Groupe de travail Réseau
Request for Comments : 2866
Catégorie : Information
RFC rendue obsolète : 2139

C. Rigney, Livingston
juin 2000

Traduction Claude Brière de L'Isle

Comptabilité de RADIUS

Statut de ce mémoire
Le présent mémoire donne des informations pour la communauté de l'Internet. Il ne spécifie aucune sorte de norme pour l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent document décrit un protocole pour transporter des informations de comptabilité entre un serveur d'accès de réseau et un serveur de comptabilité partagé.

Note de mise en oeuvre
Le présent mémoire expose le protocole de comptabilité RADIUS. Les premiers développements de la comptabilité RADIUS ont été faits sur le numéro d'accès UDP 1646, qui est en conflit avec le service "sa-msg-port". Le numéro d'accès officiellement alloué à la comptabilité RADIUS est 1813.

Table des Matières

1 Introduction

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, ils demandent une attention soutenue à la sécurité, à l'autorisation 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).

Le document RADIUS (*Remote Authentication Dial In User Service*) [2] spécifie le protocole RADIUS utilisé pour l'authentification et l'autorisation. Le présent mémoire étend l'utilisation du protocole RADIUS de façon à couvrir la livraison des informations de comptabilité du serveur d'accès réseau (NAS, *Network Access Server*) à un serveur de comptabilité RADIUS.
Le présent document rend obsolète la RFC 2139 [1]. Un résumé des changements depuis la RFC 2139 figure à la Section 8 "Journal des modifications". Les dispositifs clés de RADIUS sont :

Le modèle client/serveur : Un serveur d'accès réseau (NAS, *Network Access Server*) fonctionne comme client du serveur de comptabilité RADIUS. Le client est chargé du passage des informations de comptabilité d'usager au serveur de comptabilité RADIUS désigné.

Le serveur de comptabilité RADIUS est chargé de recevoir les demandes de comptabilité d'usager et de retourner une réponse au client indiquant qu'il a bien reçu la demande. Le serveur de comptabilité RADIUS peut agir comme client mandataire d'autres sortes de serveurs de comptabilité.

Sécurité du réseau : Les transactions entre le client et le serveur de comptabilité RADIUS sont authentifiées grâce à l'utilisation d'un secret partagé, qui n'est jamais envoyé sur le réseau.

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 la RFC 2119 [3]. Ces mots clé signifient la même chose en majuscule ou en minuscules.

1.2 Terminologie

Le présent document utilise 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 l'usager appelant constitue une session, le début de la session étant défini comme le point où le service est fourni en premier et la fin de la session étant définie comme le point où le service se termine. Un usager peut avoir plusieurs sessions en parallèle ou en série si le NAS l'accepte, chaque session générant des enregistrements de début et de fin séparés avec leur propre identifiant de session de comptabilité Acct-Session-Id.

éliminé en silence : Cela signifie que la mise en œuvre élimine le paquet sans autre traitement. La mise en œuvre DEVRAIT fournir la capacité d'enregistrer les erreurs, y compris le contenu des paquets éliminés en silence, et DEVRAIT enregistrer les événements dans un compteur à des fins statistiques.

2 Fonctionnement

Lorsqu'un client est configuré pour utiliser la comptabilité RADIUS, au début de la livraison du service, il va générer un paquet Début de comptabilité qui décrit le type de service fourni et l'usager à qui il est fourni, et il va l'envoyer au serveur de comptabilité RADIUS, qui va lui renvoyer un accusé de réception du paquet. À la fin de la fourniture du service, le client va générer un paquet d'arrêt de comptabilité qui décrit le type de service qui a été fourni et facultativement des

statistiques telles que le temps écoulé, les octets d'entrée et de sortie, ou les paquets entrés et sortis. Il va envoyer cela au serveur de comptabilité RADIUS, qui va renvoyer un accusé de réception du paquet.

La Demande-de-comptabilité (aussi bien pour le début que pour l'arrêt) est soumise au serveur de comptabilité RADIUS via le réseau. Il est recommandé que le client continue de tenter d'envoyer le paquet Demande-de-comptabilité jusqu'à ce qu'il reçoive un accusé de réception, en utilisant une forme quelconque de sauvegarde. Si aucune réponse n'est retournée dans un délai d'une heure, la demande est renvoyée un certain nombre de fois. Le client peut aussi transmettre des demandes à un ou 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 un certain nombre d'échec d'essais au serveur principal, soit à la façon round-robin. Les algorithmes de réessai et de repli font actuellement l'objet de recherches et ne sont pas spécifiés en détail dans le présent document.

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

Si le serveur de comptabilité RADIUS est dans l'incapacité d'enregistrer avec succès le paquet de comptabilité, il NE DOIT PAS envoyer d'accusé de réception Réponse-de-comptabilité au client.

2.1 Mandataire

Voir la RFC "RADIUS" [2] pour des informations sur le mandataire RADIUS. Le mandataire de comptabilité RADIUS fonctionne de la même façon, comme illustré par l'exemple suivant.

1 Le NAS envoie une Demande-de-comptabilité au serveur de transmission.

2 Le serveur de transmission enregistre la Demande-de-comptabilité (s'il le souhaite), ajoute son État-de-mandataire (si il le souhaite) après tous les autres attributs État-de-mandataire, met à jour l'authentificateur de demande, et transmet la demande au serveur distant.

3 Le serveur distant enregistre la Demande-de-comptabilité (si il le souhaite), copie tous les attributs État-de-mandataire dans l'ordre et non modifiés à partir de la demande du paquet de réponse, et envoie la réponse de comptabilité au serveur de transmission.

