Union internationale des télécommunications

UIT-T X.603.1

(02/2007)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Réseautage OSI et aspects systèmes – Réseautage

Technologies de l'information – Protocole de multidiffusion relayé: Spécification relative aux applications de groupe simplex

Recommandation UIT-T X.603.1

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	
Services et fonctionnalités	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalisation et commutation	X.50–X.89
Aspects réseau	X.90–X.149
Maintenance	X.150–X.179
Dispositions administratives	X.180–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	
Modèle et notation	X.200–X.209
Définitions des services	X.210–X.219
Spécifications des protocoles en mode connexion	X.220–X.229
Spécifications des protocoles en mode sans connexion	X.230–X.239
Formulaires PICS	X.240–X.259
Identification des protocoles	X.260–X.269
Protocoles de sécurité	X.270–X.279
Objets gérés des couches	X.280–X.289
Tests de conformité	X.290–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	
Généralités	X.300–X.349
Systèmes de transmission de données par satellite	X.350–X.369
Réseaux à protocole Internet	X.370–X.379
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	
Réseautage	**X.600–X.629**
Efficacité	X.630–X.639
Qualité de service	X.640–X.649
Dénomination, adressage et enregistrement	X.650–X.679
Notation de syntaxe abstraite numéro un (ASN.1)	X.680–X.699
GESTION OSI	
Cadre général et architecture de la gestion-systèmes	X.700–X.709
Service et protocole de communication de gestion	X.710–X.719
Structure de l'information de gestion	X.720–X.729
Fonctions de gestion et fonctions ODMA	X.730–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	
Engagement, concomitance et rétablissement	X.850–X.859
Traitement transactionnel	X.860–X.879
Opérations distantes	X.880–X.889
Applications génériques de l'ASN.1	X.890–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DES TÉLÉCOMMUNICATIONS	X.1000–

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

NORME INTERNATIONALE ISO/CEI 16512-2
RECOMMANDATION UIT-T X.603.1

Technologies de l'information – Protocole de multidiffusion relayé: Spécification relative aux applications de groupe simplex

Résumé

La présente Recommandation | Norme internationale décrit un protocole de la couche application permettant de construire une arborescence de multidiffusion pour la fourniture de données entre un expéditeur et plusieurs récepteurs sur l'Internet lorsque la multidiffusion IP n'est pas complètement déployée. Le protocole de multidiffusion relayé qui est spécifié comprend un agent de multidiffusion et un gestionnaire de session. La présente Recommandation | Norme internationale spécifie une série de fonctions et de procédures permettant à des agents de multidiffusion de construire un trajet de données relayées point à multipoint et de relayer des données simplex. Elle spécifie aussi le fonctionnement du gestionnaire de session pour la gestion de sessions de multidiffusion. Ce protocole peut être utilisé pour les applications nécessitant des services de fourniture de données point à multipoint tels que le service de transfert de flux continu multimédia, le service de diffusion de fichier, etc.

Source

La Recommandation UIT-T X.603.1 a été approuvée le 13 février 2007 par la Commission d'études 17 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8. Un texte identique est publié comme Norme Internationale ISO/CEI 16512-2.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas des renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Page

1 Domaine d'application 1
2 Références normatives 1
3 Définitions 1
4 Abréviations 2
5 Vue d'ensemble 3
5.1 Entités RMCP-2 3
5.2 Bloc de protocole RMCP-2 4
5.3 Modèle d'acheminement simplex du protocole RMCP-2 5
5.4 Types de messages RMCP-2 6
6 Fonctionnement du protocole 6
6.1 Fonctionnement du gestionnaire de session (SM) 6
6.2 Fonctionnement de l'agent de multidiffusion (MA) 8
7 Format des messages RMCP-2 19
7.1 Format commun des messages RMCP-2 19
7.2 Format des données de commande 21
7.3 Messages 22
8 Paramètres 47
8.1 Profil de retransmission de données 47
8.2 Paramètres utilisés dans le protocole RMCP-2 47
8.3 Règles de codage pour représenter les valeurs utilisées dans le protocole RMCP-2 48
Annexe A – Algorithme de configuration de l'arborescence 52
A.1 Règle d'amorçage 52
A.2 Règle de découverte des voisins 53
A.3 Règle de sélection de l'agent HMA 54
A.4 Règle d'acceptation d'agent CMA 54
A.5 Règle de décision concernant le parent 55
A.6 Règle d'amélioration de l'arborescence 56
A.7 Règle d'expulsion par l'agent PMA 56
Annexe B – Mécanisme de fourniture de données en temps réel 57
B.1 Aperçu 57
B.2 Mécanisme de tunnellisation IP-IP pour la fourniture de données en temps réel RMCP-2 57
Annexe C – Mécanisme de fourniture de données fiables 59
C.1 Aperçu 59
C.2 Fonctionnement 59
C.3 Format d'encapsulation des données 61
C.4 Profil de données 61
Annexe D – Interfaces API RMCP-2 62
D.1 Aperçu 62
D.2 Fonctions API RMCP-2 63

Introduction

La partie 2 du protocole de multidiffusion relayé (RMCP-2) est un protocole de multidiffusion relayé de la couche application destiné aux applications de groupe simplex. Le protocole RMCP-2 permet d'établir un trajet d'acheminement en mode multidiffusion relayée point à multipoint, optimisé et robuste, sur un réseau de monodiffusion, avec l'aide d'entités RMCP définies dans la Rec. UIT-T X.603 | ISO/CEI 16512-1.

Une session RMCP-2 est constituée d'un gestionnaire de session et d'un ou de plusieurs agents de multidiffusion; le gestionnaire de session démarre et termine la session RMCP-2 et gère la session RMCP-2 ainsi que les agents de multidiffusion participants. Le MA configure une arborescence RMCP-2 pour libérer des données de groupe en échangeant une série de messages de commande RMCP-2.

Le long du trajet d'acheminement en mode multidiffusion relayée, plusieurs types de canaux d'acheminement de données peuvent être mis en place conformément aux exigences des services d'application.

NORME INTERNATIONALE
RECOMMANDATION UIT-T

Technologies de l'information – Protocole de multidiffusion relayé: Spécification relative aux applications de groupe simplex

1 Domaine d'application

La présente Recommandation | Norme internationale décrit la partie 2 du protocole de multidiffusion relayé (RMCP), protocole de la couche application qui permet de construire une arborescence de multidiffusion pour la fourniture de données entre un expéditeur et plusieurs récepteurs sur l'Internet lorsque la multidiffusion IP n'est pas complètement déployée. Le protocole de multidiffusion relayé qui est spécifié comprend un agent de multidiffusion et un gestionnaire de session. La présente Recommandation | Norme internationale spécifie une série de fonctions et de procédures permettant à un agent de multidiffusion de construire un trajet de données relayées point à multipoint et de relayer des données simplex. Il spécifie également le fonctionnement du gestionnaire de session pour la gestion de sessions de multidiffusion. Ce protocole peut être utilisé pour les applications nécessitant des services d'acheminement de données point à multipoint tels que le service de transfert de flux continu multimédia, le service de diffusion de fichier, etc.

2 Références normatives

Les Recommandations et Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation | Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes Recommandations et Normes sont sujettes à révision et les parties prenantes aux accords fondés sur la présente Recommandation | Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Bureau de la normalisation des télécommunications de l'UIT tient à jour une liste des Recommandations de l'UIT-T en vigueur.

- Recommandation UIT-T X.601 (2000), *Cadre général des communications entre homologues multiples*.
- Recommandation UIT-T X.603 (2004) | ISO/CEI 16512-1:2005, *Technologies de l'information – Protocole de multidiffusion relayé: cadre général*.
- Recommandation UIT-T X.605 (1998) | ISO/CEI 13252:1999, *Technologies de l'information – Définition du service de transport de communications amélioré.*
- Recommandation UIT-T X.606 (2001) | ISO/CEI 14476-1:2002, *Technologies de l'information – Protocole de transport de communications amélioré: spécification du transport simplex en multidiffusion.*
- Recommandation UIT-T X.606.1 (2003) | ISO/CEI 14476-2:2003, *Technologies de l'information – Protocole de transport de communications amélioré: spécification de la gestion de la qualité de service pour le transport simplex en multidiffusion.*

3 Définitions

Pour les besoins de la présente Recommandation | Norme internationale, les définitions suivantes s'appliquent:

3.1 multidiffusion: système d'acheminement de données dans lequel la même unité de données est transmise à partir d'une source unique vers des destinations multiples, au cours d'une seule et même invocation de service.

3.2 multidiffusion IP: système de multidiffusion sur le réseau IP, avec l'appui de plusieurs routeurs IP avec multidiffusion activée.

3.3 multidiffusion relayée: système d'acheminement de données en mode multidiffusion qui peut être utilisé dans des environnements de monodiffusion. Le système est fondé sur des agents de multidiffusion intermédiaires qui relaient les données de multidiffusion entre un serveur média et des lecteurs médias sur une hiérarchie arborescente.

3.4 protocole de multidiffusion relayé (RMCP, *relayed multicast protocol*): protocole destiné à prendre en charge et à gérer le transport de données de multidiffusion relayé.

3.5 session RMCP-2*:* ensemble d'agents de multidiffusion qui utilise le protocole RMCP pour configurer le trajet d'acheminement des données.

3.6 agent de multidiffusion (MA): entité de transport de données intermédiaire utilisée pour relayer les données d'application de multidiffusion. En fonction du déploiement, un agent MA peut être installé sur le même système en tant que client de réception.

3.7 agent de multidiffusion expéditeur (SMA): agent de multidiffusion associé à un expéditeur dans le même système ou dans le même réseau local.

3.8 agent de multidiffusion récepteur (RMA): agent de multidiffusion associé à un récepteur dans le même système ou dans le même réseau local.

3.9 agent de multidiffusion principal (HMA): représentant de l'agent MA à l'intérieur d'un réseau local dans lequel la multidiffusion est activée.

3.10 gestionnaire de session (SM): entité RMCP responsable du fonctionnement global du protocole RMCP; peut être située dans le même système que le serveur média ou être située séparément de ce serveur.

3.11 agent de multidiffusion parent (PMA): agent de multidiffusion amont voisin sur le trajet d'acheminement des données RMCP-2.

3.12 agent de multidiffusion enfant (CMA): agent de multidiffusion aval voisin sur le trajet d'acheminement des données RMCP-2.

4 Abréviations

Pour les besoins de la présente Recommandation | Norme internationale, les abréviations suivantes s'appliquent:

AUTH	authentification (*authentication*)
CMA	agent de multidiffusion enfant (*child multicast agent*)
DMA	agent de multidiffusion spécialisé (*dedicated multicast agent*)
HANNOUNCE	message d'annonce HMA (*HMA announce message*)
HB	message de pulsation (*heartbeat message*)
HLEAVE	message de sortie HMA (*HMA leave message*)
HMA	agent de multidiffusion principal (*head multicast agent*)
HSOLICIT	message de sollicitation HMA (*HMA solicit message*)
IP-IP	IP dans IP (*IP in IP*)
LEAVANS	message de réponse de sortie (*leave answer message*)
LEAVREQ	message de demande de sortie (*leave request message*)
MA	agent de multidiffusion (*multicast agent*)
MAID	identification d'agent de multidiffusion (*multicast agent identification*)
PMA	agent de multidiffusion parent (*parent multicast agent*)
PPROBANS	message de réponse de sondage de parent (*parent probe answer message*)
PPROBREQ	message de demande de sondage de parent (*parent probe request message*)
RELANS	message de réponse de relais (*relay answer message*)
RELREQ	message de demande de relais (*relay request message)*
RMA	agent de multidiffusion récepteur (*receiver multicast agent*)
RMCP	protocole de multidiffusion relayé (*relayed multicast protocol*)
SDP	protocole de description de session (*session description protocol*)
SID	identification de session RMCP-2 (*RMCP-2 session identification*)
SMA	agent de multidiffusion expéditeur (*sender multicast agent*)
STANS	message de réponse de notification d'état (*status report answer message*)
STCOLANS	message de réponse de collecte de notification d'état (*status report collect answer message*)
STCOLREQ	message de demande de collecte de notification d'état (*status report collect request message*)
STREQ	message de demande de notification d'état (*status report request message*)
SUBSANS	message de réponse d'abonnement (*subscription answer message*)
SUBREQ	message de demande d'abonnement (*subscription request message*)

T/TCP	extensions TCP des transactions (*TCP extensions to transactions*)
TCP	protocole de commande de transmission (*transmission control protocol*)
TERMANS	message de réponse de terminaison (*termination answer message*)
TERMREQ	message de demande de terminaison (*termination request message*)
UDP	protocole datagramme d'utilisateur (*user datagram protocol*)

5 Vue d'ensemble

Le protocole RMCP-2 est un protocole au niveau application qui utilise des agents de multidiffusion (MA) et un gestionnaire de session (SM) pour prendre en charge et gérer le transport de données de multidiffusion relayé sur un réseau Internet fondé sur la monodiffusion. Avec l'aide du gestionnaire de session, le protocole RMCP-2 commence par construire une arborescence de commande de multidiffusion relayée comprenant des agents MA. Compte tenu de l'arborescence de commande préconfigurée, chaque agent MA connecte ensuite les canaux de données appropriés les uns avec les autres.

Les entités RMCP-2 dans le cas d'un modèle d'acheminement simplex sont décrites au § 5.1.

5.1 Entités RMCP-2

Les entités RMCP-2 sont les mêmes que celles qui sont décrites dans la partie 1 du protocole RMCP. Comme indiqué sur la Figure 1, chaque session RMCP-2 construit un modèle d'acheminement de données en mode multidiffusion relayé à l'aide des entités suivantes:

a) Un gestionnaire de session.

b) Un agent de multidiffusion expéditeur (SMA) par application expéditeur.

c) Un ou plusieurs agents de multidiffusion récepteurs (RMA).

d) Une ou plusieurs applications de groupe expéditeur ou récepteur.

Un gestionnaire de session peut assurer simultanément le bon déroulement d'une ou de plusieurs sessions. Il peut être implémenté séparément ou dans le cadre d'autres entités de session RMCP-2.

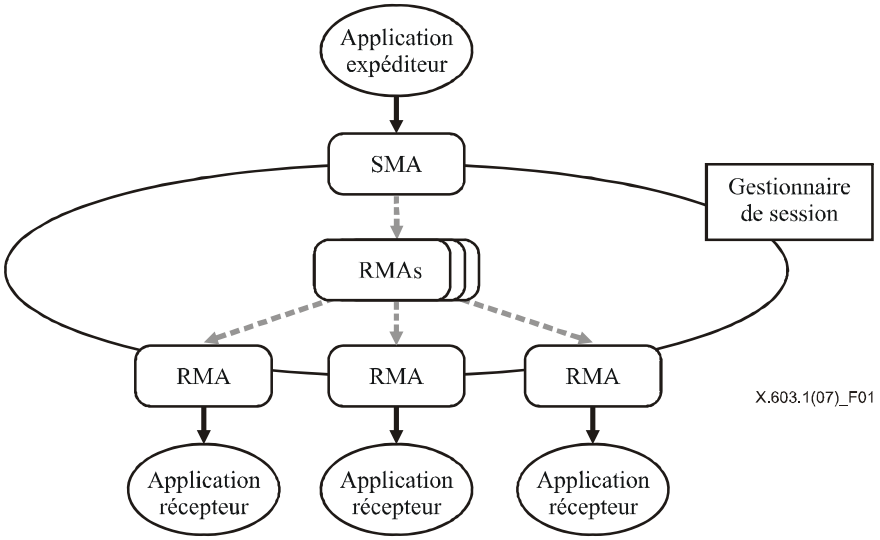

Figure 1 – Topologie de service RMCP-2

Un gestionnaire de session peut assurer les fonctions suivantes:

a) initialisation de la session;

b) libération de la session;

c) gestion des membres de la session;

d) suivi de l'état de la session.

Un agent de multidiffusion (MA), catégorie désignant à la fois l'agent SMA et l'agent RMA, établit un trajet d'acheminement en mode multidiffusion relayée entre un expéditeur et de nombreux récepteurs puis transmet les données le long du trajet établi. Il peut assurer les fonctions suivantes:

a) initialisation de la session;

b) entrée dans la session;

c) sortie de la session;

d) maintien de la session;

e) notification d'état de la session;

f) relais de données d'application.

5.2 Bloc de protocole RMCP-2

Un gestionnaire de session (SM) devrait échanger des messages de commande avec d'autres agents de multidiffusion (MA) et gérer une session RMCP-2. Les messages de commande utilisés par le gestionnaire de session devraient être acheminés de manière fiable, sans quoi la session RMCP-2 devient irrécupérable. La Figure 2 ci-après représente la pile de protocoles d'un gestionnaire de session.

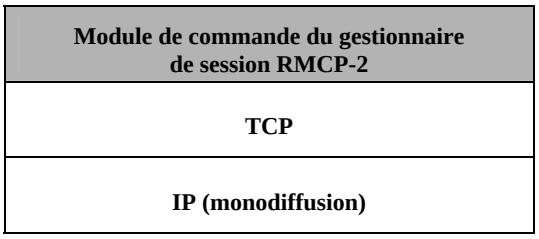

Figure 2 – Pile de protocoles d'un gestionnaire de session

Un agent de multidiffusion (MA), catégorie désignant à la fois l'agent SMA et l'agent RMA, établit un trajet d'acheminement en mode multidiffusion relayée entre un expéditeur et de nombreux récepteurs puis transmet les données le long du trajet établi. Un agent de multidiffusion est constitué d'un *module de commande* et d'un *module de transport de données RMCP-2*. Le module de commande établit le trajet d'acheminement de données relayées, tandis que le module de transport de données établit un canal de données le long du trajet établi par le module de commande puis relaie les données par le canal en question.

Le module de commande de l'agent de multidiffusion configure l'arborescence de commande depuis l'agent SMA vers chaque agent MA feuille en échangeant des messages de commande avec d'autres agents MA. Par ailleurs, le module de commande est utilisé pour la commande et la gestion de la session par le gestionnaire SM. La Figure 3 représente la pile de protocoles du module de commande d'un agent MA.

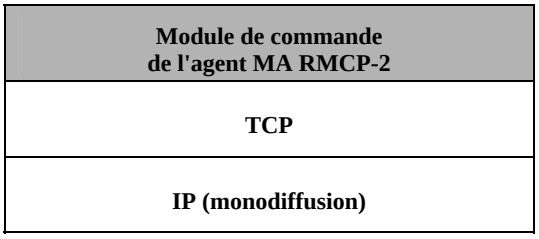

Figure 3 – Pile de protocoles du module de commande d'un agent de multidiffusion (MA)

Le module de données de l'agent MA relaie les données de l'application le long de l'arborescence configurée par le module de commande. La Figure 4 représente la pile de protocoles d'un module de données RMCP-2. Si c'est nécessaire, on peut insérer tout type de mécanisme de transport, étant donné que le protocole RMCP-2 n'impose aucune restriction quant au type de données d'application à transmettre.

Afin de veiller à ce que le protocole RMCP-2 puisse adopter tout type de mécanisme de transport de données, deux agents MA (à savoir l'agent de multidiffusion parent (PMA) et l'agent de multidiffusion enfant (CMA)) établissent un trajet d'acheminement des données sur l'arborescence de commande en échangeant les profils de données décrits ultérieurement.

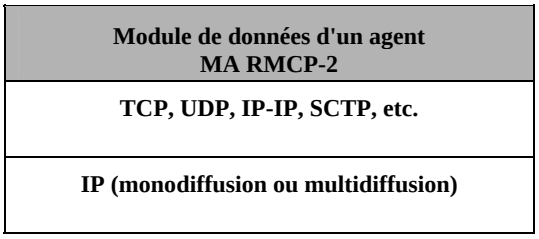

Figure 4 – Pile de protocoles d'un module de données RMCP-2

En général, les topologies des deux trajets pour la commande et la transmission de données sont les mêmes, étant donné qu'un trajet d'acheminement de données est établi le long de l'arborescence de commande RMCP-2. Le long du trajet d'acheminement des données, les données d'application provenant de l'agent SMA peuvent être acheminées vers chaque agent MA feuille. On trouvera davantage d'informations dans les Annexes B et C, qui présentent deux systèmes d'acheminement de données fiables et en temps réel pouvant être mis en œuvre.

5.3 Modèle d'acheminement simplex du protocole RMCP-2

Les services auxquels est destiné le protocole RMCP-2 sont les *services de radiodiffusion simplex* tels que la télévision Internet en direct et la diffusion de logiciels. Dans ces modèles de service, il est important d'établir un trajet d'acheminement des données optimal depuis un expéditeur vers plusieurs récepteurs. Le protocole RMCP-2 prend en charge un modèle d'acheminement des données simplex en utilisant le module de commande et le module de données de l'agent MA.

Le trajet d'acheminement des données pris en compte par le protocole RMCP-2 est une *arborescence de multidiffusion relayée pour chaque source*. Le long du trajet en mode multidiffusion relayée pour chaque source, il est possible d'établir un *canal de données unidirectionnel en temps réel ou fiable*. La Figure 5 représente l'une des arborescences de multidiffusion relayée susceptibles d'être configurées par le protocole RMCP-2 pour des *applications simplex en temps réel ou fiables*.

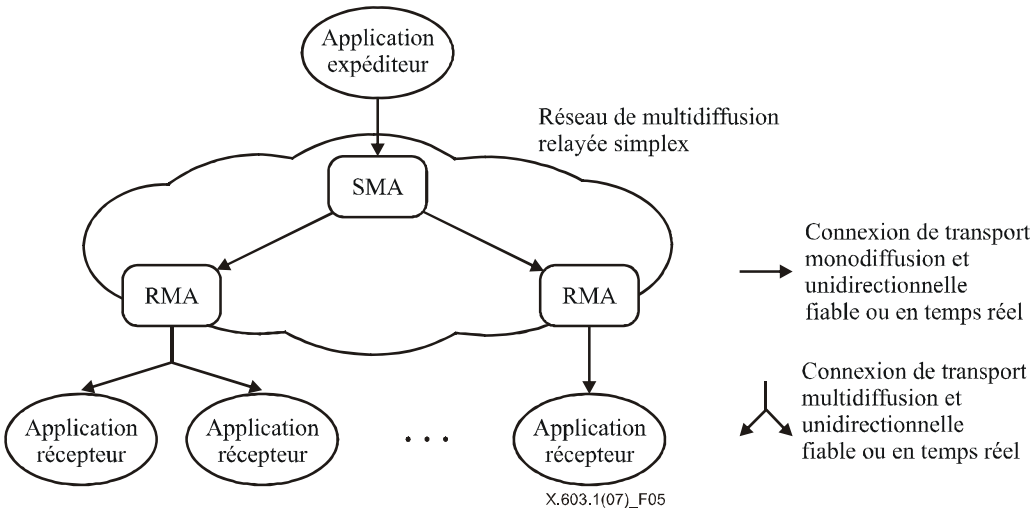

Figure 5 – Arborescence de multidiffusion relayée configurée par le protocole RMCP-2

5.4 Types de messages RMCP-2

Pour établir et maintenir une arborescence de multidiffusion relayée, plusieurs messages de commande sont échangés entre homologues RMCP-2 en mode *demande et réponse*. Le Tableau 1 énumère les messages de commande RMCP-2 selon les fonctions appropriées.

Tableau 1 – RMCP-2 messages

Messages	Descriptions	Opérations RMCP
SUBSREQ	Demande d'abonnement	Initialisation de la session
SUBSANS	Réponse d'abonnement	
PPROBREQ	Demande de sondage de parent	Découverte de carte
PPROBANS	Réponse de sondage de parent	
HSOLICIT	Sollicitation HMA	Choix de l'agent HMA
HANNOUNCE	Annonce HMA	
HLEAVE	Sortie HMA	
RELREQ	Demande de relais	Acheminement des données
RELANS	Réponse de relais	
STREQ	Demande de notification d'état	Surveillance de la session
STANS	Réponse de notification d'état	
STCOLREQ	Demande de collecte d'état	
STCOLANS	Réponse de collecte d'état	
LEAVREQ	Demande de sortie	Sortie de la session
LEAVANS	Réponse de sortie	
HB	Pulsation	Pulsation de session
TERMREQ	Demande de terminaison	Terminaison de session
TERMANS	Réponse de terminaison	

6 Fonctionnement du protocole

Le présent paragraphe décrit d'une manière détaillée les fonctions du protocole RMCP-2 et leur fonctionnement. Tous les composants présentés dans ce paragraphe sont conformes aux définitions de la Rec. UIT-T X.603 | ISO/CEI 16512-1.

6.1 Fonctionnement du gestionnaire de session (SM)

6.1.1 Ouverture de la session

Pour que le gestionnaire de session crée une nouvelle session, un fournisseur de contenu (CP, *content provider*) doit fournir un profil de session, qui donne des renseignements pour créer une session tels que le nom de la session, les caractéristiques de média et l'adresse de groupe. Pour différencier les sessions les unes des autres, le gestionnaire de session crée un identificateur de session (SID) unique. Après la création réussie d'une session, le gestionnaire de session retourne l'identificateur SID au fournisseur de contenu (CP). Les fournisseurs CP peuvent annoncer la création d'une session en utilisant un serveur web ou un système de messagerie électronique, mais les modalités d'annonce d'une session sortent du cadre de la présente spécification.

Une fois la création de la session réussie, le gestionnaire de session attend qu'une demande d'abonnement soit formulée par les agents MA. Lorsque le gestionnaire de session reçoit une demande d'abonnement d'un agent MA, il décide d'accepter ou non cette demande.

6.1.2 Contrôle d'admission

Lorsqu'il reçoit une demande d'abonnement d'un agent MA, le gestionnaire de session commence par vérifier l'identificateur SID dans le message de demande, puis il détermine si la demande est acceptable d'après la politique de la session. La session RMCP-2 peut être gérée aussi bien d'une manière privée que d'une manière publique, moyennant certains renseignements complémentaires tels que les informations sur le système et les informations d'authentification.

Lorsque l'identificateur SID se trouvant dans le message SUBSREQ de l'agent MA est valable, le gestionnaire de session vérifie l'identificateur MAID proposé et le profil de données proposé. Si l'identificateur MAID proposé par

l'agent MA a une valeur nulle ou déjà utilisée, le gestionnaire de session propose une valeur unique, sinon l'identificateur MAID proposé sera utilisé pendant la session. Si le profil de données proposé ne peut être pris en charge, le gestionnaire de session devrait rejeter la demande en en fournissant les motifs. Dans le cas contraire, le gestionnaire de session négocie le profil de données le plus efficace et retourne le profil négocié.

Lorsque le message SUBSREQ de l'agent MA est accepté, le gestionnaire de session répond avec un identificateur MAID confirmé, une liste de voisins et des informations dépendant de la session.

Pour expulser un agent MA donné, le gestionnaire de session engage la procédure de rejet en envoyant une demande de sortie (LEAVREQ) avec le code de motif expulsé (KO, *kicked-out*) puis met à jour la liste des membres de sa session. Dès réception du message LEAVREQ du gestionnaire de session, l'agent MA quitte rapidement la session. La Figure 6 illustre cette procédure, dans laquelle le gestionnaire de session envoie un message LEAVREQ avec le code de motif KO, puis l'agent MA B quitte la session en informant ses agents PMA et CMA de son expulsion.

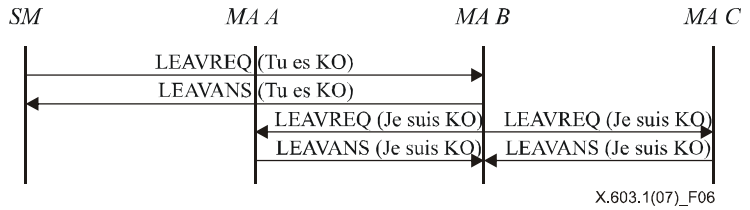

Figure 6 – Cas dans lequel un agent MA est expulsé par le gestionnaire de session

6.1.3 Surveillance de session

Le gestionnaire de session peut rechercher des informations d'état concernant un agent MA donné en échangeant avec lui des messages de demande et de réponse d'état. Dès qu'il reçoit le message de demande d'état, l'agent MA répond par un message de réponse d'état contenant les informations demandées. La Figure 7 illustre la manière dont le gestionnaire de session surveille un agent MA donné.

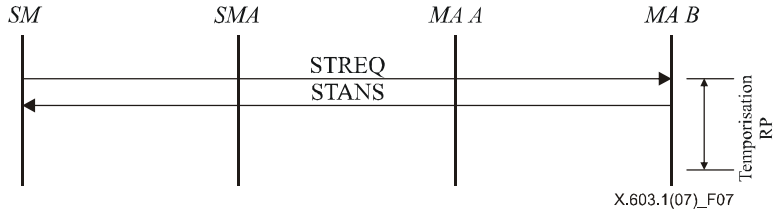

Figure 7 – Surveillance de l'arborescence – Notification d'état

Le gestionnaire de session peut également recueillir des informations d'état concernant la totalité ou une partie d'une session. En pareils cas, il envoie un message de demande de collecte d'état à l'agent MA situé au sommet de la partie de la session. Dès réception du message de demande de collecte d'état, l'agent MA devrait envoyer une réponse d'état au gestionnaire de session, avec des informations appropriées sur l'agent MA et ses enfants. Lorsque la taille de la session est importante, le recours à ce mécanisme pour la totalité de la session risque de causer une surcharge du réseau et des ressources système. Pour limiter la portée de la surveillance, le message de collecte d'état devrait contenir une option pour la profondeur.

