Groupe de travail Réseau
Request for Comments : 5191
Catégorie : Sur la voie de la normalisation

Traduction Claude Brière de L'Isle

D. Forsberg, Nokia
Y. Ohba, éditeur, Toshiba
B. Patil, Nokia Siemens Networks
H. Tschofenig, Nokia Siemens Networks
A. Yegin, Samsung
mai 2008

Protocole pour porter l'authentification pour l'accès réseau (PANA)

Résumé
Le présent document définit le protocole pour porter l'authentification pour l'accès réseau (PANA, *Protocol for carrying Authentication for Network Access*) un transport de couche réseau pour le protocole extensible d'authentification (EAP, *Extensible Authentication Protocol*) pour permettre l'authentification de l'accès réseau entre clients et réseau d'accès. Dans les termes d'EAP, PANA est une couche inférieure d'EAP fondée sur UDP qui fonctionne entre l'homologue et l'authentificateur EAP.

Table des Matières

1. Introduction

La fourniture d'un service d'accès sécurisé au réseau exige un contrôle d'accès fondé sur l'authentification et l'autorisation des clients et des réseaux d'accès. L'authentification du client au réseau fournit les paramètres nécessaires pour réguler le flux de trafic à travers les points d'application. Un protocole est nécessaire pour porter les méthodes d'authentification entre le client et le réseau d'accès.

L'objectif de ce travail est de concevoir un transport de couche réseau pour les méthodes d'authentification de l'accès réseau. Le protocole d'authentification extensible (EAP) [RFC3748] fournit de telles méthodes d'authentification. En d'autres termes, PANA porte l'EAP, qui peut porter diverses méthodes d'authentification. En permettant le transport de l'EAP au-dessus d'IP, toute méthode d'authentification qui peut être transportée comme méthode EAP est disponible pour PANA et donc à toute technologie de couche de liaison. Il existe une division du travail claire entre PANA (une couche inférieure d'EAP) l'EAP, et les méthodes d'EAP, comme décrit dans la [RFC3748].

Divers environnements et modèles d'utilisation pour PANA sont identifiés dans l'Appendice A de la [RFC4058]. Les menaces potentielles sur la sécurité pour le protocole d'authentification de l'accès à la couche réseau sont examinées dans la [RFC4016]. Ces éléments ont été essentiels pour définir les exigences [RFC4058] du protocole PANA. Noter que certaines de ces exigences sont imposées par la charge utile choisie, EAP [RFC3748].

Il y a des composants qui font partie d'une solution complète d'accès sûr au réseau mais sortent du domaine d'application de la spécification de PANA, qui incluent la découverte d'agent d'authentification PANA (PAA, *PANA Authentication Agent*) le choix de la méthode d'authentification, le protocole de point d'application d'agent d'authentification PANA (PAA-EP, *PANA Authentication Agent-Enforcement Point*) la création de filtres de contrôle d'accès, et la protection du trafic de données. Ces composants sont décrits dans des documents distincts (voir les [RFC5192] et [RFC5193]).

1.1 Spécification des exigences

Dans ce document, plusieurs mots sont utilisés pour signifier les exigences de la spécification. Ces mots sont souvent en majuscules. Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Terminologie

Client PANA (PaC) : côté client du protocole qui réside dans l'appareil d'accès (par exemple, tablette, PDA, etc.). Il est chargé de fournir les accréditifs afin de prouver son identité (authentification) pour l'autorisation d'accès au réseau. Le PaC et l'homologue EAP sont colocalisés dans le même appareil d'accès.

Agent d'authentification PANA (PAA, *PANA Authentication Agent*) : entité du protocole dans le réseau d'accès dont la responsabilité est de vérifier les accréditifs fournis par un client PANA (PaC) et autoriser l'accès réseau à l'appareil d'accès. Le PAA et l'authentificateur EAP (et facultativement le serveur EAP) sont colocalisés dans le même nœud. Noter que la procédure d'authentification et d'autorisation peut aussi, conformément au modèle EAP, être téléchargée à l'infrastrucure d'authentification, autorisation, et comptabilité (AAA) de l'arrière.

Session PANA : une session PANA est établie entre le client PANA (PaC) et l'agent d'authentification PANA (PAA) et elle se termine par suite de l'échec d'un essai d'authentification et d'autorisation ou de vie, un échec de livraison de message après que les retransmissions ont atteint la valeur maximum, l'expiration de la durée de vie de la session, un message de terminaison explicite, ou tout événement qui cause l'interruption du service d'accès. Un identifiant de session fixe est conservé sur toute la session. Une session ne peut pas être partagée à travers plusieurs interfaces réseau.

Durée de vie de session : durée qui est associée à une session PANA. Pour une session PANA établie, la durée de vie de session est limitée par la durée de vie de l'autorisation donnée actuellement au PaC. La durée de vie de session peut être étendue par un nouveau tour d'authentification EAP avant qu'elle expire. Tant qu'une session PANA est établie, la durée de vie DEVRAIT être réglée à une valeur qui permette au PaC de détecter la défaillance d'une session dans un délai raisonnable.

Identifiant de session : cet identifiant est utilisé pour identifier de façon univoque une session PANA sur le PaC et le PAA. Il est inclus dans les messages PANA pour lier le message à une session PANA spécifique. Cet identifiant bidirectionnel est alloué par le PAA dans le message de demande initial et est libéré quand la session se termine. L'identifiant de session est alloué par le PAA et est unique au sein du PAA.

Association de sécurité PANA (SA PANA) : elle est formée entre le PaC et le PAA par le partage de matériel cryptographique et du contexte associé. L'association de sécurité bidirectionnelle formée est utilisée pour protéger le trafic bidirectionnel de signalisation de PANA entre le PaC et le PAA.

Point d'application (EP, *Enforcement Point*) : nœud sur le réseau d'accès où les politiques d'application par paquet (c'est-à-dire, les filtres) sont appliqués au trafic entrant et sortant des appareils d'accès. L'EP et le PAA peuvent être colocalisés. Les EP devraient empêcher le trafic de données de et vers tout client non autorisé, sauf si ce trafic de données est soit PANA soit d'un autre type de trafic permis (par exemple, du protocole de résolution d'adresse (ARP, *Address Resolution Protocol*), de la découverte de voisin IPv6, de DHCP, etc.).

Clé maîtresse de session (MSK, *Master Session Key*) : clé déduite par l'homologue EAP et le serveur EAP et transportée à l'authentificateur EAP [RFC3748].

Pour des définitions de terminologie supplémentaires, voir le document du cadre PANA [RFC5193].

3. Vue d'ensemble du protocole

Le protocole PANA fonctionne entre un client (PaC) et un serveur (PAA) afin d'effectuer l'authentification et l'autorisation pour le service d'accès au réseau.

L'échange de messages du protocole consiste en une série de demandes et réponses, dont certaines peuvent être initiées par l'une ou l'autre extrémité. Chaque message peut porter zéro, une ou plusieurs AVP (paires d'attribut-valeur) au sein de la charge utile. La principale charge utile de PANA est EAP, qui effectue l'authentification. PANA aide le PaC et le PAA à établir une session EAP.

PANA est un protocole fondé sur UDP. Il a son propre mécanisme de retransmission pour livrer les messages de façon fiable.

Les messages PANA sont envoyés entre le PaC et le PAA au titre d'une session PANA. Une session PANA consiste en trois phases distinctes :

- Phase d'authentification et d'autorisation : c'est la phase qui initie une nouvelle session PANA et exécute EAP entre le PAA et le PaC. La session PANA peut être initiée par le PaC et par le PAA. La charge utile EAP (qui porte une méthode EAP incorporée) est ce qui est utilisé pour l'authentification. Le PAA porte le résultat de l'authentification et de l'autorisation au PaC à la fin de cette phase.

- Phase d'accès : après la réussite de l'authentification et de l'autorisation, l'appareil d'accès obtient l'accès au réseau et peut envoyer et recevoir du trafic IP à travers les EP. À tout moment durant cette phase, le PaC et le PAA peuvent facultativement envoyer des messages de notification PANA pour vérifier la vie de la session PANA chez l'homologue.

- Phase de réauthentification : durant la phase d'accès, le PAA peut, et le PaC devrait, initier la réauthentification si il veut mettre à jour la durée de vie de session PANA avant qu'elle expire. EAP est porté par PANA pour effectuer la réauthentification. Cette phase peut être facultativement déclenchée par le PaC et le PAA sans égard à la durée de vie de la session. La phase de réauthentification est une sous phase de la phase d'accès. La session passe à cette sous phase à partir de la phase d'accès quand la réauthentification démarre, et y revient à la réussite de la réauthentification.

- Phase de terminaison : le PaC ou le PAA peut choisir d'interrompre le service d'accès à tout moment. Un message explicite de déconnexion peut être envoyé par l'une ou l'autre extrémité. Si le PaC ou le PAA déconnecte sans engager un message de terminaison, il est supposé que l'expiration de la durée de vie finie de session ou l'échec d'essais de vie vont nettoyer la session à l'autre extrémité.

La protection cryptographique des messages entre le PaC et le PAA est possible si EAP en conjonction avec la méthode EAP exporte une clé partagée. Cette clé partagée est utilisée pour créer une SA PANA. La SA PANA aide à générer des codes d'authentification par message qui fournissent la protection de l'intégrité et l'authentification.

4. Détails du protocole

Les paragraphes qui suivent expliquent en détails les diverses phases d'une session PANA.

4.1 Phase d'authentification et d'autorisation

La principale tâche de la phase d'authentification et d'autorisation est d'établir une session PANA et porter les messages EAP entre le PaC et le PAA. La session PANA peut être initiée par le PaC ou le PAA.

Session initiée par le PaC : quand le PaC initie une session PANA, il envoie un message PANA-Client-Initiation au PAA. Quand le PaC n'est pas configuré avec une adresse IP du PAA avant d'initier la session PANA, DHCP [RFC5192] est utilisé comme méthode par défaut pour configurer dynamiquement l'adresse IP du PAA. D'autres méthodes pour découvrir dynamiquement l'adresse IP du PAA peuvent être utilisées pour les session initiées par le PaC, mais elles sortent du domaine d'application de la présente spécification. Le PAA qui reçoit le message PANA-Client-Initiation DOIT répondre au PaC avec un message PANA-Auth-Request.

Session initiée par le PAA : quand le PAA connaît l'adresse IP du PaC, il PEUT envoyer une PANA-Auth-Request non sollicitée au PaC. Les détails de comment le PAA peut apprendre l'adresse IP du PaC sortent du domaine d'application de cette spécification.

Un identifiant de session est alloué pour la session par le PAA et porté dans le message initial PANA-Auth-Request. Le même identifiant de session DOIT être porté dans les messages suivants échangés entre le PAA et le PaC tout au long de la session.

