Groupe de travail Réseau
Request for Comments : 2194
Catégorie : Information
septembre 1997
Traduction Claude Brière de L'Isle

B. Aboba, Microsoft
J. Lu, AimQuest Corp.
J. Alsop, i-Pass Alliance
J. Ding, Asiainfo
W. Wang, Merit Network, Inc.

Récapitulation des mises en œuvre d'itinérance

1. Statut de ce mémoire

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

2. Résumé

Le présent document passe en revue la conception et les fonctionnalités des mises en œuvre d'itinérance existantes. "Capacité d'itinérance" peut être en gros défini comme la capacité d'utiliser n'importe lequel des nombreux fournisseurs d'accès Internet (FAI) tout en conservant une relation formelle de client à fournisseur avec un seul d'entre eux. Des exemples de cas où la capacité d'itinérance peut être requise incluent des "confédérations" de FAI et la prise en charge de l'accès de réseau d'entreprise fournie par FAI.

3. Introduction

Un intérêt considérable s'est récemment manifesté pour un ensemble de caractéristiques qui entrent dans la catégorie générale de la "capacité d'itinérance" pour les utilisateurs de l'Internet. Les parties intéressées sont :

- Les fournisseurs d'accès Internet (FAI) régionaux qui fonctionnement dans un état ou région particulier, cherchant à combiner leurs efforts avec ceux d'autres fournisseurs régionaux pour offrir le service sur une plus large zone.
- Les FAI nationaux qui souhaitent combiner leurs opérations avec celles d'un ou plusieurs FAI dans d'autres pays pour offrir un service plus complet dans un groupe de pays ou sur un continent.
- Des entreprises désireuses d'offrir à leurs employés un paquetage complet des services d'accès sur une base mondiale. Ces services peuvent inclure l'accès à l'Internet ainsi qu'un accès sûr aux intranets d'entreprise via un réseau privé virtuel (VPN, *Virtual Private Network*) rendu possible par des protocoles de tunnelage tels que PPTP, L2F, ou L2TP.

Qu'est-il requis pour fournir une capacité d'itinérance ? La liste suivante est une première esquisse des exigences d'une itinérance réussie parmi un ensemble arbitraire de FAI :

La présentation du numéro de téléphone
L'échange du numéro de téléphone
La compilation de répertoires téléphoniques
La mise à jour des répertoires
La gestion de connexion
L'authentification
L'autorisation/configuration de NAS
L'allocation et l'acheminement d'adresse
La sécurité
La comptabilité

Dans le présent document, on passe en revue les mises en œuvre d'itinérance existantes, en décrivant leurs fonctionnalités dans ce cadre. En plus des mises en œuvre d'itinérance officielles, on examinera aussi des mises en œuvre qui, bien que ne satisfaisant pas à la définition stricte de l'itinérance, comportent plusieurs des éléments du problème. Ces mises en œuvre entrent normalement dans la catégorie des réseaux à utilisation partagée ou dans celle des réseaux commutés non IP.

3.1 Terminologie

Le présent document utilise fréquemment les termes suivants :

FAI de rattachement : c'est le fournisseur d'accès Internet avec lequel l'usager entretient une relation comptable.

FAI local : c'est le fournisseur d'accès Internet d'où appelle l'usager afin d'obtenir l'accès. Lorsque l'itinérance est mise en œuvre, le FAI local peut être différent du FAI de rattachement.

répertoire téléphonique : c'est une base de données ou un document qui contient les données relatives à l'accès commuté, y compris les numéros de téléphone et tous leurs attributs associés.

réseau à utilisation partagée ; c'est un réseau commuté IP dont l'utilisation est partagée par deux organisations ou plus. Les réseaux à utilisation partagée mettent normalement en œuvre l'authentification et la comptabilité réparties pour faciliter les relations entre les participants. Comme ces facilités sont aussi nécessaires pour la mise en œuvre de l'itinérance, la mise en œuvre de l'utilisation partagée est fréquemment une première étape du développement des capacités d'itinérance. En fait, une des façon qu'a un fournisseur d'offrir un service d'itinérance est de conclure des accords d'utilisation partagée avec plusieurs réseaux. Cependant, à ce jour, la capacité de réaliser cela a été entravé par le manque d'interopérabilité entre les mises en œuvre d'utilisation partagée.

réseau commuté non IP : c'est un réseau commuté qui fournit un accès d'utilisateur aux systèmes membres via des protocoles autres que IP. Ces réseaux peuvent mettre en œuvre des facilités de synchronisation de répertoire téléphonique, afin de fournir aux systèmes, administrateurs et utilisateurs une liste à jour des systèmes participants. Des exemples de réseaux commutés non IP qui prennent en charge la synchronisation des répertoires téléphoniques incluent FidoNet et WWIVnet.

4. Global Reach Internet Consortium (GRIC)

Conduits par un développeur de technologie Internet américain, AimQuest Corporation, dix fournisseurs d'accès Internet (FAI) des USA, d'Australie, Chine, Japon, Hong Kong, Malaisie, Singapour, Taiwan, et Thaïlande ont formé le consortium de connexion mondiale à l'Internet (GRIC, *Global Reach Internet Connection*) en mai 1996. Les objectifs du GRIC sont de faciliter la mise en œuvre d'un service mondial d'itinérance et de coordonner la facturation et les règlements entre les membres. Le fonctionnement commercial a commencé en décembre 1996, et le GRIC s'est étendu à plus de cent FAI et compagnies téléphoniques majeurs du monde entier, incluant NETCOM, des USA, KDD et Mitsubishi, du Japon, iStar du Canada, Easynet au Royaume Uni, Connect.com en Australie, Iprolink de Suisse, Singapore Telecom, Chunghwa Telecom de Taïwan; et Telekom Malaysia. Des informations sur le GRIC sont disponibles à http://www.gric.net/.

En mettant en œuvre leur service d'itinérance, les membres du GRIC ont choisi le logiciel développé par AimQuest. La mise en œuvre d'itinérance de AimQuest Corporation comporte les composants majeurs suivants : le serveur d'authentification AimTraveler (AAS, *AimTraveler Authentication Server*), le serveur d'acheminement AimTraveler (ARS, *AimTraveler Routing Server*) et le système de gestion Internet AimTraveler (AIMS, *AimQuest Internet Management System*), logiciel conçu pour faciliter le processus de facturation. Les informations sur la mise en œuvre d'itinérance de AimQuest sont disponibles à http://www.aimquest.com/ .

Le serveur d'authentification AimTraveler (AAS) fonctionne sur le site de chaque FAI membre, et traite les demandes d'authentification entrantes venant des appareils de NAS et des autres AAS. Le serveur d'acheminement AimTraveler (ARS) peut fonctionner n'importe où. Un seul serveur d'acheminement peut être utilisé lorsque on désire un acheminement centralisé, ou plusieurs serveurs d'acheminement peuvent fonctionner afin d'augmenter la vitesse et la fiabilité ou pour servir de passerelles pour des réseaux de partenaires particulièrement importants.

La première version du logiciel AimTraveler, déployé par AimQuest en mai 1996, prenait en charge l'authentification directe entre les membres du consortium d'itinérance, mais avec la croissance du GRIC, la gestion des relations entre les serveurs d'authentification devenait problématique. En août 1996, AimQuest a commencé à développer le serveur d'acheminement AimTraveler (ARS) afin d'améliorer l'adaptabilité.

Le serveur d'acheminement se compose de deux éléments : le serveur central de comptabilité et le serveur central d'acheminement. Le serveur central de comptabilité collecte toutes les données de comptabilité d'itinérance pour les règlements. Le serveur central d'acheminement gère et conserve les informations sur les serveurs d'authentification du consortium d'itinérance. Ajouter, supprimer, ou mettre à jour les informations du serveur d'authentification de FAI (par exemple, ajouter un nouveau FAI membre) peut se faire en éditant un fichier de configuration sur le serveur central d'acheminement. Les fichiers de configuration des serveurs d'authentification AimTraveler n'ont pas besoin d'être modifiés.

Les serveurs d'authentification et d'acheminement AimTraveler sont disponibles pour diverses plates-formes UNIX. Les versions pour Windows NT sont en cours de développement. Le serveur d'authentification AimTraveler prend en charge le fichier de mots de passe UNIX aussi bien que Kerberos.

Le système de gestion Internet AimQuest (AIMS) est conçu pour de gros FAI qui ont besoin d'un système de gestion centralisé

pour toutes les opérations du FAI, incluant les ventes, le marquage des problèmes, le service, et la facturation. AIMS produit des rapports d'état des transactions, et comporte un module de règlement pour produire les rapports de facturation/règlements pour les membres du consortium d'itinérance. Sur la base de ces rapports, les fournisseurs facturent leurs consommateurs itinérants/FAI, et payent/règlent la balance d'itinérance entre les fournisseurs. AIMS fonctionne actuellement sur Sun/Solaris/Oracle. Une version pour Windows NT et SQL Server est attendue à la fin 1996.

4.1 Présentation du numéro de téléphone

Il y a actuellement deux méthodes principales pour que les utilisateurs du GRIC puissent découvrir les numéros de téléphone disponibles : un annuaire fondé sur la Toile fourni par le secrétariat du GRIC, et un client de répertoire téléphonique GRIC sur le PC d'utilisateur avec une capacité de numérotation.

4.1.1 Annuaire fondé sur la Toile

Un annuaire des numéros de téléphone du GRIC est disponible sur la page d'accueil du GRIC, http://www.gric.com/. La liste des numéros est rangée par pays et par fournisseur. Pour chaque fournisseur dans un pays, cet annuaire, fourni sous la forme d'un tableau, offre les informations suivantes :

Adresse, téléphone et télécopie du fournisseur
Numéro de téléphone du service client
Nom de domaine du fournisseur
Serveur principal de noms de domaine
Serveur secondaire de noms de domaine
Adresse IP de numérotation
Serveur de nouvelles
Page de la Toile
Numéros de téléphone POP (c'est-à-dire, 1-408-366-9000)
Localisations POP (c'est-à-dire, Berkeley)
Adresses des mandataires
Configuration de numérotation

Pour découvrir les numéros de téléphone en utilisant l'annuaire fondé sur la Toile, il est prévu que les usagers seront en ligne, et vont naviguer jusqu'au pays et fournisseur approprié. Ils cherchent alors le numéro et l'insèrent dans le numéroteur AimQuest Ranger.

