Groupe de travail Réseau
Request for Comments : 2225
RFC rendues obsolètes : 1626, 1577
Catégorie : Sur la voie de la normalisation

M. Laubach, Com21, Inc.
J. Halpern, Newbridge Networks, Inc.
avril 1998
Traduction Claude Brière de L'Isle

IP et ARP classiques sur ATM

Table des matières

1. Résumé....1
2. Remerciements....2
3. Conventions....2
4. Introduction....2
5. Configuration de sous réseau IP....4
5.1 Fondements....4
5.2 Exigences de configuration de LIS....4
5.3 Configuration supplémentaire de routeur LIS....5
6. Format de paquet IP....5
7. Valeur par défaut de MTU IP sur AAL5 ATM....5
7.1 Circuits virtuels permanents....6
7.2 Circuits virtuels commutés....6
7.3 Découverte de la MTU de chemin exigée....7
8. Services de résolution d'adresse de LIS....7
8.1 Services équivalente ARP et InARP fondés sur ATM....7
8.2 Connexions virtuelles permanentes....7
8.3 Connexions virtuelles commutées....7
8.4 Exigences de fonctionnement pour un seul serveur ATMARP....8
8.5 Exigences de fonctionnement pour client ATMARP....8
8.6 Choix du serveur de résolution d'adresse....10
8.7 Formats de paquet ATMARP....10
8.8 Encapsulation de paquet ATMARP/InATMARP....13
9. Adresse de diffusion IP....13
10. Adresse de diffusion groupée IP....14
11. Considérations sur la sécurité....14
12. Spécification de MIB....14
13. Questions ouvertes....14
14. Références....14
15. Adresse des auteurs....15
Appendice A Informations sur les mises à jour....15
Déclaration complète de droits de reproduction....16

1. Résumé

Le présent mémoire définit une application initiale de IP et ARP classiques dans un environnement de réseau en mode de transfert asynchrone (ATM, *Asynchronous Transfer Mode*) configuré comme un sous réseau IP logique (LIS, *Logical IP Subnetwork*) comme décrit à la Section 5. Le présent mémoire n'empêche pas de développement ultérieur de la technologie ATM dans des domaines autres qu'un LIS ; spécifiquement, comme des réseaux ATM tendent à remplacer de nombreux segments de LAN local Ethernet et comme ces réseaux deviennent mondialement connectés, l'application de IP et ARP

sera traitée différemment. Le présent mémoire examine seulement l'application de ATM comme remplacement direct du "fil" et des segments de LAN locaux qui connectent les stations terminales IP ("les membres") et les routeurs qui opèrent dans le paradigme "classique" fondé sur le LAN. Les questions soulevées par le pontage de niveau MAC et l'émulation de LAN sortent du domaine d'application du présent article.

Le présent mémoire introduit la technologie et nomenclature générales d'ATM. Les lecteurs sont invités à se reporter aux références de l'ATM Forum et de l'UIT-T (anciennement CCITT) pour des informations plus détaillées sur les accords et normes de mise en œuvre d'ATM.

2. Remerciements

Les auteurs tiennent à remercier de leurs efforts les membres du groupe de travail IP sur ATM de l'IETF. Sans leur soutien substantiel, et parfois critique, du modèle classique de IP sur ATM, ce mémoire mis à jour n'aurait pas été possible. La Section 7, sur la MTU par défaut, a été incorporée directement de la RFC 1626 de Ran Atkinson, avec sa permission. Merci à Andy Malis pour sa relecture du projet et ses commentaires.

3. Conventions

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].

4. Introduction

Le but de la présente spécification est de permettre des mises en œuvre compatibles et interopérables pour transmettre des datagrammes IP et des demandes et réponses du protocole de résolution d'adresse ATM (ATMARP, *ATM Address Resolution Protocol*) sur la couche 5 d'adaptation ATM (AAL5, *ATM Adaptation Layer 5*) [RFC1483], [I.363].

Le présent mémoire spécifie le modèle de fonctionnement de base à fondations stables qui va toujours être disponible dans IP et les mises en œuvre de ARP sur ATM. Des documents ultérieurs pourront s'appuyer sur et préciser ce modèle. Cependant, en l'absence ou en cas d'échec de ces extensions, le fonctionnement reviendra par défaut aux spécifications contenues dans le présent mémoire. Par conséquent, le présent mémoire ne fera pas référence à ces autres extensions.

Le présent mémoire définit seulement le fonctionnement de IP et de la résolution d'adresse sur ATM, et n'est pas destiné à décrire le fonctionnement des réseaux ATM. Toutes les références à des connexions virtuelles, connexions virtuelles permanentes, ou connexions virtuelles commutées s'appliquent seulement aux connexions de canal virtuel utilisées pour prendre en charge IP et la résolution d'adresse sur ATM, et donc sont supposées utiliser AAL5. Le présent mémoire ne pose aucune restriction ou exigence sur les connexions virtuelles utilisées pour d'autres objets.

Le déploiement initial de ATM fournit un remplacement de segment de LAN pour :
1) Les réseaux de zone locale (par exemple, Ethernets, anneaux à jetons et FDDI).
2) Les cœurs de réseau de zone locale entre des LAN existants (non ATM).
3) Les PVV de circuits dédiés ou de relais de trame entre des routeurs IP.

Note : en 1), les routeurs IP locaux avec une ou plusieurs interfaces ATM vont être capables de connecter des îlots de réseaux ATM. En 3), des réseaux public ou privés de large zone ATM vont être utilisés pour connecter des routeurs IP, qui à leur tour peuvent ou non se connecter aux réseaux ATM locaux. Les WAN et LAN ATM peuvent être interconnectés.

Les réseaux ATM privés (locaux ou de large zone) vont utiliser la structure d'adresses ATM privées spécifiée dans la spécification UNI 3.1 de l'ATM Forum [ATMUNI] ou dans la spécification UNI 4.0 de l'ATM Forum [UNI4.0]. Cette structure est modélisée d'après le format d'une adresse de point d'accès de service réseau OSI (NSAPA, *Network Service Access Point Address*). Une adresse privée ATM identifie de façon univoque un point d'extrémité ATM.

Les réseaux publics vont utiliser soit la structure d'adresse spécifiée dans la Recommandation UIT-T E.164, soit la structure

d'adresse privée de réseau ATM. Une adresse E.164 identifie de façon univoque une interface à un réseau public.

Les caractéristiques des réseaux ATM sont différentes de celles des LAN :

- ATM fournit un environnement commuté de connexion virtuelle (VC, *Virtual Connection*). L'établissement de VC peut être fait sur une connexion virtuelle permanente (PVC, *Permanent Virtual Connection*) ou sur une connexion virtuelle commutée (SVC, *Switched Virtual Connection)* dynamique. La signalisation de gestion d'appel de SVC est effectué via les mises en œuvre du protocole UNI 3.1 [Q.93B], [ATMUNI].

- Les données à passer par un VC sont segmentées en quantités de 53 octets appelées des cellules (5 octets d'en-tête ATM et 48 octets de données).

- La fonction de transposition des unités de données de protocole (PDU, *Protocol Data Unit*) d'utilisateur en le champ d'informations de la cellule ATM et vice versa est effectuée dans la couche d'adaptation ATM (AAL, *ATM Adaptation Layer*). Quand un VC est créé, un type AAL spécifique est associé au VC. Il y a quatre types d'AAL différents, auxquels on se réfère individuellement comme "AAL1", "AAL2", "AAL3/4", et "AAL5". (Note : le présent mémoire concerne seulement la transposition de IP et ATMARP sur AAL5. Les autres types AAL sont mentionnés seulement pour mémoire.) Le type AAL est connu par les points d'extrémité de VC via le mécanisme d'établissement d'appel et n'est pas porté dans l'en-tête de cellule ATM. Pour les PVC, le type AAL est configuré administrativement aux points d'extrémité quand la connexion (circuit) est établie. Pour les SVC, le type AAL est communiqué le long du chemin du VC via UNI 3.1 au titre de l'établissement d'appel et les points d'extrémité utilisent les informations signalées pour la configuration. Les commutateurs ATM ne se soucient généralement pas du type AAL des VC. Le format AAL5 spécifie un format de paquet d'une taille maximum de (64 k - 1) octets de données d'utilisateur. Les cellules pour une PDU AAL5 sont transmises de la première à la dernière, la dernière cellule indiquant la fin de la PDU. Les normes ATM garantissent que sur un VC donné, l'ordre des cellules est préservé de bout en bout. Note : AAL5 fournit un service de transfert de données non assuré - il appartient aux protocoles de niveau supérieur d'assurer la retransmission.

