Groupe de travail Réseau
Request for Comments : 2989
Catégorie : Information

Traduction Claude Brière de L'Isle

B. Aboba, Microsoft
P. Calhoun, S. Glass, Sun Microsystems, Inc.
T. Hiller, P. McCann, H. Shiino, P. Walsh, Lucent
G. Zorn, G. Dommety, Cisco Systems, Inc., etc...
novembre 2000

Critères d'évaluation des protocoles AAA pour l'accès réseau

Résumé
Le présent document constitue un résumé des exigences des protocoles d'authentification, autorisation, et comptabilité (AAA, *Authentification, Autorisation, Accounting*) pour l'accès réseau. Pour créer le présent document, des emprunts ont été faits à des documents produits par les groupes de travail "Exigences pour les serveurs d'accès réseau de nouvelle génération" (NASREQ, *Network Access Server Requirements Next Generation*), "opérations d'itinérance" (ROAMOPS, *Roaming Operations*) et "MOBILEIP"ainsi que du TIA 45.6.

Le présent document résume les exigences collectées de ces sources, en séparant les exigences d'authentification, d'autorisation et de comptabilité. Les détails des exigences sont disponibles dans les documents d'origine.

1. Introduction

Le présent document représente un résumé des exigences pour l'accès réseau à l'égard des protocoles d'AAA. Pour la création du présent document, des emprunts ont été faits aux documents produits par les groupes de travail NASREQ [RFC3169], ROAMOPS [RFC2477], et MOBILEIP [RFC2977], ainsi que du TIA 45.6 [RFC3141]. Le présent document récapitule les exigences collectées à ces sources, séparant les exigences d'authentification, d'autorisation et de comptabilité. Les détails des exigences sont disponibles dans les documents d'origine.

1.1 Langage des exigences

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].

Prière de noter que les exigences spécifiées dans le présent document sont à utiliser dans l'évaluation des soumissions de protocoles AAA. À ce titre, le langage des exigences se réfère aux capacités de ces protocoles ; les documents de protocole vont spécifier si ces caractéristiques sont exigées, recommandées, ou facultatives. Par exemple, exiger qu'un protocole prenne en charge la confidentialité N'EST PAS la même chose qu'exiger que tout le trafic du protocole soit chiffré.

Une soumission de protocole n'est pas conforme si elle manque à satisfaire à une ou plusieurs des exigences DOIT ou NE DOIT PAS pour les capacités qu'elle met en œuvre. Une soumission de protocole qui satisfait à toutes les exigences DOIT, NE DOIT PAS, DEVRAIT et NE DEVRAIT PAS pour ses capacités est dite être "inconditionnellement conforme" ; celle qui satisfait à toutes les exigences DOIT et NE DOIT PAS mais pas à toutes les exigences DEVRAIT ou NE DEVRAIT PAS pour ses protocoles est dite être "conditionnellement conforme."

1.2 Terminologie

Comptabilité : acte de collecte des informations sur l'usage d'une ressource dans le but d'analyse des tendances, de vérification, de facturation, ou d'allocation des coûts.

Domaine administratif : un internet, ou une collection de réseaux, d'ordinateurs, et de bases de données sous une administration commune. Les entités informatiques opérant sous une administration commune peuvent être

supposées partager les associations de sécurité créées administrativement.

Participant : nœud conçu pour fournir l'interface de service entre un client et le domaine local.

Authentification : acte de vérification d'une revendication d'identité, sous la forme d'une étiquette préexistante provenant d'un espace de noms mutuellement connu, comme origine d'un message (authentification de message) ou comme point d'extrémité d'un canal (authentification d'entité).

Autorisation : acte de déterminer si un droit particulier, comme celui d'accéder à une ressource, peut être accordé au présentateur d'un accréditif particulier.

Facturation : acte de préparer une facture.

Courtier : c'est une entité qui est dans un domaine administratif différent à la fois du serveur AAA de rattachement et du fournisseur d'accès local, et qui fournit des services, comme de faciliter les payements entre le FAI local et les entités administratives de rattachement. Il y a deux types différents de courtiers : mandataire et d'acheminement.

Client : nœud qui souhaite obtenir un service d'un participant au sein d'un domaine administratif.

Bout en bout : c'est le modèle de sécurité qui exige que les informations de sécurité soient capables de traverser, et d'être validées même lorsque un message AAA est traité par des nœuds intermédiaires comme des mandataires, des courtiers, etc.