4.1.2 Client d'annuaire téléphonique GRIC

Le logiciel de client d'annuaire téléphonique GRIC fournit la présentation de l'annuaire téléphonique ainsi que la mise à jour automatique des numéros de téléphone. L'annuaire GRIC comporte une liste des codes de pays, état, ville et zone urbaine, ainsi que des informations détaillées sur le fournisseur, incluant le numéro de téléphone du service client, et les informations de configuration du serveur Internet. L'annuaire, développé avec Java, est disponible sur le site de la Toile de AimQuest et peut être téléchargé à : http://www.aimquest.com/dialer.html

4.2 Échange des numéros de téléphone

Les membres du GRIC soumettent les informations sur eux-mêmes et sur leurs POP au secrétariat du GRIC, qui est géré par AimQuest. Le secrétariat du GRIC compile alors un nouvel annuaire et en fournit les mises à jour au FTP GRIC et aux serveurs de la Toile.

Les usagers du GRIC téléchargent les numéros de téléphone en format de fichier Windows .ini ou en HTML.

4.3 Compilation d'annuaire

Les annuaires GRIC sont compilés manuellement, et représentent un enchaînement de numéros disponibles de tous les membres du consortium d'itinérance, sans application de politique. Lorsque de nouveaux POP viennent en ligne, les numéros sont transmis au GRIC, qui les ajoute aux serveurs d'annuaire.

4.4 Mise à jour d'annuaire

Les numéros de téléphone dans le client d'annuaire GRIC sont mis à jour automatiquement dès la connexion. Le serveur AimTraveler inclut un répertoire d'adresses qui contient les numéros de téléphone de tous les membres du consortium d'itinérance.

4.5 Gestion de connexion

Le logiciel AimTraveler prend en charge SLIP et PPP, ainsi que l'authentification PAP et CHAP.

4.6 Authentification

Le GRIC met en œuvre l'authentification répartie, en utilisant l'adresse de messagerie électronique de l'usager comme identifiant d'utilisateur (c'est-à-dire, "liu@Aimnet.com") présenté à l'appareil de NAS distant.

Après l'échange d'authentification PPP initial, les informations d'identifiant d'utilisateur, de domaine, et de mot de passe (ou dans le cas de CHAP, le défi et la réponse) sont alors passés par le NAS au serveur d'authentification AimTraveler qui prend en charge les deux protocoles TACACS+ et RADIUS.

Si la demande d'authentification provient d'une connexion d'un consommateur régulier, une authentification normale d'identifiant d'utilisateur et de mot de passe est effectuée. Si l'usager qui demande d'authentification est un "itinérant", (il a un identifiant d'utilisateur avec un @ et un nom de domaine) le serveur d'authentification envoie une demande au serveur d'acheminement le plus proche. Lorsque le serveur d'acheminement AimTraveler reçoit la demande d'authentification, il authentifie d'abord l'AAS qui envoie la demande, et si cela réussit, il vérifie son tableau de serveur d'authentification. Si il est capable de faire correspondre le domaine de l'usager avec celui d'un "FAI de rattachement", les informations d'acheminement du serveur d'authentification du FAI de rattachement sont alors renvoyées au serveur d'authentification du FAI local. Sur la base des informations reçues du serveur d'acheminement, l'AAS fait une demande d'authentification à l'AAS du FAI de rattachement de l'usager pour la vérification de l'identifiant d'utilisateur et du mot de passe.

Si l'usager est un utilisateur valide, le serveur d'authentification du FAI de rattachement renvoie un message "permission accordée" au serveur d'authentification du FAI local. Le serveur d'authentification du FAI local demande alors au NAS d'allouer à l'usager une adresse IP dynamique à partir de son réservoir d'adresses. Si le nom d'utilisateur ou le mot de passe est incorrect, l'AAS du FAI de rattachement va envoyer un message de rejet à l'AAS du FAI local, et l'usager sera abandonné par le NAS.

Si plusieurs serveurs d'acheminement sont installés, et si la demande au premier serveur d'acheminement ne débouche pas sur une correspondance, l'interrogation est transmise au routeur c'acheminement suivant. Les interrogations au serveur sont mises en antémémoire sur les serveurs d'acheminement, ce qui améliore la vitesse pour les interrogations répétées. L'antémémoire est conservée jusqu'à ce qu'une entrée de tableau de serveur d'acheminement soit mise à jour ou supprimée. La mise à jour ou la suppression résulte en un message à tous les serveurs d'acheminement voisins pour qu'ils suppriment leurs antémémoires.

Le serveur d'authentification local reçoit aussi les données de comptabilité provenant du NAS. Si les données sont pour une connexion d'un abonné régulier, les données ont inscrites dans le fichier de journal d'AAS du FAI local. Si les données sont pour un "itinérant", les données sont inscrites en trois endroits : le fichier journal d'AAS du FAI local, le fichier journal d'AAS du FAI de rattachement, et le fichier journal de l'ARS.

Si le serveur d'authentification du FAI local a la mise en antémémoire activée, il va alors mettre en antémémoire les informations sur les configurations de serveur d'authentification de FAI de rattachement envoyées par le serveur d'acheminement. Cela signifie que si le même domaine est demandé à nouveau, le serveur d'authentification local n'aura pas besoin d'interroger à nouveau le serveur d'acheminement. L'antémémoire locale est purgée lorsque le serveur d'authentification local reçoit un message de mise à jour de la part du serveur d'acheminement ou d'un gestionnaire du système.

4.7 Configuration/autorisation de NAS

AimTraveler possède deux composants, un client (AAS) et un serveur (ARS).

Le client AimTraveler agit comme serveur d'authentification commuté PPP. Lorsque il détecte un signe '@' dans le champ

Identifiant d'utilisateur, il interroge le serveur AimTraverler pour avoir les informations d'acheminement, puis transmet la demande d'authentification au serveur d'authentification de rattachement de l'usager. Le serveur AimTraveler, qui est un serveur d'acheminement centralisé, contient le nom de domaine du FAI autorisé, les serveurs d'authentification et d'autres informations.

AimTraveler prend actuellement en charge RADIUS et TACACS+, et pourrait être étendu de façon à prendre en charge d'autres protocoles d'authentification. Il reçoit aussi tous les enregistrements de comptabilité, qui sont ensuite utilisés comme données d'entrée pour la facturation.

Comme les appareils de NAS des FAI peuvent avoir des configurations différentes, les attributs retournés par l'AAS du FAI de rattachement sont éliminés.

4.8 Allocation d'adresse et acheminement

Toutes les adresses dans GRIC sont allouées de façon dynamique à partir du réservoir d'adresses du FAI local. Des adresses statiques et des connexions de LAN acheminées seront considérées à l'avenir, lorsque le GRIC offrira un service d'itinérance d'entreprise, avec la mise en œuvre de protocoles de tunnelage

4.9 Sécurité

Le mot de passe de l'usager est haché avec MD5 avant d'être envoyé de l'AAS du FAI local à l'AAS du FAI de rattachement. Une clé de chiffrement est partagée entre l'AAS et l'ARS. La version actuelle d'AAS AimTraveler ne prend pas en charge les cartes à jetons ni les protocoles de tunnelage.

4.10 Comptabilité

Le logiciel de serveur d'authentification AimTraveler (AAS, *AimTraveler Authentication Server*) peut agir comme serveur de comptabilité RADIUS ou TACACS+. Quand les informations comptables sont reçues du NAS, le serveur AAS local envoie les données comptables (nom d'utilisateur, nom de domaine, heure de connexion) au serveur centra l de comptabilité (qui fait partie de l'ARS) et à l'AAS du FAI de rattachement. Dans le cas de GRIC, le serveur de comptabilité central est géré par AimQuest.

Les données envoyées au serveur de comptabilité central et au FAI de rattachement sont identiques excepté pour la forme de l'identifiant d'utilisateur et l'horodatage. Pour un voyageur dont le FAI de rattachement est aux USA, mais qui voyage au Japon, l'AAS du FAI local (japonais) va recevoir un enregistrement comptable dont l'horodatage va porter l'heure du Japon, tandis que l'AAS du FAI de rattachement (US) va recevoir un enregistrement comptable dont l'horodatage aura l'heure de la zone horaire US appropriée.

Les données comptables comportent deux nouveaux attributs pour le rapport de règlement :

Attribut	**Numéro**	**Type**
Identifiant de serveur d'itinérance	101	chaîne
Identifiant de FAI	102	chaîne

L'attribut Identifiant de serveur d'itinérance identifie l'AAS qui envoie la demande d'authentification. L'attribut Identifiant de FAI identifie le FAI local. En utilisant ces informations, le FAI de rattachement peut retracer les activités d'itinérance de ses usagers (où ses usagers se connectent).

Le serveur AimTraveler qui fonctionnent chez AimQuest garde un enregistrement de toutes les transactions d'itinérance, qui sont utilisées comme entrées pour le processus de facturation et de règlement. À la fin de chaque mois, AimQuest fournit un résumé des transactions d'itinérance aux membres du GRIC en utilisant AIMS. Le logiciel AIMS est configurable de telle sorte qu'il prenne en compte les règles comptables sur lesquelles les membres du GRIC se sont mis d'accord.

5. Mise en œuvre i-Pass

5.1 Généralités

i-Pass Alliance Inc., installé à Mountain View, Californie, a développé et fait fonctionner un service commercial d'authentification et de compensation de règlements qui fournit une itinérance mondiale entre les fournisseurs d'accès Internet. Le service est pleinement opérationnel.

i-Pass Alliance Inc. a des bureaux à Toronto, Singapour, et Londres. Des informations supplémentaires sur i-Pass peuvent être obtenues à http://www.ipass.com.

Le réseau i-Pass consiste en un certain nombre de serveurs qui fournissent des services d'authentification en temps réel aux FAI partenaires. Les demandes d'authentification et les enregistrements comptables pour les utilisateurs de l'itinérance sont chiffrés et envoyés à un serveur i-Pass où ils sont enregistrés, et ensuite transmis à un FAI de rattachement pour authentification et/ou enregistrement.

Périodiquement, i-Pass récapitule tous les enregistrements comptables, génère des facturations, et agit comme un point unique de collecte et de réalisation des payements.

i-Pass ne fournit ses services qu'aux FAI et à ses partenaires. Il ne tente pas d'établir de relations d'affaires avec les clients individuels d'un FAI.

