéro de séquence ASCONF qu'un tronçon ASCONF DOIT utiliser après avoir transmis un numéro de séquence ASCONF = 2**32 - 1 est 0.

Toute arithmétique faite sur des numéros de séquence de flux DEVRAIT utiliser l'arithmétique des numéros de série (comme définie dans la [RFC1982]) où SERIAL_BITS = 16. Toutes les autres arithmétiques et comparaisons dans le présent document utilisent l'arithmétique normale.

4. Tronçons et paramètres supplémentaires

Cette section décrit l'ajout de deux nouveaux tronçons et de sept nouveaux paramètres pour permettre :
- o l'ajout dynamique d'adresses IP à une association,
- o la suppression dynamique d'adresses IP d'une association,
- o une demande d'établir l'adresse principale que l'homologue va utiliser quand il envoie à un point d'extrémité.

De plus, cette section décrit trois nouvelles causes d'erreur qui prennent en charge ces nouveaux tronçons et paramètres.

4.1 Nouveaux types de tronçons

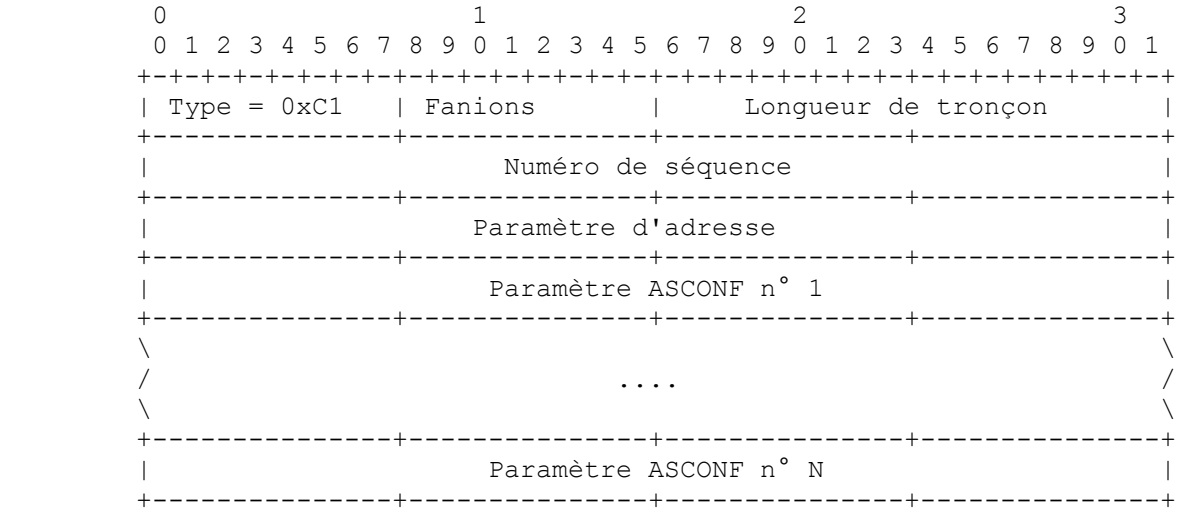
Ce paragraphe définit deux nouveaux types de tronçon qui vont être utilisés pour transférer fiablement les informations de contrôle. LeTableau 1 illustre les deux nouveaux types de tronçon.

Type de tronçon	Nom de tronçon
0xC1	Tronçon de changement de configuration d'adresse (ASCONF)
0x80	Accusé de réception de tronçon de changement de configuration d'adresse (ASCONF-ACK)

Table 1 : Tronçons de changement de configuration d'adresse

4.1.1 Tronçon de changement de configuration d'adresse (ASCONF)

Ce tronçon est utilisé pour communiquer au point d'extrémité distant une demande de changement de configuration qui DOIT être acquittée. Les informations portées dans le tronçon ASCONF utilisent la forme Type-Longueur-Valeur (TLV) comme décrit au paragraphe 3.2.1 "Format de paramètre facultatif/de longueur variable" de la [RFC4960] pour tous les paramètres variables. Ce tronçon DOIT être envoyé authentifié en utilisant le mécanisme défini dans la [RFC4895]. Si ce tronçon est reçu non authentifié, il DOIT être éliminé en silence, comme décrit dans la [RFC4895].



Numéro de séquence : 32 bits (entier non signér). Cette valeur représente un numéro de séquence pour le tronçon ASCONF. La gamme valide de numéros de séquence est de 0 à 4 294 967 295 (2**32 - 1). Les numéros de séquence reviennent à 0 après avoir atteint 4 294 967 295.

Paramètre d'adresse : 8 ou 20 octets (selon le type d'adresse). Ce champ contient un paramètre d'adresse, IPv6 ou IPv4, d'après la [RFC4960]. L'adresse est une adresse de l'envoyeur du tronçon ASCONF ; l'adresse DOIT être considérée faire partie de l' association par le point d'extrémité homologue (le receveur du tronçon ASCONF). Ce champ peut être utilisé par le receveur de l'ASCONF pour aider à trouver l'association. Si l'adresse 0.0.0.0 ou ::0 est fournie, le receveur PEUT chercher l'association par d'autres informations fournies dans le paquet. Ce paramètre DOIT être présent dans tout message ASCONF, c'est-à-dire c'est un paramètre TLV obligatoire.

Note : l'adresse du nom d'hôte NE DOIT PAS être envoyée et DOIT être ignorée si elle est reçue dans un message ASCONF.

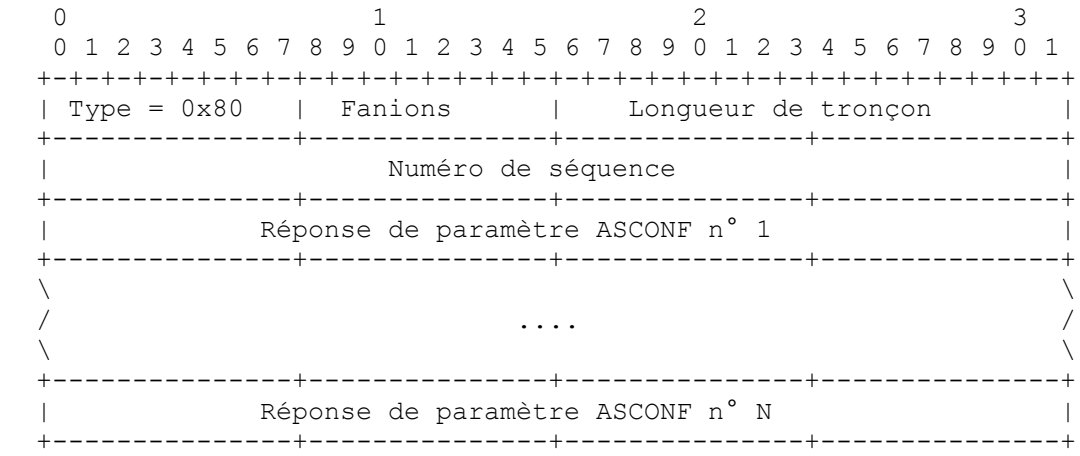
On devrait noter que le format de tronçon ASCONF exige que le receveur fasse rapport à l'envoyeur si il ne comprend pas le tronçon ASCONF. Ceci est accompli en réglant les bits de poids fort du type de tronçon comme décrit au paragraphe 3.2 de la [RFC4960]. Noter que les deux bits de poids fort du tronçon ASCONF sont réglés à un. Comme défini au paragraphe 3.2 de la [RFC4960], quand il règle ces bits de poids fort de cette manière, le receveur qui ne comprend pas ce tronçon DOIT sauter le tronçon et continuer le traitement, et le rapporter dans une erreur de fonctionnement de tronçon en utilisant la cause d'erreur "Type de tronçon non reconnu". Cela NE va PAS interrompre l'association mais indique à l'envoyeur qu'il NE DOIT PAS envoyer d'autres tronçons ASCONF.

Paramètre ASCONF : format de TLV.

Chaque changement de configuration d'adresse est représenté par un paramètre TLV, comme défini au paragraphe 4.2. Une ou plusieurs demandes peuvent être présentes dans un tronçon ASCONF.

4.1.2 Accusé de réception de tronçon de changement de configuration (ASCONF-ACK)

Ce tronçon est utilisé par le receveur d'un tronçon ASCONF pour en accuser réception. Il porte zéro, un ou plusieurs résultats pour tous les paramètres ASCONF qui ont été traités par le receveur. Ce tronçon DOIT être envoyé authentifié en utilisant le mécanisme défini dans la [RFC4895]. Si ce tronçon est reçu non authentifié, il DOIT être éliminé en silence, comme décrit dans la [RFC4895].



Numéro de séquence : 32 bits (entier non signé). Cette valeur représente le numéro de séquence pour le tronçon ASCONF reçu qui est acquitté par ce tronçon. Cette valeur est copiée du tronçon ASCONF reçu.

Réponse de paramètre ASCONF : format de TLV. La réponse de paramètre ASCONF est utilisée dans le ASCONF-ACK pour rapporter l'état du traitement d'ASCONF. Par défaut, si un point d'extrémité répondeur n'inclut aucune cause d'erreur, un succès est indiqué. Donc un envoyeur d'un ASCONF-ACK PEUT indiquer un succès complet de tous les TLV dans un ASCONF en retournant seulement le type de tronçon, les fanions de tronçon, la longueur de tronçon (réglée à 8) et le numéro de séquence.

4.2 Nouveaux types de paramètres

Les sept nouveaux paramètres ajoutés suivent le format défini au paragraphe 3.2.1 de la [RFC4960]. Les Tableaux 2, 3, et 4 décrivent les paramètres.

Paramètres de configuration d'adresse	**Type de paramètre**
Établir l'adresse principale	0xC004
Indication de couche d'adaptation	0xC006
Extensions prises en charge	0x8008

Tableau 2 : Paramètres qui peuvenat être utilisés dans un tronçon INIT/INIT-ACK

Paramètres de configuration d'adresse	Type de paramètre
Ajout d'adresse IP	0xC001
Suppression d'adresse IP	0xC002
Établir l'adresse principale	0xC004

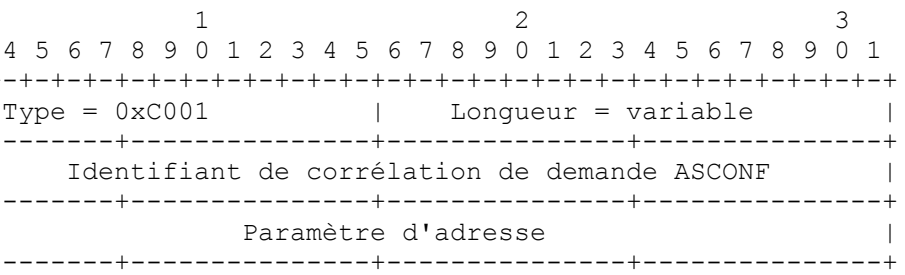
Tableau 3 : Paramètres utilisés dans un paramètre ASCONF

Paramètres de configuration d'adresse	Type de paramètre
Indication de cause d'erreur	0xC003
Indication de succès	0xC005

Tableau 4 : Paramètres utilisés dans une réponse de paramètre ASCONF

Tout paramètre qui apparaît où il n'est pas permis (par exemple, un paramètre 0xC002 apparaissant au sein d'un INIT ou INIT-ACK) PEUT recevoir en réponse un ABORT par le receveur du paramètre invalide. Si le receveur choisit de ne pas interrompre, le paramètre DOIT être ignoré. Une mise en œuvre robuste DEVRAIT ignorer le paramètre et laisser l'association intacte.