Domaine étranger : domaine administratif, visité par un client IP mobile, et contenant l'infrastructure AAA nécessaire pour mener à bien les opérations nécessaires qui permettent l'enregistrement IP mobile. Du point de vue de l'agent étranger, le domaine étranger est le domaine local.

Domaine de rattachement : domaine administratif contenant le réseau dont le préfixe correspond à celui de l'adresse de rattachement d'un nœud mobile, et contenant l'infrastructure AAA nécessaire pour mener à bien les opérations nécessaires qui permettent les enregistrements IP mobile. Du point de vue de l'agent de rattachement, le domaine de rattachement est le domaine local.

Bond par bond : c'est le modèle de sécurité qui exige que chaque ensemble d'homologues directs dans un réseau mandataire partage une association de sécurité, et que les informations de sécurité ne traversent pas une entité AAA.

Comptabilité inter domaines : c'est la collection d'informations sur l'usage des ressources d'une entité au sein d'un domaine administratif, à utiliser au sein d'un autre domaine administratif. Dans la comptabilité inter domaines, les paquets de comptabilité et les enregistrements de session vont normalement traverser les frontières administratives.

Comptabilité intra domaine : c'est la collection d'informations sur l'usage des ressources d'une entité au sein d'un domaine administratif, à utiliser au sein de ce domaine. Dans la comptabilité intra domaine, les paquets de comptabilité et les enregistrements de session ne traversent normalement pas les frontières administratives.

Domaine local : domaine administratif contenant l'infrastructure AAA intéressant immédiatement un client IP mobile lorsque il est hors de chez lui.

Mandataire : un mandataire AAA est une entité qui agit à la fois comme client et comme serveur. Lorsque une demande est reçue d'un client, le mandataire agit comme un serveur AAA. Lorsque la même demande a besoin d'être transmise à une autre entité AAA, le mandataire agit comme client AAA.

Mandataire local : c'est un serveur AAA qui satisfait à la définition d'un mandataire, et existe au sein du même domaine administratif que l'appareil réseau (par exemple, NAS) qui a produit la demande AAA. Normalement, un mandataire local va appliquer les politiques locales avant de transmettre les réponses aux appareils réseau, et est généralement utilisé pour multiplexer les messages AAA à partir d'un grand nombre d'appareils réseau.

Identifiant d'accès réseau : le NAI *(Network Access Identifier)* est l'identifiant d'utilisateur soumis par le client durant l'authentification d'accès réseau. En itinérance, l'objet du NAI est d'identifier l'utilisateur ainsi que d'aider à l'acheminement de la demande d'authentification. Le NAI peut n'être pas nécessairement le même que l'adresse de messagerie électronique de l'usager ou que l'identifiant d'utilisateur soumis dans une authentification de couche application.

Courtier d'acheminement : c'est une entité AAA qui satisfait à la définition d'un courtier, mais N'EST PAS sur le chemin de transmission des messages AAA entre le FAI local et les serveurs AAA du domaine de rattachement. Lorsque

une demande est reçue par un courtier d'acheminement, les informations sont retournées au demandeur AAA qui inclut les informations nécessaires pour qu'il soit capable de contacter directement le serveur AAA de rattachement. Certaines organisations qui fournissent des services de courtier d'acheminement PEUVENT aussi agir comme autorité de certification, permettant au courtier d'acheminement de retourner les certificats nécessaires pour que le FAI local et les serveurs AAA de rattachement communiquent en toute sécurité.

Courtier non mandataire : un routeur d'acheminement est parfois appelé un courtier non mandataire.

Courtier mandataire : c'est une entité AAA qui satisfait à la définition d'un courtier, et agit comme mandataire transparent dans le rôle d'agent de transmission pour tous les messages AAA entre le FAI local et les serveurs AAA du domaine de rattachement.

Comptabilité en temps réel : cela implique le traitement des informations sur l'usage des ressources au sein d'une fenêtre temporelle définie. Les contraintes de temps sont normalement imposées afin de limiter le risque financier.

Capacité d'itinérance : on peut la définir en gros comme la capacité à utiliser tout fournisseur d'accès Internet (FAI) tout en maintenant une relation formelle de client à fournisseur avec un seul d'entre eux. Des exemples de cas où la capacité d'itinérance peut être exigée incluent des "confédérations" de FAI et la prise en charge de l'accès à un réseau d'entreprise fournie par un FAI.