5.2 Base de données de points d'accès

i-Pass tient une liste des points d'accès d'itinérance dans une base de données Oracle. Cette liste est consultable par région géographique avec un navigateur de la Toile, et peut être téléchargée dans sa totalité avec FTP. Les informations mémorisées pour chaque point d'accès comportent :

- Nom du fournisseur de service
- Pays
- État ou province
- Ville ou région
- Numéro de téléphone
- Numéro de téléphone du soutien technique
- Types de service disponible
- Informations techniques (fichier d'aide)
- Information sur la tarification des services

La base de données des points d'accès est tenue par le personnel de i-Pass, sur la base des entrées des partenaires de i-Pass.

5.3 Présentation des numéros de téléphone

i-Pass a développé une application Windows avec une interface simple de pointage et clic appelée le "i-Pass Dial Wizard" *(assistant de connexion i-Pass)* qui aide les utilisateurs finaux à choisir un point d'accès Internet local et s'y connecter.

L'assistant de connexion permet aux utilisateurs de choisir d'abord le pays dans lequel ils se déplacent. Une liste d'états, provinces, ou autres régions dans le pays sélectionné est alors présentée. Finalement, une liste de points d'accès au sein de l'état ou province est présentée. L'assistant de connexion affiche le nom de la ville, le numéro de téléphone du modem, et les informations tarifaires pour chaque point d'accès dans l'état ou la région.

Lorsque l'utilisateur choisit le point d'accès désiré, une icône Windows 95 "DialUp Networking" est créée pour ce point d'accès. Si il y a un descriptif de connexion associé à ce point d'accès, l'outil DialUp Scripting est automatiquement configuré. Cela signifie que l'utilisateur final n'a jamais à configurer les exigences de descriptif de connexion.

L'assistant de connexion a un répertoire téléphonique incorporé qui contient tous les points d'accès i-Pass. Le répertoire peut être automatiquement rafraîchi à partir d'un fichier original conservé sur le site de la Toile des FAI.

L'assistant de connexion est fourni gratuitement aux partenaires de i-Pass. i-Pass fournit aussi le trousseau de personnalisation d'assistant de connexion i-Pass qui permet aux FAI partenaires de générer des versions personnalisées de l'assistant de connexion avec leur propre enseigne, etc.

5.4 Authentification

Trois entités sont impliquées dans le traitement d'une demande d'authentification :

FAI local : Chez le FAI local, le serveur d'authentification est modifié pour reconnaître les identifiants d'utilisateur de la forme nom-d'utilisateur@domaine-d'authentification comme étant des demandes d'authentification distantes. Ces demandes sont transmises à un serveur i-Pass.

Serveur i-Pass : Le serveur i-Pass reçoit la demande d'authentification, l'enregistre, et la transmet au FAI de rattachement identifié par la portion domaine-d'authentification de l'identifiant d'utilisateur.

FAI de rattachement : Le FAI de rattachement reçoit la demande d'authentification, effectue l'authentification en utilisant sa méthode d'authentification normale, et retourne une réponse OUI/NON au serveur i-Pass, qui à son tour transmet la réponse au FAI d'origine.

i-Pass fournit des composants logiciels qui fonctionnent sur les serveurs d'authentification des FAI locaux et de rattachement. Chaque FAI membre doit intégrer ces composants à sa propre méthode d'authentification. Pour simplifier cette tâche, i-Pass a développé des interfaces "d'ajout" pour les méthodes d'authentification les plus courantes. Au moment de la présente rédaction, les interfaces suivantes sont prises en charge :

Livingston RADIUS
Ascend RADIUS
Merit RADIUS
TACACS+
Xylogics erpcd (versions 10 et 11)

Une interface générique est aussi fournie pour authentifier sur la base du fichier de mots de passe UNIX standard. Ceci est destiné à être un point de départ pour les FAI qui utilisent des méthodes d'authentification autres que celles citées ci-dessus.

L'effort d'intégration de logiciel pour un FAI normal est de l'ordre de deux à cinq hommes/jours en incluant les essais. Les plateformes actuellement prises en charge sont :

Solaris 2.5 (Sparc).LI
Solaris 2.5 (Intel)
BSDI
Digital Unix
Linux
FreeBSD
HP/UX

Les FAI peuvent choisir de fournir l'authentification pour leurs utilisateurs finaux en itinérance ailleurs, mais pas de fournir des points d'accès au réseau i-Pass. Dans ce cas, l'effort d'intégration logicielle est largement réduit et peut descendre à 1/2 homme/jour.

5.5 Comptabilité

Les transactions comptables sont traitées de la même façon que les demandes d'authentification. En plus d'être enregistrées sur les serveurs i-Pass, les transactions comptables sont envoyées en temps réel au FAI de rattachement. Ceci est destiné à permettre aux FAI de mettre à jour en temps réel les informations de limite de crédit de l'usager (dans la mesure où cette capacité est prise en charge par les systèmes de comptabilité et de facturation).

Le règlement est effectué chaque mois. Le processus de règlement implique de calculer les coûts associés à chaque session individuelle, et de les agréger pour chaque FAI. Un montant net est alors calculé qui est soit dû par i-Pass au FAI, soit dû du FAI à i-Pass, selon le schéma d'utilisation réel.

Les rapports suivants sont fournis aux FAI membres :
Une déclaration mensuelle récapitulant les utilisations, les services fournis, et tous les ajustements ainsi que le montant net dû.
Un rapport détaillé des appels montrant les usages de l'itinérance par les clients du FAI.
Un rapport du service fourni montrant l'usage détaillé des facilités du FAI par les utilisateurs distants.

Ces rapports sont générés comme documents ASCII et sont distribués aux partenaires i-Pass sous forme électronique, soit par

messagerie, soit à partir d'une zone sécurisée du site de la Toile de i-Pass. Un résultat imprimé est disponible sur demande.

Le rapport détaillé des appels est aussi généré en fichier ASCII qui peut être importé dans la base de données de facturation des FAI. Le rapport détaillé des appels sera normalement utilisé par le FAI pour générer la facturation de l'utilisateur final pour l'utilisation de l'itinérance.

5.6 Sécurité

Toutes les transactions entre les FAI et les serveurs i-Pass sont chiffrées en utilisant le protocole SSL. Les certificats de clé publique sont vérifiés chez le client et chez le serveur. i-Pass produit ces certificats et agit comme autorité de certification.

Les transactions sont aussi vérifiées sur la base d'un certain nombre d'autres critères tels que l'adresse IP de source.

5.7 Fonctionnement

i-Pass fonctionne sur plusieurs sites de serveur d'authentification. Chaque site consiste en deux systèmes de serveurs redondants situés dans des enceintes sécurisées et "proches" du cœur de réseau Internet. Les sites de serveur d'authentification sont répartis géographiquement pour minimiser les possibilités d'échec dues à des désastres naturels, etc.

i-Pass tient un centre des opérations de réseau à Mountain View qui fonctionne jour et nuit. Ses fonctions incluent la surveillance des serveurs d'authentification i-Pass, la surveillance des serveurs d'authentification situés dans les locaux des partenaires, et le traitement des rapports de problèmes.

6. Mise en œuvre de ChinaNet

ChinaNet, propriété de China Telecom, est le plus grand cœur de réseau Internet de Chine. Construit par Asiainfo, une société d'intégration de système de Dallas, il a 31 nœuds de cœur de réseau dans 31 capitales provinciales de Chine. Chaque province construit son propre réseau provincial, a ses propres serveurs de commutation, et administre sa propre base d'utilisateurs.

Afin de permettre aux usagers de ChinaNet d'accéder aux nœuds en dehors de leur province lorsque ils sont en déplacement, un système national d'itinérance a été mis en œuvre. Le système d'itinérance a été développé par AsiaInfo, et il se fonde sur le protocole RADIUS.

6.1 Présentation des numéros de téléphone

Comme China Telecom utilise un numéro de téléphone (163) pour l'accès Internet national, la plupart des villes ont le même numéro d'accès Internet. Donc, un répertoire téléphonique n'est actuellement pas nécessaire pour la mise en œuvre de ChinaNet. Un répertoire téléphonique fondé sur la Toile sera ajouté dans une future livraison du logiciel afin de prendre en charge des numéros nationaux de FAI/CSP *(Content Service Provider, fournisseur de service de contenu)* et les adresses de serveur HTTP.

6.2 Gestion de connexion

Le client et serveur actuel d'itinérance prend en charge PPP et SLIP.

6.3 Allocation d'adresse et acheminement

ChinaNet ne prend en charge que l'allocation dynamique d'adresse IP pour les utilisateurs d'itinérance. De plus, les adresses statiques sont prises en charge pour les usagers qui s'authentifient au sein de leur province de rattachement.

6.4 Authentification

Lorsque l'usager accède à un NAS local, il fournit son identifiant d'utilisateur soit comme "nom_d'usager" soit comme "nom_d'usager@domaine". Le NAS va passer l'identifiant d'utilisateur et le mot de passe au mandataire/serveur RADIUS. Si la notation "nom_d'usager" est utilisée, le mandataire/serveur Radius supposera que l'usager est en local et va traiter en

conséquence l'authentification en local. Si c'est "nom_d'usager@domaine" qui est utilisé, le mandataire/serveur RADIUS va la traiter comme une demande d'itinérance.

Lorsque le mandataire/serveur RADIUS traite une demande provenant d'un usager en itinérance, il va d'abord vérifier dans l'antémémoire si les informations sur l'utilisateur y sont déjà mémorisées. Si c'est le cas, le mandataire/serveur RADIUS fait l'authentification locale en conséquence. Si il ne trouve pas les informations d'utilisateur dans son antémémoire, il va agir comme un mandataire, transmettant la demande d'authentification au serveur RADIUS de rattachement. Lorsque le serveur RADIUS de rattachement répond, le serveur local transmet la réponse au NAS. Si l'usager est authentifié par le serveur de rattachement, le mandataire RADIUS local va mettre en antémémoire les informations d'utilisateur pour une certaine période (3 jours par défaut).