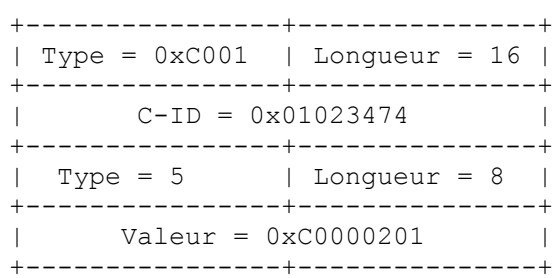
4.2.1 Ajout d'une adresse IP



Identifiant de corrélation de demande ASCONF : 32 bits. C'est un entier opaque alloué par l'envoyeur pour identifier chaque paramètre de demande. Le receveur du tronçon ASCONF va copier cette valeur de 2 bits dans le champ Identifiant de corrélation de réponse ASCONF du paramètre de réponse ASCONF-ACK. L'envoyeur de l'ASCONF peut utiliser cette même valeur dans le ASCONF-ACK pour trouver pour quelle demande est la réponse. Noter que le receveur NE DOIT PAS changer cette valeur de 32 bits.

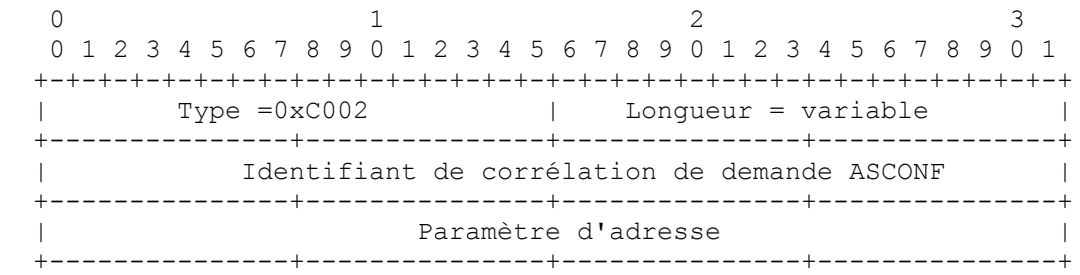
Paramètre d'adresse : TLV. Ce champ contient un paramètre d'adresse IPv4 ou IPv6 comme décrit au paragraphe 3.3.2.1 de la [RFC4960]. Le TLV complet est enveloppé au sein de ce paramètre. Il informe le receveur que l'adresse spécifiée est à ajouter à l'association existante. Ce paramètre NE DOIT PAS contenir une adresse de diffusion ou de diffusion groupée. Si l'adresse 0.0.0.0 ou ::0 est fournie, l'adresse de source du paquet DOIT être ajoutée.

Un exemple de TLV demandant que l'adresse IPv4 192.0.2.1 soit ajoutée à l'association ressemblerait à :



Apparition d'un tronçon valide : le paramètre Ajout d'adresse IP peut seulement apparaître dans le type de tronçon ASCONF.

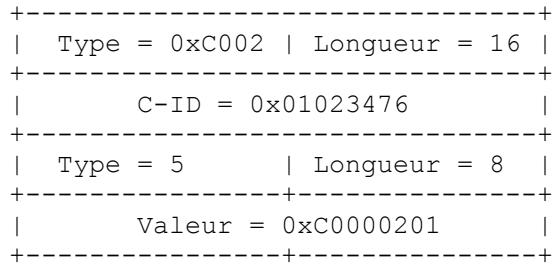
4.2.2 Suppression d'adresse IP



Identifiant de corrélation de demande ASCONF : 32 bits. C'est un entier opaque alloué par l'envoyeur pour identifier chaque paramètre de demande. Le receveur du tronçon ASCONF va copier cette valeur de 32 bits dans le champ Identifiant de corrélation de réponse ASCONF du paramètre de réponse ASCONF-ACK. L'envoyeur de l'ASCONF peut utiliser cette même valeur dans le ASCONF-ACK pour trouver à quelle demande est la réponse. Noter que le receveur NE DOIT PAS changer cette valeur de 32 bits.

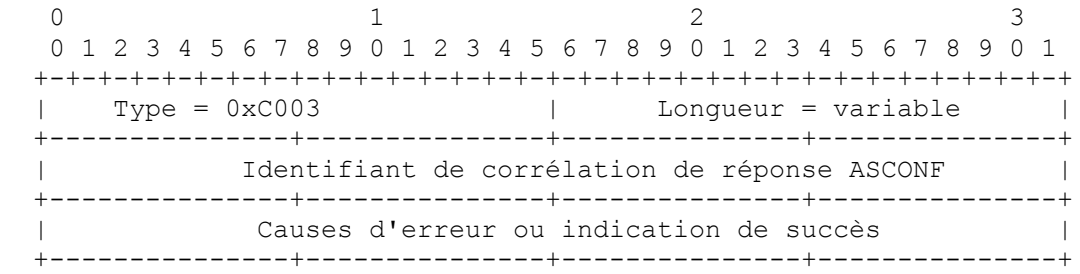
Paramètre d'adresse : TLV. Ce champ contient un paramètre d'adresse IPv4 ou IPv6, comme décrit au paragraphe 3.3.2.1 de la [RFC4960]. Le TLV complet est enveloppé au sein de ce paramètre. Il informe le receveur que l'adresse spécifiée est à supprimer de l'association existante. Ce paramètre NE DOIT PAS contenir une adresse de diffusion ou diffusion groupée. Si l'adresse 0.0.0.0 ou ::0 est fournie, toutes les adresses de l'homologue sauf l'adresse de source du paquet DOIVENT être supprimées.

Un exemple de TLV supprimant l'adresse IPv4 192.0.2.1 d'une association existante ressemblerait à :



Apparition d'un tronçon valide : le paramètre Suppression d'adresse IP peut seulement apparaître dans le type de tronçon ASCONF.

4.2.3 Indication de cause d'erreur

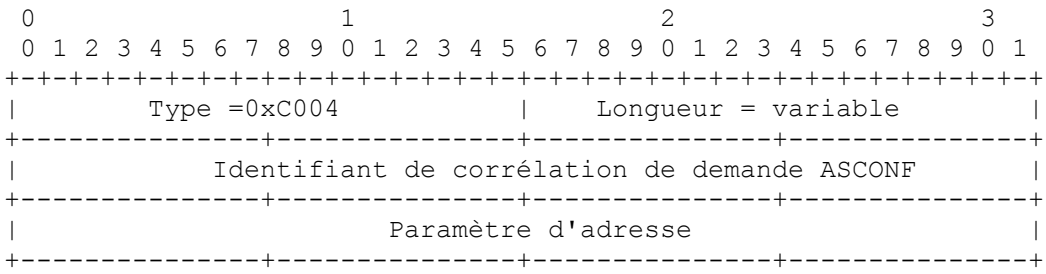


Identifiant de corrélation de réponse ASCONF : 32 bits. C'est un entier opaque alloué par l'envoyeur pour identifier chaque paramètre de demande. Le receveur du tronçon ASCONF va copier cette valeur de 32 bits provenant de l'identifiant de corrélation de demande ASCONF dans le champ Identifiant de corrélation de réponse ASCONF afin que l'homologue puisse facilement corréler la demande à cette réponse. Noter que le receveur NE DOIT PAS changer cette valeur de 32 bits.

Causes d'erreur : TLV. Quand il rapporte une erreur, ce paramètre de réponse est utilisé pour envelopper une ou plusieurs causes d'erreur standard trouvées au sein d'une erreur de fonctionnement SCTP ou d'un SCTP Abort (comme défini dans la [RFC4960]). La ou les causes d'erreur suivent le format défini au paragraphe 3.3.10 de la [RFC4960].

Apparition d'un tronçon valide : le paramètre Indication de cause d'erreur peut seulement apparaître dans le type de tronçon ASCONF-ACK.

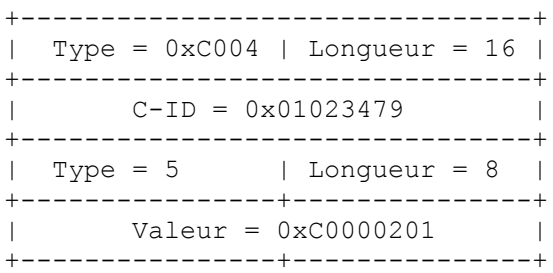
4.2.4 Établir l'adresse IP principale



Identifiant de corrélation de demande ASCONF : 32 bits. C'est un entier opaque alloué par l'envoyeur pour identifier chaque paramètre de demande. Le receveur du tronçon ASCONF va copier cette valeur de 32 bits dans le champ Identifiant de corrélation de réponse ASCONF du paramètre de réponse ASCONF-ACK. L'envoyeur de l'ASCONF peut utiliser cette même valeur dans le ASCONF-ACK pour trouver à quelle demande est la réponse. Noter que le receveur NE DOIT PAS changer cette valeur de 32 bits.

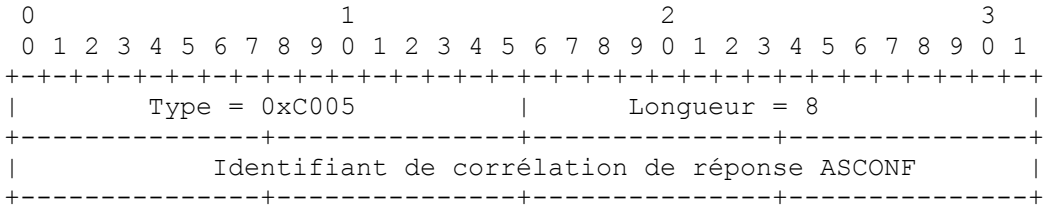
Paramètre d'adresse : TLV. Ce champ contient un paramètre d'adresse IPv4 ou IPv6, comme décrit au paragraphe 3.3.2.1 de la [RFC4960]. Le TLV complet est enveloppé au sein de ce paramètre. Il demande au receveur de marquer l'adresse spécifiée comme adresse principale où envoyer les données (voir le paragraphe 5.1.2 de la [RFC4960]). Le receveur PEUT marquer cela comme son adresse principale à réception de cette demande. Si l'adresse 0.0.0.0 ou ::0 est fournie, le receveur PEUT marquer l'adresse de source du paquet comme son adresse principale.

Un exemple de TLV demandant que l'adresse IPv4 192.0.2.1 soit l'adresse de destination principale ressemblerait à :



Apparition d'un tronçon valide : le paramètre Établir l'adresse principale peut apparaître dans le type de tronçon ASCONF, INIT, ou INIT-ACK. L'inclusion de ce paramètre dans INIT ou INIT-ACK peut être utilisée pour indiquer une préférence initiale d'adresse principale.