6.1.4 Terminaison de la session

On peut mettre fin à la session en cours du gestionnaire de session pour deux raisons:

1) demande administrative; et
2) sortie de l'agent SMA.

La Figure 8 indique la procédure de terminaison de la session du gestionnaire de session.

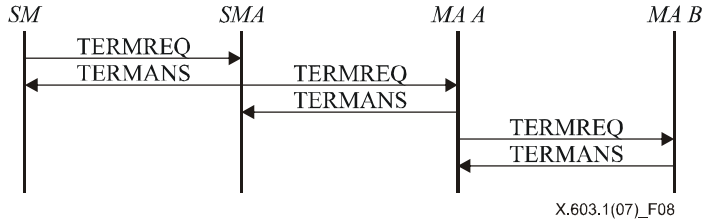

Figure 8 – Terminaison de la session par le gestionnaire de session

Etant donné qu'une session RMCP-2 ne peut se poursuivre que lorsque l'agent SMA est actif, celui-ci doit notifier sa sortie au gestionnaire de session. Une fois qu'il est informé de la sortie de l'agent SMA, le gestionnaire de session devrait rapidement mettre fin à la session. La terminaison de la session engendrée par la sortie de l'agent SMA sera décrite au § 6.2.4.4.

6.2 Fonctionnement de l'agent de multidiffusion (MA)

6.2.1 Abonnement à la session

L'abonnement constitue la première étape de l'inscription d'un agent MA à une session RMCP-2. Chaque agent MA doit s'abonner à la session en envoyant une demande d'abonnement (SUBSREQ) au gestionnaire de session. Il convient de noter que l'agent SMA doit avoir terminé son abonnement avant les autres agents MA et qu'il doit agir en tant que nœud racine dans la hiérarchie arborescente. A ce stade, chaque agent MA doit connaître en détail le profil de la session, par exemple l'adresse du gestionnaire de session et la politique.

La Figure 9 indique la procédure d'abonnement à la session RMCP-2. Une fois l'abonnement de l'agent SMA effectué, la session RMCP-2 peut être ouverte.

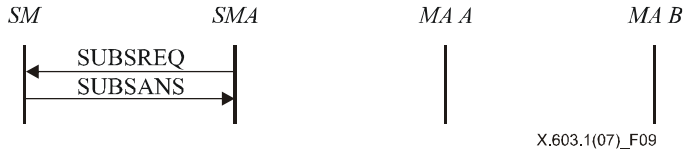

Figure 9 – Abonnement de l'agent SMA

La Figure 10 illustre la procédure d'abonnement d'un agent MA (pour les agents MA A et MA B). Pour s'abonner à une session RMCP-2, chaque agent MA envoie une demande SUBSREQ au gestionnaire de session. Dès réception de cette demande, le gestionnaire de session décide s'il accepte ou non la demande d'abonnement. Si la demande est acceptée, le gestionnaire de session répond en envoyant un message SUBSANS et des informations d'amorçage (par exemple une liste de voisins). Dans le cas contraire, il répond en envoyant un message SUBSANS avec un code de motif d'erreur approprié.

Après avoir reçu un message SUBSANS d'acceptation en provenance du gestionnaire de session, les agents MA (MA A et MA B) peuvent achever la phase d'abonnement.

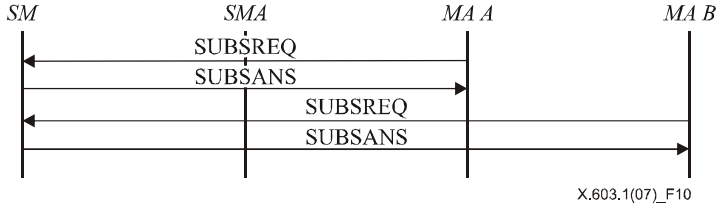

Figure 10 – Abonnement d'agent MA

6.2.2 Découverte de carte

Etant donné que les agents MA sont interconnectés de manière logique, ils éprouvent des difficultés à connaître l'état du réseau dans son intégralité. Toutefois, en utilisant des procédures de découverte de carte, chaque agent MA peut explorer d'autres agents MA dans le réseau RMCP-2 et mesurer la distance qui le sépare d'eux. Le mécanisme de découverte de carte comprend deux étapes. La première est utilisée dans la zone avec multidiffusion activée (par exemple un sous-réseau local) et la deuxième est utilisée à l'extérieur de cette zone (par exemple dans un réseau étendu).

6.2.2.1 A l'intérieur de la zone avec multidiffusion activée

Il est souhaitable d'assigner le nœud le plus proche à son agent PMA. Dans le protocole RMCP-2, la distance dans le réseau dépend de la gigue du temps de transmission, du décompte de sauts et de la largeur de bande.

En principe, un agent MA d'un même réseau est plus proche que les autres agents MA, chaque agent MA recherche un agent PMA possible dans son réseau local en acheminant par multidiffusion une sollicitation d'agent de multidiffusion principal (HSOLICIT) à une adresse spécifique assignée au préalable (radiodiffusion) dès le début. En l'absence de réponse, l'agent MA devient l'agent HMA, qui est un représentant de l'agent MA dans le réseau avec multidiffusion activée.

Une fois qu'un agent MA devient un agent HMA, celui-ci annonce son existence au réseau avec multidiffusion activée en envoyant des messages périodiques HANNOUNCE. L'agent HMA envoie rapidement un message HANNOUNCE dès réception d'un message HSOLICIT provenant de la zone avec multidiffusion activée.

Dès réception du message HANNOUNCE de l'agent HMA, chaque agent MA considère qu'un agent HMA existe déjà dans le même réseau et considère ensuite que l'agent HMA est son agent PMA possible primaire. La Figure 11 illustre la procédure de sélection de l'agent HMA.

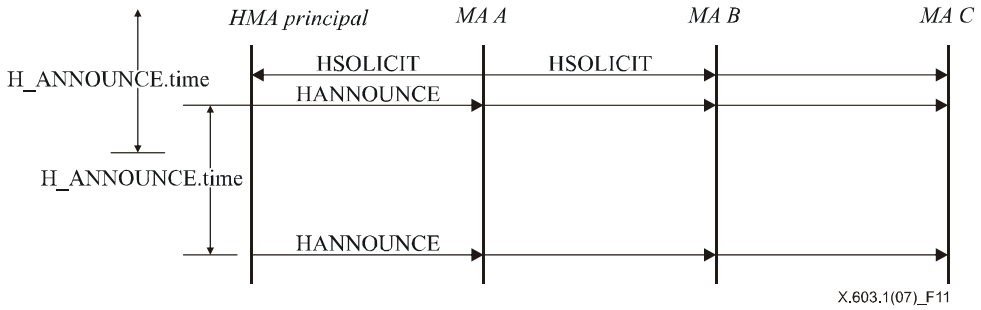

Figure 11 – Sollicitation d'agent HMA et annonce

La Figure 12 indique comment un agent MA devient un agent HMA. En l'absence de message HANNOUNCE pendant un certain temps (H_SOLICIT.time × N_SOLICIT), un agent MA devient le nouvel agent HMA et diffuse un message périodique HANNOUNCE tous les H_ANNOUNCE.time à destination de la zone avec multidiffusion activée.

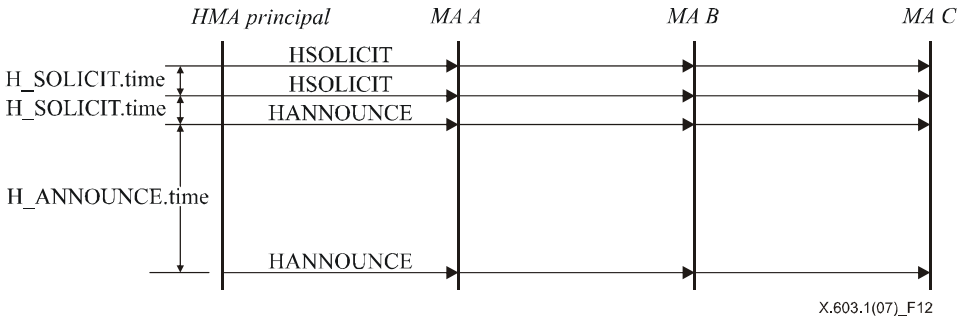

Figure 12 – Un agent MA devient le nouvel agent HMA

La Figure 13 montre comment un agent HMA reprend les activités. Une fois qu'un agent MA devient un agent HMA, il transmet un message HANNOUNCE au réseau avec multidiffusion activée tous les H_ANNOUNCE.time.

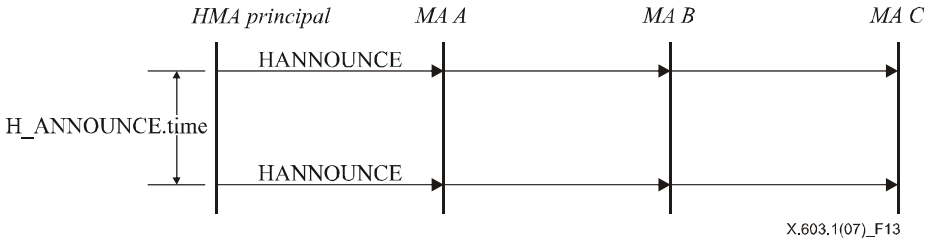

Figure 13 – Message périodique HANNOUNCE

La Figure 14 montre comment un nouvel agent HMA est choisi. En l'absence de message HANNOUNCE pendant un certain temps (H_ANNOUNCE.time × N_ANNOUNCE), l'agent HMA attend un message HANNOUNCE pendant un délai d'attente aléatoire. En l'absence de message HANNOUNCE, l'agent MA devient l'agent HMA du réseau avec multidiffusion activée. Cependant, s'il y a un message HANNOUNCE, l'agent MA rejette le délai d'attente et choisit l'agent HMA comme son agent PMA possible primaire. S'il y a plus de deux messages HANNOUNCE, l'expéditeur du message HANNOUNCE le plus précoce devient l'agent HMA. En cas de collision entre deux messages HANNOUNCE ou plus, l'agent HMA doit suivre l'algorithme de suppression de duplication.

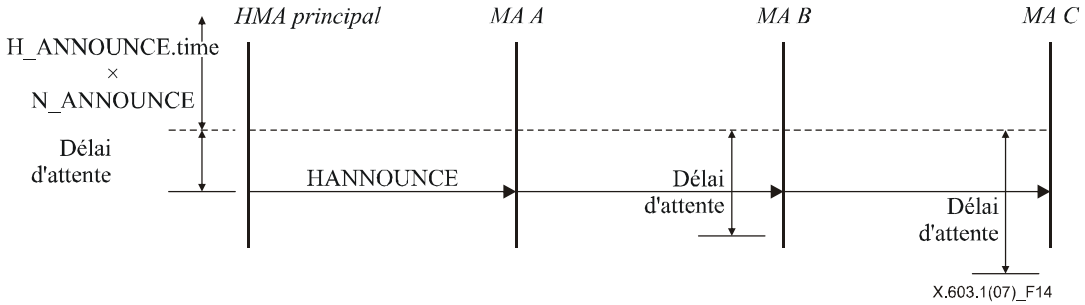

Figure 14 – Sélection d'un nouvel agent HMA

Etant donné que dans un réseau avec multidiffusion activée, chaque agent MA peut être choisi comme agent HMA, chaque agent MA doit également mettre en œuvre le mécanisme de découverte de carte pour le réseau extérieur. La procédure détaillée est décrite dans le paragraphe suivant.

6.2.2.2 A l'extérieur de la zone avec multidiffusion activée

Chaque agent MA doit engager une procédure de découverte des voisins sur la base des informations d'amorçage initiales fournies par le gestionnaire de session. Comme indiqué sur la Figure 15, chaque agent MA peut progressivement apprendre la topologie de l'arborescence RMCP-2 en échangeant les informations d'arborescence de chaque agent MA.

Le mécanisme de découverte de carte de base est le suivant: en premier lieu, en utilisant les messages PPROBREQ et PPROBANS, chaque agent MA peut échanger une liste contenant un certain nombre de voisins à chaque intervalle (PPROBE.time). Etant donné que les ressources système de chaque agent MA sont limitées, le nombre maximal de voisins dans la liste à échanger devrait être limité.

Pour éviter à chaque agent MA de subir les conséquences d'une explosion de message PPROBREQ, le nombre maximal de messages PPROBREQ pendant une période donnée devrait être limité à N_MAX_PROBE.

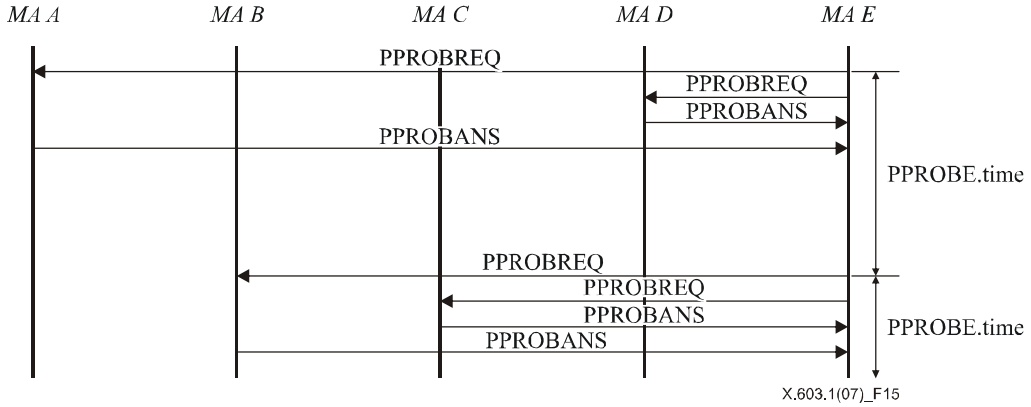

Figure 15 – Procédure de découverte de carte

6.2.3 Entrée dans l'arborescence

La procédure d'entrée dans l'arborescence permet à chaque agent MA de choisir un agent PMA à l'intérieur d'une session RMCP-2 à laquelle il s'est abonné. La Figure 16 montre comment un agent MA choisit son agent PMA sur la base de la liste de voisins indiquée par le gestionnaire de session. L'agent MA entrant (agent MA E) envoie un message PPROBREQ à un ou plusieurs nœuds indiqués dans la liste de voisins (agents MA A, C et D) et attend un message PPROBANS d'acceptation. Dès qu'il reçoit un message PPROBANS, l'agent MA E peut choisir l'agent MA le plus proche. Sur la Figure 16, l'agent MA entrant (nœud E) considère que l'agent MA D est le meilleur, puis choisit l'agent MA D comme étant son agent PMA. Après sélection de l'agent PMA, l'agent MA entrant (nœud E) enverra à l'agent MA D un message RELREQ, qui contient un *profil de données* proposé.

Si le message RELREQ est acceptable, l'agent MA D répond en envoyant un message RELANS d'acceptation, qui comprend le *profil de données* négocié à utiliser, sinon il renvoie un code de motif du rejet.

Après réception d'un message RELANS d'acceptation, le canal de données entre les agents MA D et MA E est établi conformément au profil de données négocié, sinon l'agent MA E doit essayer le deuxième meilleur agent PMA possible.

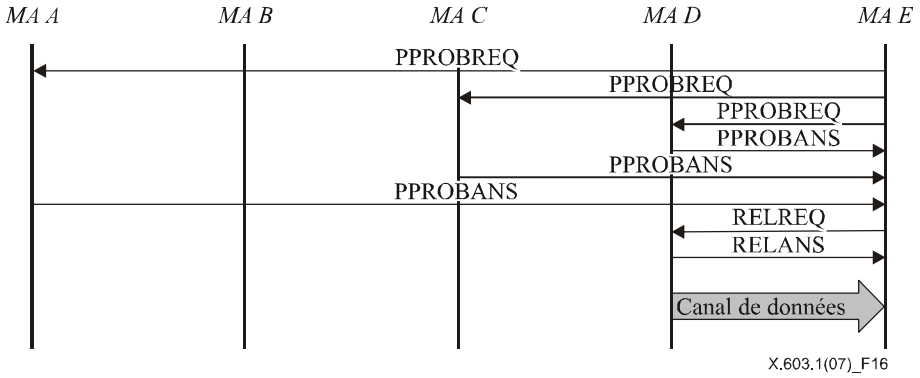

Figure 16 – Procédure d'entrée réussie dans l'arborescence

Si aucun agent MA ne veut relayer les données vers l'agent MA entrant, celui-ci peut recommencer la *procédure d'entrée dans l'arborescence* après un certain délai. Le temps nécessaire à cette nouvelle tentative peut être déterminé par l'utilisateur, encore que cette question sorte du cadre de la présente spécification. La Figure 17 indique quand tous les agents MA énumérés dans la liste de voisins fournie par le gestionnaire de session ont rejeté la demande de relais du nœud E. Toutefois, l'agent MA E connaissait déjà l'existence de l'agent MA B pendant les échanges précédents de messages PPROBREQ et PPROBANS, de sorte qu'il peut recommencer la procédure d'entrée auprès de l'agent MA B.

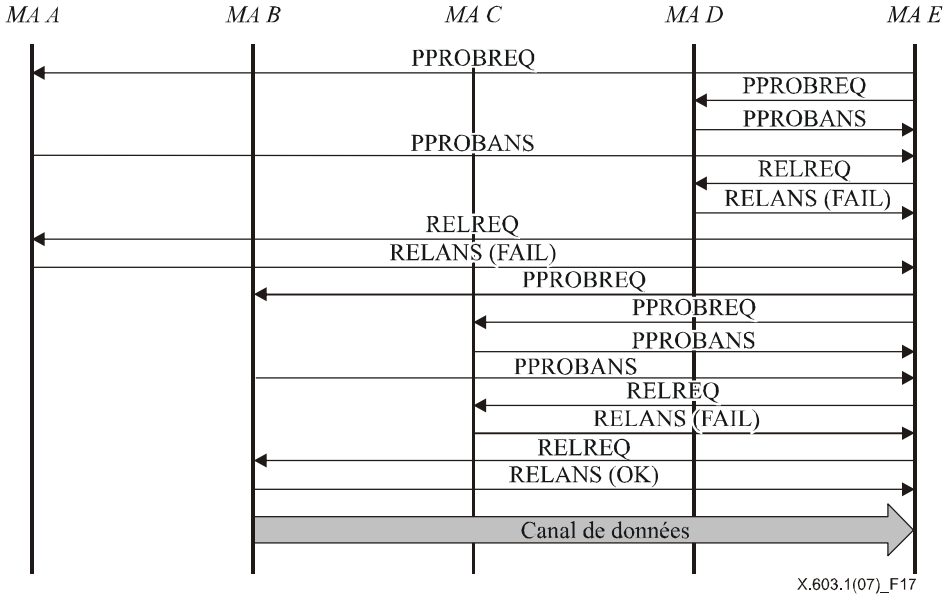

Figure 17 – Echec de l'entrée dans l'arborescence et nouvelle tentative

6.2.4 Sortie

Un agent MA RMCP-2 peut sortir d'une session pendant la durée de vie de cette session. Pour rendre robuste une arborescence RMCP-2, chaque agent MA doit informer de son départ l'agent PMA et les agents CMA. Lorsqu'ils reçoivent cette notification, l'agent PMA et chaque agent CMA doivent se conformer à la procédure appropriée.

Le protocole RMCP-2 prend en compte quatre types de sortie. Le premier s'applique à un agent MA qui quitte la session à la demande d'un utilisateur du service. Le deuxième s'applique à un agent MA qui quitte son agent PMA pour changer de parent. Le troisième s'applique à l'expulsion d'un agent MA par son agent PMA ou le gestionnaire de session. Le dernier s'applique à la sortie d'un agent SMA d'une session. Le fonctionnement détaillé de ces cas est décrit dans les paragraphes qui suivent.

6.2.4.1 Un agent MA quitte une session

Les agents MA peuvent quitter une session à tout moment pendant la durée de vie de la session. Avant de sortir, un agent MA doit informer l'agent PMA et les agents CMA de son départ. L'agent PMA supprime le nœud de la liste de ses agents CMA et réserve un espace à un nouvel agent CMA.

a) *Agent MA quittant la session dans le cas d'un système d'acheminement des données en mode sans multidiffusion*

Pour quitter une session, un agent MA envoie un message LEAVREQ à ses agents CMA. Chaque agent CMA recevant le message LEAVREQ devrait rapidement commencer à se connecter à un agent PMA de remplacement, en envoyant un message RELREQ à l'agent PMA possible. Si cette opération aboutit, chaque agent CMA envoie un message LEAVANS à son ancien agent PMA.

La Figure 18 montre comment l'agent MA C se comporte lorsque l'agent HMA quitte une session pendant laquelle le système d'acheminement de données en mode multidiffusion n'est pas utilisé. L'agent MA C essaye de quitter la session en envoyant un message LEAVREQ aux agents MA D et MA E, qui sont les agents CMA de l'agent MA C. Dès réception du message LEAVREQ, les agents MA D et MA E envoient chacun un message RELREQ à leur propre agent PMA possible.

Une fois que chaque agent MA s'est rallié avec succès à un nouvel agent PMA (MA A et MA B), chaque agent MA (MA D et MA E) envoie un message LEAVANS à l'agent PMA actuel (MA C). Dès réception du message LEAVANS de ses agents CMA, l'agent MA C envoie un message LEAVREQ à son agent PMA (MA B). L'agent PMA retire ensuite l'agent MA de sa liste d'agents CMA. Tout agent MA sortant qui n'a pas d'agent CMA se contente d'envoyer un message LEAVREQ à son agent PMA.

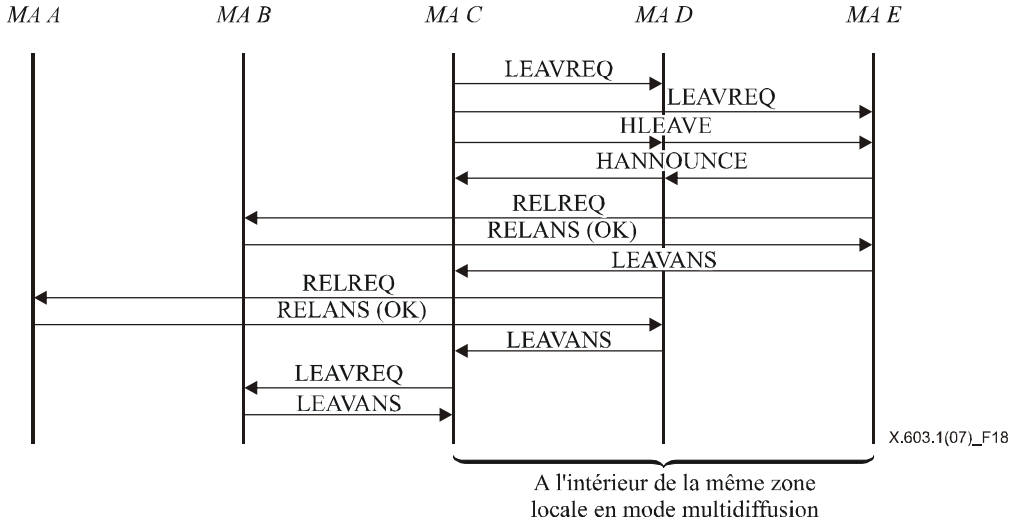

Figure 18 – Agent HMA quittant la session dans le cas d'un système d'acheminement des données en mode sans multidiffusion

La Figure 19 montre comment un agent MA, qui n'est pas un agent HMA, quitte une session lorsqu'un système d'acheminement des données en mode sans multidiffusion est utilisé. Dans ce scénario, les procédures à suivre pour quitter une session dans le cas d'un agent HMA et d'un agent non HMA sont les mêmes, à l'exception du fait que l'agent HMA suit la séquence d'échange de message HLEAVE.

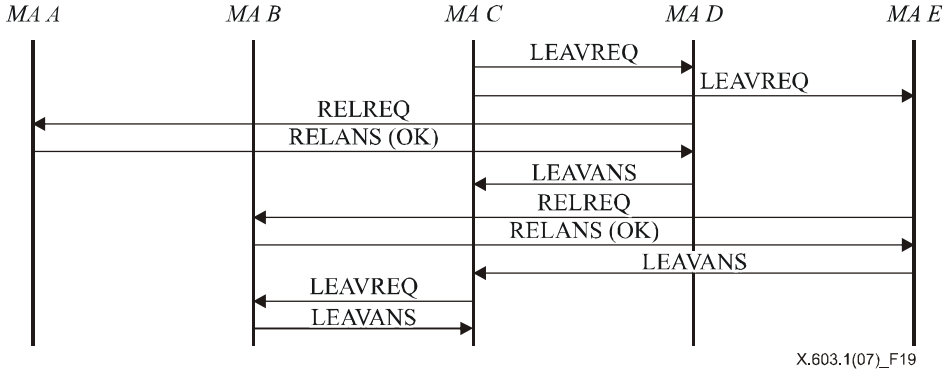

Figure 19 – Agent MA normal quittant la session dans le cas d'un système d'acheminement des données en mode sans multidiffusion

b) *Agent MA quittant la session dans le cas d'un système d'acheminement des données en mode multidiffusion*

Il existe deux cas de figure lorsqu'un agent MA quitte une session à l'intérieur d'une zone avec multidiffusion activée. Dans le premier cas, l'agent HMA quitte la session et dans le deuxième cas, c'est l'agent MA qui quitte la session. Chaque fois que l'agent HMA d'une zone avec multidiffusion activée veut quitter une session, il doit informer de son départ les agents CMA se trouvant à l'intérieur du réseau local ainsi que les agents CMA et l'agent PMA situés à l'extérieur du réseau.

La Figure 20 montre comment l'agent MA C, qui fait office d'agent HMA, quitte une session lorsque le système d'acheminement des données en mode multidiffusion est utilisé. L'agent HMA (MA C) envoie un message LEAVREQ à son agent CMA direct (MA F) à l'extérieur du réseau local. Dès réception du message, l'agent MA F commence à changer de parent et répond à l'agent MA C en envoyant un message LEAVANS et envoie par multidiffusion un message HLEAVE avec une liste d'agents HMA possibles vide au réseau local. Le message HLEAVE est utilisé pour annoncer le départ de l'agent HMA.

Dès réception du message HLEAVE provenant de l'agent HMA, l'agent MA D et l'agent MA E de la Figure 20 laissent passer un certain temps d'attente avant d'envoyer par multidiffusion le message HANNOUNCE. L'agent MA D envoie le message HANNOUNCE pour la première fois et devient un nouvel agent HMA. Cette étape intervient parce que l'agent MA D dispose d'un délai d'attente plus court que tout autre agent MA. Etant donné que l'agent MA C qui quitte

la session est un point qui est connecté à l'extérieur du réseau avec multidiffusion activée, l'agent MA D doit jouer le rôle de l'agent MA C en se connectant à l'agent PMA situé à l'extérieur du réseau. La Figure 20 montre comment l'agent MA D choisit pour son agent parent l'agent MA B, qui est l'agent PMA de l'agent MA C.

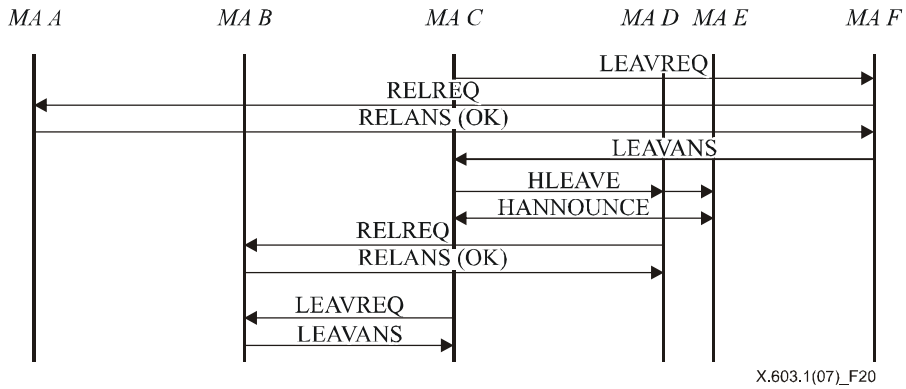

Figure 20 – Agent MA quittant la session dans le cas d'un système d'acheminement des données en mode multidiffusion

Chaque fois qu'un agent non HMA d'une zone avec multidiffusion activée veut quitter une session, il le fait sans notification. L'agent MA D ou MA E de la Figure 20 n'a pas à informer les autres agents MA de son départ.

6.2.4.2 Un agent MA quitte son agent PMA pour changer d'agent parent

Un agent MA souhaitant changer d'agent PMA peut quitter son agent PMA actuel, auquel cas il n'a pas à envoyer un message LEAVREQ à ses agents CMA. Ceux-ci n'ont pas à être informés du départ tant qu'ils reçoivent avec succès les données. Pour changer d'agent PMA, l'agent MA envoie un message RELREQ à l'autre agent PMA possible. Un ancien agent PMA recevant un message LEAVREQ avec le code de motif mis à PS (changement d'agent parent) supprime de sa liste d'agents CMA, l'agent MA sortant, mais garde les informations relatives à cet agent dans sa liste de voisins, parce que l'agent MA sortant est toujours actif dans la session.

