Groupe de travail Réseau
Request for Comments : 5080
RFC mises à jour : 2865, 2866, 2869, 3579
Catégorie : Sur la voie de la normalisation

D. Nelson, Elbrys Networks, Inc
A. DeKok, FreeRADIUS
décembre 2007
Traduction Claude Brière de L'Isle

Problèmes de mise en œuvre courants du service d'authentification distante d'utilisateur appelant (RADIUS) et solutions suggérées

Résumé
Le présent document décrit les problèmes courants vus dans les mises en œuvre du service d'authentification distante d'utilisateur appelant (RADIUS, *Remote Authentication Dial In User Service*) et suggère des correctifs. Lorsque applicable, les ambiguïtés et les erreurs des spécifications précédentes de RADIUS sont corrigées.

Table des Matières

1. Introduction

Ces dernières années ont vu une augmentation du déploiement de clients et serveurs RADIUS. Le présent document décrit les problèmes courants vus dans les mises en œuvre de RADIUS et suggère des correctifs. Lorsque applicable, les ambiguïtés et erreurs des précédentes spécifications RADIUS sont corrigées.

1.1 Terminologie

Le présent document utilise les termes suivants :

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

"authentificateur" dans la terminologie de IEEE 802.1X ou du protocole d'authentification extensible (EAP, *Extensible Authentication Protocol*) ou client RADIUS.

Service : le NAS fournit un service à l'utilisateur, tel qu'un accès réseau via le protocole 802.11 ou point à point (PPP).

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

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

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].

2. Problèmes

2.1 Définition de session

2.1.1 Attribut State

Concernant l'attribut State, le paragraphe 5.24 de la [RFC2865] déclare : "Cet attribut est disponible pour être envoyé par le serveur au client dans un Access-Challenge *(défi d'accès)* et DOIT être envoyé sans modification du client au serveur dans la nouvelle réponse à la demande d'accès à ce défi, si il en est."

Cet attribut est disponible pour être envoyé par le serveur au client dans un Access-Accept *(accès accepté)* 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 terminaison de la session en cours, il DOIT inclure l'attribut State inchangé dans cette demande d'accès.

Ceraines mises en œuvre de client RADIUS n'utilisent pas de façon appropriée l'attribut State afin de distinguer un processus redémarré d'authentification EAP de la continuation d'un processus en cours (par le même utilisateur sur le même NAS et accès). Lorsque un attribut EAP-Message est inclus dans un attribut Défi d'accès ou Accès accepté, les serveurs RADIUS DEVRAIENT aussi inclure un attribut State. Voir au paragraphe 2.1.2 le complément de l'identifiant de demande pour les avantages supplémentaires de l'utilisation de l'attribut State de cette façon.

Comme défini au Tableau 5.44 de la [RFC2865], les paquets Demande d'accès peuvent contenir un attribut State. Le tableau ne qualifie pas cette déclaration tandis que le texte du paragraphe 5.24 (cité ci-dessus) ajoute d'autres exigences non spécifiées dans ce tableau.

On étend les exigences de la [RFC2865] pour dire que les demandes d'accès qui font partie d'un processus en cours d'authentification Demande d'accès/Défi d'accès DEVRAIENT contenir un attribut State. Il est de la responsabilité du serveur, d'envoyer un attribut State dans un paquet Défi d'accès, si ce serveur a besoin d'un attribut State dans une demande d'accès suivante pour lier ensemble plusieurs demandes d'accès dans une session d'authentification. Comme défini au paragraphe 5. 24 de la [RFC2865], l'état DOIT être envoyé non modifié du client au serveur dans la nouvelle réponse Demande d'accès à ce défi, si il en est.

Alors que la plupart des mises en œuvre de serveur exigent la présence d'un attribut State dans un paquet Défi d'accès, certains systèmes de défi-réponse peuvent distinguer la demande initiale de la réponse au défi sans utiliser un attribut State pour suivre une session d'authentification. Les paquets Défi d'accès et les paquets Demande d'accès suivants pour ces systèmes n'ont pas besoin de contenir un attribut State.

D'autres mécanismes d'authentification ont besoin de lier une séquence de paquets Demande d'accès/Défi d'accès ensemble dans une session d'authentification en cours. Les serveurs qui mettent en œuvre ces mécanismes d'authentification

DEVRAIENT inclure un attribut State dans les paquets Défi d'accès.

En général, si le processus d'authentification implique une ou plusieurs séquences Demande d'accès/Défi d'accès, l'attribut State DEVRAIT être envoyé par le serveur dans les paquets Défi d'accès. Utiliser l'attribut State pour créer une session multi-paquets est aujourd'hui la méthode la plus simple disponible dans RADIUS. Alors que d'autres méthodes pour créer des sessions multi-paquets sont possibles (par exemple, [RFC3579] paragraphe 2.6.1) ces méthodes ne sont PAS RECOMMANDÉES.

Les seules valeurs permises pour un attribut State sont celles fournies dans un paquet Accès accepté, Défi d'accès, Demande de CoA ou Demande de déconnexion. Un client RADIUS DOIT utiliser seulement ces valeurs pour l'attribut State qu'il a précédemment reçues d'un serveur. Une Demande d'accès envoyée par suite d'un processus d'authentification nouveau ou redémarré NE DOIT PAS inclure l'attribut State, même si un attribut State a été précédemment reçu dans un Défi d'accès pour le même utilisateur et accès.

Les paquets Demande d'accès qui contiennent un attribut Type de service avec la valeur Autoriser seulement (17) DOIVENT contenir un attribut State. Les paquets Demande d'accès qui contiennent un attribut Type de service avec la valeur de Vérification d'appel (10) NE DEVRAIENT PAS contenir d'attribut State. Tout autre paquet Demande d'accès qui effectue des vérifications d'autorisation DOIT contenir un attribut State. Cette dernière exigence signifie souvent qu'un Accès accepté doit contenir un attribut State, qui peut alors être utilisé dans une demande d'accès ultérieure qui effectue les vérifications d'autorisation.

Le cas d'utilisation standard pour Call Check est une pré authentification fondée seulement sur les informations d'identifiant de point d'extrémité, comme un numéro de téléphone ou une adresse de contrôle d'accès au support (MAC, *Media Access Control*) dans l'identidiant de station appelante et facultativement l'identifiant de station appelée. Dans ce cas d'utilisation, le NAS n'a pas de moyen d'obtenir un attribut State convenable à inclure dans une demande d'accès. D'autres utilisations non standard de Call Check peuvent exiger ou permettre l'utilisation d'un attribut State, mais sortent du domaine d'application du présent document.

Dans une demande d'accès avec un attribut Type de service de valeur Call Check, il est NON RECOMMANDÉ que les attributs User-Name et User-Password contiennent les mêmes valeurs (par exemple, une adresse MAC). Mettre en œuvre la vérification d'adresse MAC sans utiliser un type de service de Call Check est NON RECOMMANDÉ. Cette pratique donne à un attaquant à la fois le texte en clair et le texte chiffiré du champ User-Password, ce qui permet de nombreuses attaques contre la sécurité du protocole RADIUS. Par exemple, si l'authentifiant de demande ne satisfait pas les exigences de la [RFC2865] d'unicité globale et temporelle, la pratiquce décrite ci-dessus peut conduire à la compromission de l'attribut User-Password dans d'autres demandes d'accès pour des utilisateurs sans relation. L'accès au texte chiffré permet des attaques de dictionnaire hors ligne, exposant potentiellement le secret partagé et compromettant le protocole RADIUS entier.