Quand le PaC reçoit le message initial PANA-Auth-Request d'un PAA, il répond par un message PANA-Auth-Answer, si il souhaite continuer la session PANA. Autrement, il élimine en silence le message PANA-Auth-Request.

Les messages initiaux PANA-Auth-Request et PANA-Auth-Answer DOIVENT avoir le bit "S" (Start, *début*) établi, sans considération de si la session est initiée par le PaC ou le PAA. Les mesages non initiaux PANA-Auth-Request et PANA-Auth-Answer ainsi que tous les autres messages NE DOIVENT PAS avoir le bit "S" établi.

Il est recommandé que le PAA limite le taux auquel il traite les messages PANA-Client-Initiation entrants pour donner de la robustesse contre les attaques de déni de service (DoS). Les détails de la limitation de taux sortent du domaine d'application de cette spécification.

Si une SA PANA a besoin d'être établie avec l'utilisation d'une méthode EAP de génération de clé, la fonction pseudo aléatoire (PRF, *Pseudo-Random Function*) et les algorithmes d'intégrité à utiliser pour la déduction de PANA_AUTH_KEY (voir au paragraphe 5.3) et le calcul de l'AVP AUTH (voir le paragraphe 5.4) sont négociés comme suit : le PAA envoie la PANA-Auth-Request initiale portant une ou plusieurs AVP PRF-Algorithm et une ou plusieurs AVP Integrity-Algorithm pour la PRF et les algorithmes d'intégrité pris en charge, respectivement. Le PaC choisit alors un algorithme de PRF et un algorithme d'intégrité à partir des AVP portées dans la PANA-Auth-Request initiale, et il répond avec la PANA-Auth-Answer initiale portant une AVP PRF-Algorithm et une AVP Integrity-Algorithm pour les algorithmes choisis. La négociation est protégée après que la MSK est disponible, comme décrit au paragraphe 5.3.

Si le PAA veut rester sans état en réponse à un message PANA-Client-Initiation, il n'inclut pas d'AVP EAP-Payload dans le message initial PANA-Auth-Request, et il ne devrait pas retransmettre le message sur un temporisateur. Pour cette raison, le PaC DOIT retransmettre les message PANA-Client-Initiation jusqu'à ce qu'il reçoive le second message PANA-Auth-Request (pas une retransmission du message initial) provenant du PAA.

Il est possible que le PAA et le PaC initient tous deux la session PANA au même moment, c'est-à-dire, le PAA envoie le message initial PANA-Auth-Request sans sollicitation tandis que le PaC envoie un message PANA-Client-Initiation. Pour résoudre le conflit, le PAA DOIT éliminer en silence le message PANA-Client-Initiation reçu du PaC après qu'il a envoyé le message initial PANA-Auth-Request. Le PAA utilise l'adresse IP de source et le numéro d'accès de source du message PANA-Client-Initiation pour identifier le PaC parmi plusieurs messages PANA-Client-Initiation envoyés de différents PaC.

Les messages EAP sont portés dans les messages PANA-Auth-Request. Les messages PANA-Auth-Answer sont simplement utilisés pour accuser réception des demandes. Comme optimisation, un message PANA-Auth-Answer envoyé du PaC PEUT inclure le message EAP. Cette optimisation NE DEVRAIT PAS être utilisée quand cela prend du temps pour générer le message EAP (à cause, par exemple, de l'intervention d'une entrée humaine) et dans ce cas, retourner un message PANA-Auth-Answer sans porter un message EAP peut éviter une retransmission inutile du message PANA-Auth-Request.

Une AVP Nonce *(nom occasionnel)* DOIT être incluse dans les premiers messages PANA-Auth-Request et PANA-Auth-Answer qui suivent les messages initiaux PANA-Auth-Request et PANA-Auth-Answer (c'est-à-dire, avec le bit "S" établi) et NE DOIT PAS être incluse dans un autre message, sauf durant les procédures de réauthentification (voir le paragraphe 4.3).

Le résultat de l'authentification PANA est porté dans le dernier message PANA-Auth-Request envoyé du PAA au PaC. Ce message porte le résultat de l'authentification EAP et le résultat de l'authentification PANA. Le dernier message PANA-Auth-Request DOIT être acquitté avec un message PANA-Auth-Answer. Les derniers messages PANA-Auth-Request et PANA-Auth-Answer DOIVENT avoir le bit "C" (Complete, *terminé*) établi, et aucun autre message NE DOIT avoir le bit "C" établi. La Figure 1 montre un exemple de séquence de la phase d'authentification et autorisation pour une session initiée par un PaC.

```
PaC     PAA     Message(numéro de séquence)[AVP]
  ----->        PANA-Client-Initiation(0)
  <-----        PANA-Auth-Request(x)[PRF-Algorithm,Integrity-Algorithm]   // bit "S" (début) établi
  ----->        PANA-Auth-Answer(x)[PRF-Algorithm,Integrity-Algorithm]    // bit "S" (début) établi
  <-----        PANA-Auth-Request(x+1)[Nonce,EAP-Payload]
  ----->        PANA-Auth-Answer(x+1)[Nonce]                              // pas de portage EAP
  ----->        PANA-Auth-Request(y)[EAP-Payload]
  <-----        PANA-Auth-Answer(y)
  <-----        PANA-Auth-Request(x+2)[EAP-Payload]
  ----->        PANA-Auth-Answer(x+2)[EAP-Payload]                        // portage EAP
  <-----        PANA-Auth-Request(x+3)[Result-Code, EAP-Payload, Key-Id, Session-Lifetime, AUTH]
                                                                          // bit "C" (terminé) établi
  ----->        PANA-Auth-Answer(x+3)[Key-Id, AUTH]                       // bit "C" (terminé) établi
```

Figure 1 : Exemple de séquence de phase authentification et autorisation pour une session initiée par le PaC
("Portage EAP" est le cas dans lequel une AVP EAP-Payload est portée dans le PAN)

Si une SA PANA a besoin d'être établie avec l'utilisation d'une méthode EAP de génération de clé et qu'une MSK est bien générée, le dernier message PANA-Auth-Request avec le bit "C" (terminé) établi DOIT contenir une AVP Key-Id et une AVP AUTH pour la première déduction de clés de la session, et tous les messages suivants DOIVENT contenir une AVP AUTH.

L'authentification EAP peut échouer à un authentificateur de traverse sans que soit envoyé de message d'échec EAP [RFC4137]. Quand cela arrive, le PAA DEVRAIT terminer en silence la session, supposant qu'un temporisateur de session sur le PaC va nettoyer l'état sur le PaC.

Il y a un cas où l'authentification EAP réussit à produire un message EAP Success, mais où l'autorisation d'accès au réseau échoue à cause, par exemple, du rejet de l'autorisation par un serveur AAA ou du rejet en local de l'autorisation par le PAA. Quand cela arrive, le PAA DOIT envoyer la dernière PANA-Auth-Request avec un code de résultat de PANA_AUTHORIZATION_REJECTED. Si une MSK est disponible, les derniers messages PANA-Auth-Request et PANA-Auth-Answer avec le bit "C" (terminé) établi DOIVENT être protégés avec une AVP AUTH et porter une AVP Key-Id. La session PANA DOIT être terminée immédiatement après le dernier échange de message PANA-Auth.

Pour les raisons décrites à la Section 3 de la [RFC5193], le PaC peut avoir besoin de reconfigurer l'adresse IP après une phase réussie d'authentification et d'autorisation pour obtenir une adresse IP utilisable pour échanger du trafic de données à travers l'EP. Dans ce cas, le PAA établit le bit "I"' (Reconfiguration IP) des messages PANA-Auth-Request dans la phase d'authentification et d'autorisation pour indiquer au PaC le besoin d'une reconfiguration d'adresse IP. Comment la reconfiguration d'adresse IP est effectuée sort du domaine d'application de ce document.

4.2 Phase d'accès

Une fois la phase d'authentification et d'autorisation achevée avec succès, le PaC obtient l'accès au réseau et peut envoyer et recevoir le trafic de données IP à travers le ou les EP, et la session PANA entre dans la phase d'accès. Dans cette phase, les messages PANA-Notification-Request et PANA-Notification-Answer avec le bit "P" (Ping) établi (les messages de demande ping et de réponse ping, respectivement) peuvent être utilisés pour vérifier la vie de la session PANA chez l'homologue PANA. Le PaC et le PAA sont tous deux autorisés à envoyer une demande de ping à l'homologue communiquant chaque fois qu'ils ont besoin de s'assurer de la disponibilité de la session chez l'homologue, et ils s'attendent à ce que l'homologue retourne un message de réponse ping. Les messages de demande et de réponse ping DOIVENT être protégés avec une AVP AUTH quand une SA PANA est disponible. Une demande ping NE DOIT PAS être envoyée dans la phase d'authentification et d'autorisation, la phase de réauthentification, et la phase de terminaison.

Les mises en œuvre DOIVENT limiter le taux d'exécution de cet essai. Le PaC et le PAA peuvent traiter les limitations de taux pour eux-mêmes, ils n'ont pas à effectuer de coordination l'un avec l'autre. Il n'y a pas de négociation de temporisateurs pour cela. De plus, une mise en œuvre PEUT limiter le taux de traitement des demandes de ping entrantes. On devrait noter que si un PAA ou PaC qui considère que sa connexité est perdue après un nombre relativement faible de ping sans réponse est couplé avec un homologue qui limite agressivement le taux de messages de demande et de réponse de ping, des faux positifs pourraient se produire. Donc, un PAA ou PaC ne devrait pas s'appuyer sur des opérations de ping fréquentes pour déterminer hâtivement la perte de connexité.

4.3 Phase de réauthentification

La session PANA dans la phase d'accès peut entrer dans la phase réauthentification pour étendre la durée de vie de la session en cours en exécutant à nouveau l'EAP. Une fois la phase de réauthentification achevée avec succès, la session entre à nouveau dans la phase d'accès. Autrement, la session est terminée.

Quand le PaC initie une réauthentification, il envoie un message PANA-Notification-Request avec le bit "A" (réauthentification) établi (un message de demande de réauthentification) au PAA. Ce message DOIT contenir l'identifiant de session alloué à la session à réauthentifier. Si le PAA a déjà une session PANA établie pour le PaC avec l'identifiant de session correspondant, il DOIT d'abord répondre avec un message PANA-Notification-Answer avec le bit "A" (réauthentification) établi (un message de réponse de réauthentification) suivi par un message PANA-Auth-Request qui commence une nouvelle authentification EAP. Si le PAA ne peut pas identifier la session, il DOIT éliminer en silence le message. Les premiers messages PANA-Auth-Request et PANA-Auth-Answer dans la phase de réauthentification DOIVENT avoir le bit "S" à zéro et porter une AVP Nonce.