- La signalisation du Forum ATM définit l'établissement de connexion en point à point et en point à multipoint [ATMUNI], [UNI4.0]. Le multipoint à multipoint n'est pas encore spécifié par l'UIT-T ou l'ATM Forum.

Une adresse ATM est codée soit en forme NSAP d'adresse de système d'extrémité ATM (AESA, *ATM EndSystem Address*) soit comme adresse publique UNI E.164 [ATMUNI], [UNI4.0]. Dans certains cas, les deux adresses AESA et UNI E.164 publique sont nécessaires pour qu'un client ATMARP accède à un autre hôte ou routeur.

Comme l'utilisation des adresses AESA et UNI E.164 publique par ATMARP est analogue à l'utilisation des adresses Ethernet, la notion de "adresse matérielle" est étendue pour englober les adresses ATM dans le contexte de ATMARP, bien que les adresses ATM n'aient pas besoin d'avoir une signification de matériel. Les adresses de format NSAP de l'ATM Forum (AESA) utilisent le même format de base que les NSAP OSI GOSIP d'Amérique du Nord [RFC1237].

Note : les adresses de l'ATM Forum ne devraient pas être conçues comme étant des NSAP GOSIP U.S. Elles ne le sont pas, l'administration est différente, les champs remplis sont différents, etc. Cependant, dans le présent document, ont s'y réfère comme à des NSAPA.

Le présent mémoire décrit le déploiement initial de ATM au sein de réseaux IP "classiques" comme remplacement direct des réseaux de zone locale (Ethernets) et pour les liaisons IP qui interconnectent les routeurs, au sein de ou entre domaines administratifs. Le modèle "classique" se réfère ici au traitement de l'adaptateur d'hôte ATM comme interface de réseautage à la pile de protocole IP qui opère dans un paradigme fondé sur le LAN.

Les caractéristiques du modèle classique sont :

- La même taille d'unité maximum de transmission (MTU) est par défaut pour tous les VC dans un LIS. Cependant, sur la base du VC en point à point, la taille de MTU peut être négociée durant l'établissement de connexion en utilisant la découverte de la MTU de chemin pour mieux couvrir les besoins de la paire de membres IP coopérants, ou les attributs du chemin des communications. (Voir au paragraphe 7.3.)
- L'encapsulation LLC/SNAP par défaut des paquets IP.
- L'architecture d'acheminement IP de bout en bout reste la même.
- Les adresses IP sont résolues en adresses ATM par l'utilisation d'un service ATMARP au sein du LIS – les ATMARP restent au sein du LIS. Du point de vue du client, l'architecture ATMARP reste fidèle au modèle ARP de base présenté dans la [RFC0826].
- Un sous réseau IP est utilisé pour de nombreux hôtes et routeurs. Chaque VC connecte directement deux membres IP au sein du même LIS.

Des documents futurs décriront le fonctionnement de IP sur ATM quand les réseaux ATM seront déployés et interconnectés mondialement.

Le déploiement de ATM dans la communauté Internet commence seulement et va prendre de nombreuses années pour s'achever. Durant la première partie de cette période, on s'attend à ce que le déploiement suive les frontières traditionnelles de sous réseau IP pour les raisons suivantes :

- Les administrateurs et gestionnaires de sous réseaux IP vont tendre initialement à suivre les mêmes modèles qu'ils ont déployé jusqu'à présent. L'état d'esprit de la communauté va changer lentement, le temps que ATM augmente sa couverture et construise sa crédibilité.
- Les pratiques d'administration de politique s'appuient sur la sécurité, l'accès, l'acheminement, et les capacités de filtrage des passerelles IP de l'Internet : c'est-à-dire, les pare-feu. Il ne sera pas permis à ATM d'être une "solution de remplacement" à ces mécanismes tant qu'il n'aura pas fourni de meilleures capacités de gestion que les services et pratiques existantes.
- Les normes pour l'IP mondial sur ATM prendront du temps pour être achevées et déployées.

Le présent mémoire détaille le traitement du modèle classique de IP et ATMARP sur ATM. Le présent mémoire n'empêche pas le traitement ultérieur des réseaux ATM dans le cadre IP lorsque ATM sera déployé et interconnecté mondialement ; cela fera l'objet de documents futurs. Le présent mémoire ne traite pas les questions relatives à la transparence de l'interopérabilité de la couche de liaison des données.

5. Configuration de sous réseau IP

5.1 Fondements

Dans le scénario de LIS, chaque entité administrative séparée configure ses hôtes et routeurs au sein d'un LIS. Chaque LIS opère et communique indépendamment des autres LIS sur le même réseau ATM.

Dans le modèle classique, les hôtes communiquent directement via ATM avec les autres hôtes au sein du même LIS en utilisant le service ATMARP comme mécanisme pour résoudre les adresses IP cibles en adresses de point d'extrémité ATM cible. Le service ATMARP a seulement une portée de LIS et dessert tous les hôtes dans le LIS. La communication avec les hôtes situés en dehors du LIS local est assurée via un routeur IP. Ce routeur est un point d'extrémité ATM rattaché au réseau ATM et il est configuré comme membre d'un ou plusieurs LIS. Cette configuration PEUT résulter en un certain nombre de LIS disjoints opérant sur le même réseau ATM. En utilisant ce modèle, les hôtes de différents sous réseaux IP DOIVENT communiquer via un routeur IP intermédiaire même si il est possible d'ouvrir un VC direct entre les deux membres IP sur le réseau ATM.

Par défaut, le service ATMARP et le modèle classique d'acheminement de LIS DOIT être disponible à tout client de membre IP dans le LIS.

5.2 Exigences de configuration de LIS

Les exigences pour les membres IP (hôtes, routeurs) opérant dans une configuration de LIS ATM sont :

- Tous les membres du LIS ont le même numéro de réseau/sous réseau IP et gabarit d'adresse [RFC1122].
- Tous les membres du LIS sont directement connectés au réseau ATM.
- Tous les membres du LIS DOIVENT avoir un mécanisme pour résoudre les adresses IP en adresses ATM via ATMARP (fondé sur la [RFC0826]) et vice versa via InATMARP (fondé sur la [RFC1293]) quand ils utilisent des SVC. Voir à la Section 8 "Services de résolution d'adresse de LIS".
- Tous les membres du LIS DOIVENT avoir un mécanisme pour résoudre les VC en adresses IP via InATMARP (fondé sur la [RFC1293]) quand ils utilisent des PVC. Voir à la Section 8 "Services de résolution d'adresse de LIS".
- Tous les membres du LIS DOIVENT être capables de communiquer via ATM avec tous les autres membres dans le même LIS ; c'est-à-dire que la topologie de la connexion virtuelle sous-jacente d'inter communication parmi les membres est pleinement maillée.

La liste suivante identifie l'ensemble des paramètres ATM spécifiques qui DOIVENT être mis en œuvre dans chaque station IP connectée au réseau ATM :

- Adresse de matériel ATM (atm$ha). C'est l'adresse ATM de la station IP individuelle.
- Liste d'adresses de demande ATMARP (atm$arp-req-list) : c'est une liste qui contient une ou plusieurs adresses ATM de serveurs ATMARP individuels situés au sein du LIS. Dans un environnement de SVC, les serveurs ATMARP sont utilisés pour résoudre les adresses IP cibles en adresse ATM cible via un protocole de demande/réponse ATMARP. Les

serveurs ATMARP DOIVENT avoir une responsabilité d'autorité pour résoudre les demandes ATMARP de tous les membres IP qui utilisent les SVC situés dans le LIS.

