Groupe de travail Réseau
**Request for Comments : 5193**
Catégorie : Information

Traduction Claude Brière de L'Isle

P. Jayaraman,Net.Com
R. Lopez, Univ. of Murcia
Y. Ohba, éditeur, Toshiba
M. Parthasarathy, Nokia
A. Yegin, Samsung
mai 2008

# Cadre du protocole pour porter l'authentification pour l'accès réseau (PANA)



**Résumé**
Le présent document définit les éléments fonctionnels du cadre général du protocole pour porter l'authentification pour l'accès réseau (PANA, *Protocol for carrying Authentication for Network Access*) les généralités du flux d'appel, et les environnements de déploiement.

## Table des Matières



## 1. Introduction

Le protocole pour porter l'authentification pour l'accès réseau (PANA, *Protocol for carrying Authentication for Network Access*) est un protocole d'authentification d'accès réseau qui ignore la couche de liaison et fonctionne entre un client qui veut obtenir l'accès au réseau et un serveur sur le côté réseau. PANA définit une nouvelle couche inférieure de protocole d'authentification extensible (EAP, *Extensible Authentication Protocol*) [RFC3748] qui utilise IP entre les points d'extrémité de protocole.

La raison de la définition d'un tel protocole et les exigences sont décrites dans la [RFC4058]. Les détails du protocole sont documentés dans la [RFC5191]. Après une authentification PANA réussie, la sécurité de chaque paquet de données peut être réalisée en utilisant la sécurité physique, le chiffrement de couche de liaison, ou IPsec [PANA-IPSEC]. La mise en œuvre de serveur de PANA peut ou non être colocalisée avec l'entité qui applique la fonction de contrôle d'accès par paquet. Quand le serveur pour PANA et les entités de contrôle d'accès par paquet sont séparées, un protocole (par exemple, [RFC6320]) peut être utilisé pour porter les informations entre les deux nœuds.

PANA est destiné à être utilisé dans tout réseau d'accès sans considération de la sécurité sous-jacente. Par exemple, le réseau pourrait être physiquement sécurisé, ou sécurisé au moyen de mécanismes cryptographiques après la réussite de l'authentification client-réseau. Bien qu'il soit obligatoire pour un déploiement de PANA de mettre en œuvre un comportement qui assure l'intégrité des messages PANA quand la méthode EAP produit une MSK, il n'est pas obligatoire de mettre en œuvre la prise en charge de la sécurité du réseau à la couche de liaison ou à la couche réseau.

Le présent document définit le cadre général pour décrire comment ces divers élements PANA et autres éléments d'authentification d'accès au réseau interagissent les uns avec les autres, en particulier en considérant les deux types de base d'environnements de déploiement (voir la Section 4).

### 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. Cadre général de PANA

PANA est conçu pour faciliter l'authentification et l'autorisation des clients à l'accès aux réseaux. PANA est une couche inférieure d'EAP [RFC3748] qui porte les méthodes d'authentification d'EAP encapsulées à l'intérieur de EAP entre un nœud client et un serveur dans le réseau d'accès. Bien que PANA permette le processus d'authentification entre les deux entités, il est seulement une partie d'un cadre global d'authentification, autorisation et comptabilité (AAA, *Authentication, Authorization and Accounting*) et de contrôle d'accès. Un cadre d'AAA et de contrôle d'accès utilisant PANA se compose de quatre entités fonctionnelles.

La Figure 1 illustre ces entités fonctionnelles et les interfaces (protocoles, API) entre elles.