4 Le serveur de transmission efface le dernier État-de-mandataire (s'il en avait ajouté un à l'étape 2), met à jour l'authentificateur de réponse et envoie la réponse de comptabilité au NAS.

Un serveur de transmission NE DOIT PAS modifier des attributs État-de-mandataire, ou Classe existants présents dans le paquet.

Un serveur de transmission peut soit effectuer sa fonction de transmission de façon transparente, où il fait les retransmissions aussitôt qu'il les reçoit, soit prendre la responsabilité des retransmissions, par exemple dans les cas où la liaison réseau entre le serveur de transmission et le serveur distant a des caractéristiques très différentes de celle de la liaison entre le NAS et le serveur de transmission.

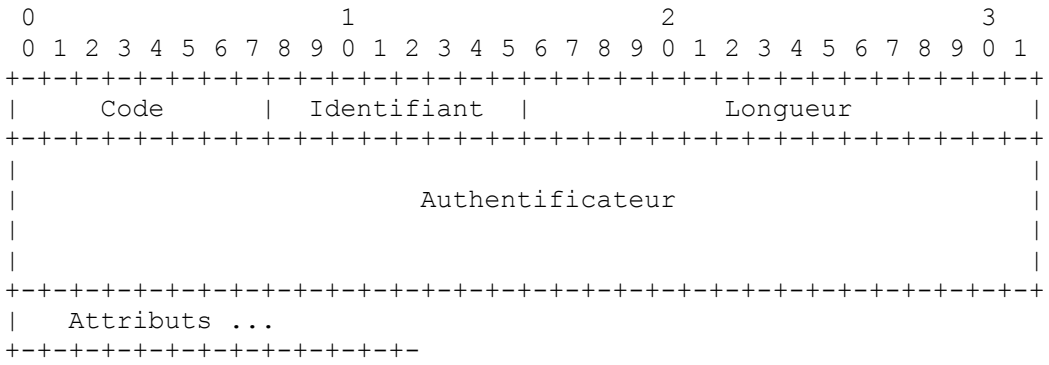
Une attention extrême devrait être portée à la mise en œuvre d'un serveur mandataire qui prend la responsabilité des retransmissions afin que sa politique de retransmission soit robuste et mesurable.

3 Format de paquet

Exactement un paquet de comptabilité RADIUS est encapsulé dans le champ de données UDP [4], et le champ Accès-de-destination UDP indique 1813 (en décimal). Lorsque une réponse est générée, les accès de source et de destination sont inversés.

Le présent mémoire expose le protocole de comptabilité RADIUS. Les premiers développements de RADIUS utilisaient le numéro d'accès UDP 1646, qui est en conflit avec le service " sa-msg-port ". Le numéro d'accès officiellement alloué pour RADIUS est 1813.

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



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

Les codes de comptabilité RADIUS (en décimal) sont allouée comme suit :

4 Demande-de-comptabilité
5 Réponse-de-comptabilité

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 plus fort poids est transmis en premier. Cette valeur est utilisée pour authentifier les messages entre le client et le serveur de comptabilité RADIUS.

Authentificateur de demande
Dans les paquets Demande-de-comptabilité, la valeur de l'authentificateur est une somme de contrôle MD5 [5] de 16 octets, appelée l'authentificateur de demande.

Le NAS et le serveur de comptabilité RADIUS partagent un secret. Le champ authentificateur de demande dans les paquets Demande-de-comptabilité contient un hachage MD5 unidirectionnel calculé sur un flux d'octets consistant en le Code + Identifiant + Longueur + 16 octets à zéro + les attributs de la demande + le secret partagé (+ indique l'enchaînement). La valeur du hachage MD5 de 16 octets est mémorisée dans le champ authentificateur du paquet Demande-de-comptabilité.

Noter que l'authentificateur de demande d'une Demande-de-comptabilité ne peut pas être constitué de la même façon que l'authentificateur de demande d'une Demande-d'accès RADIUS, parce qu'il n'y a pas d'attribut Mot-de-passe-d'utilisateur dans une Demande-de-comptabilité.

Authentificateur de réponse
Le champ Authentificateur dans un paquet Réponse-de-comptabilité est appelé authentificateur de réponse, et contient un hachage MD5 unidirectionnel calculé sur un flux d'octets comportant le code de Réponse-de-comptabilité, Identifiant, Longueur, le champ Authentificateur-de-demande tiré du paquet Demande-de-comptabilité auquel il répond, et les attributs de réponse s'il en est, suivis par le secret partagé. La valeur du hachage MD5 de 16 octets est mémorisée dans le champ Authentificateur du paquet de Réponse-de-comptabilité.

Attributs
Il peut y avoir plusieurs instances d'attributs, auquel cas l'ordre des attributs de même type DEVRAIT être préservé. L'ordre des attributs de différents types n'est pas obligatoirement préservé.

4 Types de paquet

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

4.1 Demande-de-comptabilité

Description
Les paquets Demande-de-comptabilité sont envoyés d'un client (normalement un serveur d'accès réseau ou son mandataire) au serveur de comptabilité RADIUS, et ils convoient des informations utilisées pour établir la comptabilité du service fourni à un usager. Le client transmet un paquet RADIUS avec le champ Code réglé à 4 (Demande-de-comptabilité).