Enregistrement de session : cela représente un résumé de la consommation de ressources d'un utilisateur sur la session entière. Les passerelles de comptabilité qui créent l'enregistrement de session peuvent le faire en traitant les événements de comptabilité intermédiaires.

Mandataire transparent : c'est un serveur AAA qui satisfait à la définition d'un mandataire, mais n'applique aucune politique locale (ce qui signifie qu'il n'ajoute, ne supprime, ni ne modifie aucun attribut, et ne modifie pas les informations au sein des messages qu'il transmet).

2. Résumé des exigences

Les critères d'évaluation de protocoles AAA pour l'accès réseau sont résumés ci-dessous. Les détails des exigences figurent dans les documents référencés dans les chiffres des renvois mentionnés après la force de l'exigence et qui sont récapitulés à la fin du paragraphe 2.5.

2.1 Exigences générales

Ces exigences s'appliquent à tous les aspects de AAA et sont donc considérées comme des exigences générales.

Exigences générales	**NASREQ**	**ROAMOPS**	**IP mobile**
Adaptabilité (a)	DOIT 12	DOIT 3	DOIT 30 39
Reprise sur échec (b)	DOIT 12		DOIT 31
Authentification mutuelle client/serveur AAA (c)	DOIT 16		DOIT 30
Sécurité du niveau de transmission (d)		DOIT 6	DEVRAIT 31 39
Confidentialité de l'objet de données (e)	DOIT 26	DOIT 6	DOIT 40
Intégrité de l'objet de données (f)	DOIT 16	DOIT 6	DOIT 31 39
Transport de certificat (g)	DOIT 42		DEVRAIT/DOIT 31, 33/46
Mécanisme fiable de transport AAA (h)	DOIT 22		DOIT 31 32
Fonctionne sur IPv4	DOIT 11	DOIT 1	DOIT 33
Fonctionne sur IPv6	DOIT 11	DOIT 1	DEVRAIT 47
Accepte mandataires et courtiers d'acheminement (i)	DOIT 12		DOIT 31 39
Capacité d'audit (j)	DEVRAIT 25		
Sécurité duale d'appli. et transport non exigée (k)		PEUT 6	DOIT 40
Capacité à porter des attributs spécifiques du service	DOIT 43		DEVRAIT 31 33

Notes :

(a) Le protocole AAA doit être capable de prendre en charge des millions d'usagers et des dizaines de milliers de demandes simultanées. L'architecture et le protocole AAA DOIVENT être capables de prendre en charge des dizaines de milliers d'appareils, serveurs, mandataires et courtiers AAA.

(b) En cas d'échec de communication avec un certain serveur, le protocole doit fournir un mécanisme pour changer le

service sur un autre serveur secondaire ou de secours.

(c) Cette exigence se réfère à la capacité à prendre en charge l'authentification mutuelle entre client et serveur AAA.

(d) Le protocole AAA exige l'authentification, la protection de l'intégrité et de la confidentialité à la couche transmission. Ce modèle de sécurité est aussi appelé sécurité bond par bond, puisque la sécurité est établie entre deux homologues communicants. Toute la sécurité est supprimée lorsque le message AAA est traité par une entité AAA receveuse.

(e) Le protocole AAA exige la confidentialité au niveau objet, où un objet consiste en un ou plusieurs attributs. La confidentialité de niveau objet implique que seule l'entité AAA cible qui est le destinataire ultime des données puisse les déchiffrer, sans considération du fait que le message peut traverser une ou plusieurs entités AAA intermédiaires (par exemple, des mandataires, des courtiers).

(f) Le protocole AAA exige l'authentification et la protection de l'intégrité au niveau objet, qui consiste en un ou plusieurs attributs. L'authentification au niveau objet doit être persistante à travers une ou plusieurs entités AAA intermédiaires (par exemple, mandataire, courtier, etc.) ce qui signifie que toute entité AAA dans une chaîne de mandataires peut vérifier l'authentification. Cela implique que les données qui sont couvertes par la sécurité de niveau objet NE PEUVENT PAS être modifiées par les serveurs intermédiaires.

(g) Le protocole AAA DOIT être capable de transporter les certificats. Cette exigence est destinée à optimiser, au lieu d'exiger qu'un protocole hors bande soit utilisé pour aller chercher les certificats.

