Groupe de travail Réseau
Request for Comments : 5176
RFC rendue obsolète : 3576
Catégorie : Information

Traduction Claude Brière de L'Isle

M. Chiba, Cisco Systems, Inc.
G. Dommety, Cisco Systems, Inc.
M. Eklund, Cisco Systems, Inc.
D. Mitton, RSA, Security Division of EMC
B. Aboba, Microsoft Corporation
January 2008

Extensions d'autorisation dynamique au service d'authentification à distance de l'utilisateur appelant (RADIUS)

Résumé
Le présent document décrit une extension actuellement déployée du protocole du service d'authentification à distance de l'utilisateur appelant (RADIUS, *Remote Authentication Dial In User Service*) qui permet des changements dynamiques sur une session d'utilisateur, telle que mise en œuvre par les produits de serveur d'accès réseau. Cela inclut la prise en charge de la déconnexion des utilisateurs et le changement des autorisations applicables à une session d'utilisateur.

Table des Matières

1. Introduction

Le protocole RADIUS, défini dans la [RFC2865], ne prend pas en charge les messages non sollicités envoyés du serveur RADIUS au serveur d'accès réseau (NAS, *Network Access Server*).

Cependant, il y a de nombreuses instances dans lesquelles il est désirable que des changements soient faits aux caractéristiques de la session, sans exiger que le NAS initie l'échange. Par exemple, il peut être souhaitable que les administrateurs soient capables de terminer la ou les sessions d'utilisateur en cours. Autrement, si l'utilisateur change le niveau d'autorisation, cela peut exiger que des attributs d'autorisation soient ajoutés/supprimés de la ou les sessions d'utilisateur.

Pour surmonter ces limitations, plusieurs fabricants ont mis en œuvre des commandes RADIUS supplémentaires afin de permettre que des messages non sollicités soient envoyés au NAS. Ces commandes étendues fournissent la prise en charge des paquets Déconnexion et Changement d'autorisation (CoA). Les paquets Déconnexion causent la terminaison immédiate de la ou des sessions d'utilisateur, tandis que les paquets CoA modifient les attributs d'autorisation de la session comme les filtres de données.

1.1 Applicabilité

Ce protocole est recommandé pour publication comme RFC pour information plutôt que comme RFC sur la voie de la normalisation à cause de problèmes qui ne peuvent pas être réglés sans créer d'incompatibilités avec les mises en œuvre déployées. Cela inclut des vulnérabilités pour la sécurité, ainsi que des ambiguïtés sémantiques résultént de la condeption des commandes de changement d'autorisation (CoA). Bien que des corrections soient recommandées, elles ne peuvent pas être rendues obligatoires car cela serait incompatible avec les mises en œuvre existantes.

Les mises en œuvre existantes de ce protocole ne prennent pas en charge les vérifications d'autorisation, de sorte qu'un FAI qui partage un NAS avec un autre FAI pourrait déconnecter ou changer les autorisations pour les utilisateurs d'un autre FAI. Afin de remédier à ce problème, une vérification de "transmission sur le chemin inverse" est décrite ; voir les détails au paragraphe 6.1.

Les mises en œuve existantes utilisent des algorithmes d'authentification et de protection de l'intégrité par paquet avec des faiblesses connues [MD5Attack]. Pour fournir une plus forte authentification et protection de l'intégrité par paquet, l'utilisation de IPsec est recommandée ; voir les détails au paragraphe 6.2.

Les mises en œuve existantes manquent de protection contre la répétition. Afin de prendre en charge la détection de répétition, il est recommandé qu'un attribut Horodatage d'événement soit ajouté à tous les paquets dans les situations où la protection IPsec contre la répétition n'est pas employée. Voir les détails au paragraphe 6.3.

L'approche suivie avec les commandes CoA dans les mises en œuvre existantes résulte en une ambiguïté sémantique. Les mises en œuve existantes de la demande de CoA identifient la session affectée, et assurent aussi les changements d'autorisation. Comme les attributs RADIUS inclus dans les mises en œuvre existantes de la demande de CoA peuvent être utilisés pour l'identification de session ou le changement d'autorisation, il peut n'être pas clair quelle fonction sert un certain attribut.

Le problème n'existe pas dans le protocole Diameter [RFC3588], dans lequel un changement d'autorisation initié par le serveur l'est en utilisant une commande Re-Auth-Request (RAR, *demande de réauthentification*) qui identifie la session via des paires d'attribut-valeur (AVP, *Attribute Value Pair*) User-Name *(nom d'utilisateur)* et Session-Id *(identifiant de session)* et qui contiennent une AVP Re-Auth-Request-Type *(type de demande de réauthentification)* avec la valeur "AUTHORIZE_ONLY" *(autorisation seule)*. Il en résulte en l'initiation d'une séquence standard demande/réponse où sont fournis les changements d'autorisation. Par suite, les AVP Diameter ne peuvent dans aucune commande avoir plusieurs significations potentielles.

1.2 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].

1.3 Terminologie

Le présent document utilise fréquemment les termes suivants :

Client d'autorisation dynamique (DAC, *Dynamic Authorization Client*) : entité qui génère les demandes de changement d'autorisation (CoA) ou les demandes de déconnexion. Bien qu'il soit possible que le DAC soit co-résident avec un serveur d'authentification ou de comptabilité RADIUS, cela n'est pas nécessairement le cas.

Serveur d'autorisation dynamique (DAS, *Dynamic Authorization Server*) : entité qui reçoit les paquets de demande de CoA ou de demande de déconnexion. Le DAS peut être un NAS ou un mandataire RADIUS.

Serveur d'accès réseau (NAS, *Network Access Server*) : appareil qui fournit l'accès au réseau.

Service : le NAS fournit un service à l'utilisateur, comme IEEE 802 ou le protocole point à point (PPP).

Session : chaque service fourni par le NAS à un utilisateur constitue une session, avec le début de la session défini comme le point où le service est d'abord fourni et la fin de la session définie comme le point où le service se termine. Un utilisateur peut avoir plusieurs sessions en parallèle ou à la suite si le NAS le prend en charge.

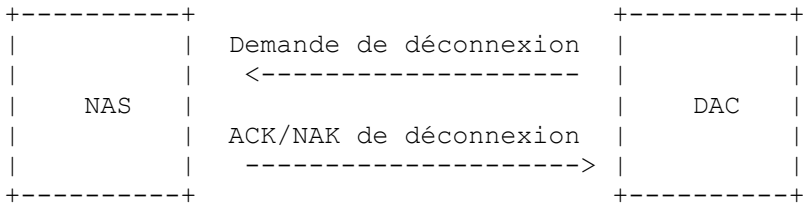
Éliminer en silence : cela signifie que la mise en œuvre élimine le paquet sans autre traitement. La mise en œuvre DEVRAIT fournir la capacité d'enregistrer l'erreur, y compris le contenu du paquet éliminé en silence, et DEVRAIT enregistrer l'événement dans un compteur de statistiques.

2. Vue d'ensemble

Cette section décrit les caractéristiques les plus couramment mises en œuvre des paquets de déconnexion et de changement d'autorisation (CoA).

2.1 Messages Disconnect (DM)

Un paquet demande de déconnexion *(Disconnect-Request)* est envoyé par le client d'autorisation dynamique afin de terminer la ou les sessions d'utilisateur sur un NAS et éliminer tout le contexte de session associé. Le paquet de demande de déconnexion est envoyé à l'accès UDP 3799, et identifie le NAS ainsi que la ou les sessions d'utilisateur à terminer par l'inclusion des attributs d'identification décrits à la Section 3.



Le NAS répond à un paquet Demande de déconnexion envoyé par un client d'autorisation dynamique par un ACK de déconnexion si tout le contexte de session associé est éliminé et si la ou les sessions d'utilisateur ne sont plus connectées, ou par un NAK de déconnexion, si le NAS n'a pas été capable de déconnecter une ou plusieurs sessions et d'éliminer tout le contexte de session associé. Un Disconnect-ACK PEUT contenir l'attribut Acct-Terminate-Cause (49) [RFC2866] avec la valeur réglée à 6 pour Admin-Reset.

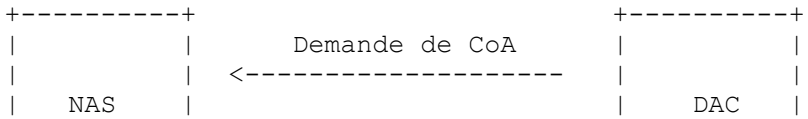
2.2 Messages Change-of-Authorization (CoA)

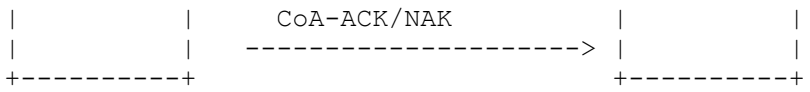
Les paquets de demande de CoA contiennent des informations pour changer dynamiquement les autorisations de session. Normalement, c'est utilisé pour changer les filtres de données. Les filtres de données peuvent être d'entrée ou de sortie, et sont envoyés en plus des attributs d'identification, comme décrit à la Section 3. L'accès utilisé et le format de paquet (décrit au paragraphe 2.3) sont les mêmes que pour les paquets de demande de déconnexion.

Les attributs suivants PEUVENT être envoyés dans une demande de CoA :

Filter-ID (11) *(identifiant de filtre)* : indique le nom d'une liste de filtres de données à appliquer pour la ou les sessions en lesquelles se transposent les attributs d'identification.