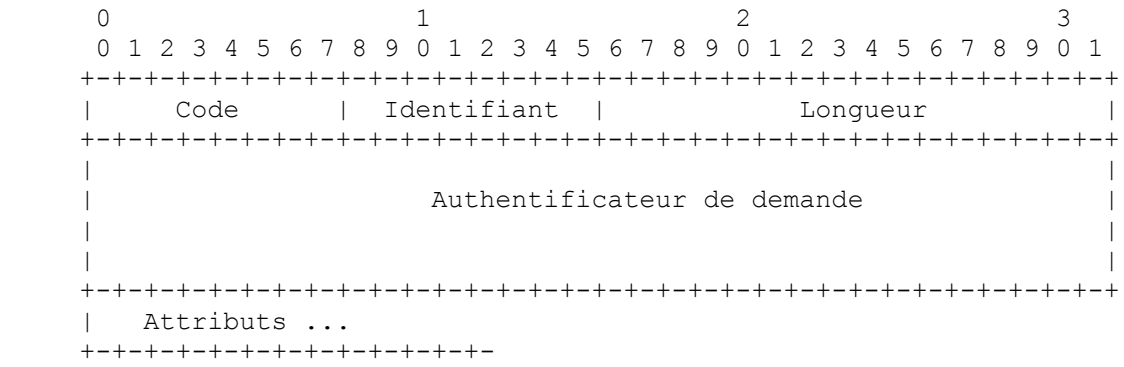
À réception d'une Demande-de-comptabilité, le serveur DOIT transmettre une réponse Réponse-de-comptabilité si il a réussit à enregistrer le paquet comptable, et NE DOIT PAS transmettre de réponse si il échoue à enregistrer le paquet comptable.

Tout attribut valide dans un paquet Demande-d'accès ou Accès-accepté RADIUS est valide dans un paquet Demande-de-comptabilité RADIUS, sauf que les attributs suivants NE DOIVENT PAS être présents dans Demande-de-comptabilité : Mot-de-passe-d'utilisateur, Mot-de-passe-CHAP, Message-de-réponse, État.

Adresse-IP-de-NAS ou Identifiant-de-NAS DOIT être présent dans une Demande-de-comptabilité RADIUS. Il DEVRAIT contenir un attribut Accès-de-NAS ou Type-d'accès-de-NAS ou les deux sauf si le service n'implique pas d'accès ou si le NAS ne fait pas de distinction entre ses accès.

Si le paquet Demande-de-comptabilité comporte une Adresse-IP-tramée, cet attribut DOIT contenir l'adresse IP de l'usager. Si l'Accès-accepté utilisait des valeurs particulières pour Adresse-IP-tramée disant au NAS d'allouer ou négocier une adresse IP pour l'usager, Adresse-IP-tramée (s'il en est une) dans la Demande-de-comptabilité DOIT contenir l'adresse IP réelle allouée ou négociée.

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



Code : 4 pour Demande-de-comptabilité.

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, lorsque le contenu est identique, l'identifiant DOIT rester inchangé.

Noter que si Durée-du-délai-de-compta est inclus dans les attributs d'une Demande-de-comptabilité, la valeur de Acct-Delay-Time sera mise à jour lorsque le paquet sera retransmis, changeant le contenu du champ Attributs et exigeant un nouvel identifiant et authentificateur de demande.

Authentificateur de demande
L'authentificateur de demande d'une Demande-de-comptabilité contient une valeur de hachage MD5 de 16 octets calculée conformément à la méthode décrite dans "Authentificateur de demande" ci-dessus.

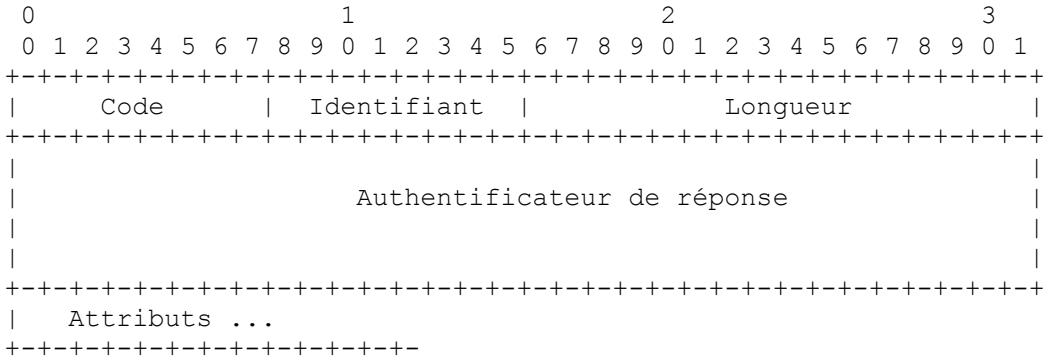
Attributs : Le champ Attribut est de longueur variable, et contient une liste des attributs.

4.2 Réponse-de-comptabilité

Description
Les paquets Réponse-de-comptabilité sont envoyés par le serveur de comptabilité RADIUS au client pour accuser bonne réception de cette Demande-de-comptabilité et de son enregistrement. Si la Demande-de-comptabilité a bien été enregistrée, le serveur de comptabilité RADIUS DOIT transmettre un paquet avec le champ Code réglé à 5 (Réponse-de-comptabilité). À réception d'une Réponse-de-comptabilité par le client, le champ Identifiant est confronté à une Demande-de-comptabilité en instance. Le champ Authentificateur de réponse DOIT contenir la réponse correcte pour la Demande-de-comptabilité en instance. Les paquets invalides sont éliminés en silence.

Une Réponse-de-comptabilité RADIUS n'est pas obligée de comporter d'attribut.

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



Code : 5 pour Réponse-de-comptabilité.