Tout paquet Demande d'accès qui effectue les vérifications d'autorisation, incluant Call Check, DEVRAIT contenir un attribut Authentifiant de message. Une réponse à une demande d'accès effectuant une vérification d'autorisation NE DOIT PAS contenir d'informations confidentielles sur un utilisateur (comme Tunnel-Password) sauf si cette demande d'accès contient un attribut State. L'utilisation de State permet ici de lier la vérification d'autorisation à une authentification d'utilisateur antérieure. Dans ce cas, le serveur PEUT répondre au NAS avec des informations confidentielles sur cet utilisateur. Le serveur NE DOIT PAS répondre à cette vérification d'autorisation avec des informations confidentielles sur un autre utilisateur.

Pour un paquet Demande d'accès qui effectue une vérification d'autorisation qui ne contient pas un attribut State, le serveur DOIT répondre avec un Rejet d'accès.

2.1.2 Compléments à l'identifiant de demande

Le paragraphe 2.6.1 de la [RFC3579] déclare : "Dans EAP, chaque session a son propre expace d'identifiants uniques. Les mises en œuvre de serveur RADIUS DOIVENT être capables de distinguer entre les paquets EAP avec le même Identifiant existants au sein de sessions distinctes, ayant leur origine sur le même NAS. À cette fin, les sessions peuvent être distinguées sur la base des attributs d'identification de NAS et de session. Les attributs d'identification de NAS incluent NAS-Identifier, NAS-IPv6-Address et NAS-IPv4-Address. Les attributs d'identification de session incluent User-Name, NAS-Port, NAS-Port-Type, NAS-Port-Id, Called-Station-Id, Calling-Station-Id et Originating-Line-Info."

Il y a des problèmes avec l'algorithme suggéré. Comme des mandataires peuvent modifier les attributs de demande d'accès comme NAS-IP-Address, dépendre de tout attribut sous le contrôle du NAS pour distinguer les identifiants de demande

peut résulter en des problèmes de déploiement.

La mise en œuvre FreeRADIUS ne retrace pas les identifiants EAP par NAS-IP-Address ou autres attributs non EAP envoyés par le NAS. À la place, elle utilise l'identifiant EAP, l'adresse de source IP, et l'attribut State comme une "clé" pour identifier de façon univoque chaque session EAP. Comme l'attribut State est sous le contrôle du serveur RADIUS, l'unicité de chaque session est contrôlée par le serveur, non par le NAS. L'algorithme utilisé dans FreeRADIUS est comme suit :

```
si (début d'EAP, ou identité EAP) {allouer un unique attribut State
        insérer la session dans un tableau "session active" avec
        clé=(identifiant EAP, State, source IP)
    } autrement { chercher une session active dans le tableau, avec la clé ci-dessus }
```

Cet algorithme paraît bien fonctionner dans diverses situations, incluant celles où les serveurs de rattachement reçoivent des messages via des mandataires RADIUS intermédiaires.

Les mises en œuvre qui n'utilisent pas cet algorithme sont souvent limitées à avoir un espace d'identifiant EAP par NAS, ou peut-être un qui est global pour la mise en œuvre. Ces restrictions sont inutiles quand l'algorithme ci-dessus est utilisé, car il donne à chaque session un espace unique d'identifiants EAP. L'algorithme ci-dessus DEVRAIT être utilisé pour retracer les sessions EAP de préférence à une autre méthode.

2.2 Conditions de surcharge

2.2.1 Comportement de retransmission

Le paragraphe 2.4 de la [RFC2865] décrit les exigences de retransmission pour les clients RADIUS : "À une extrémité, RADIUS n'exige pas une détection "sensible" de la perte de données. L'usager est d'accord pour attendre plusieurs secondes pour que l'authentification soit achevée. La retransmission généralement agressive de TCP (fondée sur un temps moyen d'aller-retour) n'est pas requise, pas plus que la redondance d'accusé de réception de TCP. À l'autre extrémité, l'usager n'est pas d'accord pour attendre plusieurs minutes pour l'authentification. Donc la livraison fiable des données de TCP après deux minutes n'est pas utile. L'utilisation plus rapide d'un serveur de remplacement permet à l'usager d'obtenir l'accès avant d'abandonner."

Certains clients RADIUS existants mettent en œuvre un comportement de retransmission excessivement aggressif, utilisant des temporisations de retransmission par défaut de une seconde ou moins sans prendre en charge le retard pour diminuer l'encombrement. Quand elles sont déployées à grande échelle, ces mises en œuvre sont susceptibles de pannes dues à l'encombrement. Par exemple, par suite d'une panne de courant, un réseau avec 3 000 appareils de NAS avec un temporisateur fixe de retransmission de une seconde va continuellement générer 3 000 demandes d'accès RADIUS par seconde. C'est suffisant pour surcharger la plupart des serveurs RADIUS.

Les solutions suggérées incluent:

a. La gigue. Pour éviter la synchronisation, un client RADIUS DEVRAIT incorporer une gigue induite dans son algorithme de retransmission, comme spécifié ci-dessous.

b. Le retard pour diminuer l'encombrement. Bien qu'il ne soit pas nécessaire pour les mises en œuvre de client RADIUS de mettre en œuvre des algorithmes complexes de retransmission, les mises en œuvre DEVRAIENT prendre en charge le retard pour diminuer l'encombrement.

Les temporisateurs de retransmission RADIUS se fondent sur le modèle utilisé dans le protocole dynamique de configuration d'hôte pour IPv6 (DHCPv6, *Dynamic Host Configuration Protocol for IPv6*) [RFC3315]. Les variables utilisées ici sont aussi empruntées à cette spécification. RADIUS est un protocole fondé sur la demande/réponse. L'échange de messages se termine quand le demandeur reçoit la réponse, ou quand l'échange de messages est considéré avoir échoué conformément au mécanisme de retransmission RECOMMANDÉ décrit ci-dessous. D'autres mécanismes de retransmission sont possibles, pour autant qu'ils satisfont les exigences sur la gigue et le retard pour diminuer l'encombrement.

Les algorithmes suivants s'appliquent à tout client qui génère des paquets RADIUS, incluant mais sans s'y limiter Access-Request, Accounting-Request, Disconnect-Request, et CoA-Request [RFC3576].

Le comportement de retransmission est contrôlé et décrit par les variables suivantes :

RT *(Retransmission Timeout)* temporisation de retransmission
IRT *(Initial Retransmission Time)* temps de retransmission initial (par défaut 2 secondes)
MRC *(Maximum Retransmission Count)* compte maximum de retransmission (par défaut 5 tentatives)
MRT *(Maximum Retransmission Time)* temps de retransmission maximum (par défaut 16 secondes)
MRD *(Maximum retransmission duration)* durée maximum de retransmission (par défaut 30 secondes)
RAND *(Randomization factor)* facteur aléatoire

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

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

L'algorithme pour choisir un nombre aléatoire n'a pas besoin d'être cohérent du point de vue cryptographique. L'algorithme DEVRAIT produire une séquence différente de nombres aléatoires à chaque invocation.