Le PaC peut recevoir une PANA-Auth-Request avant de recevoir la réponse à son message de demande de réauthentification en cours. Cette condition peut survenir à cause d'un réarrangement de paquets ou une condition de compétition entre le PaC et le PAA quand ils tentent tous deux d'engager une réauthentification. Le PaC DOIT continuer d'éliminer les messages PANA-Auth-Request reçus jusqu'à ce qu'il reçoive la réponse à sa demande.

Quand le PAA initie la réauthentification, il envoie un message PANA-Auth-Request contenant l'identifiant de session pour le PaC. Le PAA DOIT initier la réauthentification EAP avant l'expiration de la durée de vie de la session en cours.

La réauthentification d'une session PANA en cours NE DOIT PAS réinitialiser les numéros de séquence.

Pour toute réauthentification, si il y a une SA PANA établie, les messages de demande et de réponse de réauthentification et les messages PANA-Auth-Request et PANA-Auth-Answer suivants DOIVENT être protégés avec une AVP AUTH. Les messages PANA-Auth-Request et PANA-Auth-Answer finaux et tout message PANA suivant DOIVENT être protégés par l'utilisation de la clé générée à partir de la dernière authentification EAP.

```
PaC      PAA    Message(numéro de séquence)[AVP]
   ----->         PANA-Notification-Request(q)[AUTH]                  // bit "A" (réauthentification) établi
   <-----         PANA-Notification-Answer(q)[AUTH]                   // bit "A" (réauthentification) établi
   <-----         PANA-Auth-Request(p)[EAP-Payload, Nonce, AUTH]
   ----->         PANA-Auth-Answer(p)[AUTH, Nonce]
   ----->         PANA-Auth-Request(q+1)[EAP-Payload, AUTH]
   <-----         PANA-Auth-Answer(q+1)[AUTH]
   <-----         PANA-Auth-Request(p+1)[EAP-Payload, AUTH]
   ----->         PANA-Auth-Answer(p+1)[EAP-Payload, AUTH]
   <-----         PANA-Auth-Request(p+2)[Result-Code, EAP-Payload, Key-Id, Session-Lifetime, AUTH]
                                                                      // bit "C" (terminé) établi
   ----->         PANA-Auth-Answer(p+2)[Key-Id, AUTH]                 // bit "C" (terminé) établi
```

Figure 2 : Exemple de séquence pour la phase de réauthentification initiée par le PaC

4.4 Phase de terminaison

Une procédure pour terminer explicitement une session PANA peut être initiée par le PaC (c'est-à-dire, indication de déconnexion) ou par le PAA (c'est-à-dire, révocation de session). Les échanges de messages PANA-Termination-Request et PANA-Termination-Answer sont utilisés pour les procédures d'indication de déconnexion et de révocation de session.

La raison de la terminaison est indiquée dans l'AVP Termination-Cause. Quand il y a une SA PANA établie entre le PaC et le PAA, tous les messages échangés durant la phase de terminaison DOIVENT être protégés avec une AVP AUTH. Quand l'envoyeur du message PANA-Termination-Request reçoit un accusé de réception valide, tous les états conservés pour la session PANA DOIVENT être terminés immédiatement.

5. Règles de traitement

5.1 Fragmentation

PANA n'assure pas la fragmentation des messages PANA. À la place, il s'appuie sur la fragmentation fournie par les méthodes EAP et la couche IP quand c'est nécessaire.

5.2 Numéro de séquence et retransmission

PANA utilise des numéros de séquence pour assurer une livraison ordonnée et fiable des messages.

Le PaC et le PAA tiennent deux numéros de séquence : un pour régler le numéro de séquence de la prochaine demande sortante, l'autre pour la confrontation au numéro de séquence de la prochaine demande entrante. Ces numéros de séquence sont des nombres non signés de 32 bits. Ils sont augmentés régulièrement de 1 lorsque de nouvelles demandes sont générées et reçues, et reviennent à zéro au message qui suit 2^32-1. Les réponses contiennent toujours le même numéro de séquence que la demande correspondante. Les retransmissions réutilisent le numéro de séquence contenu dans le paquet original.

Les numéros de séquence initiaux (ISN, *Initial Sequence Number*) sont pris au hasard par le PaC et le PAA lorsque ils envoient leur tout premier message de demande. Le message PANA-Client-Initiation porte le numéro de séquence 0.

Quand un message de demande est reçu, il est considéré valide en termes de numéro de séquence si et seulement si son numéro de séquence correspond à la valeur attendue. Cette vérification ne s'applique pas au message PANA-Client-Initiation ni au message initial PANA-Auth-Request.

Quand un message de réponse est reçu, il est considéré valide en termes de numéros de séquence si et seulement si son numéro de séquence correspond à celui de la demande actuellement en instance. Un homologue peut seulement avoir une demande en instance à la fois.

Les messages de demande PANA sont retransmis sur la base d'un temporisateur jusqu'à ce qu'une réponse soit reçue (et dans ce cas le temporisateur de retransmission est arrêté) ou bien le nombre de retransmission atteint la valeur maximum (et dans ce cas la session PANA DOIT être immédiatement terminée).

Les temporisateurs de retransmission DEVRAIENT être calculés comme décrit à la Section 9, sauf si un déploiement choisit d'utiliser ses propres temporisateurs de retransmission optimisés pour les caractéristiques de la couche de liaison sous-jacente.

Sauf si ils sont éliminés à cause d'une limitation de taux, le PaC et le PAA DOIVENT répondre à tous les messages de demande dupliqués reçus. La dernière réponse transmise PEUT être mise en antémémoire pour le cas où elle ne serait pas reçue par l'homologue, qui génère une retransmission de la dernière demande. Quand elle est disponible, la réponse en antémémoire peut être utilisée à la place du traitement complet de la demande retransmise et de la formation d'une nouvelle réponse à partir de rien.

5.3 Association de sécurité PANA

Une SA PANA est créée comme un attribut d'une session PANA quand l'authentification EAP réussit avec la création d'une MSK. Une SA PANA n'est pas créée quand l'authentification PANA échoue ou qu'aucune MSK n'est produite par la méthode d'authentification EAP. Quand une nouvelle MSK est déduite dans la phase de réauthentification PANA, toute clé déduite de l'ancienne MSK DOIT être mise à niveau en une nouvelle déduite de la nouvelle MSK. Afin de distinguer la nouvelle MSK des anciennes, une AVP Key-Id DOIT être portée dans les derniers messages PANA-Auth-Request et PANA-Auth-Answer avec le bit "C" (terminé) établi à la fin de l'authentification EAP, qui a résulté en la déduction d'une nouvelle MSK. L'AVP Key-Id est du type Unsigned32 et DOIT contenir une valeur qui identifie de façont univoque la MSK dans la session PANA. Le dernier message PANA-Auth-Answer avec le bit "C" établi en réponse au dernier message PANA-Auth-Request avec le bit "C" établi DOIT contenir une AVP Key-Id avec le même identifiant de MSK porté dans la demande. Les derniers messages PANA-Auth-Request et PANA-Auth-Answer avec une AVP Key-Id DOIVENT aussi porter une AVP AUTH dont la valeur est calculée en utilisant la nouvelle PANA_AUTH_KEY déduite de la nouvelle MSK. Bien que la spécification ne rende pas obligatoire une méthode particulière pour le calcul de la valeur de l'AVP Key-Id, une méthode simple est d'utiliser des nombres à croissance monotone.

La durée de vie de session PANA est bordée par la durée de vie d'autorisation accordée par le serveur d'authentification (la même que la durée de vie de MSK). La durée de vie de la SA PANA (donc de PANA_AUTH_KEY) est la même que la durée de vie de la session PANA. La SA PANA créée est supprimée quand la session PANA correspondante est terminée.

Les attributs de SA PANA ainsi que les attributs de session PANA sont :

Attributs de session PANA :
* Identifiant de Session
* Adresse IP et numéro d'accès UDP du PaC
* Adresse IP et numéro d'accès UDP du PAA
* Numéro de séquence pour la prochaine demande sortante
* Numéro de séquence pour la prochaine demande entrante
* Dernière charge utile de message transmise
* Durée de vie de session
* Attributs de SA PANA

Attributs de SA PANA :
* Nom occasionnel généré par le PaC (PaC_nonce)
* Nom occasionnel généré par le PAA (PAA_nonce)
* MSK
* Identifiant de MSK
* Fonction pseudo aléatoire
* Algorithme d'intégrité

PANA_AUTH_KEY est déduit de la MSK disponible, et est utilisé pour protéger l'intégrité des messages PANA. PANA_AUTH_KEY est calculé de la façon suivante :

PANA_AUTH_KEY = prf+(MSK, "IETF PANA"|I_PAR|I_PAN|PaC_nonce|PAA_nonce|Key_ID)

où :

- La fonction prf+ est définie dans IKEv2 [RFC4306]. La fonction pseudo aléatoire à utiliser pour la fonction prf+ est négociée en utilisant l'AVP PRF-Algorithm dans l'échange initial PANA-Auth-Request et PANA-Auth-Answer avec le bit "S" établi.
- MSK est la clé de session maîtresse générée par la méthode EAP.
- "IETF PANA" est la représentation en code ASCII de la chaîne terminée par un non NUL (à l'exclusion des guillemets qui l'entourent).
- I_PAR et I_PAN sont les messages initiaux PANA-Auth-Request et PANA-Auth-Answer (l'en-tête PANA et les AVP PANA suivants) avec le bit "S" établi, respectivement.
- PaC_nonce et PAA_nonce sont les valeurs de l'AVP Nonce portée dans les premiers messages PANA-Auth-Answer et PANA-Auth-Request non initiaux dans la phase d'authentification et d'autorisation ou les premiers messages PANA-Auth-Answer et PANA-Auth-Request dans la phase de réauthentification, respectivement.
- Key_ID est la valeur de l'AVP Key-Id.

La longueur de PANA_AUTH_KEY dépend de l'algorithme d'intégrité utilisé. Voir à la Section 5.4 les détails de l'usage de PANA_AUTH_KEY.

5.4 Authentification de message

Un message PANA peut contenir une AVP AUTH pour la protection cryptographique du message.

Quand une AVP AUTH est incluse dans un message PANA, le champ Valeur de l'AVP AUTH est calculé en utilisant PANA_AUTH_KEY de la façon suivante :

valeur d'AVP AUTH = PANA_AUTH_HASH(PANA_AUTH_KEY, PANA_PDU)

où PANA_PDU est le message PANA incluant l'en-tête PANA, avec le champ Valeur d'AVP AUTH d'abord initialisé à 0. PANA_AUTH_HASH représente l'algorithme d'intégrité négocié en utilisant l'AVP Integrity-Algorithm dans l'échange initial PANA-Auth-Request et PANA-Auth-Answer avec le bit "S" établi. Le PaC et le PAA DOIVENT utiliser le même algorithme d'intégrité pour calculer une AVP AUTH qu'ils génèrent et reçoivent.