La Figure 21 montre comment un agent MA change d'agent parent. A noter qu'un agent MA peut changer d'agent parent uniquement lorsqu'il reçoit un message de pulsation (HB) afin que l'arborescence reste inchangée. Le mécanisme de pulsation est décrit au § 6.2.5.1.

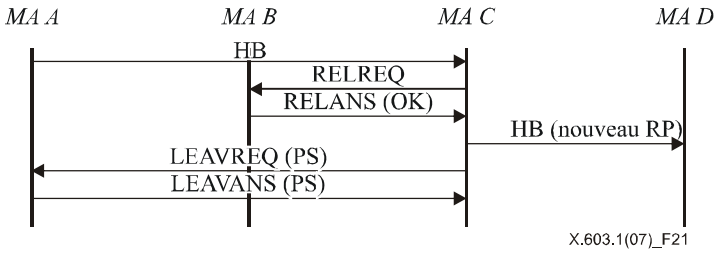

Figure 21 – Agent MA quittant la session pour changer d'agent parent

6.2.4.3 Un agent MA est expulsé

Le protocole RMCP-2 comporte un mécanisme permettant de rejeter certains agents MA, par exemple lorsqu'un gestionnaire de réseau souhaite que le gestionnaire de session rejette un agent MA donné ou lorsqu'un agent MA expulse un agent CMA après avoir appris qu'il ne peut pas prendre en charge davantage d'agents CMA.

a) *Expulsion d'un agent MA par son agent PMA*

Un agent PMA peut expulser l'un de ses agents CMA lorsqu'il est confronté à un épuisement de ressources système et ne peut plus alimenter son agent CMA, ou lorsqu'il constate que l'un de ses agents CMA a épuisé les ressources système. Un agent MA doit trouver un autre agent PMA possible, qui lui permet de disposer d'un nouvel agent PMA.

La Figure 22 illustre un exemple de flux de message. En premier lieu, un agent PMA, à savoir l'agent MA C, envoie un message LEAVREQ avec le motif KO afin d'expulser l'agent MA D. Celui-ci recherche d'autres agents PMA puis envoie une demande de relais. Après avoir changé d'agent parent, l'agent MA D transmet un message LEAVANS à son ancien agent PMA.

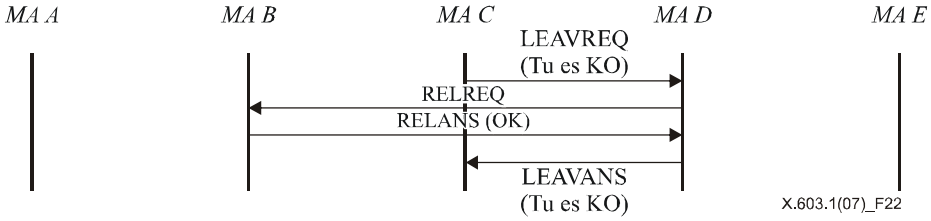

Figure 22 – Un agent MA est expulsé par son agent PMA

b) *Expulsion d'un agent MA par le gestionnaire de session*

Le gestionnaire de session peut rejeter tout agent MA en envoyant un message LEAVREQ avec le motif KO (*kicked-out*, expulsé). Lorsqu'il reçoit un message LEAVREQ du gestionnaire de session, un agent MA doit quitter rapidement la session. Après l'expulsion, le gestionnaire de session doit mettre à jour la liste des membres de sa session.

Dans le flux de message indiqué sur la Figure 23, le gestionnaire de session indique à l'agent MA B de quitter la session en envoyant un message LEAVREQ avec le motif KO. L'agent MA B doit quitter la session mais, avant de sortir, il doit informer ses agents PMA et CMA de son expulsion.

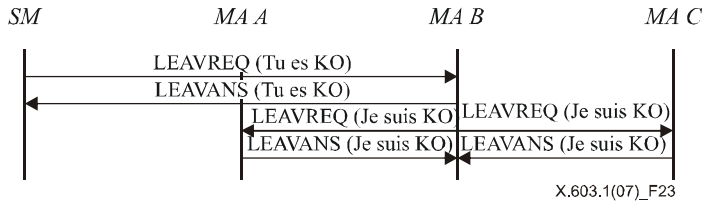

Figure 23 – Un agent MA est expulsé par le gestionnaire de session

6.2.4.4 L'agent SMA quitte la session

Etant donné qu'une session RMCP-2 ne peut exister sans agent SMA, celui-ci ne quitte jamais une session avant que celle-ci soit terminée. En pareil cas, lorsque l'agent SMA quitte la session, celle-ci doit être terminée.

La Figure 24 représente la procédure de départ d'un agent SMA d'une session. L'agent SMA envoie un message LEAVREQ au gestionnaire de session. Lorsqu'il reçoit le message LEAVREQ de l'agent SMA, le gestionnaire de session supprime les informations de la session et répond en envoyant le message LEAVANS. Lorsqu'il reçoit le message LEAVANS du gestionnaire de session, l'agent SMA envoie un message LEAVREQ avec le motif *sortie de l'agent SMA* à ses agents CMA directs. Ce message doit être relayé rapidement vers l'aval, afin de mettre fin à la session RMCP-2.

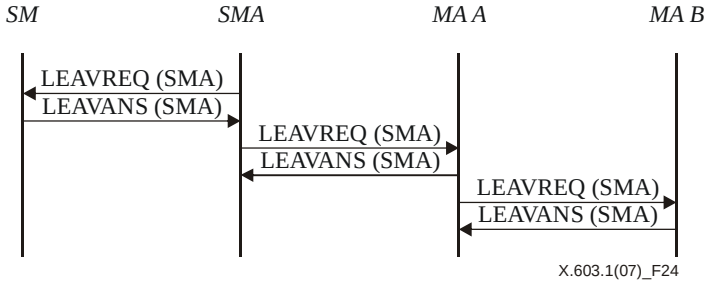

Figure 24 – Sortie de l'agent SMA

6.2.5 Maintien

6.2.5.1 Pulsation

Le message de pulsation vise à faire en sorte que l'arborescence RMCP-2 établie reste robuste. Le message de pulsation, qui fournit des informations de synchronisation homogènes à la session, aide chaque agent MA à déterminer si la session est toujours active. Il contient également des informations utiles sur le trajet d'acheminement des données, appelé ROOTPATH. L'élément ROOTPATH comprend un trajet de données relayées qui est conforme à la hiérarchie arborescente.

La Figure 25 illustre la procédure de pulsation RMCP-2. Selon cette procédure, l'agent SMA envoie le message HB le long du trajet ROOTPATH, à ses descendants. Chaque descendant ajoute ensuite à ce message les informations de saut, qui peuvent comporter l'identificateur MAID, la distance réseau pour chaque saut et des informations sur le système telles que la largeur de bande en entrée et en sortie, le nombre possible d'agents CMA, etc., et transmet le message HB modifié à ses descendants. Enfin l'élément ROOTPATH contient tous les agents MA visités le long de l'arborescence.

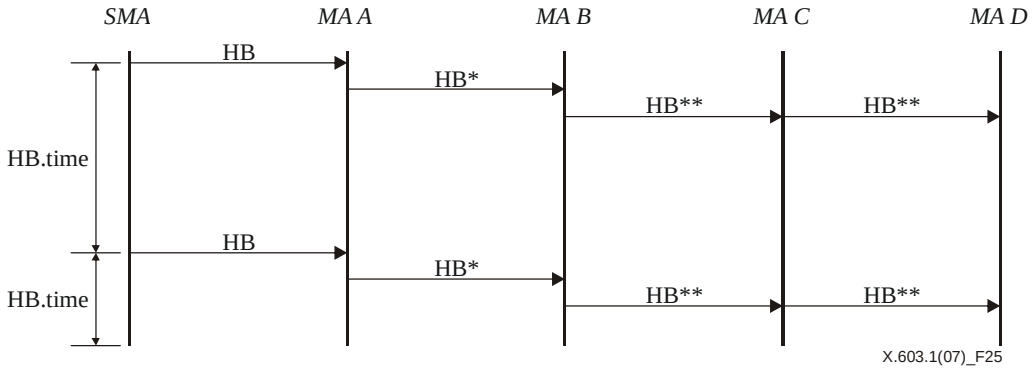

Figure 25 – Pulsation

6.2.5.2 Surveillance

Le protocole RMCP-2 comporte deux types de mécanismes de surveillance. Le premier, présenté sur la Figure 26, consiste à surveiller un agent MA donné et le second, indiqué sur la Figure 27, consiste à surveiller une partie de l'arborescence par l'intermédiaire d'un agent MA donné.

La Figure 26 montre comment un gestionnaire de session surveille un agent MA donné. Selon cette procédure, le gestionnaire de session envoie un message STREQ à l'agent MA B et demande un ou plusieurs types précis d'informations d'état à l'agent MA B. En réponse, l'agent MA B envoie au gestionnaire de session un message STANS contenant les informations demandées.

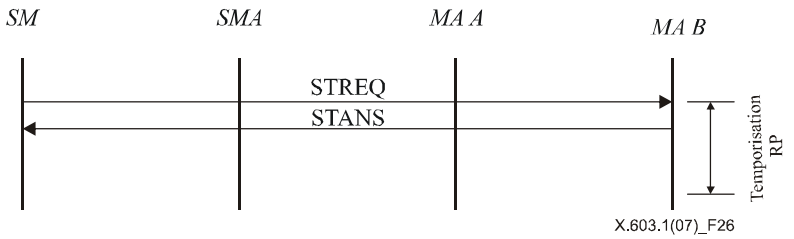

Figure 26 – Surveillance de l'arborescence au moyen de la notification d'état

La Figure 27 montre comment le gestionnaire de session demande des informations sur la zone limitée d'une arborescence: le gestionnaire de session demande des informations regroupées sur la zone limitée d'une arborescence en envoyant un message STREQ à un agent MA donné (SMA et MA A) pour recueillir des informations d'état concernant la zone limitée.

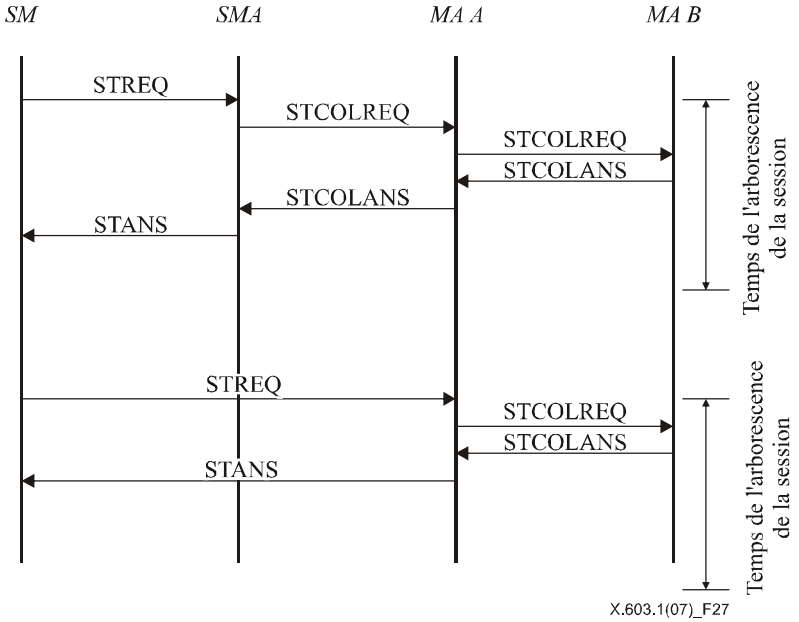

Figure 27 – Surveillance de l'arborescence par la collecte d'informations d'état

6.2.5.3 Détection des défauts et rétablissement

Cette procédure est menée à bien par un agent MA, lorsque celui-ci détecte des défauts dans le réseau et remédie aux problèmes pour rendre robuste l'arborescence RMCP-2. Les défauts dans le réseau tels que les boucles ou les partitions sont souvent dus à des mouvements fréquents et négligents de l'agent MA. Pour déceler ces défauts et y remédier, le protocole RMCP-2 fournit les mécanismes suivants de détection des défauts et de rétablissement.

a) *Détection des boucles et rétablissement*

Un agent MA peut déceler une boucle en vérifiant l'élément ROOTPATH contenu dans le message HB. Etant donné que l'élément ROOTPATH indique le parcours du trajet entre l'agent SMA et l'agent MA, un saut figurant deux fois dans l'élément ROOTPATH signifie qu'une boucle a été créée. Chaque fois qu'une boucle se présente, chaque agent MA met en œuvre le mécanisme suivant de rétablissement en cas de boucle: dans le scénario décrit sur la Figure 28, l'agent MA Y examine le message HB; il confirme ensuite l'existence d'une boucle chaque fois qu'il reçoit HB_{n+3}, étant donné que l'agent MA Z, qui est un agent CMA de l'agent MA Y, est déjà énuméré deux fois dans l'élément ROOTPATH. Pour procéder au rétablissement par suite de la boucle, l'agent MA Y envoie à l'agent MA Z un message LEAVREQ afin de procéder à une déconnexion.

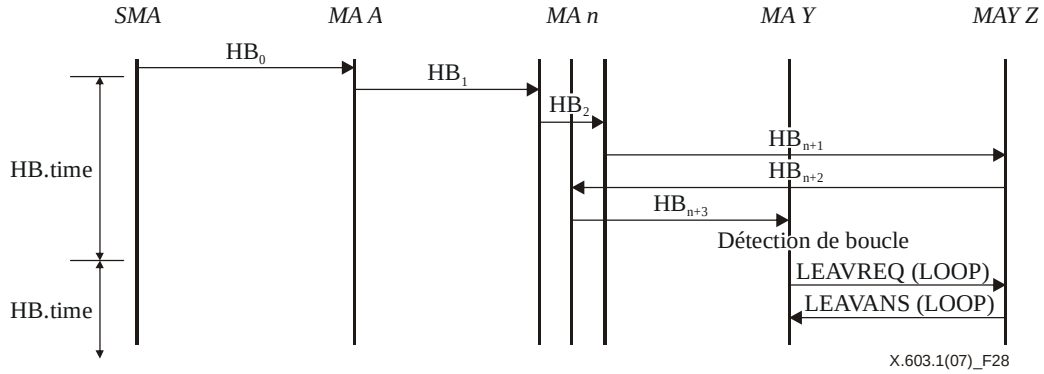

Figure 28 – Détection de boucle et rétablissement

b) *Détection d'une partition de réseau et rétablissement*

Chaque fois qu'un agent MA ne parvient pas à recevoir le message de pulsation (HB) pendant un certain temps, il présume qu'il fait l'objet d'une partition par rapport à l'arborescence. Il faut prévoir un laps de temps suffisant pour tenir compte du temps de transfert dans le réseau. Le protocole RMCP-2 définit ce laps de temps comme étant HB_TIME × MAX_PARTITION_CNT.

Une partition peut se produire chaque fois que l'un des associés de la partition échoue. L'agent MA décèle l'origine de la partition en contactant ses associés, puis il résout le problème.

La Figure 29 indique comment l'agent MA Z détecte une partition de l'arborescence: une telle partition est détectée chaque fois que l'agent MA Z ne parvient pas à recevoir le message de pulsation HB pendant un certain temps (HB_TIME × MAX_PARTITION_CNT). Le fait de ne pas pouvoir recevoir le message HB déclenche la transmission d'un certain nombre de messages PPROBREQ vers ses associés. Sur la Figure 29, l'agent MA Z reçoit un message PPROBANS des agents MA A et MA B, mais aucune réponse de l'agent MA C, qui est l'agent PMA actuel de l'agent MA Z. L'agent MA Z détecte une partition en raison de l'absence de réponse de l'agent PMA direct de l'agent MA Z. Celui-ci essaie ensuite de changer d'agent parent afin de procéder au rétablissement, par suite du partage.

Pendant qu'un agent MA répare la partition, les descendants de l'agent MA peuvent également considérer que le réseau a fait l'objet d'une partition et peuvent commencer à réparer cette partition. Il en résulte qu'une partition au niveau d'un seul agent MA peut provoquer l'effondrement de la totalité de l'arborescence. Pour éviter ce problème, un agent MA qui répare un défaut dans le réseau génère un pseudo-message HB à l'attention de ses descendants afin de les informer que la session fait l'objet d'une partition temporaire et est en cours de rétablissement.

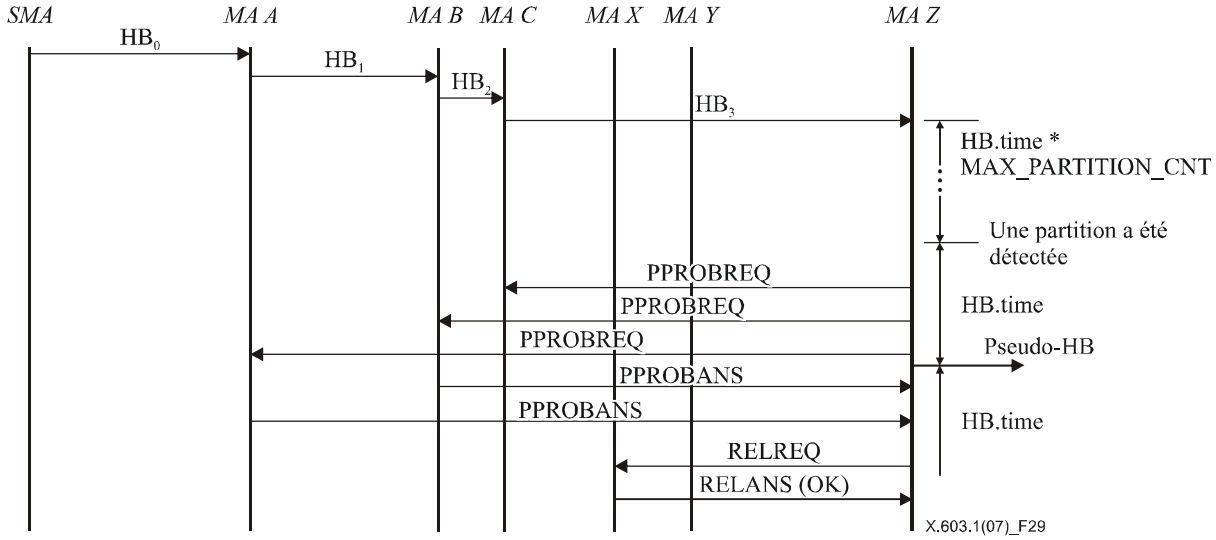

Figure 29 – Détection d'une partition de réseau et rétablissement

6.2.5.4 Amélioration de l'arborescence

La procédure d'amélioration de l'arborescence intervient lorsqu'un agent MA trouve un ou plusieurs agents PMA possibles efficaces et essaie de passer à l'agent qui a été trouvé. En poursuivant la procédure d'amélioration de l'arborescence pendant la session, il est possible d'améliorer progressivement l'arborescence RMCP-2.

La procédure permettant de trouver de meilleurs nœuds est conforme au mécanisme de découverte de carte décrit au § 6.2.2. A chaque passage de la procédure de découverte de carte, chaque agent MA compare les paramètres de qualité de service de son agent PMA actuel à ceux du nœud récemment découvert. Lorsqu'un agent MA trouve un agent MA meilleur que son agent PMA actuel, il peut remplacer son agent PMA actuel par un agent MA récemment découvert conformément à la procédure de changement d'agent parent décrite au § 6.2.4.2.

Il est certes possible d'améliorer l'arborescence, mais des défauts dans le réseau tels que les boucles ou les partitions peuvent facilement se produire. En particulier, des défauts dans le réseau peuvent intervenir dans les cas suivants: lorsque plusieurs agents MA d'une même branche essaient de changer leurs agents PMA en même temps et lorsque plusieurs agents MA le long de la branche tentent de changer successivement d'agents PMA.

Pour prémunir une arborescence contre ces risques, le protocole RMCP-2 garantit la condition atomique, dans laquelle chaque agent MA peut changer d'agent parent uniquement après avoir reçu un message HB avec un élément ROOTPATH inchangé.

6.2.6 Terminaison

Pour mettre fin à une session, le gestionnaire de session envoie un message TERMREQ à l'agent SMA, comme indiqué sur la Figure 30. Un agent SMA (ou MA) qui reçoit un message TERMREQ du gestionnaire de session (ou de l'agent PMA) renvoie le message TERMANS au gestionnaire de session (ou à l'agent PMA), puis retransmet le message TERMREQ à ses agents CMA, jusqu'à ce que ce message atteigne les nœuds d'extrémité de l'arborescence. Enfin, la session est fermée.

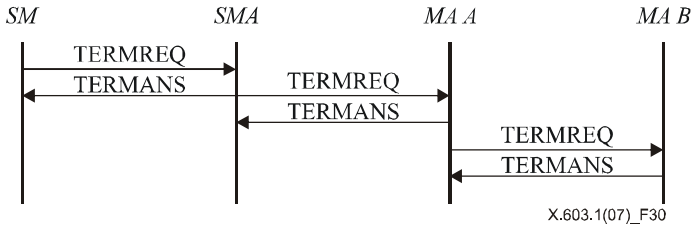

Figure 30 – Terminaison de session par le gestionnaire de session

7 Format des messages RMCP-2

Le présent paragraphe décrit les formats des messages RMCP-2 et les informations requises dans ces messages. Les informations de valeur correspondant à chaque message seront expliquées au paragraphe 8.

7.1 Format commun des messages RMCP-2

La Figure 31 représente le format commun des messages RMCP-2.

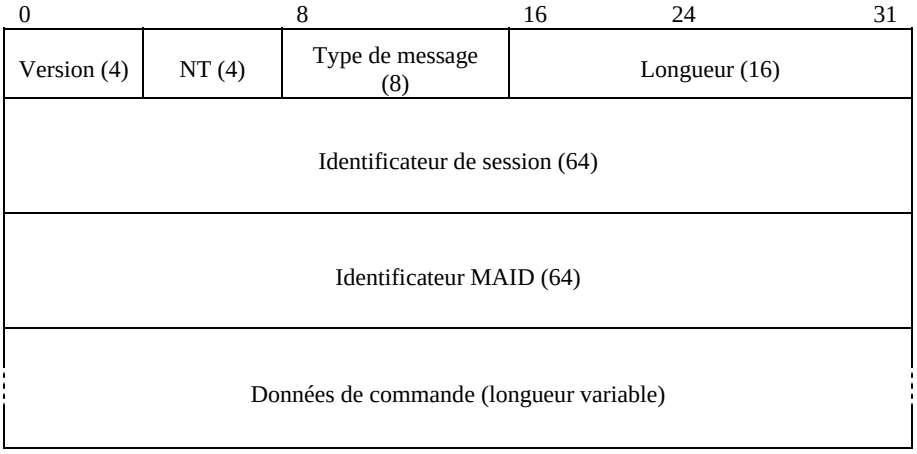

Figure 31 – Format commun des messages RMCP-2

La description de chaque champ est la suivante:

a) *Version* – version actuelle du protocole RMCP. La valeur par défaut pour le protocole RMCP-2 est fixée à 0x2.

b) *NT* (*type de nœud*) – type du nœud. Sa valeur doit être fixée de manière à s'identifier en tant que gestionnaire de session, agent SMA ou agent MA.

c) *Type de message* – type du message.

d) *Longueur* – longueur totale du message, en octets, y compris les données de commande.

e) *Identificateur de session* – entier de 64 bits qui identifie une session.

f) *Identificateur MAID* – valeur unique de 64 bits utilisée pour identifier l'agent MA pendant une certaine session.

g) *Données de commande* – données de commande utilisées par chaque message selon les besoins.

L'identificateur de session et l'identificateur MAID doivent avoir une valeur unique pour identifier respectivement la session et l'agent MA. Le protocole RMCP-2 fournit une règle permettant de générer la valeur d'identification utilisée pour une session et un agent MA.

7.1.1 Identificateur de session

L'identificateur de session (SID) est une combinaison de l'adresse IP locale du gestionnaire de session (SM) et de l'adresse de groupe de la session. L'adresse de groupe pour une nouvelle session peut être attribuée par le gestionnaire de session lorsque celui-ci est invité à créer une session. Ce faisant, l'identificateur SID peut être garanti comme étant unique d'une manière globale. La Figure 32 illustre le format de l'identificateur SID RMCP-2.

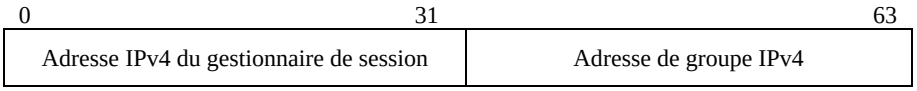

Figure 32 – Format de l'identificateur SID RMCP-2

7.1.2 Identificateur MAID

L'identificateur MAID comprend l'adresse IP locale, le numéro de port et le numéro de série comme indiqué sur la Figure 33. L'adresse IP locale est l'adresse IP de l'agent MA. L'agent MA d'une session RMCP-2 peut être amené à ouvrir plusieurs ports pour la session. Le numéro de port utilisé pour la création de son identificateur MAID est un numéro de port d'écoute qui est ouvert lorsque l'agent MA commence à utiliser le protocole RMCP-2 pour recevoir des messages de commande du gestionnaire de session ou d'autres agents MA.

Chaque agent MA peut être identifié par son numéro de port dans un système multi-utilisateur. Toutefois, il n'est pas possible d'identifier chaque agent MA à l'intérieur d'un réseau basé sur un mécanisme de traduction d'adresse de réseau (NAT, *network adress translation*), dans lequel la même adresse IP pour plusieurs agents MA peut être présentée à l'homologue de communication situé à l'extérieur du réseau. Pour traiter ce cas, le gestionnaire de session génère un identificateur MAID unique en fournissant une valeur unique dans le champ numéro de série, lorsqu'il reçoit une adresse NAT d'un agent MA, et retourne l'identificateur à l'agent MA.

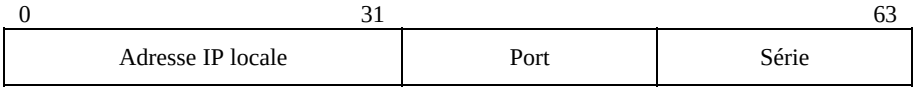

Figure 33 – Format de l'identificateur MAID RMCP-2

La Figure 34 représente l'algorithme que la version actuelle du protocole RMCP-2 utilise pour générer un identificateur MAID unique.

```
Si l'adresse IP figurant dans l'identificateur MAID reçu est une adresse NAT
        Rechercher sa NAT_address_list;
        si la même adresse existe déjà
                serial_number++;
    sinon
                ajouter la liste dans NAT_address_list
                serial_number++;
        MAID = IP_address + port_number + serial_number;
retourner l'identificateur MAID;
```

Figure 34 – Algorithme simple permettant de générer un identificateur MAID unique

7.2 Format des données de commande

La Figure 35 représente le format de données de commande RMCP-2.

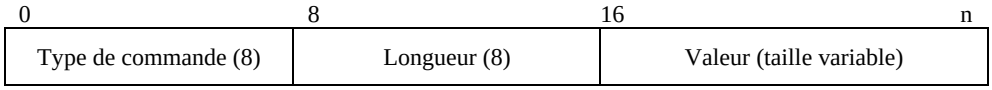

Figure 35 – Format de commande RMCP-2

a) *Type de commande* – type des données de commande.

b) *Longueur* – longueur, en octets, de la valeur des données de commande ainsi que des champs de type et de longueur, à l'exception du champ des données de sous-commande.

c) *Valeur* – valeur des données de commande.

Chaque fois que pour des données de commande RMCP-2, on veut spécifier de manière détaillée la commande, on peut fournir des données de sous-option. Le format des données de sous-option est conforme à celui des données de commande RMCP-2 comme indiqué sur la Figure 36.

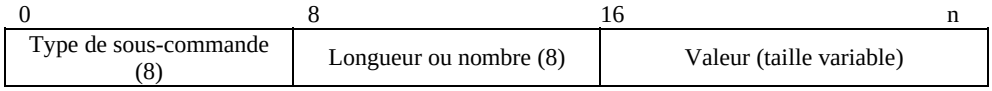

Figure 36 – Format de sous-commande RMCP-2

a) *Type de sous-commande* – type des données de sous-commande.

b) *Longueur ou nombre* – longueur, en octets, de la valeur des données de sous-commande ou en nombre d'éléments de données de sous-commandes, en fonction de la valeur des données de sous-commande.

c) *Valeur* – valeur des données de sous-commande.

Un élément de données de commande peut être représenté en n'utilisant qu'un seul élément de données de commande comme indiqué sur la Figure 37.

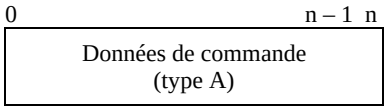

Figure 37 – Utilisation d'un élément de données de commande seul

Lorsqu'un élément de données de sous-commande est utilisé, il doit toujours être précédé d'un élément de données de commande approprié, comme indiqué sur la Figure 38.