NAS-Filter-Rule (92) *(règle de filtre de NAS)* : donne une liste de filtres à appliquer pour la ou les sessions en lesquelles se transposent les attributs d'identification [RFC4849].





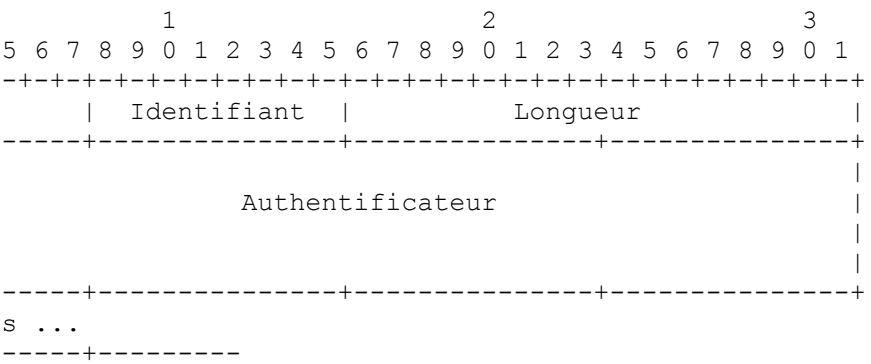
Le NAS répond à une demande de CoA envoyée par un client d'autorisation dynamique par un CoA-ACK si le NAS est capable de réussir à changer les autorisations pour la ou les sessions d'utilisateur, ou un CoA-NAK si la demande de CoA ne réussit pas. Un NAS DOIT répondre à une demande de CoA incluant un attribut Type de service avec une valeur non prise en charge par un CoA-NAK ; un attribut Cause d'erreur avec la valeur "Service non pris en charge" DEVRAIT être inclus.

2.3 Format de paquet

Pour les paquets Demande de déconnexion ou Demande de CoA, l'accès UDP 3799 est utilisé comme accès de destination. Pour les réponses, les accès de source et de destination sont inversés. Exactement un paquet RADIUS est encapsulé dans le champ Données UDP.

Un résumé du format des données est montré ci-dessous. Les champs sont transmis de gauche à droite.

Le format de paquet consiste en les champs suivants : Code, Identifiant, Longueur, Authentificateur, et Attributs en format de TLV (Type-Longueur-Valeur). Tous les champs ont la même signification que décrite dans RADIUS [RFC2865]. Le champ Authentificateur DOIT être calculé de la même façon que spécifié pour une demande de comptabilité dans la [RFC2866].



Code : le champ Code fait un octet, et identifie le type de paquet RADIUS. Les paquets reçus avec un champ Code invalide DOIVENT être éliminés en silence. Les codes RADIUS (en décimal) pour cette extension sont alloués comme suit :

40 - demande de déconnexion [RFC3575]
41 - ACK de déconnexion [RFC3575]
42 - NAK de déconnexion [RFC3575]
43 - demande de CoA [RFC3575]
44 - ACK de CoA [RFC3575]
45 - NAK de CoA [RFC3575]

Identifiant : le champ Identifiant fait un octet, et aide à confronter les demandes et les réponses. Un serveur d'autorisation dynamique qui met en œuvre la présente spécification DOIT être capable de détecter une demande dupliquée si elle a la même adresse de source, le même accès de source UDP, et le même identifiant, dans un court délai.

La responsabilité de la retransmission des paquets Demande de déconnexion et Demande de CoA incombe au client d'autorisation dynamique. Si après l'envoi de ces paquets, le client d'autorisation dynamique ne reçoit pas de réponse, il va retransmettre.

Le champ Identifiant DOIT être changé chaque fois que le contenu du champ Attributs change, ou chaque fois qu'une réponse valide a été reçue pour une réponse précédente. Pour les retransmissions où les contenus sont identiques, l'identifiant DOIT rester inchangé.

Si le client d'autorisation dynamique retransmet une demande de déconnexion ou une demande de CoA au même serveur d'autorisation dynamique que précédemment, et si les attributs n'ont pas changé, les mêmes Authentificateur de demande, Identifiant, et Accès de source DOIVENT être utilisés. Si des attributs ont changé, un nouvel Authentificateur et Identifiant DOIVENT être utilisés.

Si la demande à un serveur d'autorisation dynamique principal échoue, un serveur d'autorisation dynamique secondaire doit être interrogé, si disponible ; les questions relatives aux algorithmes de reprise sur défaillance sont décrites dans la [RFC3539]. Comme cela représente une nouvelle demande, un nouvel Authentificateur et Identifiant de demande DOIVENT être utilisés. Cependant, lorsque le client d'autorisation dynamique envoie directement au NAS, la reprise sur défaillance n'a normalement pas de sens, car les paquets de demande de CoA ou de demande de déconnexion n'ont pas besoin d'être livrés au NAS où réside la session.

Longueur : le champ Longueur fait deux octets. Il indique la longueur du paquet incluant les champs Code, Identifiant, Longueur, Authentificateur, et Attribut. Les octets en dehors de la gamme du champ Longueur DOIVENT être traités comme du bourrage et ignorés à réception. Si le paquet est plus court que ce que le champ Longueur indique, il DOIT être éliminé en silence. La longueur minimum est 20 et la longueur maximum est 4096.

Authentificateur : le champ Authentificateur est de seize (16) octets. L'octet de poids fort est transmis en premier. Cette valeur est utilisée pour authentifier les paquets entre le client d'autorisation dynamique et le serveur d'autorisation dynamique.

Authentificateur de demande : dans les paquets de demande, la valeur de l'authentificateur est une somme de contrôle MD5 de 16 octets [RFC1321], appelée Authentificateur de demande. L'authentificateur de demande est calculé de la même façon que pour une demande de comptabilité, spécifiée dans la [RFC2866].

Noter que l'authentificateur de demande d'une demande de CoA ou d'une demande de déconnexion ne peut pas être calculé de la même façon que l'authentificateur de demande d'une demande d'accès RADIUS, parce que il n'y a pas d'attribut Mot de passe d'utilisateur dans une demande de CoA ou demande de déconnexion.

Authentificateur de réponse : le champ Authentificateur dans un paquet de réponse (par exemple, ACK de déconnexion, NAK de déconnexion, ACK de CoA, ou NAK de CoA) est appelé l'authentificateur de réponse, et contient un hachage MD5 unidirectionnel calculé sur un flux d'octets consistant en les champs Code, Identifiant, Longueur, Authentificateur de demande du paquet auquel il est répondu, et les attributs de réponse si il en est, suivis par le secret partagé. La valeur de hachage MD5 résultante de 16 octets est mémorisée dans le champ Authentificateur du paquet de réponse.

Note administrative : comme noté à la Section 3 de la [RFC2865], le secret (mot de passe partagé entre le client d'autorisation dynamique et le serveur d'autorisation dynamique) DEVRAIT être au moins aussi long et non devinable qu'un mot de passe bien choisi. Le serveur d'autorisation dynamique DOIT utiliser l'adresse IP de source du paquet UDP RADIUS pour décider quel secret partagé utiliser, afin que les demandes puissent être confiées à un mandataire.

Attributs : dans les paquets de demande de CoA et de demande de déconnexion, tous les attributs DOIVENT être traités comme obligatoires. Si un ou plusieurs changements d'autorisation spécifiés dans une demande de CoA ne peuvent pas être effectués, le NAS DOIT envoyer un NAK de CoA. Un NAS DOIT répondre à une demande de CoA contenant un ou plusieur attributs ou valeurs d'attribut non pris en charge avec un NAK de CoA ; un attribut Cause d'erreur avec la valeur 401 (Attribut non pris en charge) ou 407 (Valeur d'attribut invalide) PEUT être inclus. Un NAS DOIT répondre à une demande de déconnexion contenant un ou plusieurs attributs ou valeurs d'attribut non pris en charge avec un NAK de déconnexion ; un attribut Cause d'erreur avec la valeur 401 (Attribut non pris en charge) ou 407 (Valeur d'attribut invalide) PEUT être inclus.

Les changements d'état résultant d'une demande de CoA DOIVENT être atomiques : si la demande de CoA réussit pour toutes les sessions correspondantes, le NAS DOIT envoyer un ACK de CoA en réponse, et tous les changements d'autorisation demandés DOIVENT être effectués. Si la demande de CoA ne réussit pas pour toute session correspondante, le NAS DOIT envoyer un NAK de CoA en réponse, et les changements d'autorisation demandés NE DOIVENT être faits pour aucune des sessions correspondantes. De même, un changement d'état NE DOIT PAS se poduire par suite d'une demande de déconnexion qui ne réussit pas par rapport à toute session correspondante ; un NAS DOIT envoyer un NAK de déconnexion en réponse si une des sessions correspondantes ne peut pas être terminée. Un NAS qui ne prend pas en charge les changements d'autorisation dynamiques s'appliquant à plusieurs sessions DOIT envoyer un NAK de CoA ou un NAK de déconnexion en réponse ; un attribut Cause d'erreur de valeur 508 (Choix de sessions multiples non accepté) DEVRAIT être inclus.

Dans la présente spécification, des attributs peuvent être utilisés pour l'identification, l'autorisation, ou d'autres objets. Les spécifications d'attributs RADIUS créées après la publication du présent document DEVRAIENT déclarer si un attribut peut être inclus dans les messages CoA ou Déconnexion, et si ils le peuvent, quels messages peuvent être inclus dedans et si il sert comme attribut d'identification ou d'autorisation.

