Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

J.360

(11/2006)

SÉRIE J: RÉSEAUX CÂBLÉS ET TRANSMISSION DES SIGNAUX RADIOPHONIQUES, TÉLÉVISUELS ET AUTRES SIGNAUX MULTIMÉDIAS

IPCablecom

Architecture générale IPCablecom2

Recommandation UIT-T J.360

Recommandation UIT-T J.360

Architecture générale IPCablecom2

Résumé

La Recommandation UIT-T J.360 décrit le cadre architectural et donne un aperçu technique de l'élargissement de l'architecture IPCablecom au multimédia.

Source

La Recommandation UIT-T J.360 a été approuvée le 29 novembre 2006 par la Commission d'études 9 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) 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 de 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

Recommandation UIT-T J.360

Architecture générale IPCablecom2

1 Domaine d'application et aperçu général

1.1 Domaine d'application

La version initiale de l'architecture IPCablecom [UIT-T J.160-178] s'applique à la téléphonie. L'architecture IPCablecom multimédia [UIT-T J.179] crée un pont permettant d'élargir l'architecture IPCablecom à toute une série de services multimédias. La présente Recommandation contient le cadre architectural, les bases techniques et l'organisation du projet concernant la deuxième version de la famille de Recommandations sur l'architecture IPCablecom dont l'objet est l'élargissement au domaine multimédia.

1.2 Aperçu général de l'architecture IPCablecom2

L'architecture IPCablecom2, élaborée par le secteur du câble, est destinée à favoriser la convergence de la voix, de la vidéo, des données et des technologies de mobilité. Les abonnés aux services large bande par câble se comptent en dizaines de millions et la capacité du réseau à assurer des services innovants au-delà de l'accès Internet haut débit ne cesse de s'accroître. En particulier, les services de communication en temps réel fondés sur les protocoles IP – par exemple la téléphonie utilisant le protocole Internet (VoIP, *voice over Internet protocol*) – évoluent rapidement, les dispositifs d'abonné et les types de média étant très variés. De nouvelles technologies – comme les visiocommunications IP et la capacité d'afficher des notifications de message vocal et vidéo sur un téléviseur – devraient changer la façon dont les services de communication et de divertissement sont offerts. Ces technologies de pointe offrent de nouvelles opportunités très intéressantes qui permettront aux câblo-opérateurs de fournir de façon rentable des services de premier plan aux abonnés.

L'architecture IPCablecom2 et l'ensemble de ses interfaces ouvertes sont définis sur la base de nouvelles technologies de communication, par exemple le protocole d'ouverture de session (SIP, *session initiation protocol*) de [IETF RFC 3261], afin de permettre la mise en œuvre rapide de nouveaux services fondés sur le protocole IP dans le réseau câblé. Une approche modulaire permet aux opérateurs de mettre en place de façon souple les capacités de réseau requises par leurs offres de service spécifiques, tout en maintenant l'interopérabilité des divers dispositifs provenant de plusieurs fournisseurs. Définie sciemment de façon indépendante des services, la plate-forme devrait offrir les capacités de base dont les opérateurs ont besoin pour déployer des services, par exemple dans les domaines suivants:

- VoIP résidentielle évoluée et visiocommunications IP – exemples de capacités: visiophonie; traitement des appels fondé sur la présence, la capacité des dispositifs et l'identité; fonctionnalités de type "clic de numérotation".
- Intégration croisée de fonctionnalités de plate-forme – exemples de capacités: identification du nom et du numéro de l'appelant sur le téléviseur et traitement des appels depuis le téléviseur.
- Services de mobilité et intégration avec les réseaux cellulaires et les réseaux sans fil – exemples de capacités: transfert d'appel et itinérance entre la VoIP IPCablecom sur réseaux WiFi et réseaux cellulaires; intégration de la messagerie vocale; numéro E.164 unique (par exemple numéro de téléphone).
- Applications multimédias – exemples de capacités: diffusion audio et vidéo en continu avec prise en charge de la QS.

- Extensions des services commerciaux – exemples de capacités: extension des autocommutateurs privés; services de Centrex IP pour les petites et moyennes entreprises; jonction VoIP pour les autocommutateurs privés IP d'entreprise.
- Extensions de la téléphonie SIP résidentielle – exemples de capacités: fonctionnalités téléphoniques traditionnelles (par exemple appel en instance, identité de l'appelant), services par opératrice et services d'urgence.

Comme indiqué plus haut, l'architecture est conçue pour prendre en charge une grande variété de services. L'ensemble des Recommandations portant sur IPCablecom2 définissent une architecture de base ainsi que les composants et les spécifications génériques nécessaires pour répondre à un grand nombre d'applications et de services. Les applications et services spécifiques reposent sur cette architecture de base mais sont spécifiés dans des documents distincts. Les spécifications de base devraient permettre de prendre en charge différentes applications et différents services moyennant très peu de modifications, si ce n'est aucune.

Cette version de l'architecture IPCablecom est fondée sur la version 6 du sous-système multimédia IP (IMS, IP *multimedia subsystem*) élaborée dans le cadre du projet de partenariat pour la troisième génération (3GPP). Le sous-système IMS est une architecture fondée sur le protocole SIP pour la fourniture de services multimédias. L'architecture IPCablecom2 définit des perfectionnements du sous-système IMS afin de répondre à des besoins que le sous-système IMS ne satisfait pas déjà.

Un objectif important dans ce domaine de travail est d'assurer l'interopérabilité des systèmes IPCablecom 2.0 et IMS 3GPP. L'architecture IPCablecom 2.0 est fondée sur le sous-système IMS 3GPP, mais elle comporte une fonctionnalité supplémentaire nécessaire pour satisfaire aux besoins des câblo-opérateurs. Compte tenu du nombre croissant de solutions convergentes pour les communications sans fil, filaires et par câble, l'évolution future de l'architecture IPCablecom 2.0 devrait continuer de suivre les développements du sous-système IMS réalisés dans le cadre du 3GPP et de contribuer à ces développements, le but étant d'harmoniser le sous-système IMS 3GPP et l'architecture IPCablecom 2.0.

L'architecture IPCablecom2 s'appuie sur d'autres spécifications et normes ouvertes chaque fois que c'est possible.

2 Références

2.1 Références normatives

Aucune.

2.2 Références informatives

[UIT-T J.160] Recommandation UIT-T J.160 (2005), *Cadre architectural pour l'acheminement de services à temps critique sur les réseaux de télévision par câble utilisant des câblo-modems.*

[UIT-T J.170] Recommandation UIT-T J.170 (2005), *Spécification de la sécurité sur IPCablecom.*

[UIT-T J.171.1] Recommandation UIT-T J.171.1 (2005), *Protocole de commande de passerelle de jonction (TGCCP) du système IPCablecom: profil 1.*

[UIT-T J.178] Recommandation UIT-T J.178 (2005), *Signalisation entre serveurs de gestion d'appel IPCablecom.*

[UIT-T J.179 App.I] Recommandation UIT-T J.179 (2005), *Prise en charge du multimédia par IPCablecom.* Appendice I: *Informations de base*.

[UIT-T J.361] Recommandation UIT-T J.361 (2006), *Codecs de média IPCablecom2*.

[UIT-T J.362] Recommandation UIT-T J.362 (2006), *Découverte de point de contrôle IPCablecom2*.

[UIT-T J.363] Recommandation UIT-T J.363 (2006), *Collecte de données IPCablecom2 à des fins de comptabilité*.

[UIT-T J.364] Recommandation UIT-T J.364 (2006), *IPCablecom2 provisioning, activation, configuration and management*.

[UIT-T J.365] Recommandation UIT-T J.365 (2006), *Interface de gestion des applications IPCablecom2*.

[ES-DCI] PacketCable Electronic Surveillance – *Delivery Function to Collection Function Interface Specification*, PKT-SP-ES-DCI-I01-060914 (2006), Cable Television Laboratories, Inc.

[ES-INF] PacketCable Electronic Surveillance – *Intra-Network Functions Specification*, PKT-SP-ES-INF-I01-060406, 6 April 2006, Cable Television Laboratories, Inc.

[IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

[TS 23.002] 3GPP 23.002 v6.10.0, *Network Architecture*, décembre 2005.

3 Termes et définitions

La présente Recommandation utilise les termes et définitions suivants:

3.1 adresse de contact: identificateur URI d'un agent d'utilisateur sur le réseau. Dans le contexte d'IPCablecom, les adresses de contact sont souvent, mais pas toujours, les adresses utilisées pour transmettre des demandes à un agent d'utilisateur spécifique.

3.2 E.164: Recommandation UIT-T qui définit le plan de numérotage des télécommunications publiques internationales utilisé dans le RTPC et dans d'autres réseaux de transmission de données.

3.3 tête de réseau: entité centrale dans le réseau câblé, chargée de transmettre vers l'aval des signaux vidéo de diffusion et d'autres signaux.

3.4 spécifications delta relatives au sous-système IMS: série de spécifications 3GPP relatives au sous-système IMS modifiées afin de tenir compte des modifications propres au transport par câble nécessaires pour assurer la compatibilité avec l'architecture IPCablecom.

3.5 IPCablecom multimédia: architecture de QS indépendante de l'application pour les services offerts sur des réseaux DOCSIS.

3.6 identité privée: voir identité d'utilisateur privée.

3.7 identité d'utilisateur privée: utilisée, par exemple, pour l'enregistrement, l'autorisation, l'administration et la comptabilité. Une identité d'utilisateur privée est associée à une ou plusieurs identités d'utilisateur publiques.

3.8 identité publique: voir identité d'utilisateur publique.

3.9 identité d'utilisateur publique: utilisée par n'importe quel utilisateur pour demander des communications à destination d'autres utilisateurs.

3.10 agent d'utilisateur SIP: équivalent d''agent d'utilisateur'.

3.11 serveur: élément de réseau qui reçoit des demandes, les traite et renvoie des réponses à ces demandes. Exemples de serveurs: proxys, serveurs d'agent d'utilisateur, serveurs de réacheminement et serveurs d'enregistrement.

3.12 abonné: entité (comportant un ou plusieurs utilisateurs) ayant souscrit un abonnement auprès d'un fournisseur de services.

3.13 abonnement: contrat de service(s) entre un utilisateur et un fournisseur de services.

3.14 utilisateur: personne qui, dans le contexte de la présente Recommandation, utilise un service défini ou invoque une fonctionnalité sur un équipement d'utilisateur.

3.15 agent d'utilisateur (UA, *user agent*): agent d'utilisateur SIP, au sens du document [IETF RFC 3261].

3.16 session multimédia: ensemble d'émetteurs et de récepteurs multimédias et flux de données allant des émetteurs aux récepteurs. Une conférence multimédia est un exemple de session multimédia.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

3GPP	projet de partenariat pour la troisième génération (*3rd generation partnership project*)
ALG	passerelle de couche Application (*application layer gateway*)
AM	gestionnaire d'application (*application manager*)
AS	serveur d'application (*application server*)
BGCF	fonction de commande de passerelle d'échappement (*breakout gateway control function*)
CDF	fonction de données de taxation (*charging data function*)
CDR	relevé des données d'appel (*call detail record*)
CM	câblo-modem
CMS	serveur de gestion des appels (*call management server*)
CMTS	système de terminaison de câblo-modem (*cable modem termination system*)
CPE	équipement de locaux d'abonné (*customer premises equipment*)
CSCF	fonction de commande de session d'appel (*call session control function*)
DHCP	protocole de configuration de serveur dynamique (*dynamic host configuration protocol*)
DNS	système de dénomination de domaine (*domain name system*)
DOCSIS	spécification d'interface pour service de transmission de données par câble (*data-over-cable service interface specification*)
EMS	système de gestion d'élément (*element management system*)
E-MTA	adaptateur de terminal multimédia intégré (*embedded multimedia terminal adapter*)
ENUM	conversion de numéro E.164 (*E.164 number mapping*)
ESP	charge utile de sécurité encapsulante (*encapsulating security payload*)
FQDN	nom de domaine complet (*fully qualified domain name*)
FW	pare-feu (*firewall*)
GRUU	identificateur URI d'agent d'utilisateur routable à l'échelle mondiale (*globally routable user agent URI*)

HSS	serveur d'abonnés résidentiels (*home subscriber server*)
HTTP	protocole de transfert hypertexte (*hyper text transfer protocol*)
ICE	établissement de connectivité interactive (*interactive connectivity establishment*)
I-CSCF	fonction interrogatrice de commande de session d'appel (*interrogating call session control function*)
IMS	sous-système multimédia IP (*IP multimedia subsystem*)
IP	protocole Internet (*Internet protocol*)
IPsec	sécurité IP (*Internet protocol security*)
MG	passerelle média (*media gateway*)
MGC	contrôleur de passerelle média (*media gateway controller*)
NAT	traduction d'adresse de réseau (*network address translation*)
NA(P)T	traduction d'adresse de réseau et de port (*network address and port translation*); utilisé de façon interchangeable avec NAT
NCS	signalisation d'appel fondée sur le réseau (*network-based call signalling*)
NMS	système de gestion de réseau (*network management system*)
PAC	(élément PAC) élément d'approvisionnement, d'activation et de configuration (*provisioning, activation and configuration element*)
PACM	approvisionnement, activation, configuration et gestion (*provisioning, activation, configuration, and management*)
PAM	gestionnaire d'application IPCablecom (*IPCablecom application manager*)
P-CSCF	fonction proxy de commande de session d'appel (*proxy call session control function*)
PDS	serveur de fourniture de profil (*profile delivery server*)
PSI	identité de service publique (*public service identity*)
QS	qualité de service
RKS	serveur d'archivage (*record keeping server*)
RTCP	protocole de commande de transport en temps réel (*RTP control protocol*)
RTP	protocole de transport en temps réel (*real-time transport protocol*)
RTPC	réseau téléphonique public commuté
S-CSCF	fonction serveuse de commande de session d'appel (*serving call session control function*)
SDP	protocole de description de session (*session description protocol*)
SG	passerelle de signalisation (*signalling gateway*)
SIP	protocole d'ouverture de session (*session initiation protocol*)
SLF	fonction de localisation d'abonnement (*subscription locator function*)
SNMP	protocole simple de gestion de réseau (*simple network management protocol*)
SNTP	protocole simple relatif au temps dans le réseau (*simple network time protocol*)
SS7	système de signalisation n° 7

STUN simple traversée d'un dispositif NAT par le protocole UDP (*simple traversal of UDP through NAT*)

TCP protocole de commande de transmission (*transmission control protocol*)

TGCP protocole de commande de passerelle de jonction (*trunking gateway control protocol*)

TLS sécurité de la couche transport (*transport layer security*)

TR rapport technique (*technical report*)

TURN traversée au moyen d'un dispositif NAT relais (*traversal using relay NAT*)

UA agent d'utilisateur (*user agent*)

UDP protocole datagramme d'utilisateur (*user datagram protocol*)

UE équipement d'utilisateur (*user equipment*)

URI identificateur universel de ressource (*uniform resource identifier*)

XCAP protocole d'accès à la configuration XML (*XML configuration access protocol*)

XDS serveur de données XCAP (*XCAP data server*)

5 IPCablecom2

La définition de l'architecture IPCablecom2 repose sur la description d'un ensemble de groupes fonctionnels et d'entités logiques ainsi que d'un ensemble d'interfaces (appelées points de référence) qui prennent en charge les flux d'information échangés entre les entités.

Le présent paragraphe contient:

- un aperçu de l'architecture, y compris une description des principaux groupements fonctionnels (par exemple réseau local, réseau d'accès, périphérie, centre) et des principales entités logiques (par exemple UE, P-CSCF, S-CSCF, HSS) appartenant à ces groupements;
- un ensemble d'objectifs nominaux pour l'architecture et les spécifications IPCablecom2;
- la liste des Recommandations relatives à l'architecture IPCablecom2.

5.1 Relation avec le sous-système IMS 3GPP

L'architecture IPCablecom2 est fondée sur la version 6 du sous-système multimédia IP (IMS), définie dans le cadre du projet de partenariat pour la troisième génération (3GPP). Le 3GPP est un accord de collaboration conclu entre différents organismes de normalisation. Il vise à fournir des spécifications techniques et des rapports techniques pour les réseaux GSM et les réseaux de systèmes mobiles de la troisième génération (3G).

Le 3GPP a notamment pour objet d'élaborer une architecture de communication IP fondée sur le protocole SIP pour les réseaux mobiles. Dénommée sous-système multimédia IP, cette architecture définit comment divers protocoles (par exemple, les protocoles SIP et DIAMETER) peuvent être utilisés dans une architecture au niveau du système pour fournir des services de communication SIP.

Dans le cadre général de l'architecture IPCablecom, un objectif consiste à exploiter, chaque fois que c'est possible, les normes de l'industrie existantes afin d'assurer une harmonisation avec l'architecture et les spécifications IMS élaborées dans le cadre du 3GPP. En particulier, l'architecture IPCablecom2 réutilise bon nombre des points de référence et des entités fonctionnelles de base définis dans le sous-système IMS. Cet objectif nominal vise essentiellement à assurer une harmonisation avec un ensemble de normes largement prises en charge par les

produits des fournisseurs et, par conséquent, à minimaliser les efforts à déployer pour élaborer les produits nécessaires à la mise en place des réseaux IPCablecom.

Si un grand nombre des entités fonctionnelles et des points de référence définis dans le sous-système IMS s'appliquent largement à d'autres secteurs, la Version 6 de ce sous-système est en revanche une architecture conçue pour le secteur du sans fil, l'objectif étant de satisfaire les besoins commerciaux et opérationnels de ce secteur. Par conséquent, elle ne répond pas à tous les besoins du secteur du câble. L'architecture IPCablecom2 perfectionne le sous-système IMS afin de prendre en charge les exigences techniques propres au secteur du câble et tient compte également des besoins commerciaux et opérationnels des câblo-opérateurs.

De nouvelles versions des spécifications IMS sont en cours d'élaboration dans le cadre du 3GPP. L'architecture IPCablecom sera actualisée dans l'avenir afin d'assurer une harmonisation avec ces nouvelles versions, en tant que de besoin.

On se reportera au document [TS 23.002] pour obtenir des informations supplémentaires sur l'architecture IMS 3GPP.

5.2 Aperçu général

L'architecture IPCablecom2 est fondée sur l'architecture IMS et comporte certaines extensions comme indiqué au § 5.1. Les extensions incluent l'utilisation de composants fonctionnels supplémentaires ou différents par rapport à l'architecture IMS ainsi que des perfectionnements des capacités offertes par les composants fonctionnels IMS.

Les principaux perfectionnements que l'architecture IPCablecom apporte au sous-système IMS sont notamment les suivants:

- prise en charge de la qualité de service (QS) pour les applications fondées sur le sous-système IMS dans les réseaux d'accès DOCSIS, sur la base de l'architecture IPCablecom multimédia [UIT-T J.179 App.I];
- prise en charge de la traversée des traducteurs d'adresse réseau (NAT, *network address translation*) et des pare-feu (FW, *firewall*) par la signalisation et les médias, sur la base de mécanismes de l'IETF;
- prise en charge de la capacité d'identifier sans ambiguïté un individu et de communiquer avec lui lorsque plusieurs équipements d'utilisateur sont enregistrés sous la même identité publique;
- prise en charge de mécanismes additionnels relatifs à la sécurité de la signalisation dans le réseau d'accès et à l'authentification des équipements d'utilisateur;
- prise en charge de l'approvisionnement, de l'activation, de la configuration et de la gestion des équipements d'utilisateur.

La Figure 1 donne un aperçu des éléments architecturaux et des groupements fonctionnels IPCablecom2.

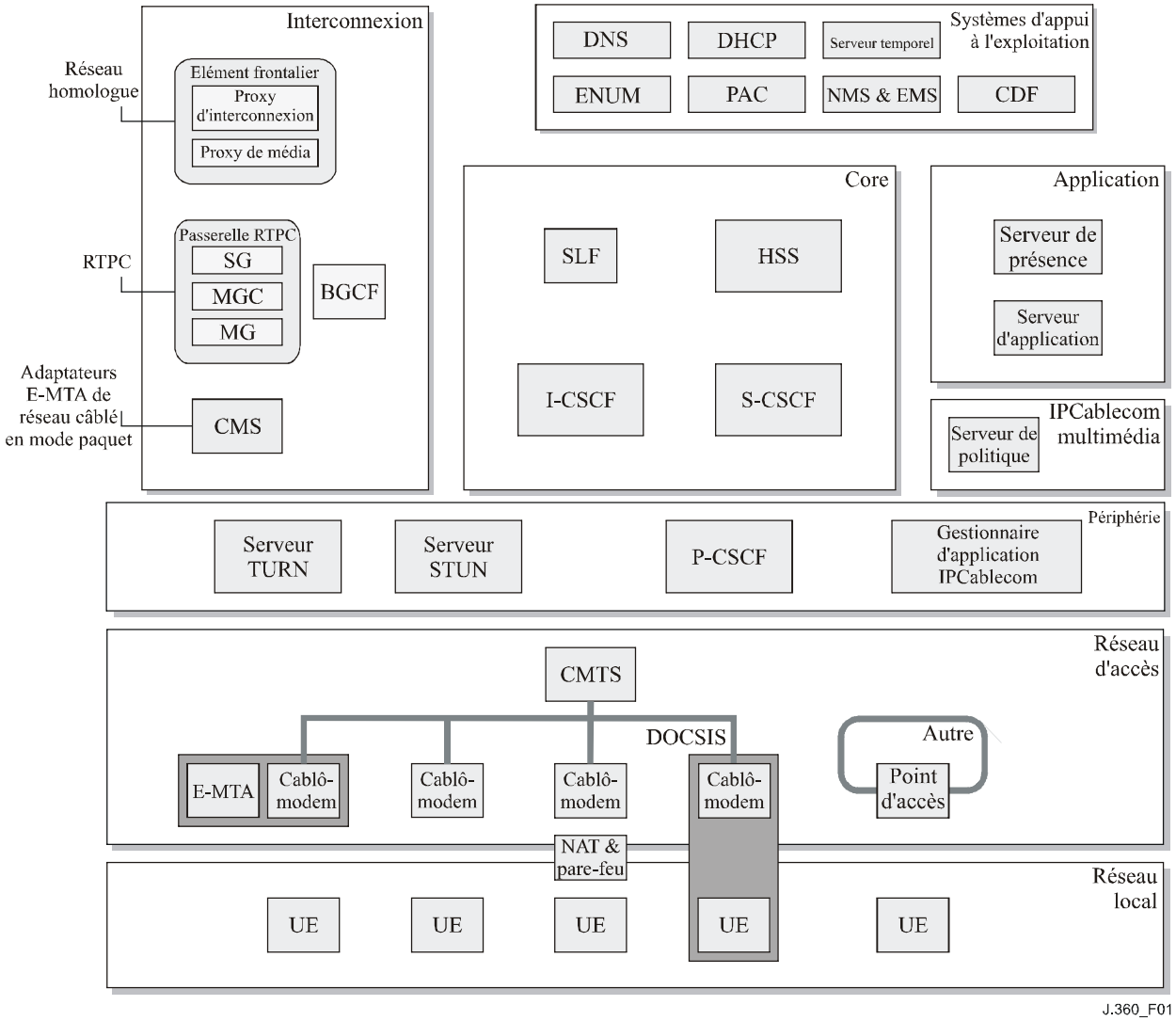


Figure 1 – Architecture de référence IPCablecom

L'architecture constitue une plate-forme riche et modulaire sur laquelle divers services de communication multimédias peuvent être définis pour différents équipements d'utilisateur. Il est à noter que l'architecture de référence illustre plusieurs scénarios différents de déploiement des équipements d'utilisateur (par exemple un équipement d'utilisateur derrière un câblo-modem, une passerelle de type NAT et pare-feu entre l'équipement d'utilisateur et le câblo-modem). Ces scénarios de déploiement visent à montrer le fait que les équipements d'utilisateur peuvent être déployés dans bon nombre de configurations et d'environnements différents. L'architecture de référence n'illustre pas tous les scénarios de déploiement de façon exhaustive.

L'architecture IPCablecom2 repose sur un modèle composé d'utilisateurs, d'identités publiques, d'équipements d'utilisateur et de dispositifs. Les relations potentielles entre les utilisateurs, les identités publiques, les équipements d'utilisateur et les dispositifs sont décrites dans l'Appendice IV. A titre d'exemple, un utilisateur peut avoir plusieurs équipements d'utilisateur (UE, *user equipment*), chacun pouvant être enregistré avec une ou plusieurs identités publiques. Une identité publique peut être un numéro E.164 ou un identificateur alphanumérique qui a un sens dans le contexte d'un service téléphonique SIP. Chaque identité publique est généralement associée à un utilisateur.

L'architecture est subdivisée en plusieurs domaines logiques ou groupements fonctionnels:

- réseau local: le réseau local est le réseau que l'équipement d'utilisateur (UE) utilise pour se raccorder au réseau d'accès. Il peut employer la technologie Ethernet, WiFi, bluetooth, ou toute autre technologie servant à raccorder des équipements d'utilisateur. Une passerelle de type NAT et pare-feu peut être présente entre le réseau local et le réseau d'accès. Dans certains cas, l'équipement d'utilisateur peut inclure un composant de réseau d'accès, auquel cas le réseau local est une interface interne à l'équipement d'utilisateur. C'est le cas lorsqu'un équipement d'utilisateur possède un câblo-modem DOCSIS intégré.

  Un équipement d'utilisateur comporte soit une application logicielle soit un dispositif matériel où les fonctionnalités de service sont invoquées, exécutées ou assurées pour l'abonné. Les équipements d'utilisateur utilisent tous la même infrastructure SIP de base pour obtenir des services multimédias et de communication IP en temps réel. Un équipement d'utilisateur IPCablecom peut être élaboré de façon modulaire et peut contenir des niveaux de fonction variables sur la base des capacités qu'il doit prendre en charge. Par exemple, il peut ne prendre en charge que la messagerie instantanée (IM, *instant messaging*) textuelle, auquel cas il n'a pas besoin de prendre en charge de codec audio ou vidéo. Un dispositif de type NAT et pare-feu peut être présent entre un équipement d'utilisateur situé dans un réseau local et le réseau d'accès. Des mécanismes sont alors nécessaires pour assurer la traversée des dispositifs NAT/FW par la signalisation et les médias;
- réseau d'accès: un équipement d'utilisateur peut résider dans le réseau d'accès DOCSIS ou y être raccordé, ou il peut obtenir des services auprès d'autres réseaux d'accès (y compris d'autres réseaux d'accès câblés en dehors du contrôle du câblo-opérateur associé à l'abonnement IPCablecom); cela est particulièrement important pour un équipement d'utilisateur mobile comme un ordinateur portable, un téléphone WiFi, etc. Lorsqu'un équipement d'utilisateur est situé dans un réseau d'accès câblé, il peut obtenir la QS du réseau d'accès en interagissant avec l'infrastructure de signalisation SIP du réseau câblé, qui à son tour interagit avec l'infrastructure IPCablecom multimédia via le gestionnaire d'application IPCablecom et le serveur de politique pour réserver des ressources dans le réseau d'accès câblé.