RT pour la première transmission de message est fondé sur IRT : RT = IRT + RAND*IRT

Pour chaque retransmission de message suivante, RT se fonde sur la précédente valeur of RT :

```
RT = 2*RTprev + RAND*RTprev
```

MRT spécifie une limite supérieure à la valeur de RT (sans considération du facteur aléatoire ajouté par l'utilisation de RAND). Si MRT a une valeur de 0, il n'y a pas de limite supérieure à la valeur de RT.Autrement :

```
si (RT > MRT)
  RT = MRT + RAND*MRT
```

MRD spécifie une limite supérieure à la durée pendant laquelle un envoyeur peut retransmettre un message. L'échange de messages échoue une fois que MRD secondes se sont écoulées depuis la première transmission du message par le client. MRD DOIT être réglé, et DEVRAIT avoir une valeur entre 5 et 30 secondes. Ces valeurs reflètent les valeurs pour une antémémoire de détection de dupliqués d'un serveur, comme décrit dans au paragraphe suivant.

MRC spécifie une limite supérieure du nombre de fois qu'un envoyeur peut retransmettre un message. Si MRC est zéro, l'échange de messages échoue une fois que MRD secondes se sont écoulées depuis la première transmission du message par le client. Si MRC n'est pas zéro, l'échange de messages échoue quand l'envoyeur a transmis le message MRC fois, ou quand MRD secondes se sont écoulées depuis la première transmission du message par le client.

Pour les paquets de demande de comptabilité, les valeurs par défaut pour MRC, MRD, et MRT DEVRAIENT être zéro. Ce réglage va permettre à un client RADIUS de continuer d'envoyer des demandes de comptabilité à un serveur RADIUS jusqu'à ce que la demande reçoive un accusé de réception. Si un de MRC, MRD, ou MRT n'est pas zéro, alors les informations comptables pourraient éventuellement être éliminées sans être enregistrées.

2.2.2 Détection de dupliqués et livraison en ordre

Quand des paquets sont retransmis par un client, le serveur peut recevoir des demandes dupliquées. Les limitations du protocole de transport utilisé par RADIUS, le protocole de datagramme d'utilisateur (UDP, *User Datagram Protocol*) signifie que les paquets Demande d'accès peuvent être reçus, et potentiellement traités, dans un ordre différent de celui dans lequel les paquets ont été envoyés. Cependant, la discussion du champ Identifiant à la Section 3 de la [RFC2865] dit : "Le serveur RADIUS peut détecter une duplication de demandes si elles ont la même adresse IP de source de client, le même accès UDP de source et le même identifiant dans un délai assez bref."

Aussi, la Section 7 de la [RFC4669] définit un objet radiusAuthServDupAccessRequests comme : "Le nombre de paquets Demande d'accès dupliqués reçu."

Ce texte a un certain nombre d'implications. D'abord, sans détection des dupliqués, un serveur RADIUS peut traiter deux fois une demande d'authentification, ce qui conduit à la conclusion erronée qu'un utilisateur s'est connecté deux fois. Ce comportement est indésirable, de sorte que la détection des dupliqués est désirable. Ensuite, le serveur peut retracer non seulement les demandes dupliquées, mais aussi les réponses à ces demandes. Ce comportement permet au serveur d'envoyer des réponses dupliquées en réponse à des demandes dupliquées, augmentant la stabilité du réseau.

Comme des paquets Demande d'accès peuvent aussi être envoyés par le client en réponse à un défi d'accès provenant du serveur, ces paquets forment un flux logiquement ordonné, et donc ont des exigences d'ordre supplémentaires par rapport aux paquets Demande d'accès pour des sessions différentes. Mettre en œuvre la détection des dupliqués résulte en ce que de nouveaux paquets soient traités seulement une fois, assurant l'ordre.

Les serveurs RADIUS DOIVENT donc mettre en œuvre la détection des dupliqués pour les paquets Demande d'accès, comme décrit à la Section 3 de la [RFC2865]. Les mises en œuvre DOIVENT aussi mettre en antémémoire les réponses (Accès-accepté, Défi-d'accès, ou Rejet-d'accès) qu'elles envoient en réponse aux paquets Demande d'accès. Si un serveur reçoit une demande d'accès dupliquée valide pour laquelle il a déjà envoyé une réponse, il DOIT envoyer à nouveau sa réponse originale sans retraiter la demande. Le serveur DOIT éliminer en silence toute demande d'accès dupliquée pour laquelle une réponse n'a pas encore été envoyée.

Chaque entrée d'antémémoire DEVRAIT être purgée après un certain temps. Ce temps NE DEVRAIT PAS être inférieur à 5 secondes, et pas plus de 30 secondes. Après environ 30 secondes, la plupart des clients RADIUS et des utilisateurs finaux auront abandonné la demande d'authentification. Donc, il n'y a aucun intérêt à avoir une plus grande temporisation d'antémémoire.

Les entrées d'antémémoire DOIVENT aussi être purgées si le serveur reçoit un paquet Demande d'accès valide qui correspond à un paquet Demande d'accès mis en antémémoire par son adresse de source, accès de source, identifiant RADIUS, et la prise de réception, mais où le champ Authentifiant de demande est différent de celui du paquet mis en antémémoire. Si la demande contient un attribut Authentifiant-de-message, la demande DOIT être traitée comme décrit au paragraphe 3.2 de la [RFC3580]. Les paquets avec des Authentifiant-de-message invalides NE DOIVENT affecter l'antémémoire d'aucune façon.

Cependant, les paquets Demande d'accès qui ne contiennent pas d'attribut Authentifiant-de-message affectent toujours l'antémémoire, même si il peut être trivial de les falsifier. Pour éviter ce problème, les mises en œuvre de serveur peuvent être configurées à exiger la présence d'un attribut Authentifiant-de-message dans les paquets Demande d'accès. Les demandes qui ne contiennent pas d'attribut Authentifiant-de-message PEUVENT alors être éliminés en silence.

Les mises en œuvre de client DEVRAIENT inclure un attribut Authentifiant-de-message dans chaque demande d'accès pour aider encore à atténuer ce problème.

Quand ils envoient des demandes, les clients RADIUS NE DOIVENT PAS réutiliser les identifiants pour une adresse de source IP et un accès de source avant qu'une réponse valide ait été reçue, ou que la demande arrive en fin de temporisation. Les clients DEVRAIENT allouer des identifiants via une méthode du "moins récemment utilisé" (LRU) pour une adresse de source IP et un accès de source particuliers.