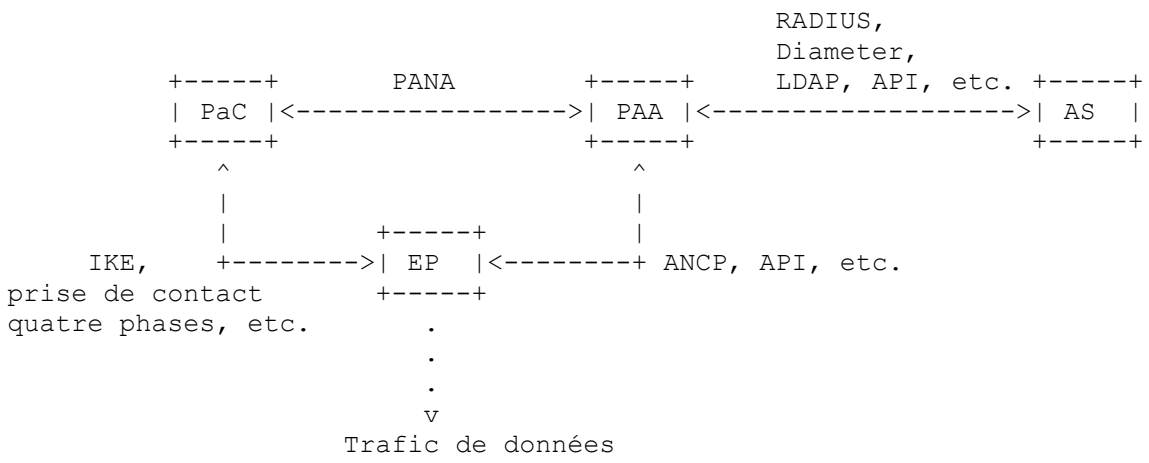


**Figure 1 : Modèle fonctionnel PANA**

Client PANA (PaC) : le PaC est la mise en œuvre de client de PANA. Cette entité réside sur le nœud qui demande l'accès au réseau. Les PaC peuvent être des hôtes d'extrémité, comme des tablettes, des PDA, des téléphones cellulaires, des ordinateurs portables, ou des routeurs qui sont connectés à un réseau via une interface filaire ou sans fil. Un PaC est chargé de demander l'accès au réseau et d'engager le processus d'authentification en utilisant PANA.

Agent d'authentification PANA (PAA, *PANA Authentication Agent*) : le PAA est la mise en œuvre de serveur de PANA. Un PAA est chargé de l'interface avec les PaC pour les authentifier et les autoriser pour le service d'accès au réseau. Le PAA consulte un serveur d'authentification afin de vérifier les accréditifs et les droits d'un PaC. Si le serveur d'authentification réside sur le même nœud que le PAA, une API est suffisante pour cette interaction. Quand ils sont séparés (un cas bien plus courant dans les réseaux d'accès publics) un protocole doit fonctionner entre les deux. Des protocoles d'AAA comme RADIUS [RFC2865] et Diameter [RFC3588] sont couramment utilisés à cette fin. Le PAA est aussi chargé de mettre à jour l'état de contrôle d'accès (c'est-à-dire, les filtres) dépendant de la création et la suppression de l'état d'autorisation. Le PAA communique l'état mis à jour aux points d'application (EP, *Enforcement Point*) dans le réseau. Si le PAA et l'EP résident sur le même nœud, une API est suffisante pour cette communication. Autrement, un protocole est nécessaire pour porter les attributs du client autorisé du PAA à l'EP. Le PAA réside sur un nœud qui est normalement appelé un serveur d'accès réseau (NAS, *Network Access Server*) dans le réseau d'accès. Par exemple, sur un serveur d'accès à distance à large bande (BRAS, *Broadband Remote Access Server*) [DSL] dans les réseaux DSL, ou sur un nœud de service de données de paquet (PDSN, *Packet Data Serving Node*) [3GPP2] dans les réseaux 3GPP2. Le PAA peut être à un ou plusieurs bonds IP des PaC.

Serveur d'authentification (AS, *Authentication Server*) : mise en œuvre de serveur qui est chargée de vérifier les accréditifs d'un PaC qui demande le service d'accès au réseau. L'AS reçoit les demandes du PAA au nom des PaC, et répond avec le résultat de la vérification ainsi que les paramètres d'autorisation (par exemple, la bande passante permise, la

configuration IP, etc). C'est le serveur qui termine l'EAP et les méthodes EAP. L'AS peut être hébergé sur le même nœud que le PAA, sur un nœud dédié sur le réseau d'accès, ou sur un serveur central quelque part dans l'Internet.