(h) Cette exigence se réfère à la résilience à la perte de paquet, incluant :
1. la retransmission bond par bond et la reprise sur échec afin que la fiabilité ne dépende pas seulement de la retransmission sur un seul bond de transport ;
2. le contrôle du mécanisme de retransmission par l'application AAA ;
3. l'accusé de réception par le transport qu'un message a bien été livré, indépendamment de l'évaluation sémantique ou syntaxique du message ;
5. le portage des accusés de réception dans les messages AAA ;
6. La livraison en temps utile des réponses AAA.

(i) Dans l'architecture AAA IP mobile, les courtiers peuvent être dans le chemin de transmission, auquel cas ils agissent comme mandataires transparents (courtiers mandataires). Autrement, il est aussi possible de concevoir des courtiers fonctionnant comme autorité de certification en dehors du chemin de transmission (courtiers d'acheminement).

(j) Un processus vérifiable est celui dans lequel il est possible de déterminer définitivement quelles actions ont été effectuées sur les paquets AAA lorsque ils voyagent du serveur de rattachement AAA à l'appareil réseau et retour.

(k) Le protocole AAA DOIT permettre que la communication soit sécurisée. Cependant, le protocole AAA DOIT aussi permettre que soit utilisé un service de sécurité sous-jacent (par exemple, IPsec). Lorsque ce dernier est utilisé, la sécurisation de la communication NE DOIT PAS être exigée.

(l) Le protocole AAA DOIT être extensible par un tiers (par exemple, d'autres groupes de travail de l'IETF) afin de définir des attributs spécifiques du service à définir. Cette exigence signifie simplement que le protocole AAA DOIT permettre à d'autres groupes que AAA de définir des attributs standard.

2.2 Exigences d'authentification

Exigences d'authentification	NASREQ	ROAMOPS	IP mobile
Prise en charge du NAI (a)	DOIT 9	DOIT 2	DEVRAIT/DOIT 32, 34, 39/40
Prise en charge de CHAP (b)	DOIT 10	DOIT 3	
Prise en charge de EAP (c)	DOIT 10	DEVRAIT 3	
Prise en charge de PAP/texte en clair|(d)	DOIT 26	NE DEVRAIT PAS 3	
Ré authentification à la demande (e)	DOIT 17		DEVRAIT 33
Autorisation seule sans authentification (f)	DOIT 9		

Notes :

(a) Le protocole AAA DOIT permettre l'utilisation d'identifiants d'accès réseau (NAI) [RFC2486] pour identifier les usagers et/ou les appareils.

(b) Le protocole AAA DOIT permettre le transport des informations d'authentification CHAP [RFC1994]. Elles sont couramment utilisées par les serveurs d'accès réseau (NAS) qui demandent l'authentification d'un usager PPP.

(c) Le protocole AAA DOIT permettre le transport d'une charge utile de protocole extensible d'authentification EAP, *Extensible Authentication Protocol*) [RFC2284]. Comme certains mécanismes d'authentification EAP exigent plus d'un aller retour, le protocole AAA doit permettre l'utilisation d'un tel mécanisme d'authentification. Le mécanisme d'authentification EAP réel négocié DOIT être transparent au protocole AAA. Lorsque EAP est utilisé, l'authentification se produit normalement entre l'usager à authentifier et son serveur AAA de rattachement.

(d) Bien que PAP soit déconseillé, son utilisation est encore largement répandue pour son objet d'origine, qui est la prise en charge des mots de passe en clair. Par suite, un protocole AAA devra être capable de transporter en toute sécurité des mots de passe en clair. Cela inclut d'assurer la confidentialité des mots de passe en clair qui voyagent sur le réseau, ainsi que la protection contre la divulgation des mots de passe en clair aux mandataires sur le chemin de transmission.

(e) Le protocole AAA DOIT permettre à un utilisateur d'être ré authentifié à la demande. Le protocole DOIT permettre que cet événement soit déclanché par l'utilisateur, par l'appareil d'accès (client AAA) ou par le serveur AAA de rattachement ou visité.

(f) Le protocole AAA NE DOIT PAS exiger que les accréditifs de l'usager soient fournis durant l'autorisation. Le protocole AAA ne prend en charge l'autorisation que par l'identification ou l'assertion.