  Des adaptateurs E-MTA IPCablecom sont inclus dans le diagramme de référence dans un souci d'exhaustivité;
- périphérie: ce groupement fonctionnel comporte les points de référence avec un équipement d'utilisateur et le réseau d'accès. Un équipement d'utilisateur obtient l'accès à l'infrastructure SIP par le biais de la fonction proxy de commande de session d'appel (P-CSCF). La fonction P-CSCF sert de proxy pour les messages SIP entre l'équipement d'utilisateur et le reste de l'architecture et maintient les associations de sécurité avec l'équipement d'utilisateur. La fonction P-CSCF peut demander des ressources de QS de réseau d'accès au moment de l'ouverture de session pour le compte de l'équipement d'utilisateur via le gestionnaire d'application IPCablecom. Celui-ci présente une interface avec le serveur de politique IPCablecom multimédia, qui "pousse" la politique de QS dans les composants du réseau d'accès câblé. Les serveurs STUN et TURN de l'IETF permettent l'accès aux médias par le biais de dispositifs NAT & FW (la fonction P-CSCF utilise un serveur STUN distinct pour l'accès à la signalisation par le biais de dispositifs NAT & FW). Les adaptateurs E-MTA IPCablecom sont desservis par leur serveur CMS comme décrit dans le Rapport technique relatif au cadre de l'architecture IPCablecom 1.5 [UIT-T J.160];
- centre: le centre contient les composants de base nécessaires pour fournir les services SIP et les données d'abonné. Ce groupement fonctionnel comporte les composants fonctionnels suivants: fonction CSCF interrogatrice (I-CSCF), fonction CSCF serveuse (S-CSCF), fonction de localisation d'abonnement (SLF, *subscription locator function*) et serveur d'abonnés résidentiels (HSS, *home subscriber server*);

- la fonction I-CSCF est le point d'entrée initial dans le centre pour les messages SIP. Elle coopère avec le serveur HSS pour déterminer la fonction S-CSCF à attribuer une identité publique et achemine les demandes provenant d'un équipement d'utilisateur à la fonction S-CSCF attribuée à l'identité publique de l'équipement d'utilisateur d'origine. La fonction I-CSCF achemine également les demandes SIP de terminaison reçues en provenance de l'intérieur du réseau ou de réseaux extérieurs. Dans ce cas, la fonction I-CSCF consulte le serveur HSS pour déterminer la fonction S-CSCF qui est attribuée à une identité publique de terminaison et achemine la demande SIP à cette fonction S-CSCF pour traitement. La fonction I-CSCF peut également assurer un masquage de la topologie lorsqu'elle communique avec des réseaux extérieurs;
- la fonction S-CSCF est chargée du traitement de session SIP. Les appels ou sessions de communication multimédias à destination et en provenance d'identités publiques sont envoyés à la fonction S-CSCF attribuée pour autorisation et traitement. La fonction S-CSCF a un cadre de commande de service qui évalue les demandes SIP par rapport à des critères de filtrage prédéfinis pour un abonné ou détermine s'il convient d'acheminer la demande SIP à un serveur d'application pour traitement. L'architecture extensible qui en découle permet de mettre en place rapidement des services et des fonctionnalités à valeur ajoutée. La fonction S-CSCF peut acheminer les messages SIP à des serveurs d'application, à des serveurs de présence, à d'autres fonctions CSCF ou à des fonctions de commande de passerelle d'échappement (BGCF, *breakout gateway control function*), selon le cas. La fonction S-CSCF inclut aussi la fonction de serveur d'enregistrement SIP, qui convertit les identités publiques en adresses de contact SIP enregistrées, attribue les identificateurs URI d'agent d'utilisateur routables à l'échelle mondiale (GRUU, *globally routable user agent*) et stocke les éventuels autres paramètres associés à l'enregistrement, par exemple les capacités d'agent d'utilisateur SIP. La fonction S-CSCF obtient les données relatives à l'abonnement auprès du serveur HSS;
- le serveur HSS permet à la fonction S-CSCF et aux serveurs d'application d'accéder aux profils d'utilisateur et aux autres données d'abonné fournies. En outre, il maintient l'attribution des identités publiques à une fonction S-CSCF. Un abonnement peut être associé à plusieurs identités publiques. Un serveur HSS associe un abonnement à une fonction S-CSCF, ce qui signifie que toutes les identités publiques seront attribuées au même serveur HSS;
- les fonctions S-CSCF et les serveurs d'application peuvent stocker certaines catégories de données associées aux abonnements dans le serveur HSS;
- la fonction SLF sert à localiser une instance de serveur HSS pour une identité donnée lorsque plusieurs serveurs HSS sont présents;
- applications: le groupement fonctionnel des serveurs d'application définit les serveurs d'application qui peuvent être invoqués dans le cadre du traitement de messages à l'entrée ou à la sortie au niveau d'une fonction S-CSCF pour un utilisateur donné ou il peut s'agir de serveurs d'application autonomes qui peuvent être invoqués et exploités de façon indépendante. Le serveur de présence est un serveur d'application spécialisé qui contient des données de présence relatives aux identités publiques. Les données de présence sont obtenues à partir de diverses sources dans le réseau et donnent une indication de la volonté et de la disponibilité de l'utilisateur en matière de communications. Le serveur de présence gère la confidentialité des données de présence et l'autorisation d'abonnement à ces données;
- interconnexion: le groupement fonctionnel d'interconnexion permet le raccordement à d'autres réseaux. L'interconnexion avec le RTPC est gérée via la fonction de commande de passerelle d'échappement (BGCF), qui détermine le contrôleur de passerelle média (MGC, *media gateway controller*) à utiliser pour l'interconnexion avec le RTPC. Le contrôleur MGC commande les passerelles de média (MG), qui assurent l'interconnexion

avec le RTPC au niveau de la couche transport et du support. Les passerelles de signalisation (SG, *signalling gateway*) assurent la connectivité SS7. Les contrôleurs MGC, passerelles de signalisation et passerelles de média IPCablecom servent à assurer l'interconnexion avec le RTPC. L'interconnexion avec les réseaux homologues de téléphonie utilisant le protocole Internet (VoIP, *voice over Internet protocol*) peut être assurée par le biais d'un élément frontalier. Celui-ci contient la fonctionnalité de proxy d'interconnexion et facultativement la fonctionnalité de proxy de média, qui peuvent se trouver sur des plates-formes distinctes. Le proxy d'interconnexion peut exécuter diverses tâches, notamment l'application de profils de protocole et la conversion de la signalisation, selon qu'il est nécessaire pour assurer l'interfonctionnement avec les autres réseaux. Le relais de média peut relayer les médias aux fins de masquage de la topologie. Le serveur CMS IPCablecom est situé dans le groupement fonctionnel d'interconnexion pour indiquer que les adaptateurs E-MTA qu'il dessert peuvent communiquer avec les équipements d'utilisateur;

- systèmes d'appui à l'exploitation: les systèmes d'appui à l'exploitation remplissent diverses fonctions comme la comptabilité et l'approvisionnement des équipements d'utilisateur. La fonction CDF collecte les messages de comptabilité provenant des divers éléments, le système DHCP distribue les adresses IP aux équipements d'utilisateur, les systèmes ENUM et DNS assurent la résolution des identificateurs URI et des noms FQDN, les systèmes PAC et XDS prennent en charge l'approvisionnement et la configuration des équipements d'utilisateur et les systèmes EMS et NMS remplissent des fonctions de surveillance et de gestion.

Il est à noter que les composants fonctionnels décrits ci-dessus sont des fonctions logiques, qui peuvent être combinées sur des plates-formes communes.

5.3 Versions IPCablecom et organisation

5.3.1 Versions IPCablecom

L'architecture IPCablecom continue d'évoluer au fur et à mesure de l'ajout de nouvelles capacités. Il en existe plusieurs versions.

- Version 1.0 – Cette version permet de prendre en charge une application de téléphonie au moyen d'adaptateurs E-MTA; elle est spécifiée dans la version initiale des Recommandations UIT-T J.160-178.
- Version 1.5 – Cette version définit des capacités supplémentaires et le protocole SIP est ajouté pour la gestion de session à l'intérieur d'un réseau IPCablecom ou entre des réseaux IPCablecom; cette version est spécifiée dans les révisions des Recommandations UIT-T J.160-178.
- Multimédia – Cette version sépare les capacités de QS et définit une architecture générique de QS; elle est spécifiée dans [UIT-T J.179].
- Version 2 – Dans cette version, on ajoute la prise en charge de points d'extrémité SIP et d'une plate-forme de services SIP qui peut être utilisée pour prendre en charge divers services.

La Figure 2 présente les versions IPCablecom. Les applications qui utilisent la plate-forme de services SIP seront définies dans des versions autonomes distinctes et ne sont pas indiquées sur la Figure 2.

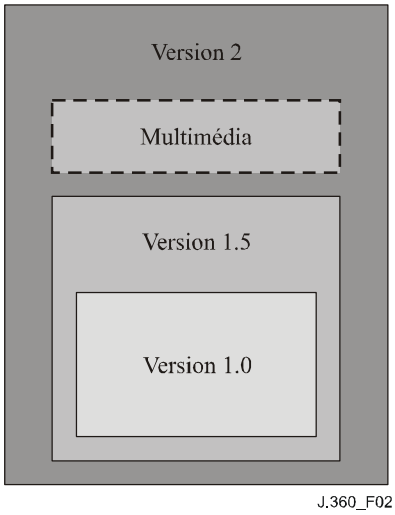


Figure 2 – Versions IPCablecom

5.3.2 Organisation de la version IPCablecom

L'organisation de cette version IPCablecom2 est fondée sur la double nécessité d'une harmonisation avec le sous-système IMS et d'une extension de ce sous-système. La Figure 3 présente le contenu de la version IPCablecom2.

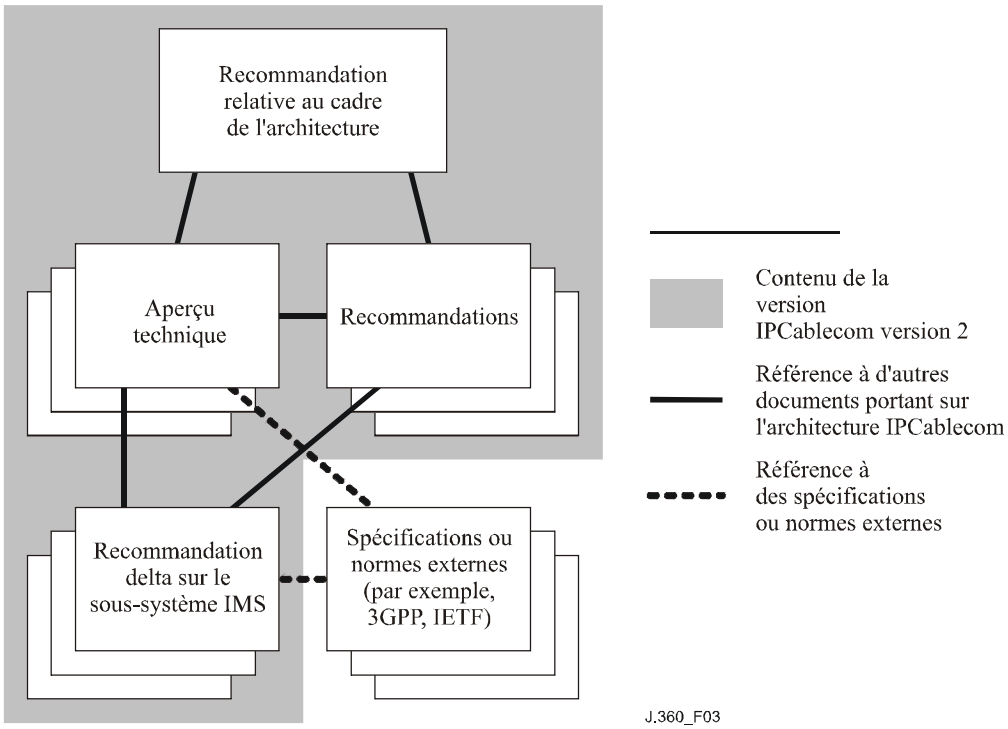


Figure 3 – Organisation de la version IPCablecom2

La présente Recommandation contient une description de haut niveau du cadre de l'architecture IPCablecom2. Les différents domaines fonctionnels (par exemple SIP, traversée de dispositif NAT/FW, sécurité) font l'objet d'appendices ou de Recommandations spécifiques. L'objet de ces documents est de traiter des questions relatives à l'architecture et de décrire l'utilisation attendue du sous-système IMS pour le câble. Un document peut être une spécification s'il contient des informations relatives à des exigences normatives et définit des points de référence qui sont propres à l'architecture IPCablecom, ou s'il apporte très peu de modifications à une spécification IMS (en d'autres termes, les modifications apportées à une spécification IMS n'étaient pas suffisamment nombreuses pour justifier la publication d'une spécification delta relative au sous-système IMS).

Dans certains cas, ces documents ne s'appuient pas sur des composants architecturaux ou des points de référence IMS. Toutefois, ces documents sont généralement fondés sur le sous-système IMS et, parfois, perfectionnent ce sous-système. Les documents qui sont fondés sur le sous-système IMS font simplement référence aux documents IMS de la même façon que tout autre document fait l'objet d'une référence normative. Les perfectionnements apportés au sous-système IMS sont décrits dans des spécifications delta relatives au sous-système IMS. Celles-ci sont des spécifications IMS republiées qui contiennent des modifications fondées sur les exigences propres au secteur du câble. Suivant la façon dont les documents IMS sont organisés, une spécification delta relative au sous-système IMS peut contenir des modifications concernant un certain nombre de rapports techniques ou spécifications IPCablecom différents. Par exemple, la spécification delta relative au sous-système IMS se rapportant à la spécification 3GPP TS 24.229 contient des modifications relatives aux domaines fonctionnels suivants: SIP, traversée du dispositif NAT & FW, sécurité et QS.

Le but est d'introduire les perfectionnements apportés par l'architecture IPCablecom au sous-système IMS dans des spécifications 3GPP à part entière, ce qui permet ensuite de supprimer les spécifications delta relatives au sous-système IMS et de les remplacer par des références directes à des spécifications 3GPP relatives au sous-système IMS.

Le Tableau 1 contient la liste des Recommandations.

Tableau 1 – Recommandations relatives à l'architecture IPCablecom2

Numéro de référence de Recommandation relative à l'architecture IPCablecom2	Titre
J.360	Cadre de l'architecture (la présente Recommandation)
Appendice I	Aperçu de la signalisation SIP IPCablecom2
Appendice II	Aperçu de la qualité de service IPCablecom2
Appendice III	Aperçu de la sécurité IPCablecom2
Appendice IV	Aperçu du serveur d'abonnés résidentiels (HSS) IPCablecom2
Appendice V	Aperçu de la traversée de dispositif NAT et de pare-feu IPCablecom2
Appendice VI	Aperçu de la stratégie IPv6 et IPv4 IPCablecom2

Tableau 1 – Recommandations relatives à l'architecture IPCablecom2

Numéro de référence de Recommandation relative à l'architecture IPCablecom	Titre
J.362	Découverte de point de commande IPCablecom2
J.365	Interface de gestion d'application IPCablecom2
J.364	Approvisionnement, activation, configuration et gestion IPCablecom2
J.361	Codecs de média IPCablecom2
J.363	Collecte de données pour la comptabilité IPCablecom2
Numéro de référence de spécification delta relative au sous-système IMS	**Titre**
J.366.0	Recommandations delta sur le sous-système IMS IPCablecom2 – Aperçu général
J.366.1	IPCablecom2 – Organisation des données d'abonné (3GPP TS 23.008)
J.366.2	IPCablecom2 – Etape 2 du modèle d'appel multimédia IP (3GPP TS 23.218)
J.363.3	IPCablecom2 – Etape 2 du sous-système multimédia IP (3GPP TS 23.228)
J.366.4	IPCablecom2 – Etape 3 des protocoles SIP et SDP (3GPP TS 24.229)
J.366.5	IPCablecom2 – Interfaces Cx et Dx (3GPP TS 29.288)
J.366.6	IPCablecom2 – Interfaces Cx et Dx et protocole Diameter (3GPP TS 29.229)
J.366.7	IPCablecom2 – Sécurité d'accès pour les services IP (3GPP TS 33.203)
J.366.8	IPCablecom2 – Sécurité dans le domaine de réseau (3GPP TS 33.210)
J.366.9	IPCablecom2 – Architecture d'authentification générique (3GPP TS 33.220)

Comme décrit au § 1.2, cette version IPCablecom2 définit une architecture de base sur laquelle des applications peuvent être définies. Ces applications reposent sur l'architecture de base mais elles sont indépendantes de cette architecture et sont spécifiées dans des documents distincts.

5.4 Considérations relatives à la conception de l'architecture IPCablecom2

Pour permettre d'assurer des communications IP en temps réel passant par l'infrastructure d'un réseau câblé, les spécifications IPCablecom2 définissent des exigences techniques et spécifient des points de référence dans les domaines suivants:

- signalisation et commande de service;
- données d'abonné;
- traversée de traduction d'adresse de réseau (NAT, *network address translation*) et de pare-feu;
- qualité de service;
- transport et codage des flux de média;
- approvisionnement, activation, configuration et gestion;
- comptabilité et utilisation du réseau;

- sécurité;
- interception licite.

5.4.1 Objectifs génériques concernant l'architecture

Concernant l'architecture IPCablecom2, les objectifs nominaux sont les suivants:

- définir une architecture indépendante des services, permettant d'ajouter de nouveaux services sans incidence sur la plate-forme de commande de service sous-jacente;
- définir une architecture modulaire, avec différentes possibilités de combinaison des composants architecturaux afin de prendre en charge une grande diversité de fonctionnalités. Par exemple, un équipement d'utilisateur peut être construit à partir de plusieurs modules de base (par exemple agents d'utilisateur SIP, points d'extrémité de média, observateurs de présence et abonnés aux événements);
- prendre en charge des relations multipoint à multipoint entre utilisateurs, dispositifs d'extrémité et sessions;
- prendre en charge une grande variété d'équipements d'utilisateur, y compris les équipements d'utilisateur sous forme logicielle ou matérielle, les équipements d'utilisateurs intelligents, les équipements d'utilisateurs filaires ou sans fil;
- prendre en charge le fonctionnement IPv4 et IPv6;
- prendre en charge l'interfonctionnement avec les versions précédentes de l'architecture IPCablecom;
- prendre en charge la mobilité des équipements d'utilisateur de manière à leur permettre d'accéder aux services depuis n'importe quel réseau d'accès et pas uniquement depuis le réseau d'accès câblé. D'une manière générale, dans le contexte de l'architecture IPCablecom, la mobilité signifie qu'un équipement d'utilisateur avec connectivité IP peut accéder aux services IPCablecom. Ce type de mobilité est différent de l'itinérance 3GPP (à savoir que la fonction P-CSCF peut être située dans le réseau visité), mais les perfectionnements apportés par l'architecture IPCablecom ne devraient pas affecter le modèle d'itinérance 3GPP;
- exploiter les normes et les protocoles ouverts existants chaque fois que c'est possible et surtout, adopter l'architecture IMS et définir les extensions nécessaires.

5.4.2 Signalisation et commande de service

Concernant la signalisation et la commande de service IPCablecom2, les objectifs nominaux sont les suivants:

- prendre en charge plusieurs modèles de commande de service: commande dans l'équipement d'utilisateur, commande dans le réseau et commande partagée. Il appartient à chaque application spécifique qui utilise l'architecture IPCablecom de définir le modèle de commande de service;
- prendre en charge la capacité pour les utilisateurs à établir des sessions de communication avec les autres utilisateurs présents dans le même réseau, avec des utilisateurs présents dans des réseaux homologues ou avec le RTPC;
- prendre en charge les équipements d'utilisateur non enregistrés pour ce qui est des services d'urgence et de la configuration d'équipement d'utilisateur.

5.4.3 Données d'abonné

Concernant les données d'abonné IPCablecom2, les objectifs nominaux sont les suivants:

- définir une entité logique qui soit le répertoire central pour les informations relatives aux utilisateurs finals ou aux abonnements nécessaires pour l'invocation ou l'exécution de services par les fonctions CSCF et les serveurs d'application;
- permettre un stockage et une distribution centralisés des données persistantes ou semi-persistantes.

5.4.4 Traversée de traducteur d'adresse réseau et de port (NA(P)T) et de pare-feu

Concernant la traversée de dispositif NAT (NAT et NAPT sont employés de façon interchangeable) et de pare-feu IPCablecom2, les objectifs nominaux sont les suivants:

- ne pas imposer d'exigences aux dispositifs NAT et ne pas exiger que le réseau ait connaissance de la présence d'un dispositif NAT;
- prendre en charge plusieurs équipements d'utilisateur derrière un même dispositif NAT;
- pouvoir prendre en charge à la fois les demandes entrantes en provenance d'équipements d'utilisateur et les demandes sortantes à destination d'équipements d'utilisateur passant par des dispositifs NAT;
- pouvoir maintenir des liens avec plusieurs fonctions P-CSCF pour assurer une fourniture fiable des messages entrants en cas de défaillance de l'une des fonctions P-CSCF;
- prendre en charge la traversée des dispositifs NAT entre l'équipement d'utilisateur et le réseau (dispositif NAT résidentiel, dispositif NAT dans un réseau visité);
- définir une solution de traversée indépendante de l'application. En d'autres termes, la solution devrait employer des mécanismes utilisables par des applications non SIP. Toutefois, un appui peut devoir être assuré par les applications pour pouvoir utiliser les mécanismes définis;
- éviter les trajets de média inutilement longs dus à l'"épinglage" des médias;
- pouvoir rétablir les communications en cas de défaillance (par exemple en cas de réamorçage de dispositif NAT/FW et de perte des liens NAT).

5.4.5 Qualité de service

Concernant la qualité de service IPCablecom2, les objectifs nominaux sont les suivants:

- exploiter la spécification de l'architecture IPCablecom multimédia afin d'assurer une certaine qualité de service lorsqu'un abonné accède au service par le biais du réseau DOCSIS;
- prendre en charge le marquage et la classification des paquets depuis le réseau d'accès de manière à pouvoir utiliser un mécanisme de QS comme DiffServ (services différenciés) dans le réseau dorsal;
- offrir un mécanisme qui ne nécessite pas que les applications aient connaissance de la topologie du réseau d'accès.

5.4.6 Transport et codage des flux de média

Concernant le transport et le codage des flux de média IPCablecom2, les objectifs nominaux sont les suivants:

- minimaliser les effets de latence, de perte de paquets et de gigue sur les flux de média sensibles (par exemple voix et vidéo) pour garantir un certain niveau de qualité dans les environnements visés (téléphonie/visiophonie, diffusion en continu de vidéo IP et communications hertziennes);

- définir un ensemble de codecs audio et vidéo et les protocoles de transmission de média associés qui peuvent être pris en charge;
- tenir compte des nouvelles technologies de codec vocal à bande étroite et à large bande;
- tenir compte des nouvelles technologies de codec vidéo pour prendre en charge des applications comme la visiophonie, la diffusion en continu de vidéo IP, etc;
- spécifier des exigences minimales concernant l'annulation d'écho et la détection d'activité vocale;
- prendre en charge la transmission transparente et sans erreur des signaux multifréquence à deux tonalités (DTMF, *dual-tone multifrequency*);
- prendre en charge le relais de télécopie, le relais de modem, le relais DTMF et le téléimprimeur;
- prendre en charge le calcul et la signalisation des valeurs de paramètres de qualité vocale.

5.4.7 Approvisionnement, activation, configuration et gestion (PACM)

Concernant l'élément PACM IPCablecom2, les objectifs nominaux sont les suivants:

- prendre en charge des modèles PACM statiques et dynamiques simples, compte tenu à la fois d'environnements contrôlés (le réseau local des équipements d'utilisateur est sous le contrôle du fournisseur de services) et d'environnements non contrôlés (le réseau local des équipements d'utilisateur n'est pas sous le contrôle du fournisseur de services);
- prendre en charge un mécanisme de découverte de fonction P-CSCF non fondé sur le protocole DHCP;
- prévoir un cadre PACM multi-couches pour les équipements d'utilisateur, les services et les utilisateurs, ce qui permet de prendre en charge des définitions PACM distinctes pour chaque couche;
- prendre en charge des méthodes de mise à niveau des logiciels pour les équipements d'utilisateur;
- prendre en charge plusieurs modèles d'exploitation (propriétaires ou non propriétaires).

5.4.8 Comptabilité et utilisation du réseau

Concernant la comptabilité et l'utilisation du réseau IPCablecom2, les objectifs nominaux sont les suivants:

- pouvoir comptabiliser en temps réel l'utilisation du réseau et les activités dans le réseau.

  Dans ce cas, la mention de temps réel se rapporte au moment où les événements sont envoyés au répertoire central mais pas au moment où la facture définitive peut être mise à la disposition de l'abonné ni au fait que des événements sont envoyés pour indiquer le supplément d'utilisation des ressources du réseau (taxation en ligne);
- permettre à plusieurs éléments de réseau de produire des événements qui peuvent être corrélés à une certaine session ou à un certain abonné;
- prendre en charge la corrélation des événements de comptabilité entre les plans de signalisation et support;
- faciliter la mise en place rapide de fonctionnalités et de services en minimalisant l'incidence sur les autres éléments de réseau et leur nécessité de signaler des informations relatives aux fonctionnalités et aux services.

5.4.9 Sécurité

Concernant la sécurité IPCablecom2, les objectifs nominaux sont les suivants:

- prendre en charge des mécanismes de confidentialité, d'authentification, d'intégrité et de contrôle d'accès;
- assurer la protection du réseau contre diverses attaques (déni de service, interruption du réseau, vol de service);
- assurer la protection des équipements d'utilisateur contre les attaques par déni de service, les vulnérabilités de sécurité, l'accès non autorisé (depuis le réseau);
- assurer le respect de la vie privée des utilisateurs finals au moyen du chiffrement et de mécanismes de contrôle d'accès aux données d'abonné (informations de présence par exemple);
- prendre en charge des mécanismes permettant d'authentifier les équipements d'utilisateur et de sécuriser l'approvisionnement, la signalisation, les médias et le téléchargement de logiciels.

5.4.10 Interception licite

Concernant l'interception licite IPCablecom2, les objectifs nominaux sont les suivants:

- prendre en charge une architecture d'interception indépendante du service et relativement indépendante des capacités de service IPCablecom de base;
- maximaliser la transparence de la surveillance dans le réseau;
- veiller à ce que l'architecture de surveillance n'impose pas de contrainte à la conception des applications;
- prendre en charge l'interception des appels fondés sur les protocoles NCS et SIP.

6 Composants fonctionnels IPCablecom

Le présent paragraphe décrit plus en détails chacune des fonctions de l'architecture IPCablecom.

6.1 Réseau local

6.1.1 Equipement d'utilisateur (UE)

L'architecture IPCablecom prend en charge des clients NCS pour les services de téléphonie. L'architecture IPCablecom multimédia offre un cadre de QS et de comptabilité indépendant du service. Dans l'architecture IPCablecom2, on ajoute la prise en charge de clients SIP avec diverses capacités (par exemple téléphone logiciel ou matériel, téléphone intelligent, téléphone filaire ou sans fil, équipement d'utilisateur avec messagerie instantanée, terminal de visiocommunications, etc.). Tout comme les clients IMS, les clients IPCablecom sont appelés équipements d'utilisateur (UE, *user equipment*). Tous les divers équipements d'utilisateur décrits précédemment utilisent la même infrastructure de base pour obtenir des services multimédias. Les équipements d'utilisateur peuvent être des dispositifs fixes ou mobiles (ordinateur portable ou téléphone WiFi par exemple). Ils peuvent se trouver dans le réseau d'accès câblé ou peuvent obtenir des services depuis d'autres réseaux d'accès. Lorsque les équipements d'utilisateur se trouvent dans le réseau d'accès câblé, ils peuvent obtenir la QS du réseau d'accès en interagissant avec l'infrastructure de signalisation, laquelle interagit à son tour avec le serveur de politique IPCablecom multimédia.

6.1.2 Dispositif NAT et pare-feu

Un dispositif NA(P)T (traduction de port et d'adresse réseau) et un pare-feu peuvent être présents entre le réseau local et le réseau d'accès. Comme le dispositif NAT peut modifier les ports et les adresses IP et qu'un pare-feu retreint l'accès, les plans de signalisation et support doivent se comporter différemment lorsque ces éléments sont insérés entre l'équipement d'utilisateur et la fonction P-CSCF.

6.2 Réseau d'accès

L'équipement d'utilisateur se raccorde à la périphérie par le biais du réseau d'accès câblé existant ou d'autres réseaux d'accès disponibles (par exemple point d'accès WiFi public, réseau de données cellulaire 3G). Les éléments du réseau d'accès fournissent la connectivité IP et les ressources de QS dont l'équipement d'utilisateur a besoin pour assurer les services IPCablecom.

6.2.1 Câblo-modem (CM)

Le câblo-modem est l'équipement de locaux d'abonné (CPE, *customer premises equipment*) utilisé conjointement avec le système CMTS pour offrir un service d'accès Internet haut débit. Un adaptateur E-MTA est un client NCS IPCablecom comportant un câblo-modem intégré. L'adaptateur E-MTA ne communique pas directement avec le réseau, mais il est important de noter qu'un service de téléphonie NCS et un service SIP peuvent être assurés par le biais du même câblo-modem.

6.2.2 Système de terminaison de câblo-modem (CMTS)

Le système CMTS se trouve dans la tête de réseau du câblo-opérateur et il est utilisé conjointement avec le câblo-modem pour offrir un service d'accès Internet haut débit. Les spécifications DOCSIS, à commencer par la Rec. UIT-T J.112, permettent d'offrir une certaine QS dans le réseau d'accès. L'architecture IPCablecom multimédia permet aux services compatibles IP de demander une certaine QS au réseau DOCSIS. L'architecture IPCablecom permet d'offrir une certaine QS pour les services SIP via les systèmes IPCablecom multimédia et DOCSIS.

6.2.3 Point d'accès

L'architecture IPCablecom peut être utilisée pour offrir un service aux équipements d'utilisateur qui obtiennent la connectivité IP par le biais d'autres types de réseaux d'accès.

6.3 Périphérie

6.3.1 Fonction proxy de commande de session d'appel (P-CSCF)

Un équipement d'utilisateur accède à l'infrastructure SIP par le biais d'une fonction P-CSCF. Celle-ci masque au réseau SIP les détails de protocole propres au réseau d'accès et assure une certaine modulabilité de l'infrastructure en gérant certaines tâches nécessitant beaucoup de ressources lors de l'interaction avec l'équipement d'utilisateur. Elle représente également la limite de confiance pour le protocole SIP entre les parties non fiables (réseau d'accès, réseau local) et les parties fiables (réseau central, application, interconnexion, systèmes d'appui à l'exploitation) du réseau. Les fonctions exécutées par la fonction P-CSCF sont les suivantes:

- routage des messages SIP de l'équipement d'utilisateur à la fonction I-CSCF ou S-CSCF et inversement;
- maintien des associations de sécurité entre elle-même et l'équipement d'utilisateur et validation des identités publiques authentifiées;
- interaction avec le gestionnaire d'application IPCablecom concernant la gestion de QS;
- prise en charge d'une fonctionnalité permettant à l'équipement d'utilisateur de traverser les dispositifs NAT et de maintenir les liens NAT pour la signalisation SIP;

- production d'identificateurs de corrélation pour la comptabilité et d'événements de comptabilité.

6.3.2 Serveurs STUN et TURN

Un serveur STUN est une entité qui reçoit des demandes STUN et envoie des réponses STUN. Les demandes STUN sont généralement des demandes de lien et servent à déterminer les liens attribués par les dispositifs NAT. L'équipement d'utilisateur envoie une demande de lien au serveur, sur UDP. Le serveur examine le port et l'adresse IP d'origine de la demande et les copie dans la réponse qui est renvoyée à l'équipement d'utilisateur.

Deux serveurs STUN sont employés par le réseau IPCablecom, l'un en tant que composant fonctionnel de la fonction P-CSCF (non illustré sur la Figure 1) et l'autre en tant que serveur STUN autonome:

- le serveur STUN faisant office de composant fonctionnel dans la fonction P-CSCF est utilisé par les équipements d'utilisateur SIP afin de maintenir les liens NAT pour la signalisation. Ces messages STUN peuvent aussi jouer le rôle de messages de maintien en vie, permettant à l'équipement d'utilisateur de déterminer la disponibilité de la fonction P-CSCF et de détecter les réamorçages de dispositif NAT;
- le serveur STUN externe illustré à la Figure 1 sert à déterminer une adresse de média possible parmi d'autres au moyen du protocole STUN.

En plus des serveurs STUN, l'architecture contient aussi un serveur TURN. Celui-ci est une entité qui reçoit des demandes TURN et envoie des réponses TURN. Il est capable de jouer le rôle de relais de données, recevant les données à l'adresse qu'il fournit aux équipements d'utilisateur et les retransmettant aux équipements d'utilisateur. Cette fonctionnalité de relais de données permet aux médias de traverser les dispositifs NAT lorsque les autres techniques de traversée de dispositif NAT sont insuffisantes.

6.3.3 Gestionnaire d'application IPCablecom

Le gestionnaire d'application IPCablecom est chargé de diverses tâches, les plus importantes étant de déterminer les ressources de QS nécessaires pour une session sur la base des descripteurs de session reçus et de gérer les ressources de QS attribuées à une session.

Pour déterminer les ressources de QS pour une session, il faut interpréter le descripteur de session et calculer la largeur de bande nécessaire, déterminer le type de programmation du trafic et remplir les classificateurs de trafic. Il faut aussi déterminer le nombre de flux nécessaires pour la session (voix uniquement ou voix et vidéo) et gérer l'association des flux au niveau de la session.