La mise en antémémoire est utilisée pour éviter d'avoir fréquemment affaire au mandatement des demandes et réponses entre le mandataire RADIUS local et le serveur RADIUS de rattachement. Lorsque le serveur RADIUS de rattachement renvoie une réponse d'authentification valide, le mandataire/serveur RADIUS local va mettre en antémémoire les informations d'utilisateur pendant un certain temps (3 jours par défaut). Lorsque l'utilisateur s'authentifie ensuite directement auprès du serveur RADIUS de rattachement, celui-ci va envoyer une demande aux serveurs locaux pour purger les informations de l'utilisateur de l'antémémoire.

6.4.1 Hiérarchie étendue

Dans certaines provinces, l'administration des télécommunications locale (FAI provincial) subdélègue le contrôle aux nœuds d'accès d'arrondissement, créant un autre niveau de hiérarchie. Ceci est fait pour améliorer l'adaptabilité et pour éviter que les bases de données des FAI provinciaux ne deviennent trop grosses. Dans la mise en œuvre actuelle, chaque FAI provincial entretient son propre serveur central RADIUS, qui comporte des informations sur tous les utilisateurs de la province, tandis que les nœuds d'arrondissement entretiennent les serveurs RADIUS répartis. Pour les demandes d'itinérance intra-province, le mandataire/serveur RADIUS local va transmettre directement la demande au serveur RADIUS de rattachement.

Cependant, pour les demandes d'itinérance inter-provinces, le serveur RADIUS local ne transmet pas la demande directement au serveur RADIUS de rattachement. La demande est plutôt transmise au serveur central provincial RADIUS pour la province de rattachement. Cette mise en œuvre ne convient que lorsque les FAI de niveau arrondissement ne voient pas d'objection à combiner et partager leurs informations d'utilisateurs. Dans cette instance, ceci est acceptable, car tous les FAI de niveau arrondissement font partie de China Telecom. Dans une livraison future, cette hiérarchie multi couches sera mise en œuvre en utilisant un mandataire RADIUS multi couches, d'une manière assez proche de celle du DNS.

6.5 Sécurité

Le chiffrement est utilisé entre le mandataire/serveur RADIUS local et le serveur RADIUS de rattachement. Le chiffrement à clé publique/privée sera pris en charge dans la prochaine version. La prise en charge du tunnelage IP et des cartes à jeton est envisagée.

6.6 Comptabilité

Les information comptables sont transférées entre le mandataire/serveur RADIUS local de comptabilité et le serveur de comptabilité RADIUS de rattachement. Chaque jour, chaque nœud envoie un enregistrement récapitulatif des informations comptables à un serveur central afin de prendre en charge un règlement au niveau national. Le serveur central est géré par le bureau central des communications de données de China Telecom. Chaque mois, le serveur central envoie la facture aux FAI provinciaux.

6.7 Itinérance inter-FAI/CSP

ChinaNet prend en charge l'itinérance aussi bien de FAI que de CSP sur son système. Par exemple, Shanghai Online, un service de contenu commercial fondé sur la Toile, utilise RADIUS pour l'authentification des utilisateurs de ChinaNet qui n'ont pas de compte Shanghai Online. Pour prendre cela en charge, les serveurs de Shanghai Online fonctionnent comme un client RADIUS par rapport au serveur RADIUS de rattachement. Lorsque les usagers accèdent à un document protégé sur le serveur HTTP, ils sont invités à envoyer un nom d'utilisateur/mot de passe pour l'authentification. L'usager répond alors par son identifiant d'utilisateur dans une notation "nom-d'usager@domaine".

Un descriptif CGI sur le serveur HTTP agit alors comme un client d'authentification RADIUS, envoyant la demande au

serveur RADIUS de rattachement. Après la réponse du serveur RADIUS de rattachement, le descriptif CGI passe les informations à l'agent local d'authentification. À partir de ce point, tout est pris en charge par le mécanisme local d'authentification de la Toile.

7. Mise en œuvre Microsoft

La mise en œuvre d'itinérance de Microsoft a été développée à l'origine pour prendre en charge le réseau Microsoft (MSN, Microsoft Network) qui offre maintenant l'accès Internet dans sept pays : USA, Canada, France, Allemagne, Royaume-Uni, Japon, et Australie. Dans chacun de ces pays, le service est offert en coopération avec des partenaires d'accès. Comme les usagers sont capables de se connecter au réseau du partenaire d'accès tout en conservant une relation de client à fournisseur avec MSN, cette mise en œuvre correspond à la définition de l'itinérance donnée dans le présent document.

7.1 Généralités sur la mise en œuvre

La première version du logiciel Microsoft d'itinérance a été déployée par les partenaires MSN en avril 1996. Cette version incluait un outil de gestion de répertoire téléphonique fonctionnant sous Windows 95, ainsi qu'une mise en œuvre de serveur/mandataire RADIUS fonctionnant sous Windows NT ; TACACS+ n'est pas pris en charge actuellement. Des composants supplémentaires actuellement en développement incluent un client de gestionnaire de connexion pour Windows 95 ainsi qu'un serveur de répertoire téléphonique fondé sur HTTP pour Windows NT. L'outil de gestionnaire de répertoire téléphonique est aussi mis à niveau pour fournir une compilation de répertoire téléphonique plus automatisée.

7.2 Présentation des numéros de téléphone

Le gestionnaire de connexion est chargé de la présentation et la mise à jour des numéros de téléphone, ainsi que de la numérotation et l'établissement des connexions. Pour choisir les numéros de téléphone, il est demandé aux utilisateurs de choisir le pays et l'état/région désirés. Les numéros de téléphone sont alors présentés dans la zone choisie. Les premiers numéros sont ceux du fournisseur de services de l'utilisateur qui correspond au type de service (analogique, RNIS, analogique & numérique), pays et région/état choisi. Les autres numéros (choisis en cliquant sur le bouton Plus) sont ceux des autres fournisseurs de service qui ont un accord d'itinérance avec le fournisseur de service de l'usager.

7.2.1 Données de coût

Les données de coût ne sont pas présentées aux usagers avec les numéros de téléphone. Cependant, de telles informations peuvent être rendues disponibles par d'autres moyens, tels qu'une page de la Toile.

7.2.2 Format d'annuaire par défaut

Le gestionnaire de connexion comporte la capacité de personnaliser le format du répertoire téléphonique, et on s'attend à ce que de nombreux FAI utilisent cette capacité. Cependant, pour ceux qui souhaitent l'utiliser "en l'état" un format de répertoire téléphonique par défaut est fourni. Le répertoire téléphonique par défaut comporte plusieurs fichiers, parmi lesquels :

Le profil de service
Le répertoire téléphonique
Le fichier des régions

Le profil de service fournit des informations sur un certain service, qui peut être un fournisseur d'accès Internet isolé, ou peut représenter un consortium d'itinérance. Le profil de service, qui est en format de fichier .ini, se compose des informations suivantes :

Le nom du service
Le nom de fichier de la grande icône du service
Le nom de fichier de la petite icône du service
La description du service
Le nom de fichier du répertoire téléphonique du service
Le numéro de version du répertoire téléphonique du service
Le fichier des régions du service
L'URL du serveur du répertoire téléphonique du service
Le préfixe utilisé par le service (c'est-à-dire, "MSN/aboba")
Le suffixe ou le domaine utilisé par le service (c'est-à-dire, "aboba@msn.com")
Si le nom d'utilisateur est facultatif pour le service
Si le mot de passe est facultatif pour le service
La longueur maximum du nom d'utilisateur pour le service
La longueur maximum du mot de passe pour le service

Les informations sur le traitement du mot de passe du service (minuscules, casse mixte, etc.)
Nombre de renumérotations pour ce service
Délai entre les renumérotations pour ce service
Références aux autres fournisseurs de service qui ont des accords d'itinérance
Les noms de fichier de profil de service pour chacune des références
Gabarit et filtres de correspondance de répertoire téléphonique pour chacune des références (chiffres de 32 bits qui sont appliqués aux fanions de capacité dans le répertoire téléphonique)
La configuration des propriétés de la connexion commutée (c'est le nom de l'identifiant de connexion DUN)

Le fichier de répertoire téléphonique est un fichier ASCII délimité par des virgules contenant les données suivantes :
Nombre unique qui identifie un enregistrement particulier (Indice)
Identifiant de pays
Indice à base zéro dans le fichier des régions
Ville
Code de zone
Numéro de téléphone local
Vitesse minimum
Vitesse maximum
Fanions de capacité :
Bit 0 : 0 = payant, 1 = gratuit
Bit 1 : 0 = X25, 1 = IP
Bit 2 : 0 = analogique, 1 = analogique refusé
Bit 3 : 0 = RNIS refusé , 1 = RNIS
Bit 4 : 0
Bit 5 : 0
Bit 6 : 0 = pas d'accès Internet, 1 = accès Internet
Bit 7 : 0 = pas d'accès signup, 1 = accès signup
Bit 8-31 : réservé
Le nom de fichier du fichier de réseau commuté (qu'on appelle normalement le descriptif associé au numéro)

Voici un exemple de fichier de répertoire téléphonique :

```
65031,1,1,Aniston,205,5551212,2400,2400,1,0,monfichier
200255,1,1,Auburn/Opelika,334,5551212,9600,28800,0,10,
200133,1,1,Birmingham,205,5551212,9600,28800,0,10,
130,1,1,Birmingham,205,3275411,9600,14400,9,0,tonfichier
65034,1,1,Birmingham,205,3285719,9600,14400,1,0,monfichier
```

7.2.3 Attributs supplémentaires

Comme décrit précédemment, il est vraisemblable que certains FAI vont exiger des attributs de numéro de téléphone ou d'informations de fournisseur supplémentaires, au delà de ceux qui sont pris en charge dans le format par défaut de répertoire téléphonique. Les attributs intéressants peuvent varier selon les fournisseurs, ou peuvent se faire jour par suite de l'introduction de nouvelles technologies. Il en résulte que l'ensemble des attributs de numéro de téléphone va vraisemblablement évoluer au fil du temps, et l'extensibilité du format du répertoire téléphonique est très souhaitable.