4.2.5 Indication de succès



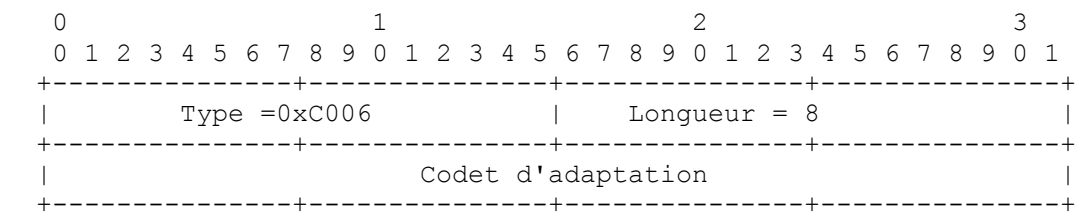
Par défaut, si un point d'extrémité répondeur ne rapporte pas une erreur pour un TLV demandé, un succès est implicitement indiqué. Donc, un envoyeur d'un ASCONF-ACK PEUT indiquer le succès complet de tous les TLV dans un ASCONF en retournant seulement le type de tronçon, les fanions de tronçon, la longueur de tronçon (réglée à 8) et le numéro de séquence.

Le point d'extrémité répondeur PEUT aussi choisir de rapporter explicitement un succès pour un TLV demandé, en retournant une réponse de paramètre ASCONF de rapport de succès.

Identifiant de corrélation de réponse ASCONF : 32 bits. C'est un entier opaque alloué par l'envoyeur pour identifier chaque paramètre de demande. Le receveur du tronçon ASCONF va copier cette valeur de 32 bits provenant de l'identifiant de corrélation de demande ASCONF dans le champ Identifiant de corrélation de réponse ASCONF afin que l'homologue puisse facilement corréler la demande à cette réponse.

Apparition d'un tronçon valide : le paramètre Indication de succès peut seulement apparaître dans le type de tronçon ASCONF-ACK.

4.2.6 Indication de couche d'adaptation



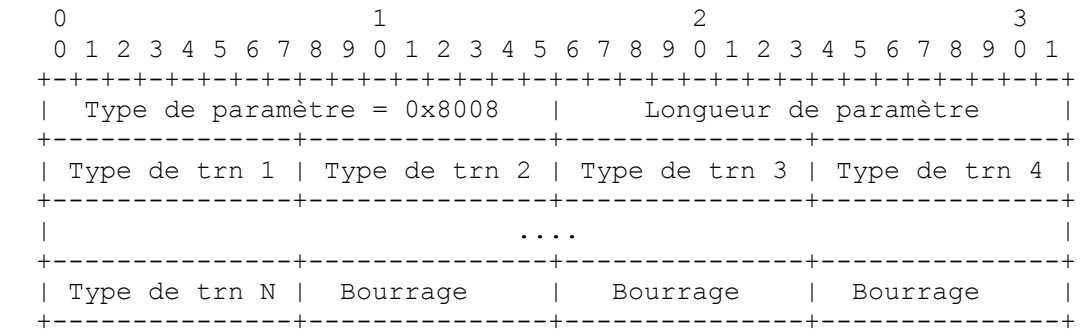
Ce paramètre est spécifié pour la communication des protocoles de couche supérieure de l'homologue. Il est envisagé de l'utiliser pour le contrôle de flux et autres couches d'adaptation qui demandent qu'une indication soit portée dans le INIT et INIT-ACK. Chaque couche d'adaptation définie qui souhaite utiliser ce paramètre DOIT spécifier un codet d'adaptation dans une RFC appropriée définissant son utilisation et sa signification. Ce paramètre NE DEVRAIT PAS être examiné par la mise en œuvre SCTP receveuse et devrait être passé de façon opaque au protocole de couche supérieure.

Note : ce paramètre n'est utilisé ni dans l'ajout ni dans la suppression des adresses mais sert à la couche supérieure. Le présent document inclut ce paramètre pour minimiser le nombre de documents SCTP.

Apparition d'un tronçon valide : le paramètre Indication de couche d'adaptation peut apparaître dans un tronçon INIT ou INIT-ACK et DEVRAIT être passé au protocole de couche supérieure du receveur sur la base de la configuration de la pile SCTP du protocole de couche supérieure. Ce paramètre NE DOIT PAS être envoyé dans d'autres tronçons, et si il est reçu dans un autre tronçon, il DOIT être ignoré.

4.2.7 Paramètre Extensions prises en charge

Ce paramètre est utilisé au démarrage pour identifier toutes les extensions supplémentaires que l'envoyeur accepte. L'envoyeur DOIT prendre en charge l'envoi et la réception de tous les types de tronçon mentionnés dans le paramètre Extensions prises en charge. Une mise en œuvre qui accepte cette extension DOIT mentionner les tronçons ASCONF, ASCONF-ACK, et AUTH dans ses paramètres INIT et INIT-ACK.



Type de paramètre : ce champ contient le type de paramètre défini par l'IANA pour le paramètre Extensions prises en charge. La valeur de ce champ est 0x8008.

Longueur de paramètre : ce champ contient la longueur du paramètre, incluant le type de paramètre, la longueur de paramètre, et toutes les extensions supplémentaires prises en charge. Note : la longueur NE DOIT PAS inclure de bourrage.

Type de tronçon X : ces champs contiennent le type de tronçon de toute extension SCTP actuellement prise en charge par

le SCTP envoyeur. Plusieurs types de tronçon peuvent être définis mentionnant chaque caractéristique supplémentaire que l'envoyeur prend en charge. L'envoyeur NE DOIT PAS inclure plusieurs paramètres Extensions prises en charge au sein d'un même tronçon.

Apparition d'un tronçon valide : ce paramètre peut apparaître dans le tronçon INIT ou INIT-ACK. Ce paramètre NE DOIT PAS apparaître dans un autre tronçon.

4.3 Nouvelles causes d'erreur

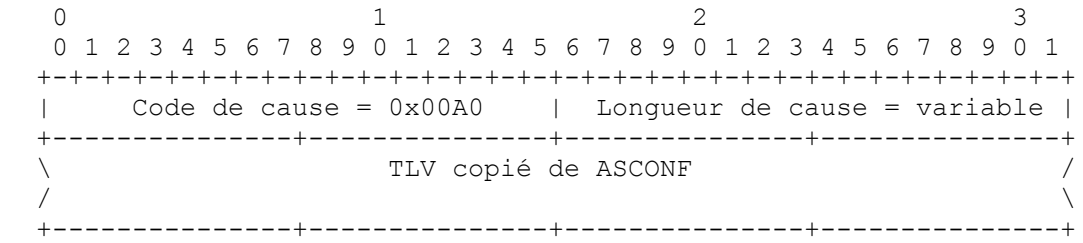
Cinq nouvelles causes d'erreur sont ajoutées aux erreurs de fonctionnement SCTP, principalement pour l'usage du tronçon ASCONF-ACK.

Valeur de code de cause	Code de cause
0x00A0	Demande de suppression de la dernière adresse IP restante
0x00A1	Opération refusée à cause du manque de ressources
0x00A2	Demande de suppression de l'adresse IP de source
0x00A3	Association interrompue à cause d'un ASCONF-ACK illégal
0x00A4	Demande refusée - pas d'autorisation

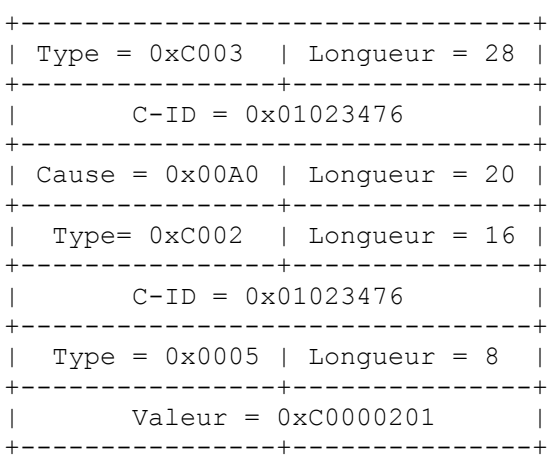
Tableau 5 : Nouvelles causes d'erreur

4.3.1 Demande de suppression de la dernière adresse IP restante

Le receveur de cette erreur a envoyé une demande de suppression de la dernière adresse IP dans son association avec son homologue. Cette erreur indique que la demande est rejetée.

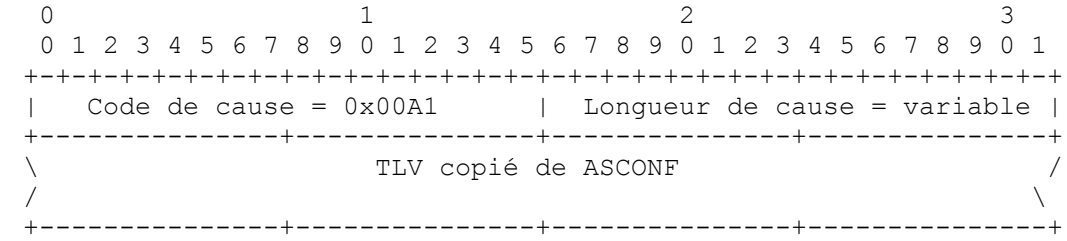


Un exemple d'un échec de suppression dans un TLV Cause d'erreur ressemblerait à ce qui suit dans le message de réponse ASCONF-ACK :

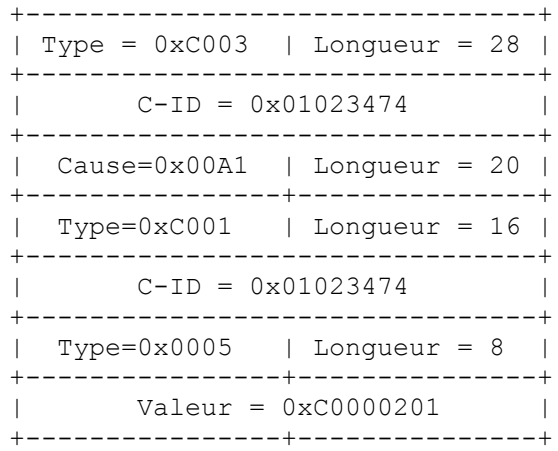


4.3.2 Opération refusée à cause du manque de ressources

Cette cause d'erreur est utilisée pour rapporter un échec du receveur à effectuer l'opération demandée due à un manque de ressources. Le TLV entier qui est refusé est copié de l'ASCONF dans la cause d'erreur.