2.3 Exigences d'autorisation

Exigences d'autorisation	**NASREQ**	**ROAMOPS**	**IP mobile**
Allocation statique et dynamique d'adresse IPv4/6 (a)	DOIT 11	DOIT 5	DOIT 32 36
Capacité de passerelle RADIUS (b)	DOIT 44	DOIT 3	DOIT 45
Capacité de rejet (c)	DOIT 12	DOIT 4	DOIT 39
Empêcher le tunnelage de couche 2	NE DOIT PAS 11	NE DOIT PAS 5	
Ré autorisation à la demande (d)	DOIT 18		DEVRAIT 30 33
Prise en charge des règles d'accès, restriction, filtres (e)	DOIT 11, 19		
Réconciliation d'état (f)	DOIT 20		
Déconnexion non sollicitée (g)	DOIT 18		

Notes :

(a) Le protocole AAA DOIT permettre à un serveur de fournir une adresse statique ou dynamique durant la phase d'autorisation d'un utilisateur et/ou appareil. L'adresse allouée DOIT être de type IPv4 ou IPv6. Si le client ET le serveur sont tous deux capables de traiter une adresse préconfigurée, elle est alors considérée comme statique. Tous le reste est dynamique.

(b) Cette exigence se réfère à la capacité d'un nouveau protocole AAA d'être suffisamment compatible avec la large base installée d'attributs pour les approches (RADIUS) existantes, de sorte qu'une mise en œuvre de serveur puisse parler les deux protocoles, ou faire la traduction de l'un à l'autre.

(c) Cette exigence se réfère à la capacité d'un courtier mandataire de refuser l'accès sans transmettre la demande d'accès au serveur AAA, ou de refuser l'accès après avoir reçu l'acceptation d'accès d'un serveur AAA.

(d) Cette exigence se réfère à la capacité d'un client ou serveur AAA de déclancher une ré autorisation, ou à la capacité du serveur d'envoyer des informations d'autorisation mises à jour à l'appareil, comme un "service d'arrêt". L'autorisation peut permettre pendant une certain temps, puis une autorisation supplémentaire devrait être demandée pour continuer. Un serveur peut initialement autoriser un usager à se connecter et recevoir des services, mais décider plus tard que l'usager n'est plus autorisé à utiliser le service, par exemple après N minutes. Les autorisations peuvent avoir une limite de temps. La ré autorisation n'implique pas nécessairement la ré authentification.

(e) Cette exigence se réfère à la capacité du protocole de décrire les limitations opérationnelles d'accès et les restrictions d'autorisation à l'usage du NAS qui incluent (mais ne se limitent pas à) :

1. les expirations de session et les fins de temporisation d'inactivité
2. les filtres de paquet
3. les chemins statiques
4. les paramètres de qualité de service.

(f) Cette exigence se réfère à la capacité du NAS d'utiliser le serveur AAA pour gérer l'état d'allocation de ressource.

Cette capacité peut aider au, mais n'est pas synonyme du contrôle simultané de connexion d'utilisateur, aux limitations d'usage d'accès, ou à la mise en commun d'adresses IP. La conception doit assurer la récupération des pertes de données dues à diverses fautes, incluant les réamorçages de NAS et de serveur AAA, et des pannes de communications de NAS/serveur AAA, et DOIT être indépendante du flux de comptabilité. La granularité de la récupération des informations d'état après une panne peut être de l'ordre d'une fraction de minute. Pour assurer la récupération d'état, des messages explicites d'état de session/ressource et de mise à jour et de déconnexion seront nécessaires. À cause de potentiels problèmes multi domaines, seul les systèmes qui allouent ou utilisent une ressource devraient suivre cet état.

(g) Cette exigence se réfère à la capacité du serveur AAA de demander au NAS de déconnecter une session active pour des raisons de politique d'autorisation.

2.4 Exigences de comptabilité

Exigences de comptabilité	NASREQ	ROAMOPS	IP mobile
Comptabilité en temps réel (a)	DOIT 14	DOIT 7	DOIT 31
Codage compact obligatoire (b)		DOIT 7	
Extensibilité d'enregistrement de comptabilité		DOIT 7	DOIT 33
Comptabilité par lots (c)	DEVRAIT 21		
Livraison garantie (d)	DOIT 22		DOIT 31
Horodatages comptables (e)	DOIT 23		DOIT 40
Comptabilité dynamique (f)	DOIT 48		