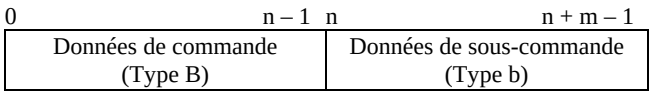

Figure 38 – Utilisation d'un élément de données de commande avec un élément de données de sous-commande

Un ou plusieurs éléments de données de commande peuvent être situés en même temps dans le champ de données de commande RMCP-2. Lorsque dans un paquet RMCP-2, on veut inclure plusieurs éléments de données de commande, ces éléments devraient être présentés comme indiqué sur la Figure 39.

Données de commande (Type A)	Données de commande (Type D)	Données de sous-commande (Type d)	Données de commande (Type E)

Figure 39 – Utilisation de plusieurs éléments de données de commande

7.3 Messages

Le présent paragraphe définit chaque message utilisé dans le protocole RMCP-2. Ce protocole définit sept ensembles de messages de *demande et réponse* (parfois dénommés *demande et confirmation*) et un message de pulsation. Les types de message et les valeurs correspondantes sont indiqués dans le Tableau 2.

7.3.1 SUBSREQ

Le message SUBSREQ est utilisé pour l'abonnement à une session RMCP-2. En émettant un message SUBSREQ, chaque agent MA peut obtenir des informations d'amorçage auprès du gestionnaire de session lorsque la demande d'abonnement est acceptable. Le format de ce message est indiqué sur la Figure 40.

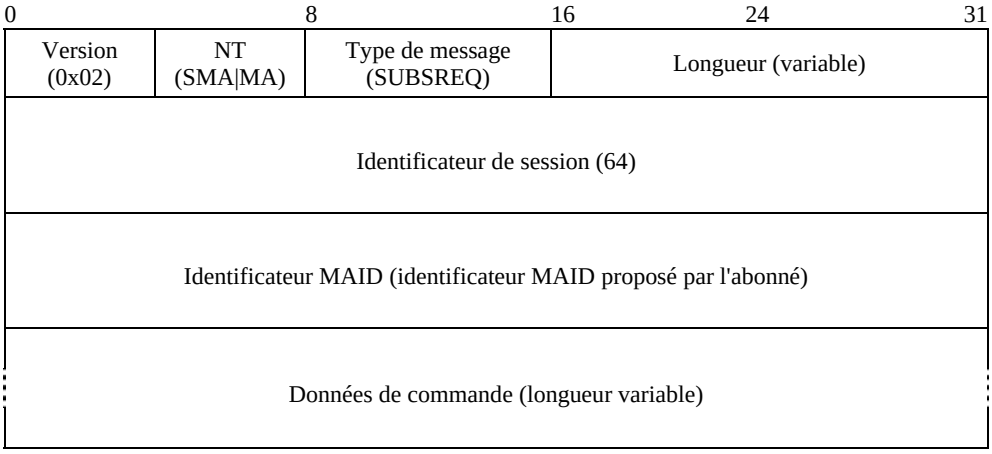

Figure 40 – Message SUBSREQ

La description de chaque champ est la suivante:

a) *Version* – version du protocole RMCP (0x02).

b) *NT* – type de nœud de l'expéditeur du message (SMA|MA).

c) *Type de message* – type du message. La valeur est fixée à SUBSREQ pour le message.

d) *Longueur* – longueur totale du message SUBSREQ, en octets.

e) *Identificateur de session* – valeur de 64 bits de l'identificateur de session RMCP.

f) *Identificateur MAID proposé* – valeur unique permettant d'identifier l'entité.

g) *Données de commande* – ce champ contient un ensemble d'informations requises pour s'abonner à la session RMCP-2. Il peut inclure les informations suivantes:

- SYSINFO

Ce message de commande donne la puissance de système de l'agent MA, par exemple la largeur de bande en entrée et en sortie et le nombre gérable d'agents CMA.

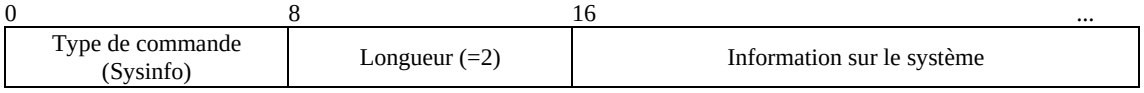

Figure 41 – Commande SYSINFO

Les données de sous-commande suivantes présentées sur les Figures 42 et 43 peuvent suivre les données de commande SYSINFO présentées sur la Figure 41.

La Figure 42 présente des données de sous-commande pouvant suivre les données de commande SYSINFO. La description de chaque champ est la suivante:

a) *Type de sous-commande* – nombre d'agents CMA disponibles (l'un des sous-types de SYS_INFO).

b) *Longueur* – longueur de la valeur des données de commande.

c) *Réservé* – réservé pour une utilisation future.

d) *Valeur* – ce champ contient des informations appropriées sur le système.

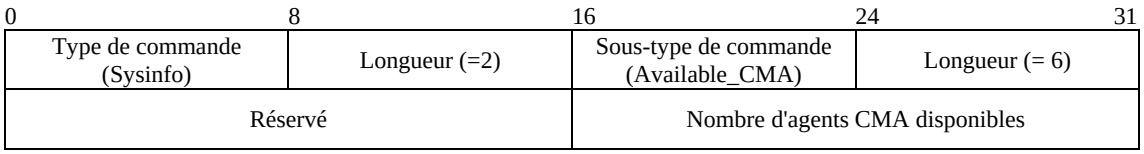

Figure 42 – Sous-commande AVAILABLE_CMA

La Figure 43 présente des données de sous-commande pouvant suivre les données de commande SYSINFO. La description de chaque champ est la suivante:

a) *Type de sous-commande* – largeur de bande possible (l'un des sous-types de SYS_INFO).

b) *Longueur* – longueur de la valeur des données de commande.

c) *Valeur* – ce champ donne la largeur de bande de retransmission que l'agent MA peut offrir.

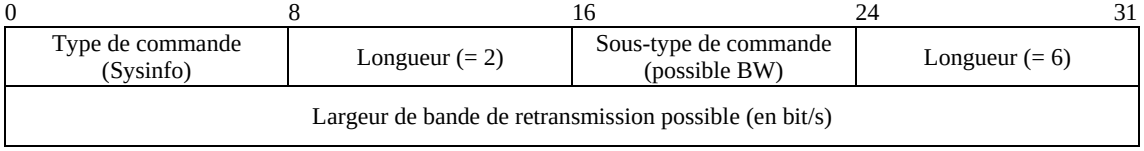

Figure 43 – Sous-commande POSSIBLE_BW

Il est à noter qu'une trame de commande de deux octets précède chaque élément de données de sous-commande.

• DATAPROFILE

La commande DATAPROFILE fournit un profil de données gérable de chaque agent MA. Elle a pour objet de permettre au gestionnaire de session de tenir à jour la liste classée des voisins lorsqu'il est au courant de la qualité de service.

Lorsque l'agent MA n'inclut pas ces données de commande dans le message SUBSREQ, le gestionnaire de session ne s'occupe pas de la gestion de la qualité de service concernant l'agent MA. La description de chaque champ est la suivante:

a) *Type de commande* – DATA_PROFILE.

b) *Longueur* – longueur du profil de données.

c) *Profil de données possible* – profil de données que l'agent MA souhaite utiliser.

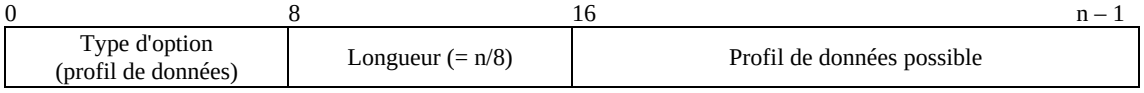

Figure 44 – Commande DATAPROFILE

Etant donné que la commande DATAPROFILE est constituée d'un message variable de type texte, sa taille peut varier. Pour que sa longueur soit un multiple de 4 octets, un ou plusieurs octets de bourrage nuls peuvent éventuellement être ajoutés comme indiqué sur la Figure 45. La description de chaque champ est la suivante:

a) *Profil de données* – caractéristiques du canal de données, conformément à un système de codage de type SDL.

b) *Zéro, un ou plusieurs octets de bourrage nuls* – pour ajuster la longueur du profil de données, un ou plusieurs octets de bourrage nuls peuvent éventuellement être ajoutés.

Figure 45 – Commande DATAPROFILE et bourrage associé

• AUTH

Des informations d'authentification peuvent être fournies au moyen de la commande AUTH. Pour pouvoir prendre en charge plusieurs types de mécanisme d'authentification, on définit un format de sous-commande AUTH détaillé après la commande AUTH de 2 octets. La description de chaque champ est la suivante:

a) *Type de commande* – AUTH.

b) *Longueur* – taille de la commande AUTH, qui devrait être de deux octets.

c) *Informations d'authentification* – ce champ contient des informations d'authentification détaillées, comme suit.

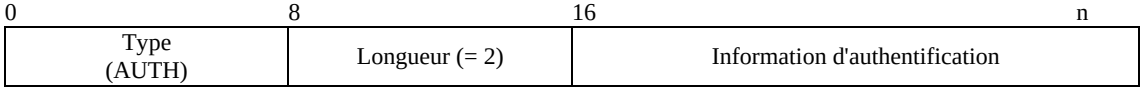

Figure 46 – Commande AUTH

La Figure 47 qui suit présente les données de sous-commande permettant de fournir les informations d'authentification à utiliser. La description de chaque champ est la suivante:

a) *Type de sous-commande* – dépend du mécanisme AUTH à utiliser.

b) *Longueur* – taille des données de sous-commande.

c) *Valeur* – données de commande.

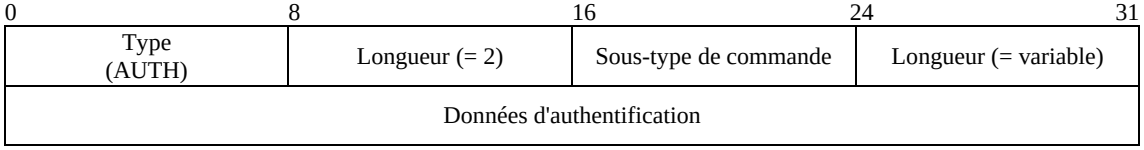

Figure 47 – Sous-commande AUTH

7.3.2 SUBSANS

Le message SUBSANS est utilisé par le gestionnaire de session pour donner les résultats de la demande d'abonnement et les informations d'amorçage pour la session. Le format du message est présenté sur la Figure 48.

La description de chaque champ est la suivante:

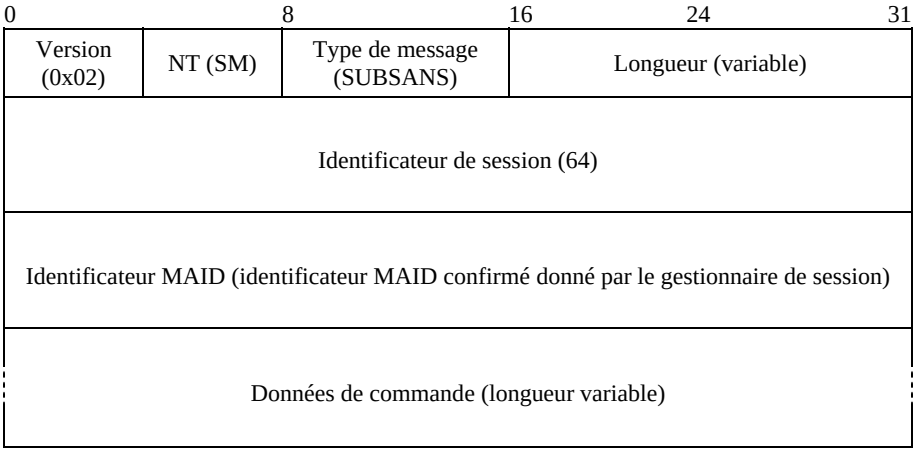

Figure 48 – Message SUBSANS

a) *Version* – version du protocole RMCP (0x02).

b) *NT* – type de nœud de l'émetteur du message (gestionnaire de session).

c) *Type de message* – type du message. La valeur est mise à SUBSANS pour le message.

d) *Longueur* – longueur totale du message SUBSANS (en octets).

e) *Identificateur de session* – valeur de 64 bits de l'identificateur de session RMCP.

f) *Identificateur MAID confirmé* – numéro d'identification de l'agent MA. Le gestionnaire de session fournit l'identificateur confirmé compte tenu de l'identificateur MAID proposé par l'agent MA dans le message SUBSREQ.

g) *Données de commande* – ce champ contient un ensemble d'informations requises pour entrer dans une arborescence de multidiffusion relayée RMCP. Il peut inclure les informations suivantes:

- RESULT

Ce message de commande indique si la demande d'abonnement de l'agent MA a abouti ou non. Si la demande a abouti, ce message donne le code de résultat OK. Dans le cas contraire, il donne un code d'erreur approprié (par exemple épuisement des ressources, destination impossible à atteindre). La Figure 49 présente le format du message de commande RESULT. Les commandes qui suivent servent à fournir les informations nécessaires à l'entrée dans une arborescence RMCP-2. Lorsque l'abonnement n'est pas autorisé, la commande suivante ne peut pas être incluse. La description de chaque champ est la suivante:

a) *Type de commande* – RESULT.

b) *Longueur* – longueur du code de résultat.

c) *Code de résultat* – résultat de la demande, les codes détaillés étant énumérés dans le Tableau 3.

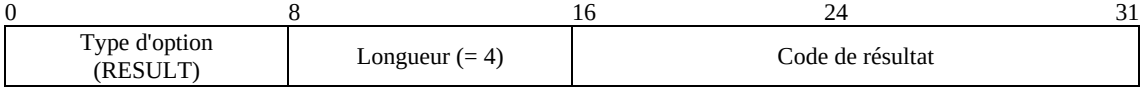

Figure 49 – Commande RESULT

• DATAPROFILE

La commande DATAPROFILE est utilisée par le gestionnaire de session pour confirmer le profil de données à l'abonné. Elle a un sens lorsque le gestionnaire de session fournit des informations de session supplémentaires à chaque abonné. Le format de la commande DATAPROFILE est présenté sur la Figure 44 et son contenu sur la Figure 84.

• NEIGHBORLIST

Lorsqu'un abonnement est autorisé, le gestionnaire de session retourne une liste de voisins suffisante à l'abonné. La commande NEIGHBORLIST est destinée à être utilisée comme informations d'amorçage par chaque abonné. La Figure 50 présente le format de la commande NEIGHBORLIST; il est à noter que seuls des identificateurs MAID sont fournis. La description de chaque champ est la suivante:

a) *Type de commande* – NEIGHBOR_LIST.

b) *Longueur* – longueur des données de commande, qui devrait être égale à 2 octets.

c) *Informations sur la liste des voisins* – ensemble d'informations relatives aux identificateurs MAID, dont l'utilisation et le format sont les suivants.

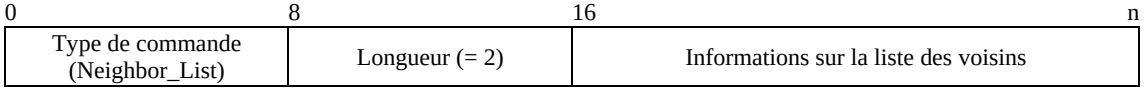

Figure 50 – Commande NEIGHBORLIST

La Figure 51 présente la sous-commande qui suit la commande NEIGHBORLIST, la signification de chaque champ étant la suivante:

a) *Type de sous-commande* – type de liste de voisins qui sera utilisé. Dans cet exemple, une liste d'identificateurs MAID est utilisée comme liste NEIGHBOR_LIST.

b) *Nombre de voisins dans la liste* – nombre d'identificateurs MAID à suivre.

c) *Identificateur*(*s*) *MAID* – liste d'identificateurs MAID fournie par le gestionnaire de session. Le nombre d'agents MA dans la liste est enregistré dans le champ nombre de voisins dans la liste.

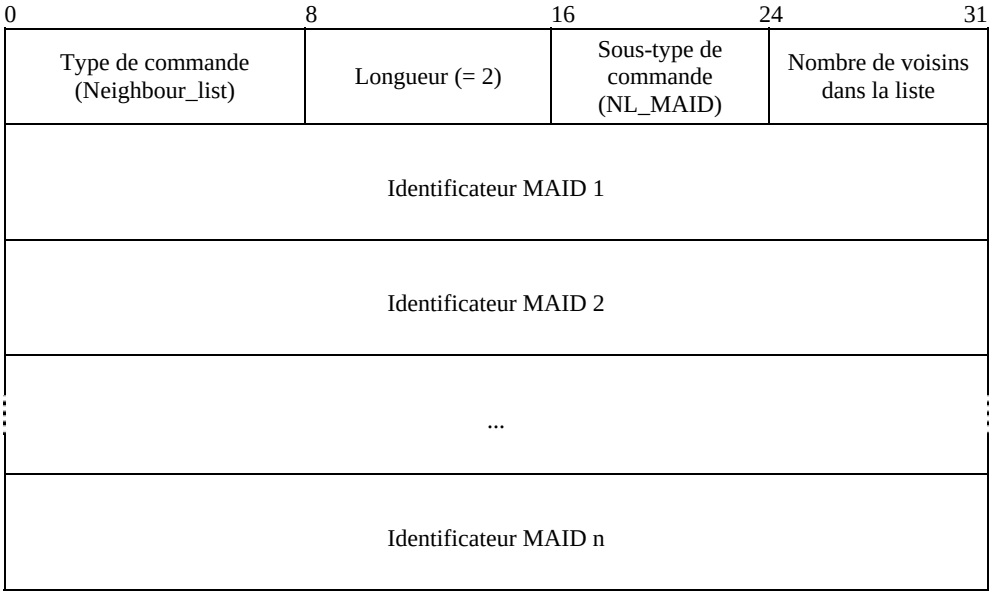

Figure 51 – Sous-commande NL_MAID

- AUTH

La commande AUTH est utilisée pour mettre à jour les informations d'authentification de session si nécessaire. S'il n'est pas nécessaire de mettre à jour les informations d'authentification, la commande ne fait que copier les données d'authentification envoyées par l'abonné. Les Figures 46 et 47 présentent le format de la commande AUTH.

7.3.3 PPROBREQ

Ce message est utilisé pour exécuter la procédure de *découverte de carte* afin de découvrir la situation réelle du réseau ainsi que d'explorer les voisins. Il est également utilisé pour vérifier si son homologue est toujours actif. La Figure 52 présente le format du message.

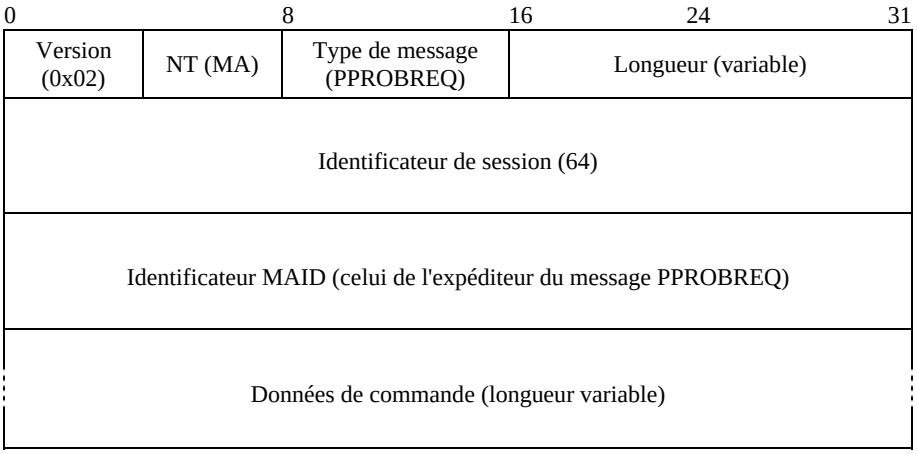

Figure 52 – Message PPROBREQ

La description de chaque champ est la suivante:

a) *Version* – version actuelle du protocole RMCP (0x02).

b) *NT* – type de nœud de l'émetteur du message (agent MA).

c) *Type de message* – type du message. La valeur est mise à PPROBREQ pour le message.

d) *Longueur* – longueur totale du message PPROBREQ, y compris les données de commande (en octets).

e) *Identificateur de session* – valeur de 64 bits de l'identificateur de session RMCP.

f) *Identificateur MAID* – identificateur MAID de l'expéditeur du message PPROBREQ.

g) *Données de commande* – ce champ peut inclure les informations suivantes afin d'obtenir les informations de carte.

- TIMESTAMP

La Figure 53 présente la commande TIMESTAMP, qui est utilisée pour examiner la distance entre deux agents MA. La description de chaque champ est la suivante:

a) *Type de commande* – TIMESTAMP.

b) *Longueur* – longueur totale de l'option Timestamp, égale à 16 octets.

c) *Réservé* – réservé à une fin ultérieure.

d) *Heure 1* – heure à laquelle l'émetteur du message PPROBREQ envoie le paquet à son homologue.

e) *Heure 2* – heure à laquelle le message PPROBREQ apparaît au niveau de l'homologue.

f) *Heure 3* – heure à laquelle le récepteur du message PPROBREQ envoie l'option Timestamp en réponse.

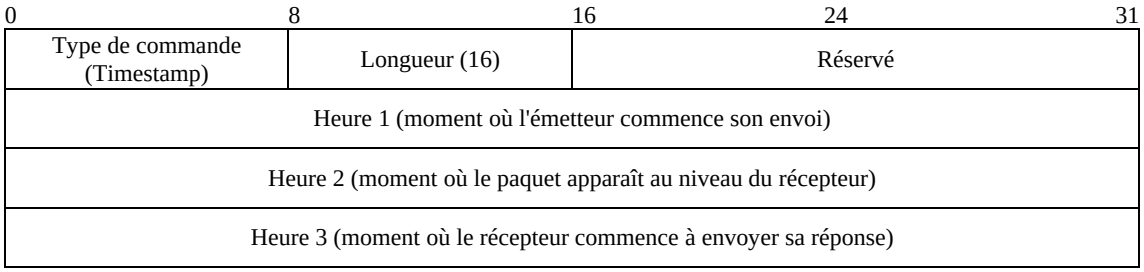

Figure 53 – Commande TIMESTAMP

- NEIGHBORLIST

Pour explorer les participants RMCP-2, chaque agent MA peut échanger des informations sur ses voisins en utilisant la commande NEIGHBORLIST. Le format et les utilisations de la commande sont présentés sur les Figures 50 et 51.

- ROOTPATH

Pour éviter les boucles et résoudre un problème triangulaire, l'agent MA sondeur peut inclure son *trajet depuis la racine* en utilisant la commande ROOTPATH qui est présentée sur la Figure 54. La description de chaque champ est la suivante:

a) *Type de commande* – ROOTPATH.

b) *Longueur* – longueur de l'option ROOTPATH, égale à 2 octets.

c) *Informations sur le trajet depuis la racine* – informations sur le trajet depuis la racine, dont le format et l'utilisation sont les suivants.

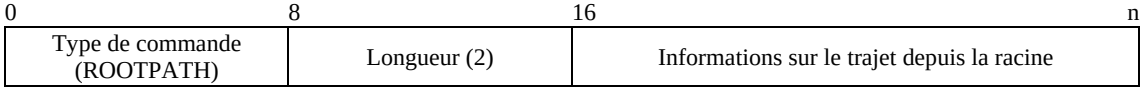

Figure 54 – Commande ROOTPATH

La Figure 55 présente les données de sous-commande de la commande ROOTPATH. La description de chaque champ est la suivante:

a) *Type de sous-commande* – type de trajet depuis la racine qui sera utilisé. Sept types sont actuellement définis et sont énumérés dans le Tableau 4.

b) *Nombre d'éléments sur le trajet ROOTPATH* – nombre d'éléments sur le trajet depuis la racine qui suivent.

c) *Un ou plusieurs éléments sur le trajet ROOTPATH* – informations sur les sauts compte tenu du type de sous-commande. La taille pour chaque type de trajet ROOTPATH est fixe et la taille peut être calculée en combinant la longueur pour chaque type. Les tailles par défaut pour chaque type de trajet ROOTPATH sont énumérées dans le Tableau 5.

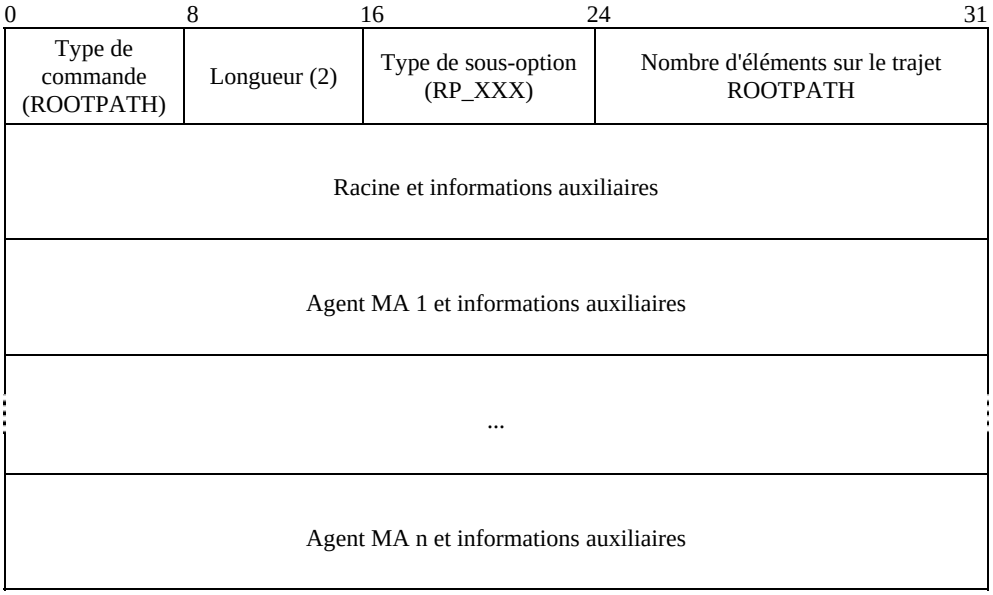

Figure 55 – Sous-commande RP_XXX

- SYSTEMINFO

Pour éviter qu'un nœud feuille uniquement ou un nœud lent puisse être placé à un niveau élevé dans la hiérarchie arborescente, des informations sur le système sont incluses (par exemple la largeur de bande en entrée et en sortie, le nombre possible d'agents CMA, etc.).

La Figure 41 présente le format de la commande SYSTEMINFO.

- DATAPROFILE

La commande DATAPROFILE est utilisée pour vérifier si l'agent MA sondé peut utiliser le mécanisme de fourniture de données que l'agent MA sondeur souhaite pour la réception. La Figure 44 présente le format de la commande DATAPROFILE et la Figure 84 son contenu.

7.3.4 PPROBANS

Ce message est une réponse au message PPROBREQ concernant l'exécution de la procédure de *découverte de carte* et la confirmation ou l'infirmation du fait que l'homologue est actif. Il peut indiquer la situation réelle du réseau et contenir un ensemble d'informations sur les voisins. La Figure 56 présente le format du message PPROBANS.

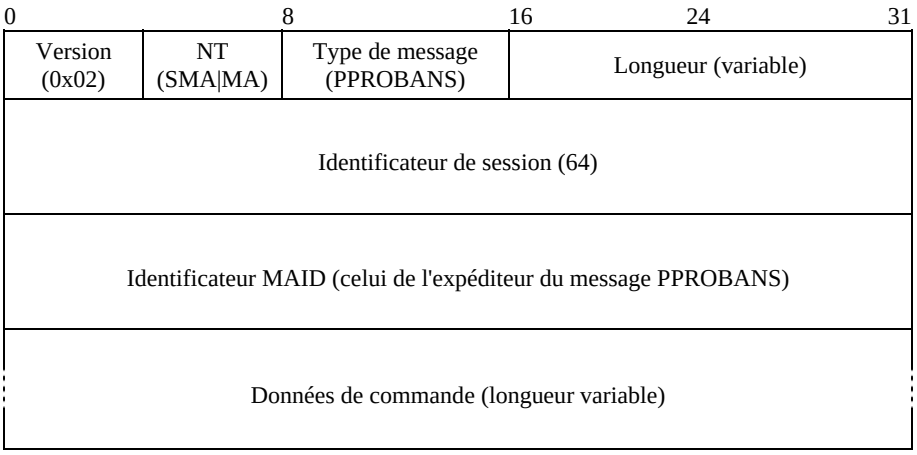

Figure 56 – Message PPROBANS

La description de chaque champ est la suivante:

a) *Version* – version actuelle du protocole RMCP (0x02).

b) *NT* – type de nœud de l'émetteur du message (agent SMA ou MA).

c) *Type de message* – type du message. La valeur est mise à PPROBANS pour le message.

d) *Longueur* – longueur totale du message PPROBANS, y compris les données de commande (en octets).

e) *Identificateur de session* – valeur de 64 bits de l'identificateur de session RMCP.

f) *Identificateur MAID* – identificateur MAID de l'émetteur du message PPROBANS.

g) *Données de commande* – ce champ devrait inclure des informations appropriées en réponse au message PPROBREQ. Il peut inclure les informations suivantes.