Par exemple, en plus des attributs fournis dans le répertoire téléphonique par défaut, les attributs supplémentaires suivants ont été demandés par les consommateurs :
Fanion de prise en charge de la diffusion groupée
Fanion externe/interne (pour différencier l'affichage selon la boîte "interne" ou la liste des "autres")
Priorité (pour le contrôle de l'ordre de présentation)
Capacités de protocole de modem (V.34, V.32bis, etc.)
Capacités de protocole RNIS (V.110, V.120, etc.)
Fanion Pas de mot de passe (pour les numéros qui utilisent la facturation fondée sur le téléphone)
Nom du fournisseur

7.2.4 Ajout d'informations sur les fournisseurs

Le répertoire téléphonique par défaut ne fournit pas de mécanisme pour afficher des informations sur les FAI individuels au sein du consortium d'itinérance, seulement pour le consortium comme un tout. Par exemple, les icônes de fournisseur (grandes et petites) sont incluses dans le profil de service. Les informations de description de service sont supposées contenir le numéro d'assistance aux consommateurs. Cependant, cette information ne peut pas être fournie sur une base individuelle pour chacun des membres d'un consortium d'itinérance. Des informations utiles supplémentaires sur le fournisseur pourraient inclure :

Le numéro de téléphone vocal du fournisseur
L'icône du fournisseur
Le numéro de télécopie du fournisseur
Le numéro d'aide aux consommateurs du fournisseur

7.3 Échange de numéro de téléphone

L'échange des numéros de téléphone n'est actuellement pas pris en charge par le serveur de répertoire téléphonique. Il en résulte que la mise en œuvre d'échange de numéros de téléphone de MSN est faite manuellement. Lorsque de nouveaux points de présence viennent en ligne, les numéros sont transmis à MSN, qui vérifie les numéros et approuve leur ajout au serveur de répertoire téléphonique. Les répertoires téléphoniques à jour sont produits et chargés sur le serveur toutes les semaines.

7.4 Compilation d'annuaire

L'outil de gestion d'annuaire a été créé afin de faciliter aux partenaires l'accès à la création et la mise à jour de leurs répertoires téléphoniques. Il prend en charge l'ajout, le retrait et l'édition des numéros de téléphone, en générant à la fois un nouvel annuaire et les fichiers de différences associés.

Avec la version 1 de l'outil d'administration d'annuaire, les répertoires téléphoniques sont compilés manuellement, et représentent une concaténation des numéros disponibles chez tous les partenaires, sans application de politique. Avec la version 1, les mises à jour sont préparées par les partenaires et transmises au MSN, qui vérifie les numéros et les approuve pour les ajouter à l'annuaire. Les mises à jour sont alors enchaînées ensemble pour former le fichier global de mise à jour.

La nouvelle version de l'outil d'administration d'annuaire automatise la plus grande partie du processus de compilation de l'annuaire, rendant possible la décentralisation de la compilation de l'annuaire, chaque partenaire entretenant son propre serveur d'annuaire téléphonique. Les partenaires peuvent alors maintenir et vérifier leur annuaire téléphonique individuel et l'envoyer sur leur propre serveur d'annuaire.

7.5 Mise à jour d'annuaire

Il existe un mécanisme pour télécharger les deltas du répertoire téléphonique, ainsi que pour télécharger des exécutables arbitraires qui peuvent effectuer un traitement de mise à jour plus complexe. Les signatures numériques ne sont utilisées que pour le téléchargement d'exécutables, car ce sont seulement eux qui représentent une menace pour la sécurité – le client de gestionnaire de connexion ne vérifie pas les signatures numériques sur les deltas parce que des deltas bogués ne peuvent pas réellement causer de dommages.

Le gestionnaire de connexion met à jour l'annuaire chaque fois que l'utilisateur se connecte. Ceci se fait via une demande HTTP GET au serveur d'annuaire. Lorsque le serveur examine la demande, il peut prendre en compte des choses comme la version du système d'exploitation du client, le langage du client, la version du gestionnaire de connexion du le client, et la version de l'annuaire chez le client, afin de déterminer ce qu'il veut renvoyer.

Dans la réponse GET, le serveur d'annuaire répond par les fichiers de différences nécessaires pour mettre à jour à la dernière version d'annuaire du client. Le client construit alors le nouvel annuaire en appliquant successivement ces fichiers de différences. Ce processus résulte en la mise à jour de l'annuaire entier, et est asses simple pour permettre sa mise en œuvre facile sur divers serveurs de HTTP, soit comme un descriptif CGI soit (sur NT) comme un DLL ISAPI.

Les fichiers de différences utilisés dans l'annuaire par défaut consistent en une liste d'entrées d'annuaire, chacune identifiée de façon univoque par son numéro d'indice. Les ajouts consistent en entrées d'annuaire avec toutes les informations remplies ; les suppressions sont signifiées par des entrées dont tous les champs sont à zéro. Un exemple de fichier de différence est présenté ci-dessous :

```
65031,1,1,Aniston,205,5551212,2400,2400,1,0,monfichier
200255,1,1,Auburn/Opelika,334,5551212,9600,28800,0,10,200133,0,0,0,0,0,0,0,0,0
130,1,1,Birmingham,205,5551211,9600,14400,9,0,tonfichier
65034,1,1,Birmingham,205,5551210,9600,14400,1,0,monfichier
```

7.6 Gestion de connexion

Le gestionnaire de connexion peut prendre en charge tout protocole qui peut être configuré via l'utilisation de Windows Dialup Networking, incluant PPP et SLIP sur IP. Le réglage par défaut est pour l'adresse IP ainsi que l'adresse IP de serveur DNS à allouer par le NAS. La capacité d'allocation de serveur DNS est décrite dans la [RFC1877].

7.7 Authentification

Le client de gestionnaire de connexion et le mandataire/serveur RADIUS prennent tous deux en charge la notation de style suffixe (c'est-à-dire, "aboba@msn.com"), ainsi qu'une notation de préfixe ("MSN/aboba").

La notation de préfixe a été développée pour être utilisée avec les appareils de NAS avec de petites longueurs maximum d'identifiant d'utilisateur. Pour ces appareils, la compacité de la notation de préfixe augmente significativement le nombre de caractères disponibles pour le champ userID. Cependant, comme un nombre croissant d'appareils de NAS prennent maintenant en charge des identifiant d'utilisateur de 253 octets (maximum supporté par RADIUS) le besoin de la notation de préfixe diminue.

Après avoir reçu l'identifiant d'utilisateur du client de gestionnaire de connexion, l'appareil de NAS passe les informations d'identifiant d'utilisateur/domaine et de mot de passe (ou dans le cas de CHAP, le défi et la réponse) au mandataire RADIUS. Le mandataire RADIUS vérifie alors si le domaine est autorisé pour l'itinérance en examinant un fichier de configuration statique. Si le domaine est autorisé, le mandataire RADIUS transmet alors la demande au serveur RADIUS approprié. La transposition de domaine à serveur est aussi faite via un fichier de configuration statique.

Bien que les fichiers de configuration statique fonctionnent bien pour les petits consortiums d'itinérance, pour les plus grands consortiums, la configuration statique va devenir fastidieuse. Des solutions potentiellement plus adaptables incluent l'utilisation d'une transposition en serveur RADIUS des enregistrements SRV du DNS pour le domaine.

7.8 Configuration/autorisation de NAS

Bien que les attributs retournés par le serveur RADIUS de rattachement puissent avoir un sens pour les appareils de NAS de rattachement, le NAS local peut être configuré différemment, ou peut être d'un fabricant différent. Il en résulte qu'il peut être nécessaire que le mandataire RADIUS édite le jeu d'attributs retourné par le serveur RADIUS de rattachement, afin de fournir au NAS local les informations de configuration appropriées. L'édition se fait via l'élimination d'attributs et l'insertion d'attributs par le mandataire.

Autrement, le serveur RADIUS de rattachement peut être configuré à ne pas retourner d'attribut spécifique du réseau, et à permettre qu'ils soient insérés par le mandataire RADIUS local.

Les attributs qui vont très probablement causer des conflits incluent :

Framed-IP-Address Framed-IP-Netmask Framed-Routing Framed-Route
Filter-Id Vendor-Specific Session-Timeout Idle-Timeout
Termination-Action

Les conflits qui se rapportent à l'allocation et à l'acheminement des adresses IP sont très courants. Lorsque on utilise l'allocation dynamique d'adresse, un réservoir d'adresses IP approprié pour le NAS local peut être substitué au réservoir d'adresses IP désigné par le serveur RADIUS de rattachement.

Cependant, tous les conflits d'adresses ne peuvent pas se résoudre par l'édition. Dans certains cas, (c'est-à-dire, ceux d'allocation d'une adresse réseau statique pour un LAN) il peut être impossible que le NAS local accepte l'allocation d'adresse du serveur RADIUS de rattachement, et donc les hôtes en itinérance peuvent n'être pas capables d'accepter une autre allocation.

Les identifiants de filtres posent aussi un problème. Il est possible que le NAS local ne puisse pas mettre en œuvre un filtre correspondant à celui désigné par le serveur RADIUS de rattachement. Même si un filtre équivalent est mis en œuvre, afin de garantir un fonctionnement correct, la configuration du mandataire doit retracer les changements de configuration des filtres de chacun des membres du consortium d'itinérance. En pratique, ceci sera probablement impraticable. Le téléchargement direct de la configuration de filtre n'est pas non plus une solution, à cause des grandes variations entre les langages de filtre pris en charge aujourd'hui par les appareils de NAS.

Comme par définition, les attributs spécifiques du fabricant n'ont de signification que pour les appareils créés par ce fabricant, l'utilisation de ces attributs est problématique dans un consortium d'itinérance hétérogène. Bien qu'il soit possible d'éditer ces attributs, ou même de les éliminer ou de leur permettre d'être ignorés, cela peut n'être pas toujours acceptable. Dans les cas où des attributs spécifiques du fabricant se rapportent à la sécurité, il peut n'être pas acceptable que le mandataire modifie ou supprime ces attributs ; la seule action acceptable peut être que le NAS local abandonne l'utilisateur. Malheureusement, RADIUS ne fait pas la distinction entre les attributs obligatoires et facultatifs, de sorte qu'il n'y a pas de moyen pour que le mandataire tire des directives du serveur.

Les conflits sur les temporisations de session ou d'inactivité peuvent se produire car le FAI local et celui de rattachement éprouvent le besoin d'ajuster ces paramètres. Alors que le FAI de rattachement peut souhaiter ajuster le paramètre de façon à

correspondre au logiciel de l'utilisateur, le FAI local peut souhaiter l'ajuster sur sa propre politique de service. Tant que les paramètres désirés ne diffèrent pas trop, un compromis est souvent possible.