Même si un NAS met en œuvre un attribut à utiliser avec l'authentification et la comptabilité RADIUS, il est possible qu'il n'accepte pas l'inclusion de cet attribut dans les paquets de demande de CoA et de demande de déconnexion, étant données les différences de la sémantique d'attribut. Ceci est vrai même pour des attributs spécifiés comme admissibles au sein des paquets Accès accepté (comme ceux définis dans les [RFC2865], [RFC2868], [RFC2869], [RFC3162], [RFC3579], [RFC4372], [RFC4675], [RFC4818], et [RFC4849]).

3. Attributs

Dans les paquets Demande de déconnexion et Demande de CoA, certains attributs sont utilisés pour identifier de façon univoque le NAS ainsi que la ou les sessions d'utilisateur sur le NAS. La combinaison du NAS et des attributs d'identification de session inclus dans un paquet Demande de CoA ou Demande de déconnexion DOIT correspondre au moins à une session afin qu'une demande réussisse ; autrement, un NAK de déconnexion ou un NAK de CoA DOIT être envoyé. Si tous les attributs d'identification de NAS correspondent, et que plus d'une session correspond à tous les attributs d'identification de session, alors une demande de CoA ou demande de déconnexion DOIT s'appliquer à toutes les sessions correspondantes.

Les attributs d'identification incluent des attributs d'identification de NAS et de session, comme décrit ci-dessous.

Attributs d'identification de NAS

Attribut	n°	Référence	Description
NAS-IP-Address	4	[RFC2865]	Adresse IPv4 du NAS.
NAS-Identifier	32	[RFC2865]	Chaîne d'identification du NAS.
NAS-IPv6-Address	95	[RFC3162]	Adresse IPv6 du NAS.

Attributs d'identification de session

Attribut	n°	Référence	Description
User-Name	1	[RFC2865]	Nom de l'utilisateur associé à une ou plusieurs sessions.
NAS-Port	5	[RFC2865]	Accès sur lequel une session se termine.
Framed-IP-Address	8	[RFC2865]	Adresse IPv4 associée à une session.
Vendor-Specific	26	[RFC2865]	Un ou plusieurs attributs d'identification spécifiques du fabricant.
Called-Station-Id	30	[RFC2865]	Adresse de la liaison à laquelle une session est connectée.
Calling-Station-Id	31	[RFC2865]	Adresse de la liaison à partir de laquelle une ou plusieurs sessions sont connectées.
Acct-Session-Id	44	[RFC2866]	Identifiant univoque d'une session sur le NAS.
Acct-Multi-Session-Id	50	[RFC2866]	Identifiant univoque des sessions concernées.
NAS-Port-Id	87	[RFC2869]	Chaîne identifiant l'accès où est une session.
Chargeable-User-Identity	89	[RFC4372]	CUI associé à une ou plusieurs sessions. Nécessaire lorsque un identifiant d'accès réseau (NAI) de confidentialité est utilisé, car alors le nom d'utilisateur (par exemple, "anonymous") ne peut pas identifier les sessions qui appartiennent à un certain utilisateur.
Framed-Interface-Id	96	[RFC3162]	Identifiant d'interface IPv6 associé à une session, toujours envoyé avec Framed-IPv6-Prefix.
Framed-IPv6-Prefix	97	[RFC3162]	Préfixe IPv6 associé à une session, toujours envoyé avec Framed-Interface-Id.

Pour traiter les questions de sécurité décrites au paragraphe 6.1, l'attribut User-Name ou Chargeable-User-Identity DEVRAIT être présent dans les paquets Demande de déconnexion et Demande de CoA.

Lorsque un client Diameter utilise le même identifiant de session pour l'autorisation et la comptabilité, l'inclusion d'un attribut Identifiant de session comptable dans une demande de déconnexion ou de CoA peut aider la traduction Diameter/RADIUS, car les commandes Diameter RAR et ASR incluent une AVP Identifiant de session. Un attribut Identifiant de session comptable DEVRAIT être inclus dans les paquets de demande de déconnexion et de demande de CoA.

Un NAS qui met en œuvre la présente spécification DEVRAIT envoyer un attribut Identifiant de session comptable ou Identifiant multi sessions comptables au sein d'une demande d'accès. Lorsque un attribut Identifiant de session comptable ou Identifiant multi sessions comptables n'est pas inclus dans une demande d'accès, le client d'autorisation dynamique ne peut pas savoir le Identifiant de session comptable ou Identifiant multi sessions comptables de la session qu'il tente de cibler, sauf si il a aussi accès aux données de comptabilité pour cette session.

Lorsque un attribut Identifiant de session comptable ou Identifiant multi sessions comptables n'est pas présent dans une demande de CoA ou demande de déconnexion, il est possible que les attributs Nom d'utilisateur ou Identité d'utilisateur facturable ne soient pas suffisants pour identifier de façon univoque une seule session (par exemple, si le même utilisateur a plusieurs sessions sur le NAS, ou si le NAI de confidentialité est utilisé). Dans ce cas, si on désire identifier une seule session, l'identification de la session PEUT être effectuée en utilisant un ou plusieurs des attributs Adresse IP tramée, Préfixe IPv6 tramé/Identifiant d'interface tramée, Identifiant de station appelée, Identifiant de station appelante, Accès de NAS, et Identifiant d'accès de NAS.

Pour aider les mandataires RADIUS à acheminer les paquets de demandes à leur destination, un ou plusieurs des attributs Adresse IP de NAS ou Adresse IPv6 de NAS DEVRAIENT être présents dans les paquets Demande de CoA et Demande de déconnexion ; l'attribut Identifiant de NAS PEUT être présent. Les questions d'usurpation d'identité avec les attributs Identification de NAS sont discutées au paragraphe 4.3.7 de la [RFC3579].

Une demande de déconnexion DOIT contenir seulement des attributs de NAS et d'identification de session. Si d'autres attributs sont inclus dans une demande de déconnexion, les mises en œuve DOIVENT envoyer un NAK de déconnexion ; un attribut Cause d'erreur de valeur "Attribut non pris en charge" PEUT être inclus.

Le DAC peut exiger l'accès aux données provenant des paquets d'authentification ou de comptabilité RADIUS. Il utilise ces données pour composer des paquets de demande de CoA ou de demande de déconnexion conformes. Par exemple, comme décrit au paragraphe 3.3, un paquet Demande de CoA qui contient un attribut Type de service avec une valeur de "Autorisation seule" est obligé de contenir un attribut État. Le NAS va ensuite transmettre cet attribut au serveur RADIUS dans une demande d'accès. Afin que le DAC inclut un attribut État que le serveur RADIUS va ensuite accepter, une certaine coordination entre les deux parties peut être nécessaire.

Cette coordination peut être réalisée de plusieurs façons. Le DAC peut être colocalisé avec un serveur RADIUS, et dans ce cas il est présumé avoir accès aux données nécessaires. Le serveur RADIUS peut aussi mémoriser ces informations dans une base de données commune. Le DAC peut alors être séparé du serveur RADIUS, tant qu'il a accès à cette base de données commune.

Lorsque le DAC n'est pas colocalisé avec un serveur RADIUS, et n'a pas accès à une base de données commune, le DAC DEVRAIT envoyer des paquets de demande de CoA ou demande de déconnexion à un serveur RADIUS agissant comme mandataire, plutôt que de les envoyer directement au NAS.

Un serveur RADIUS qui reçoit un paquet Demande de CoA ou Demande de déconnexion du DAC PEUT alors agir sur, ou mettre à jour, les attributs (comme d'ajouter des attributs d'identification de NAS ou de session ou d'ajouter un attribut État) avant de transmettre le paquet. Avoir des demandes de CoA/déconnexion transmises par un serveur RADIUS peut aussi permettre aux mandataires RADIUS en amont d'effectuer une vérification de transmission sur le chemin inverse (RPF) (voir au paragraphe 6.1).

3.1 État de mandataire

Si il y a des attributs État de mandataire dans une demande de déconnexion ou une demande de CoA reçue du client d'autorisation dynamique, le serveur d'autorisation dynamique DOIT inclure ces attributs État de mandataire dans ses réponses au client d'autorisation dynamique.

Un mandataire ou NAS qui transmet NE DOIT PAS modifier les attributs État de mandataire, État, ou Classe existants présents dans le paquet. Le mandataire ou NAS transmetteur DOIT traiter tous les attributs État de mandataire qui sont déjà dans le paquet comme des données opaques. Son fonctionnement NE DOIT PAS dépendre du contenu des attributs État de mandataire ajoutés par les mandataires précédents. Le mandataire transmetteur NE DOIT PAS modifier d'autres attributs État de mandataire qui étaient dans le paquet ; il peut choisir de ne pas les transmettre, mais il NE DOIT PAS changer leur contenu. Si le mandataire transmetteur omet les attributs État de mandataire dans la demande, il DOIT les joindre à la réponse avant de l'envoyer.

Quand le mandataire transmet une demande de déconnexion ou de CoA, il PEUT ajouter un attribut État de mandataire, mais il NE DOIT PAS en ajouter plus d'un. Si un attribut État de mandataire est ajouté à un paquet lors de sa transmission, l'attribut État de mandataire DOIT être ajouté après tous les attributs État de mandataire existants. Le mandataire transmetteur NE DOIT PAS changer l'ordre d'attributs du même type, incluant État de mandataire. Les autres attributs peuvent être placés avant, après, ou même entre les attributs État de mandataire.