Un LIS DOIT avoir une seule entrée de service ATMARP configurée et disponible pour tous les membres du LIS qui utilisent les SVC.

Dans le cas où il y a seulement un serveur ATMARP au sein du LIS, alors tous les clients ATMARP DOIVENT être configurés de façon identique à avoir seulement une entrée non nulle dans la atm$arp-req-list configurée avec la même adresse du seul service ATMARP.

Si le membre IP opère seulement avec des PVC, atm$arp-req-list DOIT alors être configurée avec toutes les entrées nulles et le client NE DOIT PAS faire d'interrogation à un service de résolution d'adresse.

Dans les restrictions mentionnées ci-dessus et à la Section 8, l'administration locale DOIT décider quelles adresses de serveur sont appropriées pour atm$arp-req-list.

Par défaut, atm$arp-req-list DOIT être configurée en utilisant la MIB [RFC2320].

La configuration manuelle des adresses et listes d'adresses présentée dans cette section dépend de la mise en œuvre et sort du domaine d'application du présent document ; c'est-à-dire que le présent mémoire n'exige aucune méthode de configuration spécifique. Le présent mémoire EXIGE que ces adresses soient complètement configurées chez le client, comme approprié pour le LIS, avant d'utiliser tout service ou opération détaillé dans le présent mémoire.

5.3 Configuration supplémentaire de routeur LIS

Il est RECOMMANDÉ que les routeurs qui fournissent la fonction de LIS sur le réseau ATM prennent aussi en charge la capacité d'interconnecter plusieurs LIS. Les routeurs qui souhaitent fournir l'interconnexion de différents LIS DOIVENT être capables de prendre en charge plusieurs ensembles de ces paramètres (un ensemble pour chaque LIS connecté) et être capables d'associer chaque ensemble de paramètres à un numéro spécifique dc réseau/sous réseau IP. De plus, il est RECOMMANDÉ qu'un routeur soit capable de fournir cette prise en charge de LIS multiples avec une seule interface physique ATM qui puisse avoir une ou plusieurs adresses de point d'extrémité ATM individuel. Note : ceci ne signifie pas nécessairement différents identifiants de système d'extrémité (ESI, *End System Identifier*) quand des NSAPA sont utilisés. Le dernier octet d'un NSAPA est le champ Sélecteur (SEL) qui peut être utilisé pour différencier jusqu'à 256 LIS différents pour le même ESI. (Voir le paragraphe 5.1.3.1, "Private Networks" dans [ATMUNI].)

6. Format de paquet IP

Les mises en œuvre DOIVENT prendre en charge l'encapsulation IEEE 802.2 LLC/SNAP décrite dans la [RFC1483]. L'encapsulation LLC/SNAP est le format par défaut de paquet pour les datagrammes IP.

Le présent mémoire reconnaît que d'autres méthodes d'encapsulation peuvent être cependant utilisées, en l'absence d'autres informations ou accords, l'encapsulation LLC/SNAP est par défaut.

Le présent mémoire reconnaît que la signalisation de bout en bout au sein d'ATM peut permettre la négociation de méthode d'encapsulation sur la base du VC.

7. Valeur par défaut de MTU IP sur AAL5 ATM

Les protocoles largement utilisés dans l'Internet, comme le système de fichier de réseau (NFS, *Network File System*), utilisent actuellement de grandes tailles de trame (par exemple, 8 kB). L'évidence empirique de diverses applications sur le protocoles de contrôle de transmission (TCP, *Transmission Control Protocol*) indique que de plus grandes tailles d'unité maximum de transmission (MTU, *Maximum Transmission Unit*) pour le protocole Internet (IP) tendent à donner de meilleures performances. La fragmentation des datagrammes IP est connue pour être très indésirable [FRAG]. Il est souhaitable de réduire la fragmentation dans le réseau et par là d'améliorer les performances en ayant une MTU IP pour AAL5 raisonnablement grande. Par défaut, NFS a une taille de trame de 8192 octets. Pour permettre les en-têtes RPC/XDR, UDP, IP, et LLC, NFS préférerait une MTU par défaut d'au moins 8300 octets. Les routeurs peuvent parfois avoir de meilleures performances avec de plus grandes tailles de paquet parce que la plupart des coûts de performance dans

les routeurs sont relatifs aux "paquets traités" plutôt qu'aux "octets transférés". Donc, il y a un certain nombre de bonnes raisons pour avoir une valeur de MTU par défaut raisonnablement grande pour IP sur ATM AAL5.

La RFC 1209 spécifie que la MTU IP sur SMDS est de 9180 octets, ce qui est supérieur à 8300 octets mais encore dans la même gamme [RFC1209]. Il n'y a pas de bonne raison pour que la MTU par défaut de IP sur ATM AAL5 soit différente de IP sur SMDS, étant donné qu'elles vont être de la même magnitude. Que les deux soient de la même taille va aider à l'interopérabilité et va aussi aider à réduire l'incidence de la fragmentation IP.

Donc, La MTU IP par défaut à utiliser avec ATM AAL5 devra être 9180 octets. Toutes les mises en œuvre conformes à la présente spécification devront prendre en charge au moins la valeur de MTU IP par défaut à utiliser sur ATM AAL5.

7.1 Circuits virtuels permanents

Les mises en œuvre qui prennent seulement en charge les circuits virtuels permanents (PVC) ne vont pas (par définition) mettre en œuvre de protocole de signalisation ATM. De telles mises en œuvre devront utiliser la valeur de MTU IP par défaut de 9180 octets sauf si les deux parties se sont accordées à l'avance sur l'utilisation d'une autre valeur de MTU IP via un mécanisme non spécifié ici.

7.2 Circuits virtuels commutés

Les mises en œuvre qui prennent en charge les circuits virtuels commutés (SVC) DOIVENT tenter de négocier la taille de CPCS-SDU AAL en utilisant le protocole de signalisation ATM. Le protocole de signalisation ATM standard de l'industrie utilise deux différentes parties de l'élément d'information appelé "Paramètres AAL" pour échanger les informations de MTU sur le circuit ATM à établir [ATMUNI]. Le champ Taille maximum de CPCS-SDU de transmission contient la valeur du chemin de l'appelant à l'appelé. Le champ Taille maximum de CPCS-SDU de retour contient la valeur sur le chemin de l'appelé à l'appelant. Le Forum ATM spécifie les valeurs valides de cet identifiant comme de 1 à 65535 inclus. Noter que la signalisation d'interface d'usager réseau (UNI, *User-to-Network-Interface*) de l'ATM Forum permet que la MTU dans une direction soit différente de la MTU dans la direction opposée, de sorte que l'identifiant de taille maximum de CPCS-SDU de transmission peut avoir une valeur différente de l'identifiant de taille maximum de CPCS-SDU de retour sur la même connexion.

Si l'appelant souhaite utiliser la MTU par défaut, il devra inclure l'élément d'information "Paramètres AAL" avec les valeurs par défaut pour la taille maximum de CPCS-SDU au titre du message SETUP du protocole de signalisation ATM [ATMUNI]. Si l'appelant désire utiliser une valeur différente que celle par défaut, il devra inclure l'élément d'information "Paramètres AAL" avec la valeur désirée pour la taille maximum de CPCS-SDU au titre du message SETUP du protocole de signalisation ATM. L'appelé va répondre en utilisant les mêmes éléments d'information et identifiants dans son message de réponse CONNECT [ATMUNI].