7.9 Allocation d'adresse et acheminement

Bien que le logiciel de gestion de connexion supporte l'allocation d'adresse statique et dynamique, dans la mise en œuvre MSN, toutes les allocations d'adresses sont dynamiques.

Cependant, des partenaires choisis offrent aussi la connexité de LAN à leurs consommateurs, usuellement via une allocation d'adresse statique. Cependant, ces comptes n'ont pas de privilèges en matière d'itinérance car aucun mécanisme n'a été mis en place pour permettre que ces chemins statiques soient passés entre les fournisseurs.

Les usagers qui cherchent à faire de l'itinérance de LAN entre les fournisseurs sont invités à choisir un routeur qui prenne en charge la traduction d'adresse réseau (NAT, *Network Address Translation*). Les versions de NAT mises en œuvre dans plusieurs routeurs d'extrémité sont compatibles avec l'adressage dynamique utilisé sur MSN, tout en prenant en charge DHCP sur le côté LAN.

7.10 Sécurité

La mise en œuvre de mandataire/serveur RADIUS n'accepte pas les cartes à jetons ni les protocoles de tunnelage.

7.11 Comptabilité

Dans la mise en œuvre d'itinérance de MSN, le processus d'échange de données comptables est spécifié en termes de format d'enregistrement comptable, et d'une méthode par laquelle les enregistrements sont transférés des partenaires à MSN, qui agit comme agent de règlement. Définir les interactions en termes de formats d'enregistrement et de protocoles de transfert implique que les partenaires ne communiquent pas avec l'agent de règlement en utilisant les protocoles comptables de NAS. Par suite, l'interopérabilité des protocoles comptables n'est pas une exigence.

Cependant, pour que cet avantage soit complet, il est nécessaire que le format d'enregistrement comptable soit extensible. Cela rend plus vraisemblable que le format puisse être adapté pour être utilisé avec la grande diversité des protocoles comptables utilisés actuellement (comme SNMP, syslog, RADIUS, et TACACS+) ainsi que de futurs protocoles. Après tout, si le format d'enregistrement ne peut pas exprimer la métrique fournie par le protocole comptable d'un partenaire particulier, le format d'enregistrement ne sera pas d'une grande utilité pour un consortium d'itinérance hétérogène.

7.11.1 Format d'enregistrement comptable

Le serveur/mandataire Microsoft RADIUS prend en charge la capacité de personnaliser le format d'enregistrement comptable et on suppose que certains FAI utiliseront cette capacité. Cependant pour ceux qui veulent l'utiliser "telle quelle" un format d'enregistrement comptable par défaut est fourni. L'enregistrement comptable comporte des informations fournies par RADIUS :

Nom d'utilisateur (chaîne ; l'identifiant de l'utilisateur, incluant préfixe ou suffixe)
Adresse IP du NAS (Entier ; l'adresse IP du NAS de l'utilisateur)
Accès du NAS (Entier ; identifie l'accès physique sur le NAS)
Type de service (Entier ; identifie le service fourni à l'usager)
Identifiant de NAS (Entier ; identifiant univoque pour le NAS)
Type d'état (Entier ; indique le début et la fin de session, ainsi que de la comptabilité)
Retard (Entier ; temps pendant lequel le client a essayé d'envoyer)
Octets entrés (Entier ; dans l'enregistrement de fin, octets reçus de l'accès)
Octets en sortie (Entier ; dans l'enregistrement de fin, octets envoyés à l'accès)
Identifiant de session (Entier ; identifiant univoque liant les enregistrements de début et de fin)
Authentification (Entier ; indique comment l'usager a été authentifié)
Heure de la session (Entier ; dans l'enregistrement de fin, secondes de service reçu)
Paquets en entrée (Entier ; dans l'enregistrement de fin, paquets reçus de l'accès)
Paquets en sortie (Entier ; dans l'enregistrement de fin, paquets envoyés à l'accès)
Cause de terminaison (Entier ; dans l'enregistrement de fin, indique la cause de terminaison)
Identifiant multi session (Chaîne ; pour relier plusieurs sessions en relations)
Compte de liaison (Entier ; nombre de liaisons actives lorsque l'enregistrement a été généré)
Type d'accès du NAS (Entier ; indique RNIS asynchrone ou synchrone, V.120, etc.)

Cependant, comme ce format par défaut n'est pas extensible, il ne peut pas être facilement adapté aux protocoles autres que

RADIUS, aux services autres que commutés (c'est-à-dire, aux connexions dédiées) ou aux événements étalonnés (c'est-à-dire, aux téléchargements de fichiers). C'est une limitation sérieuse, et par suite, les consommateurs ont demandé un format d'enregistrement comptable plus général.

7.11.2 Mécanisme de transfert

Avant d'être transférés, les enregistrements comptables sont compressés afin d'économiser la bande passante. Le transfert des enregistrements comptables est traité via FTP, le transfert étant initié par le receveur, plutôt que par l'envoyeur. Un ensemble dupliqué d'enregistrements est conservé par le FAI local pour les besoins de vérification.

8. Mise en œuvre de Merit Network

8.1 Généralités

MichNet est un réseau régional de cœur de réseau IP géré dans l'état du Michigan par Merit Network, Inc., une entreprise à but non lucratif qui a sa base à Ann Arbor, Michigan. MichNet qui a commencé en 1966 fournit actuellement la connectivité Internet au niveau cœur de réseau et des services IP commutés à ses membres et aux universités, collèges, écoles K-12, bibliothèques, institutions gouvernementales, et autres organisations à but non lucratif affilées, et à des entités commerciales.

Au 1er mai 1997, MichNet avait 11 membres et 405 affiliés. Son service commuté partagé fonctionne sur 133 sites dans le Michigan et un à Washington, D.C, avec 4774 lignes commutées. Des lignes commutées et des sites sont installés chaque jour.

MichNet fournit aussi des services commutés nationaux et internationaux à ses membres et affiliés par un numéro 800 et d'autres services externes par des contrats avec des opérateurs nationaux et mondiaux.

Les numéros de téléphone de tous les sites commutés de MichNet sont publiés sur le site de la Toile de Merit et dans les lettres d'information de MichNet. Merit fournit aussi des liaisons d'information sur les sites de service nationaux et internationaux sur les sites de la Toile de ses fournisseurs. De telles informations se trouvent à http://www.merit.edu/mich-net/shared.dialin/.

8.1.1 Services commutés partagés à l'échelle de l'état de MichNet

Chaque site de service commuté partagé de MichNet appartient et est entretenu soit par Merit, soit par une organisation membre ou affiliée. Tous les sites doivent accepter les connexions PPP et Telnet.

Chaque organisation qui participe au service commuté partagé reçoit un nom de domaine. Normalement, le nom de domaine ressemble à un nom de domaine pleinement qualifié. Les usagers qui accèdent au service commuté partagé s'identifient en utilisant un identifiant d'accès MichNet qui consiste en leur identifiant local enchaîné avec "@" suivi par le nom de domaine – par exemple, usager@domaine

Merit fait fonctionner un ensemble de serveurs d'authentification, autorisation et comptabilité (AAA, *Authentication, Authorization and Accounting*) qui acceptent le protocole RADIUS et qui sont appelés serveurs de cœur. Les serveurs de cœur prennent en charge tous les sites de service commuté et agissent comme des serveurs mandataires pour les autres serveurs AAA qui fonctionnent chez les organisations participantes. Pour des raisons de sécurité, le personnel de Merit fait fonctionner tous les serveurs de cœur, en particulier, le mot de passe d'utilisateur est en clair lorsque le serveur mandataire de cœur décode une demande entrante et ensuite la recode et la retransmet.

Les serveurs de cœur mettent aussi en application une politique commune à tous les serveurs de commutation. La politique la plus importante est que chaque fournisseur d'accès doit rendre ses accès commutés disponibles pour les autres lorsque les propres utilisateurs du fournisseur n'en ont pas besoin. Pour mettre en œuvre cette politique, le serveur mandataire distingue les domaines qui sont en sa possession et ceux qui sont invités.

Un élément de la politique de détermination de si l'organisation du fournisseur a besoin de l'accès est mis en œuvre par le fait que le serveur mandataire de cœur garde la trace des domaines associés à chaque session connectée à un faisceau de recherche de lignes particulier. Si il y a peu d'accès disponibles (ou "peu" est déterminé par une formule) l'accès est refusé aux invités. Il est aussi alloué une limite de temps aux invités et leurs sessions sont terminées après un certain délai (actuellement une heure en heure de pointe, deux heures en dehors des pointes).

L'autre partie de la politique est de limiter le nombre d'invités auxquels il est permis de se connecter. Ceci est fait en limitant le nombre de sessions d'invité simultanées pour les domaines. Il est alloué à chaque domaine des jetons d'accès simultané (SAT, *simultaneous access tokens*). Lorsque une session d'invité est autorisée, le serveur d'extrémité pour le domaine décrémente le compte de SAT disponibles, et lorsque la session est terminée, le compte de SAT est incrémenté. Un attribut spécifique de

Merit est ajouté à la demande par le cœur si la session va être "invitée" et va exiger un SAT. Le serveur d'extrémité doit inclure une réponse avec un attribut contenant le nom du "réservoir de jetons" duquel le jeton a été extrait pour cette session. L'effet de cela est de limiter le nombre d'invités connectés au réseau au nombre total de jetons alloués à ce domaine.

Chaque domaine est authentifié et autorisé par son propre serveur AAA. Les serveurs mandataires de cœur transmettent les demandes au serveur approprié sur la base d'un fichier de configuration qui montre si un domaine doit être authentifié. Les demandes provenant des domaines qui ne sont pas dans la configuration sont éliminées.

Le logiciel de serveur AAA de Merit soutient cette politique. Merit fournit ce logiciel aux organisations membres et affiliées. Le logiciel est conçu pour fonctionner avec de nombreux serveurs d'authentification existants, tels que Kerberos IV, UNIX password, TACACS, TACACS+, et RADIUS. Cela permet à la plupart des institutions d'utiliser le mécanisme d'authentification dont elles disposent.

8.1.2 Services commutés nationaux et internationaux de MichNet

En plus du service commuté partagé MichNet, Merit fournit aussi l'accès à partir de sites en dehors du Michigan en s'interconnectant avec d'autres services commutés. Ces services sont normalement facturés à la durée de connexion. Merit agit comme agent comptable entre ses membres et organisations affiliées et le fournisseur de service extérieur.