6.4 Réseau central

6.4.1 Fonction CSCF serveuse (S-CSCF)

Tous les messages SIP en dehors d'un dialogue à destination ou en provenance d'un abonné donné passent par la fonction S-CSCF qui dessert cet abonné. A un haut niveau, la fonction S-CSCF prend en charge les capacités suivantes:

- fonction de serveur d'enregistrement SIP, avec une base de données permettant de lier dynamiquement les identités publiques enregistrées (AOR) à un ensemble d'adresses de contact, d'attribuer des identificateurs GRUU et de stocker les autres paramètres associés à l'enregistrement, par exemple les capacités d'agent d'utilisateur et la ou les adresses de la fonction P-CSCF qui peuvent être utilisées pour atteindre les contacts;
- authentification et autorisation d'utilisateur SIP;
- sélection de service et filtrage;

- routage des messages vers la fonction P-CSCF des équipements d'utilisateur desservis par la fonction S-CSCF;
- routage des messages vers une fonction I-CSCF concernant les identités d'utilisateur publiques non desservies par la fonction S-CSCF;
- routage des messages vers une fonction BGCF concernant les appels destinés au RTPC;
- traitement à l'entrée: traitement des demandes entrantes de lancement de dialogue provenant d'agents d'utilisateur SIP contenus dans des équipements d'utilisateur ou des serveurs d'application desservis par la fonction S-CSCF;
- traitement à la sortie: traitement des messages SIP sortants à destination d'une identité publique desservie par la fonction S-CSCF. Cela comporte la multiplication des messages SIP dans le cas où plusieurs adresses de contact sont enregistrées pour l'identité publique considérée;
- interrogation de bases de données de routage externes (par exemple ENUM) afin de déterminer où il convient d'acheminer l'appel;
- libération de sessions lancée par le réseau;
- production d'événements de comptabilité.

Il peut y avoir plusieurs fonctions S-CSCF dans le réseau central. A un instant donné, un abonnement (et toutes les identités publiques qui lui sont associées) ne peut être géré que par une seule fonction S-CSCF.

Les abonnements sont associés à des fonctions S-CSCF. Les données relatives aux abonnements sont stockées dans un ou plusieurs serveurs d'abonnés résidentiels (HSS). La fonction S-CSCF interagit avec la fonction SLF pour identifier les serveurs HSS permettant d'obtenir les données relatives aux utilisateurs qu'elle dessert. Elle peut aussi interagir avec le serveur HSS pour stocker certains types de données relatives aux utilisateurs qu'elle dessert.

Les identificateurs GRUU sont pris en charge par les points d'extrémité et la fonction S-CSCF. Cela permet aux points d'extrémité de se voir attribuer un identificateur GRUU pendant le processus d'enregistrement et, par là même, de demander un contact spécifique au lieu d'un AOR. C'est important pour diverses fonctionnalités comme le transfert d'appel et les conférences;

6.4.2 Fonction CSCF interrogatrice (I-CSCF)

La fonction I-CSCF:

- interagit avec le serveur HSS pour déterminer le lien entre un abonnement (et les identités publiques associées) et une fonction S-CSCF;
- interroge le serveur HSS pour obtenir la fonction S-CSCF puis achemine les demandes SIP provenant d'un autre opérateur de réseau à la fonction S-CSCF correcte;
- achemine les messages aux serveurs d'application en utilisant les identités de service publiques (PSI, *public service identity*);
- achemine les messages à un élément frontalier concernant l'échange de trafic de VoIP (*VoIP peering*).

6.4.3 Serveur d'abonnés résidentiels (HSS)

Le serveur HSS est chargé de stocker les informations suivantes relatives aux abonnements:

- association entre un abonnement et une fonction S-CSCF;
- informations relatives aux profils d'abonnement (critères de filtrage);
- informations de sécurité concernant les abonnements;
- données transparentes ou opaques destinées à être utilisées par les serveurs d'application.

Le serveur HSS prend en charge le stockage, l'extraction et le traitement d'informations pour les composants du réseau. Il prend en charge les capacités suivantes:

- établissement de session – Le serveur HSS prend en charge les procédures d'établissement de session. Pour ce qui est de l'aboutissement du trafic, il fournit des informations sur la fonction S-CSCF qui est attribuée pour gérer une identité publique;
- sécurité – Le serveur HSS prend en charge divers mécanismes d'authentification en stockant les données relatives à la sécurité et en fournissant ces données lorsque c'est nécessaire pour prendre en charge les procédures de sécurité relatives aux équipements d'utilisateur;
- configuration de service – Le serveur HSS donne accès aux données relatives aux profils de service destinées à être utilisées par la fonction S-CSCF. Il peut aussi stocker des données propres à une application pour le serveur d'application.

6.4.4 Fonction de localisation d'abonnement (SLF)

La fonction SLF donne le nom du serveur HSS contenant les données requises relatives à un abonné donné. Elle est inutile dans un environnement contenant un seul serveur HSS.

6.5 Architecture IPCablecom multimédia

L'architecture IPCablecom multimédia définit une plate-forme IP pour la fourniture de services multimédias avec une certaine QS sur des réseaux d'accès DOCSIS 1.1 (la présente Recommandation utilise un système DOCSIS de version DOCSIS 1.1 ou supérieure). Cette plate-forme s'appuie sur les capacités centrales IPCablecom (par exemple autorisation et contrôle d'admission fondés sur la QS, messages d'événement pour la facturation et autres fonctions d'arrière, et sécurité) pour prendre en charge une grande variété de services IP en plus de la téléphonie. Autrement dit, tandis que le serveur CMS IPCablecom est personnalisé pour la fourniture de services téléphoniques aux particuliers, l'architecture IPCablecom multimédia constitue une plate-forme polyvalente qui permet aux câblo-opérateurs d'offrir divers services multimédias IP nécessitant un traitement de la QS.

L'architecture IPCablecom multimédia définit l'interaction entre un système CMTS, un serveur de politique et un gestionnaire d'application. Le système CMTS, décrit au § 6.2.2, est inclus dans le réseau d'accès. Le gestionnaire d'application est propre à chaque application. L'architecture IPCablecom définit un gestionnaire d'application IPCablecom, qui est décrit au § 6.3.3. Le serveur de politique, décrit ci-après, est un élément unique de l'architecture IPCablecom multimédia qui peut communiquer avec divers gestionnaires d'application.

6.5.1 Serveur de politique

Le serveur de politique joue essentiellement un rôle d'intermédiaire entre le ou les gestionnaires d'application et le ou les systèmes CMTS. Il applique les politiques du réseau aux demandes du gestionnaire d'application et sert de proxy pour les messages transmis entre le gestionnaire d'application et le système CMTS.

6.6 Application

6.6.1 Serveur d'application (AS)

Un serveur d'application (AS, *application server*) fournit des services propres à une application. Il peut avoir une incidence sur une session SIP sur la base des services qu'il prend en charge. Il peut aussi héberger et exécuter des services. Il peut lancer des services ou mettre fin à des services pour le compte d'un utilisateur.

6.6.2 Serveur de présence

Le serveur de présence est un serveur d'application spécialisé. Il coordonne le raccordement des sources d'informations de présence et des parties intéressées.

Le serveur de présence peut obtenir des informations de présence de plusieurs façons, par exemple:

- en utilisant la méthode SIP PUBLISH: la demande PUBLISH est adressée à une identité publique puis transmise par la fonction S-CSCF au serveur de présence conformément aux règles de routage normales;
- en utilisant la méthode SIP SUBSCRIBE: le serveur de présence peut aussi faire office d'observateur, auquel cas il utilise la méthode SIP SUBSCRIBE pour s'abonner aux informations de présence qui sont disponibles ailleurs, par exemple dans un serveur d'enregistrement.

Les informations de présence auxquelles les observateurs sont abonnés sont adressées à une identité publique et fournies par la fonction S-CSCF au serveur de présence. Le serveur de présence gère le dialogue pour chaque abonnement et envoie un message SIP NOTIFY au ou aux observateurs à chaque modification du statut de présence pour lequel l'observateur dispose d'un abonnement et d'une autorisation.

6.7 Interconnexion

6.7.1 Elément frontalier

L'interconnexion avec les réseaux homologues peut être assurée par le biais d'un élément frontalier. Celui-ci contient une fonction de proxy d'interconnexion et peut contenir une fonction de proxy de média.

La fonctionnalité de proxy d'interconnexion prend en charge:

- l'interfonctionnement de protocoles;
- l'application de profils SIP (traduction, adaptation ou normalisation);
- des services liés à la sécurité (par exemple le maintien d'une association de sécurité avec l'homologue);
- la gestion d'adresses IP (réseaux homologues avec le même espace d'adresses IP privées);
- l'interfonctionnement entre les réseaux IPv6 et IPv4;
- les proxys de média relaient les médias entre réseaux homologues.

L'architecture IPCablecom ne définit pas les spécifications fonctionnelles que les éléments frontaliers doivent prendre en charge: il appartient à chaque opérateur de déterminer les besoins concernant un élément frontalier.

6.7.2 Fonction de commande de passerelle d'échappement (BGCF)

La fonction BGCF choisit un réseau aux fins de routage vers le RTPC et, dans son propre réseau, elle détermine le contrôleur MGC qui est utilisé pour le raccordement au RTPC.

6.7.3 Passerelle de réseau téléphonique public commuté (passerelle de RTPC)

La passerelle de RTPC est constituée d'une passerelle de signalisation (SG), d'un contrôleur de passerelle média (MGC) et d'une passerelle média (MG). Les entités SG, MGC et MG sont définies dans des versions précédentes de l'architecture IPCablecom et sont réutilisées dans la présente version de l'architecture IPCablecom, un point de référence IPCablecom étant ajouté au contrôleur MGC. Les entités SG, MGC et MG sont des composants logiques qui peuvent exister sur des plates-formes distinctes ou qui peuvent être combinés ensemble sur une même plate-forme.

La passerelle de signalisation procède à une conversion de signalisation au niveau de la couche Transport entre le transport SS7 et le transport IP utilisé dans le réseau IPCablecom. Elle n'interprète pas la couche Application mais interprète les couches nécessaires au routage des messages de signalisation.

Le contrôleur MGC procède à une conversion de protocole entre les messages ISUP SS7 et les protocoles de commande d'appel IPCablecom et assure la commande de connexion des canaux de média dans la passerelle média.

La passerelle média assure la conversion de canal support entre le réseau à commutation de circuit et les flux de média RTP IP dans le réseau IPCablecom. Elle peut utiliser des codecs, des annuleurs d'écho, etc. selon qu'il est nécessaire pour assurer cette conversion.

6.7.4 Serveur de gestion des appels (CMS)

Un serveur de gestion des appels (CMS) IPCablecom permet de prendre en charge les services de téléphonie destinés aux clients NCS (à savoir les adaptateurs E-MTA). Le serveur CMS assure la plupart des fonctionnalités téléphoniques tout en interagissant directement avec les serveurs d'application (par exemple serveurs de conférence et serveurs de messagerie unifiée) pour fournir des applications supplémentaires aux adaptateurs E-MTA. Il se peut qu'il n'autorise pas une exploitation transparente des fonctionnalités à travers les adaptateurs E-MTA et les équipements d'utilisateur détenus par le même utilisateur.

Le serveur CMS IPCablecom communique avec les fonctions CSCF en tant qu'homologues.

6.8 Systèmes d'appui à l'exploitation

Les serveurs suivants devraient être présents dans le système d'appui à l'exploitation du réseau IPCablecom.

6.8.1 Serveur DHCP

Un serveur DHCP est utilisé lorsque le réseau local des équipements d'utilisateur est sous le contrôle du fournisseur de services. Il fournit des informations de participation au réseau IP (par exemple adresse IP et informations relatives au système DNS). Les équipements d'utilisateur situés dans des environnements qui ne sont pas sous le contrôle du fournisseur de services ne peuvent pas utiliser les services du serveur DHCP du fournisseur de services. En pareils cas, on suppose que l'équipement d'utilisateur reçoit les informations de participation au réseau IP en provenance du réseau local.

6.8.2 Serveur DNS

Un serveur DNS est utilisé pour résoudre les entités DNS (par exemple noms FQDN, enregistrements SRV) en adresses de réseau et inversement. Le service DNS du fournisseur de services devrait être utilisé par les équipements d'utilisateur ainsi que par les composants de réseau, pour la localisation d'entités ou le routage des messages.

6.8.3 Serveur ENUM

Un serveur ENUM est utilisé pour stocker et traduire les numéros E.164 en identificateurs URI SIP ou en enregistrements de serveur de noms (NS) pointant sur le serveur de noms associé à l'opérateur auquel le numéro E.164 considéré est délégué. Plus précisément, un serveur ENUM utilise le système DNS pour identifier le détenteur (fournisseur de services ou utilisateur final) d'un numéro E.164.

6.8.4 Elément d'approvisionnement, d'activation et de configuration (PAC)

L'élément PAC est un composant défini dans l'architecture IPCablecom qui est chargé de l'approvisionnement, de l'activation et de la configuration des équipements d'utilisateur. Il est aussi chargé de tenir à jour les informations de configuration des équipements d'utilisateur. Les données

de configuration contiennent les informations dont un équipement d'utilisateur a besoin pour la fourniture de services. Par ailleurs, l'élément PAC transmet les modifications de configuration d'exécution, du réseau à l'utilisateur ou en sens inverse.

L'élément PAC contient les composants logiques PDS (serveur de fourniture de profil) et XDS (serveur de données XCAP) et implémente les points de référence associés.

- Un serveur PDS est un ensemble logique comportant le notificateur et le serveur chargé de traiter les demandes d'abonnement aux informations de configuration.
- Un serveur XDS est un serveur XCAP qui stocke, modifie et extrait les données entre équipements d'utilisateur et éléments de réseau ou entre éléments de réseau.

6.8.5 Système de gestion d'élément et système de gestion de réseau

Un système de gestion d'élément (EMS, *element management server*) et un système de gestion de réseau (NMS, *network management system*) comportent une ou plusieurs entités associées respectivement à la surveillance et à la gestion d'éléments de réseau particuliers et à la surveillance et à la gestion de la totalité d'un réseau.

Les systèmes EMS ont une fonctionnalité variable et peuvent différer suivant les éléments de réseau, mais ils présentent généralement des interfaces avec les systèmes NMS qui sont chargés de suivre et de maintenir le bon fonctionnement d'un réseau.

Les systèmes EMS et NMS nécessitent des points de référence de gestion pour divers éléments (par exemple, équipements d'utilisateur, élément PAC, serveurs d'application, fonction S-CSCF). L'architecture IPCablecom ne définit les points de référence de surveillance et de gestion que pour les équipements d'utilisateur.

6.8.6 Serveur temporel

Un serveur temporel est utilisé par les équipements d'utilisateur pour obtenir l'heure.

6.8.7 Fonction de données de taxation (CDF)

La fonction de données de taxation (CDF, *charging data function*) reçoit les événements de taxation provenant des divers éléments de réseau IPCablecom via le point de référence Rf défini dans le sous-système IMS. Elle peut ensuite utiliser les informations contenues dans les événements de taxation pour construire les relevés des données d'appel (CDR, *call detail record*).

Certains éléments IPCablecom fournissent des messages d'événement (EM) IPCablecom à un serveur d'archivage (RKS). Celui-ci peut être utilisé pour prendre en charge un serveur CMS, un système CMTS, un contrôleur MGC et un serveur de politique. Toutefois, il n'est pas inclus dans l'architecture de référence.

7 Interfaces de protocole et points de référence

L'architecture IPCablecom2 définit un ensemble d'interfaces de protocole, ou points de référence, dans un certain nombre de domaines. Bon nombre de ces points de référence proviennent directement du sous-système IMS et sont perfectionnés en fonction des besoins. Certains points de référence sont définis dans l'architecture IPCablecom2. Tous ces points de référence sont identifiés au moyen de la convention applicable à leur nommage:

- IMS: deux ou trois lettres (par exemple Gm, ISC);
- points de référence définis dans l'architecture IPCablecom2: pkt-<functional area>-<reference point number>.

On se reportera aux rapports techniques et spécifications applicables pour obtenir une description plus complète et une définition des protocoles.

Il est possible que certains de ces points de référence n'existent pas dans les produits d'un fabricant donné. Par exemple, si plusieurs composants fonctionnels IPCablecom2 sont intégrés, il est possible que certains de ces points de référence soient internes au dispositif intégré.

7.1 Signalisation et commande de service

Les points de référence pour la signalisation et la commande de service IPCablecom2 sont indiqués sur la Figure 4. La plupart des points de référence sont définis dans le sous-système IMS, des modifications appropriées leur étant apportées dans l'architecture IPCablecom, comme cela est précisé dans diverses spécifications IPCablecom. Les points de référence propres à l'architecture IPCablecom sont aussi inclus.

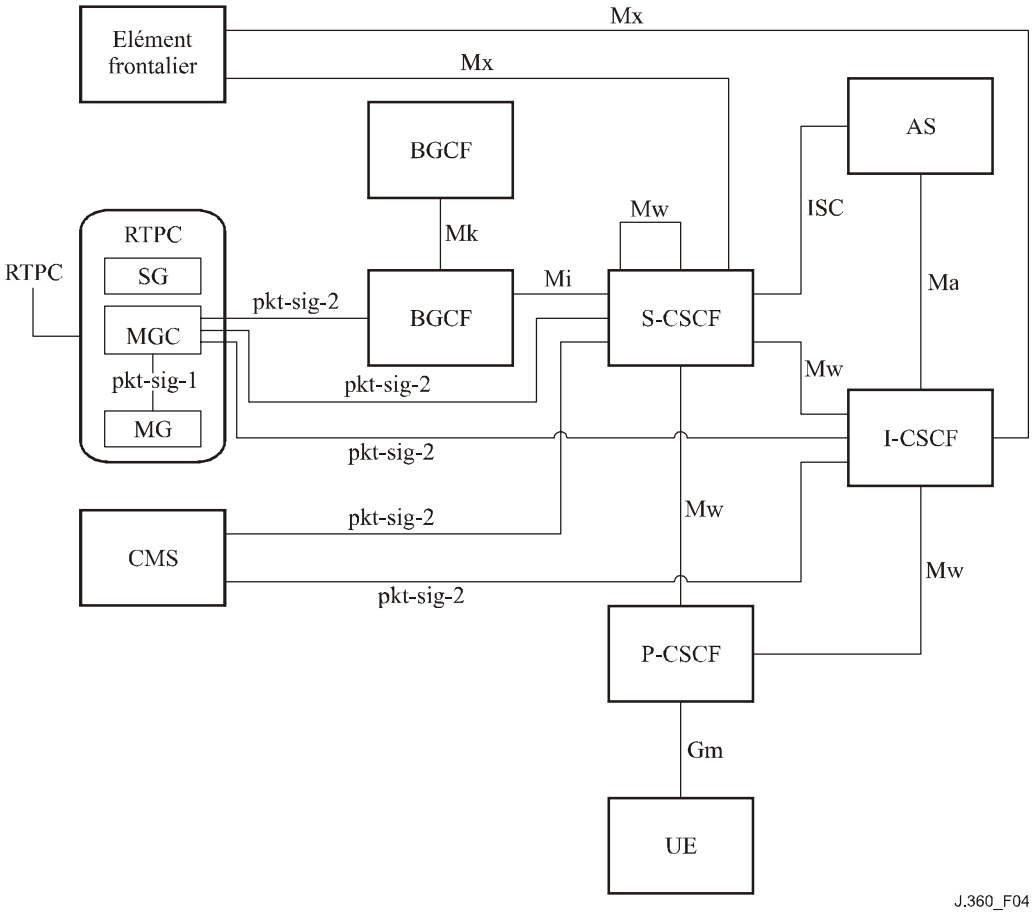


Figure 4 – Points de référence pour la signalisation

Les points de référence indiqués sur la Figure 4 sont décrits dans le Tableau 2. Tous les points de référence sont fondés sur le protocole SIP sauf indication contraire.

Tableau 2 – Description des points de référence pour la signalisation

Point de référence	Eléments de réseau IPCablecom	Description du point de référence
Mx	I-CSCF – élément frontalier S-CSCF – élément frontalier	Permet à une fonction S-CSCF ou I-CSCF de communiquer avec un élément frontalier lors de l'interfonctionnement avec un autre réseau. Par exemple, une session entre le réseau résidentiel et un réseau homologue pourrait faire l'objet d'un routage via une fonction ALG IMS contenue dans l'élément frontalier afin d'assurer l'interfonctionnement entre les réseaux SIP IPv6 et IPv4.
Mi	S-CSCF – BGCF	Permet à la fonction S-CSCF de retransmettre les messages de signalisation de session à la fonction BGCF aux fins d'interfonctionnement avec les RTPC.
Mk	BGCF – BGCF	Permet à une fonction BGCF de retransmettre les messages de signalisation de session à une autre fonction BGCF.
Mw	P-CSCF – I-CSCF P-CSCF – S-CSCF I-CSCF – S-CSCF S-CSCF – S-CSCF	Permet de communiquer et de retransmettre des messages de signalisation entre fonctions CSCF pour permettre l'enregistrement et la commande de session. Permet aussi au serveur CMS d'échanger des messages SIP avec les fonctions S-CSCF et I-CSCF concernant les appels entre adaptateurs E-MTA et équipements d'utilisateur.
Ma	I-CSCF – AS	Permet à la fonction I-CSCF de retransmettre les demandes SIP destinées à une identité de service publique hébergée par un serveur d'application directement au serveur d'application.
ISC	S-CSCF – AS	Permet à une fonction S-CSCF de communiquer avec un serveur d'application en appui à diverses applications.
Gm	UE – P-CSCF	Permet à l'équipement d'utilisateur de communiquer avec la fonction P-CSCF pour l'enregistrement et la commande de session.
pkt-sig-1	MGC – MG	Interface TGCP (protocole de commande de passerelle de jonction), définie dans la spécification du protocole TGCP IPCablecom [UIT-T J.171.1].
pkt-sig-2	CMS – S-CSCF CMS – I-CSCF MGC – BGCF MGC – S-CSCF MGC – I-CSCF	Protocole CMSS tel que défini dans la spécification de la signalisation entre serveurs CMS IPCablecom [UIT-T J.178]. Permet aux adaptateurs E-MTA IPCablecom d'établir des sessions vocales avec les éléments IPCablecom. Permet aussi aux fonctions BGCF, I-CSCF et S-CSCF d'échanger des messages de signalisation de session avec un contrôleur MGC IPCablecom aux fins d'interfonctionnement avec le RTPC.

On trouvera davantage d'informations dans l'aperçu général de signalisation SIP IPCablecom2 (Appendice I).

7.2 Données d'abonné

Les données d'abonné IPCablecom sont stockées dans le serveur HSS situé dans le réseau domestique. Le serveur HSS dessert les fonctions S-CSCF, I-CSCF et divers serveurs d'application y compris le serveur de présence. Le serveur HSS approprié pour un abonné donné peut être localisé en interrogeant la fonction SLF.

La Figure 5 montre les points de référence pour les services relatifs aux données d'abonné.

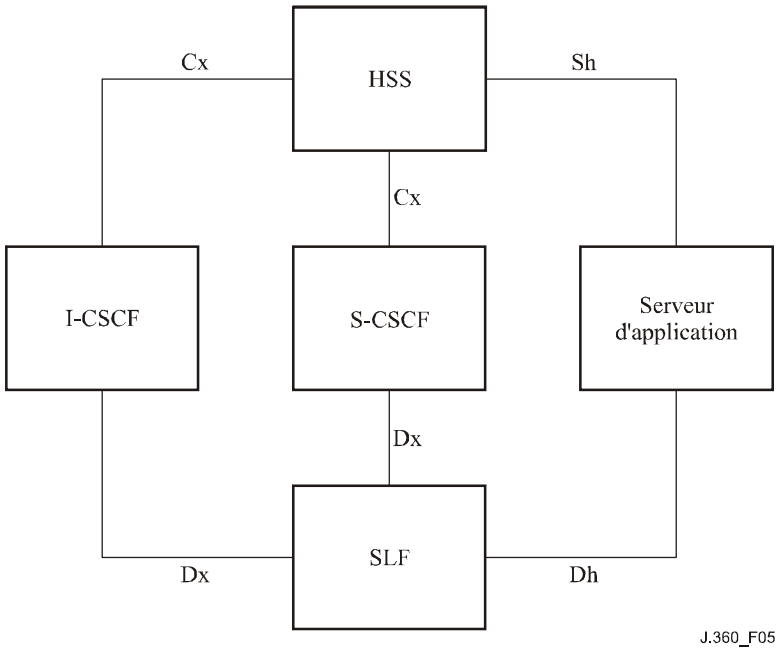


Figure 5 – Points de référence pour les données d'abonné

Les points de référence indiqués sur la Figure 5 sont décrits dans le Tableau 3.

Tableau 3 – Description des points de référence pour les données d'abonné

Point de référence	Eléments de réseau IPCablecom	Description du point de référence
Cx	I-CSCF – HSS S-CSCF – HSS	Permet à des fonctions I-CSCF et S-CSCF d'extraire du serveur HSS des informations relatives au routage, à l'autorisation et à l'authentification, au profil d'abonné et à l'attribution de fonction S-CSCF.
Sh	AS – HSS	Permet à un serveur d'application de communiquer avec le serveur HSS en appui à diverses applications.
Dx	I-CSCF – SLF S-CSCF – SLF	Permet à des fonctions I-CSCF et S-CSCF d'extraire l'adresse du serveur HSS qui héberge les données d'abonnement pour un utilisateur donné. Ce point de référence n'est pas requis dans un environnement contenant un seul serveur HSS.
Dh	AS – SLF	Permet à un serveur d'application d'extraire l'adresse du serveur HSS qui héberge les données d'abonnement pour un utilisateur donné. Ce point de référence n'est pas requis dans un environnement contenant un seul serveur HSS.

On trouvera davantage d'informations dans l'aperçu du serveur HSS IPCablecom (Appendice IV).

7.3 Qualité de service

Dans l'architecture IPCablecom2, l'approche relative à la qualité de service est fondée sur l'architecture IPCablecom multimédia. Dans l'architecture IPCablecom multimédia d'origine, toutes les fonctions du domaine de commande de service étaient regroupées dans une seule entité appelée le gestionnaire d'application (AM, *application manager*), dont il peut y avoir de nombreuses instances. L'architecture IPCablecom2 subdivise ce domaine en différents éléments et définit des points de référence. Aux fins de la fourniture d'une certaine qualité de service, un gestionnaire d'application (AM) sert d'interface entre l'architecture IPCablecom SIP et l'architecture IPCablecom multimédia. Il a pour fonction de recevoir les messages de QS provenant de la fonction P-CSCF et d'élaborer des messages appropriés destinés au serveur de politique IPCablecom multimédia. Cette fonction de gestion d'application peut être intégrée dans un serveur de politique IPCablecom multimédia, mais elle devrait être considérée comme une fonction distincte étant donné qu'elle est associée à des exigences uniques distinctes de celles qui sont associées au serveur de politique (par exemple la transformation d'une même demande de QS fondée sur une session en une série de différentes demandes de QS pour chaque flux IP). La version IPCablecom du gestionnaire d'application est le gestionnaire d'application IPCablecom (PAM).

La Figure 6 illustre la relation entre le gestionnaire d'application, la fonction P-CSCF et le serveur de politique IPCablecom multimédia. Il est également à noter que le gestionnaire d'application indiqué ici comme une fonction distincte peut être regroupé avec un serveur de politique IPCablecom multimédia ou avec une fonction P-CSCF.

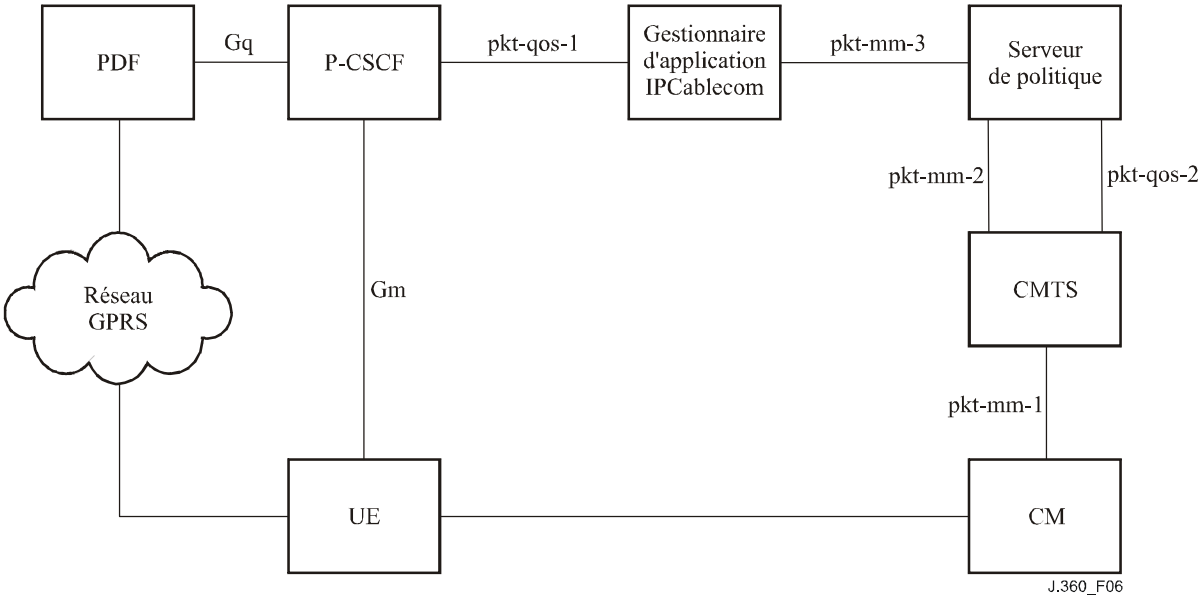


Figure 6 – Points de référence pour la QS

Comme indiqué sur la Figure 6, la fonction de gestion d'application assure le mappage entre les exigences de QS pour la session ou le dialogue indiquées par la signalisation SIP et l'état en termes de QS de chacun des flux de service IP associés dans le réseau d'accès câblé.

Les points de référence indiqués sur la Figure 6 sont décrits dans le Tableau 4.