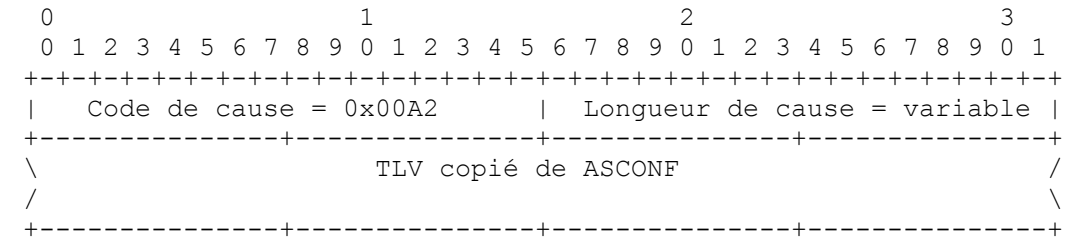


Un exemple d'un échec d'ajout dans un TLV Cause d'erreur ressemblerait à ce qui suit dans le message de réponse ASCONF-ACK :

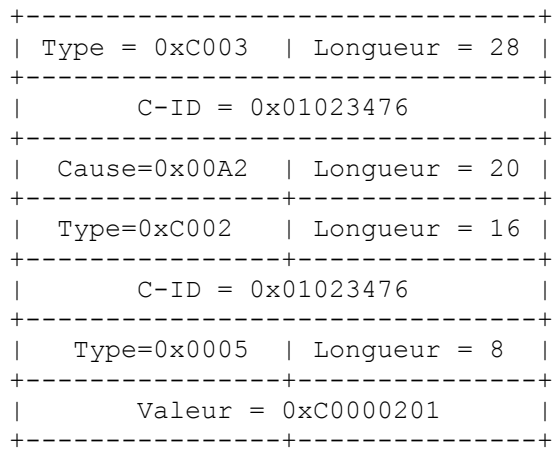


4.3.3 Demande de suppression de l'adresse IP de source

Le receveur de cette erreur a envoyé une demande de suppression de l'adresse IP de source du message ASCONF. Cette erreur indique que la demande est rejetée.



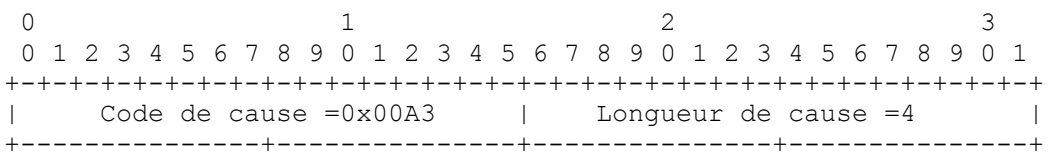
Un exemple d'un échec de suppression dans un TLV Cause d'erreur ressemblerait à ce qui suit dans le message de réponse ASCONF-ACK :



Note de mise en œuvre : Il est peu probable qu'un point d'extrémité génère un paquet à partir de l'adresse en cours de suppression, sauf si le point d'extrémité ne fait pas un choix d'adresse de source appropriée.

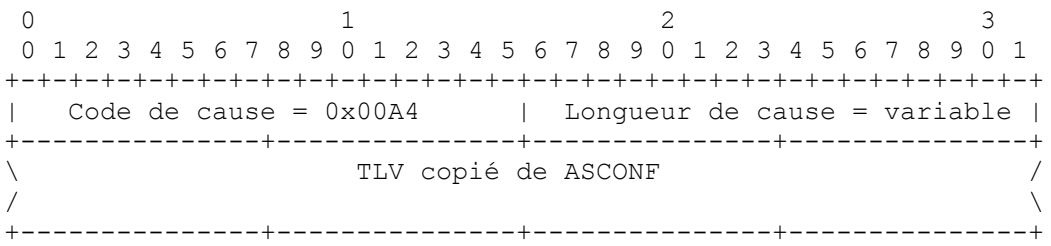
4.3.4 Association interrompue à cause d'un ASCONF-ACK illégal

Cette erreur est à inclure dans un ABORT qui est généré à cause de la réception d'un ASCONF-ACK qui n'était pas attendu mais est plus grand que le numéro de séquence actuel (voir le paragraphe 5.3, Règle F0). Noter qu'un numéro de séquence est plus grand que le dernier numéro de séquence acquitté si il est soit le prochain numéro de séquence, soit pas plus de 2**31-1 supérieur au numéro de séquence courant. Les numéros de séquence plus petits que le dernier numéro de séquence acquitté sont ignorés en silence.



4.3.5 Demande refusée - pas d'autorisation

Cette cause d'erreur peut être incluse pour rejeter une demande sur la base des politiques de sécurité locales.



5. Procédures

Cette section pose les procédures spécifiques du type de tronçon de changement de configuration d'adresse et leur traitement.

5.1 Procédures du tronçon ASCONF

Quand un point d'extrémité a un changement d'ASCONF signalé à envoyer au point d'extrémité distant, il DOIT faire ce qui suit :

A1) Créer un tronçon ASCONF comme défini au paragraphe 4.1.1. Le tronçon DOIT contenir tous les TLV d'information nécessaires à envoyer au point d'extrémité distant, et une identité de corrélation unique pour chaque demande.

A2) Un numéro de séquence DOIT être alloué au tronçon. Le numéro de séquence DOIT être supérieur de un au précédent. Le numéro de séquence DOIT être initialisé au début de l'association à la même valeur que le numéro de séquence de transmission initial (TSN) et chaque fois qu'un nouveau tronçon ASCONF est créé, il DOIT être incrémenté de un après l'allocaion du numéro de séquence au nouveau tronçon créé.

A3) Si aucun paquet SCTP avec un ou plusieurs tronçons ASCONF n'est en instance (non acquitté) avec l'homologue distant, envoyer le tronçon et passer à l'étape A4. Si un tronçon ASCONF est en instance, alors le tronçon ASCONF devrait être mis en file d'attente pour une transmission ultérieure et aucune autre action ne devrait être effectuée jusqu'à ce que le ASCONF précédent soit acquitté ou qu'une fin de temporisation se produise.

A4) L'envoyeur DOIT lancer un temporisateur de retransmission (RTO) T-4 , en utilisant la valeur de RTO de l'adresse de destination choisie (normalement, le chemin principal ; voir les détails au paragraphe 6.4 de la [RFC4960].

A5) Quand le ASCONF-ACK qui accuse réception du dernier numéro de séquence envoyé arrive, l'envoyeur DOIT arrêter

le temporisateur RTO T-4, et mettre à zéro les compteurs appropriés d'association et d'erreur de destination comme défini aux paragraphes 8.1 et 8.2 de la [RFC4960].

A6) Le point d'extrémité DOIT traiter tous les TLV au sein des ASCONF-ACK pour trouver les informations d'état particulières retournées aux diverses demandes envoyées. Utiliser les identifiants de corrélation pour corréler la demande et les réponses.

A7) Si une réponse d'erreur est reçue pour un paramètre de TLV, tous les TLV sans réponse avant le TLV en échec sont considérés comme réussis si ils ne sont pas rapportés. Tous les TLV après la réponse d'échec sont considérés comme en échec sauf si une indication de succès spécifique est présente pour le paramètre.

A8) Si il n'y a pas de réponse à des paramètres de TLV spécifiques, et si aucun échec n'est indiqué, alors toutes les demandes sont considérées comme réussies.

A9) Si l'homologue répond à un ASCONF avec un tronçon ERROR rapportant qu'il ne reconnait pas le type de tronçon ASCONF, l'envoyeur de l'ASCONF NE DOIT PAS envoyer d'autres tronçons ASCONF et DOIT arrêter son temporisateur T-4.

Si le temporisateur RTO T-4 expire, le point d'extrémité DOIT faire ce qui suit :

B1) Incrémenter les compteurs d'erreur et effectuer une détection de défaillance de chemin sur l'adresse de destination appropriée comme défini aux paragraphes 8.1 et 8.2 de la [RFC4960].

B2) Incrémenter les compteurs d'erreur de l'association et effectuer une détection de défaillance de point d'extrémité sur l'association comme défini aux paragraphes 8.1 et 8.2 de la [RFC4960].

B3) Réduire la valeur de RTO de l'adresse de destination à laquelle le tronçon ASCONF a été envoyé en doublant la valeur du temporisateur de RTO.

Note : la valeur de RTO est utilisée dans le réglage de tous les types de temporisateur pour SCTP. Chaque adresse de destination a une seule estimation de RTO.

B4) Retransmettre le dernier tronçon ASCONF envoyé et si possible choisir une autre adresse de destination (voir le paragraphe 6.4.1 de la [RFC4960]). Un point d'extrémité NE DOIT PAS ajouter de nouveaux paramètres à ce tronçon ; il DOIT être le même (incluant son numéro de séquence) que le dernier ASCONF envoyé. Un point d'extrémité PEUT, cependant, grouper un ASCONF supplémentaire avec des nouveaux paramètres ASCONF avec le numéro de séquence suivant. Pour les détails, voir le paragraphe 5.5.

B5) Redémarrer le temporisateur RTO T-4. Noter que si une destination différente est choisie, alors le RTO utilisé va être celui de la nouvelle adresse de destination.

Note : le nombre total de retransmissions est limité par B2 ci-dessus. Si le maximum est atteint, l'association va échouer et entrer dans l'état CLOSED (voir les détails au paragraphe 6.4.1 de la [RFC4960]).

5.1.1 Contrôle d'encombrement des tronçons ASCONF

Pour définir les procédures de transfert de tronçon ASCONF, il est essentiel que ces transferts NE DOIVENT PAS causer d'encombrement au sein du réseau. Pour faire cela, on met les restrictions suivantes au transfert de tronçons ASCONF :

C1) Un seul paquet SCTP contenant des tronçons ASCONF PEUT être en transit et non acquitté à la fois. Si un envoyeur, après l'envoi d'un tronçon ASCONF, décide qu'il a besoin de transférer un autre tronçon ASCONF, il DOIT attendre le tronçon ASCONF-ACK retourné du précédent tronçon ASCONF avant d'envoyer un ASCONF suivant. Note : cette restriction lie chaque côté, de sorte qu'à tout moment, deux ASCONF peuvent être en transit sur toute association donnée (un envoyé de chaque point d'extrémité). Cependant, quand un tronçon ASCONF est retransmis du fait d'une fin de temporisation, les tronçons ASCONF supplémentaires détenus peuvent être groupés dans le paquet de retransmission comme décrit au paragraphe 5.5.

C2) Un tronçon ASCONF peut être groupé avec un autre type de tronçon incluant d'autres tronçons ASCONF. Si ils sont groupés avec d'autres tronçons ASCONF, les tronçons DOIVENT apparaître dans l'ordre par rapport à leur numéro de séquence.

C3) Un tronçon ASCONF-ACK peut être groupé avec un autre type de tronçon incluant d'autres tronçons ASCONF-ACK. Si ils sont groupés avec d'autres tronçons ASCONF-ACK, les tronçons DOIVENT apparaître dans l'ordre par rapport à leur numéro de séquence.

C4) Les tronçons ASCONF et ASCONF-ACK NE DOIVENT PAS être envoyés dans un état SCTP autre que ÉTABLI, FERMETURE-EN-COURS, FERMETURE-REÇUE, et FERMETURE-ENVOYÉE.

C5) Un tronçon ASCONF et un tronçon ASCONF-ACK NE DEVRAIENT PAS être plus grands que la PMTU. Si la PMTU est inconnue, alors la PMTU devrait être réglée à la PMTU minimum. La PMTU minimum dépend de la version IP utilisée pour la transmission, et est le plus petit de 576 octets et de la la MTU du premier bond pour IPv4 [RFC1122] et 1280 octets pour IPv6 [RFC2460].