5.5 Vérification de la validité du message

Quand un message PANA est reçu, il est considéré comme étant invalide si une des conditions suivantes n'est pas satisfaite :

o Chaque champ dans l'en-tête de message contient une valeur valide incluant un numéro de séquence, la longueur de message, le type de message, des fanions, un identifiant de session, etc.

o Le type de message est d'un des types attendus dans l'état en cours. Précisément, les messages suivants sont inattendus et invalides :
  * Dans la phase authentification et autorisation :
    + PANA-Client-Initiation après l'achèvement de l'échange initial PANA-Auth-Request et PANA-Auth-Answer avec le bit "S" établi ;
    + demande de réauthentification ;
    + demande Ping ;
    + la dernière PANA-Auth-Request avec le bit "C" établi avant l'achèvement de l'échange initial PANA-Auth-Request et PANA-Auth-Answer avec le bit "S" établi ;
    + la PANA-Auth-Request initiale avec le bit "S" établi après qu'un PaC a reçu une PANA-Auth-Request non initiale valide avec le bit "S" à zéro ;
    + PANA-Termination-Request.
  * Dans la phase de réauthentification :
    + PANA-Client-Initiation,
    + la demande initiale PANA-Auth-Request.
  * Dans la phase d'accès :
    + PANA-Auth-Request.
    + PANA-Client-Initiation.
  * Dans la phase terminaison :
    + PANA-Client-Initiation ;
    + toutes les demandes sauf PANA-Termination-Request et demande de ping.

- La charge utile de message contient un ensemble valide d'AVP permises pour le type de message. Il n'y a pas d'AVP manquante qui ait besoin d'être incluse dans la charge utile, et aucune AVP qui ait besoin d'être à une position fixée n'est incluse dans une position différente de cette position fixée.

- Chaque AVP est reconnue et décodée correctement.

- Une fois l'authentification PANA réussie en utilisant une méthode EAP génératrice de clé, le message PANA-Auth-Request qui porte le EAP Success et tout message suivant dans cette session contient une AVP AUTH. La valeur de l'AVP correspond à la valeur de hachage calculée dans le message reçu.

Les messages invalides DOIVENT être éliminés afin de donner de la robustesse contre les attaques de DoS.

5.6 PaC mettant à jour son adresse IP

L'adresse IP d'un PaC utilisée pour PANA peut changer dans certaines situations, par exemple, quand la reconfiguration d'adresse IP est nécessaire pour que le PaC obtienne une adresse IP après la réussite de l'authentification PANA (voir la Section 3 de la [RFC5193]) ou quand le PaC passe d'une liaison IP à une autre au sein du même domaine de PAA. Afin de maintenir la session PANA, la PAA a besoin d'avoir la notification du changement d'adresse du PaC.

Après que le PaC a changé son adresse IP utilisée pour PANA, il DOIT envoyer tous les messages PANA valides. Si le message qui porte la nouvelle adresse IP du PaC dans le champ Adresse de source de l'en-tête IP est valide, le PAA DOIT mettre à jour la session PANA avec la nouvelle adresse du PaC. Si il y a une SA PANA établie, le message DOIT être protégé avec une AVP AUTH.

5.7 Durée de vie de session

La phase d'authentification et autorisation détermine la durée de vie de session PANA, et la durée de vie est indiquée au PaC quand l'autorisation d'accès au réseau réussit. À cette fin, quand le dernier message PANA-Auth-Request (c'est-à-dire, avec le bit "C" (terminé) établi) dans la phase d'authentification et autorisation ou dans la phase de réauthentification, porte une AVP Result-Code avec une valeur de PANA_SUCCESS, une AVP Session-Lifetime DOIT aussi être portée dans le message. Une AVP Session-Lifetime DOIT être ignorée quand elle est incluse dans d'autres messages PANA.

La durée de vie est un paramètre non négociable qui peut être utilisé par le PaC pour gérer l'état relatif à PANA. Le PaC DOIT initier la phase de réauthentification avant l'expiration de la durée de vie de la session en cours si il veut étendre la session.

Le PaC et le PAA PEUVENT utiliser des informations obtenues en dehors de PANA (par exemple, des indications de couche inférieure) pour effectuer la détection d'un homologue déconnecté. La disponibilité et la fiabilité de ces indications PEUT dépendre d'une couche de liaison spécifique ou de la topologie du réseau et sont donc seulement des conseils. Un homologue PANA DEVRAIT utiliser la demande ping et l'échange de réponse pour vérifier qu'un homologue n'est, en fait, plus actif, sauf si les informations obtenues en dehors de PANA sont utilisées pour effectuer la détection d'un homologue déconnecté.

Le paramètre durée de vie de session n'est pas en relation avec la transmission des messages de demande de ping. Ces messages peuvent être utilisés pour une vérification asynchrone de la vie de l'homologue. La décision d'envoyer un message de demande de ping est prise en local et n'exige pas de coordination entre les homologues.

6. Format de message

Cette Section définit les formats de message pour le protocole PANA.

6.1 En-têtes IP et UDP

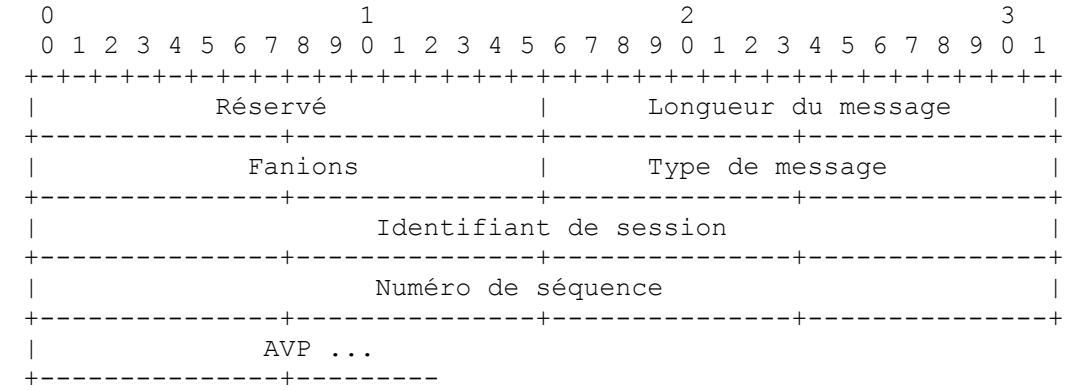
Tout message PANA est en envoi individuel entre le PaC et le PAA.

Pour tout message PANA envoyé de l'homologue qui a initié la session PANA, l'accès de source UDP est réglé à un numéro sur lequel l'homologue peut recevoir les messages PANA entrants, et l'accès de destination est réglé au numéro d'accès PANA alloué (716). Pour tout message PANA envoyé de l'autre homologue, l'accès de source est réglé au numéro d'accès alloué à PANA (716), et l'accès de destination est copié de l'accès de source du dernier message reçu. Dans le cas

où le PaC et le PAA initient tous les deux la session (c'est-à-dire, si les messages PANA-Client-Initiation et PANA-Auth-Request non sollicités se croisent) le PaC est alors identifié comme l'initiateur. Tous les homoloques PANA DOIVENT écouter sur le numéro d'accès alloué à PANA (716).

6.2 En-tête de message PANA

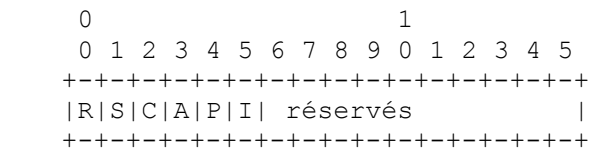
Un schéma du format de l'en-tête de message PANA est montré ci-dessous. Les champs sont transmis dans l'ordre des octets du réseau (de gauche à droite).



Réservé : ce champ de 16 bits est réservé pour une utilisation future. Il DOIT être réglé à zéro et ignoré par le receveur.

Longueur de message : champ de deux octets qui indique la longueur du message PANA incluant les champs d'en-tête.

Fanions : le champ Fanions fait deux octets. Les bits suivants sont alloués :



R (Request, *demande*) : établi (à 1) le message est une demande. À zéro, le message est une réponse.

S (Start, *début*) : établi (à 1) le message est le premier PANA-Auth-Request ou PANA-Auth-Answer dans la phase authentification et autorisation phase. Pour les autres messages, ce bit DOIT être à zéro.

C (Complete, *terminé*) : établi (à 1) le message est le dernier PANA-Auth-Request ou PANA-Auth-Answer dans la phase authentification et autorisation phase. Pour les autres messages, ce bit DOIT être à zéro.

A (réAuthentification) : établi (à 1) le message est une PANA-Notification-Request ou PANA-Notification-Answer pour initier la réauthentification. Pour les autres messages, ce bit DOIT être à zéro.

P (Ping) : établi (à 1) le message est une PANA-Notification-Request ou PANA-Notification-Answer pour un essai de vie. Pour les autres messages, ce bit DOIT être à zéro.

I (Reconfiguration IP) : établi (à 1) il indique que le PaC est obligé d'effectuer une reconfiguration d'adresse IP après une phase réussie d'authentification et autorisation pour configurer une adresse IP utilisable pour échanger du trafic de données à travers l'EP. Ce bit est établi par le PAA seulement pour les messages PANA-Auth-Request dans la phase authentification et autorisation phase. Pour les autres messages, ce bit DOIT être à zéro.

Réservé : ces bits de fanion sont réservés pour une utilisation future. Ils DOIVENT être à zéro et ignoré par le receveur.

Type de message : le champ Type de message fait deux octets, et il est utilisé pour communiquer le type de message avec le message. L'allocation des types de messages est gérée par l'IANA [IANAWEB].

Identifiant de session : ce champ contient un identifiant de session de 32 bits.

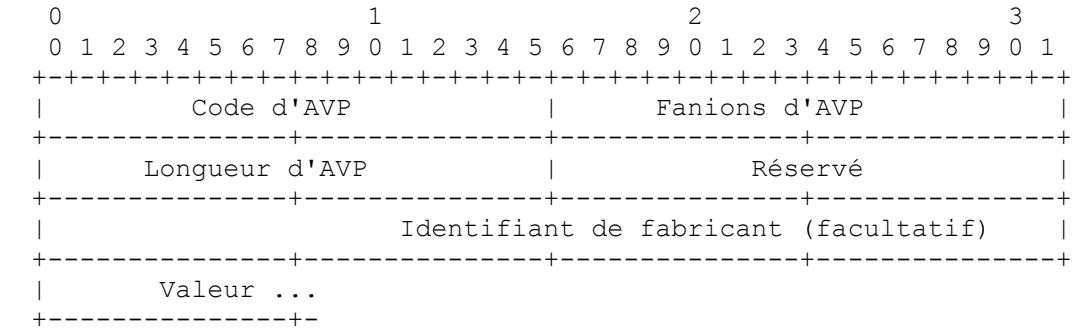
Numéro de séquence : ce champ contient un numéro de séquence de 32 bits.

