Groupe de travail Réseau
Request for Comments : 2975
Catégorie : Information
Traduction Claude Brière de L'Isle

B. Aboba, Microsoft Corporation
J. Arkko, Ericsson
D. Harrington, Cabletron Systems Inc.
octobre 2000

Introduction à la gestion comptable

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

Résumé
Le champ de la gestion comptable recouvre la collecte des données de consommation de ressources afin d'analyser les capacités et les tendances, l'allocation des coûts, la vérification et la facturation. Le présent document décrit chacun de ces problèmes, et expose les tenants et aboutissants de la conception des systèmes modernes de comptabilité.

Comme les applications comptables n'ont pas des exigences uniformes de sécurité et de fiabilité, il n'est pas possible d'imaginer un seul protocole comptable et ensemble de services de sécurité qui satisfasse tous les besoins. Donc, le but de la gestion comptable est de fournir un ensemble d'outils qui puisse être utilisé pour satisfaire les exigences de chaque application. Le présent document décrit les outils actuellement disponibles ainsi que l'état de l'art dans la conception de protocoles de comptabilité. Un document voisin, la RFC2924, passe en revue l'état de l'art des attributs de comptabilité et des formats d'enregistrement.

Table des Matières

1. Introduction

Le champ de la gestion comptable est concerné par la collecte des données de consommation de ressources pour des besoins d'analyse de capacité et de tendance, d'allocation de coût, de vérification, et de facturation. Le présent document décrit chacun de ces problèmes, et discute des questions impliquées par la conception des systèmes comptables modernes.

Comme les applications de comptabilité n'ont pas des exigences uniformes de sécurité et de fiabilité, il n'est pas possible d'imaginer un seul protocole de comptabilité et ensemble de services de sécurité qui satisfasse tous les besoins. Donc le but de la gestion comptable est de fournir un ensemble d'outils qui puisse être utilisé pour satisfaire les exigences de chaque application. Le présent document décrit les outils actuellement disponibles ainsi que l'état de l'art de la conception de protocole de comptabilité. Un document voisin, la RFC2924, passe en revue l'état de l'art des attributs et formats d'enregistrement de comptabilité.

1.1 Langage des exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

1.2 Terminologie

Le présent document utilise fréquemment les termes suivants :

Comptabilité : collecte de données de consommation de ressources pour les besoins de l'analyse de capacité et de tendance, d'allocation des coûts, de vérification, et de facturation. La gestion comptable exige que la consommation des ressources soit mesurée, évaluée, allouée, et communiquée entre les parties appropriées.

Archivage comptable : dans l'archivage comptable, le but est de collecter toutes les données comptables, de reconstruire les entrées manquantes au mieux possible dans le cas d'une perte de données, et d'archiver les données pendant une période obligatoire. Il est "usuel et coutumier" que ces systèmes soient conçus pour être très robustes à l'égard de la perte de données comptables. Cela peut inclure des dispositions pour la couche transport aussi bien que des accusés de réception de couche application, l'utilisation d'une mémorisation non volatile, des capacités de comptabilité intermédiaire (mémorisées ou transmises sur le réseau), etc. Des exigences réglementaires ou financières rendent fréquemment obligatoires les pratiques d'archivage comptable, et peuvent souvent imposer que les données restent confidentielles, sans considérer si elles sont à utiliser à des fins de facturation ou non.

Évaluation : acte de détermination du prix à facturer pour l'utilisation d'une ressource.

Facturation : acte de préparation d'une facture.

Facturation à l'utilisation : un processus de facturation qui dépend des informations d'utilisation pour préparer une facture peut être dit être "à l'utilisation". À l'opposé, un processus indépendant des informations d'usage est dit "non sensible à l'utilisation".

Vérification : action de vérifier qu'une procédure est correcte. Pour être capable de mener à bien une vérification, il est nécessaire d'être capable de déterminer de façon définitive quelles procédures ont été réellement utilisées afin d'être capable de les comparer au processus recommandé. L'accomplissement de cela peut exiger des services de sécurité comme l'authentification et la protection de l'intégrité.

Allocation des coûts : acte d'allouer des coûts entre des entités. Noter que l'allocation des coûts et l'évaluation sont des processus fondamentalement différents. Dans l'allocation des coûts, l'objectif est normalement d'allouer un coût connu à différentes entités. Dans l'évaluation, l'objectif est de déterminer la quantité à imputer pour l'utilisation d'une ressource. Dans l'allocation de coût, le coût par unité de ressource peut avoir besoin d'être déterminé ; dans l'évaluation, c'est normalement une donnée.

Comptabilité intermédiaire : la comptabilité intermédiaire donne une photographie de l'usage durant une session d'utilisateur. Cela peut être utile en cas de réamorçage d'un appareil ou autre problème réseau qui empêche la réception ou la génération d'un paquet de résumé de session ou un enregistrement de session. Les enregistrements de comptabilité intermédiaires peuvent toujours être récapitulés sans perte d'information. Noter que les enregistrement de comptabilité intermédiaire peuvent être mémorisés en interne sur l'appareil (comme dans la mémorisation non volatile) afin de survivre à un réamorçage et ne peuvent donc pas toujours être transmis sur le réseau.

Enregistrement de session : il représente une récapitulation de la consommation de ressources d'un utilisateur pendant une session entière. Les passerelles de comptabilité qui créent l'enregistrement de session peuvent le faire en traitant les événement de comptabilité intermédiaires ou les événements comptables pour plusieurs appareils qui desservent le même utilisateur.

Protocole comptable : c'est un protocole utilisé pour porter les données qui servent à la comptabilité.

Comptabilité intra domaine : elle implique la collecte des informations sur l'usage des ressources au sein d'un domaine administratif, pour les utiliser au sein de ce domaine. Dans la comptabilité intra domaine, les paquets de comptabilité et les enregistrements de session ne traversent normalement pas les frontières administratives.

Comptabilité inter domaine : elle implique la collecte des informations sur l'usage des ressources au sein d'un domaine administratif, pour les utiliser au sein d'un autre domaine administratif. Dans la comptabilité inter domaine, les paquets de comptabilité et les enregistrements de session vont normalement traverses les frontières administratives.

Comptabilité en temps réel : elle implique le traitement des informations sur l'usage des ressource au sein d'une fenêtre temporelle définie. Les contraintes de temps sont normalement imposées pour limiter les risques financiers.

Serveur de comptabilité : il reçoit les données comptables des appareils et les traduit en enregistrements de session. Le serveur de comptabilité a aussi la responsabilité de l'acheminement des enregistrements de session aux parties intéressées.

1.3 Architecture de la gestion comptable

L'architecture de gestion comptable implique des interactions entre les appareils réseau, les serveurs de comptabilité, et les serveurs de facturation. L'appareil réseau collecte les données de consommation de ressources sous la forme de métriques comptables. Ces informations sont alors transférées à un serveur de comptabilité. Cela est normalement accompli via un protocole de comptabilité, bien qu'il soit aussi possible que les appareils génèrent leurs propres enregistrements de session.

Le serveur de comptabilité traite alors les données comptables reçues de l'appareil réseau. Ce traitement peut inclure la récapitulation des informations comptables intermédiaires, l'élimination des données dupliquées, ou la génération d'enregistrements de session.

Les données comptables traitées sont ensuite soumises au serveur de facturation, qui traite normalement la génération des évaluations et des factures, mais peut aussi s'occuper des fonctions de vérification, d'allocation des coûts, d'analyse de tendance ou planification de capacités. Les enregistrements de session peuvent être regroupés et compressés par le serveur de comptabilité avant leur soumission au serveur de facturation afin de réduire le volume de données comptables et la bande passante requise pour accomplir le transfert.

Une des fonctions du serveur de comptabilité est de faire la distinction entre les événements de comptabilité inter et intra domaines et de les acheminer de façon appropriée. Pour les enregistrements de session qui contiennent un identifiant d'accès réseau (NAI, *Network Access Identifier*), décrit dans la [RFC2486], la distinction peut être faite en examinant la portion domaine du NAI. Si la portion domaine est absente ou correspond au domaine local, l'enregistrement de session est traité comme un événement de comptabilité intra domaine. Autrement, il est traité comme un événement de comptabilité inter domaines.

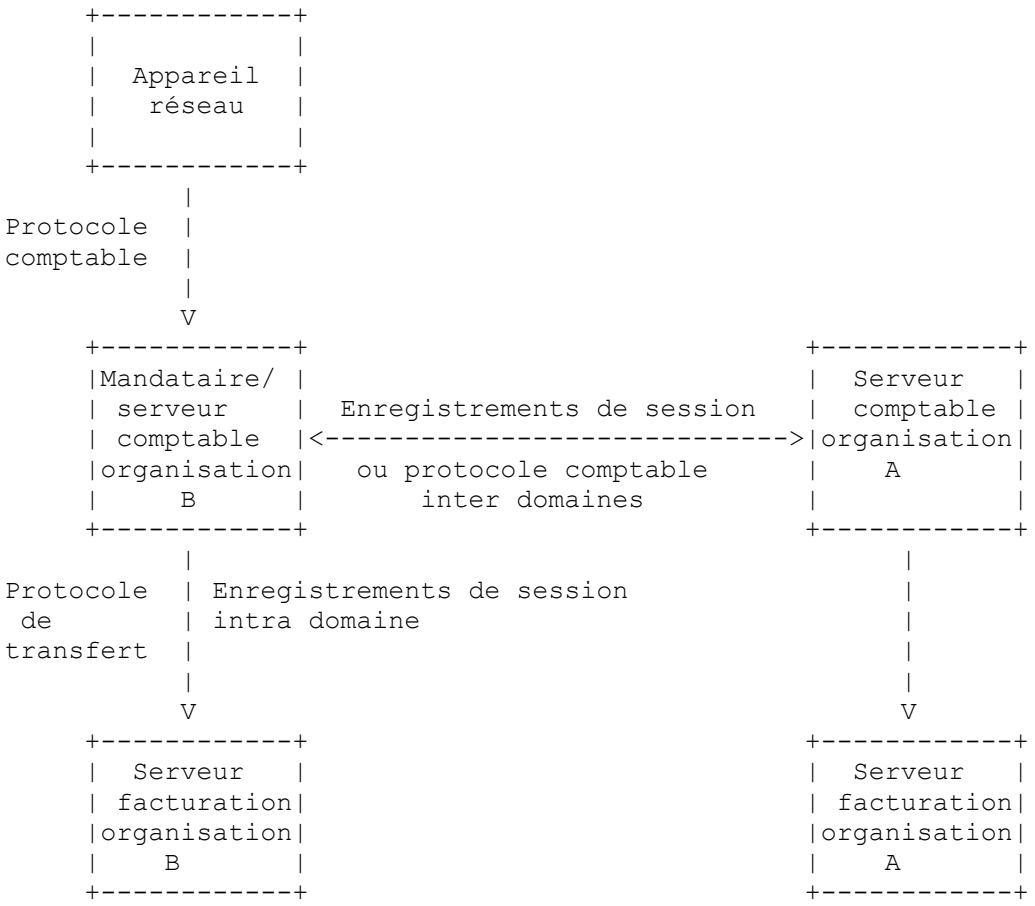
Les événements de comptabilité intra domaine sont normalement acheminés au serveur de facturation local, tandis que les événements de comptabilité inter domaines vont être acheminés aux serveurs de comptabilité qui opèrent au sein d'autres domaines administratifs. Bien qu'il ne soit pas exigé que le format des enregistrements de session utilisés dans la comptabilité inter et intra domaines soit le même, ceci est souhaitable, car cela élimine les traductions qui seraient autrement nécessaires.

Lorsque un transmetteur mandataire est employé, les contrôles d'accès fondés sur le domaine peuvent être utilisés par le transmetteur mandataire, plutôt que par les appareils eux-mêmes. L'appareil réseau va normalement parler au transmetteur mandataire selon un protocole de comptabilité, qui peut alors soit convertir les paquets de comptabilité en enregistrements de session, soit transmettre les paquets de comptabilité à un autre domaine. Dans l'un et l'autre cas, la séparation des domaines est normalement réalisée au moyen du tri par destination par le transmetteur mandataire des enregistrements de session ou des messages de comptabilité.

Lorsque le mandataire de comptabilité n'est pas de confiance, il peut être difficile de vérifier qu'il produit des enregistrements de session corrects sur la base des messages de comptabilité qu'il reçoit, car les messages de comptabilité originaux ne sont normalement pas transmis avec les enregistrements de session. Donc, lorsque la confiance est

problématique, le mandataire transmet normalement les paquets de comptabilité eux-mêmes. En supposant que le protocole comptable prend en charge la sécurité des objets de données, cela permet aux points d'extrémité de vérifier que le mandataire n'a pas modifié les données en transit ou inspecté le contenu des paquets.

Le diagramme ci-dessous illustre l'architecture de gestion comptable :



1.4. Objectifs de la gestion comptable

La gestion comptable implique la collecte des données de consommation de ressources pour les besoins d'analyse de capacité et de tendance, d'allocation des coûts, de vérification, de facturation. Chacune de ces tâches a des exigences différentes.

1.4.1 Analyse des tendances et projection des capacités

Dans l'analyse des tendances et la projection des capacités, le but est normalement une prévision de l'usage futur. Comme de telles prévisions sont par nature imparfaites, une haute fiabilité n'est normalement pas requise, et une perte de paquet modérée peut être tolérée. Lorsque il est possible d'utiliser des techniques d'échantillonnage statistique pour réduire les exigences de collecte des données tout en fournissant les prévisions avec la précision statistique désirée, on peut éventuellement tolérer une forte perte de paquets tant qu'on introduit pas de biais.

Les exigences de sécurité pour l'analyse des tendances et la projection des capacités dépendent des circonstances de la collecte des données et de la sensibilité des données. Des services de sécurité supplémentaires peuvent être requis lorsque des données sont transférées entre domaines administratifs. Par exemple, lorsque des informations sont collectées et analysées au sein du même domaine administratif, la protection de l'intégrité et l'authentification peuvent être utilisées afin de se garder contre la collecte de données invalides. Dans les applications inter domaines, la confidentialité peut être désirable pour se garder contre l'espionnage par des tiers.

1.4.2 Facturation

Lorsque les données comptables sont utilisées à des fins de facturation, les exigences dépendent de la sensibilité à l'utilisation ou non du processus de facturation.

1.4.2.1 Facturation insensible à l'usage

Comme par définition, la facturation indépendante de l'utilisation n'exige pas d'informations sur l'utilisation, en théorie, toutes les données comptables peuvent être perdues sans affecter le processus de facturation. Bien sûr, ceci affecterait aussi d'autres tâches comme l'analyse de tendance ou la vérification, de sorte qu'une telle perte globale de données serait quand même inacceptable.