Identifiant
Le champ Identifiant est une copie du champ Identifiant de la Demande-de-comptabilité qui a causé cette Réponse-de-comptabilité.

Authentificateur de réponse
L'authentificateur de réponse d'une Réponse-de-comptabilité contient une valeur de hachage MD4 de 16 octets calculée conformément à la méthode décrite dans "Authentificateur de réponse" ci-dessus.

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

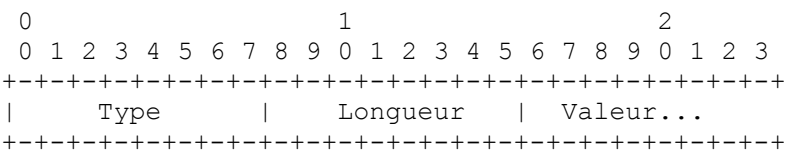
5 Attributs

Les attributs RADIUS portent les détails spécifiques d'authentification, d'autorisation, et les précisions comptables pour la demande et la réponse.

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.

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

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



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 réservées 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.

La présente spécification concerne les valeurs suivantes :

1-39	(se reporter au document RADIUS [2])
40	Type-d'état-de-compta
41	Durée-du-délai-de-compta
42	Octets-d'entrée-de-compta
43	Octets-de-sortie-de-compta
44	Identifiant-de-session-de-compta
45	Authentification-de-compta
46	Durée-de-session-de-compta
47	Paquets-d'entrée-de-compta
48	Paquets-de-sortie-de-compta
49	Cause-de-fin-de-compta
50	Identifiant-multi-session-de-compta
51	Compte-de-liaisons-de-compta
60+	(se reporter au document RADIUS [2])

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, la demande toute entière DOIT être éliminée 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 des 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 devaient veiller à ne pas utiliser strcpy() dans le traitement des chaînes. .

Il y a cinq types de données pour le format du champ Valeur. Noter que le type "texte" est un sous-ensemble du type "chaîne."

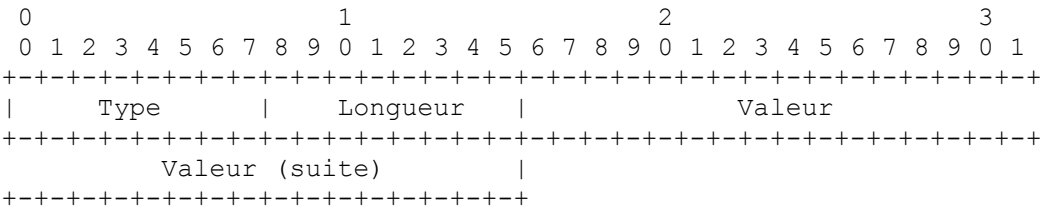
texte	1 à 253 octets contenant des caractères ISO 10646 codés en UTF-8 [7]. Un texte de longueur zéro (0) NE DOIT PAS être envoyé ; il faut à la place omettre l'attribut tout entier.
chaîne	1 à 253 octets contenant des données binaires (valeurs de 0 à 255 en décimal, incluses). Les chaînes de longueur zéro (0) NE DOIVENT PAS être envoyées ; omettre à la place l'attribut entier.
adresse	valeur de 32 bits, octet de plus fort poids en premier.
entier	valeur de 32 bits non signée, octet de plus fort poids en premier.
heure	valeur de 32 bits non signée, octet de plus fort poids en premier -- les secondes depuis 00:00:00 UTC, au 1 er janvier 1970. Les attributs standard n'utilisent pas ce type de données mais il est présenté ici pour une utilisation possible dans des attributs à l'avenir.

5.1 Type-d'état-de-compta

Description
Cet attribut indique si cette Demande-de-comptabilité marque le début du service de l'usager (Start) ou la fin (Stop). Il

PEUT être utilisé par le client pour marquer le début de la comptabilité (par exemple, à l'amorçage) en spécifiant Compta-en-cours et pour marquer la fin de la comptabilité (par exemple, juste avant un réamorçage programmé) en spécifiant Compta-terminée.

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



Type : 40 pour Type-d'état-de-compta.
Longueur : 6
Valeur : Le champ Valeur est de quatre octets.

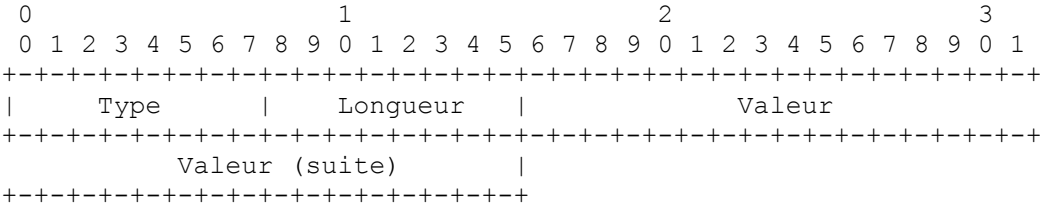
1	Début
2	Fin
3	Mise-à-jour-intérimaire
7	Compta-en-cours
8	Compta-terminée
9-14	Réservé pour un tunnel de comptabilité
15	Réservé pour l'échec

5.2 Durée-du-délai-de -compta

Description
Cet attribut indique pendant combien de secondes le client a essayé d'envoyer cet enregistrement, et peut être soustrait de l'heure d'arrivée au serveur pour trouver l'heure approximative de l'événement qui a généré cette Demande-de-comptabilité. (Le temps de transit du réseau est ignoré.)

Noter que changer Durée-du-délai-de-compta cause le changement de l'identifiant ; voir la discussion sur Identifiant ci-dessus.