AVP : les AVP sont une méthode d'encapsulation des informations relevant du message PANA. Voir au paragraphe 6.3 plus d'informations sur les AVP.

6.3 Format d'AVP

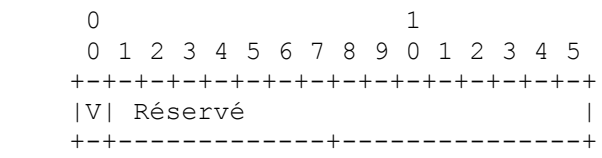
Chaque AVP de type OctetString *(chaîne d'octets)* DOIT être bourrée pour s'aligner sur une limite de 32 bits, tandis que d'autres types d'AVP s'alignent naturellement. Un certain nombre d'octets de valeur zéro sont ajoutés à la fin du champ Valeur d'AVP jusqu'à atteindre une limite de mot. La longueur du bourrage n'est pas reflétée dans le champ Longueur d'AVP [RFC3588].

Les champs dans l'AVP sont envoyés dans l'ordre des octets du réseau. Le format d'AVP est :



Code d'AVP : le code d'AVP, avec le champ facultatif Identifiant de fabricant, identifie un attribut qui suit. Si le bit V n'est pas établi, l'identifiant de fabricant n'est pas présent et le code d'AVP se réfère à un attribut de l'IETF.

Fanions d'AVP : le champ Fanions d'AVP fait deux octets. les bits suivants sont alloués :



V (Vendor, *fabricant*) : le bit "V" indique si le champ facultatif Identifiant de fabricant est présent dans l'en-tête d'AVP. Quand il est établi, le code d'AVP appartient à l'espace d'adresse spécifique du code de fabricant. Toutes les AVP définies dans le présent document DOIVENT avoir le bit "V" à zéro.

Réservé : ces bits de fanion sont réservés pour une utilisation future. Ils DOIVENT être réglés à zéro et ignorés par le receveur.

Longueur d'AVP : le champ Longueur d'AVP fait deux octets, et indique le nombre d'octets dans le champ Valeur. Les champs Longueur du code d'AVP, Longueur d'AVP, Fanions d'AVP, Réservé et Identifiant de fabricant ne sont pas comptés dans la valeur de Longueur d'AVP.

Réservé : ce champ de deux octets est réservé pour une utilisation future. Il DOIT être réglé à zéro et ignoré par le receveur.

Identifiant de fabricant : ce champ est présent si le bit "V" est établi dans le champ Fanions d'AVP. Le champ facultatif de quatre octets Identifiant de fabricant contient la valeur allouée par l'IANA de "code SMI d'entreprise de gestion de réseau" [IANAWEB], codée dans l'ordre des octets du réseau. Tout fabricant qui souhaite mettre en œuvre une AVP PANA spécifique de fabricant DOIT utiliser son propre identifiant de fabricant avec son espace d'adresses d'AVP privé, garantissant qu'il ne va pas entrer en collision avec toute autre AVP spécifique de fabricant ni avec de futures applications de l'IETF.

Valeur : le champ Valeur fait zéro, un ou plusieurs octets et contient des informations spécifiques de l'attribut. Le format du champ Valeur est déterminé par les champs Code d'AVP et Identifiant de fabricant. La longueur du champ Valeur est déterminée par le champ Longueur d'AVP.

7. Messages PANA

Chaque paire de message demande/réponse reçoit un numéro de séquence, et le sous type (c'est-à-dire, demande ou réponse) est identifié via le bit "R" (Request, *demande*) dans le champ Fanions de message de l'en-tête de message PANA.

Chaque message PANA DOIT contenir un type de message dans le champ Type de message de son en-tête, qui est utilisé pour déterminer l'action qui doit est être effectuée pour un message particulier. La Figure 3 fait la liste de tous les messages PANA définis dans le présent document :

Nom du message	Abréviation	Type de message	PaC<->PAA	Référence
PANA-Client-Initiation	PCI	1	-------->	7.1
PANA-Auth-Request	PAR	2	<------->	7.2
PANA-Auth-Answer	PAN	2	<------->	7.3
PANA-Termination-Request	PTR	3	<------->	7.4
PANA-Termination-Answer	PTA	3	<------->	7.5
PANA-Notification-Request	PNR	4	<------->	7.6
PANA-Notification-Answer	PNA	4	<------->	7.7

Figure 3 : Tableau des messages PANA

Le langage utilisé pour les définitions de message PANA (c'est-à-dire, les AVP valides pour ce type de message PANA) du paragraphe 7.1 au paragraphe 7.7, est défini en utilisant l'ABNF [RFC5234] comme suit :

```
message-def = Message-Name LWSP "::=" LWSP PANA-message
Message-Name = PANA-name
PANA-name = ALPHA *(ALPHA / DIGIT / "-")
PANA-message = header LWSP *fixed LWSP *required LWSP *optional LWSP *fixed
header  = "<" LWSP "PANA-Header:" LWSP Message-Type [r-bit] [s-bit] [c-bit] [a-bit] [p-bit] [i-bit] LWSP ">"
Message-Type = 1*DIGIT                          ; Type de message alloué au message
r-bit = ",REQ"
; S'il est présent, le bit "R" (demande) dans Fanions de message est établi, indiquant que le message est une demande, par
    opposition à une réponse. ;
s-bit      = ",STA"
; S'il est présent, le bit "S" (début) dans Fanions de message est établi, indiquant que le message est le PAR ou PAN initial
    dans la phase authentification et autorisation. ;
c-bit = ",COM"
; S'il est présent, le bit "C" dans Fanions de message est établi, indiquant que le message est le PAR et PAN final dans la
    phase authentification et autorisation ou réauthentification. ;
a-bit = ",REA"
; S'il est présent, le bit "A" (réAuthentification) dans Fanions de message est établi, indiquant que le message est une
    demande ou réponse de réauthentification. ;
p-bit = ",PIN"
; S'il est présent, le bit "P" (Ping) dans Fanions de message est établi, indiquant que le message est une demande ou réponse
    de ping. ;
i-bit = ",IPR"
; S'il est présent, le bit "I" (Reconfiguration IP) dans Fanions de message est établi, indiquant que le PaC exige une
    reconfiguration d'adresse IP après la réussite de la phase d'authentification et autorisation. ;
fixed = [qual] "<" LWSP avp-spec LWSP ">"                ; Définit la position fixée d'une AVP.
required = [qual] "{" LWSP avp-spec LWSP "}"
; l'AVP DOIT être présente et peut apparaître n'importe où dans le message. ;
optional = [qual] "[" LWSP avp-name LWSP "]"
; avp-name dans la règle "optional" ne peut pas évaluer de nom d'AVP inclus dans une règle fixée ou exigée. L'AVP peut
    apparaître n'importe où dans le message. ;
qual = [min] "*" [max]
; Voir les conventions d'ABNF au paragraphe 3.6 de la RFC 5234. L'absence de tout qualificatif dépend de si il précède une
    règle fixée, exigée, ou facultative. Si une règle fixée ou exigée n'a pas de qualificatif, alors exactement une de ces AVP
    DOIT être présente. Si une règle facultative n'a pas de qualificatif, alors 0 ou 1 de ces AVP peut être présente. ;
; Note : "[" et "]" ont une signification différente de celle de l'ABNF (voir la règle facultative ci-dessus). Ces crochets ne
    peuvent pas être utilisés pour exprimer des règles fixées facultatives (comme dans un AUTH facultatif à la fin). Pour
    faire cela, la convention est '0*1fixed'. ;
min = 1*DIGIT                   ; nombre minimum de fois que l'élément peut être présent. Par défaut la valeur est zéro.
```

```
max = 1*DIGIT
; nombre minimum de fois que l'élément peut être présent. Par défaut la valeur est infini. Une valeur de zéro implique que
    l'AVP NE DOIT PAS être présente. ;
avp-spec = PANA-name
; avp-spec doit être un AVP Name, défini dans les spécifications de base ou étendues du protocole PANA. ;
avp-name = avp-spec / "AVP"
; la chaîne "AVP" tient pour *tout* AVP Name arbitraire, qui n'entre pas en conflit avec les AVP exigées ou de position
    fixée définies dans la définition de message. ;
```

7.1 Initiation du client PANA (PCI)

Le message PANA-Client-Initiation (PCI) est utilisé pour une session initiée par le PaC. Les champs Numéro de séquence et Identifiant de session dans ce message DOIVENT être réglés à zéro (0).

```
PANA-Client-Initiation ::= < PANA-Header: 1 > *[ AVP ]
```

7.2 Demande d'authentification PANA (PAR)

Le message PANA-Auth-Request (PAR) est envoyé par le PAA ou par le PaC.

Le message NE DOIT PAS avoir à la fois établis les bits "S" (début) et "C" (terminé).

```
PANA-Auth-Request ::= < PANA-Header: 2,REQ[,STA][,COM][,IPR] >
                      [ EAP-Payload ]
                      [ Nonce ]
                     *[ PRF-Algorithm ]
                     *[ Integrity-Algorithm ]
                      [ Result-Code ]
                      [ Session-Lifetime ]
                      [ Key-Id ]
                     *[ AVP ]
                    0*1< AUTH >
```

7.3 Réponse d'authentification PANA (PAN)

Le message PANA-Auth-Answer (PAN) est envoyé par le PaC ou par le PAA en réponse à un message PANA-Auth-Request.

Le message NE DOIT PAS avoir à la fois établis les bits "S" (début) et "C" (terminé).

```
PANA-Auth-Answer ::= < PANA-Header: 2[,STA][,COM] >
                     [ Nonce ]
                     [ PRF-Algorithm ]
                     [ Integrity-Algorithm ]
                     [ EAP-Payload ]
                     [ Key-Id ]
                    *[ AVP ]
                   0*1< AUTH >
```

7.4 Demande de terminaison PANA (PTR)

Le message PANA-Termination-Request (PTR) est envoyé par le PaC ou par le PAA pour terminer une session PANA.

```
PANA-Termination-Request ::= < PANA-Header: 3,REQ >
                              < Termination-Cause >
                             *[ AVP ]
                            0*1< AUTH >
```

7.5 Réponse de terminaison PANA (PTA)

Le message PANA-Termination-Answer (PTA) est envoyé par le PaC ou par le PAA en réponse à PANA-Termination-Request.