Point d'application (EP, *Enforcement Point*) : mise en œuvre du contrôle d'accès qui est chargée de permettre l'accès (trafic de données) des clients autorisés tout en empêchant l'accès des autres. Un EP apprend du PAA les attributs des clients autorisés. L'EP utilise des filtres cryptographiques ou non cryptographiques pour permettre de façon sélective et éliminer les paquets de données. Ces filtres peuvent être appliqués à la couche de liaisn ou à la couche IP [PANA-IPSEC]. Quand un contrôle d'accès cryptographique est utilisé, un protocole d'association sûr [RFC3748] doit fonctionner entre le PaC et l'EP. Après l'achèvement du protocole d'association sûr, la sécurité par paquet de couche de liaison ou couche réseau (par exemple TKIP, IPsec ESP) est activée pour la protection de l'intégrité, l'authentification de l'origine des données, la protection contre la répétition, et facultativement la protection de la confidentialité. Un EP est situé entre le réseau d'accès (la topologie accessible à chaque client) et le réseau accédé (la topologie accessible aux seuls clients autorisés). Il doit être situé de façon stratégique dans un réseau de zone locale pour minimiser l'accès à des clients non autorisés. Il est recommandé mais pas obligatoire que l'EP soit sur le chemin entre le PaC et le PAA pour la raison susmentionnée. Par exemple, l'EP peut être hébergé sur le commutateur qui est directement connecté aux clients dans un réseau filaire. De cette façon, l'EP peut éliminer les paquets non autorisés avant qu'ils atteignent tout autre nœud client au delà du réseau de zone locale.

Certaines des entités peuvent être colocalisées selon le scénario de déploiement. Par exemple, le PAA et l'EP pourraient être sur le même nœud (BRAS) dans les réseaux DSL. Dans ce cas, une simple API est suffisante entre le PAA et l'EP. Dans des déploiements de petite entreprise, le PAA et l'AS peuvent être hébergés sur le même nœud (routeur d'accès) ce qui élimine le besoin d'un protocole qui fonctionne entre les deux. La décision de colocaliser ces entitiés ou non, et leur localisation précise dans la topologie du réseau sont des décisions de déploiement qui sortent du domaine d'aplication du présent document.

## 3. Flux d'appels

La Figure 2 illustre le flux de signalisation pour autoriser un client à accéder au réseau.

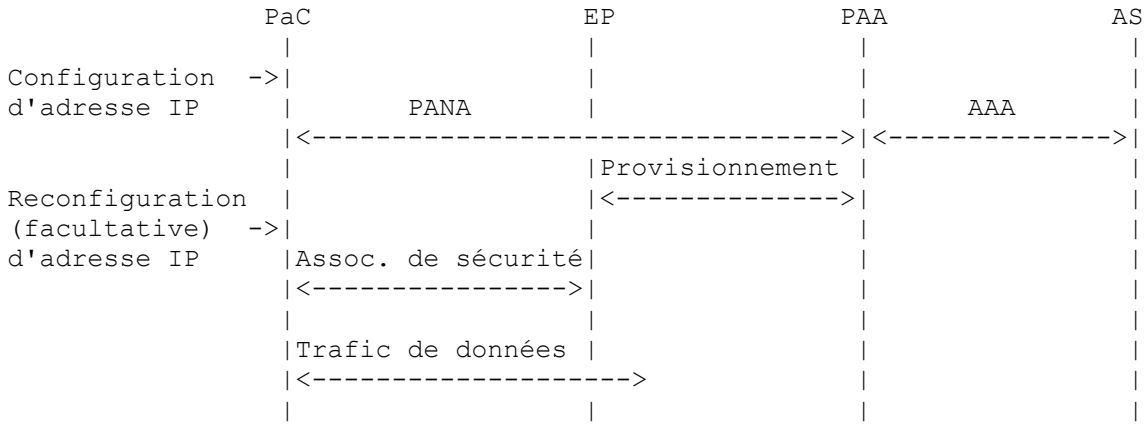


**Figure 2 : Flux de signalisation PANA**

L'EP sur le réseau d'accès permet le trafic général de données provenant de tout PaC autorisé, tandis qu'il permet seulement un type limité de trafic (par exemple, PANA, DHCP, découverte de routeur, etc.) pour les PaC non autorisés. Cela assure que les clients nouvellement rattachés ont le service d'accès minimum pour s'engager dans PANA et obtenir l'autorisation du service illimité.