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

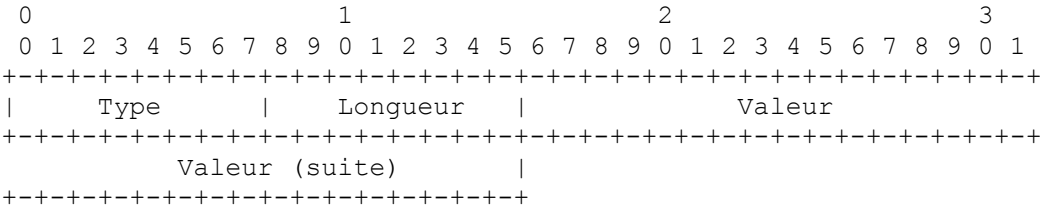


Type : 41 pour Durée-du-délai-de-compta.
Longueur : 6
Valeur : Le champ Valeur est de quatre octets.

5.3 Octets-d'entrée-de-compta

Description
Cet attribut indique combien d'octets ont été reçus de l'accès pendant le temps ou ce service a été fourni, et il ne peut être présent que dans les enregistrements de Demande-de-comptabilité où Type-d'état-de-compta est réglé à Fin.

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

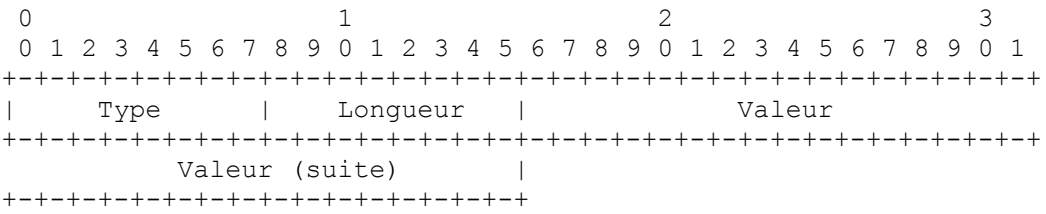


Type : 42 pour Octets-d'entrée-de-compta.
Longueur : 6
Valeur : Le champ Valeur est de quatre octets.

5.4 Octets-de-sortie-de-compta

Description
Cet attribut indique combien d'octets ont été envoyés à l'accès dans le cours de la fourniture de ce service, et il ne peut être présent dans les enregistrements de Demande-de-comptabilité que quand le Type-d'état-de-compta est réglé à Fin.

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



Type : 43 pour Octets-de-sortie-de-compta.
Longueur : 6
Valeur : Le champ Valeur est de quatre octets.

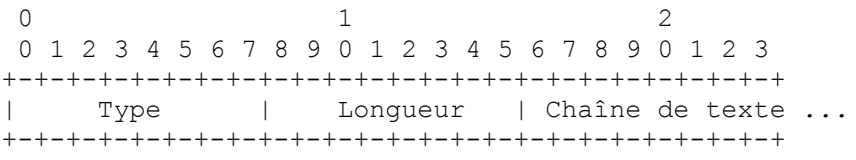
5.5 Identifiant-de-session-de-compta

Description
Cet attribut est un identifiant de comptabilité unique pour faciliter la confrontation des enregistrements de début et de fin dans un fichier de journalisation. Les enregistrements de début et de fin pour une session donnée DOIVENT avoir le même Identifiant-de-session-de-compta. Un paquet de Demande-de-comptabilité DOIT avoir un Identifiant-de-session-de-compta. Un paquet de Demande-d'accès PEUT avoir un Identifiant-de-session-de-compta ; si il en a un, le NAS DOIT alors utiliser le même Identifiant-de-session-de-compta dans les paquets de Demande-de-comptabilité pour cette session.

Identifiant-de-session-de-compta DEVRAIT contenir des caractères de la norme ISO 10646 codés en UTF-8 [7].

Par exemple, une mise en œuvre utilise une chaîne avec un nombre hexadécimal de huit chiffres en majuscules, les deux premiers chiffres s'incrémentent à chaque réamorçage (revenant à zéro tous les 256 réamorçages) et les 6 chiffres suivants comptant à partir de 0 pour la première personne qui se connecte après un réamorçage jusqu'à 2^24-1, soit environ 16 millions. D'autres codages sont possibles.

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

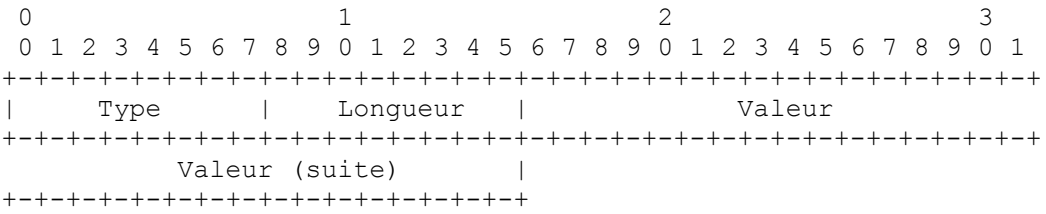


Type : 44 pour Identifiant-de-session-de-compta.
Longueur : ≥ 3
Chaîne : le champ Chaîne DEVRAIT être une chaîne de caractères de la norme ISO 10646 codés en UTF-8 [7].

5.6 Authentification-de-compta

Description
Cet attribut PEUT être inclus dans une Demande-de-comptabilité pour indiquer comment l'usager a été authentifié, par RADIUS, par le NAS lui-même, ou par un autre protocole d'authentification à distance. Les usagers à qui le service est fourni sans avoir été authentifiés NE DEVRAIENT PAS générer d'enregistrements de comptabilité.