Les clients RADIUS n'ont pas à effectuer de détection des dupliqués. Quand un client envoie une demande, il traite la premièret réponse qui a un authentifiant de réponse valide, comme défini à la Section 3 de la [RFC2865]. Toutes les réponses ultérieures DOIVENT être éliminées en silence, car elles ne correspondent pas à une demande en instance. C'est-à-dire, les réponses ultérieures sont traitées exactement de la même façon que des réponses non sollicitées, et sont éliminées en silence.

2.2.3 Réponse du serveur à la surcharge

Certaines mises en œuvre de serveur RADIUS ne sont pas robustes en présence de surcharge, éliminant des paquets avec une même probabilité sur plusieurs sessions. Dans une situation de surcharge, il en résulte un fort taux de défaillances pour des protocoles d'authentification à plusieurs tours comme EAP [RFC3579]. Normalement, les utilisateurs vont continuellement réessayer de tenter d'obtenir l'accès, augmentant encore la charge.

Une approche plus raisonnable est qu'un serveur RADIUS accepte de préférence les paquets RADIUS Demande d'accès contenant un attribut State valide, de façon à ce que les conversations d'authentification à plusieurs tours, une fois commencées, aient plus de chances de réussir. De même, un serveur qui passe les demandes par un mandataire devrait de préférence traiter les paquets Accés-accepté, Défi-d'accès, ou Rejet-d'accès provenant des serveurs de rattachement avant de traiter de nouvelles demandes provenant d'un NAS.

Ces méthodes vont permettre à certains utilisateurs d'obtenir l'accès au réseau, réduisant la charge créée par les tentatives d'accès en cours.

2.3 Problèmes de comptabilité

2.3.1 Attributs permis dans une mise à jour intermédiaire

La [RFC2866] indique que les attributs Acct-Input-Octets, Acct-Output-Octets, Acct-Session-Time, Acct-Input-Packets, Acct-Output-Packets et Acct-Terminate-Cause "peuvent seulement être présents dans les enregistrements Demande de comptabilité où le Acct-Status-Type est réglé à Stop".

Cependant le paragraphe 2.1 de la [RFC2869] déclare : "Il est envisagé qu'un enregistrement de comptabilité intermédiaire (avec Acct-Status-Type = Interim-Update (3)) contienne tous les attributs qui se trouvent normalement dans un message Arrêt de comptabilité à l'exception de l'attribut Acct-Term-Cause."

Bien que la [RFC2869] n'indique pas qu'elle met à jour la [RFC2866], c'est un oubli, et les attributs ci-dessus sont admissibles dans un enregistrement de comptabilité intermédiaire.

2.3.2 Acct-Session-Id et Acct-Multi-Session-Id

Le paragraphe 5.5 de la [RFC2866] décrit Acct-Session-Id comme texte au sein de la figure qui résume le format d'attribut, mais continue en disant que "Le champ Chaîne DEVRAIT être une chaîne de 10646 caractères codés en UTF-8".

La [RFC2865] définit le type Texte comme "contenant 10646 caractères codés en UTF-8", ce qui est compatible avec la description de Acct-Session-Id. Comme d'autres attributs sont décrits de façon cohérente comme "Texte" au sein de la figure décrivant le format d'attribut, et dans la définition d'attribut qui suit, il apparaît qu'il s'agit une faute de frappe, et que Acct-Session-Id est de type Texte, et non de type Chaîne.

La définition de l'attribut Acct-Multi-Session-Id a aussi des fautes de frappe. Elle dit : "Un résumé du format d'attribut de Acct-Session-Id ..."

Ce texte devrait se lire : "Un résumé du format de l'attribut Acct-Multi-Session-Id ..."

L'attribut Acct-Multi-Session-Id est aussi défini comme étant de type Chaîne. Cependant, le langage dans le texte recommande fortement que les mises en œuvre considèrent l'attribut comme étant de type Texte. On ne sait pas clairement pourquoi le type Chaîne a été choisi pour cet attribut alors que le type Texte serait suffisant. Cet attribut DEVRAIT être traité comme Texte.

2.3.3 Authentifiant de demande

Le paragraphe 4.1 de la [RFC2866] déclare : "L'authentifiant de demande d'une demande de comptabilité contient une valeur de hachage MD5 de 16 octets calculée conformément à la méthode décrite dans "Authentifiant de demande" ci-dessus."

Cependant, le texte n'indique aucune action à effectuer quand un paquet Demande de comptabilité contient un authentifiant de demande invalide. Le texte qui suit devrait être considéré comme faisant partie de la description ci-dessus :

"Le champ Authentifiant de demande DOIT contenir les données correctes, comme donné dans le calcul ci-dessus. Les paquets invalides sont éliminées en silence. Noter que certaines mises en œuvre anciennes règlent toujours l'authentifiant de demande tout à zéro. Les nouvelles mises en œuvre de clients RADIUS DOIVENT utiliser l'algorithme ci-dessus pour calculer le champ Authentifiant de demande. Les nouvelles mises en œuvre de serveur RADIUS DOIVENT éliminer en silence les paquets invalides."

2.3.4 Interim-Accounting-Interval

Le paragraphe 2.1 de la [RFC2869] déclare : "Il est aussi possible de configurer statiquement une valeur intérimaire sur le NAS lui-même. Noter qu'une valeur configurée en local sur le NAS DOIT outrepasser la valeur trouvée dans un Accès-Accepté."

Cette exigence peut être formulée de façon trop forte. Il est concevable qu'une mise en œuvre de NAS ait un réglage pour une valeur "minimum" de Interim-Accounting-Interval, sur la base de contraintes de ressources dans le NAS, et de la charge du réseau dans l'environnement local du NAS. Dans ce cas, la valeur fournie administrativement dans le NAS ne

devrait pas être outrepassée par une plus petite valeur provenant du message Accès-Accepté. La valeur du NAS pourrait cependant être outrepassée par une plus grande,. L'intention est que le NAS envoie les informations comptables à des intervalles fixes qui sont assez courts pour qu'une éventuelle perte de revenu facturable soit limitée, mais aussi que les mises à jour de comptabilité soient assez peu fréquentes pour que le NAS, le réseau, et le serveur RADIUS ne soient pas surchargés.

2.3.5 Valeurs de compteur dans la base de données d'informations de gestion RADIUS

Le module de MIB de client d'authentification et d'autorisation RADIUS ([RFC2618], [RFC4668]) inclut des compteurs de statistiques de paquets. Dans le texte de description du module de MIB, des formules sont fournies pour certains objets de compteur. Les mises en œuvre ont noté des incohérences apparentes dans les formules qui pourraient résulter en des valeurs négatives.

Comme le module de MIB original spécifié dans la [RFC2618] a été largement mis en œuvre, le groupe de travail RADEXT a choisi de ne pas changer les définitions d'objets ou d'en créer de nouvelles au sein de du module de MIB révisé [RFC4668]. Cependant, ce paragraphe explique les problèmes et fournit des lignes directrices concernant l'interprétation de la description textuelle et des commentaires pour certains objets de la MIB.