Les services actuellement pris en charge sont un numéro 800 national et un service via le réseau commuté ADP/Autonet. La connexion avec IBM/Advantis est en cours d'essais, et plusieurs autres interconnexions de services sont étudiées.

Les appels passés par un utilisateur membre/affilié de Merit à ces services commutés externes sont authentifiés de la façon suivante : chaque service transmet une demande d'authentification RADIUS et des messages de comptabilité à un serveur mandataire de cœur de Merit. Le cœur transmet les demandes au serveur du membre/affilié pour approbation. Les enregistrements de session sont mémorisés sur le serveur cœur de Merit et sur le serveur du membre/affilié. Merit facture mensuellement ses membres/affiliés sur la base du traitement des enregistrements comptables. Les membres et affiliés sont responsable de le répercuter sur leurs usagers.

Le logiciel Merit AAA prend en charge la capacité a demander une confirmation positive de l'acceptation des charges, et fournit des outils pour des sous totaux et des rapports d'utilisation par domaine et par utilisateur.

8.2 Authentification et autorisation

L'authentification d'une session Telnet est prise en charge en utilisant la méthode traditionnelle de l'identifiant et du mot de passe, l'identifiant étant un identifiant d'accès MichNet de la forme usager@domaine, tandis qu'une session PPP peut être authentifiée soit avec un AccessID et un mot de passe au sein d'un descriptif, soit avec PAP. La prise en charge des mécanismes d'authentification par défi/réponse avec EAP est à l'étude.

Lorsque un usager se connecte à un accès commuté partagé MichNet, le NAS envoie une demande d'accès à un serveur AAA de cœur en utilisant le protocole RADIUS. Le serveur de cœur applique d'abord toute politique de recherche de ligne d'accès appropriée à la demande. Si la demande échoue aux vérifications de politique, un rejet d'accès est retourné au NAS. Autrement, le serveur de cœur la transmet au serveur d'authentification de rattachement de l'usager conformément au domaine de l'usager. Le serveur d'authentification de rattachement authentifie et autorise la demande d'accès. Un message Access-Accept ou Access-Reject est renvoyé au serveur de cœur. Si c'est un Access-Accept qui est envoyé, le serveur de rattachement va créer un identifiant de session commutée qui est unique à cette session et l'insère dans un attribut Class dans le Access-Accept. Le serveur de cœur cherche à nouveau la demande et la réponse dans le serveur de rattachement et décide soit d'accepter soit de rejeter la demande. Finalement, le serveur de cœur envoie un Access-Accept ou un Access-Reject au NAS.

Lorsque un usager appelle un groupe de recherche de lignes d'un FAI sous contrat (service MichNet national et international) le FAI envoie une demande d'accès RADIUS à un serveur de cœur Merit. Le reste du chemin d'authentification et d'autorisation est le même que dans le service commuté partagé, sauf qu'aucune politique de recherche de ligne d'accès n'est appliquée mais un attribut Huntgroup-Service est envoyé au serveur d'authentification de rattachement avec comme valeur le nom du service, et une copie de l'attribut doit être retournée par le serveur de rattachement avec un fanion ajouté à la valeur d'origine pour indiquer une autorisation positive de l'accès d'utilisateur au service spécifié.

Le service commuté partagé MichNet exige normalement une certaine forme d'autorisation, par exemple, un usager qui appelle un groupe de recherche de ligne en tant qu'invité doit être autorisé avec un jeton provenant du domaine de l'usager. Les institutions participantes ont le contrôle de la définition des règles d'autorisation. Actuellement, l'autorisation peut être faite en utilisant toute combinaison du statut de groupe de l'usager et de son statut comptable. Un ensemble d'interfaces de programmation est aussi fourni pour incorporer les nouvelles politiques d'autorisation.

8.3 Comptabilité

Dans le serveur Merit AAA, une session est définie comme débutant au moment où l'usager se connecte au NAS, et se terminant au moment où l'usager se déconnecte. Durant le cours d'une session, le serveur de cœur et le serveur de rattachement conservent tous deux les informations d'état de la session. Cela permet aux serveurs AAA d'appliquer des politiques fondées sur l'état en cours, par exemple, de limiter l'accès des invités par domaine au nombre de jetons disponibles, ou de limiter le nombre de sessions simultanées pour un certains AccessID. Des informations comme si la session est pour un invité, si elle est utilisée comme un jeton, et d'autres informations incluses avec les informations d'arrêt de comptabilité ont amélioré le protocole RADIUS, et sont locales pour le serveur AAA, pour prendre en charge la maintenance des informations d'état de session.

Lorsque une session d'utilisateur est bien authentifiée, le NAS envoie une demande de début de comptabilité RADIUS au serveur de cœur. Celui-ci transmet cette demande au serveur de rattachement de l'utilisateur. Le serveur de rattachement met à jour l'état de la session puis répond au cœur. Le serveur de cœur répond à son tour au NAS. Dans la demande Début de comptabilité, un NAS conforme à la spécification RADIUS doit retourner l'attribut Class et la valeur qu'il a reçue dans le Access-Accept pour la session, renvoyant donc ainsi l'identifiant de session commutée créé par le serveur de rattachement de la session.

Lorsque un utilisateur termine une session, une demande d'arrêt de comptabilité est envoyée sur le même chemin. L'identifiant de session commutée est à nouveau retourné par le NAS, fournissant le moyen d'identifier une session de façon univoque. En configurant l'automate à états finis dans chacun des serveurs AAA, toute demande de comptabilité peut être enregistrée par tout serveur où les demandes de comptabilité est reçue.

Comme tous les mêmes enregistrements de session sont disponibles sur tous les serveurs dans le chemin du message d'autorisation et de comptabilité d'une session, les problèmes de réconciliation de sessions spécifiques peuvent être facilement résolus. Pour le service commuté partagé, il n'y a pas de charges d'utilisation. Merit a des outils pour vérifier que les organisations n'autorisent pas plus de sessions invitées que le nombre de SAT alloué à l'organisation. Pour les sessions surtaxées, Merit envoie tous les mois à chaque organisation une facture récapitulative. Les fichiers des enregistrements détaillés de session sont disponibles pour la résolution des problèmes. Chaque organisation est responsable de la facturation de ses propres usagers, et devrait avoir les mêmes enregistrements de sessions que ceux collectés par Merit.

Merit reçoit une facture mensuelle des autres fournisseurs de service commuté et les paye directement, après avoir d'abord vérifié que les charges correspondent aux enregistrements de session mémorisés par Merit.

8.4 Logiciel et développement

Merit a développé le logiciel de serveur AAA qui prend en charge les capacités ci-dessus en modifiant d'abord le serveur RADIUS fourni par Livingston, et ensuite en faisant une réécriture presque totale du logiciel pour rendre plus faciles les améliorations et extensions de capacités. Merit a fait une version de base de son serveur disponible gratuitement pour un usage non commercial.

Merit a lancé le consortium de serveur AAA Merit qui consiste en Merit et un certain nombre de fabricants de NAS, de FAI et de fabricants de logiciels de serveur. Le consortium prend en charge le développement courant du serveur AAA Merit. L'objectif est de construire un serveur qui prenne en charge les capacités de mandataire ainsi que de serveur d'extrémité, qui sont riches en caractéristique, et qui inter opère avec les produits de NAS de fabricants majeurs.

La pierre angulaire du serveur AAA de Merit, le vecteur de transfert d'authentification/ autorisation (AATV, *Authentication/Authorization Transfer Vector*) est un concept très puissant qui permet une extrême modularité et souplesse du serveur AAA. La structure et les méthodes du modèle AATV sont publiées avec toutes les versions du serveur AAA.

Les objets pour étendre le serveur d'autorisation sont aussi disponibles dans la version améliorée du serveur AAA. Merit cherche aussi le moyen de produire une méthode d'extension du serveur AAA dans sa forme exécutable, pour améliorer l'efficacité et l'adaptabilité du serveur, et pour fournir une meilleure surveillance, instrumentation et administration du serveur.

9. Mise en œuvre FidoNet

Depuis sa naissance en 1984, FidoNet a pris en charge la synchronisation d'annuaire entre ses nœuds membres, qui sont maintenant approximativement 35 000. Comme réseau commuté non IP, FidoNet ne fournit pas de services IP aux membres, et n'utilise pas de technologie d'authentification fondée sur IP. Les nœuds membres offrent plutôt des services de bulletins, incluant l'accès à des messages et des conférences connus sous le nom d'échos.

Pour être capable de communiquer les uns avec les autres, les systèmes membres de FidoNet requièrent un annuaire

synchronisé, appelé Nodelist. L'objet de Nodelist est de permettre la résolution des adresses FidoNet (exprimées sous la forme zone:réseau/nœud, ou 1:161/445) en numéros de téléphone. En tant que réseau commuté, FidoNet requiert des numéros de téléphone pour livrer le trafic de messages et de conférences.

Pour minimiser l'effort requis par la synchronisation régulière d'un annuaire de 35 000 entrées, les mises à jour hebdomadaires de Nodelist sont transmises comme des fichiers de différences. Ces fichiers de différences, appelés Nodediff, produisent la Nodelist pour la semaine en cours lorsque appliqués à la Nodelist de la semaine précédente. Pour minimiser le temps de transfert, les Nodediffs sont compressés avant transfert.

Les informations sur FidoNet, ainsi que sur les documents de normes techniques FidoNet (FTS, *FidoNet Technical Standard*) (incluant la spécification FidoNet) et les propositions de normes sont disponibles à l'archive FidoNet http://www.fidonet.org/.

9.1 Questions d'adaptabilité

Avec une Nodelist de 35 000 entrées, sa taille est maintenant de 3,1 Mbit, et les Nodediffs hebdomadaires font 175 kbit. En forme compressée, la Nodelist fait approximativement 1 Mbits, et la Nodediff hebdomadaires fait 90 kbit. Par suite, le transfert de Nodediff prend approximativement 45 secondes en utilisant un modem à 28 800 bit/s.

Pour améliorer l'adaptabilité, la mise en œuvre d'un service de noms de domaine est examinée dans [FTS0069]. La proposition envisage l'utilisation d'une capacité analogue à l'enregistrement RNIS du DNS afin de transposer les noms en numéros de téléphone, couplée avec un enregistrement supplémentaire pour fournir les attributs associés à un nom.