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



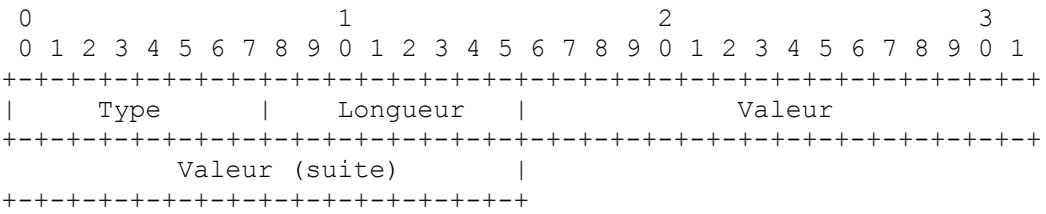
Type : 45 pour Authentification-de-compta.
Longueur : 6
Valeur : Le champ Valeur est de quatre octets.

1	RADIUS
2	Local
3	Distant

5.7 Durée-de-session-de-compta

Description
Cet attribut indique pendant combien de secondes l'usager a bénéficié du service, et il ne peut être présent que dans les enregistrements de Demande-de-comptabilité où le Type-d'état-de-compta est réglé à Fin.

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

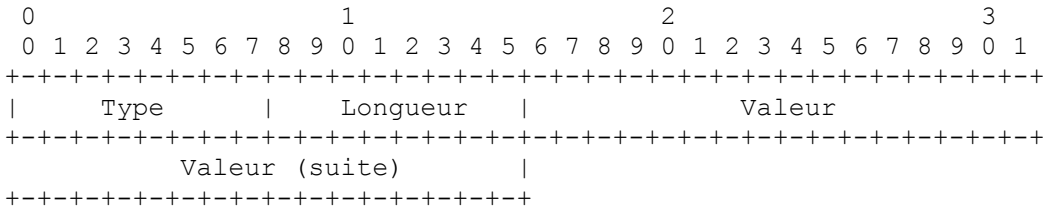


Type : 46 pour Durée-de-session-de-compta.
Longueur : 6
Valeur : Le champ Valeur est de quatre octets.

5.8 Paquets-d'entrée-de-compta

Description
Cet attribut indique combien de paquets ont été reçus de l'accès pendant le cours de la fourniture de ce service à un usager tramé, et il ne peut être présent que dans les enregistrements de Demande-de-comptabilité où le Type-d'état-de-compta est réglé à Fin.

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

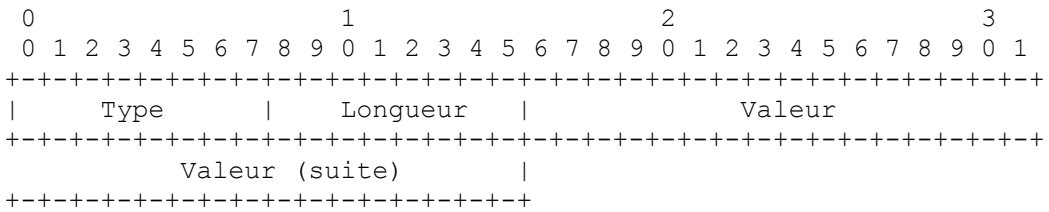


Type : 47 pour Paquets-d'entrée-de-compta.
Longueur : 6
Valeur : Le champ Valeur est de quatre octets.

5.9 Paquets-de-sortie-de-compta

Description
Cet attribut indique combien de paquets ont été envoyés sur l'accès dans le cours de la fourniture de ce service à un usager tramé, et il ne peut être présent que dans des enregistrements de Demande-de-comptabilité où le Type-d'état-de-compta est réglé à Fin.

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

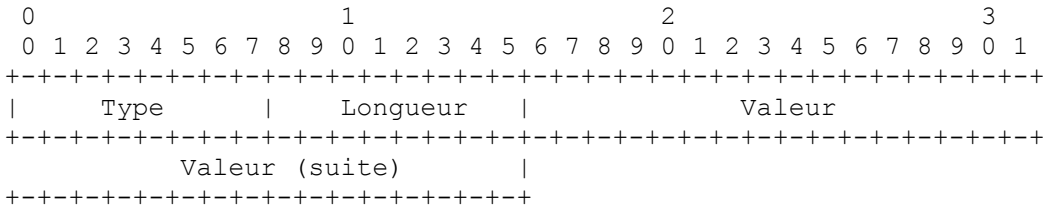


Type : 48 pour Paquets-de-sortie-de-compta.
Longueur : 6
Valeur : le champ Valeur est de quatre octets.

5.10 Cause-de-fin-de-compta

Description
Cet attribut indique comment la session s'est terminée, et il ne peut être présent que dans des enregistrements de Demande-de-comptabilité où le Type-d'état-de-compté est réglé à Fin.