- TIMESTAMP

Cette commande est utilisée pour examiner la distance entre deux agents MA pendant la séquence de sondage. La Figure 53 présente le format des données de commande TIMESTAMP.

- NEIGHBORLIST

Cette commande NEIGHBORLIST est destinée à être utilisée pour explorer les participants RMCP-2. Chaque agent MA peut rassembler des informations concernant ses voisins en utilisant la commande NEIGHBORLIST présentée sur les Figures 50 et 51.

- ROOTPATH

Cette commande ROOTPATH est utilisée par chaque agent MA pour éviter les boucles et résoudre un problème triangulaire. L'agent MA sondeur peut inclure ses informations sur le trajet depuis la racine en utilisant la commande ROOTPATH. Les Figures 54 et 55 présentent le format de la commande ROOTPATH et le format des données de sous-commande.

- SYSTEMINFO

Pour éviter qu'un nœud feuille uniquement ou un nœud lent puisse être placé à un niveau élevé dans la hiérarchie arborescente, le message PPROBANS peut inclure des informations sur le système (par exemple la largeur de bande en entrée et en sortie, le nombre possible d'agents CMA, etc.) en utilisant la commande SYSTEMINFO. La Figure 41 présente le format de la commande SYSTEMINFO.

- DATAPROFILE

La commande DATAPROFILE est utilisée pour vérifier si l'agent MA sondé peut fournir les données que l'agent MA sondeur souhaite utiliser pendant la fourniture des données. La Figure 44 présente le format de la commande DATAPROFILE et la Figure 84 son contenu.

7.3.5 HSOLICIT

Le message HSOLICIT est utilisé pour gérer l'auto-organisation dans un réseau local. Il vise à trouver l'agent HMA à l'intérieur d'un réseau local. La Figure 57 présente le format du message HSOLICIT.

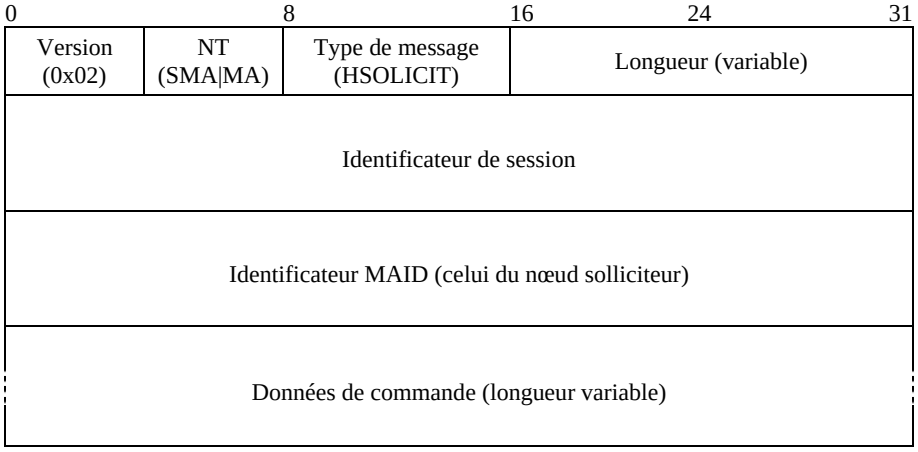

Figure 57 – Message HSOLICIT

La description de chaque champ est la suivante:

a) *Version* – version actuelle du protocole RMCP (0x02).

b) *NT* – type de nœud de l'émetteur du message (agent SMA ou MA).

c) *Type de message* – type du message. La valeur est mise à HSOLICIT pour le message.

d) *Longueur* – longueur totale du message HSOLICIT, y compris les données de commande (en octets).

e) *Identificateur de session* – valeur de 64 bits de l'identificateur de session RMCP.

f) *Identificateur MAID* – identificateur MAID du nœud qui envoie le message HSOLICIT au réseau local.

g) *Données de commande* – ce champ peut inclure des informations sur la liste des voisins. Il peut inclure les informations suivantes.

- AUTH

La commande AUTH est utilisée pour vérifier que le solliciteur est dans la même session RMCP-2. Les Figures 46 et 47 présentent la commande AUTH et sa sous-commande.

7.3.6 HANNOUNCE

En réponse au message HSOLICIT, ce message sert à annoncer l'existence de l'agent HMA dans un réseau local. La Figure 58 présente le format de ce message.

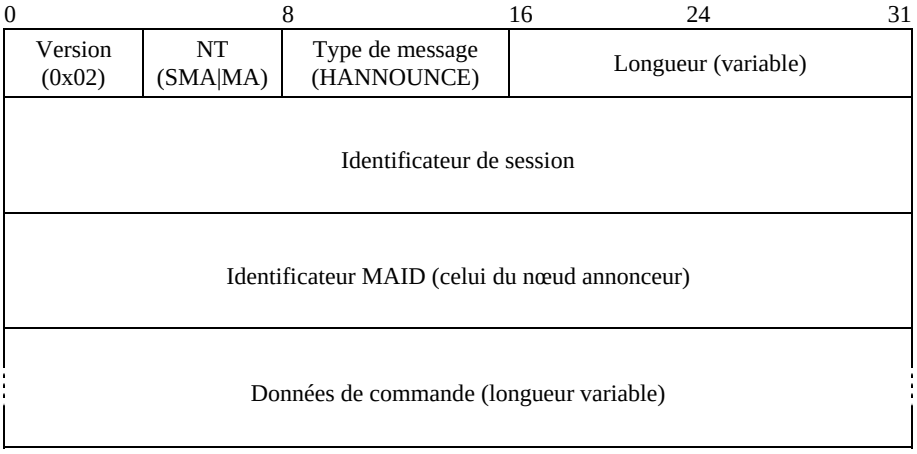

Figure 58 – Message HANNOUNCE

La description de chaque champ est la suivante:

a) *Version* – version actuelle du protocole RMCP (0x02).

b) *NT* – type de nœud de l'émetteur du message (agent SMA ou MA).

c) *Type de message* – type du message. La valeur est mise à HANNOUNCE pour le message.

d) *Longueur* – longueur totale du message HANNOUNCE, y compris les données de commande (en octets).

e) *Identificateur de session* – valeur de 64 bits de l'identificateur de session RMCP.

f) *Identificateur MAID* – identificateur MAID de l'agent HMA dans le réseau local.

g) *Données de commande* – ce champ peut inclure les informations suivantes.

- AUTH

La commande AUTH est utilisée pour vérifier que l'émetteur du message HANNOUNCE est dans la même session RMCP-2. Les Figures 46 et 47 présentent la commande AUTH et sa sous-commande.

- SYSTEMINFO

Pour indiquer sa puissance de système aux agents non HMA situés dans la même zone avec multidiffusion activée, l'agent HMA peut inclure la puissance de système d'agent MA (par exemple largeur de bande en entrée et en sortie, nombre gérable d'agents CMA). L'agent HMA peut aussi inclure des informations supplémentaires comme l'adresse IP locale ou sa durée de vie afin de pouvoir assurer un retour à la normale en cas de collision de messages HANNOUNCE.

La Figure 59 présente un message de sous-commande pour l'adresse IP locale, après la commande SYSTEMINFO. La description de chaque champ est la suivante:

a) *Type de sous-commande* – indication du fait que les données de sous-commande contiendront l'adresse IP locale.

b) *Longueur* – taille des données de sous-commande, égale à 6 octets.

c) *Adresse IP locale* – adresse IP de l'extrémité locale.

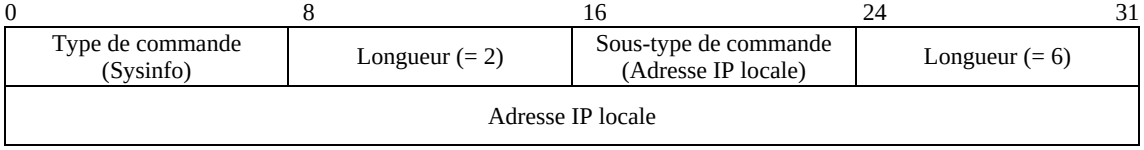

Figure 59 – Sous-commande pour l'adresse IP locale

Les données de commande pour la durée de vie de l'agent HMA sont présentées sur la Figure 60.

a) *Type de sous-commande* – type des données de sous-commande.

b) *Longueur* – taille des données de sous-commande, égale à 6 octets.

c) *Durée de fonctionnement* – durée, en secondes, après l'entrée du nœud dans la session RMCP-2.

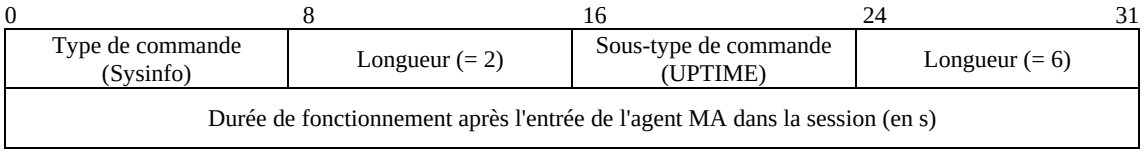

Figure 60 – Sous-commande UPTIME

• NEIGHBORLIST

Pour que les agents non HMA situés dans la même zone avec multidiffusion activée puissent partager les informations obtenues par exploration par l'agent HMA, celui-ci peut inclure la commande NEIGHBORLIST, présentée sur les Figures 50 et 51.

7.3.7 HLEAVE

Ce message est utilisé pour annoncer au réseau local que l'agent HMA sort de la session RMCP-2. La Figure 61 présente le format de ce message.

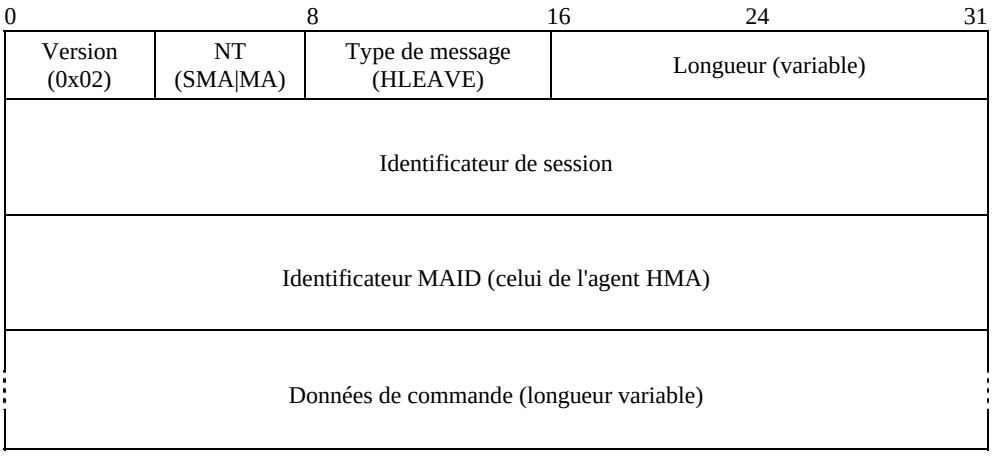

Figure 61 – Message HLEAVE

La description de chaque champ est la suivante:

a) *Version* – version actuelle du protocole RMCP (0x02).

b) *NT* – type de nœud de l'émetteur du message (agent SMA ou MA).

c) *Type de message* – type du message. La valeur est mise à HLEAVE pour le message.

d) *Longueur* – longueur totale du message HLEAVE, y compris les données de commande (en octets).

e) *Identificateur de session* – valeur de 64 bits de l'identificateur de session RMCP.

f) *Identificateur MAID* – identificateur MAID de l'agent HMA dans le réseau local.

g) *Données de commande* – ce champ peut inclure les informations suivantes.

- CANDIDATEHMA

Lorsqu'un agent HMA sort d'une session, les différents agents non HMA situés dans la zone avec multidiffusion activée peuvent se faire concurrence pour devenir le nouvel agent HMA, ce qui peut conduire à un remplissage de cette zone par des messages HANNOUNCE. Pour éviter les collisions pour le choix du nouvel agent HMA, l'agent HMA peut utiliser la commande CANDIDATEHMA, qui est présentée sur la Figure 62. La description de chaque champ est la suivante:

a) *Type de commande* – type à utiliser.

b) *Longueur* – taille des données de commande, égale à 2 octets.

c) *Informations sur les agents HMA possibles* – liste d'agents HMA possibles, le format détaillé étant le suivant.

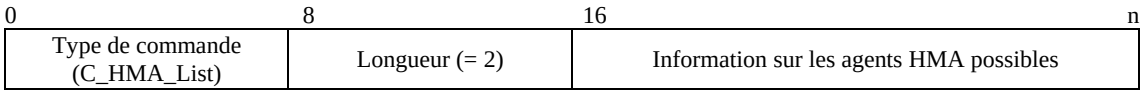

Figure 62 – Commande CANDIDATE HMA LIST

La Figure 63 présente la sous-commande de la commande CANDIDATE HMA LIST. La description de chaque champ est la suivante:

a) *Type de sous-commande* – type de liste d'agents HMA qui sera utilisé. Dans cet exemple, une liste d'identificateurs MAID est utilisée comme liste d'agents HMA possibles.

b) *Nombre de nœuds dans la liste* – nombre de nœuds dans la liste.

c) *Identificateur*(*s*) *MAID* – liste des identificateurs MAID des agents HMA possibles, fournie par l'agent HMA sortant.

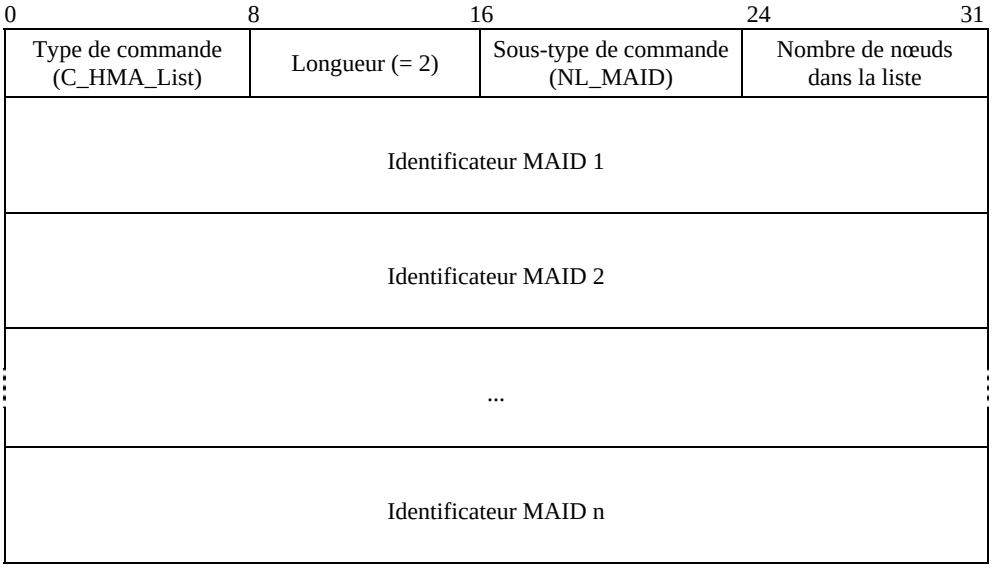

Figure 63 – Sous-commande CANDIDATE HMA LIST

- NEIGHBORLIST

Pour que les agents non HMA situés dans la même zone avec multidiffusion activée puissent partager les informations obtenues par exploration par l'agent HMA, celui-ci peut inclure la commande NEIGHBORLIST, présentée sur les Figures 50 et 51.

- ROOTPATH

L'agent HMA sortant peut inclure son trajet depuis la racine en utilisant la commande ROOTPATH de sorte que l'agent HMA nouvellement choisi puisse suivre le même trajet depuis la racine. Le type des données de commande est présenté sur les Figures 54 et 55.

- AUTH

La commande AUTH est utilisée pour vérifier que le solliciteur est dans la même session RMCP-2. Les Figures 46 et 47 présentent la commande AUTH et sa sous-commande.

- REASON

Les motifs de sortie de l'agent HMA peuvent varier en fonction de la situation. L'agent HMA peut par exemple sortir de la session de son propre gré ou parce que la session est terminée, auquel cas chaque agent non HMA situé dans la zone avec multidiffusion activée devrait sortir rapidement de la session.

Pour indiquer le motif pour lequel l'agent HMA sort d'une session, le message HLEAVE doit inclure la commande REASON telle qu'elle est présentée sur la Figure 64. La description de chaque champ est la suivante:

a) *Type de commande* – type de la commande.

b) *Longueur* – longueur des données de commande, égale à 4 octets.

c) *Code de motif* – ce champ de 2 octets contient un entier indiquant le motif particulier de la sortie. Les codes, accompagnés de leur signification, sont énumérés dans le Tableau 7.

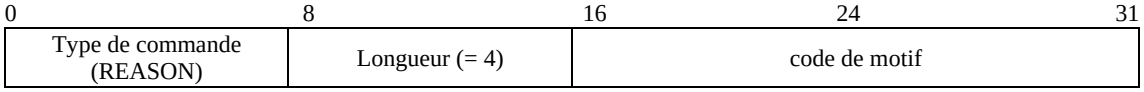

Figure 64 – Commande REASON

7.3.8 RELREQ

Ce message est utilisé par l'agent CMA pour demander à l'agent PMA la retransmission de données. Il inclut généralement un profil de données qui peut être négocié par le biais de l'échange de messages RELREQ et RELANS. La Figure 65 présente le format de ce message.

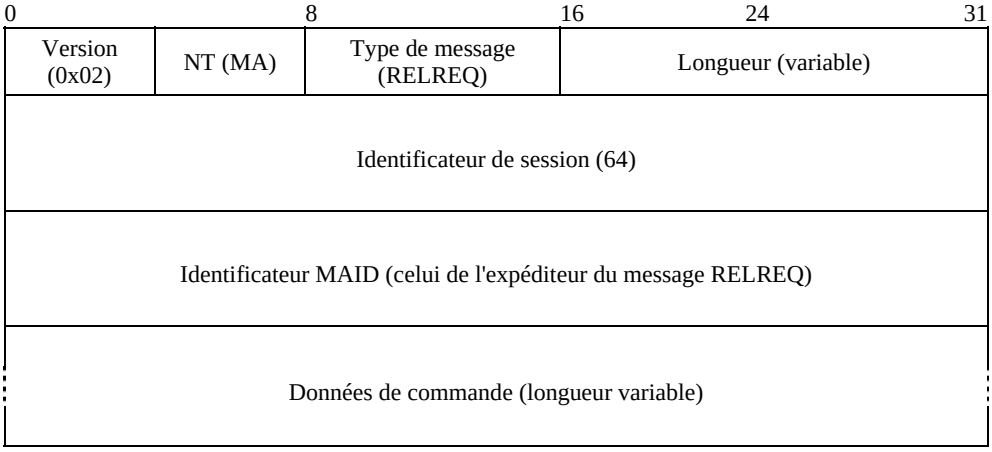

Figure 65 – Message RELREQ

La description de chaque champ est la suivante:

a) *Version* – version actuelle du protocole RMCP (0x02).

b) *NT* – type de nœud de l'émetteur du message (agent MA).

c) *Type de message* – type du message. La valeur est mise à RELREQ pour le message.

d) *Longueur* – longueur totale du message RELREQ, y compris les données de commande (en octets).

e) *Identificateur de session* – valeur de 64 bits de l'identificateur de session RMCP.

f) *Identificateur MAID* – identificateur MAID du nœud qui envoie le message RELREQ.

g) *Données de commande* – ce champ peut inclure une ou plusieurs demandes de relais. Les commandes qui peuvent être utilisées dans ce message sont les suivantes.

• COMMAND

Lorsque l'agent CMA a besoin d'obtenir des informations auprès de l'agent PMA, il peut l'interroger en utilisant la commande COMMAND dans le message RELREQ.

Par exemple, chaque fois qu'un agent MA se raccorde à un agent PMA au cours d'une procédure d'entrée ou de changement de parent, il a besoin de connaître le trajet depuis la racine de son nouvel agent PMA en vue du diagnostic de réseau et de la détection de boucle. Dans ce cas, l'agent MA utilise la commande COMMAND pour obtenir le trajet ROOTPATH de l'agent PMA auquel il se rallie.

La Figure 66 présente le format de la commande COMMAND. La description de chaque champ est la suivante:

a) *Type de commande* – type de la commande.

b) *Longueur* – longueur des données de commande, égale à 4 octets.

c) *Code de commande* – ce champ de 2 octets contient un entier indiquant le motif particulier de la sortie. La valeur codée et sa signification sont données au § 8.3.

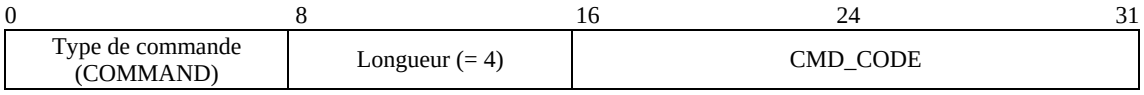

Figure 66 – Commande COMMAND

• DATAPROFILE

Chaque fois qu'un agent CMA se raccorde à un agent PMA, les deux agents MA devraient s'entendre sur le mécanisme de fourniture des données. Pour cela, chaque agent CMA utilise la commande DATAPROFILE pour procéder à une négociation avec son agent PMA. Les Figures 44 et 45 présentent le format de la commande DATAPROFILE et la Figure 84 présente son contenu.

• TIMESTAMP

Chaque agent CMA devrait mesurer le délai saut par saut entre l'agent PMA et lui-même. A cette fin, il inclut la commande TIMESTAMP telle qu'elle est présentée sur la Figure 53 dans le message RELREQ.

7.3.9 RELANS

En réponse au message RELREQ, le message RELANS est envoyé par l'agent PMA à l'agent CMA. Il a pour objet de préciser si la demande de relais est autorisée. Il peut aussi contenir des informations supplémentaires qui sont nécessaires pour négocier le canal de données entre l'agent PMA et l'agent CMA. Le format du message RELANS est présenté sur la Figure 67.

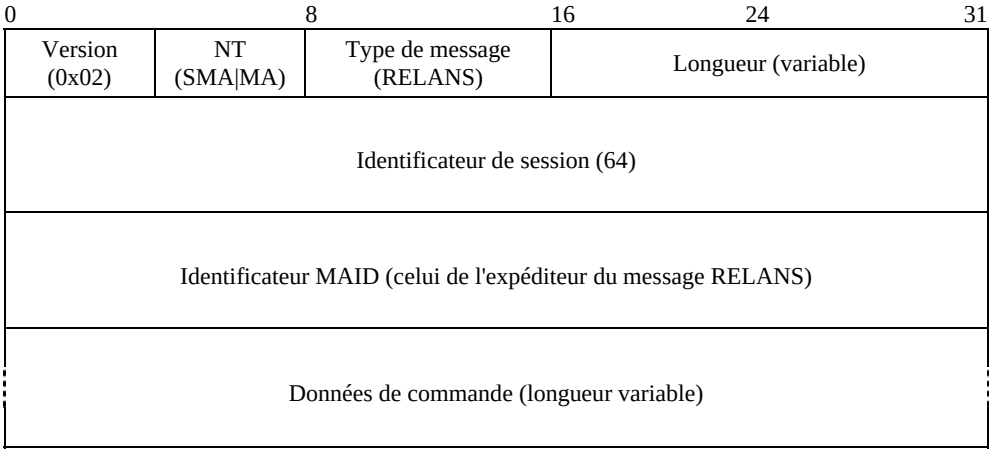

Figure 67 – Message RELANS

La description de chaque champ est la suivante:

a) *Version* – version actuelle du protocole RMCP (0x02).

b) *NT* – type de nœud de l'émetteur du message. Comme ce message peut être envoyé par l'agent SMA et par l'agent MA, le type de nœud pour le message peut être l'agent SMA ou l'agent MA.

c) *Type de message* – type du message. La valeur est mise à RELANS pour le message.

d) *Longueur* – longueur totale du message RELANS, y compris les données de commande (en octets).

e) *Identificateur de session* – valeur de 64 bits de l'identificateur de session RMCP.

f) *Identificateur MAID* – identificateur MAID du nœud qui envoie le message RELANS.

g) *Données de commande* – ce champ peut inclure une ou plusieurs des commandes suivantes.

- RESULT

Pour indiquer si la demande RELREQ de l'agent CMA a abouti, l'agent PMA utilise la commande RESULT dans chaque message RELANS. Si la demande de relais a abouti, l'agent PMA donne le code de résultat OK dans la commande RESULT. Dans le cas contraire, il donne le code d'erreur approprié (par exemple relais refusé en raison de la politique ou de l'épuisement des ressources). La Figure 49 présente le format de la commande RESULT.

- DATAPROFILE

Chaque fois qu'un agent CMA se raccorde à un agent PMA, il envoie le message RELREQ avec la commande DATAPROFILE pour négocier le mécanisme de fourniture des données. Les Figures 44 et 45 présentent le format de la commande DATAPROFILE et la Figure 84 présente son contenu.

- TIMESTAMP

La Figure 53 présente la commande TIMESTAMP, utilisée pour examiner la distance entre deux agents MA.

- ROOTPATH

Chaque fois qu'un agent CMA demande le trajet depuis la racine au moyen de la commande COMMAND, l'agent PMA répond à l'agent CMA en lui donnant les informations ROOTPATH. Les Figures 54 et 55 présentent la commande ROOTPATH.

7.3.10 STREQ

Le message STREQ est utilisé pour contrôler l'état des agents MA dans la session. La Figure 68 présente le format de ce message.

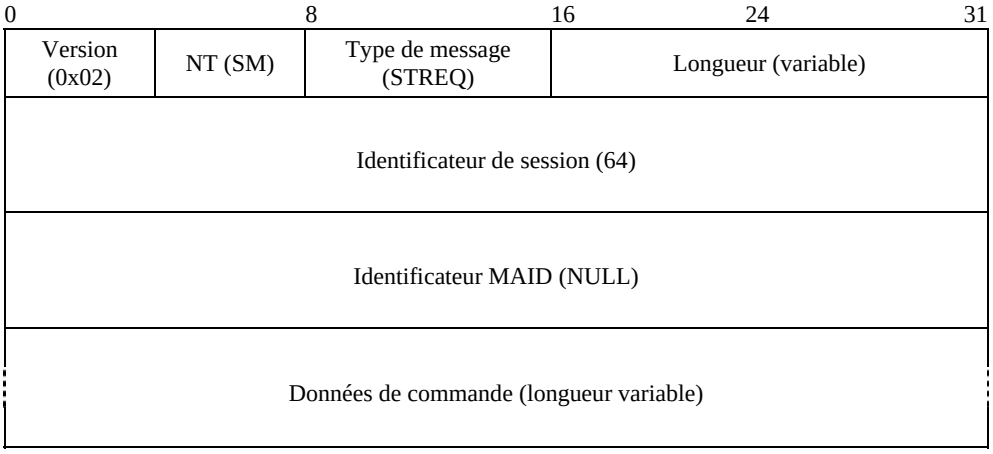

Figure 68 – Message STREQ

La description de chaque champ est la suivante:

a) *Version* – version actuelle du protocole RMCP (0x02).

b) *NT* – type de nœud de l'émetteur du message. Comme ce message ne peut être envoyé que par le gestionnaire de session, le type de nœud pour le message est uniquement le gestionnaire de session.

c) *Type de message* – type du message. Il est mis à STREQ pour le message.

d) *Longueur* – longueur totale du message STREQ, y compris les données de commande (en octets).

e) *Identificateur de session* – valeur de 64 bits de l'identificateur de session RMCP.

f) *Identificateur MAID* – comme le gestionnaire de session n'a pas d'identificateur MAID, ce champ devrait être mis à zéro.

g) *Données de commande* – ce champ peut inclure une ou plusieurs demandes de notification d'état. Les commandes qui peuvent être incluses sont les suivantes.

- COMMAND

Le message STREQ devrait inclure la commande COMMAND présentée sur la Figure 66 pour indiquer la notification d'état requise. Pour obtenir l'état d'un agent MA, le gestionnaire de session utilise la commande COMMAND dans le message STREQ. Le Tableau 6 récapitule plusieurs commandes pour le contrôle d'état et les notifications d'état attendues. La Figure 66 présente le format de la commande COMMAND.

- TREEEXPLOR

L'inspection de l'état de la totalité de l'arborescence peut entraîner un risque d'explosion des notifications. Il est donc très important de limiter la partie de l'arborescence à inspecter. La Figure 69 présente la commande TREEEXPLOR, utilisée pour limiter la partie de l'arborescence. Les champs de la commande TREEEXPLOR sont les suivants:

a) *Type de commande* – type de la commande: TreeExplor.

b) *Longueur* – longueur de l'option TreeExplor, qui devrait être égale à 4 octets.

c) *Réservé* – réservé pour une utilisation future.

d) *TREE_DEPTH* – entier de 8 bits indiquant la partie de l'arborescence.

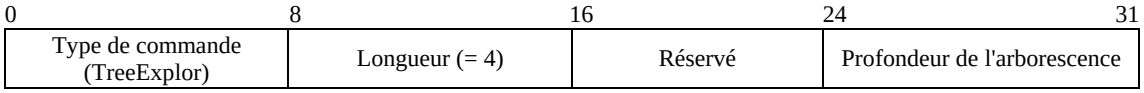

Figure 69 – Commande TREEEXPLOR

7.3.11 STANS

Ce message est utilisé pour contrôler l'état des agents MA dans la session. La Figure 70 présente le format du message STANS.