Tableau 4 – Description des points de référence pour la QS

Point de référence	Eléments de réseau IPCablecom	Description du point de référence
Gm	UE – P-CSCF	Voir le Tableau 2.
pkt-qos-1	P-CSCF – gestionnaire d'application	Il s'agit de l'interface de service web IPCablecom multimédia, qui permet à la fonction P-CSCF d'adresser des demandes de service liées à une certaine QS au gestionnaire d'application, lequel convertit ces demandes de service en demandes de politique via le point de référence pkt-mm-3. Les demandes de service liées à une certaine QS sont déduites, par la fonction P-CSCF, des messages SIP contenant des descriptions de session appropriées. Ce point de référence est défini dans la spécification de l'interface de gestion d'application IPCablecom [UIT-T J.365].
pkt-qos-2	Serveur de politique – CMTS	Le serveur de politique utilise le protocole de découverte de point de commande [UIT-T J.362] pour déterminer le système CMTS de desserte dans le réseau pour un équipement d'utilisateur donné.
pkt-mm-1	CM – CMTS	Le système CMTS charge le câblo-modem d'établir, de libérer ou de modifier un flux de service DOCSIS par le biais de la signalisation DSx. Ce point de référence est défini dans la spécification IPCablecom multimédia [UIT-T J.179 App.I].
pkt-mm-2	Serveur de politique – CMTS	Le serveur de politique pousse les décisions de politique dans le système CMTS, lequel fournit des réponses. Ce point de référence est défini dans la spécification IPCablecom multimédia [UIT-T J.179 App.I].
pkt-mm-3	Gestionnaire d'application – serveur de politique	Permet au gestionnaire d'application de demander au serveur de politique de pousser les décisions de politique dans le système CMTS. Ce point de référence est défini dans la spécification IPCablecom multimédia [UIT-T J.179 App.I].

On trouvera davantage d'informations dans l'aperçu de la qualité de service IPCablecom2 (Appendice II).

7.4 Traversée de traducteur d'adresse réseau (NAT) et de pare-feu

Les traductions d'adresse réseau (NAT) traitent les informations d'adresse et de port figurant dans l'en-tête IP et de transport, ce qui crée des difficultés aux équipements d'utilisateur lorsqu'ils communiquent sur la base du protocole SIP:

- l'équipement d'utilisateur annonce les adresses requises pour les communications de média en utilisant la signalisation SIP (protocole SDP). Toutefois, il se peut que l'adresse locale mise à la disposition d'un équipement d'utilisateur situé derrière un dispositif NAT ne soit pas atteignable par les autres équipements d'utilisateur et par les éléments de réseau;
- les dispositifs NAT/pare-feu contiennent des règles qui peuvent varier selon les modalités de traversée de pare-feu et de création des liens NAT (mappage/filtrage indépendant de l'adresse, mappage/filtrage dépendant de l'adresse ou mappage/filtrage dépendant de l'adresse et du port);
- une fois la communication établie, le dispositif NAT/pare-feu conserve l'état (micro-ouvertures de pare-feu et liens NAT) sur la base de temporisations. Si la temporisation expire, les micro-ouvertures sont fermées et les liens NAT sont supprimés. Des mécanismes doivent être mis en œuvre afin de maintenir les liens NAT et de garder les micro-ouvertures ouvertes à la fois pour la signalisation et pour les médias.

La solution de traversée de dispositif NAT/pare-feu a pour objectif de fournir un mécanisme permettant à un équipement d'utilisateur:

- d'obtenir et d'annoncer (par exemple via le protocole SDP) une adresse atteignable. Dans les cas où plusieurs adresses atteignables sont possibles, il convient de retenir la "meilleure";
- de pouvoir ouvrir des micro-ouvertures et maintenir des liens NAT à la fois pour les médias et pour la signalisation.

L'architecture IPCablecom2 utilise la méthode ICE pour obtenir et annoncer la "meilleure" adresse atteignable et respecter les objectifs nominaux. Cette méthode utilise les serveurs STUN et TURN pour obtenir les adresses possibles. Ces adresses possibles sont ensuite annoncées par l'équipement d'utilisateur au moyen des attributs SDP décrits la méthode ICE. L'équipement d'utilisateur utilise ensuite le serveur STUN pour réaliser des tests d'atteignabilité, ce qui lui permet de prendre la meilleure adresse qui utilise le moins de ressources de réseau et entraîne le moins de retard dans le réseau tout en conservant l'état dans l'équipement d'utilisateur (et non dans le réseau). Cela permet aussi d'assurer l'interfonctionnement avec les adaptateurs E-MTA, étant donné que l'adresse annoncée par les lignes de média ou de connexion du protocole SDP sera toujours une adresse atteignable.

L'aperçu de la traversée de dispositif NAT et de pare-feu IPCablecom2 (Appendice V) contient des détails supplémentaires sur la méthode ICE et décrit en particulier comment les équipements d'utilisateur localisent les serveurs STUN et TURN. Il décrit également comment les liens NAT sont ouverts et maintenus.

Il est à noter que l'un des objectifs nominaux est de mettre en œuvre un mécanisme de traversée de dispositif NAT et de pare-feu qui fonctionne indépendamment de l'endroit où les dispositifs NAT sont situés et indépendamment de la question de savoir s'ils sont imbriqués ou non. Toutefois, ce ne sera peut-être pas possible dans tous les cas.

La Figure 7 montre les points de référence pour la traversée de dispositif NAT/pare-feu.

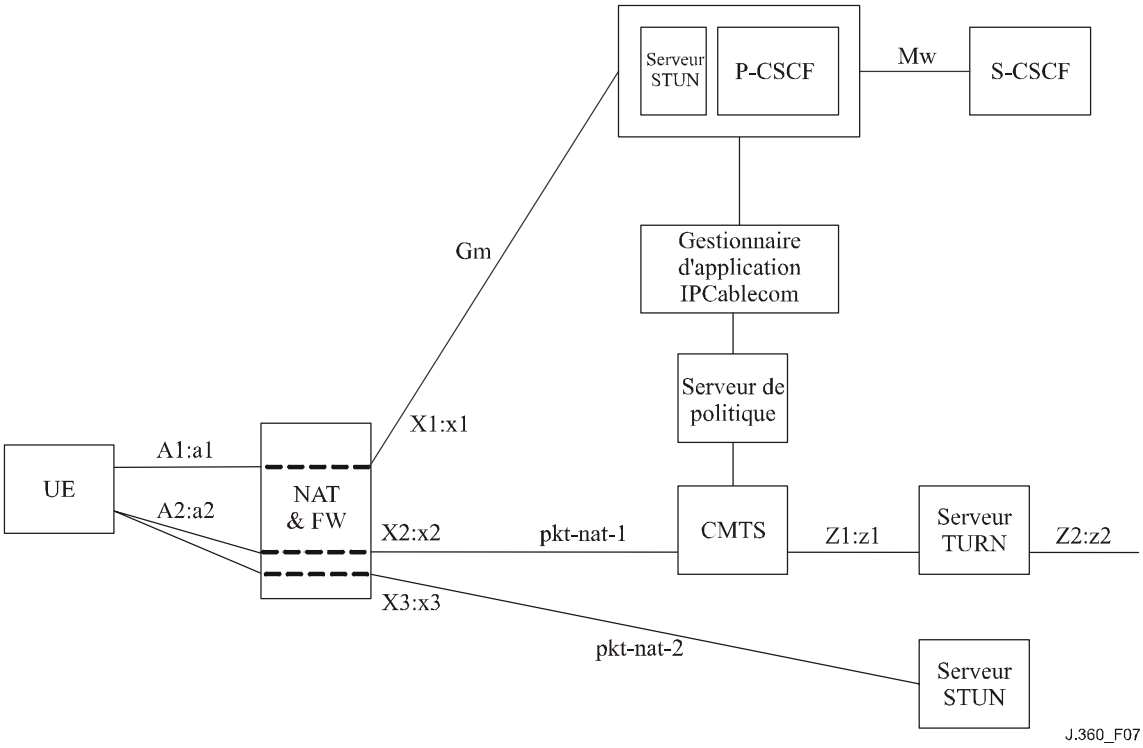


Figure 7 – Points de référence pour la traversée de dispositifs NAT et FW

Les points de référence indiqués sur la Figure 7 sont décrits dans le Tableau 5.

Tableau 5 – Description des points de référence pour la traversée de dispositifs NAT et FW

Point de référence	Eléments de réseau IPCablecom	Description du point de référence
Gm	UE – P-CSCF	Voir le Tableau 2.
Mw	P-CSCF – S-CSCF	Voir le Tableau 2.
pkt-nat-1	UE – serveur TURN	Permet à l'équipement d'utilisateur d'accéder à un serveur TURN afin de prendre en charge la traversée du dispositif NAT qui n'exécute pas de transposition indépendante de l'adresse.
pkt-nat-2	UE – serveur STUN externe	Permet à l'équipement d'utilisateur de déterminer une adresse de média parmi plusieurs adresses possibles au moyen du serveur STUN, dans le cadre de la méthode ICE.

On trouvera davantage d'informations dans l'aperçu de la traversée de dispositif NAT et de pare-feu IPCablecom (Appendice V).

7.5 Codage et transport des médias

L'architecture IPCablecom2 utilise le protocole RTP pour transporter la plupart des services de communication (essentiellement les services vocaux et vidéo).

Les principaux flux de média dans l'architecture IPCablecom2 sont indiqués sur la Figure 8.

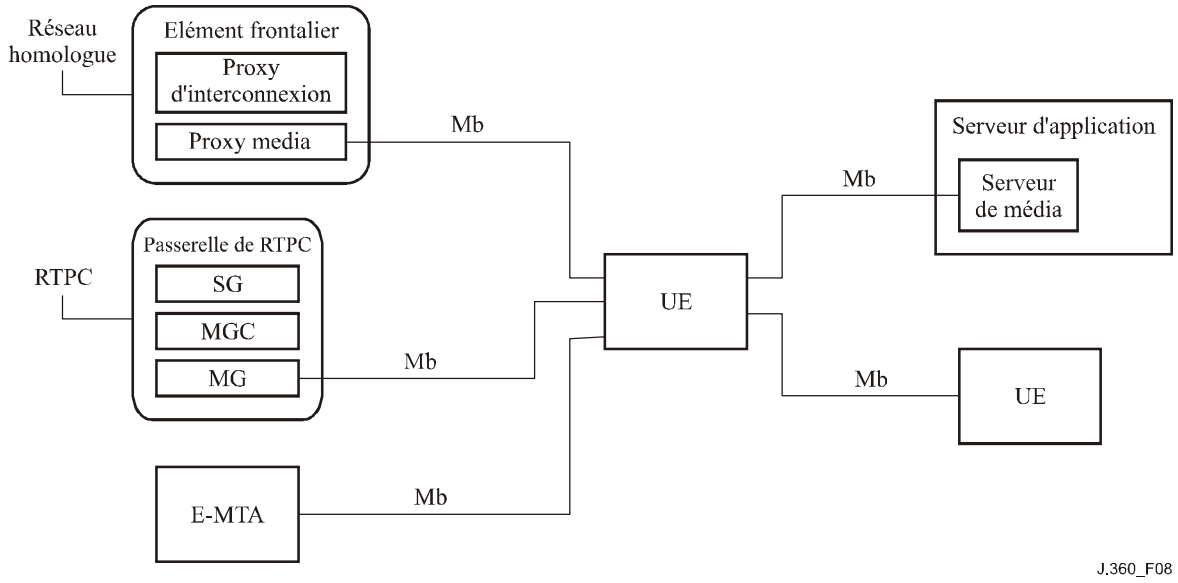


Figure 8 – Points de référence pour les flux de média

Les points de référence indiqués sur la Figure 8 sont décrits dans le Tableau 6.

Tableau 6 – Description des points de référence pour les flux de média

Point de référence	Eléments de réseau IPCablecom	Description du point de référence
Mb	UE – UE UE – MG UE – élément frontalier UE – AS UE – E-MTA	Permet aux composants dotés de capacités de média d'envoyer et de recevoir des paquets de données de média. Plus précisément, un équipement d'utilisateur peut échanger des médias avec un autre équipement d'utilisateur, une passerelle de média, un serveur d'application, un élément frontalier et un adaptateur E-MTA.

Les médias qui passent par le point de référence Mb peuvent être du trafic audio codé par des codecs audio à bande étroite ou à large bande, du trafic vidéo codé par des codecs vidéo ou une combinaison de ces deux types de trafic. Il peut aussi s'agir de données transmises dans le cadre d'un relais de télécopie, d'un relais de modem ou d'un relais DTMF.

Le protocole RTCP permet de surveiller la qualité audio aux points de référence Mb. Les paramètres relatifs aux flux vidéo ne sont pas spécifiés.

On trouvera davantage d'informations dans la spécification des codecs audio/vidéo IPCablecom [UIT-T J.361].

7.6 Approvisionnement, activation, configuration et gestion

L'architecture IPCablecom2 définit un cadre d'approvisionnement, d'activation, de configuration et de gestion (PACM) en appui aux processus réalisés dans le réseau central. Ce cadre inclut des éléments normalisés (par exemple DHCP), des protocoles (par exemple XCAP) et des éléments de réseau propres à l'architecture IPCablecom (par exemple PAC).

En outre, le cadre PACM est subdivisé en domaines et sous-domaines, indiqués ci-après:

- approvisionnement;
- participation au réseau IP (connectivité avec le réseau local);
- identification du fournisseur de services;
- flux d'approvisionnement;
- prise en charge de modèles propriétaires (c'est-à-dire liés à un opérateur particulier) et de modèles non propriétaires (c'est-à-dire utilisables quel que soit l'opérateur);
- cadre d'activation, de configuration et de gestion d'équipement d'utilisateur;
- équipement d'utilisateur, abonné et activation de service;
- cadre de configuration et de gestion d'équipement d'utilisateur;
- modèle de données;
- protocoles de transport.

La Figure 9 montre les points de référence pour l'élément PACM.

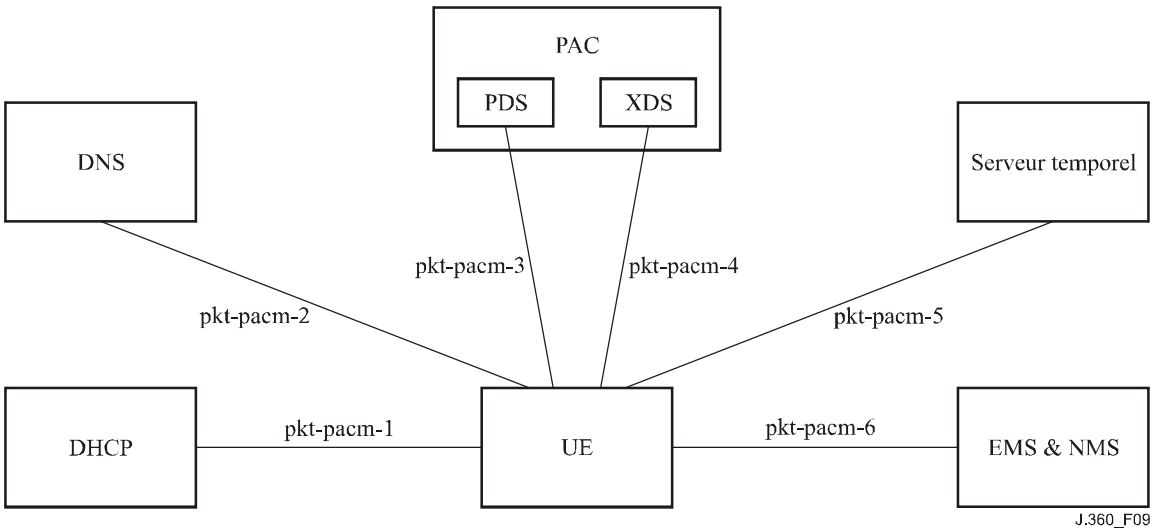


Figure 9 – Points de référence pour l'élément PACM

Les points de référence indiqués sur la Figure 9 sont décrits dans le Tableau 7.

Tableau 7 – Description des points de référence pour l'élément PACM

Point de référence	Eléments de réseau IPCablecom	Description du point de référence
pkt-pacm-1	UE – DHCP	Fournit des informations sur la participation au réseau (par exemple adresse IP, adresses de serveur DNS). Ce point de référence peut être pris en charge par le réseau local ou par un réseau d'accès non exploité par le fournisseur de services IPCablecom.
pkt-pacm-2	UE – DNS	Permet à l'équipement d'utilisateur de résoudre les noms DNS pour localiser les éléments de réseau ou acheminer les messages.
pkt-pacm-3	UE – PDS	Grâce à l'utilisation du protocole SIP, ce point de référence permet aux équipements d'utilisateur de s'abonner aux données d'état relatives à la configuration et aux fonctionnalités. Il s'agit d'un point de référence générique qui décrit l'interaction entre l'équipement d'utilisateur et le serveur XDS. Toutefois, en réalité, le serveur PDS interagit avec le reste des composants SIP en tant que serveur d'application. Les messages SIP PACM traverseront donc les interfaces Gm, Ma, Mw et ISC. NOTE 1 – Le serveur PDS décrit ici est utilisé tout particulièrement pour l'élément PACM. Toutefois, en tant que composant logique, il peut être défini pour être utilisé également dans d'autres applications.
pkt-pacm-4	UE – XDS	Ce point de référence est utilisé pour distribuer et gérer les données relatives à la configuration et aux fonctionnalités. NOTE 2 – Le serveur XDS décrit ici est utilisé tout particulièrement pour l'élément PACM. Toutefois, en tant que composant logique, il peut être défini pour être utilisé également dans d'autres applications.

Tableau 7 – Description des points de référence pour l'élément PACM

Point de référence	Eléments de réseau IPCablecom	Description du point de référence
pkt-pacm-5	UE – serveur temporel	Permet aux équipements d'utilisateur d'obtenir l'heure.
pkt-pacm-6	UE – EMS & NMS	Permet aux systèmes EMS et NMS se surveiller et de gérer les équipements d'utilisateur.

On trouvera davantage d'informations dans la spécification de l'approvisionnement, de l'activation, de la configuration et de la gestion IPCablecom2 [UIT-T J.364].

7.7 Comptabilité et utilisation du réseau

Le sous-système IMS définit des points de référence qui lui permettent de prendre en charge différents types de réseaux d'accès avec connectivité IMS. Dans le cadre de la comptabilité IPCablecom2, on suppose que le réseau d'accès HFC câblé et le sous-système IPCablecom multimédia définissent un nouveau type de réseau d'accès avec connectivité IP (IP-CAN) à incorporer dans l'architecture d'ensemble du sous-système IMS.

La Figure 10 montre les principaux composants IPCablecom concernés par la taxation différée et les points de référence entre tous ces composants.

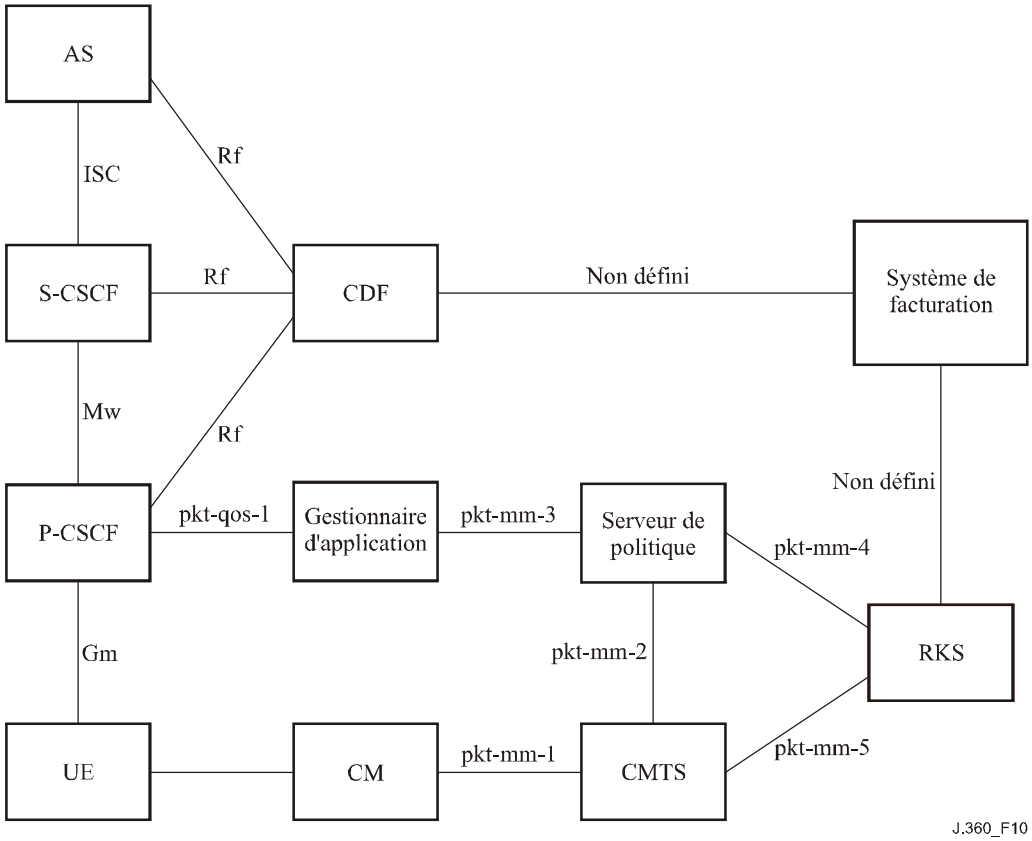


Figure 10 – Points de référence pour la comptabilité

Les points de référence indiqués sur la Figure 10 sont décrits dans le Tableau 8.

Tableau 8 – Description des points de référence pour la comptabilité

Point de référence	Eléments de réseau IPCablecom	Description du point de référence
Gm	UE – P-CSCF	Voir le Tableau 2.
Mw	P-CSCF – S-CSCF	Voir le Tableau 2.
ISC	S-CSCF – AS	Voir le Tableau 2.
Rf	CSCF – CDF	Point de référence fondé sur le protocole DIAMETER entre les nœuds IMS (fonction P-CSCF, fonction S-CSCF et serveur d'application) et la fonction de données de taxation (CDF).
pkt-qos-1	P-CSCF – gestionnaire d'application	Voir le Tableau 4.
pkt-mm-1	CM – CMTS	Voir le Tableau 4.
pkt-mm-2	Serveur de politique – CMTS	Voir le Tableau 4.
pkt-mm-3	Gestionnaire d'application – serveur de politique	Voir le Tableau 4.
pkt-mm-4	Serveur de politique – RKS	Point de référence fondé sur le protocole RADIUS entre le serveur de politique et le serveur d'archivage (RKS). Il est défini dans la spécification IPCablecom multimédia [UIT-T J.179 App.I].
pkt-mm-5	CMTS – RKS	Point de référence fondé sur le protocole RADIUS entre le système CMTS et le serveur RKS. Il est défini dans la spécification IPCablecom multimédia [UIT-T J.179 App.I].

On trouvera davantage d'informations dans la spécification de la comptabilité IPCablecom [UIT-T J.363].

7.8 Sécurité

Dans l'architecture de sécurité IPCablecom2, on décrit les points de référence pour la sécurité présents dans toute l'architecture. Pour l'organisation de ces points de référence, trois domaines de confiance différents ont été définis.

- Domaine intraréseau – Les points de référence présents dans ce domaine permettent de raccorder les éléments de réseau situés dans un domaine de fournisseur de services.
- Domaine interréseaux – Les points de référence présents dans ce domaine permettent de raccorder deux domaines. Les domaines peuvent être rattachés à des fournisseurs de services différents ou au même fournisseur.
- Domaine d'accès – Les points de référence présents dans ce domaine permettent aux équipements d'utilisateur de se raccorder à un fournisseur de services.

Ces domaines de confiance sont utilisés pour décomposer l'architecture IPCablecom.

On trouvera davantage d'informations dans l'aperçu de la sécurité IPCablecom2 (Appendice III).

7.8.1 Sécurité dans le domaine d'accès

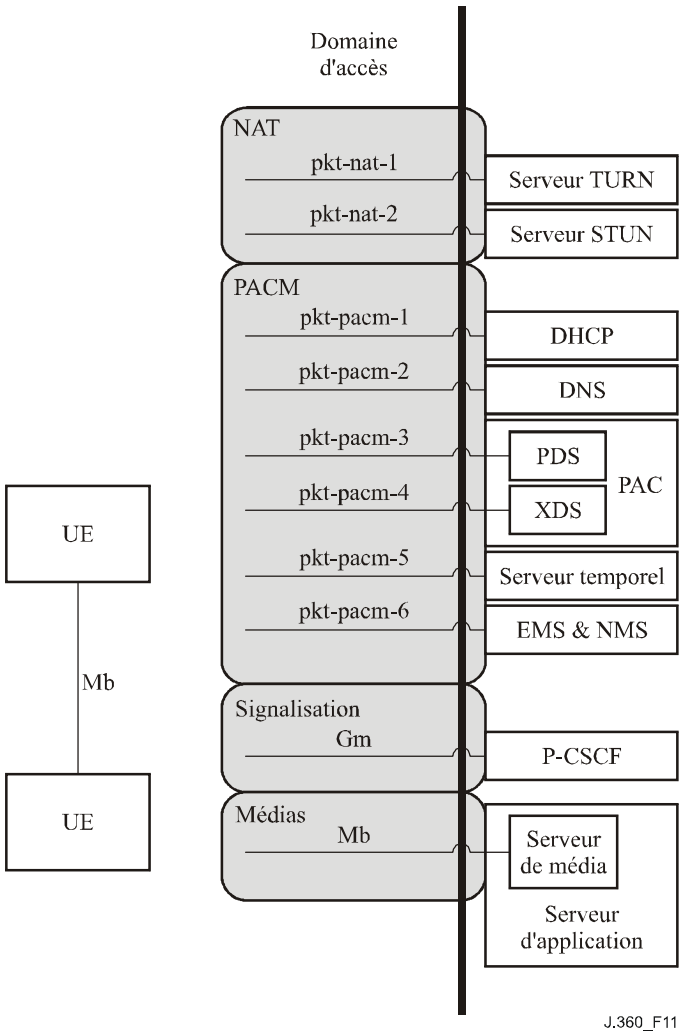


Figure 11 – Points de référence situés dans le domaine d'accès

Les interactions entre les équipements d'utilisateur et le réseau se produisent dans le domaine d'accès. Dans ce domaine, diverses méthodes sont employées (par exemple DOCSIS et accès sans fil). Ces caractéristiques font que le domaine d'accès est le siège d'une multitude de menaces, comme décrit dans l'Appendice III. Le Tableau 9 donne un aperçu de haut niveau de la manière dont les points de référence situés dans le domaine d'accès sont sécurisés.

Tableau 9 – Description des points de référence situés dans le domaine d'accès

Point de référence	Eléments de réseau IPCablecom	Description du point de référence
pkt-nat-1	UE – serveur TURN	TURN: les demandes TURN sont authentifiées et autorisées dans le cadre du protocole TURN proprement dit.
pkt-nat-2	UE – serveur STUN externe	STUN: l'intégrité des messages est assurée par des mécanismes STUN.
pkt-pacm-1	UE – serveur DHCP	DHCP: l'architecture IPCablecom ne comporte pas de définition relative à la sécurité concernant le protocole DHCP.
pkt-pacm-2	UE – serveur DNS	DNS: l'architecture IPCablecom ne comporte pas de définition relative à la sécurité concernant le protocole DNS.
pkt-pacm-3	UE – serveur PDS	SIP: intégrité et confidentialité des messages via IPSec (sécurité IP) ou TLS (sécurité de la couche transport).
pkt-pacm-4	UE – serveur XDS	XCAP: intégrité et confidentialité des messages via HTTP sur TLS
pkt-pacm-5	UE – serveur temporel	SNTP: l'architecture IPCablecom ne comporte pas de définition relative à la sécurité pour le protocole SNTP.
pkt-pacm-6	UE – serveur EMS&NMS	La sécurité au niveau de l'interface de gestion sort du cadre de la présente spécification.
Gm	UE – P-CSCF	SIP: intégrité et confidentialité des messages via IPSec ou TLS. STUN: l'intégrité des messages est assurée par des mécanismes STUN.
Mb	UE – UE UE – MG UE – élément frontalier UE – AS UE – E-MTA	RTP: la sécurité des médias sort du cadre de la présente spécification. NOTE – La Figure 11 ne montre que quelques flux de médias représentatifs.

7.8.2 Sécurité dans le domaine intraréseau

Les points de référence et composants situés dans le domaine intraréseau sont contenus dans un réseau de fournisseur de services et, par conséquent, appliquent une politique de sécurité intrinsèque. Ces points de référence sont généralement sécurisés au moyen du point de référence Zb. Celui-ci utilise la charge utile de sécurité encapsulante (ESP, *encapsulating security payload*) IPSec. Les points de référence Zb qui prennent en charge le protocole TCP peuvent aussi utiliser le protocole TLS.

Les points de référence suivants situés dans le domaine intraréseau définissent des exigences de sécurité additionnelles à appliquer éventuellement en plus ou à la place du point de référence Zb:

- pkt-qos-2 – Mécanisme d'identification cryptographique défini dans le cadre du protocole de découverte de point de commande.
- pkt-laes-4 – Mécanismes cryptographiques définis dans le cadre du protocole SNMPv3.
- pkt-laes-6 – Mécanisme d'identification cryptographique défini dans le cadre du protocole de découverte de point de commande.

7.8.3 Sécurité dans le domaine interréseaux

Les points de référence situés dans le domaine interréseaux sont les suivants:

- élément frontalier – réseau homologue – sécurisation fondée sur le point de référence Za, qui utilise la charge utile ESP IPsec. Le trafic interdomaines dans le sous-système IMS doit obligatoirement passer par une passerelle de sécurité. Celle-ci prend en charge le point de référence Za et applique une politique de sécurité aux flux de trafic interdomaines. On suppose que l'élément frontalier comporte la fonctionnalité de passerelle de sécurité, mais la passerelle de sécurité peut être un élément à part entière.
- Passerelle RTPC – RTPC – la sécurité au niveau de ce point de référence n'est pas définie.
- CMS – points d'extrémité – la sécurité au niveau de ce point de référence est définie dans la spécification de la sécurité IPCablecom [UIT-T J.170].