Notes :
(a) Cette exigence peut être en gros définie comme un rapport synchrone aux événements. Normalement la fenêtre temporelle est de l'ordre de la seconde, pas de la milliseconde.
(b) Le format des données comptables du protocole AAA NE DOIT PAS être gonflé, imposant de gros frais généraux à un ou plusieurs éléments de données comptables.
(c) Cette exigence se réfère à la capacité de mettre en mémoire tampon ou mémoriser plusieurs enregistrements de comptabilité, et de les envoyer ensemble ultérieurement.
(d) C'est un accusé de réception de couche application. C'est envoyé lorsque le serveur receveur accepte de prendre la responsabilité des données du message.
(e) Cette exigence se réfère à la capacité de refléter le moment d'occurrence d'événements comme la connexion, la déconnexion, l'authentification, l'autorisation et la comptabilité intérimaire. Elle implique aussi la capacité à fournir des horodatages sans ambiguïté.
(f) Cette exigence se réfère à la capacité de prendre en compte l'authentification et l'autorisation dynamiques. Pour prendre cela en charge, il peut y avoir plusieurs enregistrements comptables pour une seule session.

2.5 Exigences pour IP mobile seul

En plus des exigences ci-dessus, IP Mobile a les exigences supplémentaires suivantes :

Codage des messages d'enregistrement IP mobile	DOIT 33
Compatibilité aux pare-feu (a)	DOIT 35
Allocation d'agent de rattachement	DEVRAIT/DOIT 37/41

Notes
(a) Un protocole compatible aux pare-feu est celui qui est conçu pour s'accommoder d'un pare-feu qui agit comme mandataire. Par exemple, cela permettrait à un serveur AAA d'agent de rattachement situé derrière un pare-feu d'être accessible à partir de l'Internet afin de fournir des services AAA à un agent étranger IP mobile.

Renvois :
1 : paragraphe 4.2.1 de [RFC2477]
2 : paragraphe 4.2.2 de [RFC2477]. Voir aussi [RFC2486].
3 : paragraphe 4.2.3 de [RFC2477]. Voir aussi [RFC2284].
4 : paragraphe 4.2.4 de [RFC2477].
5 : paragraphe 4.2.5 de [RFC2477].
6 : paragraphe 4.2.6 de [RFC2477].
7 : paragraphe 4.3 de [RFC2477].
8 : Section 6 de [RFC3169]. Voir aussi [RFC2881].
9 : paragraphe 8.2.2.2 de [RFC3169]. Voir aussi [RFC2284].

10 : paragraphe 8.2.2.1 de [RFC3169]. Voir aussi [RFC2284].
11 : paragraphe 8.3.2.2 de [RFC3169]. Voir aussi [RFC2882].
12 : paragraphe 8.1.1 de [RFC3169].
13 : paragraphe 8.1.4.4 de [RFC3169].
14 : paragraphe 8.4.1.2 de [RFC3169].
15 : paragraphe 8.4.2 de [RFC3169].
16 : paragraphe 8.1.3 de [RFC3169].
17 : paragraphe 8.2.1.2 de [RFC3169].
18 : paragraphe 8.3.1.1 de [RFC3169].
19 : paragraphe 8.3.2.1 de [RFC3169]. Voir aussi [RFC2882].
20 : paragraphe 8.3.2.3 de [RFC3169]. Voir aussi [RFC2881], [RFC2882].
21 : paragraphe 8.4.1.3 de [RFC3169].
22 : paragraphe 8.4.1.1 de [RFC3169].
23 : paragraphe 8.4.1.4 de [RFC3169].
24 : paragraphe 8.4.3.1 de [RFC3169].
25 : paragraphe 8.4.3.2 de [RFC3169].
26 : paragraphe 8.2.3.1 de [RFC3169].
27 : paragraphe 8.3.3.1 de [RFC3169].
28 : paragraphe 8.1.4.1 de [RFC3169].
29 : se référer à [RFC2290]
30 : Section 3 de [RFC2977]
31 : paragraphe 3.1 de [RFC2977]
32 : Section 4 de [RFC2977]
33 : Section 5 de [RFC2977]
34 : paragraphe 5.1 de [RFC2977]
35 : paragraphe 5.2 de [RFC2977]
36 : paragraphe 5.3 de [RFC2977]
37 : paragraphe 5.4 de [RFC2977]
38 : paragraphe 5.5 de [RFC2977]
39 : Section 6 de [RFC2977]
40 : paragraphe 5.1 de [RFC3141]
41 : paragraphe 5.2.2 de [RFC3141]
42 : paragraphe 8.2.2.2 de [RFC3169]
43 : paragraphe 8.1.2.3 de [RFC3169]
44 : paragraphe 8.1.2.2 de [RFC3169]
45 : paragraphe 5.4 de [RFC3141]
46 : Section 7 de [RFC3141]
47 : Section 8 de [RFC2977]
48 : paragraphe 8.4.1.5 de [RFC3169]

3. Références

[RFC1570] W. Simpson, "Extensions LCP pour PPP", janvier 1994. *(P.S., MàJ par* 2484*)*

[RFC1661] W. Simpson, éditeur, "Protocole point à point (PPP)", STD 51, juillet 1994. *(MàJ par la* RFC2153)

[RFC1990] K. Sklower et autres, "Protocole multiliaison en PPP (MP)", août 1996. (*Remplace* RFC1717) *(D.S.)*

[RFC1994] W. Simpson, "Protocole d'authentification par mise en cause de la prise de contact en PPP (CHAP)", août 1996.