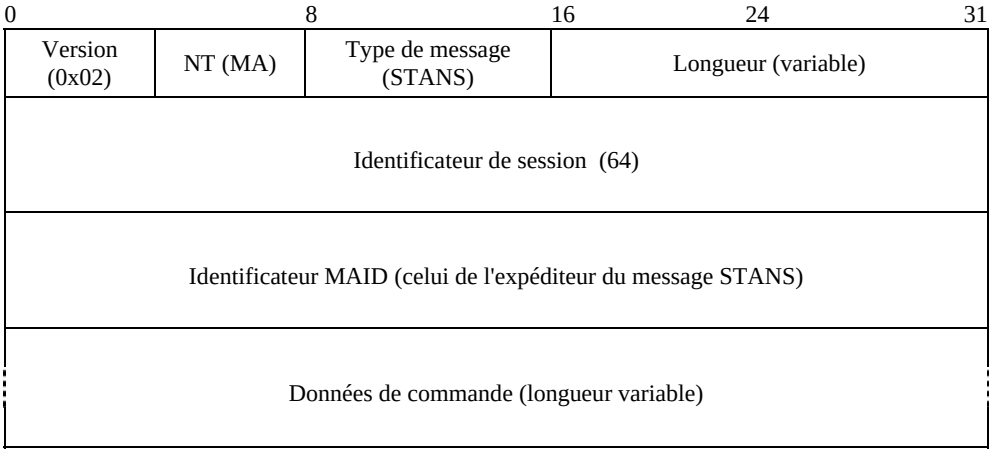

Figure 70 – Message STANS

La description de chaque champ est la suivante:

a) *Version* – version actuelle du protocole RMCP (0x02).

b) *NT* – type de nœud de l'émetteur du message. Comme ce message ne peut être envoyé que par l'agent MA, le type de nœud pour le message est l'agent MA.

c) *Type de message* – type du message. Il est mis à STANS pour le message.

d) *Longueur* – longueur totale du message STANS, y compris les données de commande (en octets).

e) *Identificateur de session* – valeur de 64 bits de l'identificateur de session RMCP.

f) *Identificateur MAID* – identificateur MAID de l'émetteur du message STANS.

g) *Données de commande* – ce champ devrait inclure une ou plusieurs réponses aux demandes de notification d'état. Il peut inclure les informations suivantes.

• REPORT

Conformément à la demande du gestionnaire de session, l'agent MA devrait répondre par une notification appropriée. Le format de message pour chaque notification est de la forme {type de commande, sous-type de commande}.

Conformément à la demande du gestionnaire de session telle qu'indiquée dans le Tableau 6, chaque agent MA retourne la notification appropriée au gestionnaire de session. Les Figures 71 à 76 présentent plusieurs notifications.

La Figure 71 présente la notification sur la place relative aux agents CMA. La description de chaque champ est la suivante:

a) *Type de sous-commande* – type de liste d'agents HMA qui sera utilisé. Dans cet exemple, la liste d'identificateurs MAID est utilisée comme liste d'agents HMA possibles.

b) *Longueur* – nombre d'éléments dans la liste.

c) *Nombre d'agents CMA attribués* – place relative aux agents CMA.

d) *Nombre d'agents CMA réservés* – place réservée par les agents CMA. Le nombre d'agents CMA disponibles correspondra donc à la différence entre le nombre d'agents CMA attribués et le nombre d'agents CMA réservés.

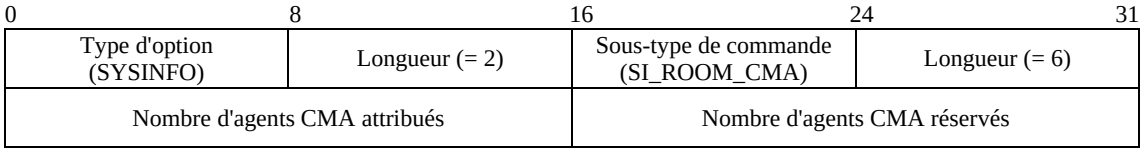

Figure 71 – Commande SYSINFO_ROOM_CMA

La Figure 72 présente la notification sur la valeur de qualité de service qui peut être prise en charge par un système. La description de chaque champ est la suivante:

a) *Type de sous-commande* – type de sous-commande à utiliser.

b) *Longueur* – taille de la sous-commande.

c) *Largeur de bande entrante de la carte NIC* – largeur de bande entrante maximale de la carte d'interface de réseau (en Mbit/s).

d) *Largeur de bande sortante de la carte NIC* – largeur de bande sortante maximale de la carte d'interface de réseau (en Mbit/s).

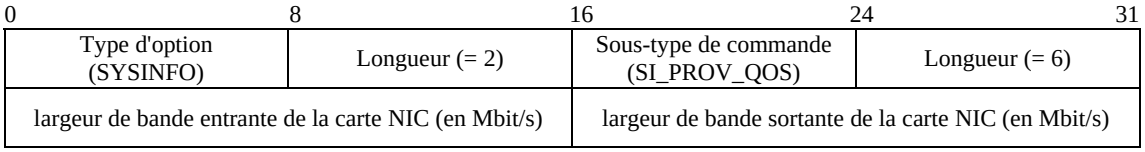

Figure 72 – Commande SYSINFO_PROVIDABLE_QOS

La Figure 73 présente la notification sur la durée de fonctionnement du système après l'entrée de l'agent MA. La description de chaque champ est la suivante:

a) *Type de sous-commande* – type de sous-commande à utiliser.

b) *Longueur* – taille de la sous-commande.

c) *Durée de fonctionnement après l'entrée de l'agent MA dans la session* – temps en secondes écoulé après l'entrée de l'agent MA dans la session.

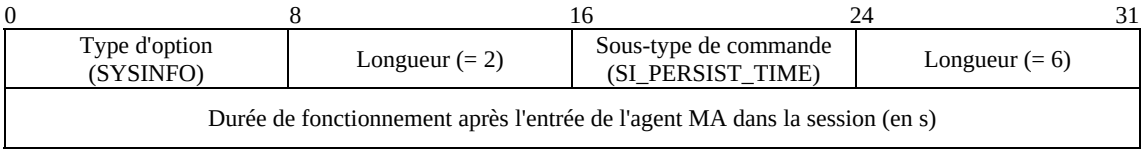

Figure 73 – Commande SYSINFO_PERSIST_TIME

La Figure 74 présente la notification sur la qualité de service perçue par chaque agent MA. La description de chaque champ est la suivante:

a) *Type de sous-commande* – type de sous-commande à utiliser.

b) *Longueur* – taille de la sous-commande, qui devrait être égale à 22 octets.

c) *Nombre d'agents PMA* – nombre d'agents PMA directement raccordés.

d) *Nombre d'agents CMA* – nombre d'agents CMA directement raccordés.

e) *Nombre total d'octets entrants* – nombre total d'octets de données entrantes.

f) *Nombre de paquets entrants* – nombre total de paquets entrants.

g) *Nombre total d'octets sortants* – nombre total d'octets de données sortantes.

h) *Nombre de paquets sortants* – nombre total de paquets sortants.

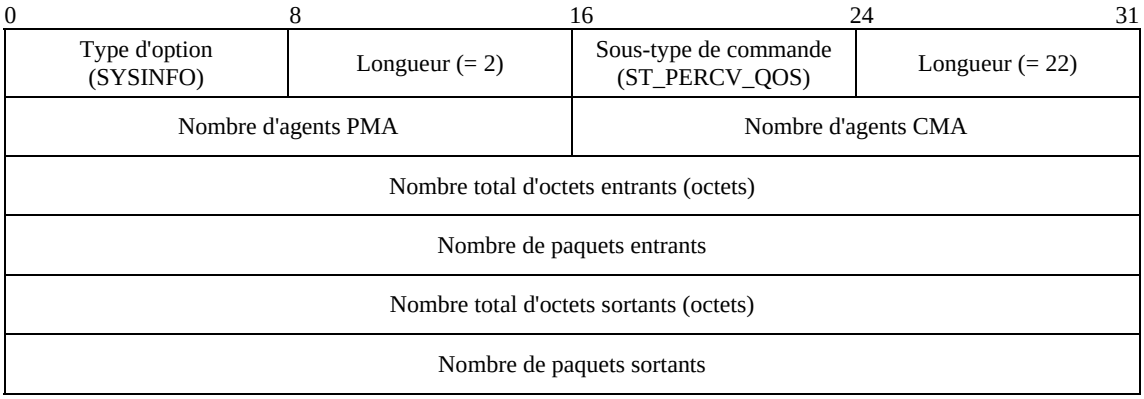

Figure 74 – Commande STATE_PERCEIVED_QOS

La Figure 75 présente la notification sur l'état de l'arborescence TREE. La description de chaque champ est la suivante:

a) *Type de sous-commande* – type de sous-commande à utiliser.

b) *Nombre d'identificateurs MAID* – nombre d'identificateurs MAID des agents HMA possibles, dont la liste est fournie par l'agent HMA sortant.

c) *Identificateur MAID d'agent PMA* – identificateur MAID de l'agent PMA directement raccordé.

d) *Identificateurs MAID d'agent CMA* – liste des identificateurs MAID des agents CMA directement raccordés.

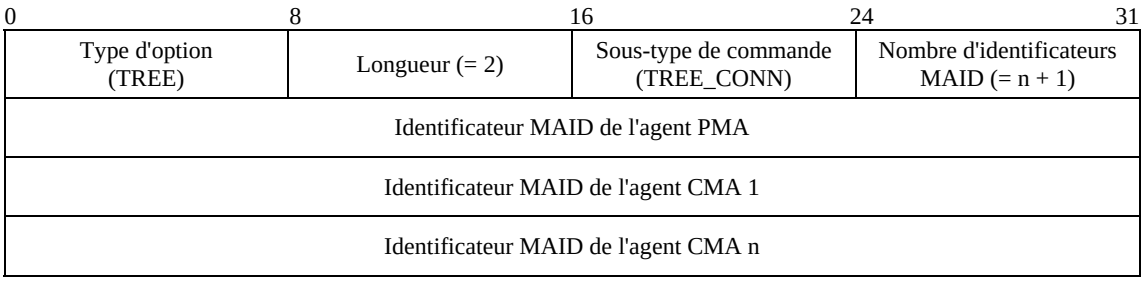

Figure 75 – Commande TREE_CONNECTION

La Figure 76 présente la notification sur les membres de l'arborescence TREE. La description de chaque champ est la suivante:

a) *Type de sous-commande* – type de sous-commande à utiliser.

b) *Nombre d'identificateurs MAID* – nombre d'identificateurs MAID énumérés dans la commande.

c) *Identificateurs MAID* – liste des identificateurs MAID d'une branche spécifique; par exemple le nœud situé au sommet de la branche spécifique sera présenté dans le champ MAID 1, le nœud situé en bas sera présenté dans le champ MAID n.

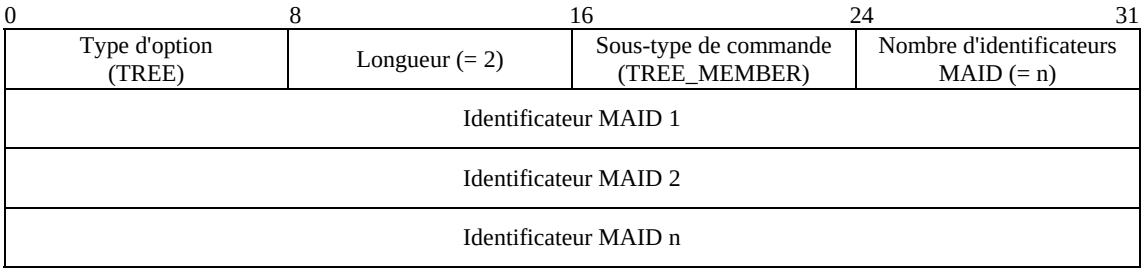

Figure 76 – Commande TREE_MEMBERSHIP

Il est à noter que chaque notification est précédée d'une commande appropriée de 2 octets.

7.3.12 STCOLREQ

Le message STCOLREQ est utilisé pour contrôler une session RMCP-2 de façon analogue au message STREQ. Mais il existe deux différences: le message STREQ est limité à un seul agent MA alors que le message STCOLREQ peut s'appliquer à tout ou partie de la session; le message STREQ peut uniquement être envoyé par le gestionnaire de session alors que le message STCOLREQ est envoyé par l'agent PMA.

Lorsqu'un agent MA reçoit le message STCOLREQ en provenance de l'agent PMA, il démarre la *procédure de collecte de l'état* et transmet ce message à ses agents CMA situés dans la zone limitée par l'option TreeExplor. La Figure 77 présente le format du message STCOLREQ.

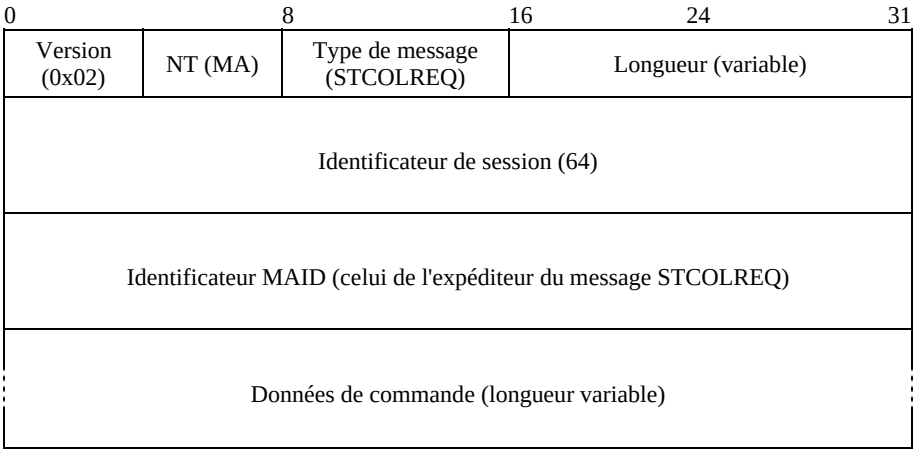

Figure 77 – Message STCOLREQ

La description de chaque champ est la suivante:

a) *Version* – version actuelle du protocole RMCP (0x02).

b) *NT* – type de nœud de l'émetteur du message. Comme ce message n'est envoyé que par l'agent PMA, le type de nœud pour le message est mis à l'agent MA.

c) *Type de message* – type du message. Il est mis à STCOLREQ pour le message.

d) *Longueur* – longueur totale du message STCOLREQ, y compris les données de commande (en octets).

e) *Identificateur de session* – valeur de 64 bits de l'identificateur de session RMCP.

f) *Identificateur MAID* – identificateur MAID de l'émetteur du message STCOLREQ. En principe, c'est l'identificateur MAID de l'agent PMA qui est communiqué à l'agent CMA.

g) *Données de commande* – ce champ peut inclure une ou plusieurs demandes de notification d'état. Il peut inclure les informations suivantes.

• COMMAND

Lorsqu'un agent PMA fait une demande d'état à ses agents CMA, il inclut la commande COMMAND dans son message STCOLREQ. Le Tableau 6 récapitule plusieurs commandes pour le contrôle d'état.

• TREEEXPLOR

L'inspection de l'état de la totalité de l'arborescence peut entraîner un risque d'explosion des notifications. Il est donc très important de limiter la partie de l'arborescence à inspecter.

La Figure 69 présente la commande TREEEXPLOR, utilisée pour limiter la partie de l'arborescence.

7.3.13 STCOLANS

La Figure 78 présente le format du message STCOLANS, utilisé pour répondre au message STCOLREQ. Le message STCOLANS communique l'état collecté d'aval en amont. Il suit la hiérarchie arborescente en sens inverse pour atteindre sa destination finale à savoir le nœud qui a envoyé le message STCOLREQ.

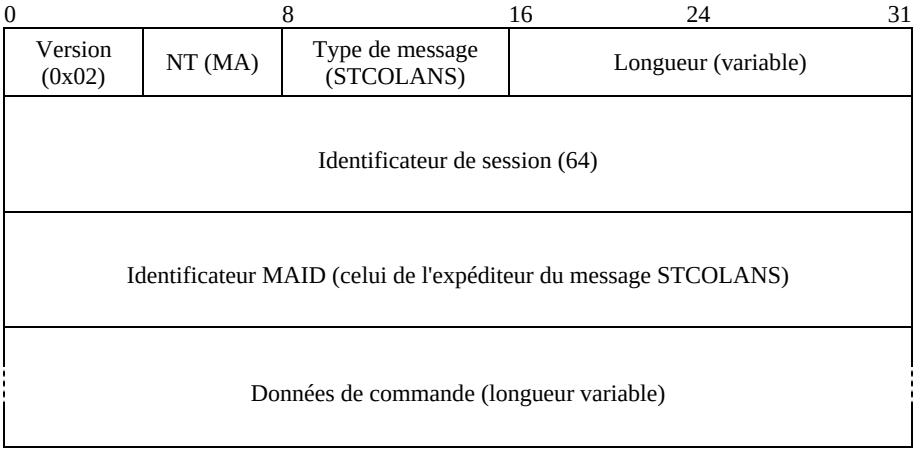

Figure 78 – Message STCOLANS

La description de chaque champ est la suivante:

a) *Version* – version actuelle du protocole RMCP (0x02).

b) *NT* – type de nœud de l'émetteur du message. Comme ce message est envoyé par l'agent CMA, le type de nœud pour le message est mis à l'agent MA.

c) *Type de message* – type du message. Il est mis à STCOLANS pour le message.

d) *Longueur* – longueur totale du message STCOLANS, y compris les données de commande (en octets).

e) *Identificateur de session* – valeur de 64 bits de l'identificateur de session RMCP.

f) *Identificateur MAID* – identificateur MAID de l'émetteur du message STCOLANS. En principe, c'est l'identificateur MAID de l'agent CMA qui est communiqué à l'agent PMA.

g) *Données de commande* – ce champ peut inclure une ou plusieurs réponses aux demandes de notification d'état. Il peut inclure les informations suivantes.

• REPORT

Conformément à la demande de l'agent PMA, l'agent CMA devrait répondre par une notification appropriée. Le format de message pour chaque notification est de la forme {type de commande, sous-type de commande}.

Conformément à la demande telle qu'indiquée dans le Tableau 6, chaque agent CMA envoie des notifications appropriées à son agent PMA. Les Figures 71 à 76 présentent plusieurs notifications.

7.3.14 LEAVREQ

Ce message est utilisé à différentes fins. Il est d'abord utilisé pour la sortie: quand un agent MA sort de la session RMCP-2 ou quand un agent MA quitte son agent PMA dans le cadre d'un changement de parent, il envoie le message LEAVREQ aux agents MA correspondant au moyen de la procédure de sortie.

Un gestionnaire de session et un agent PMA peuvent utiliser ce message mais leurs cibles sont différentes. La cible du gestionnaire de session est n'importe quel agent MA de la session alors que la cible de l'agent PMA est uniquement son agent CMA.

Enfin, ce message est utilisé pour mettre fin à une session. Lorsque l'agent SMA sort de la session, ce message devrait être transmis à l'agent MA le plus éloigné dans la hiérarchie arborescente. La Figure 79 présente le format du message LEAVREQ.

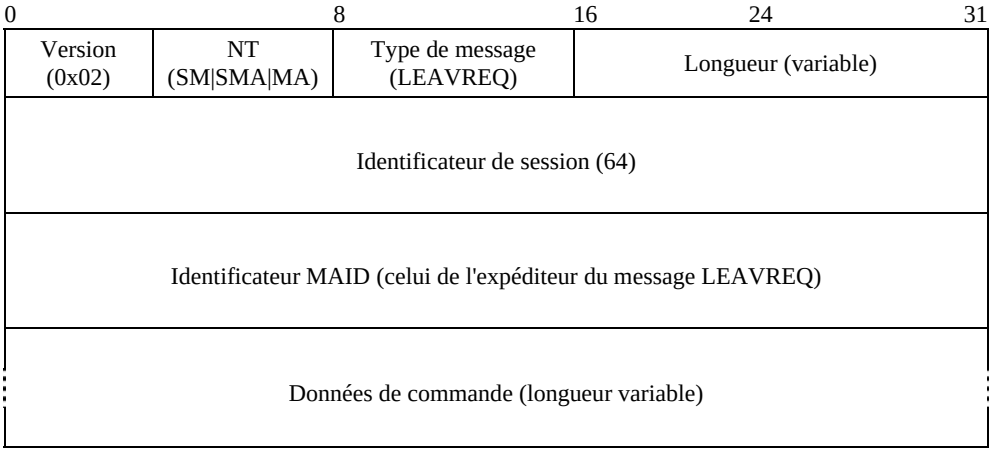

Figure 79 – Message LEAVREQ

La description de chaque champ est la suivante:

a) *Version* – version actuelle du protocole RMCP (0x02).

b) *NT* – type de nœud de l'émetteur du message. Comme ce message peut être envoyé par toutes les entités RMCP-2, le type de nœud pour le message peut être mis à l'une des entités SM, SMA ou MA.

c) *Type de message* – type du message. Il est mis à LEAVREQ.

d) *Longueur* – longueur totale du message LEAVREQ, y compris les données de commande (en octets).

e) *Identificateur de session* – valeur de 64 bits de l'identificateur de session RMCP.

f) *Identificateur MAID* – identificateur MAID de l'expéditeur du message LEAVREQ. Lorsque ce message est produit par le gestionnaire de session, ce champ doit être mis à zéro.

g) *Données de commande* – ce champ peut inclure les informations suivantes.

- REASON

Pour indiquer le motif pour lequel l'agent MA essaie de sortir d'une session, le message LEAVREQ doit inclure la commande REASON. La Figure 64 présente le format de la commande REASON.

7.3.15 LEAVANS

Pour confirmer le message LEAVREQ, l'agent MA qui reçoit le message LEAVREQ retourne un message LEAVANS. La Figure 80 présente le format du message LEAVANS.

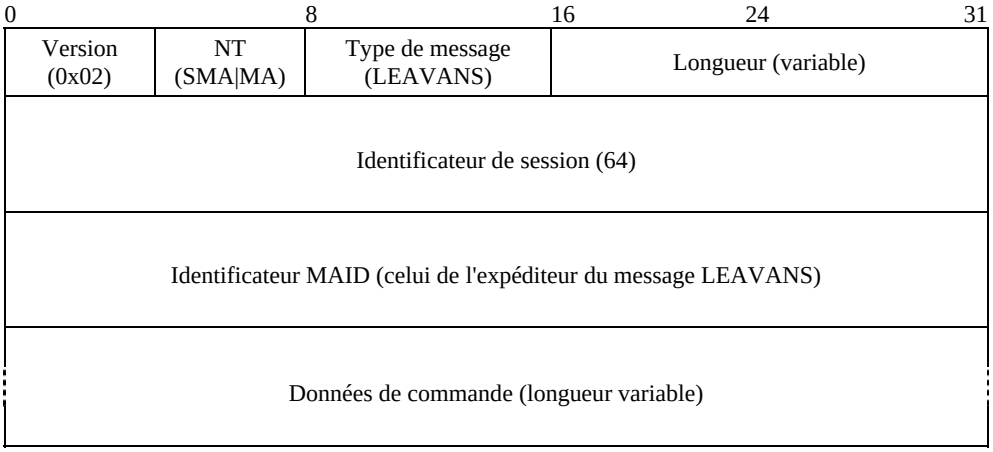

Figure 80 – Message LEAVANS

La description de chaque champ est la suivante:

a) *Version* – version actuelle du protocole RMCP (0x02).

b) *NT* – type de nœud de l'émetteur du message. Le type de nœud pour le message peut être mis à l'agent SMA ou MA.

c) *Type de message* – type du message. Il est mis à LEAVANS.

d) *Longueur* – longueur totale du message LEAVANS, y compris les données de commande (en octets).

e) *Identificateur de session* – valeur de 64 bits de l'identificateur de session RMCP.

f) *Identificateur MAID* – identificateur MAID de l'expéditeur du message LEAVANS.

g) *Données de commande* – ce champ peut inclure des options parmi celles qui sont disponibles. Il peut inclure les informations suivantes.

- RESULT

Le message LEAVANS est utilisé pour indiquer si le message LEAVREQ de l'agent MA sortant est bien arrivé. Le code de résultat de la commande RESULT devrait donc toujours avoir la signification OK.

7.3.16 HB

Le message HB est envoyé régulièrement par l'agent SMA pour donner des informations d'horloge à travers la session RMCP-2. Avec ce message, chaque agent MA peut diagnostiquer la situation du réseau. La Figure 81 présente le format du message HB.

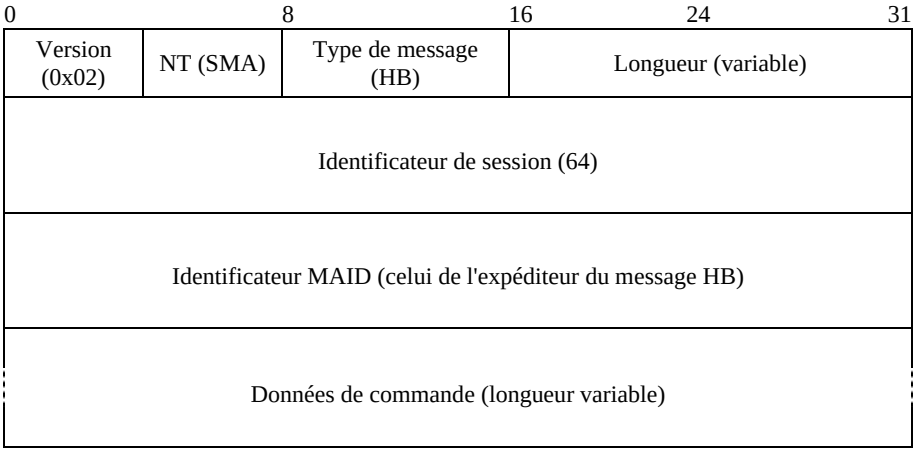

Figure 81 – Message HB

La description de chaque champ est la suivante:

a) *Version* – version actuelle du protocole RMCP (0x02).

b) *NT* – type de nœud de l'émetteur du message. Le type de nœud pour le message peut être mis à l'agent SMA.

c) *Type de message* – type du message. Il est mis à HB.

d) *Longueur* – longueur totale du message HB, y compris les données de commande (en octets).

e) *Identificateur de session* – valeur de 64 bits de l'identificateur de session RMCP.

f) *Identificateur MAID* – identificateur MAID de l'expéditeur du message HB. Le message HB est retransmis par l'agent PMA à l'agent CMA, mais ce champ n'est pas modifié par l'agent PMA intermédiaire.

g) *Données de commande* – ce champ devrait inclure l'option ROOTPATH qui est présentée sur la Figure 54. Il peut inclure les informations suivantes.

- ROOTPATH

La commande ROOTPATH est mise à jour par chaque agent MA. Depuis la racine, chaque agent MA qui sert de relais pour le message HB ajoute son identificateur MAID ainsi que des informations auxiliaires comme le délai saut par saut ou la largeur de bande saut par saut conformément à sa configuration précédente dans la session. Les Figures 54 et 55 présentent la commande ROOTPATH et sa sous-commande.

- AUTH

Pour rafraîchir les informations d'authentification pendant la session, de nouvelles informations d'authentification peuvent être fournies au moyen de la commande AUTH. Les Figures 46 et 47 présentent la commande AUTH et sa sous-commande.

- COMMAND

Lorsqu'un agent PMA essaie de revenir à un fonctionnement normal après une partition du réseau, ses descendants peuvent lancer la procédure de retour à la normale après un défaut dans le réseau par suite de l'expiration de la temporisation d'attente du message HB. En d'autres termes, une partition au niveau d'un seul point peut entraîner un effet en chaîne concernant le retour à la normale après un défaut.

Il est donc nécessaire de produire un pseudo-message HB pour retarder le lancement de la procédure de retour à la normale par les descendants et de pouvoir communiquer ce pseudo-message aux descendants.

La commande RP_PSEUDO indiquée dans le Tableau 4 est utilisée pour indiquer que la commande ROOTPATH dans le message HB contenant cette commande COMMAND est une pseudo-commande ROOTPATH.

7.3.17 TERMREQ

Le message TERMREQ est utilisé pour mettre fin à une session RMCP-2 existante. Il est envoyé par le gestionnaire de session puis il est retransmis par l'agent SMA aux agents MA les plus éloignés dans la hiérarchie arborescente. La Figure 82 présente le format du message TERMREQ.