PANA-Termination-Answer ::= < PANA-Header: 3 >
*[AVP]
0*1< AUTH >

7.6 Demande de notification PANA (PNR)

Le message PANA-Notification-Request (PNR) est utilisé pour signaler la réauthentification et effectuer un essai de vie. Voir aux paragraphes 4.3 et 4.2 les détails, respectivement, de la réauthentification et de l'essai de vie.

Le message DOIT avoir un des bits "A" (réauthentification) et "P" (Ping) exclusivement établi.

PANA-Notification-Request ::= < PANA-Header: 4,REQ[,REA][,PIN] >
*[AVP]
0*1< AUTH >

7.7 Réponse de notification PANA (PNA)

Le message PANA-Notification-Answer (PNA) est envoyé par le PAA (PaC) au PaC (PAA) en réponse à une PANA-Notification-Request provenant du PaC (PAA).

Le message DOIT avoir un des bits "A" (réauthentification) et "P" (Ping) exclusivement établi.

PANA-Notification-Answer ::= < PANA-Header: 4[,REA][,PIN] >
*[AVP]
0*1< AUTH >

8. AVP dans PANA

Le présent document utilise des formats de valeur d'AVP comme "OctetString" et "Unsigned32" comme défini au paragraphe 4.2 de la [RFC3588]. La définition de ces formats de données n'est pas répétée dans le présent document.

Le tableau qui suit donne la liste des AVP utilisées dans ce document, et spécifie dans quels messages PANA elles PEUVENT ou NON être présentes.

Le tableau utilise les symboles suivants :
0 : l'AVP NE DOIT PAS être présente dans le message.
0-1 : zéro ou une instance de l'AVP PEUT être présente dans le message. Plus d'une instance de l'AVP est considéré comme une erreur.
1 : une instance de l'AVP DOIT être présente dans le message.
0+ : zéro ou plus instances de l'AVP PEUVENT être présentes dans le message.

	Type de message						
Nom d'attribut	**PCI**	**PAR**	**PAN**	**PTR**	**PTA**	**PNR**	**PNA**
AUTH	0	0-1	0-1	0-1	0-1	0-1	0-1
EAP-Payload	0	0-1	0-1	0	0	0	0
Integrity-Algorithm	0	0+	0-1	0	0	0	0
Key-Id	0	0-1	0-1	0	0	0	0
Nonce	0	0-1	0-1	0	0	0	0
PRF-Algorithm	0	0+	0-1	0	0	0	0
Result-Code	0	0-1	0	0	0	0	0
Session-Lifetime	0	0-1	0	0	0	0	0
Termination-Cause	0	0	0	1	0	0	0

Figure 4 : Tableau d'occurrence des AVP

8.1 AVP AUTH

L'AVP AUTH (code d'AVP 1) est utilisée pour protéger l'intégrité des messages PANA. La charge utile des données de l'AVP contient le code d'authentification de message codé dans l'ordre des octets du réseau. La longueur de l'AVP varie selon l'algorithme d'intégrité utilisé. Les données de l'AVP sont du type OctetString.

8.2 AVP EAP-Payload

L'AVP EAP-Payload *(charge utile EAP)* (code d'AVP 2) est utilisée pour encapsuler le message EAP réel qui est échangé entre l'homologue EAP et l'authentificateur EAP. Les données de l'AVP sont du type OctetString.

8.3 AVP Integrity-Algorithm

L'AVP Integrity-Algorithm (code d'AVP 3) est utilisé pour porter l'algorithme d'intégrité pour calculer une AVP AUTH. Les données de l'AVP sont du type Unsigned32. Les données d'AVP contiennent un identifiant de transformation du protocole d'échange de clé Internet version 2 (IKEv2, *Internet Key Exchange Protocol version 2*) de type de transformation 3 [RFC4306] pour l'algorithme d'intégrité. Toutes les mises en œuvre de PANA DOIVENT prendre en charge AUTH_HMAC_SHA1_160 (7) [RFC4595].

8.4 AVP Key-Id

L'AVP Key-Id *(identifiant de clé)* (code d'AVP 4) est du type Integer32 et contient un identifiant de MSK. L'identifiant de MSK est alloué par le PAA et DOIT être unique au sein de la session PANA.

8.5 AVP Nonce

L'AVP Nonce *(nom occasionnel)* (code d'AVP 5) porte une valeur choisie au hasard qui est utilisée dans les calculs de clé de chiffrement. Les recommandations de la [RFC4086] s'appliquent à l'égard de la génération des valeurs aléatoires. Les données de l'AVP sont du type OctetString, et elles contiennent une valeur générée de façon aléatoire de forme opaque. La longueur des données DOIT être entre 8 et 256 octets, inclus.

La longueur des noms occasionnels est déterminée sur la base de la fonction pseudo aléatoire (PRF) disponible et du degré de confiance placé dans le PaC et le PAA pour calculer des valeurs aléatoires. La longueur de la valeur aléatoire pour le nom occasionnel est déterminée d'une des deux façons suivantes, selon que :

1. Le PaC et le PAA sont chacun probablement capables de calculer un nom occasionnel aléatoire (selon la [RFC4086]). La longueur du nom occasionnel doit être la moitié de la longueur de la clé de PRF (par exemple, 10 octets dans le cas de HMAC-SHA1).
2. Le PaC et le PAA ne sont de confiance ni l'un ni l'autre à l'égard du calcul d'un nom occasionnel aléatoire (selon la [RFC4086]). La longueur du nom occasionnel doit être la longueur complète de la clé de PRF (par exemple, 20 octets dans le cas de HMAC-SHA1).

De plus, la plus forte PRF disponible pour PANA doit être considérée dans ce calcul. Actuellement, une seule PRF (à savoir HMAC-SHA1) est disponible et donc la longueur maximum du résultat est de 20 octets. Donc, la longueur maximum de la valeur de nom occasionnel DEVRAIT être 20 octets.

8.6 AVP PRF-Algorithm

L'AVP PRF-Algorithm (code d'AVP 6) est utilisée pour porter la fonction pseudo aléatoire pour déduire PANA_AUTH_KEY. Les données de l'AVP sont du type Unsigned32. Les données de l'AVP contiennent un identifiant de transformation IKEv2 de type de transformation 2 [RFC4306]. Toutes les mises en œuvre de PANA DOIVENT prendre en charge PRF_HMAC_SHA1 (2) [RFC2104].

8.7 AVP Result-Code

L'AVP Result-Code (code d'AVP 7) est du type Unsigned32 et indique si l'authentification EAP a été achevée avec succès. Les valeurs de l'AVP Result-Code sont décrites ci-dessous :

PANA_SUCCESS : 0 les processus d'authentification et d'autorisation sont tous deux réussis.

PANA_AUTHENTICATION_REJECTED : 1 l'authentification a échoué. Quand l'authentification échoue, l'autorisation est aussi considérée comme ayant échoué.

PANA_AUTHORIZATION_REJECTED : 2 le processus d'autorisation a échoué. Cette erreur pourrait se produire quand l'autorisation est rejetée par un serveur AAA ou rejetée en local par un PAA, même si la procédure d'authentification a réussi.

8.8 AVP Session-Lifetime

L'AVP Session-Lifetime *(durée de vie de session)* (code d'AVP 8) contient le nombre de secondes restant avant que la session en cours soit considérée avoir expiré. Les données d'AVP sont du type Unsigned32.

8.9 AVP Termination-Cause

L'AVP Termination-Cause (code d'AVP 9) est utilisée pour indiquer au demandeur la raison de la terminaison d'une session. Les données d'AVP sont du type Enuméré. Les valeurs suivantes de Termination-Cause sont utilisées avec PANA :

LOGOUT : 1 (PaC -> PAA) le client a initié une déconnexion.

ADMINISTRATIVE : 4 (PAA -> PaC) l'accès n'a pas été accordé au client ou il a été déconnecté pour des raisons administratives.

SESSION_TIMEOUT : 8 (PAA -> PaC) la session est arrivée en fin de temporisation, et le service a été terminé.

9. Temporisateurs de retransmission

Le protocole PANA assure les retransmissions des messages PANA-Client-Initiation et de tous les messages de demande.

Les temporisateurs de retransmission PANA se fondent sur le modèle utilisé dans DHCPv6 [RFC3315]. Les variables utilisées ici sont aussi empruntées à cette spécification. PANA est un cprotocole fondé sur la demande/réponse. L'échange de messages se termine quand le demandeur reçoit bien la réponse, ou quand l'échange de messages est considéré avoir échoué selon le mécanisme de retransmission décrit ci-dessous.

Le comportement de retransmission est contrôlé et décrit par les variables suivantes :
RT *(Retransmission timeout)* : fin de temporisation depuis la précédente (re)transmission
IRT *(Initial ReTransmission)* : valeur de base pour RT pour la retransmission initiale
MRC (*Maximum Retransmission Count)* : compte maximum de retransmissions
MRT *(Maximum Retransmission Time)* : temps de retransmission maximum
MRD *(Maximum Retransmission Duration)* : durée de retransmission maximum
RAND *(Randomization factor)* : facteur d'aléation

À chaque transmission ou retransmission de message, l'envoyeur règle RT conformément aux règles données ci-dessous. Si RT expire avant la fin de l'échange de messages, l'envoyeur recalcule RT et retransmet le message.

Chaque calcul d'un nouveau RT inclut un facteur d'aléation (RAND) qui est un nombre aléatoire choisi avec une distribution uniforme entre -0,1 et +0,1. Le facteur d'aléation est inclus pour minimiser la synchronisation des messages.

L'algorithme pour choisir un nombre aléatoire n'a pas besoin d'être cryptographiquement significatif. L'algorithme DEVRAIT produire une séquence différente de nombres aléatoires à chaque invocation.

Pour la première retransmission de message, RT se fonde sur l'IRT : RT = IRT + RAND*IRT

Pour chaque retransmission de message suivante, RT est fondé sur la valeur précédente de RT : RT = 2*RTprev + RAND*RTprev.

MRT spécifie une limite supérieure de la valeur de RT (sans considération de l'aléa ajouté par l'utilisation de RAND). Si MRT a une valeur de 0, il n'y a pas de limite supérieure à la valeur de RT. Autrement, si (RT > MRT) RT = MRT + RAND*MRT.

MRC spécifie une limite supérieure au nombre de fois qu'un envoyeur peut retransmettre un message. Sauf si MRC est zéro, l'échange de messages échoue quand l'envoyeur a transmis le message MRC fois.

MRD spécifie une limite supérieure à la durée pendant laquelle un envoyeur peut retransmettre un message. Sauf si MRD est zéro, l'échange de messages échoue quand MRD secondes se sont écoulées depuis la première transmission du message par le client.