Les problèmes soulévés peuvent être résumés comme suit :

Problème (1) :
-- TotalIncomingPackets = Accepts + Rejects + Challenges + UnknownTypes
--
-- TotalIncomingPackets - MalformedResponses - BadAuthenticators -
-- UnknownTypes - PacketsDropped = Successfully Received
--
-- AccessRequests + PendingRequests + ClientTimeouts = Successfully Received

Il apparaît que la valeur de "Successfully Received" pourrait être négative, car divers compteurs sont soustraits de TotalIncomingPackets qui ne sont pas inclus dans le calcul de TotalIncomingPackets.

Il apparaît aussi que "AccessRequests + PendingRequests + ClientTimeouts = Successfully Received" devrait se lire "AccessRequests + PendingRequests + ClientTimeouts = Successfully Transmitted".

"TotalIncomingPackets" et "Successfully Received" sont des variables temporaires, c'est-à-dire, ce ne sont pas des objets au sein du module de MIB. Le commentaire dans les modules de MIB est en retrait, donc, pour aider à la compréhension. Ce qui importe est la cohérence des valeurs des objets dans le module de MIB, et cela ne paraît pas être impacté par les incohérences notées ci-dessus. Il apparaît, cependant, que la variable "Successfully Received" devrait être notée "Successfully Transmitted".

De plus, la définition des compteurs Accept, Reject ou Challenge indique qu'ils DOIVENT être incrémentés avant que le message soit validé. Si le message est invalide, un des compteurs MalformedResponses, BadAuthenticators, ou PacketsDropped va être incrémenté. Dans ce cas, les deux premières équations sont cohérentes, c'est-à-dire, "Successfully Received" ne pourrait pas être négatif.

Problème (2) :
Il apparaît que le compteur radiusAuthClientPendingRequests est décrémenté sur une retransmission. Cela signifierait qu'un paquet retransmis n'est pas considéré comme étant en instance, bien que de telles retransmissions puissent quand même être considérées comme étant des demandes en instances.

La définition de cet objet de MIB dans la [RFC2618] est comme suit :
"Le nombre de paquets RADIUS Demande d'accès destinés à ce serveur qui ne sont pas encore arrivés en fin de temporisation ou n'ont pas reçu de réponse. Cette variable est incrémentée quand une Demande d'accès est envoyée et décrémentée à cause de la réception d'un Accès-Accepté, Accès-Rejeté ou Défi-d'accès, d'une fin de temporisation ou d'une retransmission."

Cet objet revient à compter le nombre de paquets de demande en instance. L'interprétation de si les retransmissions d'une demande sont à compter comme paquets en instance supplémentaires ou non est ouverte. Dans l'un et l'autre cas, il semble approprié de traiter les retransmissions de façon cohérente par rapport à l'incrémentétion et la diminution de ce compteur.

2.4 Attributs Filter-ID multiples

Le paragraphe 5.11 de la [RFC2865] déclare : "Zéro, un ou plusieurs attributs Filter-Id PEUVENT être envoyés dans un paquet Accès-Accepté."

En pratique, le comportement d'un client RADIUS qui reçoit plusieurs attributs Filter-ID dépend de la mise en œuvre. Par exemple, certaines mises en œuvre traitent plusieurs instances de l'attribut Filter-ID comme des filtrss alternatifs ; le premier attribut Filter-ID qui a un nom qui correspond à un filtre défini en local est utilisé, et ceux qui restent sont éliminés. D'autres mises en œuvre peuvent combiner les filtres qui correspondent.

Par suite, l'interprétation de plusieurs attributs Filter-ID est indéfinie au sein de RADIUS. L'envoi de plusieurs attributs Filter-ID au sein d'un Accès-Accepté DEVRAIT être évité au sein de déploiements hétérogènes et de scénarios d'itinérance, où cela va probablement produire des résultats imprévisibles.

2.5 Attributs obligatoires et facultatifs

Les attributs RADIUS ne déclarent pas explicitement si ils sont facultatifs ou obligatoires. Néanmoins, il y a des instances où les attributs RADIUS doivent être traités comme obligatoires.

Le paragraphe 1.1 de la [RFC2865] déclare : "Un NAS qui ne met pas en œuvre un service donné NE DOIT PAS mettre en œuvre les attributs RADIUS pour ce service. Par exemple, un NAS qui n'est pas capable d'offrir le service ARAP NE DOIT PAS mettre en œuvre les attributs de RADIUS pour ARAP. Un NAS DOIT traiter une acceptation d'accès RADIUS autorisant un service indisponible comme un rejet d'accès."

À l'égard de l'attribut Type de service, le paragraphe5.6 de la [RFC2865] dit : "Cet attribut indique le type de service que l'utilisateur a demandé, ou le type de service à fournir. Il PEUT être utilisé dans les paquets Demande d'accès et Accès-Accepté. Un NAS n'est pas abligé de mettre en œuvre tous ces types de services, et DOIT traiter les types de services inconnus ou non pris en charge comme si un Accès-Rejeté avait été reçu à la place."

La Section 5 de la [RFC2865] déclare : "Un serveur RADIUS PEUT ignorer les attributs ayant un Type inconnu. Un client RADIUS PEUT ignorer les attributs ayant un Type inconnu."

À l'égard de l'attribut Vendor-Specific (VSA), le paragraphe 5.26 de la [RFC2865] déclare : "Les serveurs non équipés pour interpréter les informations spécifiques de fabricant envoyées par un client DOIVENT les ignorer (bien qu'elles puissent être rapportées). Les clients qui ne reçoivent pas les informations spécifiques de fabricant désirées DEVRAIENT tenter d'opérer sans elles, bien qu'ils puissent le faire (et rapporter qu'ils le font) en mode dégradé."

Il est possible pour un attribut standard ou un VSA de représenter une demande pour un service indisponible. Cependant, lorsque le Type, l'identifiant de fabricant, ou le type de fabricant, est inconnu, un client RADIUS ne va pas savoir si l'attribut définit ou non un service.

En général, il est meilleur pour un client RADIUS de se tenir dans une réserve prudente. À réception d'un Accès-Accepté incluant un attribut de type connu pour un service non mis en œuvre, un client RADIUS DOIT le traier comme un Accès-Rejeté, comme indiqué au paragraphe 1.1 de la [RFC2865]. À réception d'un Accès-Accepté incluant un attribut de type inconnu, un client RADIUS DEVRAIT supposer qu'il est une potentielle définition de service, et le traiter comme un Accès-Rejeté. Les VSA inconnus DEVRAIENT être ignorés par les clients RADIUS.

Afin d'éviter d'introduire des changements au comportement par défaut, les mises en œuvre existantes qui n'obéissent pas à cette recommandation devrait rendre le comportement configurable, avec le comportement traditionnel activé par défaut. Un fanion de configuration comme "traiter les attributs inconnus comme un rejet" peut être exposé à l'administrateur de système. Si le fanion est réglé à vrai, alors les Accès-Accepté contenant des attributs inconnus sont traités comme des Accès-Rejeté. Si le fanion est réglé à faux, alors les attributs inconnus dans les Accès-Accepté sont ignorés en silence.