1.4.2.2 Facturation selon l'usage

Comme les processus de facturation selon l'utilisation dépendent des informations sur l'utilisation, la perte de paquet peut se traduire directement en perte de revenu. Il en résulte que le processus de facturation peut devoir se conformer à des exigences de présentation financières et réglementaires, et donc une approche d'archivage comptable peut être nécessaire.

Les systèmes selon l'utilisation peuvent aussi exiger de faibles délais de traitement. Le risque de crédit est aujourd'hui couramment géré par des systèmes informatisés de détection de fraude qui sont conçus pour détecter une activité inhabituelle. Bien que le souci de l'efficacité puisse autrement imposer la transmission par lots des données comptables, lorsque il y a un risque de fraude, l'exposition financière augmente avec le délai de traitement. Donc, il peut être conseillé de transmettre chaque événement individuellement pour minimiser la taille des lots, ou même d'utiliser des techniques de qualité de service pour minimiser les délais de mise en file d'attente. De plus, il peut être nécessaire que l'autorisation dépende de la capacité de payer.

L'utilité de ces techniques varie selon l'application car le degré d'exposition financière dépend de l'application. Pour l'accès Internet par numérotation à partir d'un fournisseur local, les charges sont normalement faibles et donc le risque de pertes est petit. Cependant, dans le cas d'itinérance sur le réseau téléphonique ou de voix sur IP, les charges à la durée peuvent être substantielles et donc le risque de fraude est plus grand. Dans de telles situations, il est très souhaitable de détecter rapidement une activité de compte inhabituelle, et il peut être souhaitable que l'autorisation dépende de la capacité de payer. Dans des situations où des ressources de valeur peuvent être réservées, ou lorsque les charges peuvent être élevées, de très grosses factures peuvent être rapidement atteintes, et le traitement peut devoir être achevé dans une fenêtre de temps définie afin de limiter l'exposition.

Comme dans les systèmes selon l'utilisation, les données comptables se traduisent en revenus, les exigences de sécurité et de fiabilité sont plus grandes. Du fait des exigences financières et réglementaires, de tels systèmes doivent être capables de survivre à un audit. Donc des services de sécurité tels que l'authentification, la protection de l'intégrité et contre la répétition sont fréquemment exigés et la confidentialité et l'intégrité des objets de données peuvent aussi être désirables. Les accusés de réception de couche application sont aussi souvent exigés afin de se garder contre les défaillances du serveur de comptabilité.

1.4.3 Vérification

Avec l'expansion des dépenses de réseautage des entreprises, l'intérêt pour la vérification augmente. La vérification, qui est l'acte de vérifier qu'une procédure est correcte, s'appuie couramment sur les données comptables. Les tâches de vérification incluent de vérifier qu'une facture soumise par un fournisseur de service est correcte, ou de vérifier la conformité à une politique d'utilisation, aux accords de niveau de service, ou aux lignes directrices de sécurité.

Pour permettre une vérification crédible, le processus de collecte des données de vérification doit être au moins aussi fiable que le processus comptable utilisé par l'entité qui est vérifiée. De même, les politiques de sécurité pour la vérification devraient être au moins aussi contraignantes que celles utilisées pour la préparation de la facture originale. Du fait des exigences financières et réglementaires, les pratiques d'archivage comptable sont fréquemment exigées dans cette application.

Lorsque des procédures de vérification sont utilisées pour vérifier la conformité aux politiques d'usage ou de sécurité, des services de sécurité peuvent être désirés. Cela va normalement inclure l'authentification, la protection de l'intégrité et la protection contre la répétition ainsi que la confidentialité et l'intégrité des objets de données. Afin de permettre une réponse aux incidents de sécurité en cours, les applications de vérification sont fréquemment construites pour fonctionner avec de faibles délais de traitement.

1.4.4 Allocation des coûts

L'application de méthodes d'allocation des coûts et de refacturation par les clients professionnels n'est pas encore très répandue. Cependant, avec la convergence de la téléphonie et des communications de données, il y a un intérêt croissant pour l'application des procédures d'allocation des coûts et des procédures de refacturation des coûts de réseautage, tout

comme c'est la pratique courante avec les coûts de télécommunications.

Les modèles d'allocation des coûts, incluant les mécanismes traditionnels de valorisation décrits dans les références [21], [22], [23] et les techniques de valorisation fondées sur l'activité décrites dans [24] se fondent normalement sur l'analyse détaillée des données d'usage, et par suite, ils sont presque toujours en fonction de l'utilisation. Que ces techniques soient appliquées à l'allocation des coûts entre les partenaires d'une entrepris ou à l'allocation des coûts entre les départements d'une même entreprise, les modèles d'allocation des coûts ont souvent un profond impact comportemental et financier. Par suite, les systèmes développés à cette fin sont normalement aussi concernés par la collecte fiable des données et la sécurité que le sont les applications de facturation. Du fait des exigences financières et réglementaires, les pratiques d'archivage comptable sont fréquemment exigées dans cette application.

1.5 Comptabilité intra domaine et inter domaines

Beaucoup des travaux initiaux sur la gestion comptable se focalisaient sur les applications de comptabilité intra domaine. Cependant, avec le déploiement croissant de services tels que l'itinérance sur le réseau téléphonique, la télécopie Internet, la voix et la vidéo sur IP et la qualité de service, les applications qui exigent une comptabilité inter domaines deviennent de plus en plus courantes.

La comptabilité inter domaines diffère de la comptabilité intra domaine de plusieurs façons importantes. La comptabilité intra domaine implique la collecte des informations de consommation de ressources au sein d'un domaine administratif, pour les utiliser au sein de ce domaine. Dans la comptabilité intra domaine, les paquets de comptabilité et les enregistrements de session ne traversent normalement pas les frontières administratives. Par suite, les applications de comptabilité intra domaine subissent normalement de faibles pertes de paquet et impliquent le transfert de données entre des entités de confiance.

À l'opposé, la comptabilité inter domaines implique la collecte des informations sur la consommation de ressources au sein d'un domaine administratif, pour les utiliser au sein d'un autre domaine administratif. En comptabilité inter domaines, les paquets de comptabilité et les enregistrements de session vont normalement traverser les frontières administratives. Par suite, les applications de comptabilité inter domaines peuvent subir de substantielles pertes de paquet. De plus, les entités impliquées dans les transferts ne peuvent pas être supposées se faire confiance.

Comme les applications de comptabilité inter domaines impliquent des transferts de données comptables entre domaines, des mesures de sécurité additionnelles peuvent être désirables. De plus, pour l'authentification, la protection de l'intégrité et contre la répétition, il peut être désirable de déployer des services de sécurité tels que la confidentialité et l'intégrité de l'objet de données. En comptabilité inter domaines chaque partie impliquée exige aussi normalement une copie de chaque événement comptable pour la génération et la vérification des factures.

1.6 Production des enregistrements comptables

Normalement, un seul enregistrement de comptabilité est produit par session, ou dans certains cas, un ensemble d'enregistrements intermédiaires qui peuvent être récapitulés en un seul enregistrement aux fins de facturation. Cependant, pour prendre en charge le déploiement de services tels que l'accès sans fil ou des régimes de facturation complexes, une approche plus sophistiquée est nécessaire.

Il est nécessaires de générer plusieurs enregistrements de comptabilité à partir d'une seule session lorsque la tarification change durant une session. Par exemple, le prix d'un service peut être plus élevé durant les heures de pointe qu'en dehors de celles-ci. Pour une session qui continue d'une période tarifaire à une autre, il devient nécessaires que l'appareil fasse rapport des "paquets envoyés" durant les deux périodes.

Le temps n'est pas le seul facteur qui exige cette approche. Par exemple, dans les réseaux d'accès mobiles, l'utilisateur peut se déplacer d'un endroit à un autre tout en étant toujours connecté à la même session. Si l'itinérance cause un changement de tarif, il est nécessaire de prendre en compte les ressources consommées dans la première et dans la seconde zone. Un autre exemple est celui où des modifications sont permises à une session en cours. Par exemple, il est possible qu'une session puisse être ré autorisée avec une qualité de service améliorée. Cela exigerait la production d'enregistrements de comptabilité aux deux niveaux de QS.

Ces exemples pourraient être traités en utilisant des vecteurs ou des matrices multi dimensionnelles pour représenter la consommation de ressources au sein d'un seul enregistrement de session. Par exemple, le vecteur ou la matrice pourrait décrire la consommation de ressources pour chaque combinaison de facteurs, par exemple un élément de données pourrait être le nombre de paquets durant l'heure de pointe dans la zone de l'opérateur de rattachement. Cependant, une telle approche semble compliquée et peu souple et par suite, la plupart des systèmes courants produisent un ensemble

d'enregistrements à partir d'une session. Il faut que soit présent un identifiant de session dans l'enregistrement pour permettre aux systèmes comptables de lier les enregistrements.

Dans la plupart des cas, l'appareil réseau va déterminer quand plusieurs enregistrements de session sont nécessaires, car l'appareil local est au courant des facteurs qui affectent les tarifs locaux, comme les changements de qualité de service et l'itinérance. Cependant, de futurs systèmes sont en cours de conception pour permettre au domaine de rattachement de contrôler la génération des enregistrements de comptabilité. Cela a son importance dans la comptabilité inter domaines ou lorsque les appareils réseau n'ont pas les informations sur les tarifs. Le contrôle centralisé de la production des enregistrements de comptabilité peut être réalisé, par exemple, en faisant que les serveurs d'autorisation exigent le renouvellement de l'autorisation à certains moments et exigent la production d'enregistrements de comptabilités à chaque ré autorisation.

En conclusion, dans certains cas, il est nécessaire de produire plusieurs enregistrements de comptabilité à partir d'une seule session. Il doit être possible de faire cela sans exiger de l'utilisateur qu'il commence une nouvelle session ou recommence à s'authentifier. La production d'enregistrements multiples peut être contrôlée soit par l'appareil réseau, soit par le serveur AAA. Les exigences de délai, de sécurité et de fiabilité dans les sessions à enregistrement multiple sont les mêmes que pour les sessions à un seul enregistrement.

1.7 Résumé des exigences

Usage	Intra domaine	Inter domaines
Projection des capacités	Robustesse ou perte de paquet, Intégrité, authentification, protection contre la répétition [confidentialité]	Robustesse ou perte de paquet, Intégrité, authentification, protection contre la répétition, confidentialité [sécurité de l'objet de données]
Facturation indépendante de l'utilisation	Intégrité, authentification, protection contre la répétition [confidentialité]	Intégrité, authentification, protection contre la répétition, confidentialité [sécurité de l'objet de données]
Facturation selon l'utilisation, allocation des coûts & vérification	Archivage comptable Intégrité, authentification, protection contre la répétition [confidentialité] [Limites au délai de traitement]	Archivage comptable Intégrité, authentification, protection contre la répétition, confidentialité [sécurité de l'objet de données] [Limites au délai de traitement]
Facturation au temps, détection de fraude, itinérance	Archivage comptable Intégrité, authentification, protection contre la répétition [confidentialité] Limites au délai de traitement	Archivage comptable Intégrité, authentification, protection contre la répétition, confidentialité, [sécurité de l'objet de données et protection contre la répétition] Limites au délai de traitement

Légende : [] = facultatif

2. Adaptation et fiabilité

La poursuite de la croissance de l'Internet rend important que les systèmes de gestion comptable soient adaptables et fiables. La présente section expose les ressources consommées par les systèmes de gestion comptable ainsi que les propriétés d'adaptabilité et de fiabilité affichées par les divers modèles de collecte des données et de transport.

2.1 Résilience aux fautes

Comme on l'a noté précédemment, dans des applications comme la facturation selon l'utilisation, l'allocation des coûts et la vérification, une approche d'archivage de la comptabilité est fréquemment obligatoire, du fait des exigences financières et réglementaires. Comme dans de telles situations, la perte des données comptables peut se traduire en perte de revenus, il y a une incitation à prévoir un fort degré de résilience aux fautes. Les fautes qui peuvent se rencontrer incluent la perte de paquet, les défaillances du serveur de comptabilité, les défaillances du réseau, et les réamorçages d'appareil.

Aujourd'hui, une grande partie du débat sur la fiabilité de la comptabilité s'est focalisée sur la résilience aux pertes de paquet et aux différences entre le transport fondé sur UDP, SCTP et TCP. Cependant, on devrait comprendre que la résilience aux pertes de paquet est seulement un aspect de la satisfaction de l'exigence de l'archivage comptable.

Comme noté dans [18], "une fois que le câble est coupé, on n'a plus besoin de transmissions, on a besoin de *beaucoup*

plus de tension". Donc, le choix du transport n'a pas d'impact sur la résilience à des fautes comme une partition de réseau, une défaillance du serveur de comptabilité ou un réamorçage d'appareil. Ce qui donne la résilience à ces fautes est la mémorisation non volatile.

L'importance de la mémorisation non volatile dans la conception de systèmes comptables fiables ne soit pas être surestimée. Sans mémorisation non volatile, les systèmes fondés sur l'événement perdent des données une fois que la temporisation de transmission a été dépassée, et les conceptions par lots vont rencontrer des pertes de données une fois que la mémoire interne utilisée pour la mémorisation des données comptables sera pleine. Via l'utilisation de la mémorisation non volatile, et des enregistrements intermédiaires mémorisés en interne, la plupart de ces pertes de données peuvent être évitées.

On peut même objecter que la mémorisation non volatile est plus importante pour la fiabilité de la comptabilité que la connexité réseau, car pendant de nombreuses années, des systèmes comptables fiables ont été mis en œuvre sur la seule base d'une mémorisation physique, sans aucune connexité réseau. Par exemple, les données d'utilisation du téléphone étaient mémorisées sur un support papier, film, ou magnétique et transporté de l'endroit de collecte à une position centrale pour le traitement de la facturation.

2.1.1 Comptabilité intermédiaire

La comptabilité intermédiaire fournit une protection contre la perte des données de récapitulation de session en fournissant des informations de point de vérification qui peuvent être utilisées pour reconstruire l'enregistrement de session dans le cas de perte des information de récapitulation de session. Cette technique peut être appliquée à tous les modèles de collecte des données (c'est-à-dire pilotée par l'évènement ou par interrogation) et est prise en charge aussi bien par RADIUS [RFC2869] que par TACACS+.

Bien que la comptabilité intermédiaire puisse assurer la résilience aux pertes de paquet, aux défaillances de serveur, aux défaillances réseau de courte durée, ou aux réamorçages d'appareils, son applicabilité est limitée. La transmission des données comptables intermédiaires sur le réseau ne devrait pas être vue comme une technique d'amélioration majeure de la fiabilité car elle augmente la consommation de la bande passante du réseau en fonctionnement normal, tout en ne fournissant d'avantage qu'en cas de faute.

