

Groupe de travail Réseau
Request for Comments : 2865
 RFC rendue obsolète : 2138
 Catégorie : En cours de normalisation
 juin 2000

C. Rigney, S. Willens, Livingston
 A. Rubens, Merit
 W. Simpson, Daydreamer
 Traduction Claude Brière de L'Isle
 janvier 2008

Service d'authentification à distance de l'utilisateur appelant (RADIUS)

Statut de ce mémo

Le présent document spécifie un protocole de normalisation Internet pour la communauté de l'Internet, qui appelle à la discussion et à des suggestions pour son amélioration. Prière de se reporter à l'édition en cours des "Normes de protocole officielles de l'Internet" (STD 1) sur l'état de la normalisation et le statut de ce protocole. La distribution du présent mémo n'est soumise à aucune restriction.

Notice de Copyright

Copyright (C) The Internet Society (2000).

Note de l'IESG :

Le présent protocole est largement mis en œuvre et utilisé. L'expérience montre qu'il peut subir une dégradation des performances et des pertes de données dans les grands systèmes, en partie parce qu'il ne comporte pas de dispositions pour le contrôle de l'encombrement. Les lecteurs de ce document tireront avantage du suivi des progrès du groupe de travail AAA de l'IETF, qui développe un protocole destiné à succéder à celui-ci pour mieux s'intéresser aux questions de taille et de contrôle de l'encombrement.

Résumé

Le présent document décrit un protocole de transport des informations d'authentification, d'autorisation, et de configuration entre un serveur d'accès réseau qui désire authentifier sa liaison et un serveur d'authentification partagée.

Note de mise en œuvre

Le présent mémo présente le protocole RADIUS. Les premiers développements de RADIUS ont été faits sur l'accès UDP numéro 1645, qui est en conflit avec le service "datametrics". Le numéro d'accès officiellement alloué à RADIUS est 1812.

Table des matières

1 Introduction.....	3
1.1 Spécification des exigences.....	3
1.2 Terminologie.....	4
2 Fonctionnement.....	4
2.1 Défi/réponse.....	5
2.2 Interfonctionnement de PAP et CHAP.....	5
2.3 Mandataire.....	6
2.4 Pourquoi UDP ?.....	7
2.5 Conseils de retransmission.....	8
2.6 Maintiens en vie considérés comme dommageables.....	8
3 Format de paquet.....	8
4 Types de paquet.....	10
4.1 Demande d'accès.....	10
4.2 Accès-Accepté.....	11
4.3 Rejet-d'accès.....	11
4.4 Défi-d'accès.....	12
5 Attributs.....	13
5.1 Nom-d'utilisateur.....	15
5.2 Mot-de-passe-d'utilisateur.....	15

5.3 Mot de passe CHAP.....	16
5.4 Adresse-IP-NAS.....	16
5.5 Accès-de-NAS.....	17
5.6 Type-de-Service.....	17
5.7 Protocole-tramé.....	18
5.8 Adresse-IP-tramée.....	19
5.9 Gabarit-réseau-IP-tramé.....	19
5.10 Routage-tramé.....	19
5.11 Identifiant-de-filtre.....	20
5.12 MTU-tramée.....	20
5.13 Compression-tramée.....	21
5.14 Hôte-de-Connexion-IP.....	21
5.15 Service-de-Connexion.....	22
5.16 Port-de-connexion-TCP.....	22
5.17 (non alloué).....	22
5.18 Message-de-réponse.....	22
5.19 Numéro-de-rappel.....	23
5.20 Identifiant-de-rappel.....	23
5.21 (non alloué).....	24
5.22 Route-tramée.....	24
5.23 Réseau-IPX-tramé.....	24
5.24 État.....	25
5.25 Classe.....	25
5.26 Spécifique-du-fabricant.....	26
5.27 Durée-de-session.....	26
5.28 Durée-d'inactivité.....	27
5.29 Action-de-terminaison.....	27
5.30 Identifiant-de-station-appelée.....	28
5.31 Identifiant-de-station-appelante.....	28
5.32 Identifiant-de-NAS.....	29
5.33 État de mandataire.....	29
5.34 Service-de-connexion-LAT.....	30
5.35 Nœud-de-connexion-LAT.....	30
5.36 Groupe-de-connexion-LAT.....	31
5.37 Liaison-AppleTalk-tramée.....	31
5.38 Réseau-AppleTalk-tramé.....	32
5.39 Zone-AppleTalk-tramée.....	32
5.40 Défi-CHAP.....	33
5.41 Type-d'accès-de-NAS.....	33
5.42 Limite-d'accès.....	34
5.43 Accès-de-connexion-LAT.....	34
5.44 Tableau des attributs.....	35
6 Considérations relatives à l'IANA.....	36
6.1 Définition des termes.....	36
6.2 Politiques d'enregistrement recommandées.....	36
7 Exemples.....	37
7.1 Usager Telnet à l'hôte spécifié.....	37
7.2 Usager tramé s'authentifiant avec CHAP.....	37
7.3 Usager avec carte d'épreuve-réponse.....	38
8 Considérations pour la sécurité.....	40
9 Journal des modifications.....	40
10 Références.....	41
11 Remerciements.....	41
12 Adresse du président du groupe de travail.....	42
13 Adresse des auteurs.....	42
14. Déclaration de droits de reproduction.....	42

1 Introduction

Le présent document rend obsolète la RFC 2138 [1]. Un résumé des changements depuis la RFC 2138 figure à la Section 9 "Journal des modifications".

La gestion de lignes de série dispersées et de groupes de modems pour de grands nombres d'utilisateurs peut créer le besoin d'un soutien administratif significatif. Comme les groupes de modems sont par définition un lien avec le monde extérieur, il demandent une attention soutenue à la sécurité, aux autorisations et à la comptabilité. Le meilleur moyen d'y arriver est de tenir une seule "base de données" des utilisateurs, qui permet l'authentification (la vérification des noms d'utilisateurs et de leurs mots de passe) ainsi que les informations de configuration qui précisent le type de service à fournir à l'utilisateur (par exemple, SLIP, PPP, telnet, rlogin).

Les dispositifs clés de RADIUS sont :

Le modèle client/serveur

Un serveur d'accès réseau (NAS, *Network Access Server*) fonctionne comme client de RADIUS. Le client est chargé du passage des informations d'utilisateur aux serveurs RADIUS désignés, puis d'agir sur la réponse retournée.

Les serveurs RADIUS sont chargés de recevoir les demandes de connexion d'usager, d'authentifier l'usager, puis de retourner toutes les informations de configuration nécessaires pour que le client livre le service à l'usager.

Un serveur RADIUS peut agir comme client mandataire d'autres serveurs RADIUS ou autres sortes de serveurs d'authentification.

Sécurité du réseau

Les transactions entre le client et le serveur RADIUS sont authentifiées grâce à l'utilisation d'un secret partagé, qui n'est jamais envoyé sur le réseau. De plus, tout mot de passe d'utilisateur est envoyé chiffré entre client et serveur RADIUS, pour éliminer la possibilité que quelqu'un espionnant sur un réseau non sécurisé puisse déterminer le mot de passe d'un usager.

Mécanismes d'authentification souples

Le serveur RADIUS peut prendre en charge diverses méthodes pour authentifier un usager. Lorsqu'on lui fournit le nom de l'usager et le mot de passe original donné par l'usager, il peut prendre en charge PAP ou CHAP PPP, la connexion UNIX, et d'autres mécanismes d'authentification.

Protocole extensible

Toutes les transactions comportent des triplets attribut-longueur-valeur de longueur variable. De nouvelles valeurs d'attribut peuvent être ajoutées sans perturber les mises en œuvre existantes du protocole.

1.1 Spécification des exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans le BCP 14 [2]. Ces mots clé signifient la même chose en majuscule ou en minuscules.

Une mise en œuvre n'est pas conforme si elle ne réussit pas à satisfaire une ou plusieurs exigences marquées "doit" ou "ne doit pas" pour les protocoles qu'elle met en œuvre. Une mise en œuvre qui satisfait à toutes les exigences "doit" "ne doit pas", "devrait" et "ne devrait pas" pour ses protocoles est dite être "inconditionnellement conforme" ; celle qui satisfait à toutes les exigences "doit" et "ne doit pas" mais pas à tous les "devrait" ou "ne devrait pas" pour son protocole est dite être "conditionnellement conforme".

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 (Reject-Access).

1.2 Terminologie

Le présent document utilise fréquemment les termes suivants :

service : le NAS fournit un service à l'utilisateur appelant, comme PPP ou Telnet.

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

éliminé en silence : cela signifie qu'une 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, et DEVRAIT enregistrer l'événement dans un compteur à des fins de statistique.

2 Fonctionnement

Lorsque un client est configuré pour utiliser RADIUS, tout utilisateur du client présente des informations d'authentification au client. Cela peut être avec une amorce de connexion personnalisable, où l'utilisateur est supposé entrer son nom d'utilisateur et mot de passe. Autrement, l'utilisateur peut utiliser un protocole de tramage de liaison tel que le protocole point à point (PPP, *Point-to-Point Protocol*), qui a des paquets d'authentification qui portent ces informations.

Une fois que le client a obtenu de telles informations, il peut choisir de s'authentifier en utilisant RADIUS. Pour ce faire, le client crée une "Demande d'accès" contenant des attributs tels que le nom de l'utilisateur, le mot de passe de l'utilisateur, l'identifiant du client et l'identifiant de l'accès auquel l'utilisateur accède. Lorsque un mot de passe est présent, il est caché en utilisant une méthode fondée sur l'algorithme RSA de résumé de message MD5 [3].

La Demande d'accès est soumise au serveur RADIUS via le réseau. Si aucune réponse n'est retournée au bout d'un certain temps, la demande est renvoyée un certain nombre de fois. Le client peut aussi transmettre des demandes à un serveur ou à des serveurs de remplacement pour le cas où le serveur principal serait en panne ou injoignable. Un serveur de remplacement peut être utilisé soit après l'échec d'un certain nombre d'essais sur le serveur principal, soit à la façon round-robin. Les algorithmes de réessai et de repli continuent de faire l'objet de recherches et ne sont pas spécifiés en détail dans le présent document.

Une fois que le serveur RADIUS a reçu la demande, il valide le client d'envoi. Une demande du client pour laquelle le serveur RADIUS n'a pas de secret partagé DOIT être éliminée en silence. Si le client est valide, le serveur RADIUS consulte une base de données d'utilisateurs pour trouver l'utilisateur dont le nom correspond à la demande. L'entrée d'utilisateur dans la base de données contient une liste d'exigences qui doivent être satisfaites pour permettre l'accès à l'utilisateur. Cela inclut toujours la vérification du mot de passe, mais peut aussi spécifier le ou les clients ou accès auxquels l'utilisateur est autorisé.

Le serveur RADIUS PEUT faire des demandes aux autres serveurs afin de satisfaire la demande, auquel cas il agit comme client.

Si des attributs État de mandataire sont présents dans la demande d'accès, ils DOIVENT être copiés non modifiés et dans l'ordre dans le paquet de réponse. Les autres attributs peuvent être placés avant, après, ou même entre les attributs État de mandataire.

Si une condition n'est pas satisfaite, le serveur RADIUS envoie une réponse "Rejet-d'accès" qui indique que cette demande d'utilisateur est invalide. S'il le désire, le serveur PEUT inclure un message textuel dans le Rejet-d'accès qui PEUT être affichée par le client à l'utilisateur. Aucun autre attribut (excepté État de mandataire) n'est permis dans un Rejet-d'accès.

Si toutes les conditions sont satisfaites et si le serveur RADIUS souhaite produire une mise en cause à laquelle l'utilisateur doit répondre, le serveur RADIUS envoie une réponse "Défi-d'accès". Il PEUT inclure un message textuel à afficher par le client à l'utilisateur invitant à une réponse à la mise en cause, et PEUT inclure un attribut État.

Si le client reçoit un Défi-d'accès et s'il prend en charge le défi/réponse il PEUT afficher le texte du message, s'il en est, à l'utilisateur, et inviter ensuite l'utilisateur à répondre. Le client soumet alors à nouveau sa Demande d'accès originale avec un nouvel identifiant de demande, avec l'attribut Mot-de-passe-d'utilisateur remplacé par la réponse (chiffrée), et incluant l'attribut État tiré de Défi-d'accès, s'il en est. Seule 0 ou 1 instance de l'attribut État DEVRAIT être présente dans une demande. Le serveur peut répondre à cette nouvelle Demande d'accès par un Accès-Accepté, un Rejet-d'accès, ou un autre Défi-d'accès.

Si toutes les conditions sont satisfaites, la liste des valeurs de configuration pour l'utilisateur est placée dans une réponse

"Accès-Accepté". Ces valeurs incluent le type de service (par exemple : SLIP, PPP, Login User) et toutes les valeurs nécessaires pour livrer le service souhaité. Pour SLIP et PPP, cela peut inclure des valeurs telles que des adresses IP, un gabarit de sous-réseau, une MTU, la compression souhaitée, et les identifiants de filtre de paquet souhaités. Pour les usagers en mode caractère, cela peut inclure des valeurs telles que le protocole et l'hôte désirés.

2.1 Défi/réponse

Dans l'authentification par défi/réponse, l'utilisateur reçoit un nombre imprévisible qu'il est mis au défi de chiffrer et de redonner le résultat. Les usagers autorisés sont équipés d'un appareil spécial tel qu'une carte à puce ou un logiciel qui rend facile le calcul de la réponse correcte. Les utilisateurs non autorisés, qui n'ont pas l'appareil ou le logiciel approprié et qui ne connaissent pas la clé secrète nécessaire à l'émulation d'un tel appareil ou logiciel, peuvent seulement essayer de deviner la réponse.

Le paquet Défi-d'accès contient normalement un Message-de-réponse incluant une épreuve destinée à être affichée à l'utilisateur, comme une valeur numérique de répétition improbable. Normalement, elle est obtenue d'un serveur externe qui sait quel type d'authentifiant est en la possession de l'utilisateur autorisé et peut donc choisir un nombre aléatoire ou pseudo-aléatoire non répétable d'une racine et longueur appropriées.

L'utilisateur entre alors l'épreuve dans son appareil (ou logiciel) et il calcule une réponse, que l'utilisateur entre dans le client qui la transmet au serveur RADIUS via une seconde Demande d'accès. Si la réponse correspond à la réponse attendue, le serveur RADIUS réplique par un Accès-Accepté, et sinon par un Rejet-d'accès.

Exemple : Le NAS envoie un paquet Demande d'accès au serveur RADIUS avec Identifiant-de-NAS, Accès-de-NAS, Nom-d'utilisateur, Mot-de-passe-d'utilisateur (qui peut être simplement une chaîne comme "épreuve" ou ignoré). Le serveur renvoie un paquet Défi-d'accès avec État et un Message-de-réponse ainsi que les lignes de "Défi 12345678, entrer votre réponse à l'invite" que le NAS affiche. Le NAS invite à la réponse et envoie une NOUVELLE Demande d'accès au serveur (avec un nouvel identifiant) avec Identifiant-de-NAS, Accès-de-NAS, Nom-d'utilisateur, Mot-de-passe-d'utilisateur (la réponse qui vient d'être entrée par l'utilisateur, chiffrée), et le même attribut État qui est venu avec le Défi-d'accès. Le serveur renvoie alors un Accès-Accepté ou un Rejet-d'accès selon que la réponse correspond à la valeur requise ou non, ou il peut même envoyer une autre Défi-d'accès.