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

[RFC2002] C. Perkins, éd., "Prise en charge de la mobilité sur IP", octobre 1996. (*Obsolète, voir* RFC3220) *(P.S.)*

[RFC2284] L. Blunk, J. Vollbrecht, "Protocole extensible d'authentification (EAP) en PPP", mars 1998. (*Obs., voir* RFC3748) *(P.S.)*

[RFC2290] J. Solomon, S. Glass, "Option de configuration IPv4 mobile pour PPP IPCP", février 1998. (*MàJ par* RFC2794) *(P.S.)*

[RFC2477] B. Aboba, G. Zorn, "Critères pour l'évaluation des protocoles d'itinérance", janvier 1999. *(Information)*

[RFC2486] B. Aboba, M. Beadles, "Identifiant d'accès réseau", janvier 1999. (*Obsolète, voir* RFC4282) *(P.S.)*

[RFC2607] B. Aboba, J. Vollbrecht, "Chaînage de mandataire et mise en œuvre de politique dans l'itinérance", juin 1999. *(Info.)*

[RFC2794] P. Calhoun, C. Perkins, "Extension d'identifiant d'accès à un réseau mobile IP pour IPv4", mars 2000. *(P.S.)*

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

[RFC2866] C. Rigney, "Comptabilité RADIUS", juin 2000. (*MàJ par* RFC2867, RFC5080) *(Information)*

[RFC2881] D. Mitton, M. Beadles, "Exigences pour la prochaine génération de serveur d'accès réseau (NASREQNG) – modèle de NAS", juillet 2000. *(Information)*

[RFC2882] D. Mitton, "Exigences pour les serveur d'accès réseau : Extension de RADIUS", juillet 2000. *(Information)*

[RFC2977] S. Glass, T. Hiller, S. Jacobs, C. Perkins, "Exigences d'authentification, d'autorisation et de comptabilité pour IP mobile", octobre 2000. *(Information)*

[RFC3141] T. Hiller et autres, "Exigences de données sans fil CDMA2000 pour AAA", juin 2001. *(Information)*

[RFC3169] M. Beadles, D. Mitton, "Critères d'évaluation des protocoles de serveur d'accès réseau", septembre 2001. *(Information)*

[RFC3775] D. Johnson, C. Perkins, J. Arkko, "Prise en charge de la mobilité dans IPv6", juin 2004. *(P.S.) (Obs., voir* RFC6275)

4. Considérations sur la sécurité

Le présent document, being a les exigences document, does not have any security concerns. The security les exigences on protocols to be evaluated using this document are described in the referenced documents.

5. Considérations relatives à l'IANA

Le présent mémoire ne crée aucun nouvel espace de noms pour l'administration de l'IANA.

6. Remerciements

Merci aux membres des groupes de travail IP mobile, AAA, et NASREQ qui ont discuté et commenté ces exigences. Nous tenons aussi à remercier les membres de l'équipe d'évaluation AAA, Mike St. Johns, Barney Wolf, Mark Stevens, David Nelson, Dave Mitton, Basavaraj Patil et Stuart Barkley de leur relecture attentive du présent document.

7. Adresse des auteurs

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
téléphone : +1 425-936-6605
mél : bernarda@microsoft.com

Pat R. Calhoun
Sun Microsystems, Inc.
15 Network Circle
Menlo Park, CA 94025
téléphone : +1 650-786-7733
mél : pcalhoun@eng.sun.com

Steven M. Glass
Sun Microsystems
1 Network Drive
Burlington, MA 01845
téléphone : +1 781-442-0504
mél : steven.glass@sun.com

Tom Hiller
Lucent Technologies
263 Shuman Drive

Hajime Shiino
Lucent Technologies Japan Ltd.
25 Mori Bldg. 1-4-30 Roppongi,

Glen Zorn
Cisco Systems, Inc.
500 108th Avenue N.E., Suite 500

Room 1HP2F-218
Naperville, IL 60563
téléphone : +1 630-976-7673
mél : tom.hiller@lucent.com