Comme la plupart des pertes de paquet sur l'Internet sont dues à l'encombrement, l'envoi des données comptables intermédiaires sur le réseau peut empirer le problème en augmentant l'utilisation de la bande passante. Donc, il vaut mieux restreindre l'envoi sur le réseau des données de comptabilité intermédiaire aux données comptables de grande valeur comme les informations sur les sessions de longue durée. Pour protéger contre la perte de données sur de telles sessions, l'intervalle des rapports intérimaires est normalement réglé à plusieurs fois l'écart type standard de plus que la durée de session moyenne. Cela assure que la plupart des sessions ne vont pas générer d'événement de comptabilité intermédiaire et que la consommation supplémentaire de bande passante de la comptabilité intermédiaire restera limitée. Cependant, comme l'intervalle de comptabilité intermédiaire décroît avec la durée de session moyenne, la bande passante supplémentaire consommée par la comptabilité intermédiaire augmente sensiblement, et par suite l'intervalle doit être réglé avec précaution.

Lorsque la mémorisation non volatile est indisponible, la comptabilité intermédiaire peut aussi résulter en une consommation excessive de mémoire qui serait mieux utilisée à mémoriser les données de session. Par suite, les mises en œuvre devraient veiller à s'assurer que les nouvelles données comptables intérimaires écrasent les données précédentes plutôt que d'accumuler des enregistrements intermédiaires supplémentaires en mémoire, empirant par là le problème d'épuisement de la mémoire tampon.

Étant donnée la popularité croissante de l'utilisation de la mémorisation non volatile dans les appareils comme les caméras numériques, de tels appareils voient leur prix diminuer rapidement. Il est donc de plus en plus facile aux appareils réseau d'inclure des supports incorporés de mémorisation non volatile. Cela peut se faire, par exemple, par la prise en charge de cartes PCMCIA compactes.

Lorsque une mémorisation non volatile est disponible, cela peut être utilisé pour mémoriser les données comptables intermédiaires. Les événements intermédiaires mémorisés sont alors remplacés par des événements intermédiaires mis à jour par les données de session lorsque la session s'achève. Les données de session peuvent elles-mêmes être écrasées une fois que les données ont été transmises et acquittées à la couche application. Cette approche évite que des données intermédiaires soient transmises sur le réseau sauf dans le cas d'un réamorçage de l'appareil. Lorsque un appareil se réamorce, les enregistrements intermédiaires mémorisés en interne sont transférés au serveur de comptabilité.

2.1.2 Plusieurs enregistrements par session

La génération de plusieurs enregistrements de comptabilité au sein d'une session peut introduire des problèmes d'adaptation qui ne peuvent être contrôlés en utilisant les techniques disponibles dans la comptabilité intermédiaire.

Par exemple, dans le cas d'enregistrements intermédiaires conservés dans une mémorisation non volatile, il est possible d'écraser les enregistrements intermédiaires précédents avec les plus récents ou de les récapituler en un enregistrement de session. Lorsque les mises à jour intermédiaires sont envoyées sur le réseau, il est possible de contrôler l'utilisation de la bande passante en ajustant l'intervalle de comptabilité intermédiaire.

Ces mesures ne sont pas applicables lorsque plusieurs enregistrements de session sont produits à partir d'une seule session, car ces enregistrements ne peuvent pas être récapitulés ou écrasés sans perte d'informations. Par suite, la production d'enregistrements multiples peut résulter en une consommation accrue de bande passante et de mémoire. Les mises en œuvre devraient veiller à s'assurer que les exigences de traitement des pires cas d'enregistrements multiples n'excèdent pas les capacités de leur système.

Par exemple, un changement de tarif à un instant particulier de la journée pourrait, si il est mis en œuvre sans précautions créer une pointe soudaine de la consommation de mémoire et de bande passante lorsque les enregistrements doivent être mémorisés et/ou transportés. Plutôt que de tenter d'envoyer tous les enregistrements en une fois, il peut être souhaitable de les garder en mémoire dans une mémorisation non volatile et d'envoyer tous les enregistrements concernés ensemble dans un lot lorsque la session s'achève. Il peut aussi être souhaitable de formater le flux de trafic comptable de façon à réduire la pointe de consommation de bande passante. Cela peut se faire par l'introduction d'un intervalle avec retard aléatoire. Si le domaine de rattachement peut aussi contrôler la génération de multiples enregistrements de comptabilité, l'estimation du pire cas d'exigences de traitement peut être très difficile.

2.1.3 Perte de paquet

Comme la perte de paquet est un fait de la vie de l'Internet, le traitement par les protocoles comptables des données de session doit être résiliant à la perte de paquet. Ceci est particulièrement important dans la comptabilité inter domaines, où les paquets passent souvent à travers des points d'accès réseau (NAP, *Network Access Point*) où la perte de paquet peut être substantielle. La résilience à la perte de paquet peut être réalisée via la mise en œuvre d'un mécanisme de nouvel essai par dessus UDP, ou l'utilisation de TCP [RFC0793] ou SCTP [RFC2960]. La comptabilité intermédiaire sur le réseau ne présente que des avantages limités pour atténuer les effets des pertes de paquet.

Le transport fondé sur UDP est fréquemment utilisé dans les applications de comptabilité. Cependant, ceci n'est pas approprié dans tous les cas. Lorsque les données comptables ne tiennent pas au sein d'un seul paquet UDP sans fragmentation, l'utilisation du transport TCP ou SCTP peut être préférée à l'utilisation de multiples allers retours dans UDP. Comme noté dans la [RFC3430] et dans[49], ceci peut être un problème pour la restitution de grands tableaux.

De plus, dans les cas où de l'encombrement est probable, comme dans la comptabilité inter domaines, le contrôle d'encombrement TCP ou SCTP et l'estimation du délai d'aller retour seront très utiles, pour optimiser le débit. Dans les applications qui exigent le maintien de l'état de session, comme le contrôle de l'utilisation simultanée, TCP avec les paquets de maintien en vie de couche application ou SCTP avec ses capacités incorporées de battement de cœur, fournissent un mécanisme pour garder trace de l'état de session.

Lorsque on met en œuvre la retransmission UDP, on doit veiller à un certain nombre de problèmes : le modèle de données, le comportement de réessai, le contrôle d'encombrement, et le comportement de fin de temporisation.

La fiabilité de la comptabilité peut être influencée par la façon dont les données sont modélisées. Par exemple, il est presque toujours préférable d'utiliser des variables cumulatives plutôt que d'exprimer les données comptables en termes de changement d'un élément de données précédent. Avec les données cumulatives, l'état actuel peut être récupéré par une restitution réussie, même après la perte de nombreux paquets. Cependant, si les données sont transmises comme un changement, l'état ne sera alors pas récupéré tant que la prochaine mise à jour cumulative n'aura pas été envoyée. Donc, de telles mises en œuvre sont beaucoup plus vulnérables à la perte de paquet, et devraient être évitées chaque fois que possible.

Pour concevoir un mécanisme de réessai UDP, il est important que les temporisateurs de réessai se rapportent au délai d'aller retour, afin que les retransmissions ne se produisent normalement pas au sein de la période dans laquelle on s'attend à ce qu'arrivent les accusés de réception. La bande passante de la comptabilité peut être significative dans certaines circonstances, de sorte que le trafic ajouté par les retransmissions inutiles peut augmenter le niveau d'encombrement.

Le contrôle d'encombrement dans le transfert des données est une question assez controversée. Comme le trafic comptable est souvent considéré comme une mission critique, on a avancé que le contrôle de l'encombrement n'est pas une exigence ;

il vaut mieux que d'autre trafic moins critique soit retardé en réponse à l'encombrement. De plus, sans mémorisation non volatile, un retard dû à l'encombrement dans des applications comptables peut résulter en pertes de données dues à l'épuisement de la mémoire tampon.

Cependant, on peut aussi avancer que dans les mises en œuvre modernes de comptabilité, il est possible de mettre en œuvre le contrôle d'encombrement tout en améliorant le débit et en conservant une grande fiabilité. Dans des circonstances où il y a une perte de paquets substantielle, il n'y a simplement pas une capacité suffisante pour maintenir les taux de transmission existants. Donc, le débit agrégé va en fait s'améliorer si un retard dû à l'encombrement est mis en œuvre. Cela est dû à l'élimination des retransmissions et à la capacité d'utiliser des techniques comme la détection précoce aléatoire (RED, *Random Early Detection*) pour désynchroniser les flux. De plus, avec les mécanismes de qualité de service comme les services différenciés, il est possible de marquer les paquets de comptabilité pour un traitement préférentiel afin d'assurer une plus faible perte de paquet si désiré. Une latitude considérable est donc disponible à l'administrateur de réseau pour le contrôle du traitement des paquets de comptabilité l'adoption de comportements sans souplesse n'est pas nécessaire. Normalement, les systèmes qui mettent en œuvre la mémorisation non volatile permettent que des données comptables en retard soient placées dans une mémorisation non volatile en attendant la transmission, de sorte que l'épuisement de mémoire tampon résultant d'un retard dû à l'encombrement n'est plus un problème.

Comme UDP n'est pas réellement un protocole de transport, les protocoles comptables fondés sur UDP comme celui de la [RFC2139] ne prescrivent souvent pas de comportement de fin de temporisation. Donc, des mises en œuvre peuvent afficher des comportements largement différents. Par exemple, une mise en œuvre peut abandonner des données comptables après trois essais de durée constante sur le même serveur, tandis qu'une autre peut mettre en œuvre un retard exponentiel sur un certain serveur, puis passer à un autre serveur, jusqu'à un intervalle total de temporisation de douze heures, tout en stockant les données non transmises sur une mémorisation non volatile. La différence pratique entre ces approches est substantielle ; la première approche ne satisfera pas aux exigences d'archivage comptable tandis que la dernière le peut. Des comportements plus prévisibles peuvent être obtenus par l'utilisation du transport SCTP ou TCP.

2.1.4 Serveur comptable de secours

En cas de défaillance du serveur de comptabilité principal, il est souhaitable que l'appareil se replie sur un serveur secondaire. Fournir un ou plusieurs serveurs secondaires peut supprimer beaucoup des risques d'une défaillance du serveur de comptabilité, et par suite, l'utilisation de serveurs secondaires est devenue très courante.

Pour les protocoles fondés sur TCP, il est possible à l'appareil de maintenir les connexions avec les deux serveurs de comptabilité, le principal et le secondaire, en utilisant la connexion secondaire après l'expiration d'un temporisateur sur la connexion principale. Autrement, il est possible d'ouvrit une connexion avec le serveur de comptabilité secondaire après une fin de temporisation ou la perte de la connexion principale, ou à l'expiration d'un temporisateur. Donc, les protocoles de comptabilité fondés sur TCP sont capables de répondre plus rapidement aux défaillances de connexité que les fins de temporisation de TCP ne le permettraient autrement, aux dépens de l'augmentation du risque de dupliqués.

Avec SCTP, il est possible de contrôler le comportement de fin de temporisation de la couche transport, et donc, il n'est pas nécessaire que l'application de comptabilité entretienne ses propres temporisateurs. SCTP permet aussi le multiplexage de plusieurs connexions au sein d'une seule connexion de transport, toutes conservant le même état de contrôle d'encombrement, évitant les problèmes de "blocage de tête de ligne" qui peuvent se produire avec TCP. Cependant, comme SCTP n'est pas largement disponible, l'utilisation de ce transport peut imposer une charge de mise en œuvre supplémentaire au concepteur.

Pour les protocoles qui utilisent UDP, la transmission au serveur secondaire peut se produire après un certain nombre d'essais ou à l'expiration d'une temporisation. Pour la compatibilité avec l'évitement d'encombrement, il est conseillé d'incorporer des techniques telles que l'estimation du temps d'aller retour, le démarrage lent et le retard pour diminuer l'encombrement *(congestive back-off)*. Donc le concepteur de protocole de comptabilité qui utilise UDP est souvent conduit à réinventer des techniques déjà existantes dans TCP et SCTP. Par suite, l'utilisation du transport UDP brut dans les applications de comptabilité n'est pas recommandée.

Il est possible avec tout transport que les serveurs de comptabilité principal et secondaire reçoivent des paquets dupliqués, de sorte que la prise en charge de l'élimination des dupliqués est requise. Comme les défaillances de serveur de comptabilité peuvent résulter en l'accumulation des données sur les clients de comptabilité, l'utilisation de mémorisations non volatiles peut donner des assurances contre les pertes de données dues aux fins de temporisation de transmission ou à l'épuisement de la mémoire tampon. La comptabilité intermédiaire sur le réseau ne fournit que des avantages limités dans l'atténuation des effets des défaillances de serveur de comptabilité.

2.1.5 Accusé de réception de couche application

Il est possible que le serveur de comptabilité rencontre des défaillances partielles. Par exemple, une défaillance à la fin de la base de données pourrait laisser fonctionnel le processus ou la trame de restitution comptable tandis que le processus ou trame responsable de la mémorisation des données ne fonctionne pas. De même, il est possible que l'application de comptabilité n'ait plus d'espace disque, la rendant incapable de continuer à mémoriser les enregistrements de session entrants.

Dans de tels cas, il est désirable de distinguer entre les accusés de réception de la couche transport et ceux de la couche application. Même si les deux accusés de réception peuvent être envoyés au sein du même paquet (comme un segment TCP portant un accusé de réception de couche application avec un ACK porté par dessus) leur sémantique est différente. Un accusé de réception de couche transport signifie "la couche transport a pris la responsabilité de la livraison des données à l'application", tandis qu'un accusé de réception de couche application signifie "l'application a pris la responsabilité des données".

Une erreur courante est de croire que l'utilisation du transport TCP garantit que les données seront livrées à l'application. Cependant, comme noté dans la [RFC0793] : "Un accusé de réception par TCP ne garantit pas que les données ont été livrées à l'utilisateur final, mais seulement que le TCP receveur a pris la responsabilité de le faire."

Donc, si le TCP receveur défaille après l'envoi de l'ACK, l'application peut ne pas recevoir les données. De même, si l'application défaille avant de mettre les données en sécurité sur une mémorisation stable, celles-ci peuvent être perdues. Pour qu'une application envoyeuse soit sûre que les données envoyées ont été reçues par l'application receveuse, il faut une clôture en douceur de la connexion TCP ou un accusé de réception de couche application. Pour protéger contre la perte des données, il est nécessaire que l'accusé de réception de couche application implique que les données ont été écrites sur une mémorisation stable ou convenablement traitées de façon à les garder contre la perte.