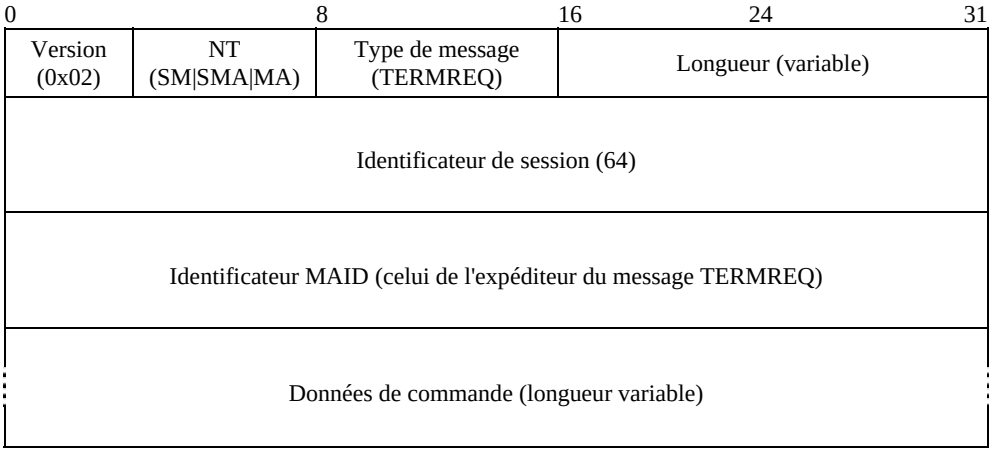

Figure 82 – Message TERMREQ

La description de chaque champ est la suivante:

a) *Version* – version actuelle du protocole RMCP (0x02).

b) *NT* – type de nœud de l'émetteur du message. Comme ce message est envoyé par le gestionnaire de session et doit être retransmis à l'agent MA le plus éloigné dans l'arborescence RMCP-2, le type de nœud pour le message peut être mis à SM, SMA ou MA.

c) *Type de message* – type du message. Il est mis à TERMREQ.

d) *Longueur* – longueur totale du message TERMREQ, y compris les données de commande (en octets).

e) *Identificateur de session* – valeur de 64 bits de l'identificateur de session RMCP.

f) *Identificateur MAID* – identificateur MAID de l'expéditeur du message TERMREQ. Lorsque ce message est envoyé par le gestionnaire de session, ce champ doit être mis à zéro. En principe, l'identificateur MAID du message TERMREQ communiqué à l'agent MA est celui de son agent PMA.

g) *Données de commande* – ce champ peut inclure le code de motif suivant pour expliquer la fin de la session.

- REASON

Pour indiquer le motif pour lequel il est mis fin à la session, le message TERMREQ devrait inclure la commande REASON telle qu'elle est présentée sur la Figure 64. Le motif sera soit qu'aucun agent SMA n'existe soit que le détenteur de la session y met fin.

7.3.18 TERMANS

La Figure 83 présente le format du message TERMANS.

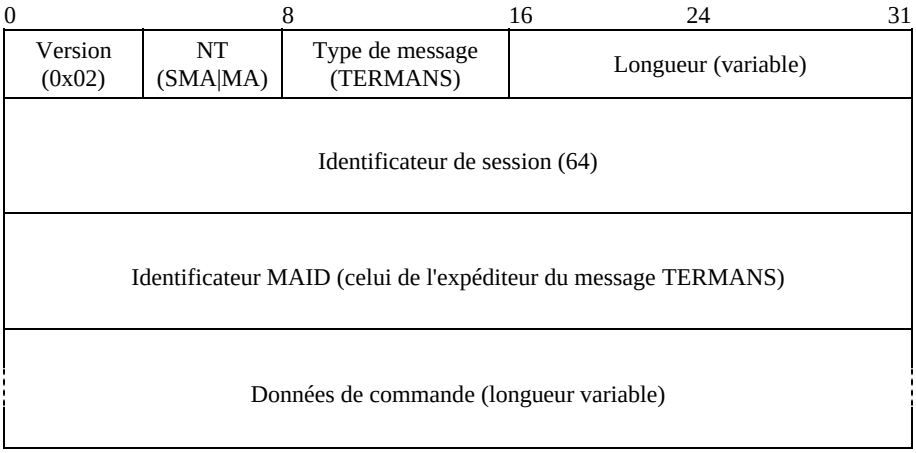

Figure 83 – Message TERMANS

La description de chaque champ est la suivante:

a) *Version* – version actuelle du protocole RMCP (0x02).

b) *NT* – type de nœud de l'émetteur du message. Comme ce message est envoyé en sens inverse de l'arborescence RMCP-2 en réponse au message TERMREQ, le type de nœud pour le message peut être mis à SMA ou MA.

c) *Type de message* – type du message. Il est mis à TERMANS.

d) *Longueur* – longueur totale du message TERMANS, y compris les données de commande (en octets).

e) *Identificateur de session* – valeur de 64 bits de l'identificateur de session RMCP.

f) *Identificateur MAID* – identificateur MAID de l'émetteur du message TERMANS. En principe, l'identificateur MAID du message TERMANS communiqué au récepteur est celui de l'un de ses agents CMA.

g) *Données de commande* – ce champ peut inclure les informations suivantes:

- RESULT

Le message TERMANS est utilisé pour indiquer si le message TERMREQ est bien arrivé. Le code de résultat indiqué sur la Figure 49 devrait donc toujours être OK.

8 Paramètres

Le présent paragraphe explique les valeurs de paramètre utilisées pour la gestion de l'arborescence RMCP-2. Le protocole RMCP-2 définit le profil de retransmission de données comme un moyen de spécifier les informations de canal de données en termes de types de données. En outre, certains des paramètres de commande servent à gérer efficacement et de façon optimale l'arborescence de commande.

8.1 Profil de retransmission de données

Le protocole RMCP-2 définit le profil de retransmission de données comme un profil qui décrit les besoins de retransmission de données entre un agent PMA et son agent CMA direct. Le profil de retransmission de données est utilisé pour négocier le canal de données en termes de types de données fournies pendant la session. Lorsque plusieurs types de données sont transmis simultanément dans une session, les informations relatives à chaque flux de données sont décrites pour la négociation.

La Figure 84 présente un profil de retransmission de données sous forme de texte SDP.

Flux1: protocole = UDP, adresse d'écoute = a.b.c.d:9898, encapsulation = IP-IP

Flux2: protocole = UDP, adresse d'écoute = a.b.c.d:9899, encapsulation = UDP

Flux3: protocole = TCP, adresse d'écoute = a.b.c.d:9899, encapsulation = TCP, n° de séq. actuel = xxxx, n° de séq. mis en mémoire tampon = yyyy, n° de séq. actuellement reçu = xxxx-1

Figure 84 – Exemple de profil de retransmission de données

8.2 Paramètres utilisés dans le protocole RMCP-2

Le protocole RMCP-2 définit certains paramètres pour la gestion de l'arborescence de commande. Ces paramètres commandent les informations temporelles de la session RMCP-2 ou définissent le nombre de messages ou fournissent d'autres informations.

8.2.1 Paramètres pour l'initialisation de session

Chaque agent MA qui souhaite entrer dans une session RMCP-2 devrait contacter le gestionnaire de session pour obtenir les informations d'amorçage pour la session. Le gestionnaire de session donne une liste de voisins comme informations d'amorçage. En raison de la limitation des ressources, la liste de voisins ne peut pas inclure tous les agents MA de la session. Le paramètre qui suit est donc utilisé pour limiter la taille de cette liste:

a) *N_StartNL*: ce paramètre définit le nombre d'agents MA figurant dans la liste de voisins. Il peut être modifié par le gestionnaire de session avant ou après le démarrage de la session. La valeur par défaut de *N_StartNL* est 100.

8.2.2 Paramètres pour la découverte de carte

Dans le protocole RMCP-2, chaque agent MA exécute une procédure de découverte de carte en échangeant régulièrement des messages PPROBREQ et PPROBANS avec les agents MA voisins. Les paramètres qui suivent sont liés à la procédure de découverte de carte:

a) *PPROB.time*: ce paramètre définit la période associée à l'envoi des messages PPROBREQ. Chaque agent MA envoie des messages PPROBREQ tous les *PPROB.time*. La valeur par défaut de *PPROB.time* est de 45 secondes mais elle peut être modifiée arbitrairement.

b) *N_MAX_PROBE*: ce paramètre limite le nombre maximal de messages PPROBREQ qui peuvent être envoyés par chaque agent MA simultanément pour éviter l'explosion des messages PPROBREQ. La valeur par défaut de *N_MAX_PROBE* est 1, mais elle peut être modifiée arbitrairement.

8.2.3 Paramètres pour le maintien de session

Le présent paragraphe porte sur le mécanisme de pulsation et de maintien de la session.

Le protocole RMCP-2 utilise le message HB pour le maintien de l'arborescence. Le message HB permet de synchroniser la totalité de la session le long du trajet de fourniture des données. A l'intérieur de la session synchronisée, chaque agent MA peut changer de parent afin d'améliorer la session RMCP-2. Le message HB permet aussi de détecter les éventuels défauts dans le réseau (par exemple boucles et partitions). Le protocole RMCP-2 définit les paramètres suivants pour la pulsation:

a) *HB.time*: ce paramètre définit la période associée au message HB. L'agent SMA d'une session envoie un message HB tous les *HB.time*. La valeur par défaut de *HB.time* est de 15 secondes.

b) *MAX_PARTITION_CNT*: ce paramètre est utilisé pour examiner si l'arborescence fait l'objet d'une partition. Si un agent MA ne reçoit pas de message HB pendant *MAX_PARTITION_CNT* * *HB.time*, il peut détecter que l'arborescence a fait l'objet d'une partition. La valeur par défaut de *MAX_PARTITION_CNT* est 3.

8.2.4 Paramètres pour le choix de l'agent HMA

Le protocole RMCP-2 permet la transmission de données de multidiffusion IP dans une zone avec multidiffusion activée. Les paramètres qui suivent permettent d'assurer cette fonctionnalité:

a) *H_SOLICIT.time*: ce paramètre définit la période associée au message HSOLICIT. Un agent MA situé dans la zone avec multidiffusion activée envoie un message HSOLICIT tous les *H_SOLICIT.time*. La valeur par défaut de *H_SOLICIT.time* est de 2 secondes.

b) *N_SOLICIT*: ce paramètre donne le nombre maximal de tentatives d'envoi du message HSOLICIT en tant qu'agent non HMA. Après avoir envoyé *N_SOLICIT* fois le message HSOLICIT, l'agent MA essaie de devenir le nouvel agent HMA dans la zone avec multidiffusion activée. La valeur par défaut de *N_SOLICIT* est 3.

c) *H_ANNOUNCE.time*: ce paramètre définit la période associée au message HANNOUNCE. L'agent HMA envoie un message HANNOUNCE tous les *H_ANNOUNCE.time*. La valeur par défaut de *H_ANNOUNCE.time* est de 6 secondes.

d) *N_ANNOUNCE*: ce paramètre définit le nombre maximal de tentatives d'envoi du message HANNOUNCE en tant qu'agent HMA. En l'absence de réception de message HSOLICIT, l'agent HMA cesse de retransmettre les données dans la zone avec multidiffusion activée. La valeur par défaut de *N_ANNOUNCE* est mise à 3.

8.2.5 Paramètres utilisés pendant la fourniture des données

Pour assurer et poursuivre le relais de données, chaque agent CMA envoie régulièrement un message RELREQ à son agent PMA. Les paramètres qui suivent sont utilisés pour prendre en charge la procédure de relais de données:

a) *RELREQ.time*: ce paramètre définit la période associée à l'envoi des messages RELREQ. Les agents PMA et CMA ont la même valeur de paramètre *RELREQ.time*. La valeur initiale de *RELREQ.time* est de 6 secondes.

b) *N_ RELREQ*: ce paramètre est utilisé pour examiner si l'agent CMA est toujours actif ou pas. Si un agent PMA ne reçoit pas de message RELREQ pendant *RELREQ.time* * *N_RELREQ*, il considère que son agent CMA est soudainement sorti de la session. La valeur par défaut de *N_ RELREQ* est 3.

8.2.6 Paramètres pour la sortie de session

Le protocole RMCP-2 autorise un agent MA à sortir prématurément d'une session. Lorsqu'un agent MA situé au milieu d'une arborescence doit sortir d'une session, il devrait patienter un certain temps pour permettre une reconfiguration progressive de l'arborescence. Les paramètres qui suivent sont utilisés pour prendre en charge la procédure de sortie de session:

a) *LEAVE.time*: ce paramètre donne la durée que l'agent PMA sortant laisse à son agent CMA pour trouver un nouvel agent PMA et s'y rallier. La valeur par défaut de *LEAVE.time* est de 10 secondes.

8.3 Règles de codage pour représenter les valeurs utilisées dans le protocole RMCP-2

8.3.1 Règle de codage des messages RMCP-2

Le Tableau 2 énumère les types de messages et les valeurs codées correspondantes pour chaque message.

Tableau 2 – Types de message RMCP-2 et valeurs codées correspondantes

Type de message	Valeur (8 bits)
SUBSREQ	$00000010_{(2)}$
SUBSANS	$00000011_{(2)}$
PPROBREQ	$00000100_{(2)}$
PPROBANS	$00000101_{(2)}$
HSOLICIT	$00000110_{(2)}$
HANNOUNCE	$00000111_{(2)}$
HLEAVE	$00001000_{(2)}$
RELREQ	$00001001_{(2)}$
RELANS	$00001100_{(2)}$
STREQ	$00010010_{(2)}$
STANS	$00010011_{(2)}$
STCOLREQ	$00010100_{(2)}$
STCOLANS	$00010101_{(2)}$
LEAVREQ	$00010110_{(2)}$
LEAVANS	$00010111_{(2)}$
HB	$00011000_{(2)}$
TERMREQ	$00011001_{(2)}$
TERMANS	$00011010_{(2)}$

8.3.2 Valeur de retour RMCP-2

Le Tableau 3 énumère les valeurs codées et la signification des codes de résultat, qui sont normalement utilisés comme codes de retour pour une demande RMCP-2 (par exemple SUBSREQ ou RELREQ).

Tableau 3 – Codes de résultat

Code de résultat	Signification
0x01 00	OK
0x02 00	Problème au niveau du système
0x03 00	Problème administratif

8.3.3 Valeurs liées à la commande ROOTPATH RMCP-2

Le Tableau 4 énumère les codes de commande qui spécifient les divers types de commande ROOTPATH. Le code de commande ROOTPATH peut être défini dans une nouvelle valeur.

Tableau 4 – Code de commande ROOTPATH

Type	Code	Signification
RP_ID	0x01 01	La commande ROOTPATH contient uniquement l'identificateur MAID de chaque saut
RP_ BW	0x01 02	La commande ROOTPATH contient uniquement la largeur de bande de chaque saut
RP_ DL	0x01 04	La commande ROOTPATH contient uniquement le délai perçu pour chaque saut
RP_ID _BW	0x01 03	La commande ROOTPATH contient l'identificateur MAID et la largeur de bande de chaque saut
RP_ID _DL	0x01 05	La commande ROOTPATH contient l'identificateur MAID et le délai pour chaque saut
RP_ID _BW_DL	0x01 07	La commande ROOTPATH contient l'identificateur MAID, la largeur de bande et le délai pour chaque saut
RP_PSEUDO	0x01 00	La commande ROOTPATH est une pseudo-commande ROOTPATH pour le retour à la normale en cas de défaut

Le Tableau 5 donne la taille pour chaque élément de commande ROOTPATH.

Tableau 5 – Taille pour chaque type de commande ROOTPATH

Type	Longueur (en octets)
RP_ID	16
RP_ BW	4
RP_ DL	4

8.3.4 Valeurs liées à la collecte de l'état RMCP-2

Le Tableau 6 énumère les valeurs des codes de commande d'un message STREQ ou STCOLREQ. Chaque code a une longueur de 2 octets. Il spécifie le type d'interrogation pour garantir que l'entité qui reçoit la demande puisse répondre correctement. Ces codes de commande peuvent être combinés pour élaborer de nouveaux codes.

Tableau 6 – Codes de commande pour l'interrogation d'état

Type	Code	Signification
SI_UPTIME	0x02 01	Durée de fonctionnement de l'agent MA
SI_DELAY	0x04 01	Etat du délai perçu par l'agent MA depuis la racine ROOT
SI_RCV_PACKET	0x08 01	Nombre de paquets reçus par l'agent MA depuis le démarrage
SI_RCV_BYTES	0x08 02	Nombre d'octets reçus par l'agent MA depuis le démarrage
SI_RCV_BW	0x08 04	Largeur de bande perçue par l'agent MA entre lui-même et son agent PMA
SI_SND_PACKET	0x0F 01	Nombre total de paquets envoyés par l'agent MA depuis le démarrage
SI_SND _BYTES	0x11 02	Nombre total d'octets envoyés par l'agent MA depuis le démarrage
SI_SND _BW	0x11 04	Largeur de bande totale consommée par l'agent PMA pour desservir ses agents CMA
TI_DEPTH	0x12 01	Profondeur de l'agent MA dans l'arborescence RMCP-2
TI_MA_LIST	0x14 01	Liste des agents MA de l'arborescence RMCP-2 limitée par l'option TreeExplor
TI_AV_DELAY	0x14 02	Délai moyen limité par l'option TreeExplor
TI_AV_BW	0x14 04	Largeur de bande moyenne limitée par l'option TreeExplor

Les huit bits de plus fort poids du code spécifient la catégorie de la commande; les huit bits de plus faible poids spécifient les éléments détaillés (par exemple largeur de bande, paquets et octets).

8.3.5 Valeurs liées à la sortie

Le Tableau 7 énumère les codes de motif de sortie. Les huit bits de plus fort poids du code spécifient le motif principal de sortie et les huit bits de plus faible poids donnent les motifs détaillés de sortie (par exemple épuisement des ressources du système, fin de session à la demande de l'utilisateur).

Tableau 7 – Codes de motif de sortie

Catégorie	Code de motif	Signification
Sortie	0x01 00	Sortie du propre gré de l'agent MA
	0x02 00	Sortie d'agent SMA
Expulsion	0x03 00	Expulsion par le gestionnaire de session
	0x03 01	Expulsion par l'agent PMA
Changement de parent	0x04 00	Changement de parent de l'agent MA

8.3.6 Valeurs liées à la fin de session

Le Tableau 8 énumère les codes de motif de fin de session. Les huit bits de plus fort poids du code spécifient le motif principal de la fin de session et les huit bits de plus faible poids donnent les motifs détaillés.

Tableau 8 – Codes de motif de fin de session

Catégorie	Code de motif	Signification
Fin de session normale	0xF1 00	Il est mis fin normalement à la session
Fin de session anormale	0xF2 00	Il est mis fin anormalement à la session sans motif
	0xF2 01	Il est mis fin anormalement à la session à la demande de l'utilisateur

Annexe A

Algorithme de configuration de l'arborescence

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale)

A.1 Règle d'amorçage

Un agent MA qui entre pour la première fois dans une session RMCP-2 devrait obtenir les informations d'amorçage auprès du gestionnaire de session pour se raccorder à l'arborescence existante. Comme aucun agent MA n'a d'informations sur l'arborescence, chaque agent MA doit collecter des informations sur l'arborescence existante. Pour que l'arborescence RMCP-2 soit élaborée de façon indépendante, le gestionnaire de session donne les informations d'amorçage aux agents MA nouvellement entrés. Les informations d'amorçage gérées par le gestionnaire de session devraient donc être aussi fiables et optimisées que possible. Elles sont essentiellement constituées d'une série de listes d'agents MA gérées par le gestionnaire de session. Comme la quantité d'informations d'amorçage est limitée, ces informations ne peuvent pas contenir la liste de tous les membres. En revanche, elles devraient inclure uniquement les informations optimales pour décrire la session.

Les informations d'amorçage optimales pour chaque agent MA figurent dans la liste des agents MA offrant la plus grande capacité de retransmission, les délais les plus courts et la plus grande possibilité de raccordement réussi. Toutefois, le gestionnaire de session ne peut pas indiquer la distance réseau exacte entre les agents MA, le gestionnaire de session donne seulement des informations sur les capacités des agents MA à préconfigurer l'espace et la vitesse du réseau en aval. Dans une session RMCP-2, l'ordre de préférence des agents MA est le suivant:

1) agent MA spécialisé;
2) agent MA présentant la profondeur d'arborescence la plus faible;
3) agent MA présentant la plus grande largeur de bande.

En outre, chaque agent MA devrait savoir combien de nœuds aval sont autorisés.

1) place disponible pour un nouvel agent CMA.

Cela étant, les informations d'amorçage, qui contiennent la liste des agents MA parents possibles, devraient être gérées par le gestionnaire de session comme suit:

si c'est un agent MA spécialisé
    donner la priorité la plus élevée
sinon
    priorité = nombre d'agents CMA disponibles * pw_cma +
        largeur de bande possible pour la retransmission * pw_bandwidth +
        niveau différentiel de saut * pw_hop
pw_cma = facteur de pondération fondé sur la politique pour l'agent CMA (%/cma)
pw_bandwidth = facteur de pondération fondé sur la politique pour la largeur de bande (%/bit/s)
pw_hop = facteur de pondération fondé sur la politique pour le saut (%/niveau)

Si tous les agents MA spécialisés d'une session ont suffisamment de place pour des agents MA en aval ou si l'administrateur de réseau souhaite conserver chaque agent MA feuille d'un agent MA donné, le gestionnaire de session envoie uniquement les informations relatives aux agents DMA. En outre, le gestionnaire de session devrait garantir que tous les agents MA indiqués dans ces informations sont actifs.

Pour garantir que la liste des agents MA est à jour, le gestionnaire de session vérifie régulièrement l'état des agents MA et utilise la règle qui suit pour tenir à jour les informations d'état.

si la temporisation MA_LIST_PROB expire

sonder et mettre à jour l'état des agents MA figurant dans la liste MA_LIST

si un agent MA s'abonne avec succès

sonder et mettre à jour l'état de l'agent MA qui s'est abonné avec succès

Si la taille d'une session RMCP-2 est relativement petite ou qu'un gestionnaire de session souhaite contrôler étroitement une session, le gestionnaire de session donne la liste complète des agents MA à chaque nouvel agent MA.

si la session RMCP-2 est contrôlée étroitement par un gestionnaire de session

sinon si le nombre d'agents MA dans la liste MA_LIST est inférieur à la capacité maximale d'un seul message SUBSANS

envoyer la liste de tous les agents MA figurant dans la base de données du gestionnaire de session

A.2 Règle de découverte des voisins

Comme les informations d'amorçage provenant du gestionnaire de session ne représentent qu'une partie de la session RMCP-2 tout entière, elles sont insuffisantes pour que chaque agent MA trouve son meilleur agent PMA. En outre, l'agent MA ne peut pas reconnaître ses plus proches voisins. Chaque agent MA devrait donc explorer ses voisins en procédant à un échange de listes de voisins, qu'il se soit déjà raccordé à la session ou non. Ce mécanisme permet aussi à l'agent MA de mesurer la distance dans le réseau et de déterminer l'état de chaque agent MA.

La liste de voisins utilisée pour la découverte des voisins est élaborée comme suit:

inclure l'agent DMA dans la liste MA_LIST_FOR_ND

si le fonctionnement de la session est fondé sur un agent DMA

interruption;

sinon

inclure son trajet depuis la racine dans MA_LIST_FOR_ND

inclure la liste des agents CMA qui lui sont directement rattachés dans MA_LIST_FOR_ND

inclure la liste des agents MA sondés ou non sondés

jusqu'à ce que la taille du message PPROB soit satisfaisante

la liste MA_LIST_FOR_ND est complète

La situation du réseau pour les deux agents MA qui participent à la découverte des voisins peut être calculée comme suit:

délai = RTT/2

largeur de bande = taille de paquet reçue/(RTT/2)

A.3 Règle de sélection de l'agent HMA

Lorsqu'il y a deux agents MA ou plus dans une même zone avec multidiffusion activée, un conflit peut se produire concernant l'agent HMA. En cas de conflit, chaque agent MA essaie d'envoyer un message HANNOUNCE pour devenir le nouvel agent HMA de sorte que chaque agent MA situé dans la zone avec multidiffusion activée peut obtenir plusieurs messages HANNOUNCE provenant de différents agents MA. On utilise la règle suivante pour détecter tout conflit concernant l'agent HMA.

si plusieurs messages HANNOUNCE contenant une commande Auth valable et le même identificateur SID arrivent en provenance de différents identificateurs MAID

en déduire qu'il y a un conflit entre messages HANNOUNCE

La règle qui suit permet de résoudre tout conflit concernant l'agent HMA:

si les heures d'entrée dans la session sont différentes

choisir l'agent qui est entré en premier dans la session en tant qu'agent HMA

sinon

choisir l'agent qui a le plus petit identificateur MAID en tant qu'agent HMA

A.4 Règle d'acceptation d'agent CMA

Dès qu'il reçoit un nouveau message RELREQ provenant d'un agent MA, un agent PMA devrait décider s'il accepte la demande de relais. La règle de décision est la suivante:

une nouvelle demande RELAY est arrivée

s'il y a suffisamment de place pour un nouvel agent CMA
si la qualité de service et la politique conviennent et que le profil et la condition concernant les données conviennent

accepter la demande de relais de l'agent MA

sinon

refuser la demande de relais de l'agent MA

A.5 Règle de décision concernant le parent

Chaque agent MA, y compris les nouveaux agents MA, devrait choisir, parmi les agents MA sondés, celui pour lequel le coût est minimal. L'agent MA choisi devient alors un agent PMA possible. Chaque fois qu'un agent MA entre pour la première fois dans une session RMCP-2, il considère l'agent PMA possible comme son agent PMA, sinon l'agent PMA possible est réservé pour le changement de parent. La règle permettant de calculer le coût et de choisir le meilleur agent PMA est exprimée comme suit:

si un agent MA est présent dans la même zone avec multidiffusion activée

si l'agent MA est situé dans le même réseau local

choisir l'agent MA comme son agent PMA possible

sinon

trouver l'agent MA pour lequel le coût est minimal

coût = niveau différentiel de délai * wt_delay +

niveau différentiel de largeur de bande * w_bandwidth +

niveau différentiel de saut * w_hop

si le coût est le même pour deux agents PMA possibles ou plus

choisir le nœud pour lequel la différence entre les deux identificateurs MAID est minimale

*) somme(wt_delay, w_bandwidth, w_hop) = 1

w_delay = facteur de pondération pour le délai

w_bandwidth = facteur de pondération pour la largeur de bande

w_hop = facteur de pondération pour la profondeur dans l'arborescence

Le calcul du coût en vue du choix de l'agent PMA peut être effectué comme suit: le protocole RMCP-2 utilise un facteur de pondération pour configurer l'arborescence de fourniture des données optimale. Ce facteur de pondération devrait être donné par un administrateur de réseau ou par le créateur de la session. On suppose que l'agent MA C a obtenu les informations suivantes concernant les agents MA A et B:

	Agent MA A	**Agent MA B**
Délai	10 ms	11 ms
Largeur de bande	100 Mbit/s	90 Mbit/s
Profondeur dans l'arborescence	Niveau 5	Niveau 7

Disposant de ces informations, l'agent MA C peut déterminer quel agent MA est le plus proche de lui. Les exemples suivants montrent comment l'agent MA C calcule le coût compte tenu du facteur de pondération:

	Cas 1	**Cas 2**	**Cas 3**
Comparaison des agents MA A et B	coût = (10-11)/E(10,11)*0,5 + (100–90)/E(100,90)*0,4 + (5-7)/E(5,7) * 0,1 = **–0,039**	coût = (10-11)/E(10,11)* 0,4 + (100–90)/E(100,90)*0,4 + (5-7)/E(5,7) * 0,2 = **–0,063**	coût = (10-11)/E(10,11)*0,4 + (100–90)/E(100,90)*0,6 + (5-7)/E(5,7) * 0,0 = **0,025**
Décision	Choisir l'agent MA A	Choisir l'agent MA A	Choisir l'agent MA B
Cas 1 facteur de pondération (w_delay/w_bandwidth/w_hop) = (0,5/0,4/0,1)			
Cas 2 facteur de pondération (w_delay/w_bandwidth/w_hop) = (0,4/0,4/0,2)			
Cas 3 facteur de pondération (w_delay/w_bandwidth/w_hop) = (0,4/0,6/0,0)			

Lorsque le coût est le même pour deux agents PMA possibles, l'agent MA utilise la règle qui suit pour choisir l'un des deux:

si le coût est le même pour deux agents PMA possibles ou plus

choisir le nœud pour lequel la différence entre les deux identificateurs MAID est minimale

A.6 Règle d'amélioration de l'arborescence

Comme chaque agent MA ne peut pas connaître exactement la totalité de la topologie du réseau, il se peut que la décision relative au parent de l'agent MA ne soit pas optimale. Chaque agent MA devrait donc améliorer progressivement la session RMCP-2 au moyen du mécanisme de changement de parent. La règle suivante permet de calculer quand le changement de parent est déclenché:

Si | (QS perçue – nouvelle QS)/QS perçue | > stabilité (politique)

déclencher le changement de parent

*) le facteur de stabilité est donné par l'administrateur au moment où la session est créée

Stabilité = 0 ~ 100% (plus le facteur de stabilité est grand, moins le changement de parent est fréquent)

A.7 Règle d'expulsion par l'agent PMA

L'agent PMA peut expulser l'un de ses agents CMA chaque fois que le nombre d'agents CMA autorisés par un agent MA diminue ou chaque fois qu'un agent CMA de l'agent PMA cause des perturbations. L'agent PMA utilise la règle suivante pour prendre une décision d'expulsion:

si (nombre maximal d'agents CMA < nombre actuel d'agents CMA)

choisir l'agent CMA le pire et lui envoyer un message LEAVREQ

sinon si (qualité de service de relais dégradée par un agent CMA)

envoyer un message LEAVREQ à l'agent CMA

Annexe B

Mécanisme de fourniture de données en temps réel

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale)

B.1 Aperçu

Chaque fois qu'un agent MA doit transférer des données en temps réel à plusieurs utilisateurs, il adopte un mécanisme de tunnellisation IP-IP pour obtenir un débit élevé. La présente annexe décrit comment la méthode de tunnellisation IP est utilisée pour la fourniture de données en temps réel. La Figure B.1 présente l'architecture générale de la tunnellisation IP.