Le PaC configure dynamiquement ou statiquement une adresse IP avant de faire fonctionner PANA. Après la réussite de l'authentification PANA, selon le scénario de déploiement, le PaC peut avoir besoin de reconfigurer son adresse IP ou de configurer des adresses IP supplémentaires. Par exemple, une adresse IPv6 de liaison locale peut être utilisée pour PANA et le PaC peut être autorisé à configurer une ou des adresses IPv6 mondiales après la réussite de l'authentification. Autre exemple : un PaC peut être limité à utiliser une adresse IPv4 de liaison locale durant PANA, et avoir la permission de reconfigurer son interface avec une adresse IPv4 non de liaison locale après l'authentification. Les applications d'utilité générale ne peuvent pas utiliser l'interface tant que l'authentification PANA n'est pas achevée avec succès et que la configuration d'adresse IP appropriée n'a pas eu lieu.

Un PaC initialement non autorisé commence l'authentification PANA par la découverte du PAA, suivie par l'échange EAP sur PANA. Le PAA interagit avec l'AS durant ce processus. À réception du résultat de l'authentification et de l'autorisation de l'AS, le PAA informe le PaC du résultat de sa demande d'accès au réseau.

Si le PaC est autorisé à accéder au réseau, le PAA envoie aussi les attributs spécifiques du PaC (par exemple, l'adresse IP, les clés de chiffrement, etc.) à l'EP en utilisant un autre protocole. L'EP utilise ces informations pour modifier ses filtres pour permettre aussi que le trafic de données de et vers le PaC passe.

Dans le cas où le contrôle d'accès cryptographique a besoin d'être activé après l'authentification PANA, un protocole d'association sûre fonctionne ente le PaC et l'EP. Les paramètres dynamiques exigés pour ce protocole (par exemple, l'identité du point d'extrémité, le secret partagé) sont déduits de l'authentification PANA réussie ; ces paramètres sont utilisés pour authentifier le PaC auprès de l'EP et vice-versa, au titre de la création de l'association de sécurité. Par exemple, voir dans [PANA-IPSEC] comment cela est fait pour IKE [RFC2409], [RFC4306] sur la base de l'utilisation d'une méthode EAP de génération de clé pour PANA entre le PaC et le PAA. L'échange de protocole d'association sûre produit les associations de sécurité requises entre le PaC et l'EP pour permettre la protection du trafic de données cryptographiques. La protection du trafic de données cryptographiques par paquet introduit des frais généraux supplémentaires par paquet mais les frais généraux existent seulement entre le PaC et l'EP et ne vont pas affecter les communications au delà de l'EP.

Finalement, les filtres qui sont installés à l'EP permettent que le trafic de données d'utilisation générale s'écoule entre le PaC et l'intranet/Internet.

## 4. Environnements

PANA peut être utilisé dans tout environnement de réseau si il y a un canal sûr de couche inférieure entre le PaC et l'EP avant PANA, ou si il en a été activé un à la suite de la réussite de l'authentification PANA.

À l'égard de l'authentification d'accès réseau, deux types de réseaux doivent être considérés :

a. Réseaux où un canal sûr est déjà disponible avant le fonctionnement de PANA : ce type de réseau est caractérisé par l'existence d'une protection contre l'usurpation d'identité et l'espionnage. Néanmoins, l'authentification et l'autorisation de l'utiliisateur sont requises pour la connexité au réseau.

   a.1. Un exemple est un réseau DSL où la sécurité de la couche inférieure est fournie par un moyen physique. La protection physique des fils du réseau assure qu'en pratique il y a seulement un client qui peut envoyer et recevoir des paquets IP sur la liaison.

   a.2. Un autre exemple est un réseau cdma2000 où la sécurité de la couche inférieure est fournie au moyen du chiffrement. Au moment où le client demande l'accès aux services de couche réseau, il est déjà authentifié et autorisé à accéder au canal radio, et le chiffrement de la couche de liaison est activé.