Minato-ku Tokyo
Japan
téléphone : +81-3-5561-3695
mél : hshiino@lucent.com

Bellevue, WA 98004
téléphone : +1 425-468-0955
mél : gwz@cisco.com

Gopal Dommety
IOS Network Protocols
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
téléphone : +1 408-525-1404
mél : gdommety@cisco.com

Charles E. Perkins
Communications Systems Lab
Nokia Research Center
313 Fairchild Drive
Mountain View, CA
téléphone : +1 650-625-2986
mél : charliep@iprg.nokia.com

Basavaraj Patil
Nokia Networks
6000 Connection Dr.
Irving, TX 75039
téléphone : +1 972-894-6709
mél : Basavaraj.Patil@nokia.com

David Mitton
Nortel Networks
880 Technology Park Drive
Billerica, MA 01821
téléphone : +1 978-288-4570
mél : dmitton@nortelnetworks.com

Serge Manning
Nortel Networks
2201 Lakeside Blvd
Richardson, TX 75082-4399
téléphone : +1 972-684-7277
mél : smanning@nortelnetworks.com

Mark Anthony Beadles
SmartPipes, Inc.
565 Metro Place South
Suite 300
Dublin, OH 43017
téléphone : +1 614-923-5657
mél : mbeadles@smartpipes.com

Pat Walsh
Lucent Technologies
263 Shuman Blvd.
1F-545
Naperville, IL
téléphone : +1 630-713-5063
mél : walshp@lucent.com

Xing Chen
Alcatel USA
1000 Coit Road
Plano, TX 75075
téléphone : +1 972-519-4142
mél : xing.chen@usa.alcatel.com

Sanjeevan Sivalingham
Ericsson Wireless Communications Inc.,
Rm Q-356C
6455 Lusk Blvd
San Diego, CA 92126
téléphone :+1 858-332-5670
mél : s.sivalingham@ericsson.com

Alan Hameed
Fujitsu
2801 Telecom Parkway
Richardson, TX 75082
téléphone : +1 972-479-2089

Mark Munson
GTE Wireless
One GTE Place
Alpharetta, GA 30004
téléphone : +1 678-339-4439
mél : mmunson@mobilnet.gte.com

Stuart Jacobs
Secure Systems Department
GTE Laboratories
40 Sylvan Road,
Waltham, MA 02451-1128
téléphone : +1 781-466-3076
mél : sjacobs@gte.com

Byung-Keun Lim
LG Electronics, Ltd.
533, Hogye-dong, Dongan-ku, Anyang-shi,
Kyungki-do,431-080
Korea
téléphone : +82-31-450-7199
mél : bklim@lgic.co.kr

Brent Hirschman
1501 Shure Dr.
Arlington Hieghts, IL 60006
téléphone : +1 847-632-1563
mél : qa4053@email.mot.com

Raymond T. Hsu
Qualcomm Inc.
6455 Lusk Blvd.
San Diego, CA 92121
téléphone : +1 619-651-3623
mél : rhsu@qualcomm.com

Haeng S. Koo
Samsung Telecommunications America, Inc.
1130 E. Arapaho Road
Richardson, TX 75081
téléphone : +1 972-761-7755
mél : hskoo@sta.samsung.com

Mark A. Lipford
Sprint PCS
8001 College Blvd.; Suite 210
Overland Park, KS 66210
téléphone : +1 913-664-8335
mél : mlipfo01@sprintspectrum.com

Ed Campbell
3Com Corporation
1800 W. Central Rd.
Mount Prospect, IL 60056
téléphone : +1 847-342-6769
mél : ed_campbell@3com.com

Yingchun Xu
WaterCove Networks
One Century Centre, Suite 550
1750 E. Golf Road
Schaumburg, IL
téléphone : +1 847-477-9280
mél : yxu@watercove.com

Shinichi Baba
Toshiba America Research, Inc.
PO Box 136,
Convent Station, NJ 07961-0136
téléphone : +1 973-829-4795
mél : sbaba@tari.toshiba.com

Eric Jaques
Vodafone AirTouch
2999 Oak Road, MS-750
Walnut Creek, CA 94596
téléphone : +1 925-279-6142
mél : ejaques@akamail.com

8. Déclaration de propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

9. Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.