7.9 Interception licite

L'architecture d'interception licite IPCablecom2 est représentée sur la Figure 12. Les éléments de commande d'appel IPCablecom (par exemple les fonctions CSCF) forment l'ensemble des points d'accès potentiels pour l'interception des données relatives aux appels. Les éléments de plan support IPCablecom (par exemple le système CMTS et la passerelle de média) forment l'ensemble des points d'accès potentiels pour l'interception du contenu des appels. La fonction de fourniture (DF) reçoit les événements liés aux appels interceptés et le contenu des appels en provenance des points d'accès pour l'interception IPCablecom, les corrèle avec un service d'abonné donné puis fournit le résultat à la fonction de collecte (CF) de l'agence d'application de la loi par le biais d'un point de référence normalisé défini dans le document [ES-DCI]. Il est à noter que la fonction de fourniture ne fait pas partie de l'architecture IPCablecom, même si l'architecture IPCablecom spécifie des points de référence pour la fonction de fourniture nécessaires pour l'interception licite dans les réseaux IPCablecom. Les éléments de commande d'appel comme les fonctions S-CSCF et P-CSCF attribuées à un abonné donné communiquent à la fonction de fourniture les événements liés aux appels. En outre, ces éléments de commande configurent dynamiquement des éléments homologues pour l'interception pendant des réacheminements d'appel ou pendant des scénarios de commande d'appel par un tiers. Les éléments frontaliers (par exemple la fonction BGCF, la fonction I-CSCF et le contrôleur MGC) communiquent à la fonction de fourniture les informations relatives aux opérateurs d'interconnexion. Pour configurer les points d'accès pour l'interception du contenu des appels, la fonction de fourniture commence par découvrir les points d'accès en utilisant le protocole de découverte de point de commande puis en configurant l'interception au niveau des points d'accès au contenu en utilisant le protocole SNMPv3. Le processus d'approvisionnement relatif au contenu des appels est lancé la première fois que la fonction de fourniture reçoit un événement de lancement d'appel en provenance des éléments de commande d'appel.

Le serveur CMS IPCablecom est mis à niveau afin d'interfonctionner avec les éléments IPCablecom pour prendre en charge l'interception des appels passant par des composants NCS et SIP. Les éléments MGC et MG IPCablecom peuvent facultativement être mis à niveau pour les points de référence IPCablecom indiqués sur la Figure 12.

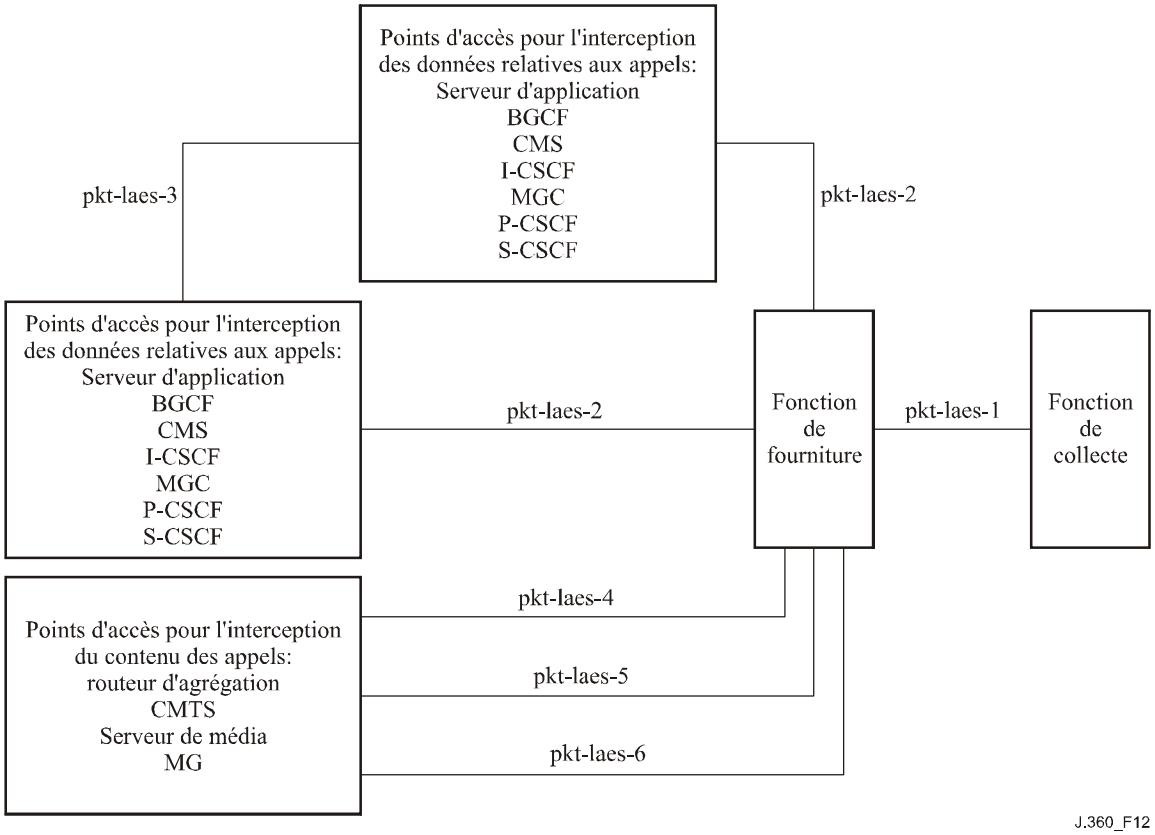


Figure 12 – Points de référence pour l'interception licite

Les points de référence indiqués sur la Figure 12 sont décrits dans le Tableau 10.

Tableau 10 – Description des points de référence pour l'interception licite

Point de référence	Eléments de réseau IPCablecom	Description du point de référence
pkt-laes-1	DF – CF	Les données relatives aux appels et le contenu des appels corrélés sont communiqués à la fonction de collecte de l'agence d'application de la loi. Définition dans le document [ES-DCI].
pkt-laes-2	Elément de commande de session – DF	Les événements liés aux appels interceptés sont communiqués à la fonction de fourniture. Ce point de référence est fondé sur le protocole DIAMETER.
pkt-laes-3	Elément de commande de session – élément de commande de session	Permet aux éléments de commande de session de configurer dynamiquement l'interception dans les éléments homologues pour les appels pour lesquels les éléments de commande attribués à l'abonné considéré ne sont plus impliqués dans l'appel. Le réacheminement d'appel est un exemple. Ce point de référence est fondé sur le protocole SIP.
pkt-laes-4	DF vers points d'accès au contenu	La fonction de fourniture configure dynamiquement les points destinés à l'interception du contenu. Ce point de référence est fondé sur le protocole SNMPv3.

Tableau 10 – Description des points de référence pour l'interception licite

Point de référence	Eléments de réseau IPCablecom	Description du point de référence
pkt-laes-5	Point d'accès au contenu vers DF	Le contenu des appels interceptés est communiqué à la fonction de fourniture. Ce point de référence est fondé sur les médias sur UDP.
pkt-laes-6	DF vers points d'accès au contenu	La fonction de fourniture, en tant que demandeur, utilise le protocole de découverte de point de commande [UIT-T J.362] pour déterminer les points d'accès appropriés dans le réseau pour l'interception du contenu des appels, ces points d'accès jouant le rôle de points de commande.

On trouvera davantage d'informations dans la spécification des fonctions intraréseau pour la surveillance électronique IPCablecom [ES-INF] et dans la spécification de l'interface entre la fonction de fourniture et la fonction de collecte pour la surveillance électronique IPCablecom [ES-DCI].

7.10 Découverte de point de commande

Au niveau du point de référence pour la découverte de point de commande, indiqué sur la Figure 13 ci-dessous, est défini un protocole fondé sur le réseau qui peut être utilisé pour trouver l'adresse IP nécessaire pour l'envoi de demandes de QS ainsi que pour l'extraction de contenu aux fins de l'interception licite.

En ce qui concerne les demandes de QS, on utilise ce point pour trouver l'adresse IP du système CMTS pour l'architecture DQoS et l'architecture IPCablecom multimédia (PCMM). En ce qui concerne l'interception licite, on l'utilise pour découvrir l'adresse IP à utiliser pour extraire le contenu au niveau du système CMTS ainsi qu'au niveau des passerelles de média et des routeurs/commutateurs d'agrégation situés avant les points d'extrémité de média. Outre la fourniture de l'adresse IP, la réponse indique le protocole à utiliser et peut aussi indiquer le sous-réseau dans lequel l'adresse de destination demandée figure.

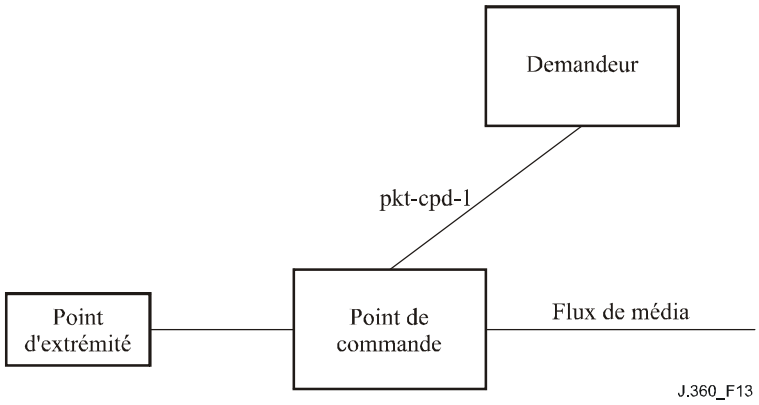


Figure 13 – Point de référence pour la découverte de point de commande

Les points de référence indiqués sur la Figure 13 sont décrits dans le Tableau 11.

Tableau 11 – Description des points de références pour la découverte de point de commande

Point de référence	Eléments de réseau IPCablecom	Description du point de référence
pkt-cpd-1	Demandeur – point de commande	Le demandeur utilise le protocole de découverte de point de commande pour déterminer le point de commande approprié dans le réseau pour un équipement d'utilisateur donné. Les autres points de référence de l'architecture sont fondés sur ce point de référence.

On trouvera davantage d'informations dans la spécification de la découverte de point de commande IPCablecom2 [UIT-T J.362].

Appendice I

Aperçu de la signalisation SIP

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

I.1 Introduction et objet

Le présent appendice contient un aperçu de l'architecture de signalisation SIP et décrit les exigences de haut niveau permettant de prendre en charge des communications SIP dans l'architecture IPCablecom2.

Il vise essentiellement à définir comment les éléments fonctionnels IPCablecom2 participant à une signalisation de session communiquent sur la base du protocole SIP IETF et de ses extensions, et à spécifier les perfectionnements apportés au sous-système IMS 3GPP.

Etant donné qu'une harmonisation étroite est assurée entre la signalisation SIP IPCablecom2 et le sous-système IMS, les exigences normatives applicables à la signalisation SIP IPCablecom2 sont définies dans des spécifications delta relatives au sous-système IMS, qui sont des spécifications 3GPP perfectionnées afin de tenir compte des besoins propres au secteur du câble. Ces exigences font l'objet de trois spécifications delta relatives au sous-système IMS: Recommandations UIT-T J.366.2, J.366.3 et J.366.4.

I.1.1 Relation avec les fonctionnalités et services IPCablecom

Le présent appendice et les spécifications delta relatives au sous-système IMS qui lui sont associées définissent la signalisation SIP de base destinée à être utilisée pour prendre en charge une grande variété de services de communication IP, allant des fonctionnalités de téléphonie existantes aux applications et services de communication nouveaux et perfectionnés. Cette signalisation SIP de base est indépendante du service. Il s'ensuit que les exigences propres à chaque service ou fonctionnalité IPCablecom sortent du cadre du présent appendice et sont définies séparément. La relation entre le présent appendice, les spécifications delta relatives au sous-système IMS concernant la signalisation SIP de base et les fonctionnalités et services IPCablecom est illustrée sur la Figure I.1.

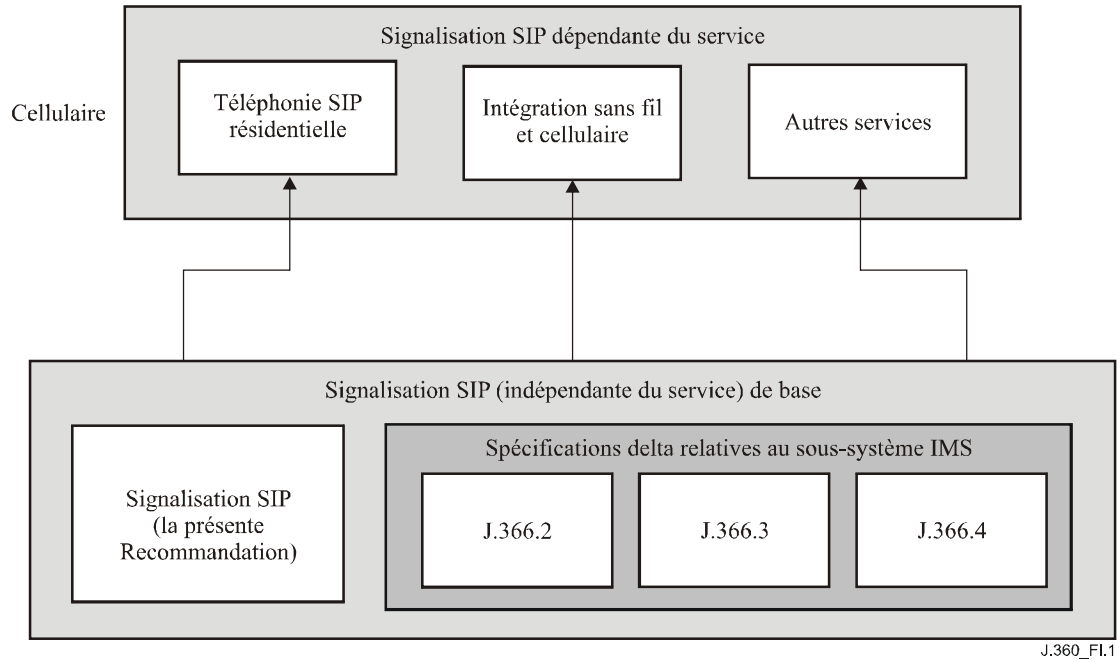


Figure I.1 – Relation entre la signalisation SIP de base et les services

I.1.2 Relation avec les autres spécifications IPCablecom2

Ensemble, les spécifications concernant la signalisation SIP de base IPCablecom2 applicables à la signalisation pour les capacités générales suivantes:

- routage de message SIP;
- enregistrement;
- établissement de session de média;
- cadre de notification d'événement;
- plate-forme de commande de service générique;
- validation d'identité.

D'autres spécifications IPCablecom2 (comptabilité, traversée de dispositif NAT, sécurité, etc.) énoncent des exigences supplémentaires applicables à la signalisation SIP et ont donc une incidence sur les mêmes spécifications delta relatives au sous-système IMS, en particulier [UIT-T J.366.4]. En outre, certains mécanismes de signalisation SIP ont une incidence sur des spécifications delta relatives au sous-système IMS ne concernant pas le protocole SIP (par exemple UIT-T J.366.5). Enfin, la signalisation SIP IPCablecom2 rend nécessaire la prise en charge, dans le cadre de [UIT-T J.178], de l'interfonctionnement entre les équipements d'utilisateur IPCablecom2 et les adaptateurs E-MTA IPCablecom. La relation entre ces diverses spécifications est illustrée sur la Figure I.2.

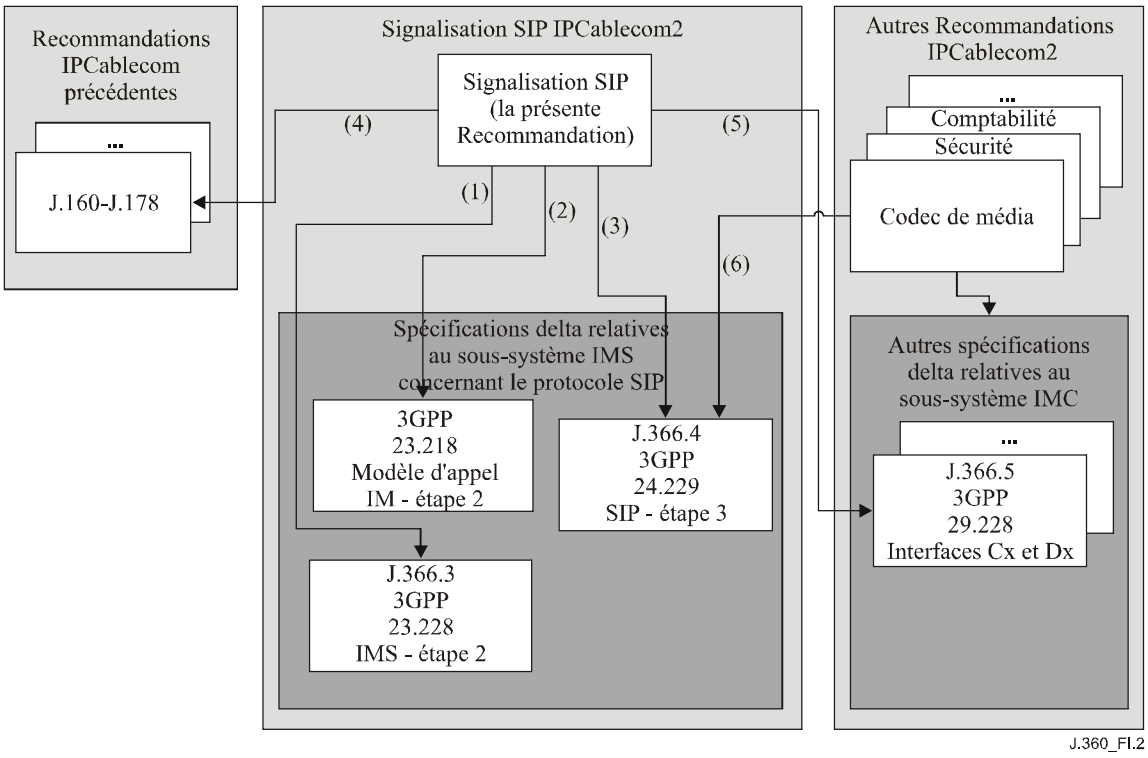


Figure I.2 – Relations entre les spécifications concernant la signalisation SIP

I.2 Références

Le présent appendice utilise les références informatives supplémentaires suivantes.

[UIT-T J.366.4] Recommandation UIT-T J.366.4 (2006), *IPCablecom2 IP Multimedia Subsystem (IMS): Session Initiation Protocol (SIP) and Session Description Protocol (SDP) – Stage 3 specification*. (3GPP TS 24.229)

[UIT-T J.366.5] Recommandation UIT-T J.366.5 (2007), *IP multimedia (IM) subsystem Cx and Dx interfaces; signalling flows and message contents specification*. (3GPP TS 29.228)

[IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

[IETF RFC 3262] IETF RFC 3262 (2002), *Reliability of Provisional Responses in the Session Initiation Protocol (SIP)*.

[IETF RFC 3311] IETF RFC 3311 (2002), *The Session Initiation Protocol (SIP) UPDATE Method*.

[IETF RFC 3312] IETF RFC 3312 (2002), *Integration of Resource Management and Session Initiation Protocol (SIP)*.

[IETF RFC 3320] IETF RFC 3320 (2003), *Signaling Compression (SigComp)*.

[IETF RFC 3329] IETF RFC 3329 (2003), *Security Mechanism Agreement for the Session Initiation Protocol (SIP)*.

[IETF RFC 3455] IETF RFC 3455 (2003), *Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)*.

[IETF RFC 3486] IETF RFC 3486 (2003), *Compressing the Session Initiation Protocol (SIP)*.

[IETF RFC 3556] IETF RFC 3556 (2003), *Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth*.

[IETF RFC 3680] IETF RFC 3680 (2004), *A Session Initiation Protocol (SIP) Event Package for Registrations*.

[IETF RFC 4032] IETF RFC 4032 (2005), *Update to the Session Initiation Protocol (SIP) Preconditions Framework*.

I.3 Termes et définitions

Le présent appendice utilise les termes et définitions supplémentaires suivants:

I.3.1 identité autorisée: une instance d''identité' autorisée dans un réseau IPCablecom2 est une représentation d'appariement autorisé entre une identité privée et une identité publique.

I.3.2 centre: le centre contient les composants de base nécessaires pour fournir les services SIP et les données d'abonné. Le groupement fonctionnel du centre est constitué des composants fonctionnels suivants: fonction CSCF interrogatrice (I-CSCF), fonction CSCF serveuse (S-CSCF), fonction de localisation d'abonnement (SLF) et serveur d'abonnés résidentiels (HSS).

I.3.3 justificatif d'identité: ensemble des informations nécessaires pour procéder à l'authentification d'une identité privée. Les informations effectives dépendent du mécanisme d'authentification.

I.3.4 fournisseur de services IPCablecom2: opérateur de réseau, exploitant un ou plusieurs domaines administratifs IPCablecom2 indépendants.

I.3.5 domaine DNS de fournisseur de services IPCablecom2: nom de domaine DNS qui est détenu et géré par un domaine administratif IPCablecom2. Il sert à former les identificateurs URI SIP qui acheminent les identificateurs publics.

I.3.6 serveur proxy: entité SIP intermédiaire faisant office à la fois de serveur et d'équipement d'utilisateur afin d'envoyer des demandes pour le compte d'autres équipements d'utilisateur. Un serveur proxy assure essentiellement une fonction de routage, ce qui signifie qu'il a pour tâche de veiller à ce qu'une demande soit envoyée à une autre entité "plus proche" de l'utilisateur visé. Les proxys sont également utiles pour la mise en œuvre d'une politique (par exemple pour vérifier qu'un utilisateur est autorisé à lancer un appel). Un proxy interprète et, si nécessaire, réécrit certaines parties d'un message de demande avant de retransmettre ledit message.

I.3.7 identificateur public: identificateur utilisé pour faire référence à une identité publique.

I.4 Abréviations et acronymes

Le présent appendice utilise l'abréviation supplémentaire suivante:

UE SIP équipement d'utilisateur qui contient un agent d'utilisateur SIP

I.5 Signalisation SIP IPCablecom2

Les applications et services IPCablecom2 sont commandés au moyen du protocole d'ouverture de session (SIP). Une harmonisation est assurée entre l'architecture IPCablecom2 et une instance particulière de l'architecture SIP définie par les spécifications relatives au sous-système multimédia IP (IMS) élaborées dans le cadre du projet de partenariat pour la troisième génération (3GPP). L'architecture IPCablecom2 est fondée sur la version 6 du sous-système IMS et perfectionne le sous-système IMS lorsque c'est nécessaire pour prendre en charge les exigences IPCablecom2.

I.5.1 Architecture de signalisation SIP IPCablecom2 et points de référence

Les points de référence pour la signalisation et la commande de service IPCablecom2 sont indiqués sur la Figure I.3. La plupart des points de référence sont définis dans le sous-système IMS, des modifications appropriées leur étant apportées dans l'architecture IPCablecom2, comme cela est précisé dans diverses spécifications IPCablecom2. Les points de référence propres à l'architecture IPCablecom2 sont aussi inclus.

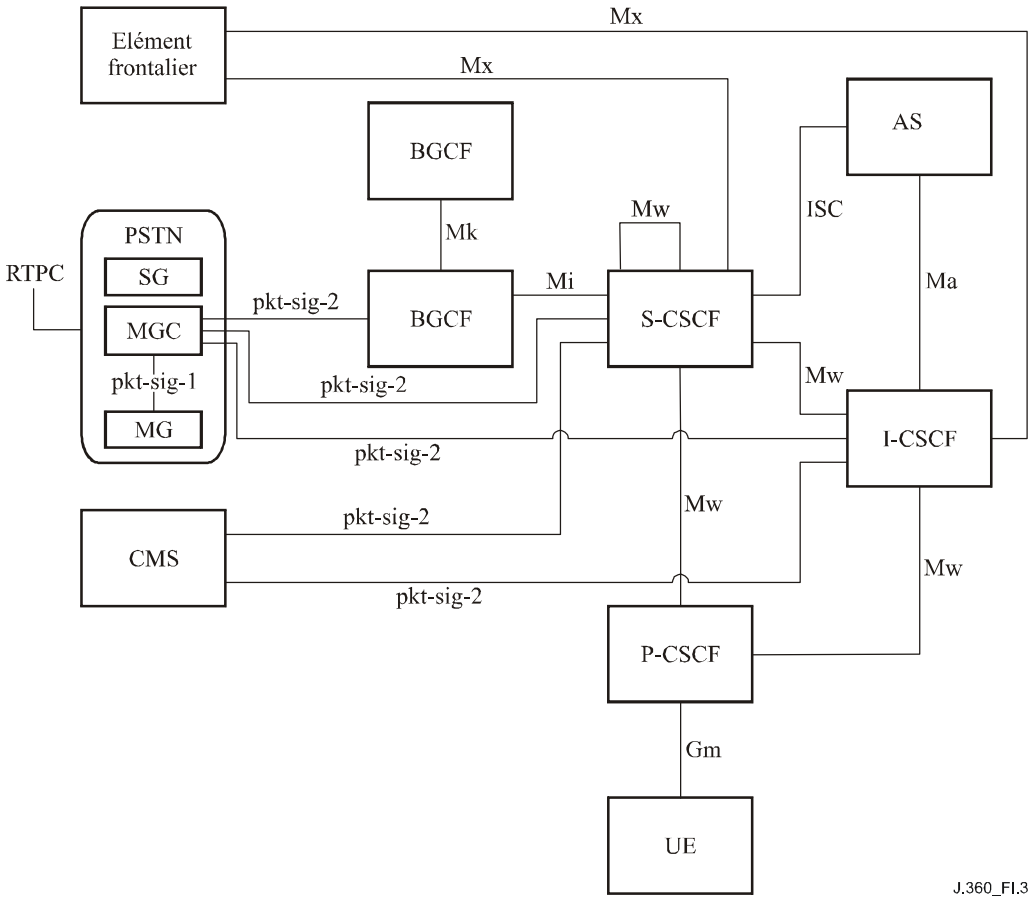


Figure I.3 – Points de référence pour la signalisation d'appel

I.5.1.1 Composants fonctionnels de signalisation SIP

I.5.1.1.1 Equipement d'utilisateur (UE)

L'architecture IPCablecom2 prend en charge des clients SIP avec diverses formes et capacités (par exemple téléphone logiciel ou matériel, téléphone intelligent, téléphone filaire ou sans fil, application de messagerie instantanée, terminal de visiocommunications, etc.). Tout comme les clients IMS, les clients IPCablecom2 sont appelés équipements d'utilisateur (UE). Tous les divers équipements d'utilisateur utilisent la même infrastructure de base pour obtenir des services multimédias. Les équipements d'utilisateur peuvent être des dispositifs fixes ou mobiles (ordinateur portable ou téléphone WiFi par exemple). Ils peuvent se trouver dans le réseau d'accès câblé ou peuvent obtenir des services depuis d'autres réseaux d'accès.

I.5.1.1.2 Fonction proxy de commande de session d'appel (P-CSCF)

Un équipement d'utilisateur accède à l'infrastructure SIP par le biais d'une fonction P-CSCF. Celle-ci masque au réseau SIP les détails de protocole propres au réseau d'accès et assure une certaine modulabilité de l'infrastructure en gérant certaines tâches nécessitant beaucoup de ressources lors de l'interaction avec l'équipement d'utilisateur. Elle représente également la limite de confiance pour le protocole SIP entre les parties non fiables (réseau d'accès, réseau local) et les parties fiables (réseau central, application, interconnexion, systèmes d'appui à l'exploitation) du réseau. La fonction P-CSCF exécute les fonctions suivantes:

- routage des messages SIP de l'équipement d'utilisateur à la fonction I-CSCF ou S-CSCF et inversement;
- maintien des associations de sécurité entre elle-même et l'équipement d'utilisateur et validation des identités publiques authentifiées;

- suivi de l'état d'enregistrement des identités publiques et suppression de l'association de sécurité avec l'équipement d'utilisateur lorsqu'une identité publique est désenregistrée par le réseau;
- vérification des données des messages entrants (par exemple vérification de l'en-tête route SIP);
- blocage de service (par exemple certaines demandes entrantes provenant d'identités publiques désenregistrées sont ignorées);
- application de politique (par exemple activation ou désactivation de la sécurité de la signalisation ou de la compression);
- production d'événements de comptabilité.

I.5.1.1.3 Fonction CSCF serveuse (S-CSCF)

La fonction S-CSCF est chargée de fournir des services aux abonnés utilisant un équipement d'utilisateur. En revanche, elle ne fournit pas de services aux adaptateurs E-MTA IPCablecom, qui sont desservis par leur serveur CMS comme décrit dans [UIT-T J.160].

Tous les messages SIP en dehors d'un dialogue à destination ou en provenance d'un abonné donné passeront par la fonction S-CSCF qui dessert cet abonné. A un haut niveau, la fonction S-CSCF prend en charge les capacités suivantes:

- fonction de serveur d'enregistrement SIP, qui tient à jour les données permettant de lier dynamiquement les identités publiques enregistrées (AOR) à un ensemble d'adresses de contact, d'attribuer des identificateurs GRUU, de stocker les autres paramètres associés à l'enregistrement (par exemple les capacités d'agent d'utilisateur et la ou les adresses de la fonction P-CSCF qui peuvent être utilisées pour atteindre les contacts) et de distribuer l'état d'enregistrement des utilisateurs aux entités qui sont abonnées au paquetage Reg-Event;
- authentification et autorisation d'utilisateur SIP;
- plate-forme de commande de service, qui applique des critères de filtrage aux demandes entrantes de lancement d'un dialogue et qui, sur la base de déclencheurs de point de service, assure le routage des demandes vers les serveurs d'application appropriés afin d'assurer des fonctionnalités et des services;
- routage des messages SIP vers une fonction P-CSCF concernant les équipements d'utilisateur desservis par la fonction S-CSCF;
- routage des messages SIP vers une fonction I-CSCF concernant les identités d'utilisateur publiques non desservies par la fonction S-CSCF;
- routage des messages vers une fonction BGCF concernant les appels destinés au RTPC;
- routage des messages vers une fonction I-CSCF homologue concernant les appels destinés à un réseau homologue;
- routage des messages vers la fonction THIG I-CSCF résidentielle afin de masquer la topologie concernant les appels destinés à un réseau homologue;
- traitement à l'entrée: traitement des demandes entrantes de lancement de dialogue provenant d'agents d'utilisateur SIP contenus dans des équipements d'utilisateur ou des serveurs d'application desservis par la fonction S-CSCF;
- traitement à la sortie: traitement des messages SIP sortants à destination d'une identité publique desservie par la fonction S-CSCF. Cela comporte la multiplication des messages SIP dans le cas où plusieurs adresses de contact sont enregistrées pour l'identité publique considérée;

- possibilité d'interrogation de bases de données de routage externes (par exemple ENUM, portabilité locale des numéros (LNP, *local number portability*) et numéros 800) afin de déterminer où il convient d'acheminer l'appel;
- production d'événements de comptabilité;
- contrôle du bon fonctionnement des sessions actives et libération de sessions en cas de défaillance d'un composant sur le trajet de signalisation (par exemple, la fonction S-CSCF peut libérer des sessions actives associées à un équipement d'utilisateur défaillant et pour le compte de cet équipement);
- libération de sessions lancée par le réseau (résultant par exemple d'une activité administrative).