Un envoyeur d'ASCONF sans ces restrictions pourrait éventuellement inonder le réseau avec un grand nombre d'opérations séparées de changement d'adresse, causant donc l'encombrement du réseau.

Si l'envoyeur d'un tronçon ASCONF reçoit une erreur de fonctionnement indiquant que le type de tronçon ASCONF n'est pas compris, l'envoyeur NE DOIT alors PAS envoyer d'autres tronçons ASCONF à l'homologue. Le point d'extrémité devrait aussi informer l'application de couche supérieure que le point d'extrémité homologue ne prend pas en charge les extensions détaillées dans le présent document.

5.2 À réception d'un tronçon ASCONF

Quand un point d'extrémité reçoit an tronçon ASCONF de l'homologue distant, des procédures spéciales peuvent être nécessaires pour identifier l'association à laquelle le tronçon ASCONF est associé. Pour trouver correctement l'association, les procédures suivantes DEVRAIT être respectées :

D1) Utiliser l'adresse de source et le numéro d'accès de l'envoyeur pour tenter d'identifier l'association (c'est-à-dire, utiliser la même méthode que définie dans la [RFC4960] pour tous les autres tronçons SCTP). Si elle est trouvée, passer à la règle D4.

D2) Si l'association n'est pas trouvée, utiliser l'adresse dans le TLV Paramètre d'adresse, combinée avec le numéro d'accès trouvé dans l'en-tête SCTP commun. Si elle est trouvée, passer à la règle D4.

D2-ext) Si plus d'un tronçon ASCONF sont empaquetés ensemble, utiliser l'adresse trouvée dans le TLV Paramètre d'adresse ASCONF de chaque tronçon ASCONF suivant. Si elle est trouvée, passer à la règle D4.

D3) Si ni D1, D2, ni D2-ext ne localise l'association, traiter le tronçon comme un paquet "sorti de nulle part" comme défini dans la [RFC4960].

D4) Suivre les règles normales pour valider l'étiquette de vérification SCTP trouvée dans la [RFC4960].

D5) Après la validation de l'étiquette de vérification, le traitement normal de tronçon devrait se poursuivre. Avant de trouver le tronçon ASCONF, le receveur DOIT rencontrer un tronçon AUTH comme décrit dans la [RFC4895]. Si l'authentification échoue, ou si le tronçon AUTH manque, le receveur DOIT éliminer en silence ce tronçon et le reste du paquet.

Après l'identification et la vérification de l'association, ce qui suit devrait être effectué pour traiter de façon appropriée le tronçon ASCONF :

E1) Si la valeur trouvée dans le numéro de séquence du tronçon ASCONF est égale au ("Numéro de séquence d'homologue" + 1) et si le numéro de séquence du tronçon ASCONF est le premier dans le paquet SCTP, le point d'extrémité PEUT purger tous les anciens ASCONF-ACK mis en antémémoire jusqu'au "Numéro de séquence d'homologue" et passer ensuite à la règle E4.

E1-ext) Si la valeur trouvée dans le numéro de séquence du tronçon ASCONF est égale à ("Numéro de séquence d'homologue" + 1) et si le tronçon ASCONF N'est PAS le premier numéro de séquence dans le paquet SCTP, passer à la règle E4, mais NE PAS purger de ASCONF- ACK ou informations d'état dans l'antémémoire.

E2) Si la valeur trouvée dans le numéro de séquence est inférieure à ("Numéro de séquence d'homologue" + 1) sauter

simplement au prochain ASCONF, et inclure dans le paquet de réponse sortant toutes les réponses ASCONF-ACK mises précédemment en antémémoire qui ont été envoyées et sauvegardées qui correspondent au numéro de séquence de l'ASCONF. Note : Il est possible qu'il n'existe pas de tronçon ASCONF-ACK en antémémoire. Cela va se produire quand un ASCONF plus ancien arrive décalé. Dans ce cas, le receveur devrait sauter le tronçon ASCONF et ne pas inclure de tronçon ASCONF-ACK pour ce tronçon.

E3) Ensuite, traiter chaque ASCONF un par un comme ci-dessus tant que le numéro de séquence de l'ASCONF est inférieur à ("Numéro de séquence d'homologue" + 1).

E4) Quand le numéro de séquence correspond au prochain attendu, traiter le ASCONF comme décrit ci-dessous et après avoir traité le tronçon ASCONF, ajouter un tronçon ASCONF-ACK au paquet de réponse et en mettre une copie en antémémoire (pour le cas où il devrait être retransmis ultérieurement).

V1) Traiter les TLV contenus au sein du tronçon en effectuant les actions appropriées indiquées par chaque type de TLV. Les TLV DOIVENT être traités dans l'ordre au sein du tronçon. Par exemple, si l'envoyeur met trois TLV dans un tronçon, le premier TLV (le plus proche de l'en-tête de tronçon) dans le tronçon DOIT être traité en premier. Le prochain TLV dans le tronçon (celui du milieu) DOIT être traité ensuite et finalement, le dernier TLV dans le tronçon DOIT être traité en dernier.

V2) En traitant le tronçon, le receveur devrait construire un message de réponse avec les TLV d'erreur appropriés, comme spécifié dans les bits de type de paramètre, pour tout paramètre ASCONF qu'il ne comprend pas. Pour indiquer un paramètre non reconnu, le type de cause 8 devrait être utilisé comme défini dans ERROR au paragraphe 3.3.10.8 de la [RFC4960]. Le point d'extrémité peut aussi utiliser la réponse pour porter les rejets pour d'autres raisons, comme des manques de ressources, etc., en utilisant le TLV Cause d'erreur et une condition d'erreur appropriée.

Note : une réponse positive est impliquée si aucune erreur n'est indiquée par l'envoyeur.

V3) Toutes les réponses DOIVENT copier le champ Identifiant de corrélation de demande ASCONF reçu dans le paramètre ASCONF provenant du TLV auquel on répond, dans le champ Identifiant de corrélation de demande ASCONF dans le paramètre de réponse.

V4) Après le traitement du tronçon entier, le receveur de l'ASCONF DOIT mettre en file d'attente le tronçon de réponse ASCONF-ACK pour transmission après le traitement du reste du paquet SCTP. Cela permet que le tronçon ASCONF-ACK soit groupé avec d'autres tronçons ASCONF-ACK ainsi qu'avec des réponses supplémentaires, par exemple, un tronçon d'accusé de réception sélectif (SACK, *Selective Acknowledgment*).

V5) Mettre à jour le "Numéro de séquence d'homologue" à la valeur trouvée dans le champ Numéro de séquence.

E5) Autrement, le tronçon ASCONF est éliminé car il doit être soit un paquet périmé, soit il provient d'un attaquant. Le receveur d'un tel paquet PEUT enregistrer l'événement pour les besoins de la sécurité.

E6) Quand tous les tronçons ASCONF sont traités pour ce paquet SCTP, renvoyer le paquet d'une seule réponse accumulés avec tous les tronçons de ASCONF-ACK. L'adresse de destination du paquet SCTP contenant les tronçons ASCONF-ACK DOIT être l'adresse de source du paquet SCTP qui contenait les tronçons ASCONF.

E7) Lors du traitement des tronçons ASCONF dans le paquet SCTP, si le paquet de réponse va excéder la PMTU du chemin de retour, le receveur DOIT arrêter d'ajouter des ASCONF-ACK supplémentaires dans le paquet de réponse mais DOIT continuer de traiter tous les tronçons ASCONF, en sauvegardant les réponses de tronçon ASCONF-ACK dans sa copie d'antémémoire. L'envoyeur du tronçon ASCONF va plus tard retransmettre les tronçons ASCONF qui n'ont pas eu de réponse, moment auquel les copies en antémémoire des réponses qui ne tiendraient PAS dans la PMTU peuvent être envoyées à l'homologue.

Note : ces règles ont été présentées dans l'hypothèse que la mise en œuvre met en antémémoire les anciens ASCONF-ACK en cas de perte de paquets SCTP sur le chemin des ACK. Il est admis qu'une mise en œuvre conserve cet état sous une autre forme si elle l'estime approprié, pour autant que cette forme résulte en la même séquence de ASCONF-ACK retournée à l'homologue que celle mentionnée ci-dessus.

5.3 Règles générales pour la manipulation d'adresse

Quand on construit les paramètres de TLV pour le tronçon ASCONF qui vont ajouter ou supprimer des adresses IP, les

règles suivantes DOIT être appliquées :

F0) Si un point d'extrémité reçoit un ASCONF-ACK supérieur ou égal au prochain numéro de séquence à utiliser mais qu'aucun tronçon ASCONF n'est en instance, le point d'extrémité DOIT interrompre l'association avec un ABORT. Noter qu'un numéro de séquence est supérieur si il n'est pas plus grand de 2^^31-1 que le numéro de séquence courant (en utilisant l'arithmétique des séries).

F1) Quand on ajoute une adresse IP à une association, l'adresse IP N'est PAS considérée pleinement ajoutée à l'association avant l'arrivée du ASCONF-ACK. Cela signifie que jusqu'au moment où le ASCONF contenant l'ajout est acquitté, l'envoyeur NE DOIT PAS utiliser la nouvelle adresse IP comme source de TOUT paquet SCTP sauf ceux portant un tronçon ASCONF. Le receveur de la demande d'ajout d'adresse IP peut utiliser immédiatement l'adresse comme destination. Le receveur DOIT utiliser la procédure de vérification de chemin pour l'adresse ajoutée avant de l'utiliser. Le receveur NE DOIT PAS envoyer de paquets à la nouvelle adresse sauf pour le tronçon ASCONF-ACK correspondant ou les tronçons HEARTBEAT pour la vérification de chemin avant que le nouveau chemin soit vérifié. Si le ASCONF-ACK est envoyé à la nouvelle adresse, il PEUT être groupé avec le tronçon HEARTBEAT pour la vérification de chemin.

F2) Après l'arrivée du ASCONF-ACK d'un ajout d'adresse IP, le point d'extrémité PEUT commencer à utiliser l'adresse IP ajoutée comme adresse de source pour tout type de tronçon SCTP.

F3a) Si un point d'extrémité reçoit un TLV Cause d'erreur indiquant que les paramètres d'ajout ou de suppression d'adresse IP n'ont pas été compris, le point d'extrémité DOIT considérer que l'opération a échoué et NE DOIT PAS tenter d'envoyer d'autre demande d'ajout ou de suppression à l'homologue.

F3b) Si un point d'extrémité reçoit un TLV Cause d'erreur indiquant que le paramètre Régler l'adresse IP comme adresse IP principale n'a pas été compris, le point d'extrémité DOIT considérer que l'opération a échoué et NE DOIT PAS tenter d'envoyer d'autre demande Établir l'adresse IP principale à l'homologue.