Si l'appelé reçoit a message SETUP contenant la "taille maximum de CPCS-SDU" dans l'élément d'information Paramètres AAL, il devra traiter l'identifiant de taille maximum de CPCS-SDU de transmission et de retour comme suit :

a) Si il est capable d'accepter les valeurs de MTU ATM proposées par le message SETUP, il devra inclure un élément d'information Paramètres AAL dans sa réponse. Les champs Taille maximum de CPCS-SDU de transmission et de retour devront être présents et leurs valeurs devront être égales aux valeurs correspondantes dans le message SETUP.

b) Si il souhaite une taille de MTU ATM plus petite que celle proposée, il devra alors régler les valeurs de taille maximum de CPCS-SDU dans les éléments d'information Paramètres AAL égaux à la valeur désirée dans le message CONNECT de réponse au message SETUP original.

c) Si le point d'extrémité appelant reçoit un message CONNECT qui ne contient pas d'élément d'information Paramètres AAL, mais si le message SETUP correspondant contenait bien l'élément d'information Paramètres AAL (incluant les champs de taille de CPCS-SDU de transmission et de retour) il devra libérer l'appel avec la cause "Paramètres AAL non pris en charge".

d) Si l'un ou l'autre point d'extrémité reçoit un message STATUS avec la cause "élément d'information non existant ou non mis en œuvre" ou la cause "Informations d'accès éliminées", et avec un champ de diagnostic indiquant l'identifiant de l'élément d'information Paramètres AAL, il devra éliminer l'appel avec la cause "Paramètres AAL non pris en charge."

e) Si l'un ou l'autre point d'extrémité reçoit des CPCS-SDU qui dépassent la taille de MTU négociée, il peut utiliser la

fragmentation IP ou peut éliminer l'appel avec la cause "Paramètres AAL non pris en charge". Dans ce cas, une erreur s'est produite due à une faute dans un système d'extrémité ou dans le réseau ATM. L'erreur devrait être notée par la gestion de réseau ATM pour un examen et intervention humaine.

Si le point d'extrémité appelé inclut incorrectement les champs de taille maximum de CPCS-SDU de transmission et de retour dans les messages CONNECT (par exemple, parce que le message SETUP original n'incluait pas ces champs) ou si il règle ces champs à une valeur invalide, l'appelant devra alors libérer l'appel avec la cause "Contenu d'élément d'information invalide".

7.3 Découverte de la MTU de chemin exigée

Le mécanisme de découverte de la MTU de chemin est une norme de l'Internet [RFC1191] et est un important mécanisme pour réduire la fragmentation IP dans l'Internet. Ce mécanisme est particulièrement important parce que le nouveau sous réseau ATM utilise des tailles de MTU par défaut significativement différentes des anciennes technologies de sous réseau comme Ethernet et FDDI.

Afin d'assurer de bonnes performances à travers l'Internet et aussi de permettre à IP de tirer pleinement parti des potentiellement plus grandes tailles de datagramme IP supportées par ATM, toutes les mises en œuvre de routeur qui se conforment à la présente spécification doivent aussi mettre en œuvre le mécanisme de découverte de la MTU de chemin IP comme défini dans la RFC 1191 et précisé dans la [RFC1435]. Les mises en œuvre d'hôtes devraient mettre en œuvre le mécanisme de découverte de la MTU de chemin IP comme défini dans la RFC 1191.

8. Services de résolution d'adresse de LIS

8.1 Services équivalente ARP et InARP fondés sur ATM

La résolution d'adresse au sein d'un LIS ATM DEVRA utiliser le protocole de résolution d'adresse ATM (ATMARP) (fondé sur la [RFC0826]) et le protocole de résolution d'adresse ATM inverse (InATMARP) (fondé sur la [RFC1293]) et comme défini dans le présent mémoire. ATMARP est le même protocole que le protocole ARP présenté dans la [RFC0826] avec les extensions nécessaires pour prendre en charge la résolution d'adresse dans un environnement de serveur d'envoi individuel ATM. InATMARP est le même protocole que le protocole InARP original présenté dans la [RFC1293] mais appliqué aux réseaux ATM. Toutes les stations IP DOIVENT prendre en charge ces protocoles tels que mis à jour et étendus dans le présent mémoire. L'utilisation de ces protocoles diffère selon que des PVC ou des SVC sont utilisés.

8.2 Connexions virtuelles permanentes

Une station IP DOIT avoir un mécanisme (par exemple, configuration manuelle) pour déterminer quels PVC elle a, et en particulier quels PVC sont utilisés avec l'encapsulation de LLC/SNAP. Les détails du mécanisme sortent du domaine d'application du présent mémoire.

Il est exigé de tous les membres IP qui prennent en charge les PVC qu'il utilisent le protocole de résolution d'adresse ATM inverse (InATMARP) (voir la [RFC1293]) sur les VC qui utilisent l'encapsulation de LLC/SNAP. Dans un environnement strict de PVC, le receveur DEVRA déduire le VC pertinent du VC sur lequel a été reçue la demande ou réponse InATMARP. Quand l'adresse ATM de source et/ou de cible est inconnue, la longueur de l'adresse ATM correspondante dans le paquet InATMARP DOIT être réglée à zéro (0) pour indiquer une longueur nulle, et aucune mémorisation ne sera allouée dans le paquet InATMARP ; autrement, les champs d'adresse appropriés devraient être remplis et la longueur correspondante réglée de façon appropriée. Les détails du format de paquet InATMARP sont présentés plus loin dans le présent mémoire.

D'après la [RFC1293] : "Quand la station demandeuse reçoit la réponse In[ATM]ARP, elle peut compléter l'entrée de tableau [ATM]ARP et utiliser les informations d'adresse fournies. Note : comme avec [ATM]ARP, les informations apprises via In[ATM]ARP peuvent être périmées ou invalidées dans certaines circonstances". Les stations IP qui prennent en charge les PVC DOIVENT re-valider les entrées de tableau ATMARP au titre du processus de vieillissement de tableau. Voir au paragraphe 8.5.1 "Péremption de tableau de client ATMARP".

Si un client a plus d'une adresse IP dans le LIS et si il utilise des PVC, quand une demande InATMARP est reçue, une réponse InATMARP DOIT être générée pour chacune de ces adresses.

8.3 Connexions virtuelles commutées

Les SVC exigent la prise en charge des services de résolution d'adresse pour résoudre les adresses IP de cible en adresses de point d'extrémité ATM cible. Tous les membres du LIS DOIVENT utiliser le même service. Ce service DOIT avoir la responsabilité d'autorité pour résoudre les demandes ATMARP de tous les membres IP au sein du LIS.

Les serveurs ATMARP n'établissent pas activement les connexions. Ils dépendent des clients dans le LIS pour initier les connexions pour la procédure d'enregistrement ATMARP et pour transmettre les demandes ATMARP. Un client individuel se connecte au serveur ATMARP en utilisant un VC point à point LLC/SNAP. Le client envoie des paquets de demande ATMARP normaux au serveur. Le serveur ATMARP examine chaque paquet de demande ATMARP pour vérifier les informations de protocole de source et d'adresse de matériel de source du client envoyeur et utilise ces informations pour construire son antémémoire de tableau ATMARP. Ces informations sont utilisées pour générer les réponses à toute demande ATMARP qu'il reçoit.

Les paquets de demande InATMARP DOIVENT spécifier des informations d'adresse valides pour le numéro de source ATM, le numéro de cible ATM, et l'adresse de protocole de source ; c'est-à-dire que ces champs DOIVENT être non nuls dans les paquets de demande InATMARP.

Le présent mémoire définit le service de résolution d'adresse dans le LIS et le contraint à consister en un seul serveur ATMARP. L'interaction client-serveur est définie en utilisant une approche à un seul serveur comme modèle de référence.

Le présent mémoire reconnaît le futur développement de normes et de mises en œuvre de modèles à plusieurs serveurs ATMARP qui vont étendre le fonctionnement comme défini dans le présent mémoire à fournir un service de résolution d'adresse de grande fiabilité.

8.4 Exigences de fonctionnement pour un seul serveur ATMARP

Un seul serveur ATMARP accepte les appels/connexions ATM provenant des autres points d'extrémité ATM. Après avoir reçu une demande ATMARP, le serveur va examiner les informations d'adresse de source et de cible dans le paquet et noter le VC sur lequel la demande ATMARP est arrivée. Il va utiliser ces informations comme nécessaire pour construire et mettre à jour ses entrées de tableau ATMARP.