À réception d'un paquet incluant un attribut de type inconnu, les mises en œuvre de serveur d'authentification RADIUS DEVRAIENT ignorer ces attributs. Cependant, les mises en œuvre de serveur de comptabilité RADIUS n'ont normalement pas besoin de comprendre les attributs afin de les écrire dans une mémorisation stable ou les passer au moteur de facturation. Donc, les mises en œuvre de serveur de comptabilité DEVRAIT être équipées pour traiter les attributs inconnus.

Pour éviter des mauvaises interprétations des demandes de service codées au sein des VSA, les serveurs RADIUS NE DEVRAIENT PAS envoyer des VSA contenant des demandes de service aux clients RADIUS qui ne sont pas connus pour

les comprendre. Par exemple, un serveur RADIUS ne devrait pas envoyer un VSA codant un filtre sans savoir si le client RADIUS prend en charge le VSA.

2.6 Interprétation de Accès-Rejeté

2.6.1 Utilisation inappropriée de Accès-Rejeté

L'intention d'un Accès-Rejeté est de refuser l'accès au service demandé. La Section 2 de la [RFC2865] déclare : "Si une condition n'est pas satifaite, le serveur RADIUS envoie une réponse "Accès-Rejeté" qui indique que cette demande d'utilisateur est invalide. Si c'est désiré, le serveur PEUT inclure un message de texte dans le Accès-Rejeté qui PEUT être affiché par le client à l'utilisateur. Aucun autre attribut (sauf Proxy-State) n'est permis dans un Accès-Rejeté."

Ce texte dit clairement que RADIUS ne permet pas le provisionnement de services au sein d'un Accès-Rejeté. Si le désir est de permettre un accès limité, alors un Accès-Accepté peut être envoyé avec des attributs provisionnant un accès limité. Les attributs au sein d'un Accès-Rejeté se restreignent à ceux nécessaires pour acheminer le message (par exemple, Proxy-State) aux attributs fournissant à l'utilisateur une indication que l'accès est refusé (par exemple, un attribut EAP-Message contenant un EAP-Échec) ou aux attributs portant un message d'erreur (par exemple, un attribut Reply-Message ou Error-Cause).

Malheureusement, il y a des exemples où cette exigence a été mal comprise. La paragraphe 2.2 de la [RFC2869] déclare : "Si cette authentification échoue, le serveur RADIUS devrait retourner un paquet Accès-Rejeté au NAS, avec des attributs facultatifs Password-Retry et Reply-Messages. La présence de Password-Retry indique que le NAS ARAP PEUT choisir d'initier un autre cycle de défi-réponse..."

Ce paragraphe est problématique de deux points de vue. D'abord, un attribut Password-Retry est retourné dans un Accès-Rejeté ; cet attribut ne rentre pas dans les catégories établies dans la [RFC2865]. Ensuite, un paquet Accès-Rejeté est envoyé dans le contexte de la poursuite d'une conversation d'authentification ; la [RFC2865] exige l'utilisation d'un Défi d'accès pour cela. La [RFC2869] utilise la phrase "défi-réponse" pour décrire cette utiliation de Accès-Rejeté, indiquant que la sémantique de Défi d'accès est utilisée.

Le paragraphe 4.4 de la [RFC2865] traite de la sémantique de Défi d'accès comme étant équivalente à Accès-Rejeté dans certains cas : "Si le NAS n’accepte pas le défi/réponse, il DOIT traiter un Défi-d’accès comme s’il avait reçu un Rejet-d’accès à la place."

Bien qu'il soit difficile de corriger les déploiements existants de la [RFC2869], on fait les recommandations suivantes :

[1] Les nouvelles spécifications et mises en œuvre de RADIUS NE DOIVENT PAS utiliser Accès-Rejeté lorsque c'est la sémantique de Défi d'accès qui est entendue.

[2] Accès-Rejeté DOIT signifier un refus d'accès au service demandé. En réponse à un Accès-Rejeté, le NAS NE DOIT PAS envoyer des paquets Demande d'accès supplémentaires pour cette session d'utilisateur.

[3] Les nouveaux déploiements de ARAP [RFC2869] DEVRAIENT utiliser des paquets Défi d'accès à la place de paquets Accès-Rejeté dans les conversations décrites au paragraphe 2.2 de la [RFC2869].

On note aussi que le tableau des attributs au paragraphe 5.19 de la [RFC2869] a une erreur pour l'attribut Password-Retry. Il dit :

Demande	Accepte	Rejet	Défi	N °	Attribut
0	0	0-1	0	75	Password-Retry

Cependant, le texte du paragraphe 2.3.2 de la [RFC2869] dit que Password-Retry peut être inclus au sein d'un paquet Défi d'accès pour les sessions d'authentification EAP. On recommande une correction au tableau qui supprime le "0-1" de la colonne Rejet, et le déplace à la colonne Défi. On ajoute aussi une "Note 2" à la suite de la "Note 1" existante dans le document pour préciser l'utilisation de cet attribut.

Demande	Accepte	Rejet	Défi	N °	Attribut
0	0	0	0-1	75	Password-Retry [Note 2]

[Note 2] Selon la RFC 3579, l'utilisation de Password-Retry dans les authentifications EAP est déconseillée. L'attribut

Password-Retry peut être utilisé seulement pour l'authentification ARAP.

2.6.2 Refus de demande de service

RADIUS a été déployé pour des besoins extérieurs d'authentification d'accès au réseau, d'autorisation, et de comptabilité. Par exemple, RADIUS a été déployé comme "base arrière" pour l'authentification des connexions de voix sur IP (VOIP), des sessions de protocole de transfert Hypertext (HTTP) (par exemple, Apache), des sessions du protocole de transfert de fichiers (FTP) (par exemple, proftpd), et la connexion de machine pour plusieurs systèmes d'exploitation (par exemple, bsdi, pam, et gina). Dans ces contextes, un Accès-Rejeté envoyé au client RADIUS DOIT être interprété comme un rejet de la demande de service, et le client RADIUS NE DOIT PAS offrir ce service à l'utilisateur.

Par exemple, quand un échec d'authentification survient dans le contexte d'une session FTP, la sémantique normale pour le rejet des services FTP s'applique. Le rejet ne cause pas nécessairement que le serveur FTP termine la connexion TCP sous-jacente, mais le serveur FTP NE DOIT PAS offrir de services protégés par l'authentification de l'utilisateur.

Les utilisateurs peuvent demander plusieurs services au NAS. Lorsque ces services sont indépendants, le déploiement DOIT traiter les sessions RADIUS comme étant indépendantes.

Par exemple, un NAS peut offrir des services multi-liaisons où un utilisateur peut avoir plusieurs connexions réseau simultanées. Dans ce cas, un Accès-Rejeté pour une demande de connexion multi-liaisons ultérieure ne signifie pas nécessairement que les connexions multi-liaisons antérieures sont supprimées. De même, si un NAS offre à la fois des services à numérotage et des services VOIP, le rejet d'une tentative VOIP ne signifie pas que la session de numérotage est supprimée.