F4) Lors de la suppression d'une adresse IP d'une association, l'adresse IP DOIT être considérée comme une adresse de destination valide pour la réception de paquets SCTP jusqu'à ce que le ASCONF-ACK arrive et NE DOIT PAS être utilisée comme adresse de source pour les paquets suivants. Cela signifie que tout datagramme qui arrive avant le ASCONF-ACK destiné à l'adresse IP à supprimer DOIT être considéré comme faisant partie de l'association courante. Une considération particulière est que les tronçons ABORT qui arrivent à destination de l'adresse IP à supprimer DOIVENT être ignorés (voir les détails au paragraphe 5.3.1).

F5) Un point d'extrémité NE DOIT PAS supprimer sa dernière adresse IP restante d'une association. En d'autres termes, si un point d'extrémité N'est PAS multi-rattachements, il NE DOIT PAS utiliser la suppression d'adresse IP sans un Ajout d'adresse IP précédant le paramètre de suppression dans le tronçon ASCONF. Ou, si un point d'extrémité envoie plusieurs demandes de suppression d'adresses IP, il NE DOIT PAS supprimer toutes les adresses IP que l'homologue a mentionnées pour le demandeur.

F6) Un point d'extrémité NE DOIT PAS établir une adresse de source d'en-tête IP pour un paquet SCTP contenant le tronçon ASCONF comme étant la même qu'une adresse en cours de suppression par le tronçon ASCONF.

F7) Si une demande de supression est reçue pour la dernière adresse IP restante d'un point d'extrémité homologue, le receveur DOIT envoyer un TLV Cause d'erreur avec la cause d'erreur réglée au nouveau code d'erreur "Demande de suppression de la dernière adresse IP restante". La suppression demandée NE DOIT PAS être effectuée ou faire l'objet d'une action autre que d'envoyer le ASCONF-ACK.

F8) Si une demande de suppression est reçue pour une adresse IP qui est aussi l'adresse de source du paquet IP qui contenait le tronçon ASCONF, le receveur DOIT rejeter cette demande. Pour rejeter la demande, le receveur DOIT envoyer un TLV Cause d'erreur réglé au nouveau code d'erreur "Demande de suppression de l'adresse IP de source" (sauf si la règle F5 a aussi été violée, et dans ce cas c'est le code d'erreur "Demande de suppression de la dernière adresse IP restante" qui est envoyé).

F9) Si un point d'extrémité reçoit une demande Ajout d'adresse IP et qu'il n'a pas les ressources locales pour ajouter cette nouvelle adresse à l'association, il DOIT retourner un TLV Cause d'erreur réglé au nouveau code d'erreur "Opération refusée à cause de manque de ressources".

F10) Si un point d'extrémité reçoit une réponse "Plus de ressources" à sa demande d'ajout d'une adresse IP à une association, il doit soit interrompre l'association avec un ABORT, soit considérer que l'adresse ne fait pas partie de

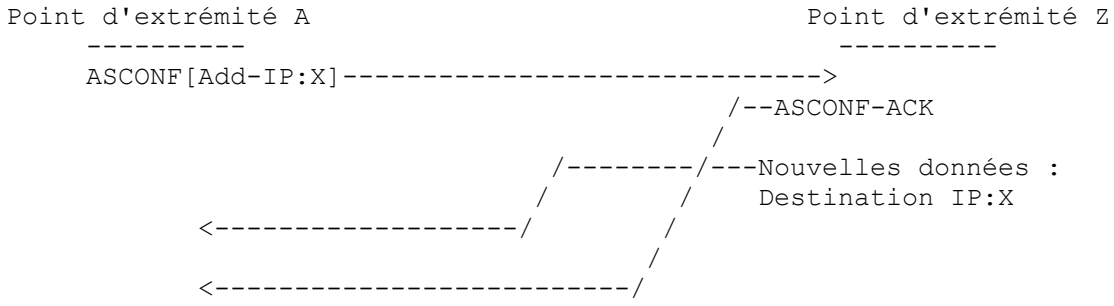
l'association. En d'autres termes, si le point d'extrémité n'interrompt pas l'association, il doit considérerque la tentative d'ajout a échoué et NE PAS utilier cette adresse car son homologue va traiter les paquets SCTP destinés à l'adresse comme des paquets "sortis de nulle part" (OOTB, *Out Of The Blue*).

F11) Quand un point d'extrémité qui reçoit un ASCONF pour ajouter une adresse IP envoie un "Plus de ressources" dans sa réponse, il DOIT aussi faire échouer toute demande suivante d'ajout ou de suppression groupée dans le ASCONF. Le receveur NE DOIT PAS rejeter un ADD et ensuite accepter un DELETE d'une adresse IP dans le même tronçon ASCONF. En d'autres termes, une fois qu'un receveur commence à faire échouer une demande ADD ou DELETE, il doit faire échouer toutes les demandes ADD ou DELETE suivantes contenues dans ce seul ASCONF.

F12) Quand un point d'extrémité reçoit une demande de supression d'une adresse IP qui est l'adresse principale actuelle, comment ce point d'extrémité choisit la nouvelle adresse principale est une décision de la mise en œuvre.

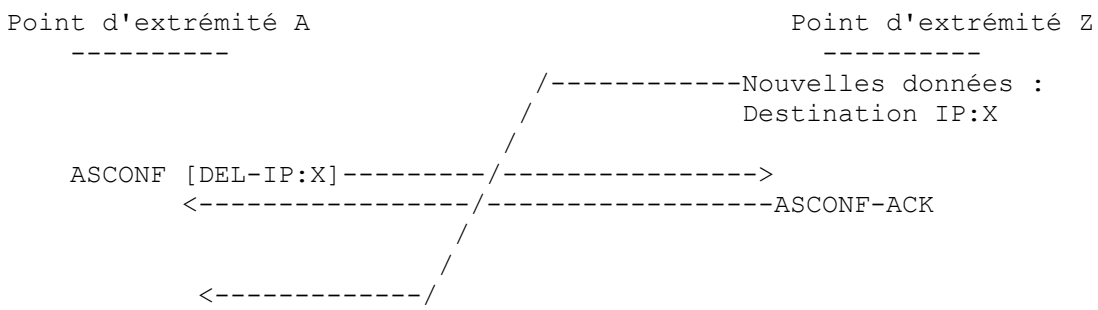
F13) Quand un point d'extrémité reçoit une demande DELETE valide sur une adresse IP, le point d'extrémité DOIT considérer que l'adresse ne fait plus partie de l'association. Il NE DOIT PAS envoyer de paquets SCTP pour l'association à cette adresse et il DOIT traiter les paquets suivants reçus de cette adresse comme sortis de nulle part. Durant l'intervalle entre l'envoi de l'ASCONF et la réception de l'ASCONF-ACK, il PEUT recevoir des tronçons DATA déclassés. Les exemples suivants illustrent ces problèmes :

F14) Toutes les adresses ajoutées par la réception d'un tronçon ASCONF DOIVENT être mises dans l'état NON CONFIRMÉ et DOIVENT avoir la vérification de chemin effectuée sur elles avant que l'adresse puisse être utilisée comme décrit au paragraphe 5.4 de la [RFC4960].



Dans l'exemple ci-dessus, on voit une nouvelle adresse IP (X) ajoutée au point d'extrémité A. Cependant, du fait du déclassement du paquet dans le réseau, un nouveau tronçon DATA est envoyé et arrive au point d'extrémité A avant le ASCONF-ACK qui confirme l'ajout de l'adresse à l'association.

Un problème similaire existe avec la suppression d'un adresse IP comme suit :



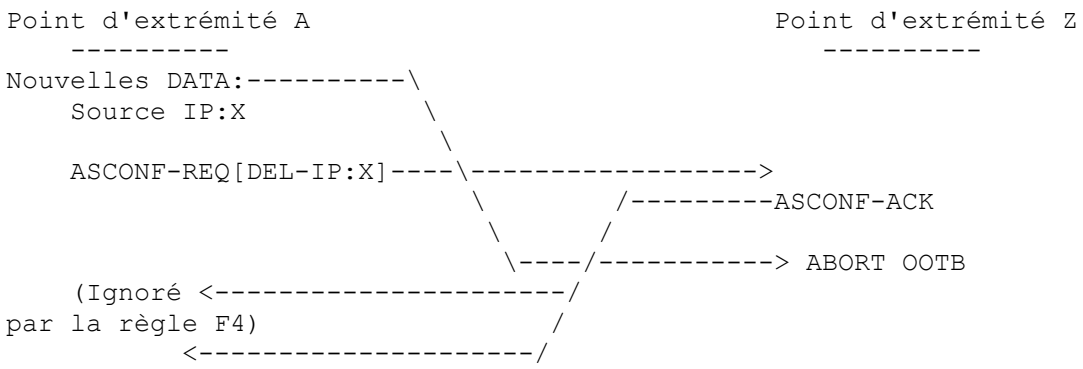
Dans cet exemple, on voit un tronçon DATA destiné à IP:X (qui est sur le point d'être supprimée) qui arrive après l'achèvement de la suppression. Pour le cas de ADD, un point d'extrémité DEVRAIT considérer la nouvelle adresse IP ajoutée pour les besoins d'envoi de données à l'association avant que l'ASCONF-ACK soit reçu. Le point d'extrémité NE DOIT PAS envoyer de données à partir de cette nouvelle adresse tant que le ASCONF-ACK n'est pas arrivé, mais il peut recevoir des données déclassées comme illustré et NE DOIT PAS traiter ces données comme un datagramme OOTB (voir au paragraphe 8.4 de la [RFC4960]). Il PEUT éliminer les données en silence ou il PEUT les considérer comme partie de l'association, mais il NE DOIT PAS répondre avec un ABORT.

Pour le cas de DELETE, un point d'extrémité PEUT répondre à l'arrivée tardive d'un paquet DATA comme à un datagramme OOTB ou il PEUT conserver l'adresse IP en cours de suppression comme encore valide pour une courte

période. Si il traite le paquet DATA comme OOTB, l'homologue va éliminer en silence le ABORT (car au moment où le ABORT est envoyé, l'homologue va avoir retiré l'adresse IP de cette association). Si le point d'extrémité choisit de garder l'adresse IP comme valide pendant un temps, il NE DOIT PAS la conserver comme valide plus longtemps que deux intervalles de RTO pour la destination en cours de suppression.

5.3.1 Cas particulier des tronçons ABORT OOTB

Un autre cas qu'il vaut la peine de mentionner est illustré ci-dessous :



Dans ce cas, durant la suppression d'une adresse IP, un ABORT DOIT être ignoré si l'adresse de destination du messsage ABORT est celle de la destination en cours de suppression.

5.3.2 Cas particulier de changement d'une adresse

Dans certaines instances, l'envoyeur peut seulement avoir une adresse IP dans une association qui est en cours de renumérotation. Quand cela se produit, l'envoyeur peut n'être pas capable d'envoyer la paire ADD/DELETE appropriée à l'homologue, et peut utiliser l'ancienne adresse comme source dans l'en-tête IP. Pour cette raison, l'envoyeur DOIT remplir le champ Paramètre d'adresse avec une adresse qui fait partie de l'association (dans ce cas, celle qui va être supprimée). Cela va permettre au receveur de localiser l'association sans utiliser l'adresse de source trouvée dans l'en-tête IP.