Pour chaque demande ATMARP :

1. Si l'adresse IP de source est la même que l'adresse IP de cible et si une entrée de tableau existe pour cette adresse IP et si l'adresse de matériel ATM de source ne correspond pas à l'adresse ATM de l'entrée de tableau et si il y a un VC associé ouvert avec cette entrée de tableau qui n'est pas la même que le VC associé à la demande ATMARP, le serveur DOIT retourner les informations d'entrée de tableau dans la réponse ATMARP, et DOIT soulever une condition "Adresse IP dupliquée détectée" à la gestion du serveur. L'entrée de tableau n'est pas mise à jour.

2. Autrement, si l'adresse IP de source est la même que l'adresse IP de cible, et si il n'y a pas d'entrée de tableau pour cette adresse IP, ou si une entrée de tableau existe pour cette adresse IP et sil il n'y a pas de VC ouvert associé à cette entrée de tableau, ou si le VC associé à cette entrée est le même que le VC pour la demande ATMARP, le serveur DOIT soit créer une nouvelle entrée, soit mettre à jour la vieille entrée comme approprié et retourner ces informations d'entrée de tableau dans la réponse ATMARP.

3. Autrement, quand l'adresse IP de source ne correspond pas à l'adresse IP de cible, le serveur ATMARP va générer la réponse ATMARP correspondante si il a une entrée pour les informations de cible dans son tableau ATMARP. Autrement, il va générer une réponse ATMARP négative (ATMARP_NAK).

4. De plus, quand l'adresse IP de source ne correspond pas à l'adresse IP de cible et quand le serveur reçoit une demande ATMARP sur un VC, alors que les adresses IP et ATM de source n'ont pas d'entrée de tableau correspondante, le serveur ATMARP DOIT créer une nouvelle entrée de tableau pour les informations de source. Explication : cela permet aux vieux clients de la RFC 1577 de s'enregistrer à ce service ATMARP juste en lui envoyant des demandes.

5. De plus, quand l'adresse IP de source ne correspond pas à l'adresse IP de cible et que les adresses IP et ATM de source correspondent à l'association qui est déjà dans le tableau ATMARP et que l'adresse ATM correspond à celle associée au VC, le serveur DOIT mettre à jour le temporisateur de tableau sur l'entrée de tableau ATMARP de source mais seulement si il s'est écoulé plus de 10 minutes depuis la dernière mise à jour. Explication : si le client est en train d'envoyer des demandes ATMARP au serveur sur le même VC qu'utilisé pour enregistrer son entrée ATMARP, le serveur devrait examiner la demande ATMARP et noter que le client est toujours "en vie" en mettant à jour le

temporisateur sur l'entrée de tableau ATMARP du client.

6. De plus, quand l'adresse IP de source ne correspond pas à l'adresse IP de cible et que les adresses IP et ATM de source ne correspondent pas à l'association qui est déjà dans le tableau ATMARP, le serveur NE DOIT PAS mettre à jour l'entrée de tableau ATMARP.

Un serveur ATMARP DOIT avoir connaissance de tous les VC ouverts qu'il a et de leur association avec une entrée de tableau ATMARP, et en particulier, de quels VC prennent en charge l'encapsulation LLC/SNAP. En fonctionnement normal, les clients ATMARP actifs vont revalider leurs entrées avant que le processus de vieillissement du serveur prenne effet.

Les entrées de tableau de serveur ATMARP sont valides pendant 20 minutes. Si une entrée reste plus de 20 minutes sans être mise à jour (rafraîchie) par le client, cette entrée est supprimée du tableau sans considération de l'état de tout VC qui peut être associé à cette entrée.

8.5 Exigences de fonctionnement pour client ATMARP

Le client ATMARP est chargé de contacter le service ATMARP pour s'enregistrer initialement et ensuite rafraîchir ses propres informations ATMARP.

Le client est aussi chargé d'utiliser le service ATMARP pour obtenir et revalider les informations ATMARP sur les autres membres IP dans le LIS (le choix du serveur est discuté au paragraphe 8.6). Comme noté au paragraphe 5.2, les clients ATMARP DOIVENT être configurés avec l'adresse ATM du serveur approprié avant l'opération du client ATMARP.

Les clients IP DOIVENT enregistrer leur adresse ATM de point d'extrémité auprès de leur serveur ATMARP en utilisant la structure d'adresse ATM appropriée pour leur connexion réseau ATM ; c'est-à-dire que les mises en œuvre de LIS sur des LAN ATM suivant UNI 3.1 devraient s'enregistrer en utilisant la structure 1 ; les mises en œuvre de LIS sur un réseau E.164 "public" ATM devraient s'enregistrer en utilisant la structure 2. Une mise en œuvre de LIS sur une combinaison de LAN ATM et de réseaux publics ATM peut devoir s'enregistrer en utilisant la structure 3. Les mises en œuvre fondées sur le présent mémoire DOIVENT prendre en charge les trois structures d'adresse ATM. Voir au paragraphe 8.7.1 les détails concernant le format de paquet de demande ATMARP.

Pour traiter le cas où un client a plus d'une adresse IP dans un LIS, quand il utilise un serveur ATMARP, le client DOIT enregistrer chacune de ces adresses.

Pour l'enregistrement initial et les rafraîchissements suivants de ses propres information auprès du service ATMARP, les clients DOIVENT :

1. Établir une connexion de VC LLC/SNAP avec un serveur dans le service ATMARP afin de transmettre et recevoir des paquets ATMARP.

Note : dans le cas de rafraîchissement de ses propres informations au service ATMARP, un client PEUT réutiliser une connexion établie existante avec le service ATMARP pourvu que la connexion ait été précédemment utilisée soit pour enregistrer initialement ses informations au service ATMARP, soit pour rafraîchir ses informations avec le service ATMARP.

2. Après l'établissement réussi d'une connexion au service ATMARP, le client DOIT transmettre un paquet ATMARP_Request, demandant une adresse ATM cible pour sa propre adresse IP comme adresse IP cible. Le client vérifie la ATMARP_Reply et si les adresses de source de matériel et de protocole correspondent aux adresses respectives de matériel et protocole cibles, le client est enregistré auprès du service ATMARP. Si les adresses ne correspondent pas, le client PEUT avoir une action, soulever des alarmes, etc. ; cependant, ces actions sortent du domaine d'application du présent mémoire. Dans le cas d'un client qui a plus d'une adresse IP dans la liste, cette étape DOIT être répétée pour chaque adresse IP.

3 Les clients DOIVENT répondre aux paquets ATMARP_Request et InATMARP_Request reçus sur tout VC de façon appropriée. (Voir la Section 7, "Fonctionnement du protocole" dans la [RFC1293].)

Note : pour des raisons de robustesse, les clients DOIVENT répondre aux ATMARP_Request.

4. Générer et transmettre les paquets de demande de résolution d'adresse au service de résolution d'adresse. Répondre aux

paquets de réponse de résolution d'adresse de façon appropriée pour construire/rafraîchir ses propres entrées de tableau ATMARP de client.

5. Générer et transmettre les paquets InATMARP_Request comme nécessaire et traiter les paquets InATMARP_Reply de façon appropriée. Les paquets InATMARP_Reply devraient être utilisés pour construire/rafraîchir ses propres entrées de tableau ATMARP de client. (Voir la Section 7, "Fonctionnement du protocole" de la [RFC1293].) Si un client a plus d'une adresse IP dans le LIS quand une demande InATMARP est reçue, une réponse InATMARP DOIT être générée pour chacune de ces adresses.

Le client DOIT rafraîchir ses informations ATMARP au serveur au moins une fois toutes les 15 minutes. Ceci est fait en répétant les étapes 1 et 2.

Un client ATMARP DOIT avoir connaissance de tous les VC ouverts qu'il a (permanents ou commutés) de leur association à une entrée de tableau ATMARP, et en particulier, quels VC prennent en charge l'encapsulation de LLC/SNAP.

8.5.1 Péremption de tableau de client ATMARP

Les entrées de tableau ATMARP de client sont valides pendant une durée maximum de 15 minutes.