2.7 Adressage

2.7.1 Adresses de liaison locale

Comme les adresses de liaison locale ne sont uniques que sur la liaison locale, si le NAS et le serveur RADIUS ne sont pas sur la même liaison, alors une adresse de liaison locale IPv6 [RFC4862] ou une adresse de liaison locale IPv4 [RFC3927] ne peut pas être utilisée pour identifier de façon univoque le NAS. Un NAS NE DEVRAIT PAS utiliser une adresse de portée liaison au sein d'un attribut NAS-IPv6-Address ou NAS-IP-Address. Un serveur RADIUS qui reçoit un attribut NAS-IPv6-Address ou NAS-IP-Address contenant une adresse de liaison locale NE DEVRAIT PAS compter un tel attribut comme satisfaisant les exigences du paragraphe 2.1 de la [RFC3162] : "NAS-IPv6-Address et/ou NAS-IP-Address PEUVENT être présents dans un paquet Demande d'accès ; cependant, si aucun de ces attributs n'est présent, alors NAS-Identifier DOIT être présent."

2.7.2 Adresses multiples

Il y a des situations dans lesquelles un client ou serveur RADIUS peut avoir plusieurs adresses. Par exemple, un hôte double pile peut avoir à la fois des adresses IPv4 et IPv6 ; un hôte qui est membre de plusieurs VLAN pourrait avoir des adresses IPv4 et/ou IPv6 sur chaque VLAN ; un hôte peut avoir plusieurs adresses IPv4 ou IPv6 sur une seule interface. Cependant, le paragraphe 5.44 de la [RFC2865] permet seulement zéro ou un attribut NAS-IP-Address au sein d'une demande d'accès, et la Section 3 de la [RFC3162] permet seulement zéro ou un attribut NAS-IPv6-Address au sein d'une demande d'accès. Quand un NAS a plus d'une adresse mondiale et pas de capacité de déterminer laquelle est utilisée pour l'identification d'une demande particulière, il est RECOMMANDÉ que le NAS inclue l'attribut NAS-Identifier dans une demande d'accès afin de s'identifier auprès du serveur RADIUS.

La Section 3 de la [RFC2865] déclare : "Un serveur RADIUS DOIT utiliser l'adresse IP de source du paquet UDP RADIUS pour décider quel secret partagé utiliser, de sorte que les demandes RADIUS puissent faire l'objet d'un mandat."

Donc, si un client RADIUS envoie des paquets à partir de plus d'une adresse de source, un secret partagé va devoir être configuré sur le client et le serveur pour chaque adresse de source.

2.8 Idle-Timeout

À l'égard de l'attribut Idle-Timeout, le paragraphe 5.28 de la [RFC2865] déclare : "Cet attribut règle le nombre maximum de secondes consécutives de connexion sans activité permis à l'usager avant la terminaison de la session ou de l'invite. Cet attribut est disponible pour envoi par le serveur au client dans un Accès-Accepté ou un Défi-d'accès."

Le paragraphe 3.18 [RFC3580] déclare : "L'attribut Idle-Timeout est décrit dans la [RFC2865]. Pour les supports IEEE 802 autres que 802.11 les supports sont toujours activés. Par suite, l'attribut Idle-Timeout n'est normalement utilisé qu'avec des supports sans fil comme IEEE 802.11. Il est possible qu'un appareil sans fil erre en dehors de la gamme de tous les points d'accès. Dans ce cas, l'attribut Idle-Timeout indique la durée maximum pendant laquelle un appareil sans fil peut rester inactif."

Dans les paragraphes ci-dessus "inactif" peut ne pas nécessairement signifier "pas de trafic" ; le NAS peut prendre en charge des filtres qui définissent quel trafic est inclus dans la détermination du temps inactif. Par suite, une "connexion inactive" est définie par la politique locale en l'absence d'autres attributs.

2.9 Identité inconnue

Le paragraphe 5.1 de la [RFC3748] déclare : "Si l'identité est inconnue, le champ Identité de réponse devrait être d'une longueur de zéro octet."

Cependant, le paragraphe 5.1 de la [RFC2865] décrit comme suit l'attribut User-Name : "Le champ Chaîne est de un ou plusieurs octets."

Comment le client RADIUS devrait-il se conduire si il reçoit une EAP-Response/Identity qui est d'une longueur de zéro octet ?

Le paragraphe 5.1 de la [RFC2865] déclare : "Cet attribut indique le nom de l'usager à authentifier. Il DOIT être envoyé dans les paquets de demande d'accès s'il est disponible."

Cela suggère que l'attribut User-Name peut être omis si il est indisponible.

Cependant, le paragraphe 2.1 de la [RFC3579] déclare : "Afin de permettre à des mandataires RADIUS sans capacité EAP de transmettre le paquet Demande d'accès, si le NAS envoie initialement un message EAP-Request/Identity à l'homologue, le NAS DOIT copier le contenu du champ Type-Data du EAP-Response/Identity reçu de l'homologue dans l'attribut User-Name et DOIT inclure le champ Type-Data du EAP-Response/Identity dans l'attribut User-Name dans chaque demande d'accès suivante."

Cela suggère que l'attribut User-Name devrait contenir le contenu du champ Type-Data du EAP-Response/Identity, même si il est d'une longueur de zéro octet.

Noter que la [RFC4282] ne permet pas un identifiant d'accès réseau (NAI, *Network Access Identifier*) de zéro octet, de sorte qu'une EAP-Response/Identity avec un champ Type-Data de zéro octet NE DOIT PAS être construit comme une demande de confidentialité (par exemple, NAI anonyme).

Quand un NAS reçoit une EAP-Response/Identity avec un champ Type-Data de longueur zéro octet, il est RECOMMANDÉ qu'il omette l'attribut User-Name dans la demande d'accès ou qu'il inclue le Calling-Station-Id dans l'attribut User-Name, avec un attribut Calling-Station-Id.

2.10 Réponses après retransmissions

Certaines mises en œuvre ne traitent pas correctement la réception des réponses RADIUS après des retransmissions. Le paragraphe 2.5 de la [RFC2865] déclare : "Si le NAS retransmet une demande RADIUS au même serveur que précédemment, et si les attributs n'ont pas changé, on DOIT utiliser le même Authentifiant de demande, le même Identifiant, et le même Accès de source. Si des attributs ont changé, on DOIT utiliser un nouvel Authentifiant de demande et un nouvel Identifiant."

Noter que changer l'identifiant de demande pour une retransmission peut avoir des effets collatéraux indésirables. Comme RADIUS n'a pas une claire définition de "session", il est parfaitement valide pour un serveur RADIUS de traiter une retransmission comme une nouvelle demande de session, et de la rejeter à cause, par exemple, de l'application de

restrictions sur plusieurs connexions simultanées.

Dans cette situation, le NAS peut recevoir un Accès-Accepté retardé pour la première demande, et un Accès-Rejeté pour la demande retransmise, qui s'appliquent tous deux à la même "session".

On suggère que le contenu des paquets Demande d'accès NE DEVRAIT PAS être changé durant les retransmissions. Si il doit être changé du fait de l'inclusion d'un attribut Event-Timestamp, par exemple, alors les réponses à des transmissions antérieures DOIVENT être éliminées en silence. Toute réponse à la demande courante DOIT être traitée comme réponse définitive, même si comme noté ci-dessus, elle est en désaccord avec des réponses antérieures.