Le receveur d'un tel tronçon DOIT toujours utiliser d'abord l'adresse de source trouvée dans l'en-tête IP en cherchant l'association. Le receveur devrait tenter d'utiliser l'adresse trouvée dans le champ Paramètre d'adresse seulement si la recherche en utilisant l'adresse de source de l'en-tête IP échoue. Le receveur DOIT dans ce cas répondre à l'adresse de source du paquet, qui est la nouvelle adresse qui a été ajoutée par le ASCONF (car l'ancienne adresse ne fait plus partie de l'association après le traitement).

5.4 Établissement de l'adresse principale

Un envoyeur du paramètre Établissement de l'adresse principale PEUT choisir d'envoyer cela combiné avec un ajout ou suppression d'une adresse. Un envoyeur DOIT seulement envoyer une demande Établissement de l'adresse principale à une adresse qui est déjà considérée comme faisant partie de l'association. En d'autres termes, si un envoyeur combine un Établissement de l'adresse principale avec une demande d'ajout de nouvelle adresse IP, le Établissement de l'adresse principale va être éliminé sauf si la demande d'ajout est à traiter AVANT le Établissement de l'adresse principale (c'est-à-dire, qu'elle précède le Établissement de l'adresse principale).

Une demande Établissement de l'adresse principale PEUT aussi apparaître dans un tronçon, INIT ou INIT-ACK qui peut donner un avis au point d'extrémité homologue sur les adresses que l'envoyeur du INIT ou INIT-ACK préfèrerait comme adresse principale.

La demande d'établir une adresse comme chemin principal est une option que le receveur DEVRAIT effectuer. Elle est considérée comme un avis au receveur de la meilleure adresse de destination à utiliser lors de l'envoi de paquets SCTP (du point de vue du demandeur). Si une demande arrive pour que le receveur établisse comme principale une adresse qui n'existe pas, le receveur NE DEVRAIT PAS honorer la demande, laissant son adresse principale existante inchangée.

5.5 Groupage de plusieurs ASCONF

Dans le cas normal, un seul ASCONF est envoyé dans un paquet et une seule réponse ASCONF-ACK est reçue. Cependant, dans le cas d'une perte d'un paquet SCTP contenant un ASCONF ou ASCONF-ACK, il est permis à l'envoyeur de grouper des ASCONF supplémentaires dans la retransmission. En groupant plusieurs ASCONF, les règles suivantes DOIVENT être respectées :

1. Les tronçons ASCONF précédemment transmis DOIVENT être laissés inchangés.

2. Chaque paquet SCTP contenant des tronçons ASCONF DOIT être groupé en commençant avec le plus petit numéro de séquence ASCONF dans le paquet (le plus prooche de l'en-tête de tronçon) et en procédant en ordre séquentiel du plus petit au plus grand numéro de séquence ASCONF.

3. Tous les ASCONF au sein du paquet DOIVENT être adjacents à chaque autre, c'est-à-dire, aucun autre type de tronçon ne doit séparer les ASCONF.

4. Chaque nouvelle adresse de recherche ASCONF DOIT être remplie comme si le précédent ASCONF avait été traité et accepté.

6. Considérations sur la sécurité

L'ajout et/ou la suppression d'une adresse IP à une association existante fournit un mécanisme supplémentaire par lequel les associations existantes peuvent être capturées. Donc, le présent document exige l'utilisaton du mécanisme d'authentification défini dans la [RFC4895] pour limiter la capacité d'un attaquant de capturer une association.

Capturer une association en utilisant l'ajout et la suppression d'une adresse IP est seulement possible pour un attaquant qui est capable d'intercepter les deux paquets initiaux de l'établissement d'association quand l'extension SCTP-AUTH est utilisée sans clé pré-partagée. Si cette menace est considérée comme possible, alors l'extension de la [RFC4895] DOIT être utilisée avec une clé préconfigurée partagée par la paire de points d'extrémité pour atténuer cette menace. Pour une analyse plus détaillée, voir la [RFC4895].

Quand le paramètre d'adresse dans les tronçons ASCONF avec des paramètres Add, IP Delete IP, ou Set Primary IP est un caractère générique, l'adresse de source du paquet est utilisée. Cette adresse n'est pas protégée par SCTP-AUTH [RFC4895] et un attaquant peut donc intercepter ce paquet et modifier l'adresse de source. Même si l'adresse de source n'est pas une qui est actuellement une solution de remplacement pour l'association, l'identification de l'association peut reposer sur les autres informations du paquet (peut-être l'étiquette de vérification, par exemple). Un attaquant sur le chemin peut donc modifier l'adresse de source comme il le désire.

Si le ASCONF inclut un Add IP avec une adresse à caractère générique, l'attaquant peut ajouter une adresse de son choix, qui fournit peu de dommages immédiats mais peut servir à établir des attaques ultérieures.

Si le ASCONF inclut un Delete IP avec une adresse à caractère générique, l'attaquant peut causer la suppression de toutes les adresses d'une association sauf une de son choix. L'adresse fournie par l'attaquant doit déjà appartenir à l'association, ce qui rend cela plus difficile pour l'attaquant. Cependant, la seule adresse restante pourrait être une que l'attaquant contrôle, par exemple, ou peut surveiller, etc. Au moins, l'envoyeur et le receveur trompé vont avoir une idée différente de ce que va être la seule adresse restante. Cela va éventuellement causer l'échec de l'association, mais en même temps, le receveur trompé pourrait transmettre des paquets à une adresse que l'envoyeur n'avait pas prévue.

Si le ASCONF inclut un Établir l'adresse IP principale avec une adresse comportant un caractère générique, alors l'attaquant peut causer l'utilisation d'une adresse comme adresse principale. Ceci est limité à une adresse qui appartient déjà à l'association, de sorte que le dommage est limité. Au moins, le résultat va être que le receveur utilise une adresse principale que l'envoyeur n'avait pas prévue. Cependant, si un Ajout d'adresse IP avec caractère générique et un Établir une adresse IP principale avec caractère génrique sont tous deux utilisés, alors l'attaquant peut modifier l'adresse de source pour à la fois ajouter à l'association une adresse de son choix et en faire l'adresse principale. Une telle combinaison présenterait à l'attaquant une opportunité de causer plus de dommages.

Noter que toutes ces attaques sont d'un attaquant sur le chemin. Les points d'extrémité qui pensent qu'il font face à une menace d'attaquants sur le chemin NE DEVRAIENT PAS utiliser d'adresses avec caractères génériques dans les paramètres ASCONF Add IP, Delete IP, ou Set Primary IP.

Si un point d'extrémité SCTP qui prend en charge cette extension reçoit un INIT qui indique que l'homologue prend en charge l'extension ASCONF mais NE prend PAS en charge l'extension de la [RFC4895], le receveur d'un tel INIT DOIT envoyer un ABORT en réponse. Noter qu'une mise en œuvre est aussi autorisée à éliminer en silence un tel INIT en option, mais dans AUCUNE circonstance une mise en œuvre n'est autorisée à poursuivre l'établissement de l'association en envoyant un INIT-ACK en réponse.

Une mise en œuvre qui reçoit un INIT-ACK qui indique que l'homologue ne prend pas en charge l'extension de la [RFC4895] NE DOIT PAS envoyer le COOKIE-ECHO pour établie l'association. À la place, la mise en œuvre DOIT éliminer le INIT-ACK et rapporter à la couche supérieure de l'utilisateur qu'une association ne peut pas être établie en détruisant le bloc de contrôle de transmission (TCB, *Transmission Control Block*).

D'autres types d'attaques, par exemple, de bombage, sont discutés en détail dans la [RFC5062]. L'attaque de bombage, en particulier, est contrée par l'utilisation d'un nom occasionnel aléatoire et est exigée par la [RFC4960].

Un attaquant sur le chemin peut modifier le paramètre INIT et INIT-ACK "Extensions prises en charge" (et les paramètres en rapport avec l'authentification) pour produire un déni de service. Si l'attaquant sur le chemin supprime les paramètres relatifs à la [RFC4895] d'un INIT qui indique qu'il prend en charge l'extension ASCONF, l'association ne sera pas établie. Si l'attaquant sur le chemin ajoute un paramètre "Extensions prises en charge" mentionnant le type ASCONF à un INIT ou INIT-ACK qui ne porte pas de paramètres relatifs à AUTH, l'association ne sera pas établie. Si l'attaquant sur le chemin supprime le paramètre "Extensions prises en charge" (ou supprime le type ASCONF de ce paramètre) de l'INIT ou INIT-ACK, alors l'association ne sera pas capable d'utiliser le dispositif ADD-IP. Si l'attaquant sur le chemin ajoute le paramètre "Extensions prises en charge" mentionnant le type ASCONF à un INIT-ACK qui n'en porte pas (mais porte des paramètres en relation avec AUTH) alors l'envoyeur de l'INIT peut utiliser ASCONF alors que l'envoyeur de l'INIT-ACK ne le prend pas en charge. Cela sera découvert plus tard si l'envoyeur de l'INIT a transmis un ASCONF, mais l'envoyeur de l'INIT pourrait avoir fait des choix de configuration à ce moment. Comme le INIT et INIT-ACK ne sont pas protégés par le dispositif AUTH, il n'y a pas de moyen de contrer de telles attaques. Noter cependant qu'un attaquant sur le chemin capable de modifier le INIT et INIT-ACK va très certainement être aussi capable d'empêcher le INIT et INIT-ACK d'être livré ou de modifier les étiquettes de vérification ou la somme de contrôle pour causer l'élimination du paquet, de sorte que les extensions prises en charge ajoutent peu de vulnérabilité supplémentaire (par rapport à empêcher la formation d'association) au protocole SCTP. La capacité d'empêcher l'utilisation de cette nouvelle caractéristique est une vulnérabilité supplémentaire de SCTP mais seulement pour cette nouvelle caractéristique.

L'indication de couche d'adaptation est sujette à corruption, insertion, ou suppression dans les tronçons INIT et INIT-ACK par un attaquant sur le chemin. Ce paramètre DEVRAIT être opaque au protocole SCTP (voir le paragraphe 4.2.6) et donc des changements au paramètre ne vont probablement pas affecter le protocole SCTP. Cependant, toute couche d'adaptation qui est définie DEVRAIT considérer ses propres vulnérabilités dans la section des considérations sur la sécurité de la RFC qui définit son codet d'adaptation.

Le paramètre" Établir l'adresse principale IP" est sujet à corruption, insertion, ou suppression par un attaquant sur le chemin quand il est inclus dans les tronçons INIT et INIT-ACK. L'attaquant pourrait utiliser cela pour influencer le receveur à choisir une adresse de son propre choix (une sur laquelle il a le contrôle, une qui serait moins désirable pour l'envoyeur, etc.). Un attaquant sur le chemin aurait aussi la capacité d'inclure ou supprimer des adresses pour l'association dans le INIT ou INIT-ACK, afin de n'être pas limité dans les adresses qu'il peut spécifier dans le Établir l'adresse principale IP. Les points d'extrémité qui souhaitent éviter cette possible menace PEUVENT différer l'envoi de la demande initiale Établir l'adresse principale IP et attendre que l'association soit pleinement établie avant d'envoyer un ASCONF pleinement protégé avec le Établir l'adresse principale IP comme son seul paramètre.