   La présence d'un canal sûr avant l'échange PANA élimine le besoin d'exécuter un protocole d'association sûr après le PANA. La session PANA peut être associée au canal de communication sur laquelle elle est portée. Aussi, le choix de la méthode d'authentification EAP dépend de la présence de cette sécurité pendant le fonctionnement de PANA.

b. Réseaux où un canal sûr est créé après le fonctionnement de PANA : ce sont les réseaux où il n'y a pas de protection de la couche inférieure avant le fonctionnement de PANA. La réussite de l'authentification PANA permet la génération de clés de chiffrement qui sont utilisées avec le protocole d'association sûre pour permettre la protection cryptographique par paquet.

   L'authentification PANA fonctionne sur un canal non sûr qui est vulnérable à l'espionnage et à l'usurpation d'identité. Le choix de la méthode EAP doit être résilient à de possibles attaques associées à cet environnement. De plus, la méthode EAP doit être capable de créer des clés de chiffrement qui vont ensuite être utilisées par le protocole d'association sûr.

Le choix d'utiliser la sécurité de couche de liaison par paquet ou la sécurité de couche réseau par paquet est une décision de mise en œuvre qui sort du domaine d'application du présent document. Cette décision dicte aussi le choix du protocole d'association sûr. Si la protection de couche de liaison est utilisée, le protocole va être spécifique de la couche de liaison. Si la protection de couche IP est utilisée, le protocole d'association sûr va être IKE et la sécurité par paquet va être fournie par IPsec AH/ESP sans considération de la technologie de couche de liaison sous-jacente.

## 5. Considérations sur la sécurité

La sécurité est discutée tout au long de ce document. Pour les considérations de sécurité spécifiques du protocole, se référer aux [RFC4016] et [RFC5191].

## 6. Remerciements

Nous tenons à remercier Bernard Aboba, Yacine El Mghazli, Randy Turner, Hannes Tschofenig, Lionel Morand, Mark Townsley, Jari Arkko, Pekka Savola, Tom Yu, Joel Halpern, Lakshminath Dondeti, David Black, et le groupe de travail IEEE 802.11 de leurs précieux commentaires.

## 7. Références

### 7.1 Références normatives

[DSL] DSL Forum Architecture and Transport Working Group, "DSL Forum TR-059 DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services", septembre 2003.

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

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

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

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

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

[RFC5191] D. Forsberg et autres, "Protocole pour porter l'authentification d'accès au réseau (PANA)", mai 2008. (*MàJ par* RFC5872) *(P.S.)*

### 7.2 Références pour information

[3GPP2] 3rd Generation Partnership Project 2, "cdma2000 Wireless IP Network Standard", 3GPP2 P.S0001-B/v2.0, septembre 2004.

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

[RFC2865] C. Rigney et autres, "Service d'authentification à distance de l'utilisateur appelant (RADIUS)", juin 2000. (*MàJ par* RFC2868, RFC3575, RFC5080, RFC8044) *(D.S.)*

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

[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)*

[RFC6320] S. Wadhwa et autres, "Protocole pour un mécanisme de contrôle de nœud d'accès dans les réseaux large bande", octobre 2011. *(P.S.)*

## Adresse des auteurs

Prakash Jayaraman
Network Equipment Technologies, Inc.

Rafa Marin Lopez
University of Murcia

Yoshihiro Ohba
Toshiba America Research, Inc.

6900 Paseo Padre Parkway
Fremont, CA 94555
USA
téléphone : +1 510 574 2305
mél : prakash_jayaraman@net.com

30100 Murcia
Spain
téléphone : +34 968 398 501
mél : rafa@um.es

1 Telcordia Drive
Piscateway, NJ 08854
USA
téléphone : +1 732 699 5305
mél : yohba@tari.toshiba.com

Mohan Parthasarathy
Nokia
313 Fairchild Drive
Mountain View, CA 94043
USA
téléphone : +1 408 734 8820
mél : mohanp@sbcglobal.net

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

## Déclaration complète de droits de reproduction