2.2 Interfonctionnement de PAP et CHAP

Pour PAP, le NAS prend l'identifiant et le mot de passe PAP et les envoie dans un paquet Demande d'accès comme Nom-d'utilisateur et Mot-de-passe-d'utilisateur. Le NAS PEUT inclure les attributs Type-de-Service = Usager-tramé et Protocole-tramé = PPP comme conseil au serveur RADIUS que le service PPP est attendu.

Pour CHAP, le NAS génère une épreuve aléatoire (de préférence de 16 octets) et l'envoie à l'utilisateur, qui retourne une réponse CHAP avec un identifiant CHAP et un nom d'utilisateur CHAP. Le NAS envoie alors un paquet de Demande d'accès au serveur RADIUS avec le nom d'utilisateur CHAP comme Nom-d'utilisateur et avec l'identifiant CHAP et la réponse CHAP comme mot de passe CHAP (Attribut 3). L'épreuve aléatoire peut être incluse dans l'attribut Défi-CHAP ou, si elle est longue de 16 octets, elle peut être placée dans le champ Authentificateur de demande du paquet de Demande d'accès. Le NAS PEUT inclure les attributs Type-de-Service = Usager-tramé et Protocole-tramé = PPP comme conseil au serveur RADIUS que le service PPP est attendu.

Le serveur RADIUS cherche un mot de passe fondé sur le Nom-d'utilisateur, chiffre l'épreuve en utilisant MD5 sur l'octet d'identifiant CHAP, ce mot de passe, et l'épreuve CHAP (d'après l'attribut Défi-CHAP s'il est présent, et autrement d'après l'authentificateur de demande), et compare ce résultat au mot de passe CHAP. Si ils correspondent, le serveur renvoie un Accès-Accepté, autrement, il renvoie un Rejet-d'accès.

Si le serveur RADIUS n'est pas capable d'effectuer l'authentification demandée, il DOIT retourner un Rejet-d'accès. Par exemple, CHAP exige que le mot de passe de l'utilisateur soit disponible en clair pour le serveur de façon qu'il puisse chiffrer l'épreuve CHAP et comparer cela à la réponse CHAP. Si le mot de passe n'est pas disponible en clair pour le serveur RADIUS, le serveur DOIT alors envoyer un Rejet-d'accès au client.

2.3 Mandataire

Avec un mandataire RADIUS, un serveur RADIUS reçoit une demande d'authentification (ou de comptabilité) d'un client RADIUS (comme un NAS), transmet la demande à un serveur RADIUS distant, reçoit la réponse du serveur distant, et

envoie cette réponse au client, éventuellement avec des changements pour refléter la politique administrative locale. Une utilisation courante pour un mandataire RADIUS est l'itinérance. L'itinérance permet à deux entités administratives ou plus de d'autoriser leurs utilisateurs réciproques à appeler dans le réseau de l'autre entité pour le service.

Le NAS envoie sa demande d'accès RADIUS au "serveur de transmission" qui la transmet au "serveur distant". Le serveur distant renvoie sa réponse (Accès-Accepté, Rejet-d'accès, ou Défi-d'accès) au serveur de transmission, qui la renvoie au NAS. L'attribut Nom-d'utilisateur PEUT contenir un Identifiant d'accès réseau [8] pour les opérations de mandataire RADIUS. Le choix du serveur qui reçoit la demande retransmise DEVRAIT être fondé sur le "domaine" d'authentification. Le domaine d'authentification PEUT être la partie domaine d'un identifiant d'accès réseau (un "domaine nommé"). Autrement, le choix du serveur qui reçoit la demande retransmise PEUT être fondé sur tout autre critère que le serveur de retransmission est configuré à utiliser, comme un identifiant de station appelée (un "domaine numéroté").

Un serveur RADIUS peut fonctionner à la fois comme serveur de transmission et comme serveur distant, servant de serveur de transmission pour certains domaines et de serveur distant pour d'autres domaines. Un serveur de transmission peut agir comme transmetteur pour un nombre quelconque de serveurs distants. Un serveur distant peut avoir un nombre quelconque de serveurs qui lui transmettent et peut fournir l'authentification pour un nombre quelconque de domaines. Un serveur de transmission peut transmettre à un autre serveur de transmission pour créer une chaîne de mandataires, mais il faut alors prendre soin d'éviter d'introduire des boucles.

Le scénario suivant illustre une communication de mandataire RADIUS entre un NAS et les serveurs RADIUS distant et de transmission :

- 1 Un NAS envoie sa demande d'accès au serveur de transmission.
- 2 Le serveur de transmission passe la demande d'accès au serveur distant.
- 3 Le serveur distant renvoie une acceptation d'accès, un rejet d'accès ou un défi-d'accès au serveur de transmission. Pour cet exemple, une acceptation d'accès est envoyée.
4. Le serveur de transmission envoie l'acceptation d'accès au NAS.

Le serveur de transmission DOIT traiter tout attribut État de mandataire déjà présent dans le paquet comme données opaques. Son fonctionnement NE DOIT PAS dépendre du contenu des attributs État de mandataire ajoutés par les serveurs précédents.

Si il y a déjà des attributs État de mandataire dans la demande reçue du client, le serveur de transmission DOIT inclure ces États de mandataire dans sa réponse au client. Le serveur de transmission PEUT inclure les attributs État de mandataire dans la demande d'accès quant il transmet la demande, ou PEUT les omettre dans la demande transmise. Si le serveur de transmission omet les attributs État de mandataire dans la demande d'accès transmise, il DOIT les rattacher à la réponse avant de l'envoyer au client. Nous allons examiner chaque étape plus en détail.

1. Un NAS envoie sa demande d'accès au serveur de transmission. Le serveur de transmission déchiffre le Mot-de-passe-d'utilisateur, s'il est présent, en utilisant le secret partagé qu'il connaît pour le NAS. Si un attribut Mot de passe CHAP est présent dans le paquet et qu'aucun attribut Défi-CHAP n'est présent, le serveur de transmission DOIT laisser le Authentificateur-de-demande inchangé ou le copier dans un attribut Défi-CHAP.

Le serveur de transmission PEUT ajouter un attribut État de mandataire au paquet. (Il NE DOIT PAS en ajouter plus d'un.) Si il ajoute un État de mandataire, l'État de mandataire DOIT apparaître après tous les autres État de mandataire dans le paquet. Le serveur de transmission NE DOIT PAS modifier un autre État de mandataire présent dans le paquet (il peut choisir de ne pas les transmettre, mais il NE DOIT PAS changer leur contenu). Le serveur de transmission NE DOIT PAS changer l'ordre d'un attribut du même type, y compris État de mandataire.

2. Le serveur de transmission chiffre le Mot-de-passe-d'utilisateur, s'il est présent, en utilisant le secret qu'il partage avec le serveur distant, règle l'identifiant comme nécessaire, et transmet la demande d'accès au serveur distant.
3. Le serveur distant (s'il est la destination finale) vérifie l'usager en utilisant le Mot-de-passe-d'utilisateur, le Mot de passe CHAP, ou telle méthode que des extensions futures pourraient imposer, et retourne une acceptation d'accès, un rejet d'accès ou un Défi-d'accès au serveur de transmission. Pour cet exemple, une acceptation d'accès est envoyée. Le serveur distant DOIT copier tous les attributs État de mandataire (et seulement les attributs État de mandataire) dans l'ordre de la demande d'accès sur le paquet de réponse, sans les modifier.
4. Le serveur de transmission vérifie l'authentificateur de réponse en utilisant le secret qu'il partage avec le serveur distant, et élimine en silence le paquet s'il échoue à la vérification. Si le paquet réussit la vérification, le serveur de

transmission retire le dernier État de mandataire (s'il en avait accroché un), signe l'authentificateur de réponse en utilisant le secret qu'il partage avec le NAS, restaure l'identifiant pour qu'il corresponde à celui de la demande d'origine par le NAS, et envoie l'acceptation d'accès au NAS.

Un serveur de transmission PEUT avoir besoin de modifier des attributs pour mettre en application une politique locale. Une telle politique sort du domaine d'application du présent document, avec les restrictions suivantes. Un serveur de transmission NE DOIT PAS modifier des attributs État de mandataire, État, ou Classe existants présents dans le paquet.

Les mises en œuvre de serveur de transmissions devraient considérer avec attention quelles valeurs elles veulent accepter pour Type-de-Service. Une considération attentive doit être apportée aux effets du passage du Type-de-Services Invite de NAS ou Administratif dans un Accès-Accepté mandaté, et les mises en œuvre peuvent souhaiter fournir des mécanismes pour bloquer ces types de service, ou d'autres attributs. De tels mécanismes sortent du domaine d'application du présent document.

2.4 Pourquoi UDP ?

Une question fréquemment posée est pourquoi RADIUS utilise UDP au lieu de TCP comme protocole de transport ?. UDP a été choisi pour des raisons strictement techniques.

Plusieurs problèmes doivent être bien compris. RADIUS est un protocole fondé sur la transaction qui a plusieurs caractéristiques intéressantes :

1. Si la demande à un serveur d'authentification primaire échoue, un serveur secondaire doit être interrogé. Pour satisfaire cette exigence, une copie de la demande doit être conservée au dessus de la couche transport pour permettre une transmission de remplacement. Cela signifie que les temporisateurs de retransmission sont toujours nécessaires.
2. Les exigences de temporisation de ce protocole particulier sont significativement différentes de celles fournies par TCP. À une extrémité, RADIUS n'exige pas une détection "sensible" de la perte de données. L'utilisateur 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'utilisateur 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'utilisateur d'obtenir l'accès avant d'abandonner.
3. La nature sans état de ce protocole simplifie l'utilisation de UDP. Les clients et les serveurs vont et viennent. Les systèmes sont réamorçés, ou sont alimentés de façon indépendante. Généralement cela ne pose pas de problème et avec des temporisations créatives et la détection de la perte des connexions TCP, le code peut être écrit pour faire face à des événements anormaux. UDP élimine complètement tous ces traitements particuliers. Chaque client et serveur peut n'ouvrir son transport UDP qu'une seule fois et le laisser ouvert malgré toutes sortes de types de défaillances survenant sur le réseau.
4. UDP simplifie la mise en œuvre du serveur. Dans les premières mises en œuvre de RADIUS, le serveur avait un seul fil. Cela signifie qu'une seule demande était reçue, traitée, et retournée. Cela s'est révélé ingérable dans des environnements où le mécanisme de sécurité de l'extrémité arrière prenait un temps réel (une ou plusieurs secondes). La file d'attente de demande du serveur se serait remplie et dans des environnements où des centaines de gens sont authentifiés à chaque minute, le temps d'aller-retour de la demande s'accroît bien plus que ce que les usagers acceptent d'attendre (c'était particulièrement sévère lorsqu'une recherche spécifique dans une base de données ou sur DNS prenait 30 secondes ou plus). La solution évidente était de rendre le serveur multi fils. C'était simple à faire avec UDP. Des processus distincts sont générés pour servir chaque demande et ces processus peuvent répondre directement au NAS client avec un simple paquet UDP sur le transport d'origine du client.

Ceci n'est pas une panacée. Comme on l'a noté, utiliser UDP exige une chose qui est incorporée dans TCP : avec UDP, on doit artificiellement gérer des temporisateurs de retransmission sur le même serveur, bien qu'ils n'exigent pas la même attention que les temporisations fournies par TCP. Ce seul inconvénient est un faible prix à payer pour les avantages d'UDP dans ce protocole.

Sans TCP, on en serait probablement toujours à utiliser des boîtes de conserve reliées par un bout de ficelle. Mais pour ce protocole particulier, UDP est un meilleur choix.

2.5 Conseils de retransmission

Si le serveur RADIUS et le serveur RADIUS de remplacement partagent le même secret, il n'y a pas de problème pour retransmettre le paquet au serveur RADIUS de remplacement avec les mêmes identifiant et authentificateur de demande, parce que le contenu des attributs n'est pas changé. Si on veut utiliser un nouvel authentificateur de demande lors de l'envoi au serveur de remplacement, on le peut.

Si on change le contenu de l'attribut Mot-de-passe-d'utilisateur (ou de tout autre attribut), on a besoin d'un nouvel authentificateur de demande et donc d'un nouvel identifiant.

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 authentificateur de demande, le même identifiant, et le même accès de source. Si un des attributs a changé, on DOIT utiliser un nouvel authentificateur de demande et un nouvel identifiant.

Un NAS PEUT utiliser le même identifiant sur tous les serveurs, ou PEUT garder trace des identifiants séparément pour chaque serveur, selon le choix de la mise en œuvre. Si un NAS a besoin de plus de 256 identifiants pour les demandes en cours, il PEUT utiliser des accès de source supplémentaires à partir desquels envoyer des demandes, et garder trace des identifiants pour chaque accès de source. Cela permet jusqu'à 16 millions de demandes simultanées sur un seul serveur.

2.6 Maintiens en vie considérés comme dommageables

Certaines mises en œuvre ont adopté la pratique d'envoyer des demandes RADIUS pour voir si un serveur est toujours actif. Cette pratique est fortement déconseillée, car elle ajoute une charge et nuit à la modularité sans apporter aucune information utile supplémentaire. Comme une demande RADIUS est contenue dans un seul datagramme, le temps qu'il faudrait pour envoyer un ping permet d'envoyer la demande RADIUS, et la réponse vous dit que le serveur RADIUS est actif. Si on n'a pas de demande RADIUS à envoyer, on ne se soucie pas de savoir si le serveur est actif ou non, puisqu'on ne l'utilise pas.

Si on veut surveiller son serveur RADIUS, il faut utiliser SNMP. C'est à cela que sert SNMP.

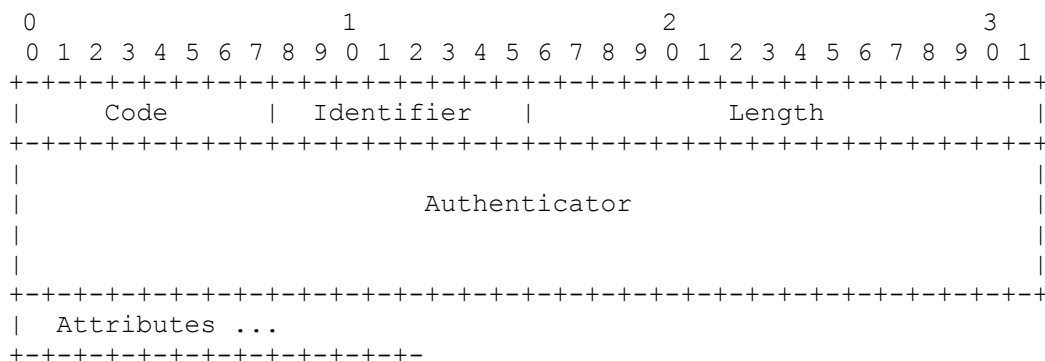
3 Format de paquet

Exactement un paquet RADIUS est encapsulé dans le champ de données UDP [4], et le champ Accès de destination UDP indique 1812 (en décimal).