7. Considérations relatives à l'IANA

Le présent document définit les nouveaux paramètres, tronçons, et erreurs SCTP suivants (http://www.iana.org/assignments/sctp-parameters) :

- deux nouveaus types de tronçon,
- six types de paramètres, et
- cinq nouvelles causes d'erreur SCTP.

Les types de tronçon avec les valeurs qui leur sont allouées sont montrés ci-dessous :

Type de tronçon	Nom de tronçon
0xC1	Changement de configuration d'adresse (ASCONF)
0x80	Accusé de réception de configuration d'adresse (ASCONF-ACK)

Les types de paramètres sont :

Type de paramètre	Nom de paramètre
0x8008	Extensions prises en charge
0xC001	Ajout d'adresse IP
0xC002	Suppression d'adresse IP
0xC003	Indication de cause d'erreur
0xC004	Établir l'adresse principale
0xC005	Indication de succès
0xC006	Indication de couche d'adaptation

Les causes d'erreur sont :

Valeur de code de cause	Code de cause
0x00A0	Demande de suppression de la dernière adresse IP restante
0x00A1	Opération refusée pour manque de ressources
0x00A2	Demande de suppression de l'adresse IP de source
0x00A3	Association interrompue à cause d'un ASCONF-ACK illégal
0x00A4	Demande refusée - pas d'autorisation

Le présent document définit aussi un codet d'adaptation. Le codet d'adaptation est un entier de 32 bits qui est alloué par l'IANA par action de consensus de l'IETF comme défini dans la [RFC2434]. Pour ce nouveau registre, aucune valeur initiale n'est ajoutée par le présent document ; cependant, la [RFC5043] va ajouter la première entrée.

8. Remerciements

Les auteurs tiennent à exprimer des remerciements particuliers à Michael Ramahlo et Phillip Conrad pour leurs extrêmes efforts dans les débuts de la formation de ce projet.

Les auteurs remercient Jon Berger, Mark Butler, Lars Eggert, Janardhan Iyengar, Greg Kendall, Seok Koh, Salvatore Loreto, Peter Lei, John Loughney, Sandy Murphy, Ivan Arias Rodriguez, Renee Revis, Marshall Rose, Ronnie Sellars, Chip Sharp, et Irene Ruengeler de leurs précieux commentaires.

Les auteurs tiennent aussi à donner une mention spéciale à Maria-Carmen Belinchon et Ian Rytina pour leurs contributions précoces à ce document et leurs commentaires pertinents.

Un merci particulier à James Polk, rédacteur abstrait de peu mais chanceux.

9. Références

9.1 Références normatives

[RFC1122] R. Braden, "Exigences pour les hôtes Internet – couches de communication", STD 3, octobre 1989. *(MàJ par* RFC6633, 8029, 9293)

[RFC1982] R. Elz, R. Bush, "Arithmétique des numéros de série", août 1996. (*MàJ* RFC1034, RFC1035) *(P.S.)*

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

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre 1998. *(Rendue obsolète par la* RFC5226)

[RFC2460] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6)", décembre 1998. *(MàJ par 5095, 6564 ; D.S ; Remplacée par RFC8200, STD 86)*

[RFC4895] M. Tuexen et autres, "Tronçons authentifiés dans le protocole de transmission de contrôle de flux (SCTP)", août 2007. *(P.S.)*

[RFC4960] R. Stewart, éd., "Protocole de transmission de commandes de flux (SCTP)", septembre 2007. (*Remplace RFC2960, RFC3309 ; P.S. ; Remplacée par RFC9260*)

9.2 Références pour information

[RFC5062] R. Stewart et autres, "Attaques contre la sécurité dans le protocole de transmission de contrôle de flux (SCTP) et contre mesures courantes", septembre 2007. *(Information)*

[RFC5043] C. Bestler et R. Stewart, éd., "Adaptation du placement direct des données (DDP) au protocole de transmission de contrôle de flux (SCTP)", octobre 2007. *(P.S. ; MàJ par RFC6581, RFC7146)*

Appendice A. Traitement d'adresse abstraite

A.1 Remarques générales

Cet appendice n'est pas normatif. Il est présent pour donner au lecteur une définition mathématique concise d'un point d'extrémité SCTP. Le texte qui suit fournit une définition de la notion de point d'extrémité pour discuter de la reconfiguration d'adresse. Il n'est pas destiné à restreindre les mises en œuvre de quelque façon que ce soit ; son but est de fournir seulement en ensemble de définitions. L'utilisation de ces définitions devrait rendre plus facile une discussion sur les questions d'adresse.

A.2 Points d'extrémité généralisés

Un point d'extrémité généralisé est une paire d'ensemble d'adresses IP et de numéro d'accès à un instant donné. La définition précise est la suivante :

Un point d'extrémité généralisé gE à l'instant t est donné par

gE(t) = ({IP1, ..., IPn}, Port)

où {IP1, ..., IPn} est un ensemble non vide d'adresses IP.

Noter que l'ajout et la suppression dynamique des adresses IP décrits dans ce document permet que l'ensemble d'adresses IP d'un point d'extrémité généralisé soit changé à un moment donné. Le numéro d'accès ne peut jamais être changé.

L'ensemble d'adresses IP d'un point d'extrémité généralisé gE à l'instant t est défini comme

Addr(gE)(t) = {IP1, ..., IPn}

si gE(t) = ({IP1, ..., IPn}, Port) tient à l'instant t.

Le numéro d'accès d'un point d'extrémité généralisé gE est défini comme

Port(gE) = Port

si gE(t) = ({IP1, ..., IPn}, Port) tient à l'instant t.

Il y a une règle fondamentale qui restreint tous les points d'extrémité généralisés :

Pour deux points d'extrémité généralisés différents gE' et gE" avec le même numéro d'accès Port(gE') = Port(gE"), les ensembles d'adresses Addr(gE')(t) et Addr(gE")(t) doivent être disjoints à tout instant.

A.3 Associations

Les associations consistent en deux points d'extrémité et les deux ensembles d'adresses connus de l'homologue à tout instant. La définition précise est la suivante :

Une association A entre deux points d'extrémité généralisés différents gE' et gE" est donnée par

A = (gE', S', gE", S")

où S'(t) et S"(t) sont un ensemble d'adresses à tout instant t tel que S'(t) est un sous ensemble non vide de Addr(gE')(t) et que S"(t) est un sous ensemble non vide de Addr(gE")(t).

Si A = (gE', S', gE", S") est une association entre les points d'extrémité généralisés gE' et gE", la notion suivante est utilisée :

Addr(A, gE') = S' et Addr(A, gE") = S".

Si la dépendance au temps est importante, la notion Addr(A, gE')(t) = S'(t) va être utilisée.

Si A est une association entre gE' et gE", alors Addr(A, gE') est le sous ensemble des adresses IP de gE', qui est connu de gE" et utilisé par gE'.

L'établissement d'association entre gE' et gE" peut être vu comme :

1. gE' et gE" existent avant l'association.

2. Si un INIT doit être envoyé de gE' à gE", les règles de portée d'adresse et autres limitations sont appliquées pour calculer le sous ensemble S' à partir de Addr(gE'). Les adresses de S' sont incluses dans le tronçon INIT.

3. Si un INIT-ACK doit être envoyé de gE" à gE', les règles de portée d'adresse et autres limitations sont appliquées pour calculer le sous ensemble S" à partir de Addr(gE"). Les adresses de S" sont incluses dans le tronçon INIT-ACK.

4. Après la prise de contact, l'association A = (gE', S', gE", S") a été établie.

5. Juste après l'établissement de l'association Addr(A, gE') et Addr(A, gE") sont les adresses qui ont été vues sur le réseau durant la prise de contact.

A.4 Relations avec la RFC 4960

La [RFC4960] définit la notion d'un point d'extrémité. Ce paragraphe montre que ces points d'extrémité sont aussi des points d'extrémité généralisés (particuliers).

La [RFC4960] n'a pas de notion de portée d'adresse ou autres limitations de traitement d'adresse et ne fournit pas de mécanisme pour changer les adresses d'un point d'extrémité.

Cela signifie qu'un point d'extrémité est simplement un point d'extrémité généralisé qui ne dépend pas du temps. Ni l'accès ni l'adresse ne font la liste des changements.

Durant l'établissement de l'association, aucune règle de portée d'adresse ni autres limitations ne vont être appliquées. Cela signifie que pour une association A entre deux points d'extrémité gE' et gE", ce qui suit est vrai :

Addr(A, gE') = Addr(gE') et Addr(A, gE") = Addr(gE").

A.5 Règles pour la manipulation d'adresse

Les règles pour la manipulation d'adresse peuvent maintenant être établies de façon simple :

1. Une adresse peut être ajoutée à un point d'extrémité généralisé gE seulement si cette adresse n'est pas une adresse d'un

point d'extrémité généralisé différent avec le même numéro d'accès.

2. Une adresse peut être ajoutée à une association A avec un point d'extrémité généralisé gE si elle a d'abord été ajoutée au point d'extrémité généralisé gE. Cela signifie que l'adresse doit d'abord être un élément de Addr(gE) et qu'ensuite elle peut devenir un élément de Addr(A, gE). mais ce n'est pas nécessaire. Si l'association ne permet pas la reconfiguration des adresses, seul Addr(gE) peut être modifiée.

3. Une adresse peut être supprimée d'une association A avec le point d'extrémité généralisé gE pour autant que Addr(A, gE) reste non vide.

4. Une adresse peut être supprimée d'un point d'extrémité généralisé gE seulement si elle a été supprimée de toutes les associations qui ont gE comme point d'extrémité généralisé.

Ces règles assurent simplement que les règles pour les points d'extrémité et associations données plus haut sont toujours satisfaites.

Adresse des auteurs

Randall R. Stewart
Cisco Systems, Inc.
4875 Forest Drive
Suite 200
Columbia, SC 29206
US
mél : rrs@cisco.com

Qiaobing Xie
Motorola, Inc.
1501 W. Shure Drive, 2-3C
Arlington Heights, IL 60004
USA
téléphone : +1-847-632-3028
mél : Qiaobing.Xie@motorola.com

Michael Tuexen
Univ. of Applied Sciences Muenster
Stegerwaldstr. 39
48565 Steinfurt
Germany
mél : tuexen@fh-muenster.de

Shin Maruyama
Kyoto University
Yoshida-Honmachi
Sakyo-ku
Kyoto, Kyoto 606-8501
JAPAN
téléphone : +81-75-753-7417
mél : mail@marushin.gr.jp

Masahiro Kozuka
Kyoto University
Yoshida-Honmachi
Sakyo-ku
Kyoto, Kyoto 606-8501
JAPAN
téléphone : +81-75-753-7417
mél : ma-kun@kozuka.jp

Déclaration complète de droits de reproduction

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.