Dans le cas d'une défaillance partielle, il est possible que la couche transport accuse réception via un accusé de réception de couche transport, sans avoir livré les données à l'application. De même, l'application peut ne pas achever les tâches nécessaires pour prendre la responsabilité des données.

Par exemple, un serveur de comptabilité peut recevoir des données de la couche transport mais être incapable de les mémoriser à cause d'un problème de base de données de l'extrémité terminale ou d'une faute de disque. Dans ce cas, il ne devrait pas envoyer d'accusé de réception de couche application, même si un accusé de réception de couche transport serait approprié. Un message d'erreur de couche application devrait plutôt être envoyé en indiquant la source du problème, comme un "mémorisation indisponible à l'extrémité distante".

Donc, la capacité de faire des accusés de réception de couche application n'exige pas seulement la capacité d'accuser réception lorsque l'application a pris la responsabilité des données, mais aussi la capacité d'indiquer quand l'application n'a pas pris la responsabilité des données, et pourquoi.

2.1.6 Défaillances du réseau

Les défaillances du réseau peuvent résulter en une perte partielle ou complète de la connexité pour le client de comptabilité. Dans le cas d'une perte partielle de connexité, il se peut qu'il ne soit pas possible d'atteindre le serveur de comptabilité principal, auquel cas il est nécessaire de passer sur le serveur de comptabilité secondaire. Dans le cas d'une partition de réseau, il peut être nécessaire de mémoriser les événements de comptabilité dans la mémoire de l'appareil ou une mémorisation non volatile jusqu'à ce que la connexité soit rétablie.

Comme avec les défaillances de serveur de comptabilité, la comptabilité intermédiaire sur le réseau ne fournit qu'un avantage limité pour atténuer les effets des défaillances du réseau.

2.1.7 Réamorçage d'appareil

Dans le cas d'un réamorçage d'appareil, il est souhaitable de minimiser la perte de données sur les sessions en cours. De telles pertes peuvent être significatives même si les appareils eux-mêmes sont très fiables, à cause des sessions de longue durée, qui peuvent comporter une fraction significative de la consommation totale de ressources. Pour se garder contre la pertes de ces sessions de grande valeur, les données comptables intermédiaires sont normalement transmises sur le réseau. Lorsque la comptabilité intermédiaire en place est combinée avec une mémorisation non volatile, il devient possible de se garder contre les pertes de données dans des sessions beaucoup plus courtes. Ceci est possible car les données comptables intermédiaires ont seulement besoin d'être mémorisées dans une mémoire non volatile jusqu'à l'achèvement de la session, moment auquel les données intermédiaires peuvent être remplacées par l'enregistrement de session. Par suite, les données comptables intermédiaires n'ont jamais besoin d'être envoyées sur le réseau, et il est possible de diminuer l'intervalle intermédiaire afin de fournir un très haut degré de protection contre la perte de données.

2.1.8 Mandataires comptables

Pour maintenir une haute fiabilité, il est important que les mandataires de comptabilité passent les accusés de réception de couche transport et application et ne transmettent pas les paquets de comptabilité en différé. Cela permet aux systèmes d'extrémité de contrôler le comportement de retransmission et d'utiliser des techniques comme la mémorisation non volatile et les serveurs secondaires pour améliorer la résilience.

Les mandataires comptables qui envoient un ACK de couche transport ou application à l'appareil sans en recevoir un du serveur de comptabilité amènent l'appareil à penser que la demande comptable a été acceptée par le serveur de comptabilité alors que ce n'est pas le cas. Par suite, l'appareil peut supprimer le paquet de comptabilité de la mémorisation non volatile avant qu'il ait été accepté par le serveur de comptabilité. Il laisse au mandataire de comptabilité la responsabilité de la livraison des paquets de comptabilité. Si le mandataire de comptabilité comporte des parties mouvantes (par exemple, un pilote de disque) alors que les appareils n'en ont pas, la fiabilité globale du système peut être réduite.

Les mandataires de comptabilité qui livrent en différé n'apportent de valeur ajoutée que dans des situations où le sous système comptable est non fiable. Par exemple, lorsque les appareils ne mettent pas en œuvre la mémorisation non volatile et que le protocole de comptabilité manque de fiabilité aux couches transport et application, en situant le mandataire de comptabilité (avec sa mémorisation stable) proche de l'appareil, on peut réduire le risque de perte de données.

Cependant, de tels systèmes ont un manque de fiabilité inhérent, de sorte qu'ils ne sont appropriés que pour la planification des capacités ou des applications de facturation non sensibles à l'utilisation. Si on désire la fiabilité de l'archivage comptable, il est nécessaires de construire un système de comptabilité fiable depuis le début en utilisant les techniques décrites dans le présent document, plutôt que de tenter de réparer un système non fiable par nature en ajoutant des mandataires de comptabilité à livraison différée.

2.1.9 Résumé de la résilience aux fautes

Faute	**Contre mesures**
Perte de paquet	Retransmission fondée sur le délai d'aller retour
	Contrôle d'encombrement
	Comportement de temporisation bien défini
	Élimination des dupliqués
	Comptabilité intermédiaire*
	Mémorisation non volatile
	Variables cumulatives
Défaillance du serveur & réseau comptable	Serveurs principal-secondaire
	Élimination des dupliqués
	Comptabilité intermédiaire*
	Accusé de réception et messages d'erreur de couche application
	Mémorisation non volatile
Réamorçage d'appareil	Comptabilité intermédiaire*
	Mémorisation non volatile

Légende : * = d'utilité limitée en l'absence de mémorisation non volatile

Note : Les mandataires comptables ne sont pas un mécanisme d'amélioration de la fiabilité.

2.2 Consommation de ressources

Dans le processus de croissance pour satisfaire aux besoins des fournisseurs et des consommateurs, les systèmes de gestion de la comptabilité consomment diverses ressources, incluant : la bande passante du réseau, de la mémoire, de la mémoire non volatile, de l'état sur le système de gestion comptable, et de la CPU sur le système de gestion et les appareils gérés. Pour comprendre les limites à l'adaptabilité, on examine tour à tour chacune de ces ressources.

2.2.1 Bande passante du réseau

Les systèmes de gestion de la comptabilité consomment la bande passante du réseau en transférant les données comptables. La bande passante du réseau consommée est proportionnelle à la quantité de données transférées, ainsi que les frais généraux du réseau comme de besoin. Comme les données comptables pour un certain événement peuvent être de

100 octets ou moins, si chaque événement est transféré individuellement, les frais généraux peuvent représenter une proportion considérable de la consommation totale de bande passante. Par suite, il est souvent désirable de transférer les données comptables par lots, permettant de répartir les frais généraux du réseau sur une charge utile plus importante, et permettant une utilisation efficace de la compression. Comme noté dans [48], la compression peut être activée dans le protocole de comptabilité, ou peut être faite à la couche IP comme décrit dans la [RFC2393].

2.2.2 Mémoire

Dans les systèmes comptables sans mémorisation non volatile, les données comptables doivent être mémorisées dans une mémoire volatile durant la période entre le moment où elles sont générées et celui où elles sont transférées. La consommation de mémoire résultante va dépendre du nombre d'essais et des algorithmes de retransmission. Comme les systèmes conçus pour une haute fiabilité vont normalement souhaiter réessayer sur de longues périodes, ou peuvent mémoriser les données comptables intermédiaires, la consommation de mémoire résultante peut être considérable. Par suite, si la mémorisation non volatile est indisponible, il peut être désirable de compresser les données comptables en attendant la transmission.
Comme noté précédemment, les mises en œuvre de comptabilité intermédiaire devraient s'assurer contre une utilisation excessive de mémoire en écrasant les plus vieilles données comptables intermédiaires avec les données les plus récentes pour la même session plutôt que d'accumuler les données intermédiaires dans la mémoire tampon.

2.2.3 Mémorisation non volatile

Comme les données comptables stockées en mémoire vont normalement être perdues en cas de réamorçage d'appareil ou sur une fin de temporisation, il peut être désirable de fournir une mémorisation non volatile pour les données comptables non livrées. Comme les coûts de mémorisation non volatile déclinent rapidement, les appareils réseau seront de plus en plus capables d'incorporer des supports de mémorisation non volatile dans les prochaines années.
La mémorisation non volatile peut être utilisée pour stocker des enregistrements intermédiaires ou de session. Comme avec l'utilisation de la mémoire, l'écrasement de la comptabilité intermédiaire est désirable afin d'empêcher une consommation excessive de capacité de stockage. Noter que l'utilisation de la représentation de données ASCII permet l'utilisation d'algorithmes de compression de texte très efficaces qui peuvent minimiser les exigences de stockage. De tels algorithmes de compression ne sont normalement appliqués qu'aux enregistrements de session afin de permettre la mise en œuvre de l'écrasement des données intermédiaires.

2.2.4 État sur le système de gestion comptable

Afin de garder trace des données comptables reçues, les systèmes de gestion de la comptabilité peuvent avoir besoin de conserver l'état sur les appareils gérés ou les sessions concurrentes. Comme le nombre d'appareils est normalement beaucoup plus petit que le nombre de sessions concurrentes, il est souhaitable de ne garder que l'état par appareil, si possible.

2.2.5 Exigences de CPU

La consommation de CPU des nœuds gérés et gérants sera proportionnelle à la complexité du traitement comptable requis. Des opérations telles que le codage et décodage ASN.1, la compression/décompression, et le chiffrement/déchiffrement peuvent consommer des ressources considérables, chez les clients et les serveurs de comptabilité.
L'effet de ces opérations sur la fiabilité du système de comptabilité ne devrait pas être sous estimé, en particulier dans le cas d'appareils avec des ressources de CPU modérées. Si les appareils sont surchargés par les tâches comptables, il est probable que la fiabilité globale de l'appareil va en souffrir.

2.2.6 Mesures d'efficacité

Ressource	Mesures d'efficacité
Bande passante du réseau	Compression par lots
Mémoire	Compression, écrasement de la comptabilité intermédiaire
Stockage non volatile	Compression, écrasement de la comptabilité intermédiaire
État du système	État par appareil
Exigences de CPU	Compression/chiffrement assisté par le matériel

2.3 Modèles de collecte des données

Plusieurs modèles de collecte des données sont actuellement utilisés aujourd'hui pour les besoins de la collecte des données comptables. Cela inclut : le modèle d'interrogation, le modèle conduit par l'événement sans mise en lots, le modèle conduit

par l'événement avec mise en lots, et le modèle d'interrogation conduit par l'événement.

2.3.1 Modèle d'interrogation

Dans le modèle d'interrogation, un gestionnaire de comptabilité va interroger les appareil sur les informations comptables à intervalles réguliers. Pour s'assurer contre la perte de données, l'intervalle d'interrogation va devoir être plus court que le temps maximum pendant lequel les données comptables peuvent être mémorisées sur l'appareil interrogé. Pour les appareils sans mémorisation non volatile, ceci est normalement déterminé par la mémoire disponible ; pour les appareils avec mémorisation non volatile, l'intervalle maximum d'interrogation est déterminé par la taille de la mémoire non volatile.

Le modèle d'interrogation résulte en une accumulation de données au sein des appareils individuels, et par suite, les données sont normalement transférées au gestionnaire de comptabilité dans un lot, résultant en un processus de transfert efficace. En termes d'état de gestionnaire de comptabilité, les systèmes d'interrogation s'adaptent au nombre d'appareils gérés, et l'usage de la bande passante par le système s'adapte à la quantité de données transférées.

Sans mémorisation non volatile, le modèle d'interrogation résulte en pertes de données comptables du fait des réamorçages d'appareils, mais pas à cause de pertes de paquet ou de défaillances du réseau de durée suffisamment courtes pour être traitées au sein de la mémoire disponible. Ceci parce que le gestionnaire de comptabilité va continuer d'interroger jusqu'à ce que les données soient reçues. Dans les situations où se rencontrent des difficultés de fonctionnement, le volume de données comptables va fréquemment augmenter de telle sorte que les pertes de données deviennent plus probables. Cependant, dans ce cas, le modèle d'interrogation va détecter le problème car les tentatives de joindre les appareils gérés vont échouer.

Le modèle d'interrogation s'adapte mal aux mises en œuvre d'utilisation partagée ou aux services d'itinérance, incluant les données sans fil, la téléphonie Internet, le provisionnement de qualité de service ou l'accès Internet. Cela parce que afin de restituer les données comptables pour les utilisateurs au sein d'un certain domaine, la station gestionnaire de comptabilité va avoir besoin d'interroger périodiquement tous les appareils dans tous les domaines, dont la plupart ne vont contenir aucune donnée pertinente. Il y a aussi des problèmes avec le délai de traitement, car l'utilisation d'un intervalle d'interrogation implique aussi un délai moyen de traitement de la moitié de l'intervalle d'interrogation. Ceci peut être trop élevé pour des données comptables qui exigent un faible délai de traitement. Donc l'approche de l'interrogation conduite par l'événement ou le pur modèle conduit par l'événement est plus appropriée pour les applications de facturation selon l'utilisation comme les mises en œuvre d'utilisation partagée ou d'itinérance.

L'état par appareil est typique des systèmes de gestion de réseau fondé sur l'interrogation, qui souvent aussi effectuent les fonctions de gestion de comptabilité, car les systèmes de gestion de réseau ont besoin de garder trace de l'état des appareils réseau pour des besoins opérationnels. Ces systèmes offrent des délais moyens de traitement égaux à la moitié de l'intervalle d'interrogation.

2.3.2 Modèle fondé sur l'événement sans mise en lots

Dans le modèle fondé sur l'événement, un appareil va contacter le serveur ou le gestionnaire de comptabilité quand il est prêt à transférer les données comptables. La plupart des systèmes comptables fondés sur l'événement, comme ceux fondés sur la comptabilité RADIUS décrite dans la [RFC2139], transfèrent seulement un événement comptable par paquet, ce qui est inefficace.

Sans mémorisation non volatile, un pur modèle fondé sur l'événement ne mémorise normalement les événements de comptabilité qui n'ont pas encore été livrés que jusqu'à ce qu'expire l'intervalle de temporisation. Par suite, ce modèle a les plus petites exigences de mémoire. Une fois l'intervalle de temporisation expiré, l'événement de comptabilité est perdu, même si l'appareil a un espace de mémoire tampon suffisant pour continuer à le mémoriser. Par suite, le modèle fondé sur l'événement est le moins fiable, car la perte de données comptables va se produire à cause du réamorçage d'appareils, de pertes de paquet soutenues, ou de défaillances du réseau de durée supérieure à l'intervalle de temporisation. Dans les protocoles fondés sur l'événement sans un message "garder en vie", les serveurs de comptabilité ne peuvent pas supposer une défaillance de l'appareil si aucun messages n'arrive pendant un certain temps. Donc, les systèmes comptables fondés sur l'événement ne sont normalement pas utile pour surveiller la bonne santé des appareils.