Lorsque une réponse est générée, les accès de source et de destination sont inversés.

Le présent mémo expose le protocole RADIUS. Les premiers développements de RADIUS utilisaient le numéro d'accès UDP 1645, qui est en conflit avec le service "datametrics". Le numéro d'accès officiellement alloué pour RADIUS est 1812.

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



Code

Le champ Code est d'un octet, et il identifie le type de paquet RADIUS. Lorsque un paquet est reçu avec un champ de code invalide, il est éliminé en silence.

Les codes RADIUS (décimaux) sont alloués comme suit :

1	Accès-demandé
2	Accès-accepté
3	Accès-rejeté
4	Demande-comptable
5	Réponse-comptable
11	Défi-d'accès
12	État-du-serveur (expérimental)
13	État-du-client (expérimental)
255	Réservé

Les codes 4 et 5 sont traités dans le document de comptabilité RADIUS [5]. Les codes 12 et 13 sont réservés pour une utilisation possible, mais ne seront plus mentionnés plus loin.

Identifiant

Le champ Identifiant est de un octet, et sert à faire correspondre demandes et réponses. 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.

Longueur

Le champ Longueur est de 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 minimale est 20 et la longueur maximale 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 la réponse provenant du serveur RADIUS, et sert dans l'algorithme de dissimulation du mot de passe.

Authentificateur de demande

Dans les paquets de demande d'accès, la valeur de l'authentificateur est un nombre aléatoire de 16 octets, appelé l'authentificateur de demande. La valeur DEVRAIT être imprévisible et unique sur la durée de vie d'un secret (le mot de passe partagé entre le client et le serveur RADIUS) car la répétition de la valeur de demande conjuguée au même secret permettrait à un attaquant de répondre avec une réponse précédemment interceptée. Comme il est prévu que le même secret PEUT être utilisé pour s'authentifier auprès de serveurs de régions géographiques diverses, le champ Authentificateur de demande DEVRAIT posséder une unicité mondiale et temporelle.

La valeur de l'authentificateur de demande dans un paquet de demande d'accès DEVRAIT aussi être imprévisible, de crainte qu'un attaquant ne trompe un serveur en répondant à une demande future prédite, et utilise alors la réponse pour se faire passer pour ce serveur lors d'une future demande d'accès.

Bien que des protocoles tels que RADIUS soient incapables de protéger contre le vol d'une session authentifiée via des attaques d'espionnage actif en temps réel, la génération d'une demande unique imprévisible peut protéger contre une large gamme d'attaques actives sur l'authentification.

Le NAS et le serveur RADIUS partagent un secret. Ce secret partagé suivi par l'authentificateur de demande est passé par un hachage MD5 unidirectionnel pour créer une valeur de résumé de 16 octets qui est combinée par opérateur OUX avec le mot de passe entré par l'utilisateur, et le résultat de la combinaison par opérateur OUX est placé dans l'attribut Mot-de-passe-d'utilisateur dans le paquet de demande d'accès. Voir l'entrée pour Mot-de-passe-d'utilisateur dans le paragraphe sur les attributs pour une description plus détaillée.

Authentificateur de réponse

La valeur du champ Authentificateur dans les paquets Accès-Accepté, Rejet-d'accès, et Défi-d'accès est appelée l'authentificateur de réponse, et contient un hachage MD5 unidirectionnel calculé sur un flux d'octets consistant en : le paquet RADIUS, commençant par le champ Code, incluant les champs Identifiant, Longueur, Authentificateur de demande tiré du paquet Demande d'accès, et les attributs de réponse, suivis par le secret partagé. C'est-à-dire que ResponseAuth =

MD5(Code+ID+Longueur+RequestAuth+Attributs+Secret) où + note l'enchaînement.

Note administrative

Le secret (mot de passe partagé entre le client et le serveur RADIUS) DEVRAIT être au moins aussi long et aussi imprévisible qu'un mot de passe bien choisi. Il est préférable que le secret soit d'au moins 16 octets. Cela pour s'assurer d'une gamme suffisamment grande pour que le secret fournisse une protection contre des attaques de recherche exhaustive. Le secret NE DOIT PAS être vide (longueur 0) car cela permettrait une falsification triviale des paquets.

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.

Lors de l'utilisation d'un mandataire de transmission, le mandataire doit être capable de modifier le paquet lorsqu'il passe dans chaque direction – lorsque le mandataire transmet la demande, le mandataire PEUT ajouter un attribut État-de-mandataire, et lorsque le mandataire transmet une réponse, il DOIT retirer son attribut État-de-mandataire s'il en a ajouté un. État-de-mandataire est toujours ajouté ou retiré après tout autre État-de-mandataire, mais aucune autre hypothèse concernant sa localisation au sein de la liste des attributs ne peut être faite. Comme les réponses Accès-Accepté et Rejet-d'accès sont authentifiées sur le contenu du paquet entier, l'effacement de l'attribut État-de-mandataire invalide la signature dans le paquet – aussi le mandataire doit-il le re-signer.

Les précisions sur la mise en œuvre du mandataire RADIUS sortent du domaine d'application du présent document.

4 Types de paquet

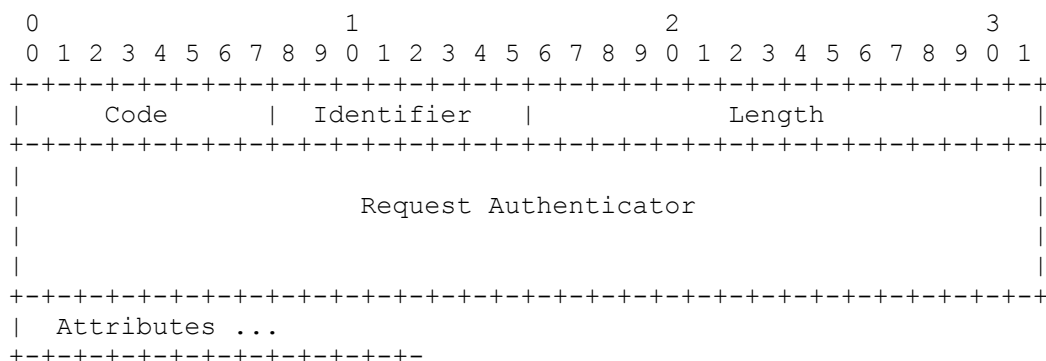
Le type de paquet RADIUS est déterminé par le champ Code dans le premier octet du paquet.

4.1 Demande d'accès

Description

Les paquets de demande d'accès sont envoyés à un serveur RADIUS, et portent des informations utilisées pour déterminer si un usager est autorisé en accès sur un NAS spécifique, et tous les services particuliers demandés pour cet usager. Une mise en œuvre qui souhaite authentifier un usager DOIT transmettre un paquet RADIUS avec le champ Code mis à 1 (Demande d'accès). À réception d'une demande d'accès provenant d'un client valide, une réponse appropriée DOIT être transmise. Une demande d'accès DEVRAIT contenir un attribut Nom-d'utilisateur. Elle DOIT contenir un attribut Adresse-IP-de-NAS ou un attribut Identifiant-de-NAS (ou les deux). Une demande d'accès DOIT contenir un Mot-de-passe-d'utilisateur ou 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 de futures extensions permettent que d'autres sortes d'informations d'authentification soient convoyées, l'attribut pour cela pourra être utilisé dans une demande d'accès au lieu d'un Mot-de-passe-d'utilisateur ou Mot-de-passe-CHAP. Une demande d'accès DEVRAIT contenir un attribut Accès-de-NAS ou Type-d'Accès-de-NAS ou les deux à moins que le type d'accès demandé n'implique pas un accès ou que le NAS ne fasse pas de distinction entre ses accès. Une demande d'accès PEUT contenir des attributs supplémentaires comme conseil au serveur, mais le serveur n'est pas obligé de suivre le conseil. Lorsque un Mot-de-passe-d'utilisateur est présent, il est caché en utilisant une méthode fondée sur l'algorithme RSA de résumé de message MD5 [3].

Un résumé du format de paquet de demande d'accès est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Code : 1 pour Demande-d'accès.

Identifiant

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

Authentificateur de demande

La valeur de l'authentificateur de demande DOIT être changée chaque fois qu'un nouvel identifiant est utilisé.

Attributs

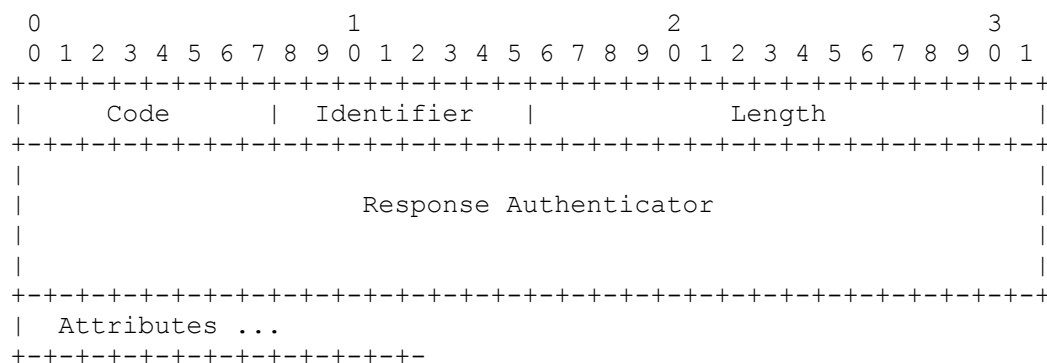
Le champ Attributs est de longueur variable, et contient la liste des attributs qui sont requis pour le type de service, ainsi que de tout attribut facultatif désiré.

4.2 Accès-Accepté

Description

Les paquets Accès-Accepté sont envoyés par le serveur RADIUS, et fournissent les informations spécifiques de configuration nécessaires pour commencer la livraison du service à l'utilisateur. Si toutes les valeurs d'attribut reçues dans une demande d'accès sont acceptables, la mise en œuvre RADIUS DOIT alors transmettre un paquet avec le champ Code mis à 2 (Accès-Accepté). À réception d'un Accès-Accepté, le champ Identifiant est confronté à une demande d'accès en instance. Le champ Authentificateur de réponse DOIT contenir la réponse correcte pour la demande d'accès en instance. Les paquets invalides sont éliminés en silence.

Un résumé du format de paquet Accès-Accepté est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Code : 2 pour Accès-Accepté.

Identifiant

Le champ Identifiant est une copie du champ Identifiant de la demande d'accès qui a causé cet Accès-Accepté.

Authentificateur de réponse

La valeur de l'authentificateur de réponse est calculée d'après la valeur de la demande d'accès, comme décrit plus haut.

Attributs

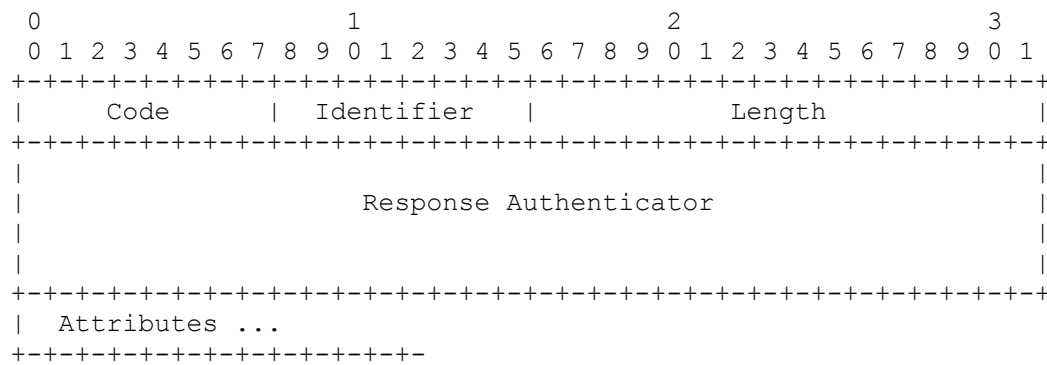
Le champ Attributs est de longueur variable, et contient une liste de zéro, un ou plusieurs attributs.

4.3 Rejet-d'accès

Description

Si une valeur quelconque des attributs reçus n'est pas acceptable, le serveur RADIUS DOIT alors transmettre un paquet avec le champ Code mis à 3 (Rejet-d'accès). Il PEUT inclure un ou plusieurs attributs Message-de-réponse avec un texte de message que le NAS PEUT afficher à l'utilisateur.

Un résumé du format de paquet Rejet-d'accès est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Code : 3 pour Rejet-d'accès.

Identifiant

Le champ Identifiant est une copie du champ Identifiant de la demande d'accès qui a causé ce Rejet-d'accès.

Authentificateur de réponse

La valeur de l'authentificateur de réponse est calculée d'après la valeur de la demande d'accès, comme décrit plus haut.

Attributs

Le champ Attribut est de longueur variable, et contient une liste de zéro, un ou plusieurs attributs.

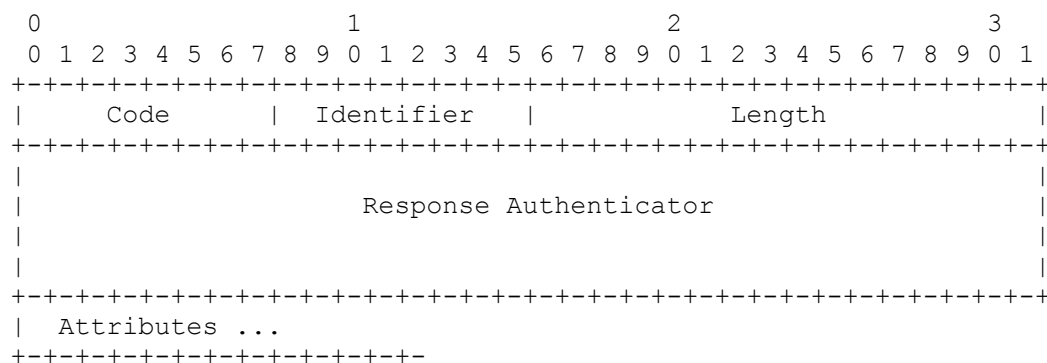
4.4 Défi-d'accès

Description

Si le serveur RADIUS désire envoyer à l'utilisateur une épreuve exigeant une réponse, le serveur RADIUS DOIT alors répondre à la demande d'accès en transmettant un paquet avec le champ Code mis à 11 (Défi-d'accès). Le champ Attributs PEUT avoir un ou plusieurs attributs Message-de-réponse, et PEUT avoir un seul attribut État, ou aucun. Les attributs Spécifique-du-fabricant, Durée-d'inactivité, Durée-de-session et État de mandataire PEUVENT aussi être inclus. Aucun autre attribut défini dans le présent document n'est permis dans un Défi-d'accès. À réception d'un Défi-d'accès, le champ Identifiant est confronté à une Demande d'accès en instance. De plus, le champ Authentificateur de réponse DOIT contenir la réponse correcte pour la Demande d'accès en instance. Les paquets invalides sont éliminés en silence. 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. Si le NAS accepte le défi/réponse, la réception d'un Défi-d'accès valide indique qu'une nouvelle Demande d'accès DEVRAIT être envoyée. Le NAS PEUT afficher le texte du message, s'il en est, à l'utilisateur, et inviter ensuite l'utilisateur à une réponse. Il envoie alors sa demande d'accès originale avec un nouvel identifiant de demande et authentificateur de demande, avec l'attribut Mot-de-passe-d'utilisateur remplacé par la réponse de l'utilisateur (chiffrée), et incluant l'attribut État tiré de Défi-d'accès, s'il en est. Seule 0 ou 1 instance de l'attribut État peut être présente dans une demande d'accès.