Il peut y avoir plusieurs fonctions S-CSCF dans le réseau central IPCablecom. A un instant donné, un abonnement (et tous les identificateurs publics qui lui sont associés) ne peut être géré que par une seule fonction S-CSCF.

Les identificateurs publics sont attribués à une fonction S-CSCF au moment de l'enregistrement. Une fois qu'un identificateur public est attribué à une fonction S-CSCF, toutes les autres instances enregistrées de cet identificateur public doivent être attribuées à la même fonction S-CSCF. En outre, tous les identificateurs publics relevant du même abonnement doivent être associés à la même fonction S-CSCF. Les données relatives aux abonnements sont stockées dans un ou plusieurs serveurs d'abonnés résidentiels (HSS). La fonction S-CSCF interagit avec les serveurs HSS appropriés pour obtenir les données relatives aux utilisateurs qu'elle dessert. Elle peut aussi interagir avec le serveur HSS pour stocker certains types de données relatives aux utilisateurs qu'elle dessert.

Les identificateurs GRUU sont pris en charge par les points d'extrémité et la fonction S-CSCF. Cela permet aux points d'extrémité de se voir attribuer un identificateur GRUU pendant le processus d'enregistrement et, par là même, de demander un contact spécifique au lieu d'un AOR. C'est important pour diverses fonctionnalités comme le transfert d'appel et les conférences.

I.5.1.1.4 Fonction CSCF interrogatrice (I-CSCF)

La fonction I-CSCF est chargée du routage des demandes entrantes vers la fonction S-CSCF de destination correcte. Elle assure en outre une fonction de passerelle d'interfonctionnement pour le masquage de la topologie (THIG, *topology hiding interworking gateway*), qui peut être utilisée pour masquer la topologie interne du réseau résidentiel auprès d'un réseau homologue ou auprès d'un équipement d'utilisateur résidentiel.

- routage vers la fonction S-CSCF correcte des messages REGISTER entrants reçus en provenance de la fonction P-CSCF;
- routage vers la fonction S-CSCF de destination correcte des demandes entrantes de lancement de dialogue reçues en provenance d'une fonction S-CSCF d'origine dans le réseau domestique ou d'une fonction S-CSCF d'origine dans un réseau homologue;
- production d'événements de comptabilité.

La fonction I-CSCF est l'entité du réseau qui assure le routage des demandes externes provenant d'autres réseaux destinées à des utilisateurs situés dans le réseau domestique. Elle communique avec le serveur HSS pour déterminer le lien entre un abonnement (et les identités publiques associées) et une fonction S-CSCF.

I.5.1.1.5 Serveur d'application (AS)

Un serveur d'application fournit des services IPCablecom à valeur ajoutée et se trouve dans le réseau domestique de l'utilisateur ou dans un autre emplacement (autre réseau ou serveur d'application autonome). Il peut avoir une incidence sur une session SIP sur la base des services qu'il prend en charge et peut héberger et exécuter des services. Il peut lancer des services ou mettre fin à des services pour le compte d'un utilisateur.

I.5.1.1.6 Elément frontalier

L'interconnexion avec les réseaux homologues peut être assurée par le biais d'un élément frontalier. Celui-ci contient une fonction de proxy d'interconnexion et peut contenir une fonction de proxy de média. Il peut remplir diverses fonctions:

- interfonctionnement de protocoles;
- application de profils SIP (traduction, adaptation ou normalisation);
- services liés à la sécurité (par exemple maintien d'une association de sécurité avec l'homologue);
- gestion d'adresses IP (réseaux homologues avec le même espace d'adresses IP privées;
- interfonctionnement entre les réseaux IPv6 et IPv4;
- relais de média entre réseaux homologues (par exemple pour la sécurité des médias ou l'interfonctionnement de codecs);
- masquage d'adresse et de topologie au niveau de la signalisation (par exemple fait office de relais de signalisation et obscurcit les informations d'adresse présentes dans les en-têtes).

I.5.1.1.7 Fonction de commande de passerelle d'échappement (BGCF)

La fonction BGCF choisit un réseau aux fins du routage vers le RTPC et, dans son propre réseau, elle détermine le contrôleur MGC à utiliser pour le raccordement au RTPC. Elle peut interroger des bases de données de routage externes pour déterminer où il convient d'acheminer l'appel.

I.5.1.1.8 Passerelle de réseau téléphonique public commuté (passerelle de RTPC)

La passerelle de RTPC est constituée d'une passerelle de signalisation (SG), d'un contrôleur de passerelle média (MGC) et d'une passerelle média (MG). Les éléments fonctionnels SG, MGC et MG sont définis dans des versions précédentes de l'architecture IPCablecom et sont réutilisés dans la présente version de l'architecture IPCablecom2, un point de référence IPCablecom2 étant ajouté au contrôleur MGC. Les entités SG, MGC et MG sont des composants logiques qui peuvent exister sur des plates-formes distinctes ou qui peuvent être combinés ensemble sur une même plate-forme.

La passerelle de signalisation procède à une conversion de signalisation au niveau de la couche Transport entre le transport SS7 et le transport IP utilisé dans le réseau IPCablecom. Elle n'interprète pas la couche Application mais interprète les couches nécessaires au routage des messages de signalisation.

Le contrôleur MGC procède à une conversion de protocole entre les messages ISUP SS7 et les protocoles de commande d'appel IPCablecom et assure la commande de connexion des canaux de média dans la passerelle média.

La passerelle média assure la conversion de canal support entre le réseau à commutation de circuit et les flux de média RTP IP dans le réseau IPCablecom. Elle peut utiliser des codecs, des annuleurs d'écho, etc., selon qu'il est nécessaire pour assurer cette conversion.

I.5.1.1.9 Serveur de gestion des appels (CMS)

Un serveur de gestion d'appels (CMS) IPCablecom permet de prendre en charge les services de téléphonie destinés aux clients NCS (à savoir les adaptateurs E-MTA). Dans l'architecture IPCablecom2, le serveur CMS assure la plupart des fonctionnalités téléphoniques tout en interagissant directement avec les serveurs d'application (par exemple serveurs de conférence et serveurs de messagerie unifiée) pour fournir des applications supplémentaires aux points d'extrémité NCS. Toutefois, il n'autorise pas une exploitation transparente des fonctionnalités à travers les adaptateurs E-MTA et les équipements d'utilisateur détenus par le même utilisateur.

I.5.1.2 Points de référence pour la signalisation SIP

Les points de référence indiqués sur la Figure I.3 sont décrits dans le Tableau I.1. Tous les points de référence sont fondés sur le protocole SIP sauf indication contraire.

Tableau I.1 – Points de référence pour la signalisation d'appel

Point de référence	Eléments de réseau IPCablecom	Description du point de référence
Mx	I-CSCF – élément frontalier S-CSCF – élément frontalier	Permet à une fonction S-CSCF ou I-CSCF de communiquer avec un élément frontalier lors de l'interfonctionnement avec un autre réseau. Par exemple, une session entre le réseau résidentiel et un réseau homologue pourrait faire l'objet d'un routage via une fonction ALG IMS contenue dans l'élément frontalier afin d'assurer l'interfonctionnement entre les réseaux SIP IPv6 et IPv4.
Mi	S-CSCF – BGCF	Permet à la fonction S-CSCF de retransmettre les messages de signalisation de session à la fonction BGCF aux fins d'interfonctionnement avec les RTPC.
Mk	BGCF – BGCF	Permet à une fonction BGCF de retransmettre les messages de signalisation de session à une autre fonction BGCF.
Mw	P-CSCF – I-CSCF P-CSCF – S-CSCF I-CSCF – S-CSCF S-CSCF – S-CSCF	Permet de communiquer et de retransmettre des messages de signalisation entre fonctions CSCF pour permettre l'enregistrement et la commande de session.
Ma	I-CSCF – AS	Permet à la fonction I-CSCF de retransmettre les demandes SIP destinées à une identité de service publique hébergée par un serveur d'application directement au serveur d'application.
ISC	S-CSCF – AS	Permet à une fonction S-CSCF de communiquer avec un serveur d'application en appui à diverses applications.
Gm	UE – P-CSCF	Permet à l'équipement d'utilisateur de communiquer avec la fonction P-CSCF pour l'enregistrement et la commande de session.

Tableau I.1 – Points de référence pour la signalisation d'appel

Point de référence	Eléments de réseau IPCablecom	Description du point de référence
pkt-sig-1	MGC – MG	Interface TGCP (protocole de commande de passerelle de jonction), définie dans la spécification du protocole TGCP IPCablecom [UIT-T J.171.1].
pkt-sig-2	CMS – S-CSCF CMS – I-CSCF MGC – BGCF MGC – S-CSCF MGC – I-CSCF	Permet aux fonctions S-CSCF et I-CSCF d'échanger des messages de signalisation de session avec le serveur CMS afin de permettre aux adaptateurs E-MTA IPCablecom d'établir des sessions vocales avec les équipements d'utilisateur. Permet aussi aux fonctions BGCF, I-CSCF et S-CSCF d'échanger des messages de signalisation de session avec le contrôleur MGC aux fins d'interfonctionnement avec le RTPC.

I.5.2 Perfectionnements apportés au sous-système IMS dans l'architecture IPCablecom2

Si un grand nombre des composants et des interfaces définis dans le sous-système IMS s'appliquent largement à d'autres secteurs, la version 6 de ce sous-système est en revanche une architecture conçue pour le secteur du sans fil, l'objectif étant de satisfaire les besoins commerciaux et opérationnels de ce secteur. Par conséquent, elle ne répond pas à tous les besoins du secteur du câble. L'architecture IPCablecom2 perfectionne le sous-système IMS afin de prendre en charge les exigences techniques propres au secteur du câble et tient compte également des besoins commerciaux et opérationnels des câblo-opérateurs.

De nouvelles versions des spécifications IMS sont en cours d'élaboration dans le cadre du 3GPP. L'architecture IPCablecom sera actualisée dans l'avenir afin d'assurer une harmonisation avec ces nouvelles versions, en tant que de besoin.

I.5.2.1 Accès large bande par câble

L'accès radioélectrique fait l'objet de limitations liées à la rareté des ressources et à la forte latence. Par conséquent, la prise en charge de mécanismes spéciaux et d'extensions SIP pour réduire ces limitations est obligatoire dans le sous-système IMS. Etant donné que les limitations en termes de largeur de bande ou de latence applicables à l'accès radioélectrique ne s'appliquent pas à l'accès large bande par câble, la prise en charge de ces capacités est facultative dans l'architecture IPCablecom2.

La prise en charge par les équipements d'utilisateur des extensions SIP suivantes, qui est obligatoire dans la version 6 du sous-système IMS, est facultative dans l'architecture IPCablecom2.

I.5.2.1.1 Modificateurs de largeur de bande RTCP

Dans [IETF RFC 3556], des attributs SDP sont ajoutés pour permettre à un équipement d'utilisateur de spécifier explicitement la largeur de bande RTCP maximale qu'il souhaite recevoir en provenance de l'équipement d'utilisateur distant. Ainsi, un équipement d'utilisateur IMS peut réduire les ressources d'accès radioélectrique qu'il utilise en spécifiant une faible valeur de largeur de bande RTCP (éventuellement zéro). Dans l'architecture IPCablecom2, la prise en charge des modificateurs de largeur de bande RTCP est facultative au niveau de l'équipement d'utilisateur. Si l'équipement d'utilisateur prend en charge cette extension, il doit respecter les attributs de largeur de bande RTCP reçus afin d'assurer l'interfonctionnement avec les équipements d'utilisateur IMS qui utilisent ces paramètres. De même, l'équipement d'utilisateur doit pouvoir envoyer les modificateurs de largeur

de bande RTCP fondés sur une valeur configurée localement (la valeur configurée peut être fondée sur le type de réseau d'accès).

I.5.2.1.2 En-tête P-Associated-URI

[IETF RFC 3455] définit un en-tête P-Associated-URI, qui est utilisé dans le cadre de l'enregistrement implicite pour informer l'équipement d'utilisateur des différentes identités publiques présentes dans l'ensemble d'identités enregistrées implicitement. Il s'ensuit une réduction du trafic des messages d'enregistrement, étant donné que plusieurs identités publiques peuvent être enregistrées moyennant une seule transaction. Dans l'architecture IPCablecom2, la prise en charge de l'en-tête P-Associated-URI est facultative au niveau de l'équipement d'utilisateur.

I.5.2.1.3 Compression SIP

[IETF RFC 3486] définit une capacité de compression de message SIP permettant de réduire la largeur de bande de signalisation utilisée et la latence dans le réseau d'accès radioélectrique. La prise en charge de la compression SIP au niveau de l'équipement d'utilisateur est facultative dans l'architecture IPCablecom2. La fonction P-CSCF contrôle si la compression SIP est activée ou non, sur la base des données configurées localement ou du type de réseau d'accès indiqué dans l'en-tête P-network-access-info.

I.5.2.1.4 Temporisations SIP

Le sous-système IMS modifie (rallonge) les temporisations SIP afin de réduire la charge de signalisation dans le réseau d'accès et de tolérer la grande latence imposée par l'accès radioélectrique. Dans l'architecture IPCablecom2, l'équipement d'utilisateur doit être conforme aux valeurs de temporisation SIP standard spécifiées dans le document [IETF RFC 3261].

I.5.2.2 Modularité

L'architecture IPCablecom2 doit obligatoirement prendre en charge la modularité au niveau de l'équipement d'utilisateur, afin de favoriser l'interfonctionnement avec les points d'extrémité SIP non 3GPP et de permettre aux opérateurs d'adapter les déploiements aux offres de services spécifiques. Par conséquent, certaines des extensions SIP qui sont obligatoires dans la version 6 du sous-système IMS sont facultatives dans l'architecture IPCablecom2.

I.5.2.2.1 Fiabilité des réponses provisoires

[IETF RFC 3262] définit une demande SIP appelée PRACK, qui est utilisée pour permettre une transmission bidirectionnelle précoce de média et pour garantir une fourniture fiable des réponses provisoires. Dans l'architecture IPCablecom2, la prise en charge du message PRACK est obligatoire au niveau de l'équipement d'utilisateur et son utilisation doit pouvoir être configurée sur l'un des deux modes suivants:

1) nécessaire – l'équipement d'utilisateur doit inclure l'étiquette d'option "100rel" dans l'en-tête Require SIP de la demande INVITE de manière à pouvoir établir des sessions uniquement avec les autres équipements d'utilisateur qui prennent aussi en charge le message PRACK;
2) négociée – l'équipement d'utilisateur doit inclure l'étiquette d'option "100rel" dans l'en-tête Supported SIP de la demande INVITE de manière à pouvoir négocier l'utilisation ou la non-utilisation du message PRACK, suivant si l'équipement d'utilisateur distant prend ou non en charge ce message.

I.5.2.2.2 UPDATE

[IETF RFC 3311] définit une demande SIP appelée UPDATE, qui sert à mettre à jour les sessions de média avant la réponse (essentiellement pour les préconditions). Dans l'architecture IPCablecom2, la prise en charge du message UPDATE est obligatoire au niveau de l'équipement d'utilisateur (en d'autres termes, l'équipement d'utilisateur doit toujours faire une annonce dans l'en-tête Allow), mais son utilisation est facultative. Par exemple, l'équipement d'utilisateur peut

choisir de ne pas envoyer du message UPDATE s'il sait que l'équipement d'utilisateur distant ne prend pas en charge ce message compte tenu de ce qu'il a reçu dans l'en-tête Allow entrant.

I.5.2.2.3 Paquetage Reg-Event

La norme [IETF RFC 3680] définit un nouveau paquetage d'événement appelé Reg-Event, qui est utilisé par le réseau pour informer l'équipement d'utilisateur du fait qu'il a été désenregistré. Le réseau peut utiliser ce paquetage d'événement pour empêcher à un équipement d'utilisateur d'accéder aux services du réseau, ou pour déclencher le réenregistrement d'un équipement d'utilisateur en vue de la réattribution d'une fonction S-CSCF. Dans l'architecture IPCablecom2, la prise en charge du paquetage Reg-Event est facultative au niveau de l'équipement d'utilisateur. S'il prend en charge ce paquetage, l'équipement d'utilisateur doit être doté de commandes de configuration permettant de désactiver son utilisation.

I.5.2.2.4 En-tête P-Access-Network-Info

La norme [IETF RFC 3455] définit un en-tête SIP appelé P-Access-Network-Info, qui permet à l'équipement d'utilisateur de communiquer au réseau la technologie d'accès (par exemple radio électrique, 802.11, DOCSIS). Dans l'architecture IPCablecom2, la prise en charge de l'en-tête P-Access-Network-Info est facultative au niveau de l'équipement d'utilisateur. S'il prend en charge cet en-tête, l'équipement d'utilisateur ne le communiquera que s'il connaît le type de technologie d'accès qu'il utilise. Par exemple, un adaptateur E-MTA peut savoir qu'il utilise la technologie d'accès DOCSIS, alors qu'un client logiciel peut ne pas savoir s'il utilise la technologie d'accès DOCSIS ou WiFi.

I.5.2.2.5 Désactivation de la sécurité de la signalisation

Dans l'architecture IPCablecom2, l'équipement d'utilisateur ainsi que la fonction P-CSCF doivent obligatoirement prendre en charge la sécurité de la signalisation. Toutefois, la fonction P-CSCF doit prendre en charge les paramètres de configuration qui permettent de désactiver la sécurité de la signalisation entre l'équipement d'utilisateur et elle-même. Elle doit prendre en charge trois modes qui s'appliquent à toutes les associations de signalisation avec les équipements d'utilisateur:

1) sécurité de la signalisation désactivée – la sécurité de la signalisation est toujours désactivée pour tous les équipements d'utilisateur desservis par la fonction P-CSCF;
2) sécurité de la signalisation activée – la sécurité de la signalisation est activée pour tous les équipements d'utilisateur desservis par la fonction P-CSCF;
3) sécurité de la signalisation négociée – la sécurité de la signalisation est activée pour les équipements d'utilisateur qui la prennent en charge (il est à noter que les équipements d'utilisateur IPCablecom2 doivent obligatoirement prendre en charge la sécurité de la signalisation) et désactivée pour les équipements d'utilisateur qui ne la prennent pas en charge.

I.5.2.3 Services

L'architecture IPCablecom2 de base doit prendre en charge certaines capacités de base supplémentaires requises par les services (téléphonie SIP résidentielle et intégration sans fil et cellulaire par exemple) qui ne sont pas pris en charge dans la version 6 du sous-système IMS.

I.5.2.3.1 Portabilité de numéro URI téléphonique et routage opérateur

Dans l'architecture IPCablecom2, la prise en charge de la portabilité de numéro est facultative pour la fonction S-CSCF et obligatoire pour le contrôleur MGC. La fonction BGCF peut prendre en charge l'ajout d'un opérateur faisant l'objet d'un abonnement préalable dans tout le réseau. La prise en charge des paramètres correspondants est facultative pour l'équipement d'utilisateur. Il est à noter qu'un équipement d'utilisateur qui prend en charge l'identificateur URI téléphonique doit aussi prendre en charge ces paramètres.

I.5.2.3.2 Identificateur URI d'agent d'utilisateur routable à l'échelle mondiale (GRUU)

Les identificateurs GRUU constituent un mécanisme permettant à un serveur d'enregistrement de fournir à un agent d'utilisateur qui s'enregistre une adresse de contact routable à l'échelle mondiale. Ce mécanisme est requis par certaines fonctionnalités (par exemple le transfert d'appel) pour lesquelles il faut pouvoir acheminer une demande de lancement de dialogue à une instance enregistrée spécifique d'un AOR, lorsqu'il existe plusieurs instances enregistrées. Dans l'architecture IPCablecom2, la prise en charge des identificateurs GRUU est facultative au niveau de l'équipement d'utilisateur, mais obligatoire pour les composants de réseau sur lesquels les identificateurs GRUU ont une incidence (par exemple la fonction S-CSCF). Un équipement d'utilisateur qui prend en charge les identificateurs GRUU doit utiliser l'AOR comme adresse de contact lors de l'interfonctionnement avec des équipements d'utilisateur distants qui ne prennent pas en charge les identificateurs GRUU.

I.5.2.3.3 Internet-draft – Paquetage Reg-event pour les identificateurs GRUU

L'enregistrement implicite permet à plusieurs identités publiques d'être enregistrées dans le cadre d'une seule transaction REGISTER. La réponse à une demande REGISTER ne peut acheminer qu'un seul identificateur GRUU. Par conséquent, lorsque les identificateurs GRUU et l'enregistrement implicite sont tous deux pris en charge, il faut prévoir un mécanisme permettant de communiquer plusieurs identificateurs GRUU à l'équipement d'utilisateur. Pour cela, on utilise une extension au paquetage Reg-event permettant de communiquer plusieurs identificateurs GRUU dans un message NOTIFY.

I.6 Exigences relatives au sous-système IMS IPCablecom2

Le présent paragraphe décrit les exigences qui ne sont pas actuellement prises en charge dans la version 6 du sous-système IMS, mais qui sont nécessaires dans l'architecture de signalisation SIP IPCablecom2.

I.6.1 Signalisation sécurisée SIP

Dans l'architecture IPCablecom2, la sécurité de la signalisation peut être désactivée entre l'équipement d'utilisateur et la fonction P-CSCF. Le présent paragraphe commence par décrire le modèle de sécurité de la signalisation défini dans le cadre du 3GPP pour les communications IMS puis décrit l'incidence sur le sous-système IMS d'une autorisation d'accès aux services IMS sans signalisation SIP sécurisée entre l'équipement d'utilisateur et la fonction P-CSCF.

I.6.1.1 Description

L'architecture de sécurité IMS [UIT-T J.366.7] est fondée sur plusieurs relations de sécurité obligatoires, dont deux sont étroitement couplées avec les procédures d'enregistrement IMS:

1) authentification mutuelle entre l'utilisateur et le réseau;
2) association de sécurité entre l'équipement d'utilisateur et la fonction P-CSCF, qui assure une protection d'intégrité et, facultativement, une protection de confidentialité de la signalisation SIP (à savoir la sécurité de la signalisation).

Conformément aux procédures d'enregistrement IMS, l'équipement d'utilisateur commence par envoyer une demande REGISTER initiale à la fonction P-CSCF, qui l'achemine à la fonction S-CSCF desservant l'utilisateur. Comme aucune association de sécurité n'a encore été établie entre l'équipement d'utilisateur et la fonction P-CSCF, la demande REGISTER initiale est envoyée sans être protégée. La fonction S-CSCF détermine que cette demande qu'elle reçoit a été envoyée sans être protégée en vérifiant le paramètre "integrity-protected" dans l'en-tête Authorization SIP. Etant donné que la demande REGISTER a été envoyée sans être protégée et que l'utilisateur n'est pas encore enregistré, la fonction S-CSCF lance les procédures d'authentification mutuelle en

produisant une réponse 401 (non autorisé) à la demande REGISTER non protégée et elle déclenche une temporisation reg-await-auth.

Après avoir reçu la réponse 401 (non autorisé), l'équipement d'utilisateur établit un ensemble d'associations de sécurité avec la fonction P-CSCF. Il envoie ensuite une deuxième demande REGISTER contenant la réponse donnée par le procédé d'authentification, qui est envoyée en étant protégée sur l'association de sécurité nouvellement établie à destination de la même fonction S-CSCF. Etant donné que la demande REGISTER a été envoyée en étant protégée et qu'une procédure d'autorisation est en cours pour cet utilisateur (une temporisation reg-await-auth est en cours pour cet utilisateur), la fonction S-CSCF authentifie l'utilisateur en vérifiant la réponse donnée par le procédé d'authentification. Une fois que la fonction S-CSCF a mené à bien les procédures d'enregistrement, une réponse 200 (OK) est envoyée à l'équipement d'utilisateur.

A l'exception de la demande REGISTER initiale, le sous-système IMS nécessite que tous les messages SIP à destination ou en provenance de l'équipement d'utilisateur soient envoyés en étant protégés sur l'association de sécurité. Celle-ci permet aussi d'authentifier l'origine des données, ce qui permet à la fonction P-CSCF de valider l'identité de l'équipement d'utilisateur.

La sécurité de la signalisation est une capacité obligatoire de l'équipement d'utilisateur dans l'architecture SIP IPCablecom2. Toutefois, l'architecture IPCablecom2 permet de désactiver la sécurité de la signalisation de diverses façons:

1) l'équipement d'utilisateur peut être configuré [UIT-T J.364] avec la sécurité de la signalisation désactivée; ou

2) la fonction P-CSCF peut être configurée avec la sécurité de la signalisation désactivée pour tous les équipements d'utilisateur qui accèdent aux services IMS par le biais de ladite fonction P-CSCF.

En outre, pour certaines demandes, il se peut que la sécurité de la signalisation ne soit pas requise. Dans le sous-système IMS IPCablecom2, la seule demande de ce type concerne l'abonnement au paquetage d'événement ua-profile.

I.6.1.2 Composants affectés

Le présent paragraphe décrit les composants IMS affectés par une autorisation d'accès aux services IMS sans signalisation SIP sécurisée entre l'équipement d'utilisateur et la fonction P-CSCF, ainsi que la nature de l'incidence sur le composant.

NOTE – On trouvera à l'Appendice III des informations supplémentaires en matière de sécurité lorsque la sécurité de la signalisation est désactivée.

I.6.1.2.1 Equipement d'utilisateur

Un équipement d'utilisateur IPCablecom2 doit prendre en charge la négociation et l'établissement d'associations de sécurité comme décrit dans le sous-système IMS. Toutefois, lorsque la sécurité de la signalisation n'est pas recommandée, un équipement d'utilisateur IPCablecom2 doit être souple et pouvoir interfonctionner dans un environnement d'opérateur dans lequel les procédures relatives à la sécurité de la signalisation ont été désactivées.

Dans l'architecture IPCablecom2, l'équipement d'utilisateur ne lance pas d'association de sécurité dans les scénarios suivants:

- la fonction P-CSCF indique à l'équipement d'utilisateur, pendant l'enregistrement initial, que la sécurité de la signalisation est désactivée;
- l'équipement d'utilisateur est configuré avec la sécurité de la signalisation désactivée comme décrit dans [UIT-T J.364] et la fonction P-CSCF ne lui a pas indiqué, pendant l'enregistrement initial, que la sécurité de la signalisation était requise.

Si l'équipement d'utilisateur inclut l'étiquette d'option "sec-agree" dans l'en-tête Require comme défini dans le document [IETF RFC 3329] lorsqu'il envoie une demande REGISTER initiale et qu'il reçoit une réponse 420 (mauvaise extension) avec la valeur de l'étiquette d'option "sec-agree" dans l'en-tête Unsupported, il devrait renvoyer la demande REGISTER sans suivre les procédures définies dans le document [IETF RFC 3329].

Si l'équipement d'utilisateur est configuré avec la sécurité de la signalisation désactivée et qu'il n'a pas reçu de réponse 494 (accord de sécurité requis), il ne doit pas suivre les procédures décrites dans le document [IETF RFC 3329].

Si l'équipement d'utilisateur mène à bien son enregistrement sans avoir établi d'association de sécurité, il procède comme suit pour toute demande initiale ou transaction autonome (sauf REGISTER):

- s'il prend en charge l'en-tête P-Preferred-Identity, il doit l'insérer et mettre comme valeur une identité publique enregistrée de l'utilisateur;
- s'il ne prend pas en charge l'en-tête P-Preferred-Identity, il doit faire en sorte que le champ d'en-tête From ait pour valeur une identité publique enregistrée de l'utilisateur. Dans ce cas, la confidentialité ne peut pas être prise en charge.

Les demandes d'abonnement au paquetage d'événement ua-profile peuvent être autorisées avant l'enregistrement, sur la base de la politique locale. Si l'équipement d'utilisateur n'est pas enregistré, il procède comme suit pour les demandes SUBSCRIBE concernant le paquetage d'événement ua-profile:

- il doit inclure l'en-tête From et mettre comme valeur l'identité d'utilisateur publique obtenue comme décrit au § I.6.13 "Routage des demandes SUBSCRIBE pour les informations de configuration";
- s'il prend en charge l'en-tête P-Preferred-Identity, il doit l'insérer et mettre comme valeur l'identité d'utilisateur publique incluse dans le champ d'en-tête From.

I.6.1.2.2 Fonction P-CSCF

Dans l'architecture IPCablecom2, la fonction P-CSCF doit prendre en charge les exigences relatives à la sécurité de la signalisation définies dans l'Appendice III.

La fonction P-CSCF peut être configurée avec la sécurité de la signalisation "désactivée" ou "requise" pour tous les équipements d'utilisateur qui accèdent aux services IMS par le biais de ladite fonction P-CSCF. Elle peut aussi être configurée avec la sécurité de la signalisation "facultative"; dans ce cas, elle détermine si la sécurité de la signalisation est désactivée pour un équipement d'utilisateur particulier sur la base d'une indication reçue en provenance de l'équipement d'utilisateur pendant l'enregistrement initial.

Si la fonction P-CSCF est configurée avec la sécurité de la signalisation "facultative" ou "désactivée", elle procède comme suit:

- elle doit accepter les demandes REGISTER qui ne contiennent pas l'étiquette d'option "sec-agree" dans l'en-tête Require comme défini dans le document [IETF RFC 3329]. Dans ce cas, elle doit ignorer les procédures relatives à l'accord sur le mécanisme de sécurité spécifiées dans [UIT-T J.364];
- elle devrait autoriser les demandes non protégées autres que REGISTER.