Quand une entrée de tableau ATMARP a vieilli, un client ATMARP DOIT invalider l'entrée de tableau. Si il n'y a pas de serveur de VC ouvert associé à l'entrée invalidée, cette entrée est supprimée. Dans le cas d'une entrée invalidée et d'un VC ouvert, le client DOIT revalider l'entrée avant de transmettre tout trafic non de résolution d'adresse sur ce VC ; cette exigence s'applique aux PVC et aux SVC. Note : il est permis au client de revalider une entrée de tableau ATMARP avant qu'elle soit périmée, réinitialisant donc le temps de vieillissement quand l'entrée de tableau est revalidée avec succès. Le client PEUT continuer d'utiliser le VC ouvert, tant que l'entrée de tableau n'est pas périmée, alors que la revalidation est en cours.

Dans le cas d'un PVC ouvert, le client revalide l'entrée en transmettant une demande InATMARP et en mettant à jour l'entrée à réception d'une réponse InATMARP.

Dans le cas d'un SVC ouvert, le client revalide l'entrée en interrogeant le service de résolution d'adresse. Si une réponse valide est reçue (par exemple, ATMARP_Reply) l'entrée est mise à jour. Si le service de résolution d'adresse ne peut pas résoudre l'entrée (c'est-à-dire, "hôte non trouvé") le SVC devrait être fermé et l'entrée de tableau associée supprimée. Si le service de résolution d'adresse n'est pas disponible (c'est-à-dire, "échec de serveur") et si le SVC est encapsulé dans LLC/SNAP, le client DOIT tenter de revalider l'entrée en transmettant une InATMARP_Request sur ce VC et en mettant l'entrée à jour à réception d'une InATMARP_Reply. Si la tentative de InATMARP_Request échoue à retourner une InATMARP_Reply, le SVC devrait être fermé et l'entrée de tableau associée supprimée.

Si un VC avec une entrée de tableau ATMARP associé invalidée est fermé, cette entrée de tableau est supprimée.

8.5.2 Opérations anormales de VC

Les détails spécifiques des procédures de client pour détecter un établissement ou clôture de connexion de VC anormal, ou des échecs de communication sur un VC établi sortent du domaine d'application du présent mémoire. Il est EXIGÉ cependant que le client supprime l'entrée ATMARP associée pour un VC qui échoue à fonctionner correctement, comme défini par le client, quand le client ferme ce VC, quand il libère les ressources pour un VC, ou avant toute tentative de rouvrir ce VC. Ce comportement EXIGE spécifiquement que le client rafraîchisse ses informations de tableau ATMARP avant toute tentative de rétablir la communication avec un membre IP après qu'un problème de communications anormales s'est produit sur un VC avec ce membre IP.

8.5.3 Utilisation de ATMARP dans des scénarios IP mobile

Quand un LIS ATM est utilisé comme réseau de rattachement dans un scénario IP mobile, il est RECOMMANDÉ que l'agent de rattachement NE conserve PAS de connexions à long terme avec le service ATMARP. L'absence de ce VC va permettre que l'enregistrement d'un nœud mobile, après son retour au réseau de rattachement, préempte immédiatement l'enregistrement gratuit précédent de l'agent de rattachement.

8.6 Choix du serveur de résolution d'adresse

Si le client prend en charge seulement les PVC, la liste de serveurs ATMARP est vide et le client NE DOIT PAS générer de

demande de résolution d'adresse autre qu'une demande InATMARP sur un PVC nécessaire pour valider ce PVC.

Si le client prend en charge les SVC, le client DOIT alors avoir une atm$arp-req-list non NULLE pointant sur le ou les serveurs ATMARP qui fournissent le service ATMARP pour le LIS.

Le client DOIT s'enregistrer auprès d'un serveur figurant dans la atm$arp-req-list.

Le client DEVRA tenter de communiquer avec un des serveurs jusqu'à ce qu'un enregistrement réussi soit réalisé. L'ordre dans lequel le client choisit les serveurs pour tenter l'enregistrement est une affaire locale, comme l'est le nombre d'essais et les temporisations pour ces tentatives.

8.6.1 Des PVC aux serveurs ATMARP

Dans un environnement mixte de LIS PVC et SVC, un client ATMARP PEUT avoir un PVC avec un serveur ATMARP. Dans ce cas, ce PVC est utilisé pour les demandes et réponses ATMARP comme si il y avait un SVC établi. Note : si ce PVC est à utiliser pour du trafic IP, le serveur ATMARP DOIT alors être prêt à accepter et répondre de façon appropriée au trafic InATMARP.

8.7 Formats de paquet ATMARP

Les adresses Internet sont allouées indépendamment des adresses ATM. Chaque mise en œuvre d'hôte DOIT connaître sa ou ses propres adresses IP et ATM et DOIT répondre aux demandes de résolution d'adresse de façon appropriée. Les membres IP DOIVENT aussi utiliser ATMARP et InATMARP pour résoudre les adresses IP en adresses ATM quand nécessaire.

Note : le format de paquet ATMARP présenté dans le présent mémoire est de nature générale en ce que les champs Numéro ATM et Sous adresse ATM DEVRAIENT se transposer directement en les champs UNI 3.1 correspondants utilisés pour les messages de signalisation d'établissement d'appel/connexion ATM. Le groupe de travail IP sur ATM s'attend à ce que les numéros NSAPA de l'ATM (structure 1) prennent le pas sur les numéros E.164 (structure 2) comme identifiants de point d'extrémité ATM dans les LAN ATM. La spécification d'acheminement de VC de l'ATM Forum n'est pas complète pour l'instant et donc son impact sur l'utilisation opérationnelle de la structure 3 d'adresse ATM n'est pas défini. L'ATM Forum va définir cette relation à l'avenir. C'est pour cette raison que les membres IP doivent prendre en charge les trois structures d'adresse ATM.

8.7.1 Formats de paquet de demande et réponse ATMARP/InATMARP

Les protocoles de demande et réponse ATMARP et InATMARP utilisent les mêmes formats de données de type de matériel (ar$hrd), type de protocole (ar$pro), et code d'opération (ar$op) que les protocoles ARP et InARP [RFC0826], [RFC1293]. Les localisations de ces trois champs dans le paquet ATMARP sont dans les mêmes positions d'octets que dans les paquets ARP et InARP. Une valeur unique de type de matériel a été allouée pour ATMARP. De plus, ATMARP utilise un code d'opération supplémentaire pour ARP_NAK. Le reste du format de paquet ATMARP/InATMARP est différent du format de paquet ARP/InARP.

Les protocoles ATMARP et InATMARP ont plusieurs champs qui ont le format et les valeurs suivantes :

Données :

ar$hrd	16 bits	type de matériel
ar$pro	16 bits	type de protocole
ar$shtl	8 bits	type & longueur (TL) de numéro ATM de source (q)
ar$sstl	8 bits	type & longueur (TL) de sous adresse ATM de source (r)
ar$op	16 bits	code d'opération (demande, réponse, ou NAK)
ar$spln	8 bits	longueur d'adresse de protocole de source (s)
ar$thtl	8 bits	type & longueur (TL) de numéro ATM cible (x)
ar$tstl	8 bits	type & longueur (TL) de sous adresse ATM cible (y)
ar$tpln	8 bits	longueur d'adresse de protocole de cible (z)
ar$sha	q octets de numéro ATM de source	
ar$ssa	r octets de sous adresse ATM de source	
ar$spa	s octets d'adresse de protocole de source	
ar$tha	x octets de numéro ATM cible	
ar$tsa	y octets de sous adresse ATM cible	