Un NAS qui accepte PAP PEUT transmettre le Message-de-réponse au client appelant et accepter une réponse PAP qu'il peut utiliser comme si l'utilisateur avait entré la réponse. Si le NAS ne peut faire ainsi, il DOIT traiter le Défi-d'accès comme si il avait reçu un Rejet-d'accès à la place.

Un résumé du format de paquet Défi-d'accès est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Code : 11 pour Défi-d'accès.

Identifiant
Le champ Identifiant est une copie du champ Identifiant de la demande d'accès qui a causé cette Défi-d'accès.

Authentificateur de réponse
La valeur de l'authentificateur de réponse est calculée à partir de la valeur de la demande d'accès, comme décrit plus haut.

Attributs
Le champ Attributs est de longueur variable, et contient une liste de zéro, un ou plusieurs attributs.

5 Attributs

Les attributs RADIUS portent les détails spécifiques d'authentification, d'autorisation, d'information et de configuration pour la demande et la réponse.

La fin de la liste des attributs est indiquée par la longueur du paquet RADIUS.

Certains attributs PEUVENT être inclus plus d'une fois. L'effet de cette répétition est spécifique de l'attribut, et est spécifié dans chaque description d'attribut. Un tableau de récapitulation est fourni à la fin de la section "Attributs".

Si plusieurs attributs de même type sont présents, l'ordre des attributs de même type DOIT être conservé par tout mandataire. L'ordre des attributs de type différent ne doit pas obligatoirement être conservé. Un serveur ou client RADIUS NE DOIT PAS dépendre de l'ordre des attributs des différents types. Un serveur ou client RADIUS NE DOIT PAS exiger que des attributs du même type soient contigus.

Lorsque une description d'attribut limite dans quelle sorte de paquet elle peut être contenue, cela ne s'applique qu'aux types de paquets définis dans le présent document, à savoir Demande d'accès, Accès-Accepté, Rejet-d'accès et Défi-d'accès (Codes 1, 2, 3, et 11). D'autres documents définissant d'autres types de paquet peuvent aussi utiliser les attributs décrits ici. Pour déterminer quels attributs sont permis dans les paquets Demande-de-comptabilité et Réponse-de-comptabilité (Codes 4 et 5) se reporter au document sur la comptabilité RADIUS [5].

De même, lorsque les types de paquet définis ici établissent que seuls certains attributs sont permis avec eux, des documents futurs définissant de nouveaux attributs devraient indiquer dans quels types de paquet les nouveaux attributs peuvent être présents.

Un résumé du format d'attribut est indiqué ci-dessous. Les champs sont transmis de gauche à droite.

```

      0                               1                               2
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |                               |                               |
  |      Type                     |      Length                 |      Value ...
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type
Le champ Type est d'un octet. Les valeurs mises à jour du champ Type de RADIUS sont spécifiées dans la RFC des "Numéros alloués" [6] la plus récente. Les valeurs 192 à 223 sont réservée pour des utilisations expérimentales, les valeurs 224 à 240 sont réservées pour des utilisations spécifiques d'une mise en œuvre, et les valeurs 241 à 255 sont réservées et ne devraient pas être utilisées.

Un serveur RADIUS PEUT ignorer les attributs ayant un Type inconnu.

Un client RADIUS PEUT ignorer les attributs ayant un Type inconnu.

La présente spécification concerne les valeurs suivantes :

1	Nom-d'utilisateur
2	Mot-de-passe-d'utilisateur
3	Mot-de-passe-CHAP
4	Adresse-IP-de-NAS
5	Accès-de-NAS

6	Type-de-Service
7	Protocole-tramé
8	Adresse-IP-tramée
9	Gabarit-de-réseau-IP-tramé
10	Routage-tramé
11	Identifiant-de-filtre
12	MTU-tramée
13	Compression-tramée
14	Hôte-de-Connexion-IP
15	Service-de-Connexion
16	Accès-de-connexion-TCP
17	(non alloué)
18	Message-de-réponse
19	Numéro-de-rappel
20	Identifiant-de-rappel
21	(non alloué)
22	Route-tramée
23	Réseau-IPX-tramé
24	État
25	Classe
26	Spécifique-du-fabricant
27	Durée-de-session
28	Durée-d'inactivité
29	Action-de-terminaison
30	Identifiant-de-station-appelée
31	Identifiant-de-station-appelante
32	Identifiant-de-NAS
33	État de mandataire
34	Service-de-connexion-LAT
35	Noeud-de-connexion-LAT
36	Groupe-de-connexion-LAT
37	Liaison-AppleTalk-tramée
38	Réseau-AppleTalk-tramé
39	Zone-AppleTalk-tramée
40-59	(réservé pour la comptabilité)
60	Défi-CHAP
61	Type-d'accès-de-NAS
62	Limite-d'accès
63	Accès-de-connexion-LAT

Longueur

Le champ Longueur est d'un octet, et indique la longueur de cet attribut y compris les champs Type, Longueur et Valeur. Si un attribut est reçu dans une demande d'accès mais avec une longueur invalide, un Rejet-d'accès DEVRAIT être transmis. Si un attribut est reçu dans un paquet Accès-Accepté, Rejet-d'accès ou Défi-d'accès avec une longueur invalide, le paquet DOIT être traité comme un Rejet-d'accès ou autrement être éliminé en silence.

Valeur

Le champ Valeur est de zéro, un ou plusieurs octets et contient des informations spécifiques de l'attribut. Le format et la longueur du champ Valeur sont déterminés par les champs Type et Longueur.

Noter qu'aucun des types dans RADIUS ne se termine par un NUL (hex 00). En particulier, les types "texte" et "chaîne" dans RADIUS ne se terminent pas par NUL (hex 00). L'attribut a un champ Longueur et n'utilise pas de terminaison. Texte contient caractères ISO 10646 codés en UTF-8 [7] et Chaîne contient des données binaires de 8 bits. Les serveurs et les clients DOIVENT être capables de traiter les nuls incorporés. Les mises en œuvre de RADIUS qui utilisent le langage C devraient veiller à ne pas utiliser strcpy() dans le traitement des chaînes.

Le format du champ Valeur est un parmi cinq types de données. Noter que le type "texte" est un sous-ensemble du type "chaîne".

texte 1 à 253 octets contenant des caractères ISO 10646 codés en UTF-8 [7]. Un texte de longueur zéro (0) NE DOIT

page - 15 -

La méthode est tirée du livre "Network Security" de Kaufman, Perlman et Speciner [9] pages 109-110. Une explication plus précise de la méthode suit :

Appelons S le secret partagé et RA l'authentificateur de demande pseudo aléatoire de 128 bits. Coupons le mot de passe en tranches de 16 octets p1, p2, etc. avec le dernier bourré à la fin avec des zéros jusqu'à une frontière de 16 octets. Appelons les blocs de texte chiffré c(1), c(2), etc. Nous aurons besoin de valeurs intermédiaires b1, b2, etc.

b1 = MD5(S + RA) c(1) = p1 xor b1
b2 = MD5(S + c(1)) c(2) = p2 xor b2

·
·
·

b_i = MD5(S + c(i-1)) c(i) = p_i xor b_i

La chaîne va contenir c(1)+c(2)+...+c(i) où + marque l'enchaînement.

À réception, le processus est inversé pour donner le mot de passe original.

Un résumé du format de l'attribut Mot-de-passe-d'utilisateur est indiqué ci-dessous. Les champs sont transmis de gauche à droite.

```

      0                               1                               2
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|      Type      |      Length      |      String ...
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+

```

Type : 2 pour Mot-de-passe-d'utilisateur.

Longueur : Au moins 18 et pas plus de 130.

Chaîne : Le champ Chaîne est entre 16 et 128 octets de long, inclus.

5.3 Mot de passe CHAP

Description

Cet attribut indique la valeur de réponse fournie par un utilisateur du protocole d'authentification par dialogue à énigme (CHAP, *Challenge-Handshake Authentication Protocol*) PPP en réponse à l'épreuve. Il n'est utilisé que dans les paquets de demande d'accès.

La valeur de l'épreuve CHAP est trouvée dans l'attribut Défi-CHAP (60) s'il est présent dans le paquet, autrement, dans le champ authentificateur de demande.

Un résumé du format de l'attribut Mot de passe CHAP est indiqué ci-dessous. Les champs sont transmis de gauche à droite.

```

      0                               1                               2
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|      Type      |      Length      |  CHAP Ident  |      String ...
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+

```

Type : 3 pour Mot de passe CHAP.

Longueur : 19

Ident. CHAP

Ce champ est d'un octet, et contient l'identifiant CHAP provenant de la réponse CHAP de l'utilisateur.

Chaîne : Le champ Chaîne est de 16 octets, et contient la réponse CHAP de l'utilisateur.

5.4 Adresse-IP-NAS

Description

Cet attribut indique l'adresse IP qui identifie le NAS qui demande l'authentification de l'utilisateur, et DEVRAIT être unique au NAS dans le domaine d'application du serveur RADIUS. Adresse-IP-NAS n'est utilisé que dans les paquets de demande d'accès. Adresse-IP-NAS ou Identifiant-de-NAS DOIT être présent dans un paquet de demande d'accès.

Noter que Adresse-IP-NAS NE DOIT PAS être utilisé pour choisir le secret partagé qui sert à authentifier la demande. L'adresse IP de source du paquet de demande d'accès DOIT être utilisée pour choisir le secret partagé.

Un résumé du format de l'attribut Adresse-IP-NAS est donné ci-dessous. Les champs sont transmis de gauche à droite.

```

      0               1               2               3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|      Type      |      Length      |      Address      |
+-----+-----+-----+-----+-----+-----+-----+-----+
|      Address (cont)      |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Type : 4 pour Adresse-IP-NAS.

Longueur : 6

Adresse : Le champ Adresse est de quatre octets.

5.5 Accès-de-NAS

Description

Cet attribut indique le numéro de l'accès physique du NAS qui authentifie l'utilisateur. Il n'est utilisé que dans les paquets de demande d'accès. Noter que cela utilise "accès" au sens d'une connexion physique avec le NAS, et non au sens d'un numéro d'accès TCP ou UDP. Accès-de-NAS ou Type-d'Accès-de-NAS (61), ou les deux, DEVRAIT être présent dans un paquet de demande d'accès, si le NAS fait une différenciation parmi ses accès.