Le modèle fondé sur l'événement est fréquemment utilisé dans les réseau à utilisation partagée et l'itinérance, car ce modèle envoie des données aux domaines receveurs sans exiger d'eux qu'ils interrogent un grand nombre d'appareils, dont la plupart n'ont pas de données pertinentes. Comme le modèle fondé sur l'événement ne prend normalement pas en charge le traitement par lots, il permet d'envoyer les enregistrements de comptabilité avec de faibles délais de traitement, permettant l'application de techniques de prévention de fraude. Cependant, parce que les événements de comptabilité d'itinérance sont fréquemment de grande valeur, la mauvaise fiabilité de ce modèle pose problème. Par suite, le modèle d'interrogation fondé sur l'événement peut être plus approprié.

L'état par session est typique des systèmes fondés sur l'événement sans mise en lots. Par suite, l'approche fondée sur l'événement s'adapte mal. Cependant, les systèmes fondés sur l'événement offrent le plus faible délai de traitement car les événements sont traités immédiatement et il n'est pas possible qu'un événement requérant de faibles délais de traitement soit pris derrière un transfert par lot.

2.3.3 Modèle fondé sur l'événement avec mise en lots

Dans le modèle fondé sur l'événement avec mise en lots, un appareil va contacter le serveur ou gestionnaire de comptabilité quand il est prêt à transférer les données comptables. L'appareil peut contacter le serveur lorsque un lot d'une certaine taille a été rassemblé, lorsque des données d'un certain type sont disponibles, ou après l'écoulement d'une durée minimum. De tels systèmes peuvent transférer plus d'un événement de comptabilité par paquet et sont donc plus efficaces.

Un système fondé sur l'événement avec mise en lots va mémoriser les événements de comptabilité qui n'ont pas encore été livrés jusqu'à sa limite de mémoire. Par suite, des pertes de données comptables vont se produire à cause du réamorçage d'appareils, mais pas à cause de pertes de paquet ou de défaillances du réseau de durée suffisamment courte pour être traitées au sein de la mémoire disponible. Noter qu'alors que l'efficacité du transfert va augmenter avec la taille de lot, sans mémorisation non volatile, la perte de données potentielle résultant d'un réamorçage d'appareil va aussi augmenter.

Lorsque les systèmes fondés sur l'événement avec mise en lots ont un intervalle de garde en vie et fonctionnent sur un transport fiable, le serveur de comptabilité peut supposer qu'une défaillance s'est produite si aucun message n'est reçu dans l'intervalle de garde en vie. Donc, de telles mises en œuvre peuvent être utiles pour surveiller la santé des appareils. Lorsque ils sont utilisés dans ce but, le délai moyen avant la détection d'une défaillance est de la moitié de l'intervalle de garde en vie.

Par la mise en œuvre d'un algorithme de programmation, les systèmes fondés sur l'événement avec mise en lots peuvent assurer un service approprié aux événements de comptabilité qui exigent de faibles délais de traitement. Par exemple, des événements de comptabilité inter domaines de grande valeur pourront être envoyés immédiatement, permettant ainsi d'utiliser des techniques de prévention de fraude, tandis que tous les autres événements seront mis en lots. Cependant, il existe une possibilité qu'un événement exigeant un faible délai de traitement soit pris derrière un transfert par lots en cours. Le délai de traitement maximum est donc proportionnel à la taille maximum de lot divisée par la vitesse de la liaison.

Les systèmes fondés sur l'événement avec mise en lots s'adaptent selon le nombre d'appareils actifs. Par suite cette approche s'adapte mieux que l'approche conduite par l'événement pur ou même l'approche de l'interrogation, et est équivalente en termes d'adaptation à l'approche de l'interrogation fondée sur l'événement. Cependant, l'approche fondée sur l'événement avec mise en lots a de plus faibles délais de traitement que l'approche de l'interrogation fondée sur l'événement car la livraison des données comptables exige moins d'allers retours, et les événements qui exigent un faible délai de traitement peuvent avoir satisfaction si on emploie un algorithme de programmation.

2.3.4 Modèle d'interrogation fondé sur l'événement

Dans le modèle d'interrogation fondé sur l'événement, un gestionnaire de comptabilité ne va interroger l'appareil sur les données comptables que lorsque il reçoit un événement. Le client de comptabilité peut générer un événement lorsque un lot d'une certaine taille a été rassemblé, lorsque des données d'un certain type sont disponibles, ou après l'écoulement d'un délai minimum. Noter qu'alors que l'efficacité du transfert va augmenter avec la taille du lot, sans mémorisation non volatile, la perte de données potentielle résultant d'un réamorçage d'appareil va aussi augmenter.

Sans mémorisation non volatile, un modèle d'interrogation fondé sur l'événement va perdre des données à cause du réamorçage d'appareil, mais pas à cause de pertes de paquets, ou de partitions de réseau de courte durée. Si un intervalle minimum de livraison n'est pas fixé, les systèmes d'interrogation fondée sur l'événement ne sont pas utiles pour surveiller la santé de l'appareil.

Le modèle d'interrogation fondé sur l'événement peut être convenable pou l'utilisation en itinérance car il permet d'envoyer les données comptables aux partenaires de l'itinérance avec un faible délai de traitement. En même temps, la comptabilité qui n'est pas d'itinérance peut être traitée via des techniques d'interrogation plus efficaces, fournissant ainsi le meilleur des deux systèmes.

Lorsque la mise en lots peut être mise en œuvre, l'état requis dans l'interrogation fondée sur l'événement peut être réduit pour s'adapter au nombre d'appareils actifs. Si des portions du réseau ont de grosses variations d'activité, cet état peut en fait être moindre que celui de l'approche de l'interrogation. Noter que le délai de traitement dans cette approche est supérieur à celui de la comptabilité fondée sur l'événement avec mise en lots car au moins deux allers retours sont nécessaires pour livrer les données : un pour la notification d'événement, et un pour l'interrogation résultante.

2.3.5 Collecte des données, résumé

Modèle	Avantages	Inconvénients
Interrogation	État par appareil Robuste contre perte de paquet Transfert par lots	Pas robuste contre réamorçage d'appareil, défaillances du serveur ou du réseau* Intervalle d'interrogation déterminé par la limite de mémorisation Fort délai de traitement Ne convient pas pour l'itinérance
Fondé sur l'événement, pas de mise en lots	Plus faible délai de traitement Convient pour l'itinérance	Pas robuste contre perte de paquet, réamorçage d'appareil, ou défaillances du réseau* Faible efficacité État par session
Fondé sur l'événement, avec mise en lots et programmation	Latence d'un seul aller retour Transfert par lots Convient pour l'itinérance État par appareil actif	Pas robuste contre réamorçage d'appareil et défaillances du réseau*
Interrogation fondée sur l'événement	Transfert par lots Convient pour l'itinérance État par appareil actif	Pas robuste contre réamorçage d'appareil et défaillances du réseau* Latence de deux allers retours

Légende : * = traité par une mémorisation non volatile

3. Protocoles de comptabilité

Des systèmes comptables ont été mis en œuvre avec succès en utilisant des protocoles comme RADIUS, TACACS+, et SNMP. La présente section décrit les caractéristiques de chacun de ces protocoles.

3.1 RADIUS

La comptabilité RADIUS, décrite dans la [RFC2139], a été développée comme un additif au protocole d'authentification RADIUS, décrit dans la [RFC2138]. Par suite, la comptabilité RADIUS partage l'approche fondée sur l'événement de l'authentification RADIUS, sans prise en charge de la mise en lots ni de l'interrogation. Par suite, la comptabilité RADIUS s'adapte au nombre d'événements de comptabilité au lieu du nombre d'appareils, et les transferts de comptabilité sont inefficaces.

Comme la comptabilité RADIUS se fonde sur UDP et que des paramètres de temporisation et de réessai ne sont pas spécifiés, les mises en œuvre varient largement dans leur approche de la fiabilité, certaines mises en œuvre réessayant jusqu'à livraison ou saturation de la mémoire tampon, et d'autres qui perdent les données comptables après quelque essais. Comme la comptabilité RADIUS ne fournit pas d'accusé de réception de couche applications ou de messages d'erreur, une "Accounting-Response" RADIUS est équivalente à un accusé de réception de couche transport et ne donne pas de protection contre les dysfonctionnements de couche application. Du fait du manque de fiabilité, il n'est pas possible de faire un contrôle d'usage simultané sur la base de la seule comptabilité RADIUS. Normalement une autre source de données d'appareil est nécessaire, comme l'interrogation d'une MIB de session ou une session de ligne de commande sur telnet.

Les mises en œuvre de comptabilité RADIUS sont vulnérables à la perte de paquet ainsi qu'aux défaillances de couche application, aux défaillances du réseau, et aux réamorçages d'appareils. Ces déficiences sont aggravées en comptabilité inter domaines qui est exigée dans l'itinérance ([RFC2194], [RFC2477]). D'un autre côté, l'approche fondée sur l'événement de la comptabilité RADIUS est utile lorsque un faible délai de traitement est requis, comme dans la gestion du risque de crédit ou la détection de fraude.

Bien que la comptabilité RADIUS assure bien l'authentification bond par bond et la protection de l'intégrité, et qu'IPsec puisse être employé pour fournir la confidentialité bond par bond, la sécurité de l'objet de données n'est pas prise en charge, et donc, les systèmes fondés sur la comptabilité RADIUS ne peuvent pas être déployés avec des mandataires qui ne sont pas de confiance, ou dans des situations qui exigent une capacité de vérification, comme noté dans la [RFC2477].

Bien que RADIUS ne prenne pas en charge la compression, la compression IP, décrite dans la [RFC2393], peut être employée pour y pouvoir. Bien qu'en principe extensible avec la définition de nouveaux attributs, RADIUS souffre de son très petit espace d'attributs standard (256 attributs).

3.2 TACACS+

TACACS+ offre un modèle de comptabilité avec des messages de début, d'arrêt, et de mise à jour intérimaire. Comme TACACS+ se fonde sur TCP, les mises en œuvre sont normalement résilientes à la perte de paquet et aux partitions de réseau de courte durée, et TACACS+ s'adapte au nombre d'appareils. Comme TACACS+ fonctionne sur TCP, il offre la prise en charge des accusés de réception de couche transport et de couche application, et il convient pour le contrôle d'usage simultané et le traitement des événements de comptabilité qui exigent un délai de traitement modéré mais pas le plus court.

TACACS+ assure l'authentification bond par bond et la protection de l'intégrité ainsi que la confidentialité bond par bond. La sécurité de l'objet de données n'est pas prise en charge, et donc les systèmes fondés sur la comptabilité TACACS+ ne peuvent pas être déployés en présence de mandataires qui ne sont pas de confiance. Bien que TACACS+ ne prenne pas en charge la compression, la compression IP, décrite dans la [RFC2393], peut être employée pour la fournir.

3.3 SNMP

SNMP, décrit dans les [RFC1905], [RFC2570], [RFC2571], a été largement déployé dans des applications de comptabilité intra domaine très diverses, utilisant normalement le modèle de collecte des données par interrogation. L'interrogation permet de collecter les données simultanément sur plusieurs événements de comptabilité, d'où résulte un état par appareil. Les applications de gestion sont capables de répéter les demandes quand une réponse n'est pas reçue, fournissant la résilience contre la perte de paquet ou même les partitions de réseau de courte durée. Les mises en œuvre sans mémorisation non volatile ne sont pas robustes contre le réamorçage d'appareil ou les défaillances du réseau, mais lorsque combinées avec la mémorisation non volatile, elles peuvent être très fiables.

SMIv1, le langage de modélisation des données de SNMPv1, a des alarmes *(traps)* pour permettre l'interrogation fondée sur l'alarme, mais il n'y a pas d'accusé de réception des alarmes, et une alarme perdue peut conduire à une perte de données. SMIv2, utilisé par SNMPv2c et SNMPv3, a des demandes d'information *(Inform Request)* qui sont des notifications soumises à accusé de réception. Cela rend possible de mettre en œuvre un modèle d'interrogation fondé sur l'événement ou modèle fondé sur l'événement avec mise en lots plus fiables. Cependant, on n'a pas connaissance pour l'instant d'une mise en œuvre de comptabilité fondée sur SNMP construite sur l'utilisation de ces demandes d'information.

3.3.1 Services de sécurité

SNMPv1 et SNMPv2c prennent en charge l'authentification par paquet et les profils en lecture seule et en lecture-écriture, via la chaîne "community". Cette approche de mot de passe en clair ne fournit qu'une authentification triviale, et aucune protection de l'intégrité par paquet, ni protection contre la répétition ou de la confidentialité. Le contrôle d'accès fondé sur la vue [RFC2575] peut être pris en charge en utilisant la snmpCommunityMIB, définie dans la [RFC2576], et les messages SNMPv1 ou SNMPv2c. L'architecture SNMP mise à jour [RFC2571] prend en charge l'authentification par paquet bond par bond, la protection de l'intégrité et contre la répétition, la confidentialité et le contrôle d'accès.

Le modèle de sécurité d'utilisateur (USM, *User Security Model*) SNMP [RFC2574] utilise des secrets partagés, et lorsque le produit du nombre de domaines par les appareils est grand, comme dans les applications de comptabilité inter domaines, le nombre de secrets partagés peut devenir ingérable. La capacité de clé localisée dans USM permet à un gestionnaire d'avoir une clé centrale, qu'il partage avec de nombreuses entités SNMP d'une façon localisée tout en empêchant les autres entités d'accéder aux données des autres. Cela peut aider à la sécurité inter domaines si c'est déployé correctement.

SNMPv3 ne prend pas en charge l'intégrité et la confidentialité d'objet de données de bout en bout ; les entités mandataires de SNMP déchiffrent et rechiffrent les données qu'elles transmettent. En présence d'une entité mandataire qui n'est pas de confiance, cela serait inadéquat.

3.3.2 Accusés de réception de couche application

SNMP utilise des accusés de réception de couche application pour indiquer que les données ont été traitées. Les réponses SNMP aux demandes get, get-next, ou get-bulk retournent les données demandées, ou un code d'erreur indiquant la nature de l'erreur rencontrée.

Une réponse SNMP noError à une commande SET indique que les allocations demandées ont été faites par l'application. Les SET SNMP sont atomiques ; la commande réussit ou échoue. Une réponse d'erreur indique que l'entité a reçu la demande, mais n'a pas réussi à l'exécuter.