ar$tpa z octets d'adresse de protocole de cible

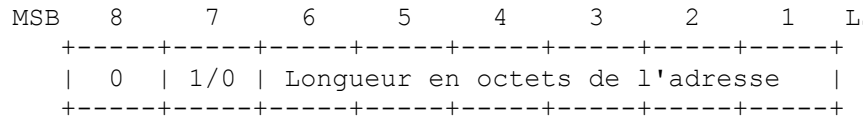
Où :
ar$hrd - alloué à la famille d'adresse ATM Forum et est 19 décimal (0x0013) [RFC1700].
ar$pro - voir les numéros alloués pour le numéro de type de protocole pour l'utilisation de ATMARP. (IP est 0x0800).
ar$shtl - type et longueur du numéro ATM de source. Voir les détails de codage de TL au paragraphe 8.7.4.
ar$sstl - type et longueur de sous adresse ATM de source. Voir les détails de codage de TL au paragraphe 8.7.4.
ar$op - valeur de type d'opération (en décimal) :
ATMARP_Request = ARP_REQUEST = 1
ATMARP_Reply = ARP_REPLY = 2
InATMARP_Request = InARP_REQUEST = 8
InATMARP_Reply = InARP_REPLY = 9
ATMARP_NAK = ARP_NAK = 10
ar$spln - longueur en octets de l'adresse de protocole de source. Valeur 0 ou 4 (décimal). Pour IPv4 ar$spln est 4.
ar$thtl - type et longueur de numéro ATM cible. Voir les détails de codage de TL au paragraphe 8.7.4.
ar$tstl - type et longueur de sous adresse ATM cible. Voir les détails de codage de TL au paragraphe 8.7.4.
ar$tpln - longueur en octets de l'adresse de protocole cible . Valeur 0 ou 4 (décimal). Pour IPv4 ar$tpln est 4.
ar$sha - numéro ATM de source (E.164 ou NSAPA ATM Forum)
ar$ssa - sous adresse ATM de source (NSAPA ATM Forum)
ar$spa - adresse de protocole de source
ar$tha - numéro ATM cible (E.164 ou NSAPA ATM Forum)
ar$tsa - sous adresse ATM cible (NSAPA ATM Forum)
ar$tpa - adresse de protocole cible

8.7.2 Réception de paquets ATMARP inconnus

Si un client ATMARP reçoit un message ATMARP avec un code d'opération (ar$op) qu'il n'est pas codé à prendre en charge, il DOIT éliminer le message en douceur et continuer le fonctionnement normal. Il N'EST PAS EXIGÉ d'un client ATMARP qu'il retourne de message à l'envoyeur du message non pris en charge.

8.7.3 Codage de TL, de numéro ATM, et de sous adresse ATM

Le codage des champs de 8 bit TL (type et longueur) dans les paquets ATMARP et In_ATMARP est le suivant :



Où :
bit 8 (réservé) = 0 (pour utilisation future).
bit 7 (type) = 0 : format NSAPA d'ATM Forum ; = 1 : format E.164.
bits 6 à 1 (longueur) = longueur en octets de 6 bits non signée de l'adresse (MSB = bit 6, LSB = bit 1) La gamme des valeurs est de 0 à 20 (décimal).

Les adresses ATM, comme défini par la spécification de signalisation UNI 3.1 de l'ATM Forum [ATMUNI], incluent un élément d'information "Numéro d'appelant" et un élément d'information "Sous adresse de l'appelant". Ces IE DEVRAIENT se transposer respectivement en numéro ATM de source ATMARP/InATMARP et en sous adresse ATM de source. De plus, le Forum ATM définit un élément d'information "Numéro d'appelé" et un élément d'information "Sous adresse de l'appelé". Ces IE se transposent respectivement en numéro ATM cible ATMARP/InATMARP et sous adresse ATM cible.

Le Forum ATM définit trois structures pour l'utilisation combinée des numéros et sous adresses [ATMUNI] :

	Numéro ATM	**Sous adresse ATM**
Structure 1	NSAPA ATM Forum	nulle
Structure 2	E.164	nulle
Structure 3	E.164	NSAPA ATM Forum

Les demandes et réponses ATMARP et InATMARP pour les structures d'adresse ATM 1 et 2 DOIVENT indiquer une sous adresse ATM nulle ou inconnue en réglant la longueur de sous adresse appropriée à zéro ; c'est-à-dire, ar$sstl.length = 0 ou ar$tstl.length = 0, le champ de type correspondant (ar$sstl.type ou ar$tstl.type) DOIT être ignoré et l'espace physique pour la mémoire tampon de sous adresse ATM NE DOIT PAS être alloué dans le paquet ATMARP. Par exemple, si

ar$sstl.length=0, la mémorisation pour la sous adresse ATM de source n'est pas allouée et le premier octet de l'adresse de protocole de source ar$spa suit immédiatement après le dernier octet de l'adresse de matériel de source ar$sha dans le paquet.

Les adresses ATM nulles ou inconnues DOIVENT être indiquées en réglant la longueur d'adresse appropriée à zéro ; c'est-à-dire, ar$shtl.length et ar$thtl.length sot zéro et le champ de type correspondant (ar$sstl.type ou ar$tstl.type) DOIT être ignoré et l'espace physique pour la mémoire tampon d'adresse ou sous adresse ATM NE DOIT PAS être alloué dans le paquet ATMARP.

8.7.4 Format de paquet ATMARP_NAK

Le format de paquet ATMARP_NAK est le même que le format de paquet ATMARP_Request reçu avec le code d'opération réglé à ARP_NAK, c'est-à-dire que les données du paquet ATMARP_Request sont copiées exactement (par exemple, en utilisant bcopy) pour la transmission avec le code d'opération ATMARP_Request changé en la valeur ARP_NAK.

8.7.5 Exigences de longueur variable pour paquets ATMARP

Les paquets ATMARP et InATMARP sont de longueur variable.

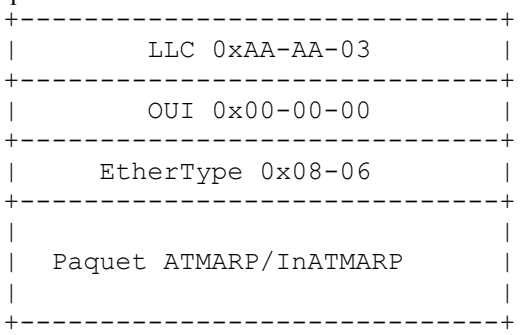
Une adresse de protocole de source ou de cible nulle ou inconnue est indiquée par la longueur correspondante réglée à zéro ; par exemple, quand ar$spln ou ar$tpln est zéro, l'espace physique pour la structure d'adresse correspondante NE DOIT PAS être allouée dans le paquet.

Pour la rétro compatibilité avec les mises en œuvre précédentes, une adresse de protocole IPv4 nulle peut être reçue avec longueur = 4 et une adresse allouée dans la mémorisation réglée à la valeur 0.0.0.0. Les stations receveuses DOIVENT être libérales en acceptant ce format d'adresse IPv4 nulle. Cependant, en transmettant un paquet ATMARP ou InATMARP, une adresse IPv4 nulle DOIT seulement être indiquée par la longueur réglée à zéro et NE DOIT PAS avoir de mémorisation allouée.

8.8 Encapsulation de paquet ATMARP/InATMARP

Les paquets ATMARP et InATMARP sont à coder en PDU AAL5 en utilisant l'encapsulation LLC/SNAP. Le format du champ de charge utile CPCS-SDU AAL5 pour les PDU ATMARP/InATMARP est :

Format de charge utile pour les PDU ATMARP/InATMARP :



La valeur de LLC de 0xAA-AA-03 (3 octets) indique la présence d'un en-tête SNAP.

La valeur de OUI de 0x00-00-00 (3 octets) indique que les deux octets qui suivent décrivent un EtherType.

La valeur d'EtherType de 0x08-06 (2 octets) indique ARP [RFC1700].

La taille totale de l'en-tête LLC/SNAP est fixée à 8 octets. Cela aligne le début du paquet ATMARP sur une frontière de 64 bits par rapport au début de la CPCS-SDU AAL5.

L'encapsulation LLC/SNAP pour ATMARP/InATMARP présentée ici est cohérente avec le traitement de l'encapsulation multi protocoles de IP sur ATM AAL5 comme spécifié dans la [RFC1483] et avec le format de ATMARP sur réseaux IEEE 802 comme spécifié dans la [RFC1042].

Traditionnellement, les demandes de résolution d'adresse sont diffusées à tous les membres IP directement connectés au sein d'un LIS. Il est concevable à l'avenir que des réseaux ATM de plus grande portée puissent traiter des demandes ATMARP pour des destinations en dehors du LIS d'origine, peut-être même mondialement ; les questions soulevées par l'utilisation de ATMARP en dehors du LIS ou par un mécanisme ATMARP mondial sortent du domaine d'application du présent mémoire.