Un résumé du format de l'attribut Accès-de-NAS est indiqué ci-dessous. Les champs sont transmis de gauche à droite.

```

      0               1               2               3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|      Type      |      Length      |      Value      |
+-----+-----+-----+-----+-----+-----+-----+-----+
|      Value (cont)      |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Type : 5 pour Accès-de-NAS .

Longueur : 6

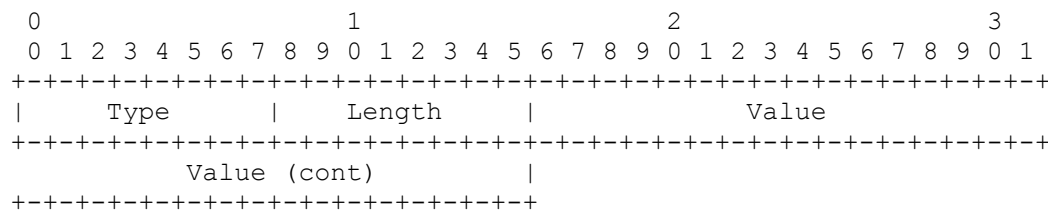
Valeur : Le champ Valeur est de quatre octets.

5.6 Type-de-Service

Description

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 obligé de mettre en œuvre tous ces types de service, et DOIT traiter les types de service inconnus ou non pris en charge comme si un Rejet-d'accès avait été reçu à la place.

Un résumé du format de l'attribut Type-de-Service est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 6 pour Type-de-Service.

Longueur : 6

Valeur : Le champ Valeur est de quatre octets.

- | | |
|----|-------------------------|
| 1 | Connexion |
| 2 | Tramé |
| 3 | Connexion de rappel |
| 4 | Rappel tramé |
| 5 | Sortant |
| 6 | Administratif |
| 7 | Invite de NAS |
| 8 | Authentification seule |
| 9 | Invite de rappel de NAS |
| 10 | Vérification d'appel |
| 11 | Rappel administratif |

Les types de service sont définis comme suit lorsqu'ils sont utilisés dans Accès-Accepté. Lorsqu'ils sont utilisés dans Demande d'accès, ils PEUVENT être considérés comme des conseils au serveur RADIUS que le NAS a des raison de penser que l'utilisateur préférerait le type de service indiqué, mais le serveur n'est pas obligé de suivre le conseil.

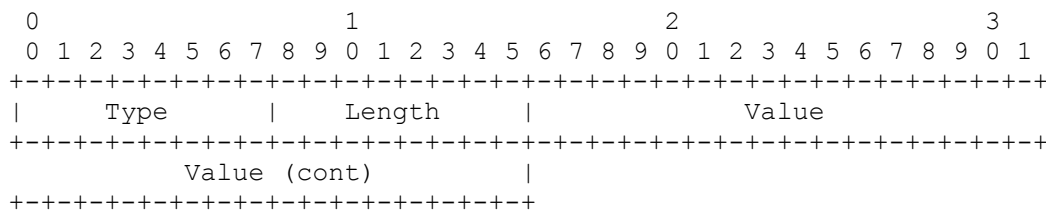
Connexion	L'utilisateur devrait être connecté à un hôte.
Tramé	Un protocole tramé devrait être lancé pour l'utilisateur, tel que PPP ou SLIP.
Connexion de rappel	L'utilisateur devrait être déconnecté et rappelé, puis connecté à un hôte.
Rappel tramé	L'utilisateur devrait être déconnecté et rappelé, puis un protocole tramé devrait être lancé pour l'utilisateur, tel que PPP ou SLIP.
Sortant	L'utilisateur devrait recevoir l'accès aux appareils de sortie.
Administratif	L'utilisateur devrait recevoir l'accès à l'interface administrative avec le NAS à partir de laquelle des commandes privilégiées peuvent être exécutées.
Invite de NAS	L'utilisateur devrait recevoir une invite de commandes sur le NAS à partir duquel des commandes non privilégiées peuvent être exécutées.
Authentification seule	Seule l'authentification est demandée, et aucune information d'autorisation n'a besoin d'être retournée dans Accès-Accepté (normalement utilisé par les serveurs mandataires plutôt que par le NAS lui-même).
Invite de rappel de NAS	L'utilisateur devrait être déconnecté et rappelé, puis pourvu d'une invite de commande sur le NAS à partir duquel des commandes non privilégiées peuvent être exécutées.
Vérification d'appel	Utilisé par le NAS dans des paquets de demande d'accès pour indiquer qu'un appel est en cours de réception et que le serveur RADIUS devrait renvoyer un Accès-Accepté en réponse à l'appel, ou un Rejet-d'accès pour ne pas accepter l'appel, normalement sur la base des attributs Identifiant-de-station-appelée ou Identifiant-de-station-appelante. Il est recommandé qu'une telle demande d'accès utilise la valeur de Identifiant-de-station-appelante comme valeur du Nom-d'utilisateur.
Rappel administratif	L'utilisateur devrait être déconnecté et rappelé, puis obtenir l'accès à l'interface administrative avec le NAS à partir duquel des commandes privilégiées peuvent être exécutées.

5.7 Protocole-tramé

Description

Cet attribut indique le tramage à utiliser pour l'accès tramé. Il PEUT être utilisé aussi bien pour les paquets de demande d'accès que d'Accès-Accepté.

Un résumé du format d'attribut Protocole-tramé est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 7 pour Protocole tramé.

Longueur : 6

Valeur : Le champ Valeur est de quatre octets.

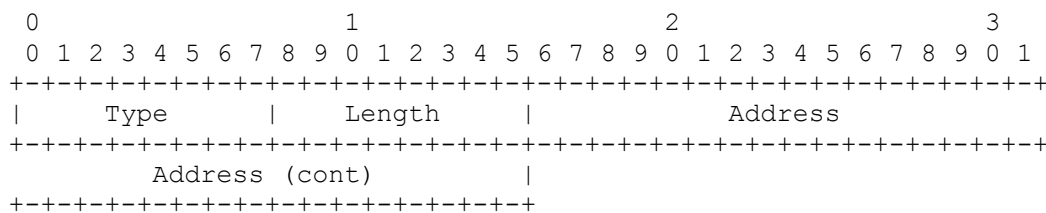
- 1 PPP
- 2 SLIP
- 3 Protocole d'accès distant AppleTalk (ARAP)
- 4 Protocole propriétaire Gandalf Ligne unique/Multiligne
- 5 IPX/SLIP propriétaire Xylogics
- 6 X.75 synchrone

5.8 Adresse-IP-tramée

Description

Cet attribut indique l'adresse à configurer pour l'utilisateur. Il PEUT être utilisé dans les paquets Accès-Accepté. Il PEUT être utilisé dans un paquet de demande d'accès comme indication du NAS au serveur qu'il préférerait cette adresse, mais le serveur n'est pas obligé de suivre cette indication.

Un résumé du format d'attribut Adresse-IP-tramée est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 8 pour Adresse-IP-tramée.

Longueur : 6

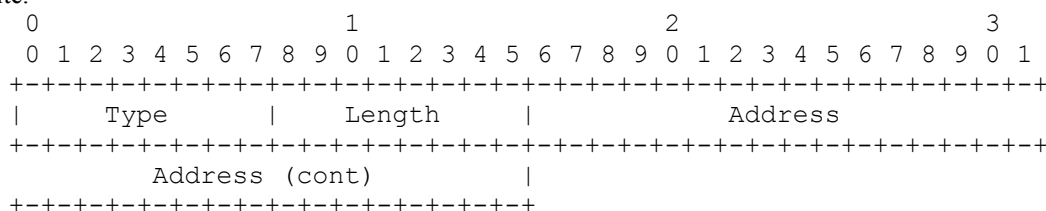
Adresse : Le champ Adresse est de quatre octets. La valeur 0xFFFFFFFF indique que le NAS devrait permettre à l'utilisateur de choisir une adresse (par exemple négociée). La valeur 0xFFFFFFF0 indique que le NAS devrait choisir une adresse pour l'utilisateur (par exemple, allouée à partir d'un réservoir d'adresses conservées par le NAS). D'autres valeurs valides indiquent que le NAS devrait utiliser cette valeur comme adresse IP de l'utilisateur.

5.9 Gabarit-réseau-IP-tramé

Description

Cet attribut indique le gabarit de réseau IP à configurer pour l'utilisateur quand l'utilisateur est un routeur pour un réseau. Il PEUT être utilisé dans des paquets Accès-Accepté. Il PEUT être utilisé dans un paquet de demande d'accès comme indication du NAS au serveur qu'il préférerait ce gabarit de réseau, mais le serveur n'est pas obligé de suivre cette indication.

Un résumé du format de l'attribut Gabarit-réseau-IP-tramé est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 9 pour Gabarit-réseau-IP-tramé.

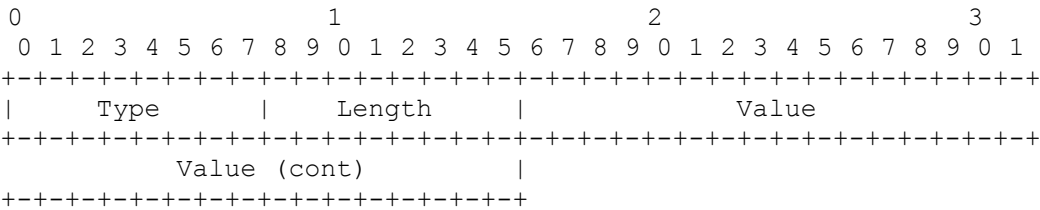
Longueur : 6

Adresse : Le champ Adresse est de quatre octets spécifiant le gabarit de réseau IP de l'utilisateur.

5.10 Routage-tramé

Description
Cet attribut indique la méthode d'acheminement pour l'utilisateur, quand l'utilisateur est un routeur pour un réseau. Il n'est utilisé que dans les paquets Accès-Accepté.

Un résumé du format de l'attribut Routage-tramé est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 10 pour Routage-tramé.

Longueur : 6

Valeur : Le champ Valeur est de quatre octets.

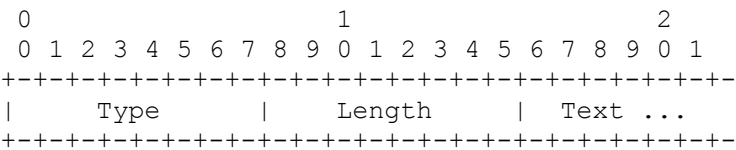
- 0 Aucun
- 1 Envoi des paquets d'acheminement
- 2 Attente des paquets d'acheminement
- 3 Envoi et attente

5.11 Identifiant-de-filtre

Description
Cet attribut indique le nom de la liste de filtres pour cet usager. Zéro, un ou plusieurs attributs Identifiant-de-filtre PEUVENT être envoyés dans un paquet Accès-Accepté.

Identifier une liste de filtres par un nom permet d'utiliser le filtre sur différents NAS sans égard aux détails de mise en œuvre de la liste des filtres.

Un résumé du format de l'attribut Identifiant-de-filtre est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 11 pour Identifiant-de-filtre.

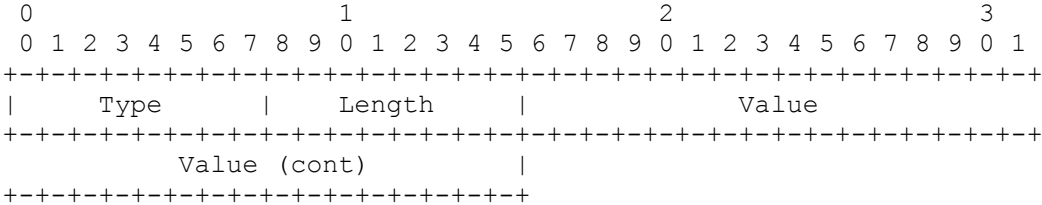
Longueur : ≥ 3

Texte
Le champ Texte est de un ou plusieurs octets, et son contenu dépend de la mise en œuvre. Il est destiné à être lu par l'homme et NE DOIT PAS affecter le fonctionnement du protocole. Il est recommandé que le message contienne des caractères ISO 10646 codés en UTF-8 [7].

5.12 MTU-tramée

Description
Cet attribut indique l'unité de transmission maximum à configurer pour l'utilisateur, quand elle n'est pas négociée par d'autres moyens (comme PPP). Il PEUT être utilisé dans des paquets Accès-Accepté. Il PEUT être utilisé dans un paquet de demande d'accès comme indication du NAS au serveur qu'il préférerait cette valeur, mais le serveur n'est pas obligé de suivre cette indication.

Un résumé du format de l'attribut MTU-tramée est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 12 pour MTU-tramée.

Longueur : 6

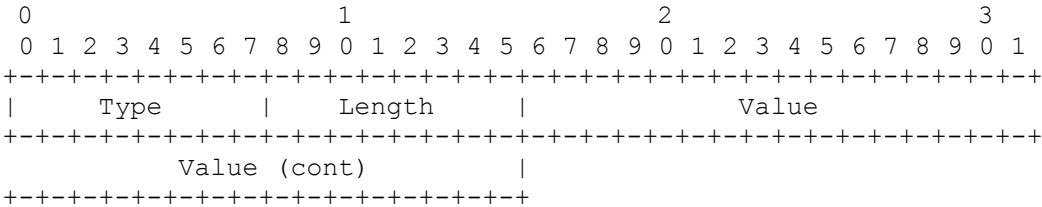
Valeur : Le champ Valeur est de quatre octets. En dépit de la taille du champ, la gamme des valeurs est de 64 à 65 535.

5.13 Compression-tramée

Description
Cet attribut indique un protocole de compression à utiliser pour la liaison. Il PEUT être utilisé dans les paquets Accès-Accepté. Il PEUT être utilisé dans un paquet de demande d'accès comme indication au serveur que le NAS préférerait utiliser cette compression, mais le serveur n'est pas obligé de suivre cette indication.

Plus d'un attribut Protocole de compression PEUT être envoyé. Il est de la responsabilité du NAS d'appliquer le protocole de compression approprié au trafic de liaison approprié.

Un résumé du format de l'attribut Compression-tramée est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 13 pour Compression-tramée.

Longueur : 6

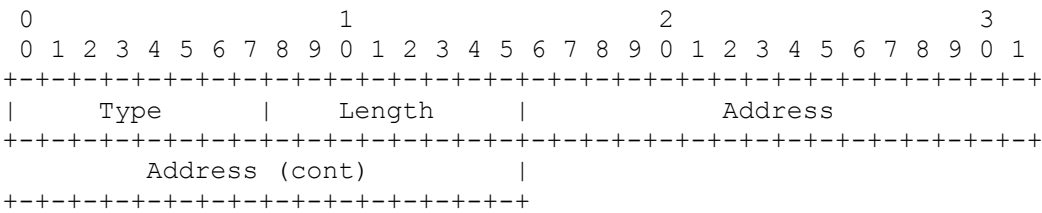
Valeur : Le champ Valeur est de quatre octets.

- 0 Aucune
- 1 Compression d'en-tête TCP/IP VJ [10]
- 2 Compression d'en-tête IPX
- 3 Compression Stac-LZS

5.14 Hôte-de-Connexion-IP

Description
Cet attribut indique le système avec lequel connecter l'utilisateur, lorsque l'attribut Service-de-Connexion est inclus. Il PEUT être utilisé dans les paquets Accès-Accepté. Il PEUT être utilisé dans un paquet de demande d'accès comme indication au serveur que le NAS préférerait utiliser cet hôte, mais le serveur n'est pas obligé de suivre cette indication.

Un résumé du format de l'attribut Hôte-de-Connexion-IP est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 14 pour Hôte-de-Connexion-IP.

Longueur : 6

Adresse

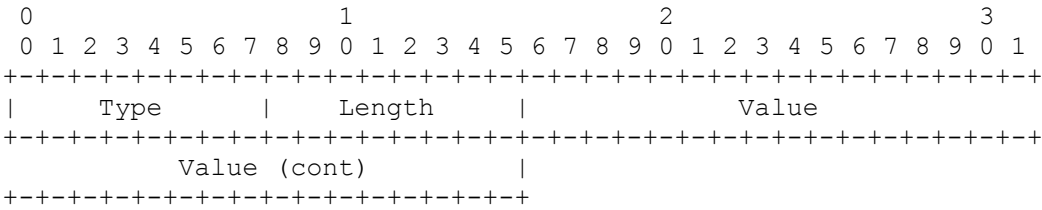
Le champ Adresse est de quatre octets. La valeur 0xFFFFFFFF indique que le NAS DEVRAIT permettre à l'utilisateur de choisir une adresse. La valeur 0 indique que le NAS DEVRAIT choisir un hôte auquel connecter l'utilisateur. Les autres valeurs indiquent l'adresse à laquelle le NAS DEVRAIT connecter l'utilisateur.

5.15 Service-de-Connexion

Description

Cet attribut indique le service à utiliser pour connecter l'utilisateur à l'hôte de connexion. Il n'est utilisé que dans les paquets Accès-Accepté.

Un résumé du format de l'attribut Service-de-Connexion est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 15 pour Service-de-Connexion.

Longueur : 6

Valeur : Le champ Valeur est de quatre octets.

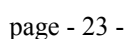
- 0 Telnet
- 1 Rlogin
- 2 TCP Clear
- 3 PortMaster (propriétaire)
- 4 LAT
- 5 X25-PAD
- 6 X25-T3POS
- 8 TCP Clear Quiet (supprime toute chaîne de connexion générée par le NAS)

5.16 Accès-de-connexion-TCP

Description

Cet attribut indique l'accès TCP auquel l'utilisateur doit être connecté, quand l'attribut Service-de-Connexion est aussi présent. Il n'est utilisé que dans les paquets Accès-Accepté.

Un résumé du format de l'attribut Accès-de-connexion-TCP est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 19 pour Numéro-de-rappel.

Longueur : ≥ 3

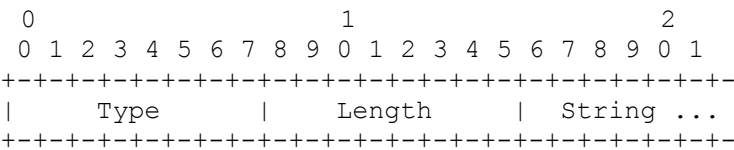
Chaîne
Le champ Chaîne est de un ou plusieurs octets. Le format réel des informations est spécifique du site ou de l'application, et une mise en œuvre robuste DEVRAIT prendre en charge le champ comme des octets indistincts.

La codification de la gamme des usages admis pour ce champ sort du domaine d'application de la présente spécification.

5.20 Identifiant-de-rappel

Description
Cet attribut indique le nom d'un endroit à appeler, à interpréter par le NAS. Il PEUT être utilisé dans des paquets Accès-Accepté.

Un résumé du format de l'attribut Identifiant-de-rappel est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 20 pour Identifiant-de-rappel.

Longueur : ≥ 3

Chaîne
Le champ Chaîne est de un ou plusieurs octets. Le format réel des informations est spécifique du site ou de l'application, et une mise en œuvre robuste DEVRAIT prendre en charge le champ comme des octets indistincts.

La codification de la gamme des usages admis pour ce champ sort du domaine d'application de la présente spécification.

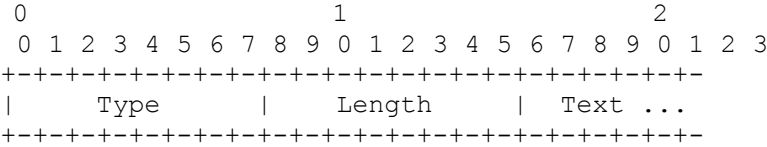
5.21 (non alloué)

Description
L'ATTRIBUT DE TYPE 21 N'A PAS ÉTÉ ALLOUÉ.

5.22 Route-tramée

Description
Cet attribut fournit des informations d'acheminement à configurer pour l'utilisateur sur le NAS. Il est utilisé dans le paquet Accès-Accepté et peut apparaître plusieurs fois.

Un résumé du format de l'attribut Route-tramée est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 22 pour Route-tramée.

Longueur : ≥ 3

Texte
Le champ Texte est de un ou plusieurs octets, et son contenu dépend de la mise en œuvre. Il est destiné à être lu par

l'homme et NE DOIT PAS affecter le fonctionnement du protocole. Il est recommandé que le message contienne des caractères de la norme ISO 10646 codés en UTF-8 [7].

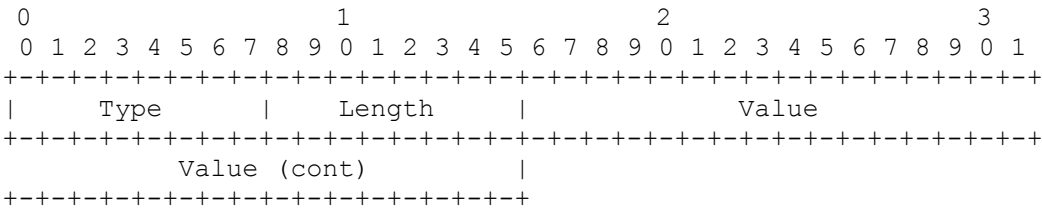
Pour les routes IP, il DEVRAIT contenir un préfixe de destination en forme quadratique séparée par des point suivi facultativement par une barre oblique et un déterminant de longueur décimale établissant combien de bits de plus fort poids du préfixe utiliser. Il est suivi d'une espace, d'une adresse de passerelle en forme quadratique séparée par des points, d'une espace, et d'une ou plusieurs métriques séparées par des espaces. Par exemple, "192.168.1.0/24 192.168.1.1 1 2 -1 3 400". Le déterminant de longueur peut être omis, auquel cas, il a la valeur par défaut de 8 bits pour les préfixes de classe A, de 16 bits pour les préfixes de classe B, et de 24 bits pour les préfixes de classe C. Par exemple, "192.168.1.0 192.168.1.1 1".

Chaque fois que l'adresse de la passerelle est spécifiée par "0.0.0.0" l'adresse IP de l'utilisateur DEVRAIT être utilisée comme adresse de passerelle.

5.23 Réseau-IPX-tramé

Description
Cet attribut indique le numéro de réseau IPX à configurer pour l'utilisateur. Il est utilisé dans les paquets Accès-Accepté.

Un résumé du format de l'attribut Réseau-IPX-tramé est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 23 pour Réseau-IPX-tramé.

Longueur : 6

Valeur
Le champ Valeur est de quatre octets. La valeur 0xFFFFFFFFE indique que le NAS devrait choisir un réseau IPX pour l'utilisateur (par exemple alloué à partir d'un réservoir d'un ou plusieurs réseaux IPX conservés par le NAS). Les autres valeurs devraient être utilisées comme réseau IPX pour la liaison avec l'utilisateur.

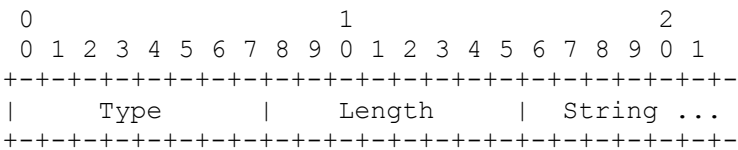
5.24 État

Description
Cet attribut est disponible pour être envoyé par le serveur au client dans un Défi-d'accès et DOIT être envoyé sans modification du client au serveur dans la réponse de nouvelle demande d'accès à cette épreuve, s'il en est.

Cet attribut est disponible pour envoi par le serveur au client dans un Accès-Accepté qui inclut aussi un attribut Action-de-termination 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 État inchangé dans cette demande d'accès.

Dans l'une ou l'autre utilisation, le client NE DOIT PAS interpréter l'attribut localement. Un paquet doit avoir seulement zéro ou un attribut État. L'usage de l'attribut État dépend de la mise en œuvre.

Un résumé du format de l'attribut État est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 24 pour État.

Longueur : ≥ 3

Chaîne

Le champ Chaîne est de un ou plusieurs octets. Le format réel des informations est spécifique du site ou de l'application, et une mise en œuvre robuste DEVRAIT prendre en charge le champ comme des octets indistincts.

La codification de la gamme des usages admis pour ce champ sort du domaine d'application de la présente spécification.

5.25 Classe

Description

Cet attribut est disponible pour envoi par le serveur au client dans un Accès-Accepté et DEVRAIT être envoyé non modifié par le client au serveur de comptabilité au titre du paquet Demande-de-comptabilité si la comptabilité est prise en charge. Le client NE DOIT PAS interpréter l'attribut localement.

Un résumé du format de l'attribut Classe est indiqué ci-dessous. Les champs sont transmis de gauche à droite.