Les notifications n'utilisent pas d'accusé de réception pour indiquer que les données ont été traitées. La notification Inform retourne un accusé de réception, mais pas de traitement, par conception. Comme l'architecture SNMP mise à jour traite les entités comme des homologues avec divers niveaux de fonctionnalités, il est possible d'utiliser les SET dans l'une ou l'autre direction entre entités coopérantes pour réaliser les traitements des accusés de réception.

Il y a dix huit codes d'erreur SNMP. La conception de SNMP rend les codes d'erreur spécifiques du service inutiles et indésirables.

3.3.3 Transmetteurs mandataires

Dans l'architecture de gestion comptable, les transmetteurs mandataires jouent un rôle important, en transmettant les événements de comptabilité intra et inter domaines aux destinations correctes. Le transmetteur mandataire peut aussi jouer un rôle dans une architecture d'interrogation ou d'interrogation fondée sur l'événement.

La fonctionnalité d'un transmetteur mandataire SNMP est définie dans la [RFC2573]. Par exemple, les appareils réseau peuvent être configurés à envoyer des notifications pour tous les domaines au transmetteur mandataire, et les appareils peuvent être configurés à permettre au transmetteur mandataire d'accéder à toutes les données de MIB.

L'utilisation du transmetteur mandataires peut réduire le nombre de secrets partagés requis pour la comptabilité inter domaines. Avec des transmetteurs mandataires, les domaines peuvent partager un secret avec le transmetteur mandataire, et à son tour, le transmetteur mandataire peut partager un secret avec chaque appareil. Donc, le nombre de secrets partagés va s'ajuster à la somme du nombre des appareils et des domaines plutôt qu'à leur produit.

Le moteur d'un transmetteur mandataire SNMP ne regarde pas à l'intérieur de la PDU du message sauf pour déterminer à quel moteur SNMP devrait être transmise la PDU ou quelle application locale SNMP devrait traiter la PDU. Le transmetteur mandataire SNMP ne modifie pas les valeurs de varbind ; il ne modifie pas la liste des varbind sauf pour traduire entre les versions SNMP et il ne fournit aucun contrôle d'accès de niveau varbind.

3.3.4 Contrôles d'accès fondés sur le domaine dans SNMP

Les contrôles d'accès fondés sur le domaine sont nécessaires lorsque plusieurs domaines administratifs sont impliqués, comme dans les réseaux à utilisation partagée et les associations d'itinérance décrites dans la [RFC2194]. Comme le même appareil peut être accessible par plusieurs organisations, il est souvent nécessaire de contrôler l'accès aux données comptables conformément à l'organisation de l'utilisateur. Cela assure que les organisations peuvent recevoir l'accès aux données comptables qui se rapportent à leurs utilisateurs, mais pas aux données relevant d'utilisateurs d'autres organisations.

Pour appliquer des contrôles d'accès fondés sur le domaine, dans la comptabilité inter domaines, il est d'abord nécessaire d'identifier le sous ensemble de données qui doit se voir appliqué le contrôle d'accès. Plusieurs abstractions conceptuelles sont utilisées pour identifier les sous ensembles de données dans SNMP. Cela inclut des moteurs, des contextes, et des vues. Cette section décrit comment cette fonctionnalité peut être appliquée dans la comptabilité intra et inter domaines.

3.3.4.1 Moteurs

La nouvelle architecture SNMP, décrite dans la [RFC2571], ajoutait le concept de moteur SNMP pour améliorer la prise en charge de la mobilité et pour identifier quelle source de données est référencée. Le moteur est la portion d'une entité SNMP qui construit les messages, fournit les fonctions de sécurité, et transpose dans la couche transport. Les agents et gestionnaires traditionnels contiennent chacun un moteur SNMP . Un identifiant de moteur (engineID) permet à un moteur SNMP d'être identifié de façon univoque, indépendamment de l'adresse à laquelle il est rattaché au réseau.

Un champ securityEngineID dans un message identifie le moteur qui fournit l'accès aux accréditifs de sécurité contenus dans l'en-tête de message. Un champ contextEngineID dans un message identifie le moteur qui donne l'accès aux données contenues dans la PDU.

Le format de message SNMPv3 passe explicitement les deux. Dans SNMPv1 et SNMPv2c, l'origine des données est normalement supposée être le point d'extrémité de communication (agent SNMP). Les messages SNMPv1 et SNMPv2c contiennent un nom de communauté ; le nom de communauté et l'adresse de source peuvent être transposés en un engineID via le snmpCommunityTable, décrit dans la [RFC2576].

3.3.4.2 Contextes

Les contextes sont utilisés pour identifier des sous ensembles d'objets, dans la portée du moteur, qui sont liés à

l'instrumentation. Un nom de contexte *(contextName)* se réfère à un sous ensemble particulier au sein d'un moteur.

Les contextes sont généralement liés aux composants matériels, aux entités logiques relatives aux composants matériels, ou à des services logiques. Par exemple, "contextNames" pourrait inclure tableau5, tableau7, répéteur1, répéteur2, etc.

Un agent SNMP remplit un tableau dynamique en lecture seule pour dire au gestionnaire quels contextes il reconnaît. Les contextes typiques sont définis par l'agent plutôt que par le gestionnaire car si le gestionnaire les définit, l'agent ne va pas savoir comment lier les contextes à l'instrumentation sous-jacente. Il est possible que des modules de MIB soient définis pour permettre à un gestionnaire d'allouer des contextNames à un sous ensemble logique d'instrumentation.

Bien que chaque contexte puisse prendre en charge des instances de plusieurs modules de MIB, chaque contextName est limité à une instance d'un module de MIB particulier. Si plusieurs instances d'un module de MIB sont nécessaires par moteur, des noms de contexte uniques doivent alors être définis (par exemple répéteur1, répéteur2). Le contexte par défaut "" est utilisé pour les moteurs qui ne prennent en charge qu'une seule instance de module de MIB, et il est utilisé pour les modules de MIB pour lesquels il n'y aurait pas de sens d'avoir autre chose qu'une instance de ce module de MIB dans un moteur et cette instance doit être facile à localiser, comme la MIB système ou les MIB de sécurité.

Les messages SNMPv3 contiennent des noms de contexte dont la portée est limitée au contextEngineID dans le message. Les messages SNMPv1 et SNMPv2c contiennent des communautés qui peuvent être transposées en noms de contexte au sein du moteur local, ou peuvent être transposées en contextNames au sein d'autres moteurs via le snmpCommunityTable, décrit dans la [RFC2576].

3.3.4.3 Vues

Les vues sont définies dans le modèle de contrôle d'accès fondé sur la vue (VACM, *View-based Access Control Model*). Une vue est un gabarit qui est utilisé pour déterminer l'accès aux objets gérés dans un contexte particulier. La vue identifie quels objets sont visibles, en spécifiant les OID des sous arborescences incluses et exclues. Il y a aussi un mécanisme pour permettre des caractères génériques dans la spécification des OID.

Par exemple, il est possible de définir une vue qui inclut des tableaux de surveillance à distance (RMON, *Remote MONitoring*) et une autre vue qui inclut seulement les tableaux relatifs à la sécurité SNMPv3. En utilisant ces vues, il est possible de permettre l'accès à la vue RMON pour les utilisateurs Joe et Josephine (les administrateurs RMON) et l'accès aux tableaux de sécurité SNMPv3 pour l'utilisateur Adam (l'administrateur de sécurité SNMP).

Les vues peuvent être établies avec des caractères génériques. Pour un tableau qui est indexé en utilisant des adresses IP, l'accès peut être permis à Joe à toutes les rangées dans les tableaux RMON donnés (par exemple le tableau des hôtes RMON) qui sont sur le sous réseau 10.2.x.x, tandis que l'accès est donné à Josephine à toutes les rangées pour le sous réseau 10.200.x.x.

Les vues filtrent au niveau du nom (OID), non au niveau de la valeur, de sorte que définir des vues sur la base de valeurs de données non indexées n'est pas accepté. Dans cet exemple, où l'adresse IP est utilisée simplement comme élément de données plutôt que comme index, il ne serait pas possible d'utiliser le contrôle d'accès fondé sur la vue pour atteindre l'objectif désiré (délégation de responsabilité administrative selon le sous réseau).

Le contrôle d'accès fondé sur la vue est indépendant de la version de message. Il peut être utilisé par des entités qui utilisent les formats de message SNMPv1, SNMPv2c, ou SNMPv3.

3.3.5 Autres contrôles d'accès inter domaines

Lorsque augmente le nombre des appareils réseau au sein d'un réseau à utilisation partagée ou d'itinérance, le modèle d'interrogation pour la collecte des données devient de plus en plus impraticable car la plupart des appareils ne vont pas porter de données en rapport avec l'organisation qui fait l'interrogation. Par suite, les réseaux à utilisation partagée ou les associations d'itinérance qui s'appuient sur la comptabilité fondée sur SNMP ont généralement collecté les données pour toutes les organisations et ont ensuite trié les enregistrements de session résultants pour les livrer à chaque organisation. Bien que fonctionnelle, cette approche va normalement résulter en un délai de traitement qui augmente avec le nombre d'organisations et d'enregistrements de données.

Cette question peut être réglée dans SNMP en utilisant l'approche fondée sur l'événement, de l'interrogation fondée sur l'événement ou fondée sur l'événement avec mise en lots. Les alarmes *(trap)* et les informations permettent aux appareils à capacité SNMP de notifier aux domaines qu'ils ont des données comptables qui attendent la collecte. Les applications SNMP [RFC2573] définissent un module standard pour gérer les notifications.

Pour utiliser les approches fondées sur l'événement, l'appareil doit être capable de déterminer quand l'information est disponible pour un domaine. Les données spécifiques d'un domaine peuvent être différenciées au niveau de l'agent SNMP avec l'utilisation du domaine comme index, et la séparation des données en contextes spécifiques du domaine.

3.3.5.1 Domaine comme indice

Le contrôle d'accès fondé sur la vue [RFC2575] permet d'allouer à des groupes d'utilisateurs spécifiques plusieurs vues de granularité fine d'une MIB SNMP, de telle façon que les droits d'accès aux éléments de données inclus dépendent de l'identité de l'utilisateur qui fait la demande.

Par exemple, tous les utilisateurs de bigco.com à qui l'accès à l'appareil est permis seront définis dans le module de MIB de sécurité fondée sur l'utilisateur (ou autre module de MIB de modèle de sécurité). Pour simplifier, dans l'administration du contrôle d'accès, les usagers peuvent être groupés en utilisant un vacmGroupName *(nom de groupe VACM)*, par exemple bigco. Une vue d'un sous ensemble des objets de données dans la MIB peut être définie dans le vacmViewFamilyTreeTable *(tableau d'arborescence de famille de vue VACM)*. Un vacmAccessTable *(tableau d'accès VACM)* apparie les groupes et les vues. Pour les messages reçus des usagers dans le groupe bigco, l'accès ne serait fourni qu'aux données dont la vue est permise aux utilisateurs de bigco, comme défini dans l'arborescence de la famille de vue. Cela exige que chaque domaine qui accède aux données reçoive un ou plusieurs vacmGroupNames séparés, qu'un ViewTable approprié soit défini, et que le vacmAccessTable soit configuré pour chaque groupe.

Les vues filtrent au niveau du nom (OID) non au niveau des données (valeur). Lorsque on utilise des vues pour filtrer par domaine, il est nécessaire d'utiliser le domaine comme un index. Le contrôle d'accès standard fondé sur la vue n'est pas conçu pour filtrer sur la base des valeurs sur des champs non indexés.

Par exemple, un tableau de données de session pourrait être indexé par numéro d'enregistrement et domaine, permettant de définir une vue qui pourrait restreindre l'accès aux données de bigco aux administrateurs du domaine bigco.

Un avantage de l'utilisation des domaines comme index est que cette technique peut être utilisée avec les agents SNMPv1 et SNMPv2c aussi bien que SNMPv3. Un inconvénient est que les modules de MIB doivent être spécifiquement conçus à cette fin. Comme les modules de MIB existants utilisent rarement le domaine comme index, la séparation de domaines ne peut pas être activée au sein des modules de MIB traditionnels qui utilisent cette technique.

SNMP prend en charge une convention RowPointer *(pointeur de rangée)* qui pourrait être utilisée pour définir un nouveau tableau, indexé par domaine, qui contiendrait les couplages entre le domaine et les rangées existantes de données. Cela introduirait des problèmes de synchronisation entre tableaux.

3.3.5.2 Contextes

ContextNames peut être utilisé pour différencier plusieurs instances d'un module de MIB au sein d'un moteur.

Les domaines individuels, comme bigco.com, pourraient être transposés en contextes logiques, comme un contexte bigco. L'agent aurait besoin de créer et reconnaître les nouveaux contextes et de savoir quelle instrumentation est associée au contexte logique. L'agent a besoin de collecter les données comptables par domaine et de rendre les données accessibles via des contextes distincts, afin que le contrôle d'accès puisse être appliqué au contexte pour empêcher la divulgation d'informations sensibles au mauvais domaine. Les vues de contrôle d'accès VACM sont appliquées par rapport au contexte, de sorte qu'une opération peut être permise ou refusée à un utilisateur sur la base du contexte qui contient les données.

La séparation de domaines est traitée en utilisant le contextName pour différencier plusieurs tableaux virtuels. Par exemple, si des données comptables ont été collectées sur les utilisateurs sur les domaines bigco.com et smallco.com, Une instance virtuelle séparée du tableau d'enregistrements de session de comptabilité va exister pour chaque domaine, et chaque domaine aura un contextName correspondant. Lorsque une demande get-bulk est faite avec un nom de contexte de bigco, les données provenant du tableau virtuel dans le contexte bigco, c'est-à-dire, correspondant au domaine bigco.com, seraient alors retournées.

Il y a un certain nombre d'approches conceptuelles pour créer de nouveaux contextes et associer les contextes à l'instrumentation appropriée, principalement l'approche du sous agent et l'approche de la MIB configurée par un gestionnaire.

L'agent X [RFC2741], qui normalise un protocole d'enregistrement entre les sous agents et les agents maîtres pour simplifier la mise en œuvre d'agent SNMP, permet la création et la reconnaissance de nouveaux noms de contexte lorsque un sous agent s'enregistre pour fournir la prise en charge d'une gamme particulière de sous arborescence de MIB. Le sous agent sait comment prendre en charge une fonctionnalité particulière, par exemple l'instrumentation exposée via une gamme d'objets de MIB. Sur la base des valeurs détectées dans les données, comme source=bigco.com, le sous agent peut

déterminer qu'un nouveau domaine a dû être retracé et créer le contexte approprié pour la collecte des données, plus les entrées appropriées de contrôle d'accès. La détermination pourrait être fondée sur le tableau, en utilisant la configuration de MIB.