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



Type : 49 pour Cause-de-fin-de-compta

Longueur : 6

Valeur : Le champ Valeur est de quatre octets, contenant un entier qui spécifie la cause de la fin de la session, comme suit :

1	Demande de l'usager
2	Perte de la porteuse
3	Perte du service
4	Fin de temporisation d'inactivité
5	Fin de temporisation de session
6	Redémarrage administratif
7	Réamorçage administratif
8	Erreur d'accès
9	Erreur de NAS
10	Demande du NAS
11	Réamorçage du NAS
12	Accès non nécessaire
13	Accès préempté
14	Accès suspendu
15	Service indisponible
16	Rappel
17	Erreur de l'usager
18	Demande de l'hôte

Les causes de fin sont les suivantes :

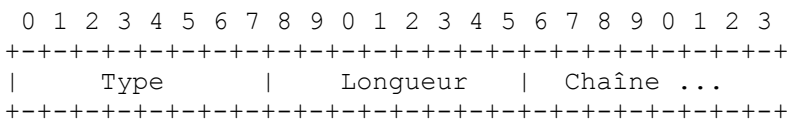
Demande de l'usager	L'usager a demandé la fin du service, par exemple avec LCP Terminate ou en déconnectant
Perte de la porteuse	Le détecteur de la porteuse de données a été abandonné sur l'accès
Perte du service	Le service ne peut plus être fourni ; par exemple, la connexion de l'usager à un hôte a été interrompue.
Fin de temporisation d'inactivité	Le temporisateur d'inactivité est arrivé à expiration
Fin de temporisation de session	Le temporisateur de longueur maximum de session est arrivé à expiration
Redémarrage administratif	L'administrateur a redémarré l'accès ou la session.
Réamorçage administratif	L'administrateur met fin au service sur le NAS, par exemple avant de réamorcer le NAS.
Réamorçage administratif	Le NAS a détecté sur l'accès une erreur qui exige de mettre fin à la session.
Erreur de NAS	Le NAS a détecté une erreur (autre que d'accès) qui exige la fin de session.
Demande du NAS	Le NAS met fin à la session pour une raison autre qu'une erreur non autrement précisée ici.
Réamorçage du NAS	Le NAS termine la session pour un réamorçage non administratif ("crash").
Accès non nécessaire	Le NAS termine la session parce que l'utilisation de la ressource est tombé en dessous du niveau minimum (par exemple, si un algorithme de bande passante à la demande décide que l'accès n'est plus nécessaire).
Accès préempté	Le NAS termine la session afin d'allouer l'accès à un usage de plus forte priorité
Accès suspendu	Le NAS termine la session pour suspendre une session virtuelle.
Service indisponible	Le NAS n'a pas été capable de fournir le service demandé.
Rappel	Le NAS termine la session en cours afin d'effectuer un rappel pour une nouvelle session.
Erreur de l'usager	Les entrées de l'usager sont erronées, causant la fin de la session.
Demande de l'hôte	L'hôte de connexion a terminé la session normalement.

5.11 Identifiant-multi-session-de-compta

Description
Cet attribut est un identifiant unique de comptabilité pour faciliter la liaison de plusieurs sessions en relation dans un fichier de journalisation. Chaque session liée avec les autres aura un Identifiant-de-session-de-compta unique mais le même Identifiant-multi-session-de-compta. Il est fortement recommandé que l'Identifiant-multi-session-de-compta contienne des caractères de la norme ISO 10646 codés en UTF-8 [7].

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

```
0                   1                   2
```

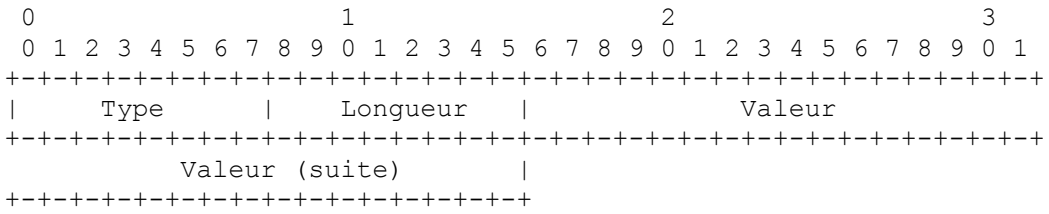


Type : 50 pour Identifiant-multi-session-de-compta.
Longueur : ≥ 3
Chaîne : le champ Chaîne DEVRAIT contenir des caractères de la norme ISO 10646 codés en UTF-8 [7].

5.12 Compte-de-liaisons-de-compta

Description
Cet attribut donne le compte des liaisons qui sont connues pour avoir été dans une session multi-liaisons donnée au moment où a été généré l'enregistrement de comptabilité. Le NAS PEUT inclure l'attribut Compte-de-liaisons-de-compta dans toute Demande-de-comptabilité qui pourrait avoir des liaisons multiples.

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



Type : 51 pour Compte-de-liaisons-de-compta.
Longueur : 6
Valeur : Le champ Valeur est de quatre octets, et contient le nombre de liaisons connues pour cette session multi-liaisons.

Il peut être utilisé pour faciliter à un serveur de comptabilité le recensement des enregistrements pour une session multi-liaison donnée. Lorsque le nombre de Demande-de-comptabilité reçu avec Type-d'état-de-compta = Fin et le même Identifiant-multi-session-de-compta et l'Identifiant-de-session-de-compta unique égal à la plus grande valeur de Compte-de-liaisons-de-compta vu dans ces Demande-de-comptabilité, toutes les Fin de Demande-de-comptabilité pour cette session multi-liaison auront été reçues.

Un exemple montrant 8 Demande-de-comptabilité devraient rendre les choses plus claires. Pour les besoins de l'exemple, seul les attributs pertinents figurent ici, mais des attributs supplémentaires comportant les informations comptables seront aussi présents dans la Demande-de-comptabilité.