```

      0                               1                               2
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Type      |      Length      |      String ...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Type : 25 pour Classe.

Longueur : ≥ 3

Chaîne

Le champ Chaîne est de un ou plusieurs octets. Le format réel des informations est spécifique du site ou de l'application, et une mise en œuvre robuste DEVRAIT prendre en charge le champ comme des octets indistincts.

La codification de la gamme des usages admis pour ce champ sort du domaine d'application de la présente spécification..

5.26 Spécifique-du-fabricant

Description

Cet attribut est disponible pour permettre aux fabricants de prendre en charge leurs propres attributs d'extension ne convenant pas à une utilisation générale. Il NE DOIT PAS affecter le fonctionnement du protocole RADIUS.

Les serveurs qui ne sont pas équipés pour interpréter les informations spécifiques de fabricant envoyées par un client DOIVENT l'ignorer (bien qu'il puisse être rapporté). Les clients qui ne reçoivent pas les informations spécifiques du fabricant désirées DEVRAIENT tenter de fonctionner sans lui, bien qu'ils puissent le faire (et rapporter qu'ils le font) en mode dégradé.

Un résumé du format de l'attribut Spécifique-du-fabricant est indiqué ci-dessous. Les champs sont transmis de gauche à droite.

```

      0                               1                               2                               3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Type      |      Length      |      Vendor-Id
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Vendor-Id (cont)      |      String...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Type : 26 pour Spécifique du fabricant.

Longueur : ≥ 7

Identifiant de fabricant

L'octet de plus fort poids est à 0 et les 3 octets de moindre poids sont le code SMI d'entreprise privée de gestion de réseau du fabricant dans l'ordre des octets du réseau, comme défini dans la RFC des "Numéros alloués" [6].

Chaîne

Le champ Chaîne est de un ou plusieurs octets. Le format réel des informations est spécifique du site ou de l'application, et une mise en œuvre robuste DEVRAIT prendre en charge le champ comme des octets indistincts.

La codification de la gamme des usages admis pour ce champ sort du domaine d'application de la présente spécification..

Il DEVRAIT être codé comme une séquence de champs type de fabricant / longueur du fabricant / valeur, comme suit. Le champ Spécifique-de-l'attribut dépend de la définition de cet attribut par le fabricant. Un exemple de codage de l'attribut Spécifique-de-l'attribut utilisant cette méthode est :

```

      0               1               2               3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|      Type      | Length      |      Vendor-Id      |
+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+-----+
| Attribute-Specific...
+-----+-----+-----+-----+-----+-----+-----+

```

Plusieurs sous-attributs PEUVENT être codés au sein d'un seul attribut Spécifique-du-fabricant, mais ce n'est pas obligatoire.

5.27 Durée-de-session**Description**

Cet attribut règle le nombre maximum de secondes de service à fournir à l'utilisateur avant la terminaison de la session ou de l'invite. Cet attribut est disponible pour l'envoi par le serveur au client dans un Accès-Accepté ou une Défi-d'accès.

Un résumé du format de l'attribut Durée-de-session est indiqué ci-dessous. Les champs sont transmis de gauche à droite.

```

      0               1               2               3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|      Type      | Length      |      Value      |
+-----+-----+-----+-----+-----+-----+-----+
| Value (cont)   |
+-----+-----+-----+-----+-----+-----+-----+

```

Type : 27 pour Durée-de-session.

Longueur : 6

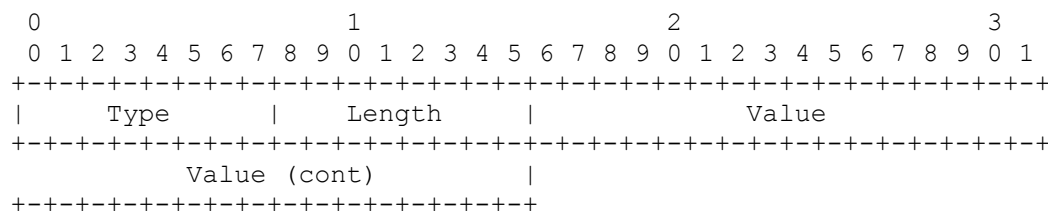
Valeur

Le champ est de 4 octets, contenant un entier de 32 bits non signé avec le nombre maximum de secondes pendant lesquelles cet usager devrait être admis à rester connecté par le NAS.

5.28 Durée-d'inactivité**Description**

Cet attribut règle le nombre maximum de secondes consécutives de connexion sans activité permis à l'utilisateur avant 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.

Un résumé du format de l'attribut Durée-d'inactivité est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 28 pour Durée-d'inactivité.

Longueur : 6

Valeur

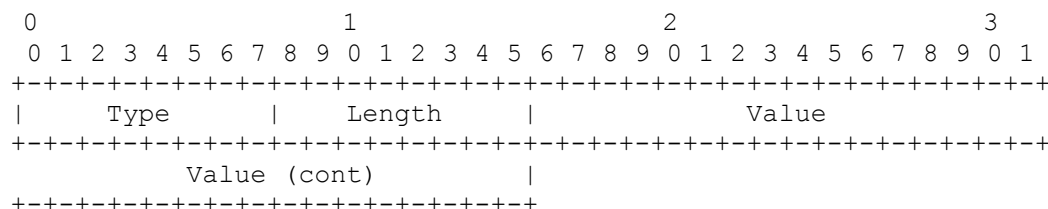
Le champ est de 4 octets, contenant un entier de 32 bits non signés avec le nombre maximum de secondes consécutives d'inactivité permises à cet usager avant déconnexion par le NAS.

5.29 Action-de-terminaison

Description

Cet attribut indique quelle action le NAS devrait entreprendre lorsque le service spécifié est achevé. Il n'est utilisé que dans les paquets Accès-Accepté.

Un résumé du format de l'attribut Action-de-terminaison est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 29 pour Action-de-terminaison.

Longueur : 6

Valeur : Le champ Valeur est de quatre octets.

0 Défaut

1 Demande-RADIUS

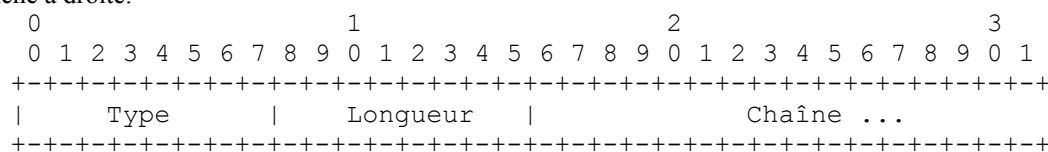
Si la valeur est réglée à Demande-RADIUS, à l'achèvement du service spécifié, le NAS PEUT envoyer une nouvelle demande d'accès au serveur RADIUS, incluant l'attribut État s'il en est.

5.30 Identifiant-de-station-appelée

Description

Cet attribut permet au NAS d'envoyer dans le paquet de demande d'accès le numéro de téléphone sur lequel est venu l'appel de l'utilisateur, en utilisant l'identification du numéro appelé (DNIS, *Dialed Number IdentificationS*) ou une technologie similaire. Noter que cela peut être différent du numéro de téléphone d'où vient l'appel. Il n'est utilisé que dans les paquets de demande d'accès.

Un résumé du format de l'attribut Identifiant-de-station-appelée est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 30 pour Identifiant-de-station-appelée.

Longueur : ≥ 3

[illegible]

Le champ Chaîne est de un ou plusieurs octets, et contient l'identité du service LAT à utiliser. L'architecture LAT permet que la chaîne contienne \$ (dollar), - (trait d'union), . (point), _ (souligné), des chiffres, des lettres majuscules et minuscules, et l'extension du jeu de caractères ISO Latin-1 [11]. Toutes les comparaisons de chaîne LAT sont insensibles à la casse.

[illegible]

Le champ Chaîne est de un ou plusieurs octets, et contient l'identité du nœud LAT auquel connecter l'utilisateur. L'architecture LAT permet à cette chaîne de contenir \$ (dollar), - (trait d'union), . (point), _ (souligné), des chiffres, des lettres majuscules et minuscules, et l'extension du jeu de caractères ISO Latin-1 [11]. Toutes les comparaisons de chaîne LAT sont insensibles à la casse.

Les administrateurs peuvent allouer un ou plusieurs des bits du code de groupe au fournisseur de service LAT ; il n'acceptera que des connexions LAT qui ont ces codes de groupe établis dans la matrice de concordance binaire. Les administrateurs allouent une matrice de concordance binaire de codes de groupe autorisé à chaque utilisateur ; LAT les obtient du système d'exploitation, et les utilise dans ses demandes aux fournisseurs de service.

Un résumé du format de l'attribut Groupe-de-connexion-LAT est indiqué ci-dessous. Les champs sont transmis de gauche à droite.

```

      0                               1                               2
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Type      |      Longueur      |      Chaîne ...      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Type : 36 pour Groupe-de-connexion-LAT.

Longueur : 34

Chaîne

Le champ Chaîne est une matrice de concordance binaire de 32 octets, celui de plus fort poids en premier. Une mise en œuvre robuste DEVRAIT prendre en charge le champ comme des octets indistincts.

La codification de la gamme des usages admis pour ce champ sort du domaine d'application de la présente spécification.

5.37 Liaison-AppleTalk-tramée

Description

Cet attribut indique le numéro de réseau AppleTalk qui devrait être utilisé pour le lien série avec l'utilisateur, qui est un autre routeur AppleTalk. Il n'est utilisé que dans les paquets Accès-Accepté. Il n'est jamais utilisé quand l'utilisateur n'est pas un autre routeur.