Quand le mandataire reçoit une réponse à une demande de CoA ou une demande de déconnexion, il DOIT supprimer son propre attribut État de mandataire (le dernier État de mandataire dans le paquet) avant de transmettre la réponse. Comme les réponses Déconnexipn et CoA sont authentifiées sur le contenu entier du paquet, la suppression de l'attribut État de mandataire invalide la vérification d'intégrité, de sorte que le mandataire DOIT la recalculer.

3.2 Autorisation seule

Pour simplifier la traduction entre RADIUS et Diameter, des clients d'autorisation dynamique peuvent inclure un attribut Type de service de valeur "Autorisation seule" au sein d'une demande de CoA ; voir à la Section 4 les détails des considérations sur Diameter. La prise en charge d'une demande de CoA incluant un attribut Type de service avec la valeur "Autorisation seule" est FACULTATVE sur le NAS et le client d'autorisation dynamique. Un attribut Type de service NE DOIT PAS être inclus dans une demande de déconnexion.

Un NAS DOIT répondre à une demande de CoA incluant un attribut Type de service avec la valeur "Autorisation seule" avec un NAK de CoA ; un ACK de CoA NE DOIT PAS être envoyé. Si le NAS ne prend pas en charge une valeur de type de service de "Autorisation seule", alors il DOIT répondre avec un NAK de CoA ; un attribut Cause d'erreur d'une valeur de 405 (Service non pris en charge) DEVRAIT être inclus.

Une demande de CoA contenant un attribut Type de service de valeur "Autorisation seule" DOIT de plus contenir seulement des attributs d'identification de NAS ou de session, ainsi qu'un attribut État. Si d'autres attributs sont inclus dans une telle demande de CoA, un NAK de CoA DOIT être envoyé ; un attribut Cause d'erreur de valeur 401 (Attribut non pris en charge) DEVRAIT être inclus.

Si un paquet Demande de CoA incluant une valeur Type de service de "Autorisation seule" est traité avec succès, le NAS DOIT répondre avec un NAK de CoA contenant un attribut Type de service avec la valeur "Autorisation seule", et un attribut Cause d'erreur avec la valeur 507 (Demande initiée). Le NAS DOIT alors envoyer une demande d'accès au serveur RADIUS incluant un attribut Type de service avec la valeur "Autorisation seule", avec un attribut État. Cette demande d'accès DEVRAIT contenir les attributs d'identification de NAS provenant de la demande de CoA, ainsi que les attributs d'identification de session provenant de la demande de CoA permis dans une demande d'accès ; elle PEUT aussi contenir d'autres attributs permis dans une demande d'accès.

Comme noté au paragraphe 5.19 de la [RFC2869], un attribut Authentificateur de message DEVRAIT être inclus dans une demande d'accès qui ne contient pas d'attribut Mot de passe d'utilisateur, Mot de passe CHAP, Mot de passe ARAP, ou Message EAP. Le serveur RADIUS va alors répondre à la demande d'accès avec un Accès accepté pour (ré-)autoriser la session ou un Accès rejeté pour refuser de la (ré-)autoriser.

3.3 État

L'attribut État est disponible pour être envoyé par le client d'autorisation dynamique au NAS dans un paquet Demande de CoA et DOIT être envoyé non modifié du NAS au client d'autorisation dynamique dans un paquet ACK ou NAK suivant.

Le paragraphe 5.44 de la [RFC2865], déclare : "Une demande d’accès DOIT contenir soit un Mot-de-passe-d’utilisateur soit un Mot-de-passe-CHAP ou un État. Une demande d’accès NE DOIT PAS contenir à la fois un Mot-de-passe-d’utilisateur et un Mot-de-passe-CHAP. Si des extensions futures permettent que d’autres sortes d’informations d’authentification soient convoyées, l’attribut pour cela peut être utilisé dans une Demande-d’accès au lieu du Mot-de-passe-d’utilisateur ou du Mot-de-passe-CHAP."

Afin de satisfaire les exigences du paragraphe 5.44 de la [RFC2865], une demande d'accès avec l'attribut Type de service de valeur "Autorisation seule" DOIT contenir un attribut État.

Afin de fournir un attribut État au NAS, un client d'autorisation dynamique qui envoie une demande de CoA avec un attribut Type de service d'une valeur de "Autorisation seule" DOIT inclure un attribut État, et le NAS DOIT envoyer l'attribut État non modifié au serveur RADIUS dans la demande d'accès résultante, si il en est. Un NAS qui reçoit une demande de CoA contenant un attribut Type de service de valeur "Autorisation seule" mais sans un attribut État DOIT envoyer un NAK de CoA et DEVRAIT inclure un attribut Cause d'erreur avec la valeur de 402 (Attribut manquant).

L'attribut État est aussi disponible pour être envoyé par le client d'autorisation dynamique au NAS dans une demande de CoA qui inclut aussi un attribut Action de terminaison avec la valeur de Demande RADIUS. Si le NAS effectue l'action de terminaison par l'envoi d'une nouvelle demande d'accès à la fin de la session en cours, il DOIT inclure l'attribut État inchangé dans cette demande d'accès. Dans les deux utilisations, le serveur d'autorisation dynamique NE DOIT PAS

interpréter l'attribut localement. Un paquet Demande de CoA DOIT avoir seulement zéro ou un attribut État. L'usage de l'attribut État dépend de la mise en œuvre.

3.4 Authentificateur de message

L'attribut Authentificateur de message PEUT être utilisé pour authentifier et protéger l'intégrité des paquets Demande de CoA, ACK de CoA, NAK de CoA, Demande de déconnexion, ACK de déconnexion, et NAK de déconnexion afin d'empêcher l'usurpation d'identité.

Un serveur d'autorisation dynamique qui reçoit une demande de CoA ou une demande de déconnexion avec un attribut Authentificateur de message présent DOIT calculer la valeur correcte de l'authentificateur de message et éliminer en silence le paquet si il ne correspond pas à la valeur envoyée. Un client d'autorisation dynamique qui reçoit un ACK de CoA/déconnexion ou un NAK de CoA/déconnexion avec un attribut Authentificateur de message présent DOIT calculer la valeur correcte de l'authentificateur de message et éliminer en silence le paquet si il ne correspond pas à la valeur envoyée.

Quand un attribut Authentificateur de message est inclus dans une demande de CoA ou demande de déconnexion, il est calculé comme suit :

Authentificateur de message = HMAC-MD5 (Type, Identifiant, Longueur, Authentificateur de demande, Attributs)

Quand la vérification d'intégrité de message HMAC-MD5 est calculée, le champ Authentificateur de demande et l'attribut Authentificateur de message DOIVENT chacun être considérés comme étant de seize octets de zéros. L'attribut Authentificateur de message est calculé et inséré dans le paquet avant le calcul de l'authentificateur de demande.

Quand un attribut Authentificateur de message est inclus dans un ACK de CoA, NAK de CoA, ACK de déconnexion, ou NAK de déconnexion, il est calculé comme suit :

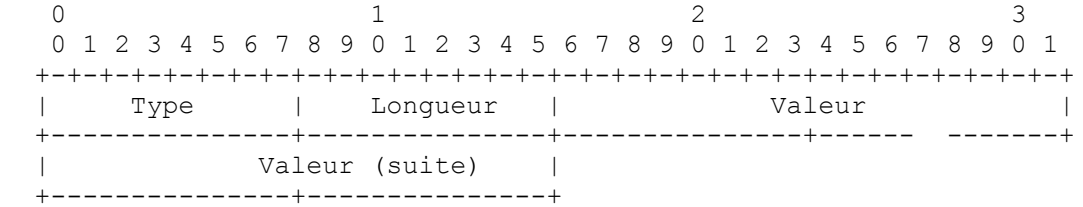
Authentificateur de message = HMAC-MD5 (Type, Identifiant, Longueur, Authentificateur de demande, Attributs)

Quand la vérification d'intégrité de message HMAC-MD5 est calculée, l'attribut Authentificateur de message DOIT être considéré comme étant de seize octets de zéros. L'authentificateur de demande est pris de la demande de CoA/déconnexion correspondante. L'authentificateur de message est calculé et inséré dans le paquet avant le calcul de l'authentificateur de réponse.

3.5 Cause d'erreur

Description : Il est possible qu'un serveur d'autorisation dynamique ne puisse pas honorer des paquets Demande de déconnexion ou Demande de CoA pour une raison quelconque. L'attribut Cause d'erreur donne plus de détails sur la cause du problème. Il PEUT être inclus dans des paquets NAK de CoA et NAK de déconnexion.