Identifiant-multi-session	Identifiant-de-session	Type-d'état	Compte-de-liaisons
"10"	"10"	Start	1
"10"	"11"	Start	2
"10"	"11"	Stop	2
"10"	"12"	Start	3
"10"	"13"	Start	4
"10"	"12"	Stop	4
"10"	"13"	Stop	4
"10"	"10"	Stop	4

5.13 Tableau des attributs

Le tableau suivant est un guide des attributs qui peuvent se trouver dans les paquets Demande-de-comptabilité. Aucun attribut ne devrait se trouver dans les paquets de Réponse de comptabilité sauf État-de-mandataire et éventuellement Spécifique-du-fabricant.

Entrées	**Attribut**
0-1	Nom-d'utilisateur

0	Mot-de-passe-d'utilisateur
0	Mot-de-passe-CHAP
0-1	Adresse-IP-de-NAS [Note]
0-1	Accès-de-NAS
0-1	Type-de-service
0-1	Protocole-tramé
0-1	Adresse-IP-tramée
0-1	Gabarit-réseau-IP-tramé
0-1	Routage-tramé
0+	Identifiant-de-filtre
0-1	MTU-tramée
0+	Compression-tramée
0+	Hôte-de-connexion-IP
0-1	Service-de-connexion
0-1	Port-de-connexion-TCP
0	Message-de-réponse
0-1	Numéro-de-rappel
0-1	Identifiant-de-rappel
0+	Route-tramée
0-1	Réseau-IPX-tramé
0	Réseau-IPX-tramé
0+	Classe
0+	Spécifique-du-fabricant
0-1	Durée-de-session
0-1	Durée-d'inactivité
0-1	Action-de-terminaison
0-1	Identifiant-de-station-appelée
0-1	Identifiant-de-station-appelante
0-1	Identifiant-de-NAS [Note]
0+	État-de-mandataire
0-1	Service-LAT-de-connexion
0-1	Nœud-LAT-de-connexion
0-1	Groupe-LAT-de-connexion
0-1	Liaison-AppleTalk-tramée
0-1	Réseau-AppleTalk-tramé
0-1	Zone-AppleTalk-tramée
1	Type-d'état-compta
0-1	Durée-du-délai-de-compta
0-1	Octets-d'entrée-de-compta
0-1	Octets-de-sortie-de-compta
1	Identifiant-session-compta
0-1	Authentification-de-compta
0-1	Durée-de-session-de-compta
0-1	Paquets-d'entrée-compta
0-1	Paquets-de-sortie-compta
0-1	Cause-de-fin-de-compta
0+	Identifiant-compta-multi-session
0+	Compte-de-liaison-compta
0	Épreuve-CHAP
0-1	Type-d'accès-de-NAS
0-1	Limite-d'accès
0-1	Accès-de-connexion-LAT

[Note] Une Demande-de-comptabilité DOIT contenir une Adresse-IP-de-NAS ou un Identifiant-de-NAS (ou les deux).

Le tableau suivant définit les 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

Les codes de type de paquet, les types d'attribut, et les valeurs d'attribut définis dans le présent document sont enregistrés par l'autorité d'allocation des numéros de l'Internet (IANA, Internet Assigned Numbers Authority) à partir des espaces de nom RADIUS comme décrit dans la section "Considérations relatives à l'IANA" de la RFC 2865 [2], conformément au BCP 26 [8].

7 Considérations pour la sécurité

Les questions de sécurité sont exposées dans les paragraphes concernant l'authentificateur inclus dans les demandes et réponses de comptabilité, en utilisant un secret partagé qui n'est jamais envoyé sur le réseau.

8 Journal des modifications

US-ASCII remplacé par UTF-8.
Ajout de notes sur mandataire.
Adresse-IP-tramée devrait contenir l'adresse IP réelle de l'usager.
Si ID-de-session-compta a été envoyé dans une demande d'accès, il doit être utilisé dans la Demande-de-comptabilité pour cette session.
De nouvelles valeurs sont ajoutées à Type-d'état-compta.
Ajout de la section Considérations relatives à l'IANA.
Mise à jour des références.
Les chaînes Texte sont identifiées comme un sous-ensemble de chaîne, pour préciser l'utilisation de UTF-8.

9 Références

[1] C. Rigney, "Comptabilité de RADIUS", RFC 2139, avril 1997.
[2] C. Rigney, S. Willens, A. Rubens et W. Simpson, "Service d'authentication à distance de l'usager appelant (RADIUS)", RFC 2865, juin 2000.
[3] S. Bradner, "Mots clés à utilise dans les RFC pour indiquer les niveaux d'exigence", BCP 14, RFC 2119, mars 1997.
[4] J. Postel, "Protocole de datagramme d'utilisateur", STD 6, RFC 768, août 1980.
[5] R. Rivest et S. Dusse, "Algorithme MD5 de résumé de message", RFC 1321, avril 1992.
[6] J. Reynolds et J. Postel, "Allocation des numéros", STD 2, RFC 1700, octobre 1994.
[7] F. Yergeau, "UTF-8, format de transformation de ISO 10646", RFC 2279, janvier 1998.
[8] H. Alvestrand et T. Narten, "Lignes directrices pour la rédaction d'une section de Considérations relatives à l'IANA dans les RFC", BCP 26, RFC 2434, octobre 1998.

10 Remerciements

RADIUS et la comptabilité RADIUS ONT été développés à l'origine par Steve Willens de Livingston Enterprises pour leur série PortMaster de serveurs d'accès réseau.

11 Adresse du président

Le groupe de travail RADIUS 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

12 Adresse de l’auteur

Les questions sur le présent mémo peuvent aussi être adressées à
Carl Rigney
Livingston Enterprises
4464 Willow Road
Pleasanton, California 94588
mél : cdr@telemancy.com

13 Déclaration complète de droits de propriété

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