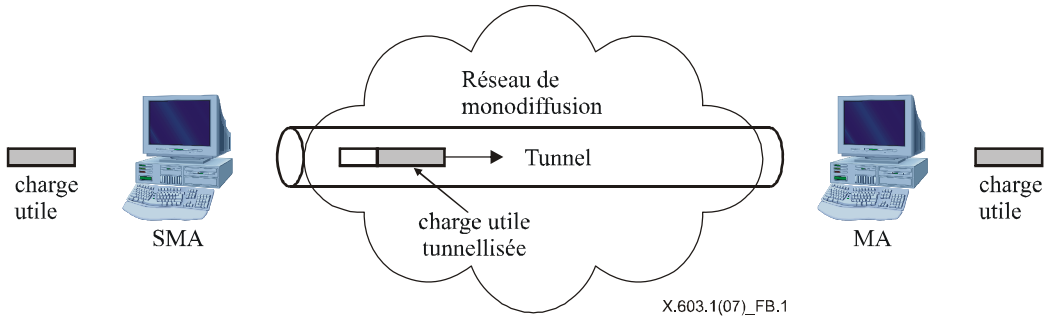

Figure B.1 – Mécanisme de tunnellisation IP

B.2 Mécanisme de tunnellisation IP-IP pour la fourniture de données en temps réel RMCP-2

Après l'échange d'un ensemble de messages de commande RMCP-2, un trajet de fourniture de données en mode multidiffusion est établi sur le trajet de commande. L'agent MA établit le trajet de fourniture de données vers ses agents MA subordonnés. Le module de commande contient un module de données avec l'adresse IP des agents MA subordonnés et un mécanisme d'encapsulation, les informations correspondantes étant contenues dans le profil de données du message SUBSREQ afin d'établir la table de fourniture de données. Le module de données de chaque agent MA stocke l'adresse des agents MA subordonnés dans la table de fourniture. Dans cette méthode, un canal de fourniture de données en temps réel est établi entre les agents PMA et CMA, pour pouvoir fournir les données en temps réel de l'agent SMA à chacun des agents MA feuilles. Après l'établissement du canal de fourniture de données, l'application de groupe fonctionne comme si elle appartenait au réseau de multidiffusion IP, comme représenté sur la Figure B.2.

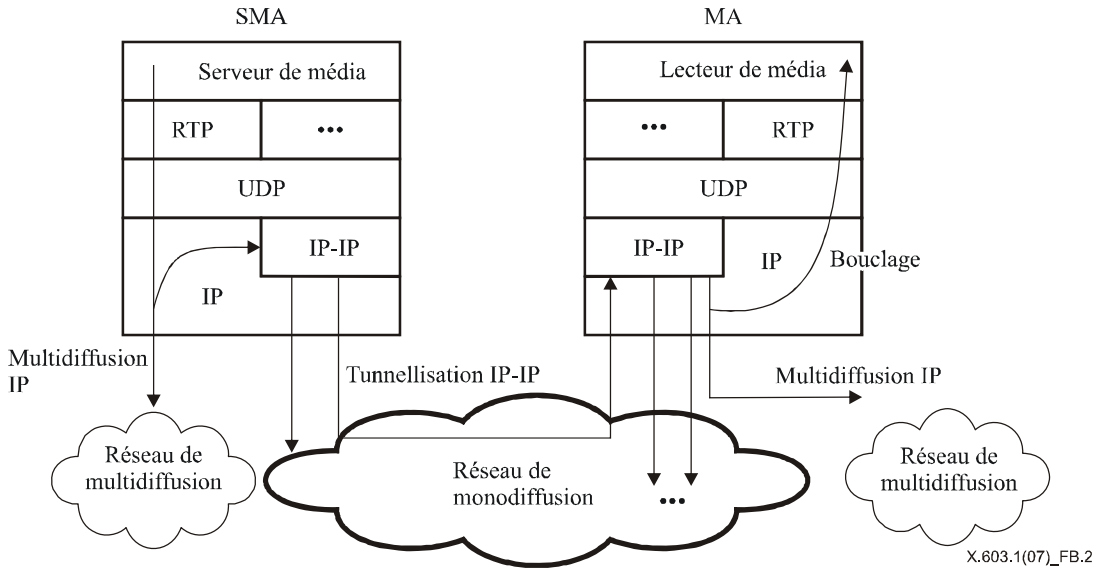

Figure B.2 – Canal de fourniture de données en temps réel avec encapsulation IP-IP

L'agent SMA encapsule les paquets de données de multidiffusion IP dans des paquets de données de monodiffusion et transmet les données encapsulées aux agents MA en aval en procédant à une monodiffusion de ces données sur le réseau de monodiffusion. Il procède aussi à une multidiffusion des paquets de données de multidiffusion IP vers une zone avec multidiffusion activée. Dès qu'il reçoit des paquets de données tunnellisées, chaque agent CMA les décapsule pour obtenir les paquets de données de multidiffusion IP.

Lorsque les agents CMA sont situés dans la même région de multidiffusion, l'agent PMA retransmet simplement les données de multidiffusion dans cette région. Si un ou plusieurs agents CMA sont situés dans la région de monodiffusion, l'agent PMA devrait encapsuler les paquets de données de multidiffusion IP puis transmettre les données tunnellisées à ses agents CMA.

Annexe C

Mécanisme de fourniture de données fiables

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale)

C.1 Aperçu

Le mécanisme décrit ici est un mécanisme superposé de multidiffusion pour la fourniture de données fiables. Les nœuds de la relation parent-enfant échangent des profils de données pour trouver un ensemble de données disponibles. Pour cela, chaque nœud ouvre la connexion TCP pour la fourniture de données fiables. Une fois que le canal de fourniture de données est établi, chaque nœud reçoit des données en provenance de son parent puis retransmet les données reçues à son nœud aval s'il y en a un. De cette manière, les données provenant de la racine peuvent parvenir aux nœuds feuilles via plusieurs nœuds intermédiaires.

Au moyen de profils de données, chaque nœud peut rechercher un nœud disposant des données nécessaires et, si besoin est, tout nœud qui utilise ce mécanisme peut changer de nœud amont. Le paragraphe qui suit décrit les procédures utilisées dans le cadre du mécanisme superposé de multidiffusion pour la fourniture de données fiables simplex.

C.2 Fonctionnement

C.2.1 Connexion de canal

La Figure C.1 présente la procédure de connexion de canal, qui comporte les quatre étapes suivantes:

1) L'agent CMA envoie à l'agent PMA un profil de données qui contient l'adresse locale du nouvel entrant et le numéro de séquence à recevoir. Lorsque le nouvel entrant ne dispose d'aucune information sur la fourniture des données, le numéro de séquence à recevoir sera mis à NEWEST.
2) Après avoir reçu le profil de données provenant de l'agent CMA, l'agent PMA répond par un profil de données qui contient l'adresse d'écoute et le numéro de séquence actuel.
3) Les deux agents MA, qui échangent des informations de canal, établissent une connexion TCP entre eux puis attribuent un identificateur de canal à la connexion établie.
4) L'agent PMA envoie des données d'utilisateur encapsulées avec l'identificateur de canal, attribué par lui-même ainsi que le numéro de séquence.

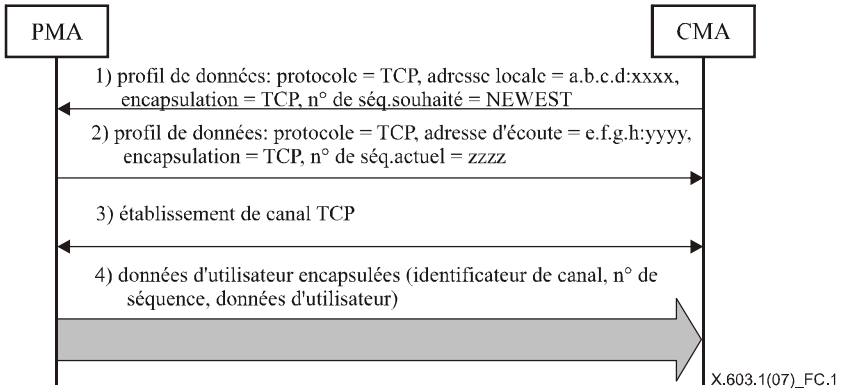

Figure C.1 – Procédure de connexion de canal

C.2.2 Déconnexion de canal

Comme indiqué sur la Figure C.2, la procédure de déconnexion de canal comporte les trois étapes suivantes:

1) Une connexion TCP est établie entre les deux agents MA.
2) L'agent PMA envoie des données d'utilisateur encapsulées avec l'identificateur de canal, qui est attribué par lui-même, ainsi que le numéro de séquence.
3) L'un ou l'autre agent MA peut éliminer le canal TCP en en demandant la fermeture.

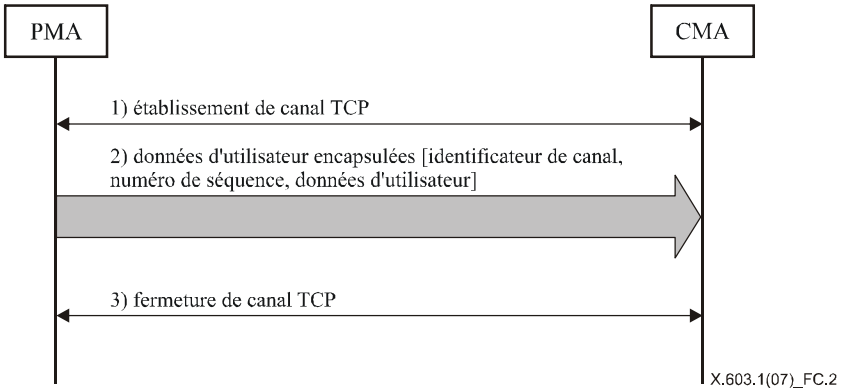

Figure C.2 – Procédure de déconnexion de canal

C.2.3 Changement de canal

Comme indiqué sur la Figure C.3, la procédure de changement de canal comporte les sept étapes suivantes:

1) Une connexion TCP est établie entre les deux agents MA.
2) L'agent PMA envoie des données encapsulées avec l'identificateur de canal, attribué par lui-même ainsi que le numéro de séquence et des données d'utilisateur.
3) L'agent CMA envoie un profil de données, qui contient son adresse locale et le numéro de séquence à recevoir, au nouvel agent PMA.
4) Dès qu'il reçoit le profil de données provenant de l'agent CMA, le nouvel agent PMA répond par un profil de données qui contient l'adresse d'écoute, le numéro de séquence actuel et le numéro de séquence mis en mémoire tampon.
5) Si le numéro de séquence souhaité est compris entre le numéro de séquence mis en mémoire tampon et le numéro de séquence actuel, l'agent CMA déconnecte le canal TCP avec l'ancien agent PMA.
6) Le nouvel agent PMA et l'agent CMA, qui sont reliés par une connexion TCP, attribuent à cette connexion un nouvel identificateur de canal.
7) Le nouvel agent PMA envoie des données d'utilisateur encapsulées avec l'identificateur de canal attribué par lui-même et un numéro de séquence à partir du numéro de séquence souhaité.

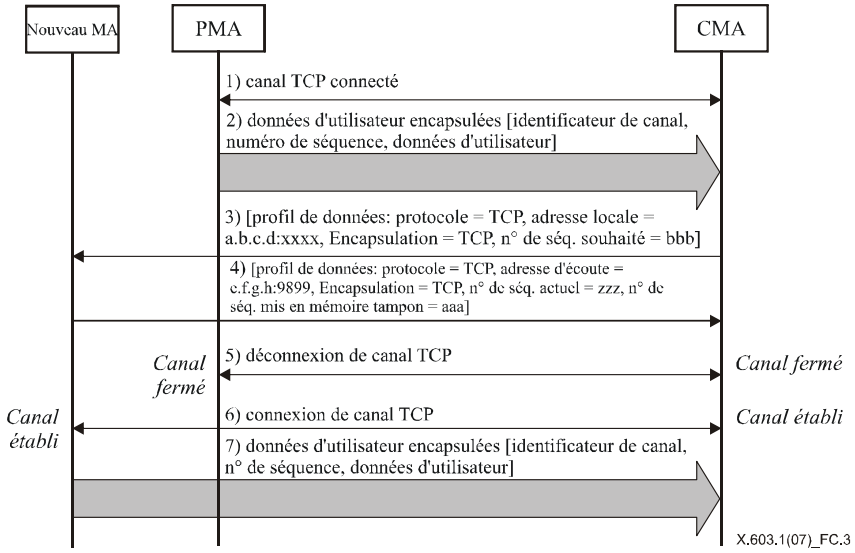

Figure C.3 – Procédure de changement de canal

C.3 Format d'encapsulation des données

La Figure C.4 présente le message de données d'utilisateur pour la fourniture de données fiables:

a) Réservé: réservé pour une utilisation future et mis à zéro pour le moment.

b) Longueur: longueur totale en octets du message considéré.

c) Identificateur de canal: identificateur du canal de données entre les sauts de données.

d) Numéro de séquence: numéro de séquence attribué par un agent SMA pour l'unité de données de service considérée; cette valeur peut être attribuée globalement de façon circulaire.

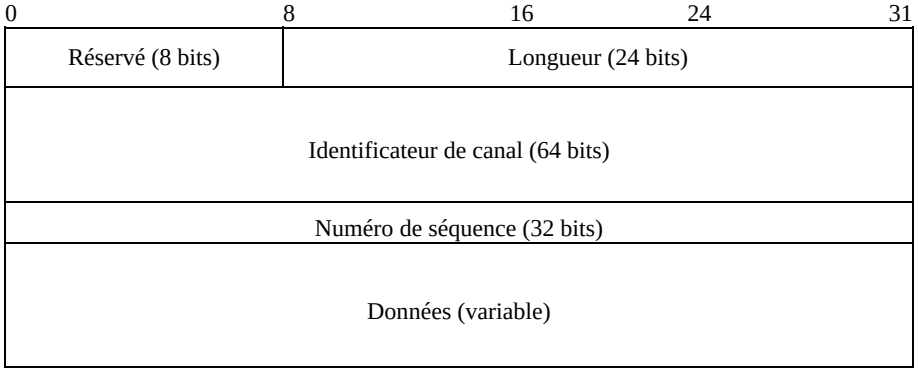

Figure C.4 – Format d'encapsulation des données

C.4 Profil de données

Lorsque le mécanisme de tunnellisation des données est utilisé dans le protocole RMCP-2, il convient d'utiliser le format suivant pour le profil de données:

"Protocole = TCP, adresse d'écoute = a.b.c.d:9899, encapsulation = TCP, n° de séq. actuel = xxxx, n° de séq. mis en mémoire tampon = yyyy, n° de séq. souhaité = zzz"

Annexe D

Interfaces API RMCP-2

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale)

La présente annexe spécifie les interfaces de programmation d'application (API) pour le protocole RMCP-2. Les interfaces API décrites dans la présente annexe peuvent être utilisées dans des applications qui utilisent les capacités du protocole RMCP-2.

Les interfaces API RMCP-2 sont inspirées des interfaces API des connecteurs de Berkeley. Toutefois, pour différencier les interfaces API RMCP-2 des fonctions existantes des connecteurs de Berkeley, on ajoute le préfixe 'rmcp2_' (par exemple, rmcp2_socket) pour les interfaces API RMCP-2.

D.1 Aperçu

D.1.1 Interfaces API

Le Tableau D.1 récapitule les fonctions API dans le protocole RMCP-2:

Tableau D.1 – Récapitulation des interfaces API RMCP-2

Catégorie	Nom	Description
Commande d'agent MA	*rmcp2_socket()*	Crée un nouveau connecteur RMCP-2.
	rmcp2_bind()	Associe un ensemble d'informations concernant la session, par exemple identificateur de session, rôle, adresse locale et adresse de groupe, profil de données, etc.
	rmcp2_connect()	Entre dans une session RMCP-2.
	rmcp2_close()	Met fin à la connexion et libère le connecteur.
	rmcp2_setsockopt()	Fixe les options de connecteur et de protocole dans le module de commande d'agent MA RMCP-2.
	rmcp2_getsockopt()	Obtient les options de connecteur et de protocole auprès du module de commande d'agent MA RMCP-2.
	rmcp2_recv()	Fournit les données reçues à l'application.
	rmcp2_send()	Envoie les données de l'application à un groupe RMCP-2.
Fourniture de données	*rmcp2_recv()*	Fournit les données reçues à l'application.
	rmcp2_send()	Envoie les données de l'application à un groupe RMCP-2.
Gestion de session	*rmcp2_session_open()*	Crée une nouvelle session RMCP-2.
	rmcp2_session_close()	Met fin à la session RMCP-2 et libère les ressources attribuées.
	rmcp2_member_out()	Expulse le fauteur de trouble de la session.
	rmcp2_status_report()	Examine la situation d'une session RMCP-2 particulière.
	rmcp2_char_change()	Fixe ou modifie les caractéristiques de session RMCP-2.

D.1.2 Utilisation des interfaces API RMCP-2

La Figure D.1 illustre l'utilisation des interfaces API RMCP-2 et présente des séquences API sur la base d'un gestionnaire de session et de deux agents MA.

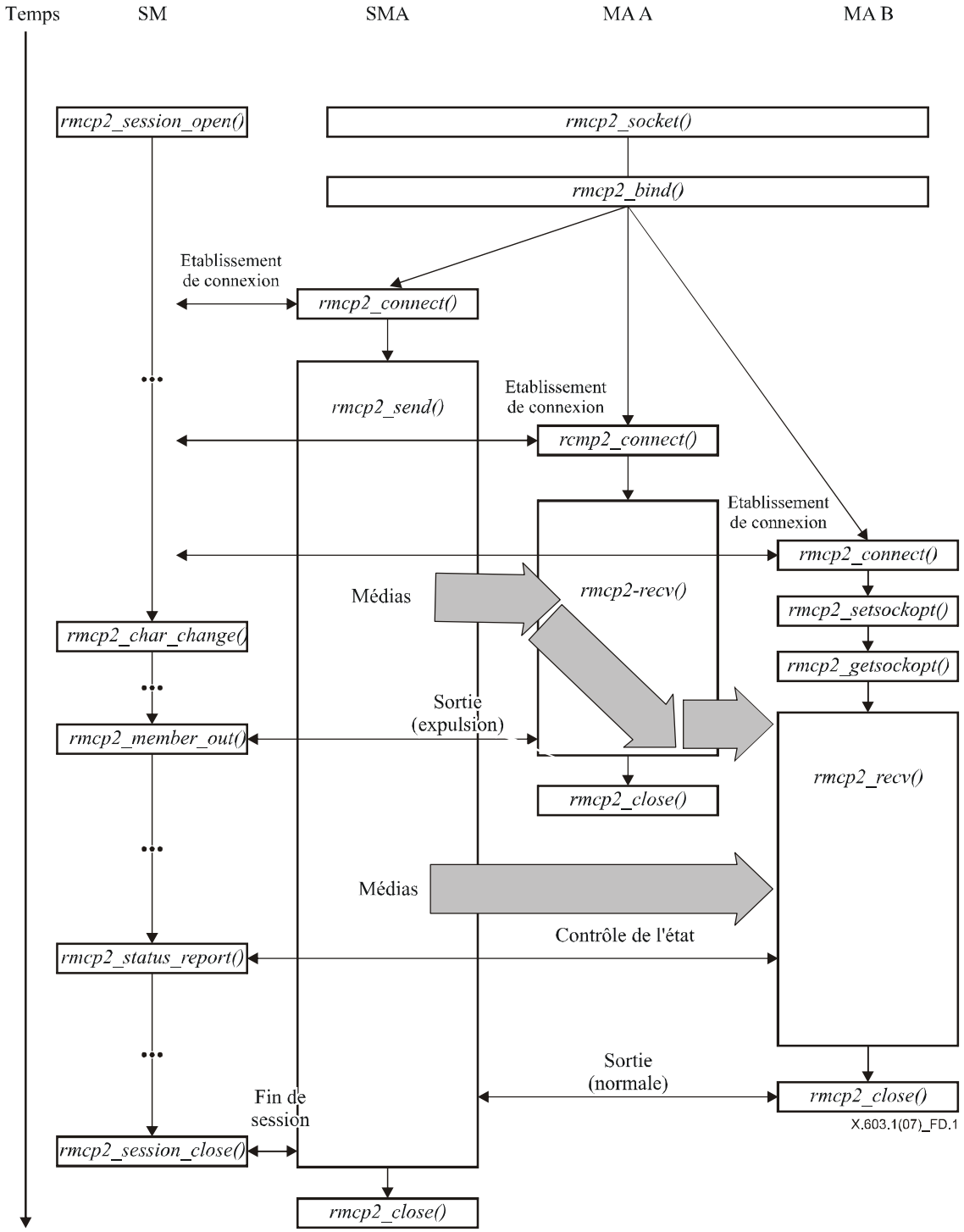

Figure D.1 – Utilisation des interfaces API RMCP-2

D.2 Fonctions API RMCP-2

D.2.1 Fonctions liées à la commande d'agent MA

Le présent paragraphe définit un ensemble d'interfaces API RMCP-2 qui sont liées à l'agent MA. Les applications RMCP-2 utilisent les fonctions définies ici pour l'entrée dans les sessions RMCP-2 et la sortie de ces sessions. Les fonctions à utiliser pour l'envoi et la réception de données sont définies dans le paragraphe d'après.

int rmcp2_socket (void)

Dans le cadre du protocole RMCP-2, une application demande à un agent MA RMCP-2 de démarrer une session RMCP-2 en appelant la fonction *rmcp2_socket()*. Si la demande aboutit, cette fonction retourne un identificateur de connecteur RMCP-2 non nul; dans le cas contraire, elle retourne une valeur négative avec des codes d'erreur.

*int rmcp2_bind(int sd, session_profile *profile, int profile_len)*

Chaque fois qu'une application RMCP-2 souhaite imposer certaines informations concernant une session, elle peut appeler la fonction *rmcp2_bind()*. Celle-ci fixe les informations qui sont indispensables pour l'entrée d'un agent MA dans une session RMCP-2. Les informations les plus importantes concernant une session sont notamment les suivantes:

a) identificateur de session;

b) rôle de l'agent MA dans la session RMCP-2 (par exemple agent MA côté émetteur, agent MA feuille);

c) adresse spécifique de l'agent MA à utiliser;

d) adresse de groupe;

e) profil de données dont l'utilisation est souhaitée;

f) autres informations propres au fournisseur, etc.

Après un rattachement réussi, cette fonction retourne zéro; dans le cas contraire, elle retourne une valeur négative avec le code d'erreur approprié.

*int rmcp2_connect(int sd, struct sockaddr *sm_addr, int addrlen)*

C'est uniquement après un rattachement réussi qu'une application RMCP-2 peut commencer l'entrée dans une session RMCP-2. En appelant la fonction *rmcp2_connect()*, chaque application RMCP-2 peut invoquer l'agent MA pour s'abonner à une session RMCP-2 et entrer dans cette session. Les arguments associés à cette fonction sont l'adresse du gestionnaire de session et l'identificateur de session pour pouvoir entrer dans une session RMCP-2. Après une entrée réussie dans la session, cette fonction retourne zéro; dans le cas contraire, elle retourne une valeur négative avec un code d'erreur.

int rmcp2_close(int sd)

Pour sortir d'une session, une application RMCP-2 appelle la fonction *rmcp2_close()*. En appelant cette fonction, une application peut provoquer le lancement d'une procédure de départ par un agent MA RMCP-2, le bloc de commande de protocole étant ensuite libéré. Après une sortie réussie de la session, cette fonction retourne zéro; dans le cas contraire, elle retourne un entier négatif avec le code d'erreur approprié.

*int rmcp2_setsockopt(int sd, int opt_type, char *opt, int optlen)*

La fonction *rmcp2_setsockopt()* permet à une application de fixer ou de modifier un ou plusieurs paramètres de protocole. Si l'opération réussit, cette fonction retourne zéro; dans le cas contraire, elle retourne un entier négatif avec le code d'erreur approprié.

*int rmcp2_getsockopt(int sd, int opt_type, char *opt, int *optlen)*

Une application qui souhaite obtenir des informations sur un ou plusieurs paramètres de protocole auprès de l'agent MA appelle la fonction *rmcp2_getsockopt()* en offrant un argument *opt_type* et un argument **opt* vide suffisamment grand pour pouvoir inclure les informations résultantes données par l'agent MA. Si l'opération réussit, cette fonction retourne zéro; dans le cas contraire, elle retourne un entier négatif avec le code d'erreur approprié.

D.2.2 Fonctions liées à la fourniture de données

Le présent paragraphe définit un ensemble d'interfaces API RMCP-2 qui sont liées à la fourniture de données RMCP-2. Ces interfaces API sont utilisées par les applications pour l'envoi ou la réception de données RMCP-2.

*int rmcp2_recv(int sd, char *buf, int len, int flags)*

Une application réceptrice qui souhaite recevoir des données en provenance d'une session RMCP-2 appelle la fonction *rmcp2_recv()* et copie les données de l'argument *len* reçues en provenance du module de données de l'agent MA. Si l'opération réussit, cette fonction retourne zéro; dans le cas contraire, elle retourne une valeur négative avec un code d'erreur.

*int rmcp2_send(int sd, char *buf, int len, int flags)*

Pour envoyer des données à une session RMCP-2, une application RMCP-2 appelle la fonction *rmcp2_send()*. Toutefois, comme le protocole RMCP-2 ne prend en charge qu'un service de fourniture de données point à multipoint, l'agent MA de l'application émettrice doit être un agent SMA. Cette fonction copie les données de l'argument *len* dans le

module de données de l'agent MA. Si l'opération réussit, cette fonction retourne le nombre d'octets qu'elle envoie; dans le cas contraire, elle retourne une valeur négative avec un code d'erreur.

D.2.3 Fonctions liées à la gestion de session

Une application du gestionnaire de session peut lancer, gérer ou mettre fin à une session RMCP-2 en appelant l'une des interfaces API définies dans le présent paragraphe. Pour lever toute ambiguïté entre *une application qui utilise le gestionnaire de session RMCP-2* et *le gestionnaire de session RMCP-2* proprement dit, on emploie l'expression *application du gestionnaire de session* pour désigner l'application qui utilise le gestionnaire de session RMCP-2.

*SID rmcp2_session_open(session_profile *session_profile)*

Une application du gestionnaire de session qui souhaite que le gestionnaire de session démarre une session RMCP-2 appelle la fonction *session_open()* avec le profil de session. L'argument *session_profile* devrait contenir des informations suffisantes pour pouvoir créer et gérer une session RMCP-2. Dès qu'il reçoit le profil de session, le gestionnaire de session attribue suffisamment de place pour une session RMCP-2 spécifique. Si une session est créée avec succès, cette fonction retourne l'identificateur de la session créée; dans le cas contraire, elle retourne zéro avec un code d'erreur approprié.

int rmcp2_session_close(SID session_id)

Une application du gestionnaire de session qui souhaite que le gestionnaire de session mette fin à une session RMCP-2 appelle l'interface API *session_close()*. Cette fonction demande au gestionnaire de session de démarrer la procédure permettant de mettre fin à une session RMCP-2, une place suffisante étant ensuite libérée. S'il est mis fin à la session avec succès, cette fonction retourne une valeur non négative; dans le cas contraire, elle retourne une valeur négative avec un code d'erreur.

int rmcp2_member_out(SID session_id, MAID maid)

Chaque fois qu'un membre d'une session, ou un agent MA, cause de graves problèmes ou transgresse la politique de la session, l'application du gestionnaire de session peut expulser le fauteur de trouble de la session. Si une application du gestionnaire de session souhaite qu'un gestionnaire de session expulse un membre particulier de la session, elle appelle l'interface API *member_out()* avec un identificateur de session, ainsi que l'identificateur du membre à expulser.

*int rmcp2_status_report(SID session_id, int command, char *result, int *result_len)*

La fonction *status_report()* permet à une application du gestionnaire de session d'examiner la situation d'une session. Elle est généralement appelée avec des arguments comme l'identificateur de session, les commandes de fonctionnement et une mémoire tampon pour les résultats. Si l'opération réussit, cette fonction retourne zéro; dans le cas contraire, elle retourne une valeur négative et un code d'erreur.

*int rmcp2_char_change(SID session_id, int command, char *opt, int optlen)*

La fonction *rmcp2_ char _change setsockopt()* permet à une application du gestionnaire de session de fixer ou de modifier les caractéristiques d'une session RMCP-2 (informations AUTH par exemple). Si l'opération réussit, cette fonction retourne zéro; dans le cas contraire, elle retourne un entier négatif avec un code d'erreur approprié.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2008