9. Adresse de diffusion IP

ATM ne prend pas en charge l'adressage de diffusion, donc il n'y a pas de transposition disponible des adresses de diffusion IP en services de diffusion ATM. Note : cette absence de transposition n'empêche pas les membres de transmettre ou recevoir des datagrammes IP spécifiant une des quatre formes standard d'adresse de diffusion IP comme décrit dans la [RFC1122]. Les membres, à réception d'une diffusion IP ou d'une diffusion de sous réseau pour leur LIS, DOIVENT traiter le paquet comme si il était adressé à cette station.

Le présent mémoire reconnaît le futur développement de normes et mises en œuvre qui vont étendre les opérations comme défini dans le présent mémoire pour fournir une capacité de diffusion IP à l'usage du client classique.

10. Adresse de diffusion groupée IP

ATM ne prend pas directement en charge les services d'adresse de diffusion groupée IP, donc il n'y a pas de transposition disponible des adresses de diffusion groupée IP en services de diffusion groupée ATM. Les mises en œuvre courantes de diffusion groupée IP (c'est-à-dire, MBONE et le tunnelage IP, voir la [RFC1112]) vont continuer de fonctionner sur les sous réseaux logiques IP fondés sur ATM si ils opèrent dans la configuration de WAN.

Le présent mémoire reconnaît les futurs développements d'adressage de service de diffusion groupée ATM par le Forum ATM. Quand il sera disponible et largement mis en œuvre, le passage de l'architecture actuelle de diffusion groupée IP à cette nouvelle architecture ATM sera direct.

Le présent mémoire reconnaît le futur développement de normes et de mises en œuvre qui vont étendre les opérations comme définies dans le présent mémoire pour fournir une capacité de diffusion groupée IP à l'usage du client classique.

11. Considérations sur la sécurité

Toutes les questions de sécurité relatives à IP sur ATM ne sont pas clairement comprises pour l'instant, dû à l'état fluide des spécifications ATM, de la nouveauté de la technologie et d'autres facteurs.

Il est estimé que les facilités de ATM et d'IP pour authentifier la gestion d'appel, les communications authentifiées de bout en bout, et le chiffrement des données vont être nécessaires dans les réseaux ATM connectés mondialement. De telles facilités de sécurité futures et leur utilisation par les réseaux IP sortent du domaine d'application du présent mémoire.

Il y a des questions de sécurité connues relatives à l'usurpation d'identité d'hôte via les protocoles de résolution d'adresse utilisés dans l'Internet [TCPSEC]. Aucun mécanisme de sécurité particulier n'a été ajouté au mécanisme de résolution d'adresse défini ici pour être utilisé avec les réseaux IP sur ATM.

12. Spécification de MIB

Les clients construits sur la présente spécification DOIVENT mettre en œuvre et fournir une base de données d'informations de gestion (MIB, *Management Information Base*) comme défini dans "Définitions des objets gérés pour IP et ARP classiques sur ATM avec SMIv2" [RFC2320].

13. Questions ouvertes

- Les services de configuration automatique des adresses de client ATM via DHCP [RFC1541] ou via l'interface de gestion locale intérimaire (ILMI, *Interim Local Management Interface*) ATM UNI 3.1 seraient une extension de service utile au présent document et devraient être traités dans un document distinct.

- Les paquets ATMARP ne sont pas authentifiés. C'est une faille potentiellement sérieuse du système global qui permet un mécanisme par lequel des informations corrompues peuvent être introduites dans le système serveur.

14. Références

[ATMUNI] ATM Forum, "ATM User-Network Interface (UNI) Specification Version 3.1.", ISBN 0-13-393828-X, Prentice-Hall, Inc., Upper Saddle River, NJ, 07458, septembre 1994.

[FRAG] Kent C., et J. Mogul, "Fragmentation Considered Harmful", Proceedings of the ACM SIGCOMM '87 Workshop on Frontiers in Computer Communications Technology, août 1987.

[I.363] CCITT, "Draft Recommendation I.363", CCITT Study Group XVIII, Geneva, 19-29 janvier 1993.

[Q.93B] CCITT, "Draft text for Q.93B", CCITT Study Group XI, 23 septembre - 2 octobre 1992.

[RFC0826] D. Plummer, "Protocole de résolution d'adresses Ethernet : conversion des adresses de protocole réseau en adresses Ethernet à 48 bits pour transmission sur un matériel Ethernet", STD 37, novembre 1982.

[RFC1112] S. Deering, "Extensions d'hôte pour diffusion groupée sur IP", STD 5, août 1989. *(Mise à jour par la* RFC2236*)*

[RFC1122] R. Braden, "Exigences pour les hôtes Internet – couches de communication", STD 3, octobre 1989. *(MàJ par* RFC6633, 8029)

[RFC1191] J. Mogul et S. Deering, "Découverte de la MTU de chemin", novembre 1990.

[RFC1209] D. Piscitello et J. Lawrence, "Transmission de datagrammes IP sur le service SMDS", STD 52, mars 1991.

[RFC1237] R. Colella, E. Gardner et R. Callon, "Lignes directrices pour l'allocation de NSAP OSI dans l'Internet", juillet 1991. (*Obsolète, voir* RFC1629)

[RFC1293] T. Bradley et C. Brown, "Protocole de résolution inverse d'adresse", janvier 1992. *(Remplacée par* 2390*)*

[RFC1042] J. Postel et J. Reynolds, "Norme pour la transmission des datagrammes IP sur les réseaux IEEE 802", février 1988.

[RFC1435] S. Knowles, "Avis de l'IESG d'une expérience avec découverte de la MTU de chemin", mars 1993. *(Info)*

[RFC1483] Juha Heinanen, "Encapsulation multiprotocole sur couche 5 d'adaptation ATM", juillet 1993. *(remplacée par* 2684)

[RFC1541] R. Droms, "Protocole de configuration dynamique d'hôte", octobre 1993. *(P.S., remplacé par* 2131*)*

[RFC1700] J. Reynolds et J. Postel, "Numéros alloués", STD 2, octobre 1994. *(Historique, voir www.iana.org*))

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2320] M. Greene, J. Luciani, K. White, T. Kuo, "Définitions des objets gérés pour IP et ARP classiques sur ATM avec SMIv2 (IPOA-MIB)", avril 1998. *(P.S.)*

[TCPSEC] Bellovin, Steven M., "Security Problems in the TCP/IP Protocol Suite", ACM Computer Communications

Review, Vol. 19, Issue 2, pp. 32-48, 1989.

[UNI4.0] ATM Forum, "ATM User-Network Interface (UNI) Specification Version 4.0", ATM Forum specfication af-sig-0061.000, ftp://ftp.atmforum.com/, juillet 1996.

15. Adresse des auteurs

Mark Laubach
Com21, Inc.
750 Tasman Drive
Milpitas, CA 95035
USA
téléphone : 408.953.9175
Fax: 408.953.9299
mél : laubach@com21.com

Joel Halpern
Newbridge Networks, Inc.
593 Herndon Parkway
Herndon, VA 22070-5241
USA
téléphone : 703.736.5954
Fax : 703.736.5959
mél : jhalpern@Newbridge.com

Appendice A Informations sur les mises à jour

Le présent mémoire représente une mise à jour des RFC 1577 et RFC 1626. Les changements suivants sont inclus dans le présent mémoire :

- un pointeur sur la MIB I-D classique pour le réglage des variables,
- une seule adresse de serveur ATMARP pour la liste de serveurs ATMARP, configurable via la MIB,
- le texte de la RFC 1626 remplace la section sur la MTU,
- la procédure d'enregistrement de client de In_ATMARP pour la première demande ATMARP,
- précision de la longueur variable du format de paquet ATMARP,
- précision du format de paquet ARP_NAK,
- précision du format de paquet InATMARP pour les adresse IPv4 nulles,
- précision de l'enregistrement ATMARP et l'utilisation de InATMARP_Reply pour les clients qui ont plus d'une adresse IP dans un LIS.

Déclaration complète de droits de reproduction