Un sommaire du format d'attribut Cause d'erreur est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 101 Cause d'erreur

Longueur : 6

Valeur : le champ Valeur fait quatre octets, contenant un entier qui spécifie la cause de l'erreur. Les valeurs 0 à 199 et 300 à 399 sont réservées. Les valeurs de 200 à 299 représentent un achèvement réussi, de sorte que ces valeurs peuvent seulement être envoyées dans des paquets ACK de CoA ou ACK de déconnexion et NE DOIVENT PAS être envoyées dans un paquet NAK de CoA ou de déconnexion. Les valeurs de 400 à 499 représentent des erreurs fatales commises par le client d'autorisation dynamique, de sorte qu'elles PEUVENT être envoyées dans des paquets CoA-NAK ou Disconnect-NAK, et NE DOIVENT PAS être envoyées dans des paquets CoA-ACK ou Disconnect-ACK. Les valeurs de 500 à 599 représentent des erreurs fatales survenant sur un serveur d'autorisation dynamique, de sorte qu'elles

PEUVENT être envoyées dans des paquets CoA-NAK et Disconnect-NAK, et NE DOIVENT PAS être envoyées dans des paquets CoA-ACK ou Disconnect-ACK. Les valeurs de cause d'erreur DEVRAIENT être enregistrées par le client d'autorisation dynamique. Les valeurs de code d'erreur (exprimées en décimal) incluent :

N°	Valeur
201	Contexte de session résiduel supprimé
202	Paquet EAP invalide (ignoré)
401	Attribut non pris en charge
402	Attribut manquant
403	Discordance d'identification de NAS
404	Demande invalide
405	Service non pris en charge
406	Extension non prise en charge
407	Valeur d'attribut invalide
501	Administrativement interdit
502	Demande non acheminable (mandataire)
503	Contexte de session non trouvé
504	Contexte de session non amovible
505	Autre erreur de traitement de mandataire
506	Ressources indisponibles
507	Demande initiée
508	Choix de plusieurs sessions non pris en charge

"Contexte de session résiduel supprimé" est envoyé en réponse à une demande de déconnexion si une ou plusieurs sessions utilisatrices ne sont plus actives, mais du contexte résiduel de session a été trouvé et bien supprimé. Cette valeur est seulement envoyée dans un ACK de déconnexion et NE DOIT PAS être envoyée dans un CoA-ACK, Disconnect-NAK, ou CoA-NAK.

"Paquet EAP invalide (ignoré)" est une erreur non fatale qui NE DOIT PAS être envoyée par les mises en œuve de la présente spécification.

"Attribut non pris en charge" est une erreur fatale envoyée si une demande contient un attribut (comme Spécifique de fabricant ou Message EAP) qui n'est pas pris en charge.

"Attribut manquant" est une erreur fatale envoyée si des attributs critiques (comme des attributs d'identification de NAS ou de session) manquent dans une demande.

"Discordance d'identification de NAS" est une erreur fatale envoyée si un ou plusieurs attributs d'identification de NAS (voir la Section 3) ne correspondent pas à l'identité du NAS qui reçoit la demande.

"Demande invalide" est une erreur fatale envoyée si un autre aspect de la demande est invalide, comme si un ou plusieurs attributs (comme des attributs Message EAP) ne sont pas formatés correctement.

"Service non pris en charge" est une erreur fatale envoyée si un attribut Type de service inclus dans la demande est envoyé avec une valeur invalide ou non prise en chare. Cette erreur ne peut pas être envoyée en réponse à une demande de déconnexion.

"Extension non prise en charge" est une erreur fatale envoyée du fait de la non prise en charge d'une extension comme des paquets Déconnexion et/ou CoA. Cela va normalement être envoyé par un mandataire qui reçoit un message ICMP Accès injoignable après avoir tenté de transmettre une demande de CoA ou demande de déconnexion au NAS.

"Valeur d'attribut invalide" est une erreur fatale envoyée si une demande de CoA ou demande de déconnexion contient un attribut avec une valeur non prise en charge.

"Administrativement interdit" est une erreur fatale envoyée si le NAS est configuré à interdire d'honorer les paquets de demande de CoA ou de demande de déconnexion pour la session spécifiée.

"Demande non acheminable" est une erreur fatale qui PEUT être envoyée par un mandataire et NE DOIT PAS être envoyée par le NAS. Elle indique que le mandataire n'a pas été capable de déterminer comment acheminer une demande de CoA ou demande de déconnexion au NAS. Par exemple, cela peut arriver si les entrées requises ne sont pas présentes dans le tableau d'acheminement de domaine du mandataire.

"Contexte de session non trouvé" est une erreur fatale envoyée si le contexte de session identifié dans la demande de CoA ou demande de déconnexion n'existe pas sur le NAS.

"Contexte de session non amovible" est une erreur fatale envoyée en réponse à une demande de déconnexion si le NAS a été capable de localiser le contexte de session, mais n'a pas pu le supprimer pour une raison quelconque. Elle NE DOIT PAS être envoyée dans un CoA-ACK, CoA-NAK, ou Disconnect-ACK, seulement dans un NAK de déconnexion.

"Autre erreur de traitement de mandataire" est une erreur fatale envoyée en réponse à une demande de CoA ou de déconnexion qui n'a pas pu être traitée par un mandataire, pour des raisons autres que d'acheminement.

"Ressources indisponibles" est une erreur fatale envoyée quand une demande de CoA ou de déconnexion n'a pas pu être honorée par manque de ressources de NAS disponibles (mémoire, mémorisation non volatile, etc.).

"Demande initiée" est une erreur fatale envoyée par un NAS en réponse à une demande de CoA incluant un attribut Type de service avec une valeur de "Autorisation seule". Elle indique que la demande de CoA n'a pas encore été honorée, mais que le NAS envoie une ou plusieurs demandes d'accès RADIUS incluant un attribut Type de service avec la valeur "Autorisation seule" au serveur RADIUS.

"Choix de plusieurs sessions non pris en charge" est une erreur fatale envoyée par un NAS en réponse à une demande de CoA ou demande de déconnexion dont les attributs d'identification de session correspondent à plusieurs sessions, alors que le NAS ne prend pas en charge les demandes s'appliquant à plusieurs sessions.

3.6 Tableau des attributs

Le tableau suivant donne des indications sur quels attributs peuvent se trouver dans quels paquets, et en quelle quantité.

Messages Changement d'autorisation :

Demande	ACK	NAK	N°	Attribut
0-1	0	0	1	Nom d'utilisateur (Note 1)
0-1	0	0	4	Adresse IP de NAS (Note 1)
0-1	0	0	5	Accès de NAS (Note 1)
0-1	0	0-1	6	Type de service
0-1	0	0	7	Protocole tramé (Note 3)
0-1	0	0	8	Adresse IP tramée (Notes 1, 6)
0-1	0	0	9	Gabarit de réseau IP tramé (Note 3)
0-1	0	0	10	Acheminement tramé (Note 3)
0+	0	0	11	Identifiant de filtre (Note 3)
0-1	0	0	12	MTU tramée (Note 3)
0+	0	0	13	Compression tramée (Note 3)
0+	0	0	14	Connexion d'hôte IP (Note 3)
0-1	0	0	15	Connexion de service (Note 3)
0-1	0	0	16	Connexion d'accès TCP (Note 3)
0+	0	0	18	Message de réponse (Note 2)
0-1	0	0	19	Numéro de rappel (Note 3)
0-1	0	0	20	Identifiant de rappel (Note 3)
0+	0	0	22	Chemin tramé (Note 3)
0-1	0	0	23	Réseau IPX tramé (Note 3)
0-1	0-1	0-1	24	État
0+	0	0	25	Classe (Note 3)
0+	0	0	26	Spécifique de fabricant (Note 7)
0-1	0	0	27	Fin de temporisation de session (Note 3)
0-1	0	0	28	Temporisation au repos (Note 3)
0-1	0	0	29	Action de terminaison (Note 3)
0-1	0	0	30	Identifiant de la station appelée (Note 1)
0-1	0	0	31	Identifiant de la station appelante (Note 1)
0-1	0	0	32	Identifiant de NAS (Note 1)
0+	0+	0+	33	État de mandataire
0-1	0	0	34	Connexion de service LAT (Note 3)
0-1	0	0	35	Connexion de nœud LAT (Note 3)
0-1	0	0	36	Connexion de groupe LAT (Note 3)

0-1	0	0	37	Liaison AppleTalk tramée (Note 3)
0+	0	0	38	Réseau AppleTalk tramé (Note 3)
0-1	0	0	39	Zone AppleTalk tramée (Note 3)
0-1	0	0	44	Identifiant de session comptable (Note 1)
0-1	0	0	50	Identifiant multi sessions comptables (Note 1)
0-1	0-1	0-1	55	Horodatage d'événement
0+	0	0	56	Identifiant de VLAN de sortie (Note 3)
0-1	0	0	57	Filtres d'entrée (Note 3)
0+	0	0	58	Nom de VLAN de sortie (Note 3)
0-1	0	0	59	Tableau de priorité d'utilisateur (Note 3)
0-1	0	0	61	Type d'accès de NAS (Note 3)
0-1	0	0	62	Limite d'accès (Note 3)
0-1	0	0	63	Connexion d'accès de LAT (Note 3)
0+	0	0	64	Type de tunnel (Note 5)
0+	0	0	65	Type de support de tunnel (Note 5)
0+	0	0	66	Point d'extrémité de client de tunnel (Note 5)
0+	0	0	67	Point d'extrémité de serveur de tunnel (Note 5)
0+	0	0	69	Mot de passe de tunnel (Note 5)
0-1	0	0	71	Caractéristiques ARAP (Note 3)
0-1	0	0	72	Accès de zone ARAP (Note 3)
0+	0	0	78	Jeton de configuration (Note 3)
0+	0-1	0	79	Message EAP (Note 2)
0-1	0-1	0-1	80	Authentificateur de message
0+	0	0	81	Identifiant de tunnel de groupe privé (Note 5)
0+	0	0	82	Identifiant d'allocation de tunnel (Note 5)
0+	0	0	83	Préférence de tunnel (Note 5)
0-1	0	0	85	Intervalle comptable intermédiaire (Note 3)
0-1	0	0	87	Identifiant d'accès de NAS (Note 1)
0-1	0	0	88	Réservoir tramé (Note 3)
0-1	0	0	89	Identité d'utilisateur facturable (Note 1)
0+	0	0	90	Identifiant d'autorisation de client de tunnel (Note 5)
0+	0	0	91	Identifiant d'autorisation de serveur de tunnel (Note 5)
0-1	0	0	92	Règle de filtre de NAS (Note 3)
0	0	0	94	Informations sur la ligne d'origine
0-1	0	0	95	Adresse IPv6 de NAS (Note 1)
0-1	0	0	96	Identifiant d'interface tramée (Notes 1, 6)
0+	0	0	97	Préfixe IPv6 tramé (Notes 1, 6)
0+	0	0	98	Connexion d'hote IPv6 (Note 3)
0+	0	0	99	Chemin IPv6 tramé (Note 3)
0-1	0	0	100	Réservoir IPv6 tramé (Note 3)
0	0	0+	101	Cause d'erreur
0+	0	0	123	Préfixe IPv6 délégué (Note 3)