Ce problème peut être rendu pire par des mises en œuvre qui utilisent une temporisation fixe de retransmission (30 secondes est courant). On répète les suggestions du paragraphe 2.1 sur l'utilisation du retard pour encombrement. Dans ce cas, les réponses à des transmissions antérieures PEUVENT être utilisées comme des points de données pour le retard pour encombrement, même si leur contenu est éliminé.

2.11 Framed-IPv6-Prefix

Le paragraphe 2.3 de la [RFC3162] dit : "Cet attribut indique un préfixe IPv6 (et le chemin correspondant) à configurer pour l'utilisateur. Il PEUT être utilisé dans des paquets Accès-Accepté, et peut apparaître plusieurs fois. Il PEUT être utilisé dans un paquet Demande d'accès comme conseil du NAS au serveur qu'il prefèreraît ces préfixes, mais le serveur n'est pas obligé d'honorer le conseil. Comme on suppose que le NAS va sonder un chemin correspondant au préfixe, il n'est pas nécessaire que le serveur envoie aussi un attribut Framed-IPv6-Route pour le même préfixe."

Un fournisseur de service Internet (FAI) peut désirer prendre en charge la délégation de préfixe [RFC4818] au même moment où il voudrait allouer un préfixe pour la liaison entre le NAS et l'utilisateur. L'intention du paragraphe était de permettre au NAS d'annoncer le préfixe (comme via une annonce de routeur). Si l'attribut Framed-Routing est utilisé, il est aussi possible que le préfixe soitt annoncé dans un protocole d'acheminement comme le protocole d'informations d'acheminement de nouvelle génération (RIPNG).

Le paragraphe 5.10 de la RFC 2865 décrit l'objet de Framed-Routing : "Cet attribut indique la méthode d'acheminement pour l'usager, quand l'usager est un routeur pour un réseau. Il n'est utilisé que dans les paquets Accès-Accepté."

La description du champ Longueur de préfixe dans la RFC 3162 indique une latitude excessivement large : "La longueur du préfixe, en bits. Au moins 0 et pas plus de 128."

Cette longueur paraît trop grande, parce que ce qu'un NAS devrait faire avec un préfixe de plus grande granularité que /64 n'est pas clair. Par exemple, le Framed-IPv6-Prefix peut contenir un /128. Cela n'impluqe pas que le NAS devrait allouer une adresse IPv6 à l'utilisateur final, parce que la RFC 3162 a déjà défini un attribut Framed-IPv6-Identifier pour traiter la portion Identifiant.

Il apparaît que le Framed-IPv6-Prefix est utilisé pour la liaison entre le NAS et l'équipement local d'abonné (CPE, *Customer Premises Equipment*) seulement si un préfixe /64 est alloué. Quand un préfixe /64 ou plus grand est envoyé, l'intention est que le NAS envoie une annonce de chemin contenant les informations présentes dans l'attribut Framed-IPv6-Prefix.

Le CPE peut aussi exiger un préfixe délégué pour son propre usage, si il décrémente le champ Limite de bonds des en-têtes IP. Dans ce cas, il devrait lui être délégué un préfixe par le NAS via l'attribut Delegated-IPv6-Prefix [RFC4818]. Si le CPE ne décrémente pas la limite de bonds, il n'exige pas de préfixe délégué.

3. Considérations sur la sécurité

Le contenu de l'attribut State est disponible au client RADIUS et à ceux qui observent le protocole RADIUS. Les mises en œuvre de serveur RADIUS devraient s'assurer que l'attribut State ne divulgue pas d'informations sensibles à un client RADIUS ou à des tiers qui observent le protocole RADIUS.

Le mécanisme d'antémémoire décrit au paragraphe 2.2.2 est vulnérable aux attaques quand des paquets Demande d'accès ne contiennent pas d'attribut Authentifiant-de-message. Si le serveur accepte des demandes sans un attribut Authentifiant-de-message, il est alors trivial à un attaquant de falsifier les messages RADIUS. Les entrées d'antémémoire peuvent alors

être forcée d'arriver à expiration, niant l'utilité de l'antémémoire. Cette attaque peut être atténuée en suivant les suggestions de la Section 4 de la [RFC3579], ou en exigeant la présence d'un Authentifiant-de-message, comme décrit aux paragraphes 2.1.1 et 2.2.2.

Comme le présent document décrit l'utilisation de RADIUS pour les besions d'authentification, d'autorisation, et de comptabilité dans une grande variété de réseaux, les applications qui utilisent ces spécifications sont vulnérables à toutes les menaces qui sont présentes dans les autres applications RADIUS. Pour une discussion de ces menances, voir les [RFC2865], [RFC2607], [RFC3162], [RFC3579], et [RFC3580].

4. Références

4.1 Références normatives

[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.)*

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

4.2 Références pour information

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

[RFC2618] B. Aboba, G. Zorn, "MIB de client d'authentification RADIUS", juin 1999. (*Obsolète, voir* RFC4668) *(P.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)

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

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

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

[RFC3580] P. Congdon et autres, "Lignes directrices pour l'utilisation du service d'authentification distante d'utilisateur appelant (RADIUS) par IEEE 802.1X", septembre 2003. *(Information)*

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

[RFC3927] S. Cheshire, B. Aboba, E. Guttman, "Configuration dynamique des adresses IPv4 de liaison locale", mai 2005. *(P.S.)*

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

[RFC4668] D. Nelson, "MIB de client d'authentification RADIUS pour IPv6", août 2006. (*Remplace* RFC2618) *(P.S.)*

[RFC4669] D. Nelson, "MIB de serveur d'authentification RADIUS pour IPv6", août 2006. (*Remplace* RFC2619) *(P.S.)*

[RFC4862] S. Thomson et autres, "Auto configuration d'adresse IPv6 sans état", septembre 2007. (*Remplace* RFC2462) *(D.S.)*

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

Remerciements

Les auteurs tiennent à remercier Glen Zorn et Bernard Aboba de leurs contributions au présent document.

L'algorithme de remplacement du paragraphe 2.6.1 de la [RFC3579] qui est décrit au paragraphe 2.1.2 du présent document a été conçu par Raghu Dendukuri.

Le texte qui discute des retransmissions au paragraphe 2.2.1 est tiré avec de mineures corrections rédactionnelles de la Section 9 du "Protocole pour porter l'authentification pour l'accès réseau (PANA)" [RFC5191].

Alan DeKok souhaite remercier de sa prise en charge par Quiconnect Inc., où il a été employé durant la plupart du temps où il a travaillé au présent document.

David Nelson souhaite remercier de sa prise en charge par Enterasys Networks, où il a été employé durant la plupart du temps où il a travaillé au présent document.

Adresse des auteurs

David B. Nelson
Elbrys Networks, Inc.
75 Rochester Ave., Unit 3
Portsmouth, N.H. 03801 USA
téléphone : +1.603.570.2636
mél : dnelson@elbrysnetworks.com

Alan DeKok
The FreeRADIUS Server Project
http://freeradius.org/
mél : aland@freeradius.org

Déclaration complète de droits de reproduction

http://www.ietf.org/ipr.

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