9.2 Présentation de numéro de téléphone

Bien que les systèmes membres de FidoNet effectuent la synchronisation des annuaires téléphoniques, les usagers ont seulement besoin de connaître l'adresse FidoNet des systèmes qu'ils souhaitent contacter. Par suite, les usagers n'ont pas besoin de garder des copies de la Nodelist sur leur propre système. Ceci est similaire à l'Internet, où le DNS prend soin de la transposition du nom de domaine en adresse IP, de sorte que les usagers n'ont pas à se souvenir des adresses IP.

Néanmoins, les systèmes FidoNet trouvent souvent utile d'être capables de présenter des listes de nœuds, et par suite, les compilateurs de Nodelist de FidoNet produisent normalement une représentation de la Nodelist qui peut être recherchée ou affichée en ligne, ainsi que celle qui est utilisée par le composeur du système.

9.2.1 Format Nodelist de FidoNet

Le format de Nodelist de FidoNet est documenté en détails dans [FTS0005]. Le fichier Nodelist consiste en lignes de données ainsi qu'en lignes de commentaires, qui commencent par un point-virgule. La première ligne de la Nodelist est une ligne de commentaire d'intérêt général qui comporte la date et le numéro du jour, ainsi qu'un CRC de 16 bits. Le CRC est inclus afin de permettre au système qui assemble la nouvelle Nodelist de vérifier son intégrité.

Chaque ligne de données de Nodelist contient huit champs séparés par des virgules

- Mot-clé
- Numéro de zone/région/réseau/nœud
- Nom de nœud
- Localisation
- Nom Sysop
- Numéro de téléphone
- Débit maximum en bauds
- Fanions (facultatif)

Les Nodelists FidoNet sont rangées géographiquement, avec les systèmes dans la même zone, région, et réseaux regroupés ensemble. Par suite, les Nodelists FidoNet n'ont pas besoin d'un fichier de régions séparé. Entre autres choses, le champ Mot-clé peut être utilisé pour indiquer qu'un système est temporairement hors service.

La référence [FTS0005] explique en détails les fanions Nodelist. Entre autres choses, les fanions incluent des informations sur les modulations de modem prises en charge et les protocoles de correction d'erreurs. La référence [FTS0091] propose aussi une série de fanions de capacités RNIS, et [FTS0062] propose des fanions pour indiquer les heures de disponibilité du système.

9.3 Échange de numéro de téléphone

Les coordonnateurs de FidoNet sont chargés de tenir à jour les informations sur leurs réseaux, régions, et zones. Les

coordonnateurs de réseau soumettent chaque semaine à leur coordonnateur régional les versions mises à jour de leur portion de la Nodelist. Les coordonnateurs régionaux compilent alors les soumissions provenant de leurs coordonnateurs de réseau, et les soumettent au coordonnateur de zone. Les coordonnateurs de zones échangent alors leurs soumissions pour produire la nouvelle Nodelist. Par suite, il est possible que la vue des différentes zones puisse différer à un certain moment.

9.3.1 Format Nodediff

Le format du Nodediff est exposé en détails dans [FTS0005]. En préparant les Nodediffs, les coordonnateurs de réseau ne peuvent transmettre que leurs mises à jour de différences, qui peuvent être colligées pour produire directement le Nodediff.

Une faiblesse de l'approche actuelle est qu'aucune sécurité n'est appliquée aux soumissions des coordonnateurs. Cela laisse ouverte la possibilité de propagation de mises à jour frauduleuses. Pour traiter cela, [FTS0055] propose l'ajout d'un secret partagé pour les fichiers de mise à jour.

9.3.2 Ajout de nœuds

Pour postuler à l'allocation d'une adresse FidoNet et adhérer à la Nodelist, les systèmes doivent démontrer qu'ils fonctionnent en envoyant un message au coordonnateur de réseau local. Une fois que le coordonnateur de réseau local a reçu la demande, il peut alors allouer une nouvelle adresse FidoNet, et ajouter une entrée à la Nodelist.

9.3.3 Suppression de nœuds

Comme il est exigé des nœuds FidoNet qu'ils fonctionnent durant l'heure des messages de la zone afin de recevoir les messages, et comme les nœuds reçoivent chaque semaine la Nodelist hebdomadaire de leurs coordonnateurs de réseau local, il y a un mécanisme incorporé pour découvrir les nœuds non fonctionnels.

Les nœuds trouvés inactifs sont rapportés au coordonnateur de réseau local et ensuite marqués comme morts dans la Nodelist. Les nœuds qui restent morts pendant plus de deux semaines sont retirés de la Nodelist, à la discrétion du coordonnateur de réseau.

9.4 Mise à jour d'annuaire

La Nodelist contient les numéros de téléphone et les attributs associés de chaque système participant. Les nouvelles Nodelists sont disponibles le vendredi, et sont mises à la disposition des systèmes participants par leur coordonnateur de réseau local, qui à son tour les reçoit des coordonnateurs régionaux et de zone.

Bien que la pratique standard soit que les systèmes participants obtiennent leur Nodelist de leur coordonnateur de réseau local, si celui-ci n'est pas disponible pour une raison quelconque, la mise à jour ou la Nodelist complète peut être prise sur un autre coordonnateur de réseau, ou régional. Noter que comme la vue depuis des zones différentes peut diverger, les nœuds qui souhaitent mettre à jour leur Nodelist ne devraient pas contacter des systèmes extérieurs à leur zone.

9.5 Compilation d'annuaire

Une fois que les systèmes FidoNet ont reçu la Nodediff, ils l'appliquent à la Nodelist de la semaine précédente afin de préparer la nouvelle Nodelist. Pour recevoir les Nodediffs et compiler la Nodelist, le logiciel suivant est requis :

Une mise en œuvre de messageur compatible FidoNet, utilisé pour transférer les fichiers
Un compilateur Nodelist

Un des objets du compilateur Nodelist est d'appliquer les Nodediffs à la Nodelist précédente afin de produire une Nodelist mise à jour. L'autre objet est de compiler la Nodelist mise à jour dans le format requis par la mise en œuvre de messageur particulière utilisée par le système membre. Il est important de noter qu'alors que les formats de Nodelist et de Nodediff sont normalisés (FTS-0005) comme l'est le protocole de transfert (FTS-0001), le format compilé utilisé par chaque messageur dépend de la mise en œuvre.

Une des raisons pour laquelle les formats compilés diffèrent est l'ajout d'informations hors bande à la Nodelist durant le processus de compilation. Les informations ajoutées incluent les coûts des appels téléphoniques ainsi que les secrets partagés.

9.5.1 Données de coût

Bien que les informations de coût ne fassent pas partie de la Nodelist, en compilant la Nodelist dans le format utilisé par le messageur, les compilateurs de Nodelist prennent en charge l'ajout des informations de coût. Ces informations sont ensuite

utilisées ultérieurement pour guider le comportement des messageurs.

Comme les coûts des appels téléphoniques dépendent des taux facturés par la compagnie de téléphone locale, ces informations sont locales par nature et sont normalement entrées dans le fichier de configuration du compilateur de Nodelist par l'administrateur du système.

9.5.2 Secrets partagés

Dans FidoNet, les secrets partagés sont utilisés pour l'authentification des sessions entre les systèmes. De telles sessions authentifiées sont particulièrement importantes entre les coordonnateurs locaux, régionaux et de zone qui traitent la préparation et la transmission des Nodediffs. Un seul secret partagé est utilisé par système.

9.6 Comptabilité

Au sein de FidoNet, le besoin de comptabilité survient principalement du besoin qu'ont les coordonnateurs locaux, régionaux et de zone d'être remboursés de leurs dépenses. Pour prendre cela en charge, des utilitaires ont été développés pour tenir compte de l'usage du réseau au niveau système selon diverses métriques. Cependant, les techniques comptables ne sont pas appliquées au niveau de l'utilisateur. L'authentification et la comptabilité réparties ne sont pas mises en œuvre et donc les utilisateurs ne peuvent pas se déplacer entre les systèmes.

10. Remerciements

Merci à Glen Zorn de Microsoft et à Lynn Liu et Tao Wang de AimQuest pour les discussions utiles sur cet espace de problème.

Considérations sur la sécurité

Les questions de sécurité sont exposées aux paragraphes 5.6 et 6.5.

11. Références

[FTS0005] Baker, B., R. Moore, D. Nugent. "The Distribution Nodelist." FTS-0005, février 1996.

[FTS0009] Gwinn, R., D. Dodell. "Nodelist Flag Changes Draft Document." FSC-0009, novembre 1987.

[FTS0055] Kolin, L. "Security Passwords in Nodelist Update Files." FSC-0055, mars 1991.

[FTS0062] Thomas, D. J. "A Proposed Nodelist flag indicating Online Times of a Node." FSC-0062, avril 1996.

[FTS0069] Heller, R. "A Proposal for A FidoNet Domain Name Service." FSC-0069, décembte 1992.

[FTS0091] Lentz, A. "ISDN Nodelist flags." FSC-0091, juin 1996.

[RFC1877] S. Cobb, "Extensions du protocole de contrôle de réseau pour la configuration d'adresses de serveurs de noms sur IP en PPP", décembre 1995. *(Information)*

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

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

[RFC2068] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, T. Berners-Lee, "Protocole de transfert Hypertext -- HTTP/1.1", janvier 1997. (*Obsolète, voir* RFC2616) *(P.S.)*

12. Adresse des auteurs

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
téléphone : 206-936-6605
mél : bernarda@microsoft.com

Juan Lu
AimQuest Corporation
1381 McCarthy Blvd.
Milpitas, California 95035
téléphone : 408-273-2730 ext. 2762
mél : juanlu@aimnet.net

John Alsop
i-Pass Alliance Inc.
650 Castro St., Suite 280
Mountain View, CA 94041
téléphone : 415-968-2200
mél : jalsop@ipass.com

James Ding
Asiainfo
One Galleria Tower
13355 Noel Road, #1340
Dallas, TX 75240
téléphone : 214-788-4141
mél : ding@bjai.asiainfo.com

Wei Wang
Merit Network, Inc.
4251 Plymouth Rd., Suite C
Ann Arbor, MI 48105-2785
téléphone : 313-764-2874
mél : weiwang@merit.edu