Messages Déconnexion :

Demande	**ACK**	**NAK**	**N°**	**Attribut**
0-1	0	0	1	Nom d'utilisateur (Note 1)
0-1	0	0	4	Adresse IP de NAS (Note 1)
0-1	0	0	5	Accès de NAS (Note 1)
0	0	0	6	Type de service
0	0	0	8	Adresse IP tramée (Note 1)
0+	0	0	18	Message de réponse (Note 2)
0	0	0	24	État
0+	0	0	25	Classe (Note 4)
0+	0	0	26	Spécifique du fabricant (Note 7)
0-1	0	0	30	Identifiant de station appelée (Note 1)
0-1	0	0	31	Identifiant de station appelante (Note 1)
0-1	0	0	32	Identifiant de NAS (Note 1)
0+	0+	0+	33	État de mandataire
0-1	0	0	44	Identifiant de session de comptabilité (Note 1)
0-1	0-1	0	49	Cause de terminaison de comptabilité
0-1	0	0	50	Identifiant multi sessions comptables (Note 1)

0-1	0-1	0-1	55	Horodatage d'événement
0	0	0	61	Type d'accès de NAS
0+	0-1	0	79	Message EAP (Note 2)
0-1	0-1	0-1	80	Authentificateur de message
0-1	0	0	87	Identifiant d'accès de NAS (Note 1)
0-1	0	0	89	Identité d'utilisateur facturable (Note 1)
0-1	0	0	95	Adresse IPv6 de NAS (Note 1)
0	0	0	96	Identifiant d'interface tramée (Note 1)
0	0	0	97	Préfixe IPv6 tramé (Note 1)
0	0	0+	101	Cause d'erreur

La signification des entrées des tableaux ci-dessus est définie comme suit :
0 : cet attribut NE DOIT PAS être présent dans le paquet.
0+ : zéro, une, ou plusieurs instances de cet attribut PEUVENT être présentes dans le paquet.
0-1 : zéro ou une instance de cet attribut PEUT être présente dans le paquet.
1 : exactement une instance de cet attribut DOIT être présente dans le paquet.

Note 1 : Lorsque le NAS ou les attributs d'identification de session sont inclus dans les paquets de demande de déconnexion ou de demande de CoA, ils sont utilisés seulement pour l'identification. Ces attributs NE DOIVENT PAS être utilisés pour d'autre objet que l'identification (par exemple, dans les paquets de demande de CoA pour demander des changements d'autorisation).

Note 2 : l'attribut Message de réponse est utilisé pour présenter un message affichable à l'utilisateur. Le message est seulement affiché par suite de la réussite d'une demande de déconnexion ou de CoA (où un ACK de déconnexion ou ACK de CoA est ensuite envoyé). Lorsque le protocole extensible d'authentification (EAP, *Extension Authentication Protocol*) est utilisé pour l'authentification, un attribut Message EAP/Demande de notification est envoyé à la place, et les paquets ACK de déconnexion ou ACK de CoA contiennent un attribut Message EAP/Réponse de notification.

Note 3 : Quand ils sont inclus dans une demande de CoA, ces attributs représentent une demande de changement d'autorisation. Quand un de ces attributs est omis d'une demande de CoA, le NAS suppose que la valeur de l'attribut doit rester inchangée. Les attributs inclus dans une demande de CoA remplacent toutes les valeurs existantes du ou des mêmes attributs.

Note 4 : Quand il est inclus dans une demande de déconnexion réussie (où un ACK de déconnexion est ensuite envoyé) l'attribut Classe DEVRAIT être envoyé non modifié par le NAS au serveur de comptabilité RADIUS dans le paquet Arrêt de comptabilité. Si la demande de déconnexion ne réussit pas, l'attribut Classe n'est alors pas traité.

Note 5 : Quand ils sont inclus dans une demande de CoA, ces attributs représentent une demande de changement d'autorisation. Lorsque des attributs de tunnel sont inclus dans une demande de CoA réussie, tous les attributs de tunnel existants sont supprimés et remplacés par le ou les nouveaux attributs.

Note 6 : Comme les attributs Adresse IP tramée, Préfixe IPv6 tramé, et Identifiant d'interface tramé sont utilisés pour l'identification de session, le renumérotage ne peut pas être accompli en incluant les valeurs de ces attributs dans une demande de CoA. On envoie plutôt une demande de CoA incluant un attribut Type de service avec une valeur de "Autorisation seule" ; des nouvelles valeurs peuvent être fournies dans un Accès accepté envoyé en réponse à la demande d'accès qui suit. Noter que le renumérotage ne va pas être possible dans toutes les situations. Par exemple, afin de changer un adresse IP, une re-négociation IPCP ou IPv6CP pourrait être requise, qui n'est pas prise en charge par toutes les mises en œuvre de PPP.

Note 7 : Dans les paquets de demande de déconnexion, des attributs spécifiques de fabricant (VSA, *Vendor-Specific Attribute*) PEUVENT être utilisés pour l'identification de session. Dans les paquets de demande de CoA, des VSA PEUVENT être utilisés pour l'identification de session ou le changement d'autorisation. Cependant, le même Attribut NE DOIT PAS être utilisé pour les deux objets simultanément.

4. Considérations sur Diameter

Du fait des différences de traitement des demandes de changement d'autorisation dans RADIUS et dans Diameter, il peut être difficile ou impossible à une passerelle Diameter/RADIUS de réussir à traduire une demande de ré-autorisation (RAR, *Re-Auth-Request*) Diameter en demande de CoA et vice versa. Par exemple, comme une demande de CoA initie seulement

un changement d'autorisation mais n'initie pas de ré-authentification, une commande RAR contenant une AVP Type de demande de ré-authentification de valeur "AUTHORIZE_AUTHENTICATE" ne peut pas être directement traduite en une demande de CoA. Une passerelle Diameter/RADIUS qui reçoit une demande de CoA contenant des changements d'autorisation va avoir besoin de la traduire en deux échanges Diameter. D'abord, la passerelle Diameter/RADIUS va produire une commande RAR incluant une AVP Identifiant de session et une AVP Type de demande de ré-authentification de valeur "AUTHORIZE ONLY". Ensuite la passerelle Diameter/RADIUS va répondre à la demande d'accès qui s'ensuit avec une réponse incluant les attributs d'autorisation trouvés dans la demande de CoA. Pour permettre la traduction, la demande de CoA DEVRAIT inclure un attribut Identifiant de session comptable. Si le client Diameter utilise le même identifiant de session pour l'autorisation et la comptabilité, la passerelle Diameter/RADIUS peut alors copier le contenu de l'attribut Identifiant de session comptable dans l'AVP Identifiant de session ; autrement, elle va devoir transposer la valeur de l'identifiant de session comptable en un identifiant de session équivalent à utiliser dans une commande RAR.

Lorsque un attribut Identifiant de session comptable n'est pas présent dans une demande de CoA ou demande de déconnexion, une passerelle Diameter/RADIUS va soit devoir déterminer l'identifiant de session comptable approprié, soit, si elle ne peut pas le faire, envoyer un NAK de CoA ou NAK de déconnexion en réponse, éventuellement en incluant un attribut Cause d'erreur de valeur 508 (Choix de multiples sessions non pris en charge).

Pour simplifier la traduction entre RADIUS et Diameter, les clients d'autorisation dynamique peuvent inclure un attribut Type de service avec la valeur "Autorisation seule" dans une demande de CoA, comme décrit au paragraphe 3.2. Une passerelle Diameter/RADIUS qui reçoit une demande de CoA contenant un attribut Type de service de valeur "Autorisation seule" la traduit en une RAR avec l'AVP Type de demande de réauthentification de valeur "AUTHORIZE ONLY". Le RAA reçu est alors traduit en un NAK de CoA avec un attribut Type de service de valeur "Autorisation seule". Si l'AVP Code de résultat dans le RAA a une valeur dans la catégorie succès, alors un attribut Cause d'erreur de valeur "Demande initiée" est inclus dans le NAK de CoA. Si l'AVP Code de résultat dans le RAA a une valeur indiquant une erreur de protocole ou une défaillance transitoire ou permanente, alors un autre attribut Cause d'erreur est retourné comme suggéré ci-dessous.

Dans Diameter, un serveur peut demander qu'une session soit interrompue par l'envoi d'une demande d'interruption de session (ASR, *Abort-Session-Request*) identifiant la session à terminer avec les AVP Identifiant de session et Nom d'utilisateur. La commande ASR est traduite en une demande de déconnexion contenant les attributs Identifiant de session comptable et Nom d'utilisateur. Si le client Diameter utilise le même identifiant de session dans l'autorisation et la comptabilité, alors la valeur de l'AVP Identifiant de session peut être placée dans l'attribut Identifiant de session comptable ; autrement, la valeur de l'AVP Identifiant de session n'aura pas besoin d'être transposée en un attribut Identifiant de session comptable approprié. Pour permettre la traduction d'une demande de déconnexion en une ASR, un attribut Identifiant de session comptable DEVRAIT être présent.