Un résumé du format de l'attribut Liaison-AppleTalk-tramée est indiqué ci-dessous. Les champs sont transmis de gauche à droite.

```

      0                               1                               2                               3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Type      |      Longueur      |      Valeur      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Valeur (suite)      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Type : 37 pour Liaison-AppleTalk-tramée.

Longueur : 6

Valeur

Le champ Valeur est de quatre octets. En dépit de la taille du champ, la gamme des valeurs va de 0 à 65 535. La valeur particulière de 0 indique que c'est un lien série non numéroté. Une valeur de 1 à 65 535 signifie que la ligne série entre le NAS et l'utilisateur devrait se voir allouer cette valeur comme numéro de réseau AppleTalk.

5.38 Réseau-AppleTalk-tramé

Description

Cet attribut indique le numéro de réseau AppleTalk que le NAS devrait sonder pour allouer un nœud AppleTalk à l'utilisateur. Il n'est utilisé que dans les paquets Accès-Accepté. Il n'est jamais utilisé quand l'utilisateur est un autre routeur. Plusieurs instances de cet attribut indiquent que le NAS peut sonder en utilisant n'importe lequel des numéros de réseau spécifiés.

Un résumé du format de l'attribut Réseau-AppleTalk-tramé est indiqué ci-dessous. Les champs sont transmis de gauche à droite.

```

      0                               1                               2                               3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Type      |      Longueur      |      Valeur      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Valeur (suite)      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```


Type : 38 pour Réseau-AppleTalk-tramé.

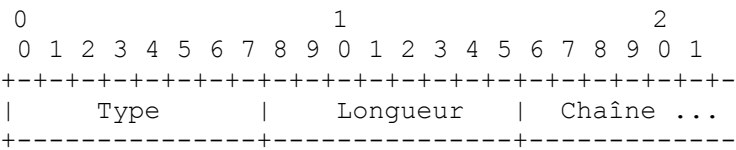
Longueur : 6

Valeur
Le champ Valeur est de quatre octets. En dépit de la taille du champ, la gamme des valeurs va de 0 à 65 535. La valeur particulière de 0 indique que le NAS devrait allouer un réseau à l'utilisateur, en utilisant sa gamme de câble par défaut. Une valeur entre 1 et 65535 (inclus) indique le réseau AppleTalk que le NAS devrait sonder pour trouver une adresse pour l'utilisateur.

5.39 Zone-AppleTalk-tramée

Description
Cet attribut indique la zone AppleTalk par défaut à utiliser pour cet usager. Il n'est utilisé que dans les paquets Accès-Accepté. Plusieurs instances de cet attribut dans le même paquet ne sont pas admises.

Un résumé du format de l'attribut Zone-AppleTalk-tramée est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 39 pour Zone-AppleTalk-tramée.

Longueur : ≥ 3

Chaîne
Le nom de la zone AppleTalk par défaut à utiliser pour cet usager. Une mise en œuvre robuste DEVRAIT prendre en charge le champ comme des octets indistincts.

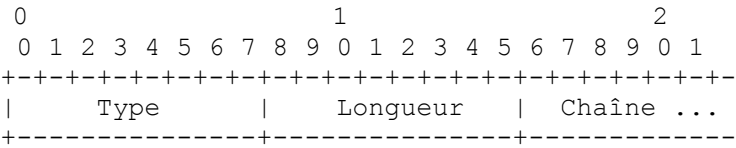
La codification de la gamme des usages admis pour ce champ sort du domaine d'application de la présente spécification.

5.40 Défi-CHAP

Description
Cet attribut contient l'épreuve CHAP envoyée par le NAS à un utilisateur du protocole d'authentification par dialogue à énigme (CHAP, *Challenge-Handshake Authentication Protocol*) PPP. Il n'est utilisé que dans des paquets de demande d'accès.

Si la valeur de l'épreuve CHAP est longue de 16 octets, elle PEUT être placée dans le champ Authentificateur de demande au lieu d'utiliser cet attribut.

Un résumé du format de l'attribut Défi-CHAP est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 60 pour Défi-CHAP.

Longueur : ≥ 7

Chaîne : Le champ Chaîne contient l'épreuve CHAP.

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
Type										Longueur										Valeur																			
Valeur (suite)																																							

Le champ est de 4 octets, contenant un entier de 32 bits non signé avec le nombre maximum d'accès que cet usager devrait être admis à connecter sur le NAS.

[illegible]

Le champ Chaîne est de un ou plusieurs octets, et contient l'identité de l'accès LAT à utiliser. L'architecture LAT permet que la chaîne contienne \$ (dollar), - (trait d'union), . (point), _ (souligné), des chiffres, des lettres majuscules et minuscules, et l'extension du jeu de caractères ISO Latin-1 [11]. Toutes les comparaisons de chaîne LAT sont insensibles à la casse.

Demande	Accepté	Rejeté	Défi	n°	Attribut
0-1	0-1	0	0	1	Nom-d'utilisateur
0-1	0	0	0	2	Mot-de-passe-d'utilisateur [Note 1]
0-1	0	0	0	3	Mot de passe CHAP [Note 1]
0-1	0	0	0	4	Adresse-IP-NAS [Note 2]
0-1	0	0	0	5	Accès-de-NAS
0-1	0-1	0	0	6	Type-de-Service
0-1	0-1	0	0	7	Protocole-tramé
0-1	0-1	0	0	8	Adresse-IP-tramée
0-1	0-1	0	0	9	Gabarit-réseau-IP-tramé
0	0-1	0	0	10	Routage-tramé
0	0+	0	0	11	Identifiant-de-filtre
0-1	0-1	0	0	12	MTU-tramée

0+	0+	0	0	13	Compression-tramée
0+	0+	0	0	14	Hôte-de-Connexion-IP
0	0-1	0	0	15	Service-de-Connexion
0	0-1	0	0	16	Port-de-connexion-TCP
0	0+	0+	0+	18	Message-de-réponse
0-1	0-1	0	0	19	Numéro-de-rappel
0	0-1	0	0	20	Identifiant-de-rappel
0	0+	0	0	22	Route-tramé
0	0-1	0	0	23	Réseau-IPX-tramé
0-1	0-1	0	0-1	24	État [Note 1]
0	0+	0	0	25	Classe
0+	0+	0	0+	26	Spécifique-du-fabricant
0	0-1	0	0-1	27	Durée-de-session
0	0-1	0	0-1	28	Durée-d'inactivité
0	0-1	0	0	29	Action-de-termination
0-1	0	0	0	30	Identifiant-de-station-appelée
0-1	0	0	0	31	Identifiant-de-station-appelante
0-1	0	0	0	32	Identifiant-de-NAS [Note 2]
0+	0+	0+	0+	33	Etat-de-mandataire
0-1	0-1	0	0	34	Service-LAT-de-connexion
0-1	0-1	0	0	35	Nœud-LAT-de-connexion
0-1	0-1	0	0	36	Groupe-LAT-de-connexion
0	0-1	0	0	37	Liaison-AppleTalk-tramée
0	0+	0	0	38	Réseau-AppleTalk-tramé
0	0-1	0	0	39	Zone-AppleTalk-tramée
0-1	0	0	0	60	Défi-CHAP
0-1	0	0	0	61	Type-d'accès-de-NAS
0-1	0-1	0	0	62	Limite-d'accès
0-1	0-1	0	0	63	Accès-de-connexion-LAT

[Note 1] 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.

[Note 2] Une demande d'accès DOIT contenir une Adresse-IP-de-NAS ou un Identifiant-de-NAS (ou les deux).

Le tableau suivant définit la signification des entrées du tableau ci-dessus :

- 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.

6 Considérations relatives à l'IANA

La présente section donne des lignes conductrices pour l'Autorité d'allocation des numéros de l'Internet (IANA, *Internet Assigned Numbers Authority*) concernant l'enregistrement des valeurs relatives au protocole RADIUS, conformément au BCP 26 [13].

Il y a trois espaces de noms dans RADIUS qui exigent l'enregistrement : Codes de types de paquet, Types d'attribut, et Valeurs d'attribut (pour certains attributs).

RADIUS n'est pas destiné à un protocole d'utilisation générale de gestion de serveur d'accès réseau (NAS, *Network Access Server*), et les allocations ne devraient pas être faites pour des objets sans rapport avec l'authentification, l'autorisation ou la comptabilité.

6.1 Définition des termes

Les termes suivants sont utilisés ici avec la signification définie dans le BCP 26 : "espace de nom", "valeur allouée", "enregistrement".

Les politiques suivantes sont utilisées ici avec la signification définie dans le BCP 26 : "Utilisation privée", "Premier entré, premier servi", "Révision par des experts", "Spécification exigée", "Consensus de l'IETF", "Action de normalisation".

6.2 Politiques d'enregistrement recommandées

Pour les demandes d'enregistrement où un expert désigné devrait être consulté, le Directeur de zone des opérations de l'IESG devrait nommer l'expert désigné.

Pour les demandes d'enregistrement exigeant la révision par des experts la liste de diffusion ietf-radius devrait être consultée.

Les codes de type de paquet ont une gamme de 1 à 254, dont 1 à 5 et 11 à 13 ont été alloués. Parce qu'un nouveau type de paquet a un impact considérable sur l'interopérabilité, un nouveau code de type de paquet exige une action de normalisation, et devrait être alloué à partir de 14.

Les types d'attribut ont une gamme de 1 à 255, et sont la ressource la plus rare de RADIUS, et ils doivent donc être alloués avec soin. Les attributs 1 à 53, 55, 60 à 88, 90 et 91 ont été alloués, 17 et 21 étant disponibles et réutilisables. Les attributs 17, 21, 54, 56 à 59, 89, 92 à 191 peuvent être alloués suite à révision par des experts, avec spécification exigée. La libération de blocs de types d'attribut (plus de 3 à la fois pour un objet donné) devrait requérir le consensus de l'IETF. Il est recommandé que les attributs 17 et 21 ne soient utilisés qu'après épuisement de tous les autres.

Noter que RADIUS définit un mécanisme pour les extensions Spécifique-du-fabricant (Attribut 26) et l'utilisation de ce mécanisme devrait être encouragée plutôt que l'allocation de types d'attributs mondiaux, pour des fonctions spécifiques d'une mise en œuvre de RADIUS d'un seul fabricant, lorsque aucune interopérabilité n'est réputée utile.

Comme établi dans la section "Attributs" ci-dessus :

"Les valeurs de [Type d'attribut] 192 à 223 sont réservées à des utilisations expérimentales, les valeurs 224 à 240 sont réservées à des utilisations spécifiques d'une mise en œuvre, et les valeurs 241 à 255 sont réservées et ne devraient pas être utilisées."

Donc les valeurs d'attribut 192 à 240 sont considérées d'utilisation privée, et les valeurs 241 à 255 exigent une action de normalisation.

Certains attributs (par exemple, Type-d'accès-de-NAS) dans RADIUS définissent une liste de valeurs qui correspondent à diverses significations. Il peut y avoir 4 milliards (2^{32}) de valeurs pour chaque attribut. L'ajout de valeurs supplémentaires à la liste peut être fait par l'IANA sur la base du premier arrivé, premier servi.

7 Exemples

Quelques exemples sont présentés pour illustrer le flux de paquets et l'utilisation des attributs typiques. Ces exemples ne sont pas destinés à être exhaustifs, de nombreux autres sont possibles. Les représentations hexadécimales de ces paquets exemples sont données dans l'ordre des octets du réseau, en utilisant le secret partagé "xyzyzy5461".

7.1 Usager Telnet à l'hôte spécifié

Le NAS à 192.168.1.16 envoie un paquet Demande d'accès UDP au serveur RADIUS pour un usager nommé nemo connecté à l'accès 3 avec le mot de passe "arctangent".

L'authentificateur de demande est un nombre aléatoire de 16 octets généré par le NAS.

Le Mot-de-passe-d'utilisateur est un mot de passe de 16 octets bourré à la fin avec des zéros, combiné par opérateur OUX avec MD5 (Authentificateur de demande à secret partagé).

01 00 00 38 0f 40 3f 94 73 97 80 57 bd 83 d5 cb 98 f4 22 7a 01 06 6e 65 6d 6f 02 12 0d 00 70 8d 93 d4 13 ce 31 96 e4 3f 78 2a 0a ee 04 06 c0 a8 01 10 05 06 00 00 00 03

1 Code = Demande d'accès (1)
 1 ID = 0
 2 Longueur = 56
 16 Authentificateur de demande

Attributs :

6 Nom-d'utilisateur = "nemo"
 18 Mot-de-passe-d'utilisateur
 6 Adresse-IP-NAS = 192.168.1.16
 6 Port-NAS = 3

Le serveur RADIUS authentifie nemo, et envoie un paquet UDP Accès-Accepté au NAS lui disant de passer nemo par telnet à l'hôte 192.168.1.3.

L'authentificateur de réponse est une somme de contrôle MD5 de 16 octets du code (2), de l'identifiant (0), de la longueur (38), de l'authentificateur de demande ci-dessus, des attributs dans cette réponse, et du secret partagé.

02 00 00 26 86 fe 22 0e 76 24 ba 2a 10 05 f6 bf 9b 55 e0 b2 06 06 00 00 00 01 0f 06 00 00 00 00 0e 06 c0 a8 01 03

1 Code = Accès-Accepté (2)
 1 ID = 0 (le même que dans la demande d'accès)
 2 Longueur = 38
 16 Authentificateur de réponse

Attributs :

6 Type-de-Service (6) = Connexion (1)
 6 Service-de-Connexion (15) = Telnet (0)
 6 Hôte-de-Connexion-IP (14) = 192.168.1.3

7.2 Usager tramé s'authentifiant avec CHAP

Le NAS à 192.168.1.16 envoie un paquet Demande d'accès UDP au serveur RADIUS pour un usager nommé flopsy qui se connecte à l'accès 20 avec PPP, s'authentifie en utilisant CHAP. Le NAS envoie aussi les attributs Type-de-Service et Protocole-tramé comme indication au serveur RADIUS que cet usager recherche PPP, bien que le NAS ne soit pas obligé de le faire.

L'authentificateur de demande est un nombre aléatoire de 16 octets généré par le NAS, et est aussi utilisé comme Défi-CHAP.

Le Mot-de-passe-CHAP consiste en un identifiant CHAP de 1 octet, dans ce cas, 22, suivi par la réponse CHAP de 16 octets.

01 01 00 47 2a ee 86 f0 8d 0d 55 96 9c a5 97 8e 0d 33 67 a2 01 08 66 6c 6f 70 73 79 03 13 16 e9 75 57 c3 16 18 58 95 f2 93 ff 63 44 07 72 75 04 06 c0 a8 01 10 05 06 00 00 00 14 06 06 00 00 00 02 07 06 00 00 00 01

1 Code = 1 (Demande d'accès)
 1 ID = 1
 2 Longueur = 71
 16 Authentificateur de demande

Attributs :

8 Nom-d'utilisateur (1) = "flopsy"
 19 Mot-de-passe CHAP (3)
 6 Adresse-IP-de-NAS (4) = 192.168.1.16
 6 Accès-de-NAS (5) = 20
 6 Type-de-Service (6) = Tramé (2)
 6 Protocole-tramé (7) = PPP (1)

Le serveur RADIUS authentifie flopsy, et envoie un paquet UDP Accès-Accepté au NAS lui disant de commencer le service PPP et allouant une adresse pour l'utilisateur, tirée de son réservoir d'adresses dynamique.