Si MRC et MRD sont tous deux différents de zéro, l'échange de messages échoue chaque fois que l'une des conditions spécifiées dans les deux paragraphes précédents est satisfaite.

Si MRC et MRD sont tous deux à zéro, le client continue de transmettre le message jusqu'à la réception d'une réponse.

9.1 Paramètrre de transmission et de retransmission

On présente ici un tableau des valeurs utilisées pour décrire le comportement de retransmission des messages de demandes PANA (REQ_*) et du message PANA-Client-Initiation (PCI_*). Le tableau montre les valeurs par défaut.

Paramètre	Valeur par défaut	Description
PCI_IRT	1 s	Fin de temporisation du PCI initial.
PCI_MRT	120 s	Valeur de la temporisation de Max PCI.
PCI_MRC	0	Maximum de tentatives de retransmissions de Max PCI.
PCI_MRD	0	Durée de retransmission de Max PCI.
REQ_IRT	1 s	Temporisation de demande initiale.
REQ_MRT	30 s	Valeur de la temporisation de Max Request.
REQ_MRC	10	Maximum de tentatives de retransmissions de Max Request.
REQ_MRD	0	Durée de retransmission de Max Request.

Ainsi, par exemple, le premier RT pour le message PANA-Auth-Request (PAR) est calculé en utilisant REQ_IRT comme IRT : RT = REQ_IRT + RAND*REQ_IRT

10. Considérations relatives à l'IANA

Cette Section donne des directives à l'Autorité d'allocation des numéros de l'Internet (IANA, *Internet Assigned Numbers Authority*) concernant l'enregistrement des valeurs relatives au protocole PANA, en accord avec le BCP 26 [RFC2434]. Les politiques suivantes sont utilisées ici avec les significations définies dans le BCP 26 : "Utilisation privée", "Premier arrivé, premier servi", "Revue d'expert", "Spécification exigée", "Consensus de l'IETF", et "Action de normalisation".

Cette Section explique les critères à utiliser par l'IANA pour l'allocation des numéros au sein des espaces de noms définis dans ce document.

Pour les demandes d'enregistrement où un expert désigné devrait être consulté, le directeur de zone de l'IESG responsable devrait appointer l'expert désigné. Pour un expert désigné avec spécification exigée, la demande est envoyée à la liste de diffusion du groupe de travail PANA (ou, si il a été dissous, un successeur désigné par le directeur de zone) pour commentaires et relecture, et DOIT inclure un pointeur sur une spécification publique. Avant l'écoulement d'une période de 30 jours, l'expert désigné va soit approuver, soit refuser la demande d'enregistrement et publier une note de la décision à la liste de diffusion du groupe de travail PANA ou son successeur. Une note de refus doit être justifiée par une explication et, dans les cas où c'est possible, des suggestions concrètes sur la façon dont la demande peut être modifiée afin qu'elle devienne acceptable.

L'IANA a créé un registre pour PANA.

10.1 Numéro d'accès UDP pour PANA

PANA utilise un numéro daccès UDP bien connu (voir au paragraphe 6.1) qui a été alloué par l'IANA (716).

10.2 En-tête de message PANA

Comme défini au paragraphe 6.2, l'en-tête de message PANA contient deux champs qui requièrent la gestion par l'IANA de l'espace de noms, des champs Type de message et Fanions.

10.2.1 Type de message

L'espace de noms de type de message est utilisé pour identifier les messages PANA. Le type de message 0 n'est pas utilisé et n'est pas alloué par l'IANA. La gamme de valeurs de 1 à 65 519 est pour les types de messages permanents standard, alloués par consensus de l'IETF [RFC2434]. Le présent document définit la gamme des valeurs de 1 à 4. Le même type de message est utilisé pour les messages de demande et de réponse, sauf pour le type 1. Le bit "R" distingue les demandes des réponses. Voir à la Section 7 l'allocation de l'espace de noms dans cette spécification.

La gamme des valeurs de 65 520 à 65 535 (valeurs hexadécimales 0xfff0 à 0xffff) est réservée pour les messages expérimentaux. Comme ces codes sont seulement pour des besoins expérimentaux et d'essai, aucune garantie d'interopérabilité n'est donnée entre le PaC et le PAA communiquants qui utilisent des commandes expérimentales, comme précisé dans la [RFC3692].

10.2.2 Fanions

Il y a 16 bits dans le champ Fanions de l'en-tête de message PANA. Le présent document allloue les bits 0 ("R"), 1 ("S"), 2 ("C"), 3 ("A"), 4 ("P"), et 5 ("I") au paragraphe 6.2. Les bits restants DOIVENT seulement être alloués via une action de normalisation [RFC2434].

10.3 En-tête d'AVP

Comme défini au paragraphe 6.3, l'en-tête d'AVP contient trois champs qui exigent la gestion de l'espace de noms par l'IANA : les champs Code d'AVP, Fanions d'AVP, et Identifiant de fabricant, où seuls le code d'AVP et les fanions d'AVP ont créé de nouveaux espaces de noms.

10.3.1 Code d'AVP

L'espace de noms de code d'AVP de 16 bits est utilisé pour identifier les attributs. Il y a plusieurs espaces de noms. Les fabricants peuvent avoir leur propre espace de noms de codes d'AVP, qui va être identifié par leur identifiant de fabricant (aussi appelé numéro d'entreprise) et ils contrôlent les allocations de leurs codes d'AVP spécifique de fabricant au sein de leur propre espace de noms. L'absence d'un identifiant de fabricant identifie l'espace de noms de codes d'AVP de l'IETF contrôlé par l'IANA. Les codes d'AVP, et parfois aussi de possibles valeurs dans une AVP, sont contrôlés et tenus par l'IANA.

Le code d'AVP 0 n'est pas utilisé et n'est pas alloué par l'IANA. Le présent document définit les codes d'AVP 1 à 9. Voir dans les paragraphes 8.1 à 8.9 les allocations de l'espace de noms dans cette spécification.

Les AVP peuvent être allouées suivant la politique de revue par expert désigné avec spécification exigée [RFC2434] ou action de normalisation.

Noter que PANA définit un mécanisme pour les AVP spécifique de fabricant, où le champ Identifiant de fabricant dans l'en-tête d'AVP est réglé à une valeur non zéro. Les codes d'AVP spécifiques de fabricant sont pour utilisation privée et devraient être encouragés plutôt que l'allocation de types d'attributs mondiaux, pour des fonctions spécifiques de seulement une mise en œuvre de fabricant de PANA, où aucune interopérabilité n'est réputée utile. Lorsque une AVP spécifique de fabricant est mise en œuvre par plus d'un fabricant, l'allocation d'AVP mondiales devrait plutôt être encouragée.

10.3.2 Fanions

Il y a 16 bits dans le champ Fanions d'AVP de l'en-tête d'AVP, défini au paragraphe 6.3. Le présent document alloue le bit 0 ("V").Les bits restants devraient seulement être alloués via une action de normalisation.

10.4 Valeurs d'AVP

Certaines AVP dans PANA définissent une liste de valeurs avec des significations diverses. Pour les attributs autres que ceux spécifiés dans ce paragraphe, l'ajout de valeurs supplémentaires à la liste peut être faite sur la base du premier arrivé, premier servi par l'IANA [RFC2434].

10.4.1 Valeurs d'AVP Result-Code

Comme défini au paragraphe 8.7, l'AVP Result-Code (code d'AVP 7) définit les valeurs 0-2.

Toutes les valeurs restantes sont disponibles pour allocation via consensus de l'IETF [RFC2434].

10.4.2 Valeurs d'AVP Termination-Cause

Comme défini au paragraphe 8.9, l'AVP Termination-Cause (code d'AVP 9) définit les valeurs 1, 4, et 8.

Toutes les valeurs restantes sont disponibles pour allocation via consensus de l'IETF [RFC2434].

11. Considérations sur la sécurité

Le protocole PANA définit une encapsulation d'EAP fondée sur UDP qui fonctionne entre deux nœuds à capacité IP. Diverses menaces sur la sécurité qui sont pertinentes pour un protocole de cette nature sont soulignées dans la [RFC4016]. Les considérations de sécurité qui découlent de l'utilisation d'EAP et des méthodes d'EAP sont discutées dans les [RFC3748] et [RFC5247]. Cette Section discute des questions de sécurité relatives au cadre et à la conception de PANA.

Un important élément pour assurer la sécurité de la conception et du déploiement de PANA dans un réseau est la présence d'une sécurité de couche inférieure. Dans le contexte du présent document, les couches inférieures sont dites sûres si leur environnement fournit une protection adéquate contre l'usurpattion d'identité et assure la confidentialité sur la base de ses besoins de fonctionnement. Par exemple, la sécurité de couche inférieure des réseaux DSL et cdma2000 est activée même avant d'avoir effectué la première authentification fondée sur PANA. En l'absence d'un tel canal sûr préétabli avant de faire fonctionner PANA, il peut en être créé un après la réussite de l'authentification PANA en utilisant un mécanisme cryptographique de couche réseau (par exemple, IPsec).

11.1 Mesures générales de sécurité

PANA fournit plusieurs mécanismes pour sécuriset une session PANA.

Les messages PANA portent des numéros de séquence qui sont augmentés de un à chaque nouveau message de demande. Ces numéros sont initialisés au hasard au début de la session, et ils sont confrontés aux numéros attendus à réception. Un message dont le numéro de séquence est différent de celui attendu est éliminé en silence. En plus d'accomplir une livraison ordonnée des messages EAP et une élimination des dupliqués, ce schéma aide aussi à empêcher un adversaire d'usurper des messages pour perturber les sessions PANA et EAP en cours sauf si il peut aussi espionner pour se synchroniser avec le numéro de séquence attendu. De plus, l'impact des attaques en répétition est réduit parce que tout message périmé (c'est-à-dire, une demande ou réponse avec un numéro de séquence inattendu et/ou un identifiant de session pour une session non existante) et toute réponse dupliquée sont immédiatement éliminés, et une demande dupliquée peut déclencher la transmission de la réponse mise en antémémoire (c'est-à-dire, il n'est pas besoin de traiter la demande et de générer une nouvelle réponse).

Le cadre PANA définit des EP, qui sont idéalement situés sur un appareil du réseau qui peut filtrer le trafic provenant des PaC avant qu'il entre dans l'Internet/intranet. Un ensemble de filtres peut être utilisé pour éliminer les paquets non autorisés, comme le message initial PANA-Auth-Request qui est reçu du segment de réseau d'accès, lorsque seuls les PaC sont supposés être connectés (c'est-à-dire, pour empêcher l'usurpation d'identité d'un PAA).

Le protocole assure aussi l'authentification et la protection de l'intégrité des messages PANA quand la méthode EAP utilisée peut générer des clés de session cryptographiques. Une SA PANA est générée sur la base de la MSK exportée par la méthode EAP. Cette SA est utilisée pour générer une AVP AUTH pour protéger l'en-tête de message et la charge utile PANA (incluant le message EAP complet).