Une approche fondée sur le gestionnaire pourrait utiliser un module de MIB pour prédéfinir des noms de contexte correspondants aux domaines d'intérêt, et pour indiquer quels objets devraient être collectés, comment différencier à quel domaine les données devraient être appliquées sur la base d'une condition spécifiée, et quelles règles de contrôle d'accès appliquer au contexte.

L'une ou l'autre technique peut associer les modules de MIB existants aux contextes spécifiques de domaines, de sorte que la séparation des domaines peut être appliquée aux modules de MIB non spécifiquement conçus en vue d'une séparation de domaine. Les agents traditionnels ne sont pas conçus pour faire cela et il faudra les mettre à jour pour qu'ils prennent en charge la séparation inter domaines et le contrôle d'accès VACM.

L'utilisation des noms de contextes pour la séparation inter domaines représente un nouveau territoire, de sorte qu'une considération attentive devrait être apportée à la conception des modules et applications de MIB pour fournir les transpositions de domaine en contexte et de contexte en instrumentation, et pour assurer que la sécurité n'est pas affaiblie.

3.3.6 Questions en cours

Une question se pose lorsque on utilise SNMP pour le transfert de données brutes, qui inclut les questions de latence, de frais généraux du réseau, et de restitution de tableaux, comme exposé dans [49].

Dans les applications de comptabilité, les stations de gestion doivent souvent restituer de grands tableaux. La latence peut être élevée, même avec l'opération get-bulk, parce que la réponse doit tenir dans la plus grande taille de paquet acceptée, exigeant plusieurs allers retours. Les transferts peuvent être mis en série et la latence résultante sera une combinaison de plusieurs temps d'aller retour, une éventuelle fin de temporisation et des délais de retransmission et de redondance de traitement, qui peuvent résulter en des performances inacceptables. Comme les données peuvent changer durant le cours de multiples restitutions, il peut être difficile d'en avoir une image cohérente.

Pour les transferts en vrac, les frais généraux du réseau SNMP peuvent être élevés du fait du manque de compression, de l'inefficacité du codage BER, de la transmission de préfixes d'OID redondants, et du "problème de l'exagération de get-bulk". Dans le transfert en vrac d'un tableau, les OID transférés sont redondants : tous les préfixes d'OID jusqu'au numéro de colonne sont identiques, comme le sont les postfixes d'identifiant d'instance de toutes les entrées d'une même rangée de tableau. Donc, il est possible de réduire cette redondance en compressant les OID, ou en ne transférant pas un OID avec chaque variable.

Le "problème de l'exagération de get-bulk", décrit dans la référence [50], survient lors de l'utilisation de la PDU get-bulk. Le problème est que normalement le gestionnaire ne connaît pas le nombre de rangées dans le tableau. Par suite, il doit demander trop de rangées, restituant des données inutiles, ou pas assez, résultant en le besoin de plusieurs demandes get-bulk. Noter que le "problème de l'exagération de get-bulk" peut être prévenu du côté de l'agent. La [RFC1905] déclare qu'un agent peut terminer le get-bulk à cause de "contraintes locales" (voir les points 1 et 3 des pages 15/16 de la [RFC1905]). Cela pourrait être interprété comme signifiant qu'il est possible de s'arrêter à la fin d'un tableau.

3.3.6.1 Recherches en cours

Pour traiter les questions de latence et d'efficacité, le groupe de recherches sur la gestion de réseau (NMRG, *Network Management Research Group*) a été formé au sein de l'équipe de recherche de l'Internet (IRTF, *Internet Research Task Force*). Comme le NMRG a mené ses recherches et n'a pas abouti à un texte sur la voie de la normalisation, on doit comprendre que les propositions du NMRG ne pourront jamais être normalisées, ou peuvent changer substantiellement durant le processus de normalisation. Par suite, ces propositions représentent des travaux en cours et ne sont pas directement disponibles à l'utilisation.

Les propositions en discussion au groupe de recherches sur la gestion de réseau (NMRG) de l'IRTF sont décrites dans [46]. Elles incluent une transposition de transport SNMP sur TCP, décrite dans la [RFC3430], la compression de charge utile SNMP, décrite dans [48], et l'ajout d'une PDU "sous arborescence get" ou la MIB de restitution de sous arborescence [50].

La transposition de transport SNMP sur TCP peut résulter en de substantielles réductions de latence dans la restitution des tableaux. La réduction de latence d'une transposition de transport SNMP sur TCP va probablement se manifester principalement dans les modes d'interrogation, d'interrogation fondée sur l'événement et fondée sur l'événement avec mise en lots.

Les méthodes de compression de charge utile incluent la compression des paquets IP, décrite dans la [RFC2393] ou la compression de la charge utile SNMP, décrite dans [48].

Les améliorations proposées à la restitution de tableau incluent une MIB de restitution de sous arborescence et l'ajout d'une PDU get-subtree. La MIB de restitution de sous arborescence [50] n'exige pas de changement au protocole SNMP ni au moteur de protocole SNMP, de sorte qu'il peut être mis en œuvre et déployé plus facilement qu'un changement au protocole. L'ajout d'une PDU get-subtree implique des changements au protocole et aux moteurs de toutes les entités SNMP qui devraient la prendre en charge. Comme il est possible de traiter le "problème de l'exagération de get-bulk" sans changement au protocole SNMP, la nécessité de cette modification est controversée.

La référence [49] discute aussi de la mémorisation sur fichier des données SNMP, et de l'utilisation d'une MIB FTP, pour permettre le stockage de données SNMP dans une mémorisation non volatile, et ensuite du transfert en vrac via FTP. Cette approche exigerait la mise en œuvre de modules de MIB supplémentaires ainsi que de FTP, et exige des mécanismes de sécurité séparé tels que IPsec pour assurer l'authentification, la protection de l'intégrité et de confidentialité et contre la répétition pour les données en transit. L'approche du transfert fondé sur le fichier présente un important avantage – la compatibilité avec la mémorisation non volatile.

La proposition du NMRG pose un problème avec les supports traditionnels existants. Les appareils qui ne mettent pas en œuvre la nouvelle fonctionnalité auraient besoin d'être adaptés. Ceci est particulièrement problématique pour les transmetteurs mandataires, qui peuvent avoir besoin d'agir comme traducteurs entre les nouvelles entités et les traditionnelles. Dans ces situations, les frais généraux de traduction peuvent dépasser les avantages de la nouvelle technologie.

3.3.6.2 Recherches en cours sur l'extension de la sécurité

Afin de simplifier la gestion de clés et permettre l'utilisation d'une sécurité fondée sur le certificat dans SNMPv3, un modèle de sécurité Kerberos (KSM, *Kerberos Security Model*) pour SNMPv3 a été proposé dans [44]. Ce mémoire n'est pas sur la voie de la normalisation, et n'est donc pas encore disponible à l'utilisation.

L'utilisation de Kerberos avec SNMPv3 exige la mémorisation d'une clé sur le centre de distribution de clés (KDC, *Key Distribution Centre*) pour chaque appareil et domaine, tout en générant de façon dynamique une clé de session pour les conversations entre domaines et appareils. En termes de clés mémorisées, l'approche du KSM s'adapte bien à la somme des appareils et des domaines ; en termes de clés de session dynamiques, elle s'adapte au produit des domaines et des appareils.

Comme Kerberos a été étendu pour permettre l'authentification initiale via une clé publique, comme décrit dans la [RFC4556], et l'authentification inter domaines, comme décrit dans [RFC4556], le KSM hérite de ces capacités. Par suite, cette approche peut avoir un potentiel de réduction ou même de suppression du problème de la gestion du secret partagé. Cependant, on devrait aussi noter que l'authentification fondée sur le certificat peut restreindre les limites de taille de paquet UDP prises en charge dans les mises en œuvre SNMP, de sorte que d'autres transpositions de transport peuvent être nécessaires pour la prendre en charge.

Un modèle de sécurité fondé sur IPsec pour SNMPv3 a été discuté. La mise en œuvre d'un tel modèle de sécurité exigerait que le moteur SNMPv3 soit capable de restituer les propriétés de l'association de sécurité IPsec utilisée pour protéger le trafic SNMPv3. Ceci inclurait les services de sécurité invoqués, ainsi que les informations relatives à l'autre point d'extrémité, comme la méthode d'authentification et l'identité présentée et le certificat. À ce jour des API n'ont pas été largement mises en œuvre, et de plus, la plupart des mises en œuvre IPsec ne prennent en charge que les certificats de machine, qui ne peuvent pas fournir la granularité d'identification requise. Donc, un modèle de sécurité fondé sur IPsec pour SNMPv3 prendre probablement plusieurs années pour porter ses fruits.

3.3.7 Résumé de SNMP

Étant donnée la richesse des modules de MIB existants relatifs à la comptabilité, il est probable que SNMP restera un protocole de comptabilité populaire dans l'avenir prévisible.

La prise en charge des notifications rend possible de mettre en œuvre les modèles fondés sur l'événement, l'interrogation fondée sur l'événement et fondé sur l'événement avec mise en lots. Cela rend possible de notifier aux domaines la disponibilité des données plutôt que d'exiger d'elles qu'elle interrogent sur leur existence, ce qui est critique dans les réseaux à utilisation partagée et en itinérance.

Étant données les améliorations de la sécurité de SNMPv3, il est souhaitable que les mises en œuvre de comptabilité intra domaine SNMP se mettent à niveau avec SNMPv3. Une telle mise à niveau est virtuellement obligatoire pour les applications inter domaines.

En comptabilité inter domaine, la charge de la gestion des secrets partagés SNMPv3 peut être réduite via la capacité de clé localisée ou via la mise en œuvre d'un transmetteur mandataire. À long terme, d'autres modèles de sécurité comme le modèle de sécurité Kerberos pourront encore réduire l'effort nécessaire pour gérer la sécurité et permettre un fonctionnement inter domaines aminci.

La comptabilité fondée sur SNMP a des limitations en termes d'efficacité et de latence qui peuvent rendre son utilisation inappropriée dans les situations qui exigent de faibles délais de traitement ou de faibles frais généraux. Cela inclut les applications de facturation selon l'usage où la détection des fraudes peut être nécessaire. Ces questions peuvent être traitées via des propositions en discussion dans le groupe de recherches sur la gestion de réseau (NMRG) de l'IRTF. La transposition expérimentale de transport SNMP sur TCP peut se révéler utile pour réduire la latence. Selon le volume de données, certaines formes de compression peuvent aussi valoir la peine d'être prises en compte. Cependant, comme ces propositions en sont encore à l'état de recherches, et ne sont pas sur le chemin de la normalisation, ces capacités ne sont pas encore disponibles, et leur spécification pourrait changer considérablement avant qu'elle atteigne sa forme finale.

SNMP prend en charge la séparation des données comptables par domaine, utilisant l'une ou l'autre des deux approches générales du modèle de contrôle d'accès VACM. L'approche du domaine comme index peut être utilisée si le module de MIB désiré prend en charge l'indexation de domaine, ou elle peut être mise en œuvre en utilisant un tableau supplémentaire. L'approche du contexte de domaine peut être utilisée dans les agents qui prennent en charge les contextes logiques dynamiques et un mécanisme de transposition de domaine en contexte et de contexte en instrumentation. L'une et l'autre de ces approches peut être prise en charge en utilisant les messages SNMPv1, SNMPv2c, ou SNMPv3, en utilisant le snmpCommunitytable [RFC2576] pour fournir une transposition de communauté en contexte.

4. Transfert des données comptables

Pour que les enregistrements de session soient transmis entre les serveurs de comptabilité, un protocole de transfert est nécessaire. Les protocoles de transfert utilisés aujourd'hui incluent SMTP, FTP, et HTTP. Pour une revue des attributs et formats d'enregistrements de comptabilité, voir la [RFC2924].

La référence [49] contient une discussion des divers codages des types de données de SMI, ainsi que des différents protocoles pour la transmission des données comptables. Par exemple, [49] décrit comment les étiquettes MIME et les DTD XML peuvent être utilisés pour coder les messages SNMP ou les types de données de SMI. Cela permet que les données des MIB SNMP soient transportées en utilisant tout protocole qui peut encapsuler MIME ou XML, incluant SMTP et HTTP.

4.1 SMTP

Aujourd'hui, peu de systèmes de gestion de la comptabilité ont été construits sur SMTP car la mise en œuvre d'un système de message à livraison différée a traditionnellement exigé l'accès à une mémorisation non volatile qui n'était pas largement disponible sur les appareils réseau. Cependant, les mises en œuvre fondées sur SMTP ont de nombreuses caractéristiques désirables, en particulier à l'égard de la sécurité.

Les systèmes de gestion de la comptabilité qui utilisent SMTP pour les transfert de comptabilité vont normalement prendre en charge la mise en lots de sorte que les frais généraux du traitement de message vont être étalés sur plusieurs enregistrement de comptabilités. Par suite, ces systèmes résultent en un état par appareil actif. Comme les systèmes comptables qui utilisent SMTP comme mécanisme de transfert ont accès à une mémorisation non volatile substantielle, ils peuvent générer, compressés si nécessaire, et stocker les enregistrements de comptabilité jusqu'à ce qu'ils soient transférés au site de collecte. Par suite, les systèmes comptables mis en œuvre avec SMTP peuvent être très efficaces et adaptables. En utilisant IPsec, TLS ou Kerberos, les services de sécurité bond par bond tels que l'authentification, la protection de l'intégrité et de la confidentialité peuvent être fournis.

Comme décrit dans la [RFC2015] et la [RFC1847], la sécurité de l'objet de données est disponible pour SMTP, et de plus, les facilités décrites dans la [RFC2298] rendent possible de demander et recevoir des récépissés signés, ce qui permet la non répudiation, comme décrit dans les [RFC1521] et [RFC2298]. Par suite, les systèmes comptables qui utilisent SMTP pour les transfert des données comptables sont capables de satisfaire aux exigences de sécurité les plus strictes. Cependant, de tels systèmes ne sont normalement pas capables d'assurer un faible délai de traitement, bien que ceci puisse être réglé par les améliorations décrites dans la [RFC3965].

4.2 Autres protocoles

Des protocoles de transfert de fichier comme FTP et HTTP ont été utilisés pour le transfert des données comptables. Par exemple, la [RFC2512] décrit un moyen pour représenter en ASN.1 les données comptables à stocker sur un support d'archivage. Par l'utilisation de la MIB de fichier en vrac, les données comptables d'une MIB SNMP peuvent être stockées en format ASN.1, binaire brut ou ASCII en vrac, et ensuite restituées comme nécessaire en utilisant la MIB de client FTP.