Si la fonction P-CSCF est configurée avec la sécurité de la signalisation "désactivée", elle procède comme suit:

- elle doit accepter les demandes REGISTER qui ne contiennent pas l'étiquette d'option "sec-agree" dans l'en-tête Require comme défini dans le document [IETF RFC 3329] Dans ce cas, elle doit ignorer les procédures relatives à l'accord sur le mécanisme de sécurité spécifiées dans [UIT-T J.366.4];

- si elle reçoit d'un équipement d'utilisateur une demande REGISTER qui inclut l'étiquette d'option "sec-agree" dans l'en-tête Require comme défini dans le document [IETF RFC 3329], elle doit rejeter la demande avec une réponse 420 (mauvaise extension) et inclure l'étiquette d'option "sec-agree" dans l'en-tête Unsupported;
- elle devrait autoriser les demandes non protégées autres que REGISTER.

Si la fonction P-CSCF est configurée avec la sécurité de la signalisation "requise", elle procède comme suit:

- si elle reçoit d'un équipement d'utilisateur une demande REGISTER qui ne contient pas l'étiquette d'option "sec-agree" dans l'en-tête Require comme défini dans le document [IETF RFC 3329], elle doit rejeter la demande avec une réponse 494 (accord de sécurité requis).

La fonction P-CSCF devrait valider l'identité de l'entité à l'origine de la demande (en insérant un en-tête P-Asserted-Identity) et supprimer l'en-tête P-Preferred-Identity s'il est présent, uniquement pour les demandes autres que REGISTER reçues sur une association de sécurité.

Si la fonction P-CSCF reçoit une demande autre que REGISTER qui ne contient pas d'en-tête Route (à savoir une demande provenant d'un utilisateur non enregistré), elle retransmettra la demande à la fonction I-CSCF de l'utilisateur desservi.

I.6.1.2.3 Fonction I-CSCF

Dans l'architecture IPCablecom2, la fonction I-CSCF doit prendre en charge les exigences relatives à la sécurité de la signalisation définies dans l'Appendice III.

I.6.1.2.4 Fonction S-CSCF

Dans l'architecture IPCablecom2, la fonction S-CSCF doit prendre en charge les exigences relatives à la sécurité de la signalisation définies dans l'Appendice III.

La fonction S-CSCF peut être configurée avec la sécurité de la signalisation "requise" pour tous les équipements d'utilisateur qui accèdent aux services IMS par le biais de ladite fonction S-CSCF. Elle peut aussi être configurée avec la sécurité de la signalisation "facultative"; dans ce cas, elle accepte les demandes REGISTER non protégées qui sont authentifiées. La configuration des fonctions S-CSCF et P-CSCF doit être coordonnée par l'opérateur.

Si les fonctions S-CSCF et P-CSCF sont configurées pour permettre l'accès aux services IMS sans signalisation SIP sécurisée pour un ou plusieurs équipements d'utilisateur, alors:

- si la fonction S-CSCF reçoit une demande REGISTER et que l'authentification est en cours pour cet utilisateur (la temporisation reg-await-auth est en cours), la fonction S-CSCF exécutera les procédures d'enregistrement spécifiées dans [UIT-T J.366.4] comme si le paramètre "integrity-protected" dans l'en-tête Authorization avait la valeur "yes";
- lors de l'exécution du traitement à l'entrée pour une identité d'utilisateur publique enregistrée, si la fonction S-CSCF reçoit une demande dans laquelle il manque un en-tête P-Asserted-Identity requis dans [UIT-T J.366.4], alors:
  - la fonction S-CSCF identifiera l'expéditeur sur la base de la valeur contenue dans l'en-tête P-Preferred-Identity si celui-ci est présent, ou dans l'en-tête From si l'en-tête P-Preferred-Identity est absent;
  - si la demande contient une réponse d'authentification valable, la fonction S-CSCF insérera un en-tête P-Asserted-Identity et supprimera l'en-tête P-Preferred-Identity si celui-ci est présent;
  - si la demande ne contient pas de réponse d'authentification valable, la fonction S-CSCF devrait lancer les procédures d'authentification en produisant une réponse 401 (non autorisé).

Si la fonction S-CSCF reçoit une demande SUBSCRIBE concernant le paquetage d'événement ua-profile en provenance d'une identité d'utilisateur publique non enregistrée mais connue, elle devrait exécuter le traitement à l'entrée comme si l'utilisateur était enregistré.

I.6.1.3 Spécification delta relative au sous-système IMS IPCablecom2

La spécification delta relative au sous-système IMS IPCablecom2 suivante contient les exigences concernant la signalisation sécurisée SIP: [UIT-T J.366.4].

I.6.2 Prise en charge de IPv4 et IPv6

I.6.2.1 Description

[UIT-T J.366.4] spécifie que des adresses IPv6 sont attribuées aux équipements d'utilisateur et aux entités du sous-système IMS. Dans le cadre de la prise en charge du "large bande fixe" dans la version 7 du sous-système IMS 3GPP, cette spécification est élargie et permet d'attribuer des adresses IPv4, des adresses IPv6 ou les deux aux équipements d'utilisateur et aux sous-systèmes IMS. L'architecture IPCablecom2 nécessite la prise en charge de IPv4 et les deux types d'adresses doivent être pris en charge par les composants du sous-système IMS et les équipements d'utilisateur IPCablecom2.

Certaines procédures définies dans [UIT-T J.366.4] sont explicitement décrites comme étant propres au protocole IPv6. Ces procédures ne s'appliquent pas aux clients IPv4. ("Changement d'adresse IPv6 en raison de la confidentialité".)

I.6.2.2 Composants affectés

Les modifications nécessaires à la prise en charge de IPv4 sont incorporées dans [UIT-T J.366.4]. Le document 3GPP Change Request correspondant inclut les modifications suivantes:

- modification des attributions d'identificateur URI et d'adresse, pour permettre d'attribuer des adresses IPv4 ou IPv6 ou les deux aux entités du sous-système IMS et aux équipements d'utilisateur (§ 4.2 de [UIT-T J.366.4]).
  - L'utilisation de IPv6 dans l'architecture IPCablecom2 doit faire l'objet d'un complément d'étude. Seule l'utilisation de IPv4 est supposée au départ. La modification fait partie des modifications 3GPP.
- Modification des procédures relatives à la fonction S-CSCF, avec généralisation d'une procédure de vérification d'un type d'adresse IP dans le protocole SDP, dans le cas d'un scénario d'erreur dans lequel l'extrémité distante indique que le type d'adresse n'est pas pris en charge (§ 5.4.3.2 de [UIT-T J.366.4]).
  - L'interfonctionnement entre un réseau IPCablecom2 fondé sur IPv4 et des réseaux IPv6 doit faire l'objet d'un complément d'étude, mais cette modification est incluse afin d'incorporer toutes les modifications connexes provenant du document 3GPP R7 CR.
  - Modification des procédures au niveau de l'équipement d'utilisateur pour la découverte de la fonction P-CSCF afin de faire référence aux procédures DHCP IPv4 applicables (§ 9.2.1 de [UIT-T J.366.4]).
  - Cette modification particulière ne s'applique pas à l'architecture IPCablecom2 car d'autres procédures sont utilisées pour la découverte de la fonction P-CSCF, mais elle est incluse afin d'incorporer toutes les modifications connexes provenant du document 3GPP R7 CR.

I.6.2.3 Spécification delta relative au sous-système IMS IPCablecom2

La spécification delta relative au sous-système IMS IPCablecom2 suivante contient les exigences concernant la prise en charge de IPv4 et IPv6: paragraphes 4.2, 5.4.3.2 et 9.2.1 de [UIT-T J.366.4].

I.6.3 Compression SIP

I.6.3.1 Description

Dans la version 6 du sous-système IMS 3GPP [UIT-T J.366.4], l'équipement d'utilisateur et la fonction P-CSCF doivent obligatoirement prendre en charge la compression de signalisation (SigComp) définie dans [IETF RFC 3320] et la compression SIP définie dans [IETF RFC 3486]. La compression SIP est obligatoire afin de minimaliser les délais au niveau d'un accès 3GPP à faible largeur de bande. Pour la partie de l'architecture IPCablecom2 relative à l'accès large bande câblé, ces considérations ne s'appliquent pas. Il est à noter que, dans le cadre de la prise en charge du "large bande fixe" dans la version 7 du sous-système IMS 3GPP, la prise en charge et l'utilisation de la compression SIP est facultative pour les équipements d'utilisateur utilisant une technologie d'accès large bande et l'utilisation de la compression SIP par la fonction P-CSCF (par exemple lorsque cette compression est prise en charge par le client) n'est pas requise si l'équipement d'utilisateur utilise une technologie d'accès large bande.

L'architecture IPCablecom2 incorpore ces modifications relatives à la compression SIP décrites dans la version 7 du sous-système IMS 3GPP: la mise en œuvre par l'équipement d'utilisateur IPCablecom2 et l'utilisation par la fonction P-CSCF de la compression de signalisation (SigComp) définie dans [IETF RFC 3320] et de la compression SIP définie dans [IETF RFC 3486] sont facultatives.

L'implémentation de l'exigence ci-dessus dépend de la connaissance du fait que l'équipement d'utilisateur se trouve dans un réseau large bande câblé, une nouvelle valeur de type d'accès étant utilisée dans l'en-tête P-Access-Network-Info, représentant une technologie de réseau d'accès large bande DOCSIS. On trouvera davantage de détails au § I.6.12.1.2.

NOTE – La solution décrite dans la version 7 du sous-système IMS 3GPP pourra faire l'objet d'un complément d'étude dans le cadre du 3GPP afin d'examiner s'il existe de meilleures méthodes pour déterminer les délais au niveau de l'accès et s'il convient d'utiliser la compression SIP. L'architecture IPCablecom2 pourra ensuite être modifiée afin de tenir compte des futures modifications qui pourront être apportées dans ce domaine.

I.6.3.2 Composants affectés

Les modifications requises sont identifiées et incorporées dans la version 7.

I.6.3.2.1 Equipement d'utilisateur

La prise en charge de la compression SigComp et de la compression SIP est facultative pour les équipements d'utilisateur qui sont destinés à être utilisés dans un réseau d'accès large bande.

Si l'équipement d'utilisateur prend en charge la compression SigComp et la compression SIP, il ne devrait pas les utiliser s'il se trouve dans un réseau d'accès large bande (sur la base du type d'accès figurant dans P-Access-Network-Info) ou s'il ne connaît pas le type d'accès.

I.6.3.2.2 Fonction P-CSCF

La prise en charge de la compression SigComp et de la compression SIP est requise pour la fonction P-CSCF déployée dans un réseau d'accès large bande câblé mais son utilisation effective est facultative.

Si la compression SigComp est prise en charge par l'équipement d'utilisateur, l'utilisation de la compression SIP ne devrait pas être proposée par la fonction P-CSCF si l'équipement d'utilisateur se trouve dans un réseau d'accès large bande câblé (sur la base du type d'accès figurant dans P-Access-Network-Info) ou si le type d'accès est inconnu.

I.6.3.3 Spécification delta relative au sous-système IMS IPCablecom2

La spécification delta relative au sous-système IMS IPCablecom2 suivante contient les exigences concernant la compression SIP: paragraphe 8 de [UIT-T J.366.4].

I.6.4 Fiabilité des réponses provisoires SIP

I.6.4.1 Description

La fiabilité de la réponse provisoire dans le protocole SIP est une extension définie dans [IETF RFC 3262] en appui à plusieurs applications. Elle est d'abord nécessaire lors de l'établissement de sessions au moyen de l'extension relative aux préconditions SIP. Elle permet ensuite un échange offre/réponse SDP dans le cadre d'une demande INVITE et d'une réponse provisoire initiale, qui est nécessaire pour la prise en charge de médias précoces (par exemple, dans certains scénarios d'interfonctionnement avec le RTPC). Enfin, elle garantit que la mesure prise par un équipement d'utilisateur à la réception d'une réponse provisoire est réellement exécutée (par exemple elle garantit qu'un équipement d'utilisateur d'origine applique une tonalité de retour d'appel dès qu'il reçoit une réponse 180 à un message INVITE).

Dans la version 6 du sous-système IMS 3GPP, l'équipement d'utilisateur doit obligatoirement prendre en charge la fiabilité des réponses provisoires lors de l'ouverture de sessions, en appui à l'extension relative aux préconditions SIP. Dans l'architecture IPCablecom2, ces exigences vont être mises à jour afin de permettre à l'équipement d'utilisateur, sur la base des données de configuration, d'interfonctionner avec les équipements d'utilisateur non 3GPP qui ne prennent pas en charge cette extension SIP.

I.6.4.2 Composants affectés

Pour ce qui est de permettre à un équipement d'utilisateur d'interfonctionner avec les points d'extrémité qui ne prennent pas en charge l'extension SIP relative à la fiabilité des réponses provisoires, les incidences sont localisées au niveau de l'équipement d'utilisateur proprement dit.

I.6.4.2.1 Equipement d'utilisateur

Un équipement d'utilisateur qui prend en charge des sessions doit prendre en charge l'extension relative à la fiabilité des réponses provisoires définie dans le document [IETF RFC 3262].

Un équipement d'utilisateur peut être configuré pour nécessiter la prise en charge de l'extension relative à la fiabilité des réponses provisoires. Dans ce cas, l'établissement de session avec un autre équipement d'utilisateur qui ne prend pas en charge la même extension échouera.

Autre solution: un équipement d'utilisateur peut être configuré pour négocier la prise en charge de l'extension relative à la fiabilité des réponses provisoires. Ainsi, l'extension n'est utilisée que si elle est prise en charge aussi bien par l'équipement d'utilisateur d'origine que par celui de destination.

I.6.4.3 Spécification delta relative au sous-système IMS IPCablecom2

La spécification delta relative au sous-système IMS IPCablecom2 suivante contient les exigences concernant la fiabilité des réponses provisoires SIP:

voir paragraphe 5.1 et Tableau A.4 de [UIT-T J.366.4].

I.6.5 UPDATE SIP

I.6.5.1 Description

La méthode relative à l'extension UPDATE SIP définie dans [IETF RFC 3311] permet à un client SIP de mettre à jour les paramètres d'une session. En particulier, elle est utilisée en appui aux préconditions SIP [IETF RFC 3312].

Dans la version 6 du sous-système IMS 3GPP, la prise en charge de la méthode UPDATE est obligatoire dans le cadre de l'extension relative aux préconditions. Dans l'architecture IPCablecom2, ces exigences sont élargies afin de permettre une utilisation facultative de l'extension UPDATE en dehors de préconditions. Plus précisément, un équipement d'utilisateur IPCablecom2 doit prendre en charge l'extension UPDATE, mais devrait adopter des procédures permettant de maximaliser

l'interfonctionnement avec les équipements d'utilisateur qui ne prennent pas en charge cette extension (par exemple nouveau message INVITE de remplacement).

I.6.5.2 Composants affectés

Pour ce qui est de permettre à un équipement d'utilisateur d'interfonctionner avec les points d'extrémité qui ne prennent pas en charge l'extension UPDATE SIP, les incidences sont localisées au niveau de l'équipement d'utilisateur proprement dit.

I.6.5.2.1 Equipement d'utilisateur

Un équipement d'utilisateur doit prendre en charge l'extension UPDATE pour les sessions qui sont établies sur la base de préconditions.

Un équipement d'utilisateur peut aussi nécessiter la prise en charge de l'extension UPDATE pour les sessions qui sont établies sans préconditions. Dans ce cas, l'établissement de session avec un autre équipement d'utilisateur qui ne prend pas en charge l'extension UPDATE échouera.

Autre solution: un équipement d'utilisateur peut négocier la prise en charge de l'extension UPDATE pour les sessions qui sont établies sans préconditions. Ainsi, l'extension n'est utilisée que si elle est prise en charge aussi bien par l'équipement d'utilisateur d'origine que par celui de destination.

I.6.5.3 Spécification delta relative au sous-système IMS IPCablecom2

La spécification delta relative au sous-système IMS IPCablecom2 suivante contient les exigences concernant l'extension UPDATE SIP: voir paragraphe 5.1 et Tableau A.4 de [UIT-T J.366.4].

I.6.6 Préconditions SIP

I.6.6.1 Description

La prise en charge de préconditions dans le protocole SIP, comme défini dans [IETF RFC 3312] et mis à jour dans [IETF RFC 4032], est une fonctionnalité facultative de l'architecture de signalisation IPCablecom2. Obligatoires au départ dans le sous-système IMS, les exigences relatives aux préconditions SIP ont été assouplies. Les préconditions SIP ne sont plus obligatoires dans la version 6 du sous-système IMS 3GPP. Les modifications seront incorporées dans la prochaine version des spécifications relatives à la version 6 du sous-système IMS.

I.6.6.2 Composants affectés

Le présent paragraphe décrit les incidences sur les composants de la prise en charge facultative par les équipements d'utilisateur de l'extension relative aux préconditions SIP.

I.6.6.2.1 Equipement d'utilisateur

Les équipements d'utilisateur IPCablecom2 peuvent prendre en charge les préconditions SIP. Si c'est le cas, ils doivent se conformer aux documents [IETF RFC 3312] et [IETF RFC 4032].

L'équipement d'utilisateur IPCablecom2 devrait négocier l'utilisation des préconditions SIP. Il devrait indiquer sa prise en charge des préconditions SIP dans les en-têtes SIP appropriés (Supported et Require) et il devrait être souple pour ce qui est de permettre l'établissement de sessions avec des équipements d'utilisateur qui ne prennent pas en charge les préconditions. Par exemple, un équipement d'utilisateur de destination pour un dialogue SIP devrait inclure l'étiquette d'option "precondition" dans l'en-tête Require si la demande de lancement de dialogue reçue en provenance de l'équipement d'utilisateur d'origine indiquait que les préconditions SIP sont prises en charge avec l'étiquette d'option "preconditions" dans l'en-tête Supported.

I.6.6.3 Spécification delta relative au sous-système IMS IPCablecom2

La spécification delta relative au sous-système IMS IPCablecom2 suivante contient les exigences concernant les préconditions SIP: voir paragraphes 5.1.3, 5.1.4 et 6.1 de [UIT-T J.366.4].

I.6.7 Modificateurs SDP de largeur de bande RTCP

I.6.7.1 Description

Le protocole SDP standard n'offre pas de mécanisme permettant de contrôler explicitement la largeur de bande RTCP, qui est implicitement fixée à 5% de la largeur de bande de session. Le document [IETF RFC 3556] introduit deux nouveaux modificateurs SDP de largeur de bande RTCP, qui peuvent être utilisés pour fixer explicitement la largeur de bande RTCP à une valeur quelconque indépendamment de la largeur de bande de la session RTP. Le sous-système IMS utilise ce mécanisme pour limiter la largeur de bande RTCP à une valeur inférieure à 5% (éventuellement zéro) dans les déploiements dans lesquels les ressources d'accès radioélectrique sont rares et onéreuses.

Etant donné que les restrictions en matière de largeur de bande applicables à l'accès radioélectrique ne s'appliquent pas à l'accès large bande câblé, il n'est pas nécessaire de limiter la largeur de bande RTCP à une valeur inférieure à la valeur par défaut de 5% dans le réseau d'accès IPCablecom. Toutefois, il est utile qu'un équipement d'utilisateur IPCablecom2 prenne en charge ces modificateurs de largeur de bande lorsqu'il les reçoit d'un équipement d'utilisateur IMS afin d'éviter de dépasser l'attribution de largeur de bande RTCP dans le réseau d'accès radioélectrique IMS. Par conséquent, la prise en charge des modificateurs de largeur de bande RTCP est facultative pour les équipements d'utilisateur IPCablecom2.

I.6.7.2 Composants affectés

Le présent paragraphe décrit les incidences sur les composants de la prise en charge facultative par les équipements d'utilisateur des modificateurs de largeur de bande RTCP.

I.6.7.2.1 Equipement d'utilisateur

La prise en charge du document [IETF RFC 3556] est facultative pour les équipements d'utilisateur IPCablecom2 déployés dans un réseau d'accès large bande câblé.

I.6.7.3 Spécification delta relative au sous-système IMS IPCablecom2

La spécification delta relative au sous-système IMS IPCablecom2 suivante contient les exigences concernant les modificateurs SDP de largeur de bande RTCP:

voir paragraphe 6 de [UIT-T J.366.4].

I.6.8 Paquetage d'événement d'état d'enregistrement

Le paquetage d'événement SIP d'état d'enregistrement est une fonction facultative des équipements d'utilisateur IPCablecom2.

I.6.8.1 Description

Lorsqu'un équipement d'utilisateur mène à bien son enregistrement initial, un état d'enregistrement est créé dans un serveur d'enregistrement SIP (fonction S-CSCF), avec la liste des identificateurs URI associés à l'identité d'utilisateur publique qui a été enregistrée. Cette liste contient l'identité d'utilisateur publique qui a été enregistrée explicitement (sauf si elle est interdite), l'ensemble associé d'identités d'utilisateur publiques enregistrées implicitement et éventuellement d'autres identités d'utilisateur publiques associées.

L'état d'enregistrement d'un identificateur URI de la liste peut être modifié dynamiquement, pour diverses raisons, notamment:

- désenregistrement à l'initiative du réseau: conformément à la politique de l'administrateur local, le réseau peut désenregistrer une identité d'utilisateur publique. Cela peut par exemple se produire lorsque des factures ne sont pas réglées;

- nouvelle authentification à l'initiative du réseau: conformément à la politique de l'administrateur local, le réseau peut réduire la durée de validité d'un enregistrement en cours, afin de forcer l'équipement d'utilisateur à procéder à une nouvelle authentification. Cela peut par exemple se produire lorsqu'une fraude est détectée;
- enregistrement à partir de plusieurs dispositifs: les adresses de contact liées à un identificateur URI quelconque de la liste peuvent changer, en raison d'enregistrements à partir d'autres dispositifs.

Conformément aux procédures d'enregistrement IMS, l'équipement d'utilisateur est tenu de s'abonner aux informations d'état d'enregistrement après avoir mené à bien l'enregistrement initial et de conserver cet abonnement jusqu'à ce que tous les identificateurs URI de la liste soient passés à l'état désenregistré. Cet abonnement permet au serveur d'enregistrement SIP de notifier à l'équipement d'utilisateur des événements comme les changements d'état d'enregistrement (de "actif" à "terminé"), la réduction de validité d'un enregistrement et les modifications des liens concernant les adresses de contact.

I.6.8.2 Composants affectés

Le présent paragraphe décrit les incidences sur les composants de la prise en charge facultative par les équipements d'utilisateur du paquetage Reg Event.

I.6.8.2.1 Equipement d'utilisateur

La prise en charge de [IETF RFC 3680] est facultative pour les équipements d'utilisateur IPCablecom2. Si un équipement d'utilisateur ne prend pas en charge le paquetage d'événement d'état d'enregistrement décrit dans [IETF RFC 3680], il n'exécute pas les procédures définies dans [UIT-T J.366.4] concernant l'abonnement aux informations d'état d'enregistrement et la notification de ces informations.

Les principales incidences de l'absence de prise en charge du document [IETF RFC 3680] sont les suivantes:

- l'équipement d'utilisateur ne reçoit pas d'indication explicite que des AOR supplémentaires sont enregistrés implicitement, sauf s'il prend en charge l'en-tête P-Associated-URI facultatif (voir § I.6.12);
- l'équipement d'utilisateur peut passer à l'état désenregistré sans en avoir connaissance. Si cela se produit, l'équipement d'utilisateur ne pourra plus recevoir de demandes et la plupart des demandes autres que REGISTER qu'il enverra seront éliminées ou rejetées par la fonction P-CSCF suivant si une association de sécurité existait ou non (voir § I.6.1).

Si l'équipement d'utilisateur détermine qu'il a été désenregistré (par exemple une demande qu'il a envoyée expire ou est rejetée avec un code d'erreur approprié), il devrait tenter une reprise au moyen de procédures propres à la mise en œuvre. Par exemple, il pourrait exécuter les procédures de désenregistrement à l'initiative du réseau décrites dans [UIT-T J.366.4].

Si l'équipement d'utilisateur prend en charge le paquetage d'événement d'état d'enregistrement, il devrait aussi prendre en charge l'en-tête P-Associated-URI afin de déterminer si l'identité d'utilisateur publique utilisée pour l'enregistrement est interdite (voir § I.6.12.2.1).

I.6.8.2.2 Fonction P-CSCF

Il n'a y pas d'incidence sur la fonction P-CSCF. Dans le sous-système IMS, il est déjà possible (par exemple en tant que cas anormal) que la fonction P-CSCF reçoive de l'équipement d'utilisateur des demandes qui sont passées sans le savoir à l'état désenregistré. Le nombre de ces demandes peut augmenter si le réseau IPCablecom2 exécute à son initiative un désenregistrement ou une nouvelle authentification et qu'il existe des équipements d'utilisateur qui ne prennent pas en charge le paquetage d'événement d'état d'enregistrement.

I.6.9 Portabilité de numéro

I.6.9.1 Description

L'architecture IPCablecom prend en charge la portabilité locale des numéros et le routage opérateur avec accès équitable. Le présent paragraphe décrit comment les données relatives à la portabilité de numéro et au routage opérateur sont obtenues et utilisées dans un réseau IPCablecom2.

Pour prendre en charge la portabilité locale des numéros (LNP) le réseau IPCablecom2 devrait déterminer, au moment approprié, si le numéro appelé est porté ou non. Si le numéro appelé est porté vers une destination dans le RTPC, le réseau IPCablecom2 devrait appliquer la politique de routage sur la base du numéro de routage LNP et il doit transmettre le numéro de routage et l'indicateur de recherche de base de données LNP au RTPC. Le mécanisme d'obtention des données LNP sort du cadre du présent appendice et peut varier en fonction du composant IPCablecom2 qui obtient ces données.

Les procédures IMS existantes définissent que la fonction S-CSCF résout un identificateur URI téléphonique contenant une adresse E.164 en un identificateur URI SIP au moyen d'un mécanisme ENUM/DNS. Dans l'architecture IPCablecom2, on suppose que pour la résolution d'un tel identificateur URI téléphonique en un identificateur URI SIP, aucune interrogation LNP n'est requise par le réseau IPCablecom2. Dans ce cas, le routage de la demande peut se faire sur la base de l'identificateur URI SIP. On suppose en réalité que le serveur ENUM/DNS contenant le mappage entre l'adresse E.164 et l'identificateur URI SIP est synchronisé avec les procédures de portage LNP. Les procédures/mécanismes applicables à cette synchronisation sortent du cadre du présent appendice.

Lorsqu'un identificateur URI téléphonique contenant un numéro E.164 ne peut pas être résolu en un identificateur URI SIP, le réseau IPCablecom2 devra obtenir les données LNP relatives au numéro appelé, lorsque c'est nécessaire (par exemple, si la demande doit être acheminée à un opérateur intercentraux, il n'est pas nécessaire que le réseau IPCablecom2 effectue l'interrogation. En revanche, c'est l'opérateur "N – 1" qui devrait généralement effectuer l'interrogation).

Par défaut, lorsque l'interrogation LNP est requise, elle est effectuée par le contrôleur MGC, si aucune interrogation LNP n'a encore été effectuée pour la demande. (Il est à noter que, étant donné que seul le portage "local" est pris en charge, il est raisonnable d'estimer que la demande sera normalement acheminée à un contrôleur MGC capable de procéder à un routage approprié sur la base des résultats d'une interrogation).

La fonction S-CSCF peut aussi prendre en charge des capacités LNP. Si c'est le cas, la nécessité ou l'absence de nécessité d'utilisation de ces capacités devrait être configurable, une certaine souplesse étant alors offerte quant à l'endroit où l'interrogation LNP est effectuée. Les mécanismes permettant à une fonction S-CSCF d'obtenir des données LNP sort du cadre du présent appendice. Ils pourraient inclure des mécanismes fondés sur ENUM, y compris des mécanismes d'obtention des données LNP à partir de la demande de résolution d'adresse E.164 en un identificateur URI SIP. Ces mécanismes font l'objet de documents IEFT Internet Draft en cours d'évolution. Les politiques de routage à appliquer dans le cas où la fonction S-CSCF résout un identificateur URI téléphonique en un identificateur URI SIP et obtient les données LNP associées à l'identificateur URI téléphonique, sortent du cadre du présent appendice.

Pour prendre en charge le routage opérateur avec accès équitable, le réseau IPCablecom2 choisit la route à destination du RTPC sur la base de l'opérateur qui correspond au numéro composé ou qui a fait l'objet d'un abonnement préalable et transmet l'identificateur d'opérateur et l'indicateur de numérotation ouverte au RTPC. Il s'ensuit que l'identificateur URI téléphonique devrait inclure les paramètres "cic" et "dai", de sorte que le contrôleur MGC puisse choisir le groupe de circuits correct et qu'il puisse aussi transmettre l'identificateur d'opérateur et l'indicateur de numérotation ouverte au RTPC.

Il est à noter que, dans l'architecture IPCablecom2 actuelle, il n'est pas exigé de prendre en charge l'abonnement préalable à un opérateur abonné par abonné. En revanche, un opérateur peut faire l'objet d'un abonnement préalable pour tous les abonnés d'un réseau. La fonction BGCF peut prendre en charge l'ajout de l'opérateur attribué au réseau dans l'identificateur URI téléphonique via le paramètre "cic" ainsi que la mise à jour du paramètre "dai". En cas de prise en charge, la fonction BGCF ajoute ces paramètres sur la base de la configuration/politique de routage. Il est à noter que ces paramètres ont déjà pu être ajoutés par un composant de réseau précédent et, dans ce cas, ne devraient pas être annulés et remplacés par la fonction BGCF.

Les tâches suivantes liées à l'accès équitable relèvent d'un serveur d'application:

- fixer/régler l'indicateur de numérotation ouverte pour un identificateur d'opérateur fourni par un équipement d'utilisateur dans une demande;
- obtenir l'identificateur d'opérateur pour les communications libre appel;
- indiquer l'opérateur et l'indicateur de numérotation ouverte pour un opérateur faisant l'objet d'un abonnement préalable, lorsqu'un tel opérateur a été configuré pour un abonné particulier.

  NOTE – Comme indiqué précédemment, cette configuration n'est pas exigée actuellement, mais si elle devait l'être, elle pourrait être prise en charge de cette façon.

L'architecture IPCablecom2 prend en charge les exigences relatives à la portabilité de numéro et au routage opérateur au moyen de paramètres LNP et de routage opérateur dans l'identificateur URI téléphonique ainsi que du paramètre d'indication de numérotation ouverte défini dans [UIT-T J.178].