L'authentificateur de réponse est une somme de contrôle MD5 de 16 octets du code (2), de l'identifiant (1), de la longueur (56), de l'authentificateur de demande de ci-dessus, des attributs dans cette réponse, et du secret partagé.

```
02 01 00 38 15 ef bc 7d ab 26 cf a3 dc 34 d9 c0 3c 86 01 a4 06 06 00 00 00 02 07 06 00 00 00 01 08 06 ff ff ff fe 0a 06 00
00 00 02 0d 06 00 00 00 01 0c 06 00 00 05 dc
```

1 Code = Accès-Accepté (2)
 1 ID = 1 (le même que dans Demande-d'accès)
 2 Longueur = 56
 16 Authentificateur de réponse

Attributs :

6 Type-de-Service (6) = Tramé (2)
 6 Protocole-tramé (7) = PPP (1)
 6 Adresse-IP-tramée (8) = 255.255.255.254
 6 Routage-tramé (10) = Aucun (0)
 6 Compression-tramée (13) = Compression d'en-têteTCP/IP VJ (1)
 6 MTU-tramée (12) = 1500

7.3 Usager avec carte de Défi-réponse

Le NAS à 192.168.1.16 envoie un paquet de demande d'accès UDP au serveur RADIUS pour un usager nommé mopsy se connectant à l'accès 7. L'utilisateur entre le mot de passe factice "challenge" dans cet exemple. L'épreuve et la réponse générées par la carte à puce pour cet exemple sont "32769430" et "99101462".

L'authentificateur de demande est un nombre aléatoire de 16 octets généré par le NAS.

Le Mot-de-passe-d'utilisateur est 16 octets de mot de passe, dans ce cas "challenge", bourré à la fin avec des zéros, composés par l'opérateur OUX avec (secret partagé|Authentificateur de demande)MD5.

```
01 02 00 39 f3 a4 7a 1f 6a 6d 76 71 0b 94 7a b9 30 41 a0 39 01 07 6d 6f 70 73 79 02 12 33 65 75 73 77 82 89 b5 70 88 5e
15 08 48 25 c5 04 06 c0 a8 01 10 05 06 00 00 00 07
```

1 Code = Demande d'accès (1)
 1 ID = 2
 2 Longueur = 57
 16 Authentificateur de demande

Attributs :

7 Nom-d'utilisateur (1) = "mopsy"
 18 Mot-de-passe-d'utilisateur (2)
 6 Adresse-IP-de-NAS (4) = 192.168.1.16
 6 Accès-de-NAS (5) = 7

Le serveur RADIUS décide de mettre mopsy à l'épreuve, en lui renvoyant une chaîne d'épreuve et attendant une réponse. Le serveur RADIUS envoie donc un paquet UDP Défi-d'accès au NAS.

L'authentificateur de réponse est une somme de contrôle MD5 de 16 octets du code (11), de l'identifiant (2), de la longueur (78), de l'authentificateur de demande de ci-dessus, des attributs dans cette réponse, et du secret partagé.

Le Message-de-réponse est "Challenge 32769430. Entre la réponse à l'invite."

L'État est un mouchard magique à retourner avec la réponse de l'utilisateur ; dans cet exemple, 8 octets de données (33 32 37 36 39 34 33 30 en hexadécimal).

```
0b 02 00 4e 36 f3 c8 76 4a e8 c7 11 57 40 3c 0c 71 ff 9c 45 12 30 43 68 61 6c 6c 65 6e 67 65 20 33 32 37 36 39 34 33 30
```

2e 20 20 45 6e 74 65 72 20 72 65 73 70 6f 6e 73 65 20 61 74 20 70 72 6f 6d 70 74 2e 18 0a 33 32 37 36 39 34 33 30

1 Code = Défi-d'accès (11)
 1 ID = 2 (le même que dans Demande-d'accès)
 2 Longueur = 78
 16 Authentificateur de réponse

Attributs :

48 Message-de-réponse (18)
 10 État (24)

L'utilisateur entre sa réponse, et le NAS envoie une nouvelle Demande-d'accès avec cette réponse, et inclut l'attribut État.

L'authentificateur de demande est un nouveau nombre aléatoire de 16 octets.

Le Mot-de-passe-d'utilisateur est 16 octets de la réponse de l'utilisateur, dans ce cas "99101462", bourrés de zéros à la fin, composés par l'opérateur OUX avec (secret partagé|authentificateur de demande) MD5.

L'état est le mouchard magique tiré du paquet Défi-d'accès, inchangé.

01 03 00 43 b1 22 55 6d 42 8a 13 d0 d6 25 38 07 c4 57 ec f0 01 07 6d 6f 70 73 79 02 12 69 2c 1f 20 5f c0 81 b9 19 b9 51
 95 f5 61 a5 81 04 06 c0 a8 01 10 05 06 00 00 00 07 18 10 33 32 37 36 39 34 33 30

1 Code = Demande-d'accès (1)
 1 ID = 3 (Noter que celui-là change.)
 2 Longueur = 67
 16 Authentificateur de demande

Attributs :

7 Nom-d'utilisateur = "mopsy"
 18 Mot-de-passe-d'utilisateur
 6 Adresse-IP-de-NAS (4) = 192.168.1.16
 6 Accès-de-NAS (5) = 7
 10 État (24)

La réponse était incorrecte (pour les besoins de l'exemple), aussi le serveur RADIUS dit au NAS de rejeter la tentative de connexion.

L'authentificateur de réponse est une somme de contrôle MD5 de 16 octets de code (3), identifiant (3), longueur (20), de l'authentificateur de demande de ci-dessus, des attributs dans cette réponse (dans ce cas, aucun), et du secret partagé.

03 03 00 14 a4 2f 4f ca 45 91 6c 4e 09 c8 34 0f 9e 74 6a a0

1 Code = Rejet-d'accès (3)
 1 ID = 3 (le même que dans Demande-d'accès)
 2 Longueur = 20
 16 Authentificateur de réponse

Attributs : (aucun, bien qu'un Message-de-réponse ait pu être envoyé).

8 Considérations pour la sécurité

Les questions de sécurité sont le principal objet du présent document.

En pratique, au sein de chaque serveur RADIUS, ou associé à lui, se trouve une base de données comportant les noms des usagers associés à des informations d'authentification (des "secrets"). Il n'est pas prévu qu'un usager nommé particulier puisse être authentifié par plusieurs méthodes. Cela rendrait l'utilisateur vulnérable à des attaques qui négocieraient la méthode la moins sûre de l'ensemble. Au lieu de cela, il devrait y avoir pour chaque usager nommé une indication d'exactly une méthode utilisée pour authentifier ce nom d'utilisateur. Si un utilisateur a besoin d'utiliser différentes méthodes d'authentification

dans des circonstances différentes, des noms d'utilisateur distincts DEVRAIENT être employés, chacun d'eux identifiant exactement une méthode d'authentification.

Les mots de passe et autres secrets devrait être mémorisés chacun de leur côté de telle sorte que leur accès soit aussi limité que possible. Idéalement, les secrets ne devraient être accessibles qu'au processus qui exige l'accès pour effectuer l'authentification.

Les secrets devrait être distribués avec un mécanisme qui limite le nombre d'entités qui traitent (et donc ont connaissance) du secret. Idéalement, aucune personne non autorisée ne devrait jamais avoir connaissance des secrets. Il est possible d'accomplir cela avec les protocoles de sécurité SNMP [14], mais un tel mécanisme sort du domaine d'application de la présente spécification.

D'autres méthodes de distribution sont actuellement en cours d'étude et d'expérimentation. Le document sur la sécurité SNMP [14] donne aussi une excellente vue générale des menaces sur les protocoles réseau.

Le mécanisme de dissimulation du Mot-de-passe-d'utilisateur décrit au paragraphe 5.2 n'a pas été soumis à des quantités significatives d'analyse cryptographique dans les publications. Au sein de la communauté de l'IETF, certains se sont émus de ce que cette méthode pourrait ne pas fournir une protection suffisante de la confidentialité [15] aux mots de passe transmis en utilisant RADIUS. Les usagers devraient évaluer les menaces de leur environnement et considérer si des mécanismes de sécurité supplémentaires devraient être employés.

9 Journal des modifications

Les changements suivants ont été apportés depuis la RFC 2138 :

Les chaînes devraient utiliser UTF-8 au lieu de l'US-ASCII et devraient être traitées comme des données en octets de 8 bits.

Les entiers et les dates sont maintenant définis comme des valeurs de 32 bits non signées.

La liste mise à jour des attributs qui peuvent être inclus dans Epreuve-d'accès pour être cohérent avec le tableau des attributs.

Le Nom-d'utilisateur mentionne les identifiants d'accès réseau.

Le Nom-d'utilisateur peut maintenant être envoyé dans Accès-Accepté pour être utilisé avec accounting et Rlogin.

Des valeurs sont ajoutées pour Type-de-Service, Service-de-Connexion, Protocole-tramé, Compression-tramée, et Type-d'accès-de-NAS.

Accès-de-NAS peut maintenant utiliser tous les 32 bits.

Les exemples comportent maintenant l'affichage hexadécimal des paquets.

Le port UDP de source doit être utilisé conjointement avec l'identifiant de demande lors de l'identification de doublons.

Plusieurs sous attributs peuvent être admis dans un attribut spécifique de fabricant.

Il est maintenant exigé qu'une Demande-d'accès contienne un attribut Adresse-IP-de-NAS ou Identifiant-de-NAS (ou peut contenir les deux).

Ajout de notes sous "Fonctionnement" avec plus d'informations sur mandataires, retransmissions, et garder-en-vie. Si plusieurs attributs du même Type sont présents, l'ordre des attributs du même type DOIT être préservé par tous les mandataires.

Précision de État-de-mandataire.

Précision que les attributs ne doivent pas dépendre de leur position au sein du paquet, tant que les attributs de même type sont gardés dans l'ordre.

Ajout d'une section de Considérations relatives à l'IANA.

Mise à jour du paragraphe sur "Mandataire" dans "Fonctionnement".

MTU-tramée peut maintenant être envoyé comme indication dans une demande d'accès.

Mise à jour des Considérations sur la sécurité.

Les chaînes Texte sont identifiées comme sous-ensemble de Chaîne, pour préciser l'utilisation de UTF-8.

10 Références

- [1] C. Rigney, A. Rubens, W. Simpson et S. Willens, "Service d'authentification à distance de l'utilisateur appelant (RADIUS)", RFC 2138, avril 1997.

- [2] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, RFC 2119, mars 1997.
- [3] R. Rivest et S. Dusse, "Algorithme MD5 de résumé de message", RFC 1321, avril 1992.
- [4] J. Postel, "Protocole de datagramme d'utilisateur", STD 6, RFC 768, août 1980.
- [5] C. Rigney, "Comptabilité RADIUS", RFC 2866, juin 2000.
- [6] J. Reynolds et J. Postel, "Allocation des numéros", STD 2, RFC 1700, octobre 1994.
- [7] F. Yergeau, "UTF-8, un format de transformation de ISO 10646", RFC 2279, janvier 1998 (*rendue obsolète par la RFC 3629, novembre 2003*).
- [8] B. Aboba et M. Beadles, "Identifiant d'accès du réseau", RFC 2486, janvier 1999.
- [9] C. Kaufman, R. Perlman et M. Speciner, "Sécurité du réseau : Communications privées dans un monde public", Prentice Hall, mars 1995, ISBN 0-13-061466-1.
- [10] V. Jacobson, "Compression des en-têtes TCP/IP pour les liaisons séries à basse vitesse", RFC 1144, février 1990.
- [11] Norme internationale ISO 8859. – Traitement de l'information – Jeux de caractères codés sur un seul octet de 8 bits -- Partie 1 : Alphabet latin n° 1, ISO 8859-1:1987.
- [12] K. Sklower, B. Lloyd, G. McGregor, D. Carr et T. Coradetti, "Protocole multi liaisons PPP (MP)", RFC 1990, août 1996.
- [13] H. Alvestrand et T. Narten, "Lignes directrices pour la rédaction de la section Considérations relatives à l'IANA dans les RFC", BCP 26, RFC 2434, octobre 1998.
- [14] J. Galvin, K. McCloghrie et J. Davin, "Protocoles de sécurité SNMP", RFC 1352, juillet 1992.
- [15] H. Dobbertin, "L'état de MD5 après les attaques récentes", CryptoBytes Vol.2 n° 2, été 1996.

11 Remerciements

RADIUS a été développé à l'origine par Steve Willens de Livingston Enterprises pour leur série PortMaster de serveurs d'accès réseau.

12 Adresse du président du groupe de travail

Le groupe de travail peut être contacté par l'intermédiaire de son président :

Carl Rigney
Livingston Enterprises
4464 Willow Road
Pleasanton, California 94588
téléphone : +1 925 737 2100
mél : cdr@telemancy.com

13 Adresse des auteurs

Les questions au sujet du présent mémo peuvent aussi être adressées à :

Carl Rigney	Allan C. Rubens
Livingston Enterprises	Merit Network, Inc.
4464 Willow Road	4251 Plymouth Road
Pleasanton, California 94588	Ann Arbor, Michigan 48105-2785

Téléphone : +1 925 737 2100	USA
mél : cdr@telemancy.com	mél : acr@merit.edu

William Allen Simpson	Steve Willens
Daydreamer	Livingston Enterprises
Computer Systems Consulting Services	4464 Willow Road
1384 Fontaine	Pleasanton, California 94588
Madison Heights, Michigan 48071	USA
mél : wsimpson@greendragon.com	mél : steve@livingston.com

14. Déclaration de droits de reproduction

Copyright (C) The Internet Society (2000). Tous droits réservés.

Le présent document et ses traductions PEUVENT être copiées et fournis à des tiers et les travaux dérivés qui le commentent ou l'explique ou aident à sa mise en œuvre PEUVENT être préparés, copiés, publiés et distribués, en tout ou en partie, sans restrictions d'aucune sorte, pourvu que la déclaration de droits de propriété intellectuelle ci dessus et le présent paragraphe soient inclus dans toute copies et travaux dérivés. Cependant, le présent document lui-même NE PEUT être modifié d'aucune façon, telle qu'en retirant la déclaration de copyright ou les références à la Internet Society ou autres organisations Internet, excepté en tant que de besoin pour le développement des normes Internet, auquel cas les procédures de copyright définies dans le processus de normalisation Internet DOIVENT être suivies, ou comme nécessaire pour le traduire dans des langues autres que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles ne seront pas révoquées par la Internet Society, ses successeurs ou ayants droit.

Le présent document et les informations qu'il contient sont fournis sur une base "EN L'ETAT" et la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toute responsabilité, explicite ou implicite, y compris, mais non limitée à toute garantie que l'utilisation des informations ci-enclosent ne violent aucun droit ou aucune garantie implicite de commerciabilité ou d'adaptation à un objet particulier.

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.

Remerciement

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