Si le client Diameter utilise le même identifiant de session dans l'autorisation et la comptabilité, alors la valeur de l'attribut Identifiant de session comptable peut être placé dans l'AVP Identifiant de session au sein de l'ASR ; autrement, la valeur de l'attribut Identifiant de session comptable va devoir être transposée en une AVP Identifiant de session appropriée.

Une commande de réponse à l'interruption de session (ASA, *Abort-Session-Answer*) est envoyée en réponse à une commande ASR afin d'indiquer que la demande a été traitée. Une passerelle Diameter/RADIUS qui reçoit un ACK de déconnexion le traduit en une commande ASA avec une AVP Code de résultat de "DIAMETER_SUCCESS". Un NAK de déconnexion reçu du NAS est traduit en une commande ASA avec une AVP Code de résultat qui dépend de la valeur de l'attribut Cause d'erreur. Les traductions suggérées entre les valeurs d'attribut Cause d'erreur et les valeurs d'AVP Code de résultat sont incluses ci-dessous :

N°	**Valeur de l'attribut Cause d'erreur**	**AVP Code de résultat**
201	Contexte de session résiduel supprimé	DIAMETER_SUCCESS
202	Paquet EAP invalide (ignoré)	DIAMETER_LIMITED_SUCCESS
401	Attribut non pris en charge	DIAMETER_AVP_UNSUPPORTED
402	Attribut manquant	DIAMETER_MISSING_AVP
403	Discordance d'identification de NAS	DIAMETER_REALM_NOT_SERVED
404	Demande invalide	DIAMETER_UNABLE_TO_COMPLY
405	Service non pris en charge	DIAMETER_COMMAND_UNSUPPORTED
406	Extension non prise en charge	DIAMETER_APPLICATION_UNSUPPORTED
407	Valeur d'attribute invalide	DIAMETER_INVALID_AVP_VALUE
501	Administrativement interdit	DIAMETER_AUTHORIZATION_REJECTED
502	Demande non acheminable (mandataire)	DIAMETER_UNABLE_TO_DELIVER
503	Contexte de session non trouvé	DIAMETER_UNKNOWN_SESSION_ID
504	Contexte de session non amovible	DIAMETER_AUTHORIZATION_REJECTED
505	Autre erreur de traitement de mandataire	DIAMETER_UNABLE_TO_COMPLY

506	Ressources indisponibles	DIAMETER_RESOURCES_EXCEEDED
507	Demande initiée	DIAMETER_SUCCESS

Comme les deux échanges ASR/ASA et demande de déconnexion/NAK/ACK de déconnexion impliquent juste une demande et une réponse, l'inclusion d'un type de service "Autorisation seule" dans une demande de déconnexion n'est pas nécessaire pour aider la traduction Diameter/RADIUS, et peut rendre la traduction plus difficile. Par suite, comme noté au paragraphe 3.2, l'attribut Type de service NE DOIT PAS être utilisé dans une demande de déconnexion.

5. Considérations relatives à l'IANA

Le présent document utilise l'espace de noms de RADIUS [RFC2865] ; voir <http://www.iana.org/assignments/radius-types>. En plus des allocations déjà faites dans les [RFC3575] et [RFC3576], la présente spécification alloue des valeurs supplémentaires de l'attribut Cause d'erreur (101) :

N°	**Valeur**
407	Valeur d'attribut invalide
508	Choix de plusieurs sessions non pris en charge

6. Considérations sur la sécurité

6.1 Questions d'autorisation

Lorsque un NAS est partagé par plusieurs fournisseurs, il n'est pas souhaitable qu'un fournisseur soit capable d'envoyer des demandes de déconnexion ou des demandes de CoA affectant les sessions d'un autre fournisseur.

Un serveur d'autorisation dynamique DOIT éliminer en silence les paquets de demande de déconnexion ou de demande de CoA provenant de sources non sûres. Dans les situations où le client d'autorisation dynamique est co-résident avec un serveur d'authentification ou de comptabilité RADIUS, un mandataire PEUT effectuer une vérification de "transmission sur le chemin inverse" (RPF) pour vérifier qu'une demande de déconnexion ou demande de CoA a bien pour origine un client d'autorisation dynamique autorisé. De plus, il DEVRAIT être possible d'autoriser explicitement des sources supplémentaires de paquets de demande de déconnexion ou de demande de CoA relatifs à certaines classes de sessions. Par exemple, une source particulière peut être explicitement autorisée à envoyer des paquets de demande de CoA relatifs à des utilisateurs au sein d'un ensemble de domaines.

Pour effectuer la vérification de RPF, le serveur d'autorisation dynamique utilise les attributs d'identification de session inclus dans les paquets de demande de déconnexion ou de demande de CoA, afin de déterminer le ou les serveurs RADIUS auxquels une demande d'accès équivalente pourrait être acheminée. Si l'adresse de source de la demande de déconnexion ou demande de CoA est dans cet ensemble, la demande de CoA ou demande de déconnexion est alors transmise ; sinon, elle DOIT être éliminée en silence.

Normalement, le serveur d'autorisation dynamique va extraire le domaine de l'identifiant d'accès reseau [RFC4282] inclus dans l'attribut Nom d'utilisateur ou Identité d'utilisateur facturable, et déterminer les serveurs RADIUS correspondants dans les tableaux d'acheminement du domaine. Si le serveur d'autorisation dynamique conserve à long terme l'état de session, il PEUT effectuer la vérification d'autorisation sur la base des attributs d'identification de session dans la demande de CoA. Les attributs d'identification de session peuvent être utilisés pour lier une session à un mandataire ou ensemble de mandataires particuliers, comme avec le domaine NAI.

Lorsque aucun mandataire n'est présent, la vérification de RPF peut seulement être effectuée par le NAS si il tient son propre tableau d'acheminement de domaine. Si le NAS ne tient pas de tableau d'acheminement de domaine (par exemple, il choisit les mandataires de transmission sur la base de la configuration primaire/secondaire et/ou des vérifications de vie) alors une vérification de RPF ne peut pas être effectuée.

Comme l'autorisation d'envoyer une demande de déconnexion ou demande de CoA est déterminée sur la base de l'adresse de source et du secret partagé correspondant, le serveur d'autorisation dynamique DEVRAIT configurer un secret partagé différent pour chaque client d'autorisation dynamique.

6.2 Lignes directrices sur l'utilisation de IPsec

En plus des vulnérabilités pour la sécurité spécifiques des paquets de déconnexion ou de CoA, les échanges de protocole décrits dans ce document sont susceptibles des mêmes vulnérabilités que RADIUS [RFC2865]. Il est RECOMMANDÉ que IPsec soit employé pour permettre un meilleure sécurité, en utilisant le profil décrit au paragraphe 4.2 de la [RFC3579].

Pour les serveurs d'autorisation dynamique qui mettent en œuvre la présente spécification, la politique IPsec serait "IPsec exigé, de tous à moi, accès UDP de destination 3799". Cela fait que le serveur d'autorisation dynamique exige l'utilisation de IPsec. Si certains client d'autorisation dynamique ne prennent pas en charge IPsec, une politique de granularité plus fine va être exigée : "IPsec exigé, de DAC à capacité IPsec à moi".

Pour les clients d'autorisation dynamique qui mettent en œuvre la présente spécification, la politique IPsec serait "Initier IPsec, de moi à tous, accès de destination UDP 3799". Cela fait que le client d'autorisation dynamique initie IPsec quand il envoie du trafic d'autorisation dynamique à tout serveur d'autorisation dynamique. Si certains serveurs d'autorisation dynamique contactés par le client d'autorisation dynamique ne prennent pas en charge IPsec, une politique de granularité plus fine va être exigée, telle que "Initier IPsec, de moi à un DAS à capacité IPsec, accès de destination UDP 3799".

6.3 Protection contre la répétition

Lorsque la protection contre la répétition d'IPsec n'est pas utilisée, un attribut Horodatage d'événement (55) [RFC2869] DEVRAIT être inclus dans les paquets de demande de CoA et de demande de déconnexion, et PEUT être inclus dans les paquets ACK de CoA, NAKde CoA, ACK de déconnexion, et NAK de déconnexion.

Quand l'attribut Horodatage d'événement est présent, le serveur d'autorisation dynamique et le client d'autorisation dynamique DOIVENT tous deux vérifier que l'attribut Horodatage d'événement est actuel dans une fenêtre temporelle acceptable. Si l'attribut Horodatage d'événement n'est pas actuel, le paquet DOIT alors être éliminé en silence. Cela implique le besoin d'une synchronisation lâche au sein du réseau, qui peut être réalisée par divers moyens, incluant le protocole simple de l'heure du réseau (SNTP, *Simple Network Time Protocol*) comme décrit dans la [RFC4330]. Les mises en œuvre DEVRAIENT être configurables à éliminer les paquets de demande de CoA ou de demande de déconnexion qui ne contiennent pas un attribut Horodatage d'événement.