En donnant accès à une mémorisation non volatile suffisante, les systèmes comptables fondés sur des formats d'enregistrement et des protocoles de transfert peuvent éviter la perte de données due à des partitions de réseau de longue durée, des défaillances de serveur ou des réamorçages d'appareils. Comme il est possible que le transfert soit piloté depuis le site de collecte, le collecteur peut réessayer le transfert jusqu'à ce qu'il réussisse, ou avec HTTP peut même être capable de recommencer un transfert partiellement achevé. Par suite, les systèmes fondés sur le transfert peuvent être rendus très fiables, et la mise en lots des enregistrements de comptabilité rend possible des transferts efficaces et l'application des services de sécurité requis avec des frais généraux moindres.

5. Résumé

Comme noté précédemment dans le présent document, les applications de comptabilité ont des exigences de sécurité et de fiabilité variables. Certaines utilisations comme la planification des capacités peuvent n'exiger que l'authentification, la protection de l'intégrité et contre la répétition, et une modeste fiabilité. D'autres applications comme la facturation inter domaine selon l'utilisation peuvent exiger le plus haut degré de sécurité et de fiabilité, car dans ce cas, le transfert des données comptables va conduire directement au transfert de fonds.

Comme les applications de comptabilité n'ont pas des exigences uniformes de sécurité et de fiabilité, il n'est pas possible d'imaginer un seul protocole de comptabilité et ensemble de services de sécurité qui satisfasse tous les besoins. Le but de la gestion de la comptabilité devrait plutôt être de fournir un ensemble d'outils qui puisse être utilisé pour construire des systèmes comptables satisfaisant les exigences d'une application individuelle. Par suite, il est important d'analyser une application de comptabilité donnée pour s'assurer que les méthodes choisies satisfont les exigences de sécurité et de fiabilité de l'application.

Sur la base de l'analyse des exigences, il apparaît que les protocoles existants déployés sont capables de satisfaire les exigences de planification des capacités intra domaine et de facturation non sensible à l'utilisation. Dans ces applications un transfert efficace de données en vrac est utile bien que non critique. Donc, il est possible d'utiliser SNMPv3 pour satisfaire ces exigences, sans les extensions du NMRG. Cela inclut la transposition de transport TCP, la restitution de sous arborescence, et la compression d'OID.

Dans la planification des capacités inter domaines et la facturation non sensible à l'utilisation, les exigences de sécurité et de fiabilité sont plus importantes. Par suite, aucun protocole déployé existant ne satisfait les exigences. Par exemple, les protocoles existants ne prennent pas en charge la sécurité d'objet de données, et les extensions pour améliorer l'adaptabilité de l'authentification sont nécessaires, comme le modèle de sécurité Kerberos (KSM) pour SNMPv3.

Pour les application de facturation selon l'utilisation, ainsi que d'allocation des coûts et de vérification, l'exigence de fiabilité est plus grande. Ici, la fiabilité de la couche transport est exigée pour assurer la robustesse contre la perte de paquet, ainsi que des accusés de réception de couche application pour assurer la robustesse contre les défaillances du serveur de comptabilité. Les opérations SNMP à l'exception de InforRequest fournissent des accusés de réception de couche application, et la transposition de transport TCP proposée par le NMRG assure la robustesse contre la perte de paquet. Le fonctionnement inter domaines peut bénéficier de la sécurité de l'objet de données (qu'aucun protocole existant ne fournit) ainsi que des améliorations du modèle de sécurité inter domaines (comme le KSM).

Lorsque des sessions de grande valeur sont impliquées, comme dans l'itinérance, IP mobile, ou la téléphonie, il peut être nécessaire de limiter le délai de traitement. Cela implique de réduire la latence. Par suite, les extensions du NMRG sont nécessaires dans les applications de facturation selon l'utilisation, incluant la transposition de transport TCP, les capacités de get-subtree et la compression d'OID. Une haute fiabilité est aussi requise dans cette application, ce qui implique le besoin d'accusés de réception de couche application aussi bien que de couche transport. SNMPv3 avec les extensions du NMRG et les améliorations d'adaptabilité de la sécurité comme le KSM peut satisfaire aux exigences de l'utilisation intra domaine.

Cependant, dans l'utilisation inter domaines, des précautions de sécurité supplémentaires comme la sécurité de l'objet de données et la prise en charge de récépissés sont nécessaires. Aucun protocole existant ne peut satisfaire à ces exigences. Un résumé est donné dans le tableau de la page suivante.

Usage	Intra domaine	Inter domaines
Capacité de planification	SNMPv3 & RADIUS #%@ TACACS+ @	SNMPv3 &<*
Facturation non sensible à l'utilisation	SNMPv3 &RADIUS #%@ TACACS+ @	SNMPv3 &<*
Facturation selon l'utilisation, allocation des coûts & vérification	SNMPv3 &>$ TACACS+ &$@	SNMPv3 &<>*$
Facturation à la durée, détection de fraude, itinérance	SNMPv3 &>$	Pas de protocole existant

Légende :
= pas de prise en charge de la confidentialité
* = pas de sécurité de l'objet de données
% = robustesse limitée contre la perte de paquet
& = pas d'accusé de réception de couche application (par exemple InformRequest de SNMP)
$ = exige une mémorisation non volatile
@ = pas de prise en charge de la mise en lots
< = pas de prise en charge de certificat (KSM, travaux en cours)
> = pas de prise en charge de des paquets de grande taille (transposition de transport TCP, expérimental)

6. Considérations sur la sécurité

Les questions de sécurité sont discutées tout au long du présent mémoire.

7. Remerciements

Les auteurs aimeraient remercier Bert Wijnen (Lucent), Keith McCloghrie (Cisco Systems), Jan Melen (Ericsson) et Jarmo Savolainen (Ericsson) pour les utiles discussions sur de domaine.

8. Références

[RFC0793] J. Postel (éd.), "Protocole de commande de transmission – Spécification du protocole du programme Internet DARPA", STD 7, septembre 1981.

[RFC1155] M. Rose et K. McCloghrie, "Structure et identification des informations de gestion pour les internets fondés sur TCP/IP", STD 16, mai 1990.

[RFC1157] J. Case, M. Fedor, M. Schoffstall et J. Davin, "Protocole simple de gestion de réseau", STD 15, mai 1990. *(Historique)*

[RFC1212] M. Rose et K. McCloghrie, "Définitions concises de MIB", STD 16, février 1991.

[RFC1215] M. Rose, "Convention pour la définition de filtres à utiliser avec le SNMP", mars 1991. *(Info)*

[RFC1521] N. Borenstien et N. Freed, "MIME (Extensions multi-usage de messagerie Internet) Partie 1 : Mécanismes pour spécifier et décrire le format des corps de message Internet", septembre 1993. *(Obsolète, voir* RFC 2045 *à* 2049*)*

[RFC1767] D. Crocker,"Encapsulation MIME d'objets EDI", mars 1995. *(P.S.)*

[RFC1847] J. Galvin, S. Murphy, S. Crocker, N. Freed, "Sécurité multiparties pour MIME : multipartie/signée et multipartie/chiffrée", octobre 1995. *(P.S.)*

[RFC1892] G. Vaudreuil, "Type de contenu multipart/rapport pour les rapports de messages administratifs de systèmes de messagerie", janvier 1996. *(Obsolète, voir* RFC3462*) (P.S.)*

[RFC1901] J. Case, et autres "Introduction à SNMPv2 fondé sur la communauté", janvier 1996. *(Hist.)*

[RFC1905] J. Case, K. McCloghrie, M. Rose, S. Waldbusser "Opérations de protocole pour la version 2 du protocole simple de gestion de réseau (SNMPv2)", janvier 1996. (*Obsolète, voir* RFC3416) *(D.S.)*

[RFC1906] J. Case, K. McCloghrie, M. Rose, S. Waldbusser "Transpositions de transport pour la version 2 du protocole simple de gestion de réseau (SNMPv2)", janvier 1996. (*Obsolète, voir* RFC3417) *(D.S.)*

[RFC2015] M. Elkins, "Sécurité de MIME avec Pretty Good Privacy (PGP)", octobre 1996. (*MàJ par* RFC3156) *(P.S.)*

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

[RFC2138] C. Rigney, A. Rubens, W. Simpson, S. Willens, "Service d'authentification distante d'utilisateur appelant (RADIUS)", avril 1997. *(Remplace* RFC2058) (*Obsolète, voir* RFC2865) *(P.S.)*

[RFC2139] C. Rigney, "Comptabilité de RADIUS", avril 1997. (*Remplace* RFC2059) (*Obsolète, voir* RFC2866) *(Information)*

[RFC2194] B. Aboba, J. Lu, J. Alsop, J. Ding, W. Wang, "Récapitulation des mises en œuvre d'itinérance", septembre 1997. *(Info.)*

[RFC2298] R. Fajman, "Format de message extensible pour les notifications de disposition de message", mars 1998. (*Obsolète, voir* RFC3798) *(P.S.)*

[RFC2393] A. Shacham et autres, "Protocole de compression de charge utile IP (IPComp)", décembre 1998. (*Obs., voir* RFC3173)

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

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

[RFC2512] K. McCloghrie, J. Heinanen, W. Greene, A. Prasad, "Informations de comptabilité pour réseaux ATM", février 1999. *(P.S.)*

[RFC2513] K. McCloghrie, J. Heinanen, W. Greene, A. Prasad, "Objets gérés pour contrôler la collecte et la mémorisation des informations de comptabilité pour les réseaux orientés connexion", février 1999. *(P.S.)*

[RFC2570] J. Case, R. Mundy, D. Partain, B. Stewart, "Introduction à la version 3 du cadre de gestion de réseau de l'Internet", avril 1999. (*Obsolète, voir* RFC3410) *(Information)*

[RFC2571] B. Wijnen, D. Harrington, R. Presuhn, "Architecture pour la description des cadres de gestion SNMP", avril 1999. (*Obsolète, voir* RFC3411) *(D.S.)*

[RFC2572] J. Case, D. Harrington, R. Presuhn, B. Wijnen, "Traitement et répartition de message pour le protocole simple de gestion de réseau (SNMP)", avril 1999. (*Obsolète, voir* RFC3412) *(D.S.)*

[RFC2573] D. Levi, P. Meyer, B. Stewart, "Applications SNMP", avril 1999. (*Obsolète, voir* RFC3413) *(D.S.)*

[RFC2574] U. Blumenthal, B. Wijnen, "Modèle de sécurité fondé sur l'utilisateur (USM) pour la version 3 du protocole simple de gestion de réseau (SNMPv3)", avril 1999. (*Obsolète, voir* RFC3414) *(D.S.)*

[RFC2575] B. Wijnen, R. Presuhn, K. McCloghrie, "Modèle de contrôle d'accès fondé sur la vue (VACM) pour le protocole simple de gestion de réseau (SNMP)", avril 1999. (*Obsolète, voir* RFC3415) *(D.S.)*

[RFC2576] R. Frye, D. Levi, S. Routhier, B. Wijnen, "Coexistence entre les version 1, version 2 et version 3 du cadre de gestion de réseau de l'Internet" mars 2000. (*Obsolète, voir* RFC3584) *(P.S.)*

[RFC2578] K. McCloghrie, D. Perkins, J. Schoenwaelder, "Structure des informations de gestion, version 2 (SMIv2)", avril 1999. (STD0058)

[RFC2579] K. McCloghrie, D. Perkins, J. Schoenwaelder, "Conventions textuelles pour SMIv2", avril 1999. (STD0058)

[RFC2580] K. McCloghrie, D. Perkins, J. Schoenwaelder, "Déclarations de conformité pour SMIv2", avril 1999. (STD0058)

[RFC2741] M. Daniele et autres, "Protocole d'extensibilité d'agent (AgentX) version 1", janvier 2000. *(D.S.)*

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

[RFC2924] N. Brownlee, A. Blount, "Attributs de comptabilité et formats d'enregistrements", septembre 2000. *(Info.)*

[RFC2960] R. Stewart et autres, "Protocole de transmission de commandes de flux", octobre 2000. (*Obsolète, voir* RFC4960) *(P.S.)*

[RFC3430] J. Schoenwaelder, "Transposition de transport du protocole simple de gestion de réseau sur le protocole de contrôle de transmission", décembre 2002. *(Expérimentale)*

[RFC3965] K. Toyoda et autres, "Mode simple de télécopie utilisant la messagerie Internet", décembre 2004. *(D.S.)*

[RFC4556] L. Zhu, B. Tung, "Cryptographie à clé publique pour authentification initiale dans Kerberos (PKINIT)", juin 2006. *(P.S.)*

[18] Rose, M.T., "The Simple Book", Second Edition, Prentice Hall, Upper Saddle River, NJ, 1996.

[21] Johnson, H. T., Kaplan, R. S., "Relevance Lost: The Rise and Fall of Management Accounting", Harvard Business School Press, Boston, Massachusetts, 1987.

[22] Horngren, C. T., Foster, G., "Cost Accounting: A Managerial Emphasis". Prentice Hall, Englewood Cliffs, New Jersey, 1991.

[23] Kaplan, R. S., Atkinson, Anthony A., "Advanced Management Accounting", Prentice Hall, Englewood Cliffs, New Jersey, 1989.

[24] Cooper, R., Kaplan, R. S., "The Design of Cost Management Systems". Prentice Hall, Englewood Cliffs, New Jersey, 1991.

[44] Hornstein, K. and W. Hardaker, "A Kerberos Security Model for SNMPv3", Travail en cours.

[46] Network Management Research Group Web page, http://www.ibr.cs.tu-bs.de/projects/nmrg/

[48] Schoenwaelder, J., "SNMP Payload Compression", Travail en cours.

[49] Sprenkels, R., Martin-Flatin, J.,"Bulk Transfers of MIB Data", Simple Times, http://www.simple-times.org/pub/simple-times/issues/7-1.html , mars 1999.

[50] Thaler, D., "Get Subtree Retrieval MIB", Travail en cours.

9. Adresse des auteurs

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

Jari Arkko
Oy LM Ericsson Ab
02420 Jorvas
Finland
téléphone : +358 40 5079256
mél : Jari.Arkko@ericsson.com

David Harrington
Cabletron Systems Inc.
P.O.Box 5005
Rochester NH 03867-5005
USA
téléphone : +1 603 337 7357
mél : dbh@cabletron.com

10. Propriété intellectuelle

des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

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

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

11. Déclaration complète de droits de reproduction

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