La protection cryptographique empêche un adversaire d'agir comme interposé, d'injecter des messages, de répéter les messages et de modifier le contenu des messages échangés. Tout paquet qui échoue à la vérification de AUTH est éliminé en silence. Le plus tôt que cette protection peut être activée est quand le message PANA-Auth-Request qui signale la réussite de l'authentification (EAP Success) est généré. En commençant par ces messages, tout message PANA suivant peut être protégé cryptographiquement jusqu'à ce que la session soit supprimée.

La durée de vie de la SA PANA est réglée à la durée de vie de session PANA, qui est bordée par la durée de vie d'autorisation accordée par le serveur d'authentification. Une mise en œuvre PEUT ajouter une période de grâce à cette valeur. Sauf si la session PANA est étendue par l'exécution d'une autre authentification EAP, la SA PANA est supprimée quand la session en cours arrive à expiration.

La capacité d'utiliser la protection cryptographique au sein de PANA est déterminée par la méthode EAP utilisée, qui est généralement dictée par l'environnement de déploiement. Des couches inférieures non sûres nécessitent l'utilisation de méthodes EAP qui génèrent des clés. Dans les réseaux où les couches inférieures sont déjà sécurisées, la protection cryptographique des messages PANA n'est pas nécessaire.

11.2 Échange initial

L'échange initial PANA-Auth-Request et PANA-Auth-Answer est vulnérable aux attaques en usurpation car ces messages ne sont ni authentifiés ni protégés en intégrité. Afin d'empêcher des attaques de DoS très basiques, un adversaire ne devrait pas être capable de causer de création d'état par l'envoi de messages PANA-Client-Initiation au PAA. Cette protection est réalisée en permettant à celui qui répond (PAA) de créer aussi peu d'état que possible dans l'échange initial de messages. Cependant, il est difficile d'empêcher entièrement toutes les attaques d'usurpation dans l'échange de messages initial.

11.3 Méthodes EAP

L'espionnage des messages EAP pourrait causer des problèmes quand la méthode EAP est faible et permet des attaques de dictionnaire ou de répétition ou même permet à un adversaire d'apprendre directement le mot de passe à long terme. De plus, si la charge utile facultative Réponse/Identité EAP est utilisée, alors cela permet à l'adversaire d'apprendre l'identité du PaC. Dans ce cas, le problème de confidentialité est prévalent.

Pour prévenir ces menaces, la [RFC5193] suggère d'utiliser des méthodes EAP appropriées pour les environnements particuliers. Selon l'environnement de déploiement, une méthode EAP d'authentification qui prend en charge la confidentialité de l'identité de l'utilisateur, la protection contre les attaques de dictionnaire, et l'établissement de clés de session, doit être utilisée. Il est donc de la responsabilité des opérateurs de réseau et des utilisateurs de choisir la méthode EAP appropriée.

11.4 Clés de chiffrement

Quand la méthode EAP exporte une MSK, cette clé est utilisée pour produire une SA PANA avec PANA_AUTH_KEY avec un identifiant de clé distinct. La PANA_AUTH_KEY est unique pour la session PANA, et elle prend des valeurs de nom occasionnel fondées sur PANA dans le calcul pour la séparer cryptographiquement de la MSK.

La PANA_AUTH_KEY est seulement utilisée pour l'authentification et la protection de l'intégrité des messages PANA au sein de la session désignée.

La durée de vie de la SA PANA est limitée par la durée de vie de la MSK. Une autre exécution de la méthode EAP donne une nouvelle MSK, et elle met à jour la SA PANA, la PANA_AUTH_KEY, et l'identifiant de clé.

11.5 Chiffrement par paquet

Les réseaux qui ne sont pas sécurisés aux couches inférieures avant de lancer PANA peuvent s'appuyer sur l'activation d'un chiffrement du trafic de données par paquet dès la réussite de l'établissement de la SA PANA. Le cadre PANA permet la génération de clés de chiffrement à partir de la SA PANA et utilise les clés avec un protocole d'association sûr pour permettre la protection cryptographique par paquet, comme le chiffrement de couche de liaison ou fondé sur IPsec [PANA-IPSEC]. Ces mécanismes établissent en fin de compte un lien cryptographique entre le trafic de données généré par et pour un client et l'identité authentifiée du client. Le trafic de données peut être authentifié quant à l'origine des données, protégé en intégrité et contre la répétition, et facultativement chiffré en utilisant les clés de chiffrement. Comment ces clés sont générée à partir de la SA PANA et utilisées avec un protocole d'association sûr sort du domaine d'application de ce document.

11.6 Communication de PAA à EP

Le cadre PANA permet la séparation du PAA et de l'EP. L'échange de protocole entre le PAA et l'EP pour le provisionnement des informations de PaC autorisé sur l'EP doit être protégé pour l'authentification, la protection de l'intégrité et contre la répétition.

11.7 Vérification de vie

Une session PANA est associée à une durée de vie de session. La session est terminée sauf si elle est rafraîchie par un nouveau tour d'authentification EAP avant son expiration. Donc, le plus tard qu'une déconnexion de client peut être détectée est quand sa session expire. Une déconnexion peut aussi être détectée plus tôt avec les messages ping PANA.

Un message de demande peut être généré par le PaC ou le PAA à tout moment en phase d'accès dans l'attente que l'homologue réponde avec un message de réponse. Un aller-retour réussi de cet échange est une simple vérification que l'homologue est en vie.

Cet essai peut être engagé quand il y a une possibilité que l'homologue soit déconnecté (par exemple, après l'interruption du trafic de données pendant une longue période). L'utilisation périodique de cet échange comme mécanisme de maintien en vie exige une attention supplémentaire, car il pourrait en résulter de l'encombrement et donc de fausses alarmes.

Cet échange est protégé cryptographiquement quand une SA PANA est disponible afin de prévenir les menaces associées à l'abus de cette fonctionnalité.

Tout message de réponse PANA valide reçu en réponse à un message de demande récemment envoyé peut être pris comme indication de vie de l'homologue. Le PaC ou le PAA PEUT s'abstenir d'envoyer un message de demande ping explicite si un récent échange a déjà confirmé que l'homologue est en vie.

11.8 Terminaison précoce de session

Le protocole PANA prend en charge la capacité pour le PaC et le PAA de transmettre un message de terminaison avant l'expiration de la durée de vie de la session. Ce message cause la suppression de l'état, un arrêt de la procédure comptable et supprime l'état par PaC installé sur le ou les EP. Ce message est protégé cryptographiquement quand une SA PANA est présente.

12. Remerciements

Nous tenons à remercier Mark Townsley, Jari Arkko, Mohan Parthasarathy, Julien Bournelle, Rafael Marin Lopez, Pasi Eronen, Randy Turner, Erik Nordmark, Lionel Morand, Avi Lior, Susan Thomson, Giaretta Gerardo, Joseph Salowey, Sasikanth Bharadwaj, Spencer Dawkins, Tom Yu, Bernard Aboba, Subir Das, John Vollbrecht, Prakash Jayaraman, et tous les membres du groupe de travail PANA de leurs précieux commentaires sur ce document.

13. Références

13.1 Références normatives

[RFC2104] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", février 1997.

[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)

[RFC3588] P. Calhoun et autres, "Protocole fondé sur Diameter", septembre 2003. (*Remplacée par la* RFC6733) *(P.S.)*

[RFC3748] B. Aboba et autres, "Protocole extensible d'authentification (EAP)", juin 2004. *(P.S., MàJ par* RFC5247)

[RFC4086] D. Eastlake 3rd, J. Schiller, S. Crocker, "Exigences d'aléa pour la sécurité", juin 2005. (*Remplace* RFC1750) (BCP0106)

[RFC5192] L. Morand et autres, "Options DHCP pour identifier des agents d'authentification de protocole pour porter l'authentification d'accès au réseau (PANA)", mai 2008. *(P.S.)*

[RFC5234] D. Crocker, P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", janvier 2008. (STD0068)

13.2 Références pour information

[IANAWEB] IANA, "Number assignment", http://www.iana.org.

[PANA-IPSEC] Parthasarathy, M., "PANA Enabling IPsec based Access Control", Travail en cours, juillet 2005.

[RFC3315] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins et M. Carney, "Protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)", juillet 2003. (*MàJ par* RFC6422 et RFC6644, RFC7227 *; rendue obsolète par* RFC8415)

[RFC3692] T. Narten, "L'allocation de numéros expérimentaux et d'essai est considérée comme utile", janvier 2004. (BCP0082)

[RFC4016] M. Parthasarathy, "Analyse des menaces et exigences de sécurité pour le protocole de transport d'authentification et d'accès au réseau (PANA)", mars 2005. *(Information)*

[RFC4058] A. Yegin et autres, "Exigences pour le protocole de transport d'authentification pour l'accès au réseau (PANA)", mai 2005. *(Information)*

[RFC4137] J. Vollbrecht et autres, "Automates à états pour homologue et authentificateur du protocole d'authentification extensible (EAP)", août 2005. *(Information)*

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005. *(Obsolète, voir la* RFC5996)

[RFC4595] F. Maino, D. Black, "Utilisation de IKEv2 dans le protocole de gestion d'association de sécurité de canal fibre", juillet 2006. *(Information)*

[RFC5193] P. Jayaraman et autres, "Cadre du protocole pour porter l'authentification d'accès au réseau (PANA)", mai 2008. *(Info.)*

[RFC5247] B. Aboba et autres, "Cadre de gestion des clés du protocole d'authentification extensible (EAP)", août 2008. (*P. S. ;MàJ* RFC3748 *; MàJ par* RFC8940*)*

Adresse des auteurs

Dan Forsberg
Nokia Research Center
P.O. Box 407
FIN-00045 NOKIA GROUP
Finland
téléphone : +358 50 4839470
mél : dan.forsberg@nokia.com

Yoshihiro Ohba
Toshiba America Research, Inc.
1 Telcordia Drive
Piscataway, NJ 08854
USA
téléphone : +1 732 699 5305
mél : yohba@tari.toshiba.com

Basavaraj Patil
Nokia Siemens Networks
6000 Connection Drive
Irving, TX 75039
USA
mél : basavaraj.patil@nsn.com

Hannes Tschofenig
Nokia Siemens Networks
Linnoitustie 6 Espoo 02600
Finland
téléphone : +358 (50) 4871445
mél : Hannes.Tschofenig@nsn.com
URI : http://www.tschofenig.priv.at

Alper E. Yegin
Samsung
Istanbul,
Turkey
mél : a.yegin@partner.samsung.com

Déclaration complète de droits de reproduction