Si l'attribut Horodatage d'événement est inclus, il représente l'heure à laquelle le paquet d'origine a été envoyé, et donc, il NE DEVRAIT PAS être mis à jour quand le paquet est retransmis. Si l'attribut Horodatage d'événement n'est pas mis à journ, cela implique que l'identifiant n'est pas changé dans les paquets retransmis. Par suite, la capacité de détecter des répétitions dans le fenêtre temporelle va dépendre de la prise en charge de la détection de dupliqués dans cette même fenêtre. Comme noté au paragraphe 2.3, la détection de dupliqués est EXIGÉE pour les serveurs d'autorisation dynamique qui mettent en œuvre la présente spécification.

La fenêtre de temps utilisée pour la détection de dupliqués DOIT être la même que la fenêtre utilisée pour détecter un attribut Horodatage d'événement périmé. Comme l'identifiant RADIUS ne peut pas être répété dans la fenêtre de temps choisie, pas plus de 256 demandes ne peuvent être acceptées dans la fenêtre de temps. Par suite, la fenêtre de temps choisie va dépendre du volume maximum de demande de CoA/déconnexion attendu, afin que des éliminations inutiles puissent être évitées. Une fenêtre de temps par défaut de 300 secondes devrait être adéquate dans de nombreuses circonstances.

7. Exemple de traces

Demande de déconnexion avec nom d'utilisateur :

```
0: xxxx xxxx xxxx xxxx xxxx 2801 001c 1b23    .B.....$.-(....#
16: 624c 3543 ceba 55f1 be55 a714 ca5e 0108    bL5C..U..U...^..
32: 6d63 6869 6261
```

Demande de déconnexion avec Identifiant de session comptable :

```
0: xxxx xxxx xxxx xxxx xxxx 2801 001e ad0d    .B..... ~.(.....
16: 8e53 55b6 bd02 a0cb ace6 4e38 77bd 2c0a    .SU.......N8w.,.
32: 3930 3233 3435 3637                       90234567
```

Demande de déconnexion avec Adresse IP tramée :

```
0: xxxx xxxx xxxx xxxx xxxx 2801 001a 0bda    .B....."2.(.....
```

16: 33fe 765b 05f0 fd9c c32a 2f6b 5182 0806 3.v[.....*/kQ...
32: 0a00 0203

8. Références

8.1 Références normatives

[RFC1321] R. Rivest, "Algorithme de résumé de message MD5", avril 1992. *(Information)*

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

[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.)*

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

[RFC2869] C. Rigney, W. Willats, P. Calhoun, "Extensions à RADIUS", juin 2000. (*MàJ par* RFC3579, RFC5080) *(Information)*

[RFC3162] B. Aboba, G. Zorn, D. Mitton, "RADIUS et IPv6", août 2001. *(P.S. ; MàJ par* RFC8044)

[RFC3575] B. Aboba, "Considérations relatives à l'IANA pour le service d'authentification distante d'utilisateur appelant (RADIUS)", juillet 2003. (*MàJ* RFC2865) *(P.S.)*

[RFC3579] B. Aboba, P. Calhoun, "Prise en charge du protocole d'authentification extensible (EAP) par RADIUS", septembre 2003. (*MàJ par* RFC5080) *(Information)*

[RFC4282] B. Aboba et autres, "L'identifiant d'accès réseau", décembre 2005. *(P.S., Remplacée par* RFC7542)

8.2 Références pour information

[MD5Attack] Dobbertin, H., "The Status of MD5 After a Recent Attack", CryptoBytes Vol.2 No.2, Summer 1996.

[RFC2868] G. Zorn et autres, "Attributs RADIUS pour la prise en charge du protocole de tunnel", juin 2000. *(Info.)*

[RFC3539] B. Aboba, J. Wood, "Profil de transport d'authentification, d'autorisation et de comptabilité (AAA)", juin 2003. *(P.S.)*

[RFC3576] M. Chiba et autres, "Extensions d'autorisation dynamique au service d'authentification distante d'utilisateur appelant (RADIUS)", juillet 2003. (*Obsolète, voir* RFC5176) *(Information)*

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

[RFC4330] D. Mills, "Version 4 du protocole simple de l'heure du réseau (SNTP) pour IPv4, IPv6 et OSI", janvier 2006. (*Remplace* RFC2030, RFC1769) *(Information) (Remplacée par* RFC5905)

[RFC4372] F. Adrangi et autres, "Identité de l'utilisateur facturé", janvier 2006. *(P.S.)*

[RFC4675] P. Congdon et autres, "Attributs RADIUS pour LAN virtuel et prise en charge de priorité", septembre 2006. *(P.S.)*

[RFC4818] J. Salowey, R. Droms, "Attribut de préfixe IPv6 délégué pour RADIUS", avril 2007. *(P.S.)*

[RFC4849] P. Congdon et autres, "Attribut RADIUS de règle de filtre", avril 2007. *(P.S.)*

9. Remerciements

Ce protocole a d'abord été développé et distribué par Ascend Communications. Un exemple de code a été distribué gratuitement sur le modèle de serveur.

Les auteurs tiennent à remercier de leurs précieuses suggestions et retours Avi Lior, Randy Bush, Steve Bellovin, Glen Zorn, Mark Jones, Claudio Lapidus, Anurag Batta, Kuntal Chowdhury, Tim Moore, Russ Housley, Joe Salowey, Alan DeKok, et David Nelson.

Appendice A. Changements par rapport à la RFC 3576

Cet Appendice fait la liste des changements majeurs entre la [RFC3576] et le présent document. Les changements mineurs, incluant de style, de grammaire, d'orthographe, et rédactionnels, ne sont pas mentionnés.

- Le terme "client d'autorisation dynamique" est utilisé à la place de "serveur RADIUS" lorsque il s'applique à l'origine des paquets de demande de CoA et de demande de déconnexion. Le terme de "serveur d'autorisation dynamique" est utilisé à la place de "NAS" lorsque il s'applique au receveur des paquets de demande de CoA et de demande de déconnexion. La définition de ces termes a été ajoutée (paragraphe 1.3).

- Ajout de l'exigence de la détection de dupliqués sur le serveur d'autorisation dynamique (paragraphe 2.3).

- Précisé le comportement attendu quand les attributs d'identification de session correspondent à plus d'une session (paragraphes 2.3, 3, 3.5, et Section 4).

- Ajout de Identité d'utilisateur facturable comme attribut d'identification de session. Retrait de NAS-Port-Type comme attribut d'identification de session (Section 3).

- Ajout de la recommandation qu'un attribut Identifiant de session comptable ou Identifiant multi sessions comptables soit inclus dans une demande d'accès (Section 3).

- Ajout d'une discussion des scénarios dans lesquels le "client d'autorisation dynamique" et le serveur RADIUS ne sont pas colocalisés (Section 3).

- Ajout de détails relatifs au traitement de l'état Attribut de mandataire (paragraphe 3.1).

- Ajout de la précision que la prise en charge d'un attribut Type de service avec la valeur "Autorisation seule" est facultative sur le NAS et le client d'autorisation dynamique (paragraphe 3.2). L'utilisation de l'attribut Type de service dans une demande de déconnexion est interdite (paragraphes 3.2, 3.6).

- Ajout de l'exigence de l'inclusion de l'attribut État dans les paquets de demande de CoA qui incluent un attribut Type de service avec une valeur de "Autorisation seule" (paragraphe 3.3).

- Ajout de précisions sur le calcul de l'attribut Authentificateur de message (paragraphe 3.4).

- Des valeurs supplémentaires d'attribut Cause d'erreur sont allouées pour la valeur Attribut invalide (407) et Choix de plusieurs sessions non pris en charge (508) (paragraphe 3.5, Section 4).

- Mise à jour du tableau de l'attribut Demande de CoA pour inclure les attributs Règle de filtre, Préfixe IPv6 délégué, VLANID de sortie, Filtres d'entrée, Nom de VLAN de sortie, et Priorité d'utilisateur (paragraphe 3.6).

- Ajout de l'attribut Identité de l'utilisateur facturable au tableau d'attribut de demande de CoA et demande de déconnexion (paragraphe 3.6).

- L'utilisation des attributs Spécifique de fabricant (VSA) pour l'identification de session et le changement d'autorisation a été précisée (paragraphe 3.6).

- Ajout de la Note 6 sur l'utilisation de la demande de CoA pour la renumérotation, et de la Note 7 sur l'utilisation des attributs Spécifique de fabricant (paragraphe 3.6).

- Ajout des Considérations sur Diameter (Section 4).

- L'attribut Horodatage d'événement ne devrait pas être recalculé à la retransmission. Les implications pour la répétition et la détection de dupliqués sont discutées (paragraphe 6.3).

- Le fonctionnement de la vérification de transmission sur le chemin inverse (RPF, *Reverse Path Forwarding*) a été précisé. L'utilisation de la vérification de RPF est facultative plutôt que recommandée par défaut (paragraphe 6.1).

- Le texte sur l'usurpation d'identité (inclus au paragraphe 4.3.7 de la [RFC3579]) et le fonctionnement de IPsec (inclus au paragraphe 4.2 de la [RFC3579]) a été supprimé, et est maintenant référencé.

Adresse des auteurs

Murtaza Chiba
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose CA, 95134
mél : mchiba@cisco.com
téléphone : +1 408 525 7198

Gopal Dommety
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134
mél : gdommety@cisco.com
téléphone : +1 408 525 1404

Mark Eklund
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134
mél : meklund@cisco.com
téléphone : +1 865 671 6255

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
mél : bernarda@microsoft.com
téléphone : +1 425 706 6605

David Mitton
RSA, Security Division of EMC
174 Middlesex Turnpike
Bedford, MA 01730
mél : david@mitton.com

Déclaration complète de droits de reproduction