I.6.9.2 Composants affectés

Pour la prise en charge de la portabilité de numéro et du routage opérateur, des informations de portabilité de numéro doivent être transportées dans le cadre de la signalisation SIP. En particulier, l'identificateur URI téléphonique doit inclure les paramètres "rn", "cic" et "npdi" ainsi que le paramètre "dai" défini dans [UIT-T J.178]. Ces informations sont utilisées par les proxys de routage (par exemple la fonction BGCF) pour choisir le point d'échappement correct vers le RTPC et par la passerelle de RTPC, pour communiquer les informations de routage correctes au RTPC. Ces paramètres peuvent être acheminés dans un identificateur URI téléphonique d'origine ou dans l'équivalent SIP d'un identificateur URI téléphonique dans le cas user=phone.

I.6.9.2.1 Equipement d'utilisateur

Pour le routage opérateur, la seule tâche de l'équipement d'utilisateur consiste à indiquer au réseau un opérateur correspondant au numéro composé par l'utilisateur pour un appel dont il est à l'origine. Pour cela, l'équipement d'utilisateur reconnaît les chiffres d'opérateur composés par l'utilisateur fournis via un script de numérotation et indique l'opérateur dans le paramètre "cic" de l'identificateur URI téléphonique du message INVITE d'origine.

Autre solution: le script de numérotation peut spécifier que l'équipement d'utilisateur doit communiquer tous les chiffres composés, y compris les chiffres d'opérateur, dans un identificateur URI SIP avec le paramètre "user=dialstring". Dans le cadre de cette solution, un serveur d'application serait tenu d'extraire le code CIC et de normaliser l'identificateur URI téléphonique.

Les mécanismes de configuration du script de numérotation pour commander le comportement de l'équipement d'utilisateur sortent du cadre du présent appendice.

L'équipement d'utilisateur ne joue aucun autre rôle concernant la portabilité de numéro.

I.6.9.2.2 Fonction S-CSCF

Comme spécifié dans [UIT-T J.366.4] lorsque la fonction S-CSCF d'origine reçoit une demande contenant un identificateur URI téléphonique, elle doit tenter de résoudre l'adresse E.164 en un

identificateur URI SIP routable à l'échelle mondiale au moyen de ENUM. Si la résolution échoue, la fonction S-CSCF suppose que l'appel est destiné au RTPC et retransmet le message INVITE à la fonction BGCF pour la poursuite du routage.

Dans l'architecture IPCablecom2, ces exigences sont modifiées afin de prendre en charge la portabilité de numéro. La fonction S-CSCF peut prendre en charge des capacités de portabilité de numéro. Si c'est le cas, elle devrait être dotée de commandes de configuration permettant à l'opérateur d'activer ou de désactiver les procédures de portabilité de numéro. Ainsi, l'opérateur pourra choisir si l'interrogation LNP est effectuée par la fonction S-CSCF ou par une entité aval (contrôleur MGC ou RTPC par exemple).

Si la fonction S-CSCF a été configurée pour prendre en charge la portabilité de numéro, alors après avoir déterminé qu'un appel est destiné au RTPC, la fonction S-CSCF d'origine doit déterminer si le numéro appelé est porté ou non et, si c'est le cas, elle doit ensuite déterminer le numéro de routage réel. La façon dont la fonction S-CSCF obtient ces informations n'est pas spécifiée (par exemple, par le biais d'une interrogation ENUM). Si le numéro est porté, la fonction S-CSCF d'origine doit ajouter un paramètre "rn" à l'identificateur URI téléphonique de la demande pour identifier le numéro de routage et ajouter un paramètre "npdi" pour indiquer que la recherche de base de données LNP a été effectuée.

Si la fonction S-CSCF est configurée de manière à ne pas prendre en charge la portabilité de numéro, elle retransmettra à la fonction BGCF les demandes destinées au RTPC sans remplir les paramètres de portabilité de numéro de l'identificateur URI téléphonique.

Les politiques et les procédures applicables aux scénarios dans lesquels une tentative de résolution d'une adresse E.164 en un identificateur URI SIP permet d'obtenir à la fois un identificateur URI SIP et un identificateur URI téléphonique avec des informations de portabilité de numéro (si cela est possible avec certains mécanismes) sortent du cadre du présent appendice.

I.6.9.2.3 Fonction BGCF

La fonction BGCF reçoit des demandes INVITE provenant de la fonction S-CSCF et choisit la meilleure route vers le RTPC compte tenu de la politique de routage configurée localement. Comme spécifié dans [UIT-T J.366.4], la décision de routage est fondée sur le numéro de téléphone appelé indiqué dans l'identificateur URI téléphonique figurant dans la demande INVITE. Dans l'architecture IPCablecom2, les exigences de routage sont modifiées afin d'inclure les paramètres "cic" et "rn" dans l'identificateur URI téléphonique. Il s'ensuit que la fonction BGCF peut utiliser ces paramètres dans la décision de routage. La façon dont ces paramètres influent sur le routage n'est pas spécifiée.

La fonction BGCF peut prendre en charge l'ajout des paramètres "cic" et "dai" dans l'identificateur URI téléphonique, afin de prendre en charge l'abonnement préalable à un opérateur dans l'ensemble d'un réseau. L'ajout de ces paramètres est fondé sur la politique de routage. Les attributs de la demande acheminée permettent de déterminer si un paramètre "cic" est ajouté. Ces paramètres ont pu déjà être ajoutés à la demande par un autre composant de réseau, auquel cas la fonction BGCF ne doit pas les annuler et les remplacer.

I.6.9.2.4 Contrôleur MGC

Le contrôleur MGC reçoit des demandes provenant de la fonction BGCF à acheminer au RTPC ou provenant du RTPC à acheminer dans le réseau IPCablecom.

Les demandes provenant de la fonction BGCF peuvent comporter un identificateur URI téléphonique contenant les paramètres d'opérateur ("cic") et/ou de portabilité de numéro ("npdi", "rn"). Les demandes provenant du RTPC peuvent aussi contenir des paramètres de portabilité de numéro.

Le contrôleur MGC déterminera s'il convient d'effectuer une interrogation LNP sur la base de la configuration locale et du contenu de la demande, y compris des paramètres de portabilité de numéro reçus.

La politique de routage du contrôleur MGC est fondée sur les paramètres d'opérateur et de portabilité de numéro. Les détails de cette politique sortent du cadre du présent appendice.

I.6.10 Identificateur URI d'agent d'utilisateur routable à l'échelle mondiale (GRUU)

I.6.10.1 Description

La prise en charge de l'identificateur URI d'agent d'utilisateur routable à l'échelle mondiale (GRUU) SIP est facultative pour l'équipement d'utilisateur dans l'architecture SIP IPCablecom2. L'identificateur GRUU est utile dans l'architecture IPCablecom2; il permet en effet, dans le cadre de certaines fonctionnalités d'appel (transfert d'appel par exemple), d'adresser précisément des demandes SIP à une instance d'agent d'utilisateur SIP particulière d'un équipement d'utilisateur. Il permettra aussi une application précise de fonctionnalités à définir aux demandes destinées à une instance d'agent d'utilisateur SIP particulière d'un équipement d'utilisateur plutôt qu'une application générale de ces fonctionnalités à une identité d'utilisateur publique. Par exemple, lorsqu'une demande est adressée à un équipement d'utilisateur particulier via un identificateur GRUU, il peut être souhaitable de s'abstenir d'adresser à nouveau la demande à une messagerie vocale.

I.6.10.2 Composants affectés

Le présent paragraphe décrit les incidences sur les composants de la prise en charge de l'identificateur GRUU.

I.6.10.2.1 Equipement d'utilisateur

Un équipement d'utilisateur IPCablecom2 prenant en charge l'identificateur GRUU devra se conformer aux exigences et lignes directrices relatives à l'agent d'utilisateur qui sont en cours d'élaboration.

- l'équipement d'utilisateur doit demander un identificateur GRUU au moment de son enregistrement et extraire et conserver l'identificateur GRUU fourni dans la réponse d'enregistrement;
- si l'identité d'utilisateur publique enregistrée fait partie d'un ensemble d'identités enregistrées implicitement, l'équipement d'utilisateur doit aussi obtenir et conserver l'identificateur GRUU pour chaque identité d'utilisateur publique enregistrée implicitement. (Voir le § I.6.10.3 pour plus d'informations).

Lors de l'envoi de demandes ou de réponses SIP nécessitant une adresse de contact, l'équipement d'utilisateur devrait utiliser un identificateur GRUU et non l'identificateur URI de contact qu'il a enregistré.

- En particulier, l'équipement d'utilisateur doit utiliser comme adresse de contact l'identificateur GRUU conservé correspondant lorsqu'il envoie des demandes SIP avec un en-tête "From" contenant une identité d'utilisateur publique enregistrée.
- L'équipement d'utilisateur doit aussi utiliser comme adresse de contact l'identificateur GRUU conservé correspondant lorsqu'il répond à des demandes SIP dans lesquelles l'en-tête P-called-party contient une identité d'utilisateur publique enregistrée implicitement.

I.6.10.2.2 Fonction S-CSCF

La fonction S-CSCF doit être capable de répondre aux demandes d'enregistrement dans lesquelles il est demandé de retourner des identificateurs GRUU. Dans ce cas, cette fonction doit élaborer et retourner un identificateur GRUU qui est lié à l'identité d'utilisateur publique et à l'identificateur d'instance fournies.

En plus de la réponse aux demandes adressées aux identités d'utilisateur publiques dont elle est responsable, une fonction S-CSCF doit aussi répondre aux demandes adressées à n'importe quel identificateur GRUU qui a été précédemment attribué à une identité d'utilisateur publique dont elle est responsable. Cela reste valable même lorsque la responsabilité d'une identité d'utilisateur publique est transférée d'une fonction S-CSCF à une autre.

Par convention, le format de l'identificateur GRUU pour l'architecture IPCablecom2 est défini comme suit:

- l'identificateur GRUU associé à une identité d'utilisateur publique dans le format SIP ou SIPS est l'identificateur URI correspondant à l'identité d'utilisateur publique avec, en plus, un paramètre URI 'gruu' et un paramètre 'opaque';
- pour un identificateur URI contenant un numéro de téléphone, un identificateur GRUU peut être demandé sur la base d'un identificateur URI SIP qui inclut un numéro de téléphone correctement formaté dans la partie utilisateur ainsi que le nom de domaine du fournisseur et un paramètre 'user=phone'. En réalité, un identificateur GRUU ne peut pas être demandé pour une identité d'utilisateur publique figurant dans un identificateur URI téléphonique car un tel identificateur URI ne peut pas être enregistré. L'identificateur GRUU résultant peut être utilisé à la fois pour une identité d'utilisateur publique de type SIP et pour une identité d'utilisateur publique de type téléphonique;
- le paramètre 'opaque' de l'identificateur GRUU retourné par la fonction S-CSCF est constitué d'un nom de paramètre 'opaque=' suivi par une valeur identique à la valeur du paramètre 'sip.instance' fourni par l'équipement d'utilisateur dans la demande REGISTER.

Lorsqu'une demande est adressée à un identificateur GRUU, le profil d'utilisateur doit pouvoir déterminer les services qui doivent être appliqués à la demande suivant si la cible de la demande est un identificateur GRUU, ou une identité d'utilisateur publique. Pour cela, on peut avoir recours à un déclencheur de point de service (SPT, *service point trigger*), qui détermine si l'identificateur URI de la demande contient ou non un paramètre URI 'gruu'.

Comme décrit dans la spécification GRUU, lorsqu'une demande SIP est adressée à un identificateur URI de type GRUU, la logique de routage est dictée par le fait que ce soit un identificateur GRUU. Par conséquent, la logique de la fonction S-CSCF pour la traduction de l'identificateur URI d'une demande est différente pour un identificateur GRUU et pour une identité d'utilisateur publique. Pour un identificateur GRUU, la seule cible possible est un contact enregistré avec l'identité d'utilisateur publique et l'identificateur d'instance associés à l'identificateur GRUU.

I.6.10.3 Spécification delta relative au sous-système IMS IPCablecom2

Les spécifications delta relatives au sous-système IMS IPCablecom2 suivantes contiennent les exigences concernant l'identificateur URI d'agent d'utilisateur routable à l'échelle mondiale (GRUU): Recommandations UIT-T J.366.2, J.366.3, [UIT-T J.366.4] et [UIT-T J.366.5].

I.6.11 Extension du paquetage d'événement d'état d'enregistrement pour les identificateurs GRUU

I.6.11.1 Description

Des extensions supplémentaires sont définies pour prendre en charge l'acheminement des identificateurs GRUU dans le paquetage d'événement d'enregistrement SIP. L'extension du paquetage d'événement d'enregistrement pour les identificateurs GRUU doit être prise en charge si les identificateurs GRUU sont pris en charge par les éléments IPCablecom2 (équipement d'utilisateur, fonction S-CSCF et serveur HSS). Dans le cas contraire, la prise en charge de cette extension est facultative dans l'architecture de signalisation SIP IPCablecom2.

La prise en charge de l'extension du paquetage Reg-event pour les identificateurs GRUU est facultative dans l'architecture de signalisation SIP IPCablecom2. Cette extension complète par un

identificateur GRUU les informations fournies par le paquetage Reg-event si un tel identificateur est attribué pour un contact enregistré.

Cette fonctionnalité est incluse dans l'architecture IPCablecom2 car elle permet à un équipement d'utilisateur d'obtenir tous les identificateurs GRUU associés à un ensemble d'identités enregistrées implicitement. De fait, lorsqu'un équipement d'utilisateur s'enregistre et demande l'attribution d'un identificateur GRUU, la réponse contiendra l'identificateur GRUU correspondant à l'identité d'utilisateur publique qui a été enregistrée. Toutefois, si l'identité d'utilisateur publique fait partie d'un ensemble d'identités enregistrées implicitement, des enregistrements du même contact sont faits pour chacune des identités d'utilisateur publiques. Chacun se traduit par l'attribution d'un identificateur GRUU distinct, mais il est impossible d'obtenir ces identificateurs GRUU dans la réponse à la demande REGISTER. Si l'équipement d'utilisateur est abonné au paquetage d'événement d'enregistrement, l'inclusion de l'extension du paquetage d'événement d'enregistrement pour les identificateurs GRUU signifie que l'équipement d'utilisateur recevra les identificateurs GRUU associés à un ensemble d'identités enregistrées implicitement dans une notification.

I.6.11.2 Composants affectés

Le présent paragraphe décrit les incidences sur les composants de la prise en charge facultative par les équipements d'utilisateur de l'extension du paquetage Reg-event pour les identificateurs GRUU.

I.6.11.2.1 Equipement d'utilisateur

Si un équipement d'utilisateur est abonné au paquetage Reg-event et reçoit ensuite une notification indiquant qu'un enregistrement implicite s'est produit pour un contact que l'équipement d'utilisateur a enregistré, l'équipement d'utilisateur doit conserver l'identificateur GRUU provenant de la notification pour utilisation future. La manière d'utiliser cet identificateur fait l'objet du § I.6.10.

I.6.11.2.2 Fonction S-CSCF

Lorsqu'elle envoie une notification concernant le paquetage Reg-Event, la fonction S-CSCF doit utiliser ce paquetage et inclure les identificateurs GRUU attribués aux différents contacts enregistrés.

I.6.11.3 Spécification delta relative au sous-système IMS IPCablecom2

La spécification delta relative au sous-système IMS IPCablecom2 suivante contient les exigences concernant l'extension du paquetage d'événement d'état d'enregistrement pour les identificateurs GRUU: [UIT-T J.366.4].

I.6.12 En-têtes 3GPP privés

Un ensemble d'en-têtes SIP privés à utiliser par le 3GPP sont décrits dans [IETF RFC 3455]. Parmi ces en-têtes, il existe deux en-têtes P dont les spécifications applicables dans l'architecture IPCablecom2 diffèrent de celles qui s'appliquent dans le sous-système IMS.

NOTE – Les en-têtes P décrits dans le document [IETF RFC 3455] qui ne sont pas indiqués dans le présent paragraphe sont pris en charge par l'architecture IPCablecom2 sans modification.

I.6.12.1 Description

I.6.12.1.1 En-tête P-Associated-URI

L'en-tête P-Associated-URI est reçu par l'équipement d'utilisateur dans la réponse 200 (OK) à une demande REGISTER. Conformément à [UIT-T J.366.4], il contient l'identité d'utilisateur publique enregistrée et l'ensemble associé d'identités d'utilisateur publiques enregistrées implicitement.

NOTE – Cela diffère de la description contenue dans le document [IETF RFC 3455].

Conformément aux procédures d'enregistrement IMS, l'équipement d'utilisateur est tenu de prendre en charge cet en-tête, qui lui donne les informations suivantes:

- l'ensemble des identités d'utilisateur publiques enregistrées implicitement;
- l'identité d'utilisateur publique par défaut, qui sera validée par la fonction P-CSCF dans les le cadre des procédures relatives à l'en-tête P-Asserted-Identity si l'équipement d'utilisateur n'inclut pas d'en-tête P-Preferred-Identity ou n'inclut pas d'identité d'utilisateur publique enregistrée dans l'en-tête P-Preferred-Identity;
- autorisation ou interdiction de l'identité d'utilisateur publique utilisée pour l'enregistrement, étant donné que les identités interdites ne sont pas incluses dans l'en-tête P-Associated-URI.

Dans l'architecture IPCablecom2, la prise en charge de l'en-tête P-Associated-URI est facultative pour l'équipement d'utilisateur.

I.6.12.1.2 En-tête P-Access-Network-Info

Conformément au sous-système IMS, l'en-tête P-Access-Network-Info doit être inclus par l'équipement d'utilisateur dans tout message SIP (à quelques exceptions près) envoyé avec protection de l'intégrité. Il identifie la technologie d'accès utilisée pour la connectivité IP (IP-CAN) et il est transmis par la fonction S-CSCF aux serveurs d'application de confiance dans le cadre de l'enregistrement par un tiers.

Ses utilisations potentielles sont notamment les suivantes:

- services d'urgence, comme décrit au § 5.2.10 de [UIT-T J.366.4];
- détermination de la nécessité ou non d'une compression SIP entre l'équipement d'utilisateur et la fonction P-CSCF, comme décrit au § I.6.3;
- optimisation des valeurs des temporisations SIP, comme décrit au § I.6.14;
- optimisation des services compte tenu du type de réseau d'accès.

Dans l'architecture IPCablecom2, l'en-tête P-Access-Network-Info n'est inclus par l'équipement d'utilisateur que si la technologie d'accès est connue.

NOTE – La ou les nouvelles valeurs de type d'accès pour l'architecture IPCablecom2 doivent être enregistrées auprès de l'organisme de normalisation compétent.

I.6.12.2 Composants affectés

Le présent paragraphe décrit les incidences sur les composants de la prise en charge facultative des en-têtes P-Associated-URI et P-Access-Network-Info.

I.6.12.2.1 Equipement d'utilisateur

Si l'équipement d'utilisateur ne prend pas en charge l'en-tête P-Associated-URI, il n'a aucun moyen de savoir si l'identité d'utilisateur qu'il a utilisée pendant l'enregistrement est interdite ou autorisée. Par conséquent, il faut veiller à ce que les équipements d'utilisateur ne prenant pas en charge l'en-tête P-Associated-URI ne s'enregistrent pas avec une identité interdite. Les identités interdites ne sont pas liées aux informations de contact et ne peuvent pas être utilisées pour la validation d'identité. Les principales conséquences de l'absence de prise en charge de l'en-tête P-Associated-URI sont les suivantes:

- l'équipement d'utilisateur ne reçoit pas d'indication explicite que des AOR supplémentaires sont enregistrés implicitement, sauf s'il prend en charge le paquetage d'événement d'état d'enregistrement facultatif (voir § I.6.8);
- si l'identité d'utilisateur publique utilisée pour l'enregistrement est interdite, l'équipement d'utilisateur ne pourra pas mener à bien son abonnement au paquetage d'événement d'état d'enregistrement, s'il n'existe pas d'association de sécurité;

- si une demande est envoyée avec un en-tête P-Preferred-Identity contenant une identité d'utilisateur publique interdite, la fonction P-CSCF l'ignorera et insérera à la place un en-tête P-Asserted-Identity avec une identité d'utilisateur publique par défaut connue.

L'équipement d'utilisateur doit prendre en charge les procédures relatives à l'en-tête P-Access-Network-Info décrites dans [UIT-T J.366.4], moyennant la précision suivante:

- L'en-tête P-Access-Network-Info n'est inséré par l'équipement d'utilisateur que si la technologie du réseau d'accès est connue.

I.6.12.2.2 Fonction P-CSCF

Si la fonction P-CSCF reçoit une demande REGISTER qui ne contient pas d'en-tête P-Access-Network-Info et qu'elle a connaissance de la technologie d'accès utilisée au niveau de l'équipement d'utilisateur, elle insérera l'en-tête P-Access-Network-Info.

NOTE – Etant donné qu'il est possible que l'en-tête P-Access-Network-Info ne soit inséré ni par l'équipement d'utilisateur ni par la fonction P-CSCF (lorsque aucun des deux n'a connaissance de la technologie d'accès), les fonctionnalités et les services qui utilisent cet en-tête doivent gérer de façon appropriée son absence.

I.6.12.2.3 Fonction S-CSCF

Si l'en-tête P-Associated-URI n'est pas pris en charge par l'équipement d'utilisateur et que la sécurité de la signalisation est désactivée ou facultative, la fonction S-CSCF d'origine peut recevoir des demandes autres que REGISTER qui contiennent, dans l'en-tête P-Preferred-Identity et/ou From, une identité d'utilisateur publique interdite. Dans ce cas, la fonction S-CSCF rejettera la demande en produisant une réponse 403 (interdit).

I.6.13 Routage des demandes SUBSCRIBE pour les informations de configuration

I.6.13.1 Description

Les équipements d'utilisateur IPCablecom2 obtiennent des informations de configuration au moyen du protocole SIP en s'abonnant au paquetage d'événement ua-profile. La demande initiale d'abonnement aux informations de configuration est adressée à un identificateur URI de demande spécial qui est propre à un dispositif. L'équipement d'utilisateur élabore cet identificateur à partir d'un identificateur de dispositif qui lui est propre, combiné au nom de domaine du fournisseur. La demande initiale d'abonnement aux informations de configuration doit être acheminée à un élément PAC IPCablecom2 qui est capable de fournir un profil de dispositif approprié pour l'équipement d'utilisateur.

Il est important de distinguer deux catégories d'équipements d'utilisateur pour lesquels les demandes SUBSCRIBE pour les informations de configuration doivent être traitées:

1) les équipements d'utilisateur dont l'identificateur URI de dispositif est connu du système;

2) les équipements d'utilisateur dont l'identificateur URI de dispositif est inconnu du système.

Les procédures décrites ci-dessous permettent un routage correct des demandes SUBSCRIBE pour les informations de configuration dans l'un ou l'autre cas.

Un équipement d'utilisateur ne sait pas nécessairement si son identificateur URI de dispositif est connu ou inconnu du réseau. Si cet identificateur est inconnu, l'équipement d'utilisateur ne pourra pas s'enregistrer. La procédure qui suit fonctionnera dans les deux cas. L'équipement d'utilisateur envoie une demande d'abonnement pour son profil avant de s'enregistrer. Cette demande est adressée à l'identificateur URI propre à un dispositif. Elle inclut un en-tête From contenant cet identificateur URI et devrait inclure un en-tête P-Preferred-Identity contenant aussi cet identificateur. Pour ce faire, l'équipement d'utilisateur suit les procédures du § I.6.1.2.1 qui s'appliquent lorsqu'il n'y a pas d'association de sécurité entre l'équipement d'utilisateur et la fonction P-CSCF et que l'équipement d'utilisateur ne s'est pas enregistré.

Comme l'équipement d'utilisateur ne s'est pas enregistré, la fonction P-CSCF ne dispose d'aucune base pour authentifier la demande. Elle laisse donc l'en-tête P-Preferred-Identity tel quel, reportant l'authentification à un serveur ultérieur. Elle utilise l'en-tête P-Preferred-Identity s'il est présent, ou l'en-tête From si le premier est absent, pour choisir une fonction I-CSCF pour la suite du traitement, et lui transmet la demande.

En l'absence d'en-tête P-Asserted-Identity, la fonction I-CSCF utilise l'en-tête P-Preferred-Identity s'il est présent, ou l'en-tête From si l'en-tête P-Preferred-Identity est également absent, pour déterminer la cible du routage de la demande pour traitement à l'entrée.

Si l'identificateur URI de dispositif est connu, il fera l'objet d'une entrée explicite dans le serveur HSS, en tant qu'identité d'utilisateur publique. La fonction I-CSCF achemine ensuite la demande à la fonction S-CSCF qui dessert cette identité d'utilisateur publique.

L'identificateur URI d'un dispositif inconnu est par définition inconnu du serveur HSS. Aucune entrée correspondante exacte n'est donc présente dans le serveur HSS. Toutefois, lorsqu'on souhaite prendre en charge les dispositifs inconnus, une entrée PSI générique sera présente dans le serveur HSS et correspondra à l'identificateur URI de tous les dispositifs inconnus souhaités. Par exemple, les deux valeurs suivantes peuvent suffire:

sip:MAC%3a!.*!@provider.net

sip:urn%3auuid%3a!.*!@provider.net

L'entrée du serveur HSS devrait indiquer un élément PAC qui gère les demandes d'abonnement provenant de dispositifs inconnus. Ces demandes sont alors routées par la fonction I-CSCF vers ce serveur pour traitement à l'entrée.

L'élément PAC est responsable de l'authentification ou de l'autorisation qu'il choisit de faire pour les dispositifs inconnus. Le serveur choisit alors d'honorer la demande ou de la refuser. Il a été invoqué pour réaliser le traitement à l'entrée, ainsi la demande pourrait devoir être acheminée ailleurs pour le traitement à la sortie. Toutefois, dans l'architecture IPCablecom2, le seul cas applicable est lorsque l'adresse est la même pour l'entrée et la sortie. Ainsi le serveur peut simplement honorer la demande sans autre routage. Il utilise les informations présentes dans la demande d'abonnement (par exemple les informations sur le type de dispositif) pour choisir une configuration par défaut appropriée pour le dispositif – une configuration qui permettra au dispositif d'utiliser n'importe quelles capacités restreintes que le fournisseur peut choisir d'autoriser. Cette configuration n'est généralement destinée à être utilisée que pour la communication initiale suffisante pour établir une relation commerciale entre le fournisseur et l'utilisateur du dispositif, après quoi le dispositif changera de statut et deviendra *connu* du système. Pour plus d'informations, on se reportera à [UIT-T J.364].

I.6.13.2 Composants affectés

Le présent paragraphe décrit les incidences sur les composants de la prise en charge de l'abonnement au paquetage d'événement ua-profile avant l'enregistrement.

I.6.13.2.1 Equipement d'utilisateur

Un équipement d'utilisateur devrait s'abonner au profil de dispositif, en utilisant l'identificateur URI propre à un dispositif, sans commencer par s'enregistrer en utilisant cet identificateur URI. Pour ce faire, il suivra les procédures du § I.6.1.2.1 relatives à la sécurité de la signalisation pour l'équipement d'utilisateur.

I.6.13.2.2 Fonction P-CSCF

Voir le § I.6.1.2.2 concernant la sécurité de la signalisation pour la fonction P-CSCF.

I.6.13.2.3 Fonction I-CSCF

Voir le § I.6.1.2.3 concernant la sécurité de la signalisation pour la fonction I-CSCF.

I.6.13.2.4 Fonction S-CSCF

Voir le § I.6.1.2.4 concernant la sécurité de la signalisation pour la fonction S-CSCF.

I.6.13.2.5 Serveur HSS

Le serveur HSS doit gérer le cas dans lequel un identificateur URI de demande correspond à deux entrées dans le serveur HSS – l'une concernant une identité PSI générique et l'autre une identité d'utilisateur publique. Dans ce cas, l'entrée concernant l'identité d'utilisateur publique l'emporte sur celle concernant l'identité PSI générique.

I.6.13.2.6 Elément PAC

Pour un identificateur URI de dispositif connu, l'élément PAC fera office de serveur d'application de destination pour le compte de l'utilisateur correspondant. La présence d'un en-tête P-Asserted-Identity contenant l'identificateur URI de dispositif permet à l'élément PAC de détecter que le dispositif est connu.

Pour un identificateur URI de dispositif inconnu, l'élément PAC fera office de serveur PSI d'origine. L'absence d'en-tête P-Asserted-Identity permet à l'élément PAC de détecter que le dispositif est inconnu.

I.6.13.3 Spécification delta relative au sous-système IMS IPCablecom2

La spécification delta relative au sous-système IMS IPCablecom2 suivante contient les exigences concernant le routage des demandes SUBSCRIBE pour les informations de configuration: [UIT-T J.366.4].

I.6.14 Temporisations SIP

I.6.14.1 Description

Pour tenir compte des délais de traitement et de transmission à l'interface radioélectrique 3GPP, la version 6 du sous-système IMS 3GPP [UIT-T J.366.4] spécifie un ensemble modifié de valeurs de temporisation SIP (par rapport à l'ensemble défini dans [IETF RFC 3261]) à appliquer par la fonction P-CSCF en direction de l'équipement d'utilisateur et en sens inverse. Pour l'accès large bande, cette spécification ne s'applique pas et les valeurs de temporisation SIP [IETF RFC 3261] standards s'appliquent en principe. Dans le cadre de la prise en charge du "large bande fixe" dans la version 7 du sous-système IMS 3GPP, les équipements d'utilisateur utilisant la technologie d'accès large bande, et une fonction P-CSCF qui interagit avec un équipement d'utilisateur de ce type, utilisent les valeurs de temporisation SIP [IETF RFC 3261] standards.

L'architecture IPCablecom2 incorpore ces modifications des valeurs de temporisation SIP figurant dans la version 7 du sous-système IMS 3GPP.

Cette solution dépend de la spécification d'un nouveau type d'accès pour l'en-tête P-Access-Network-Info, représentant la technologie du réseau d'accès large bande IPCablecom2. Voir le § I.6.12.1.2 pour plus de détails.

Comme l'équipement d'utilisateur et la fonction P-CSCF ont besoin d'utiliser un ensemble cohérent de valeurs de temporisation SIP, si l'équipement d'utilisateur ne fournit pas d'en-tête P-Access-Network-Info, l'équipement d'utilisateur et la fonction P-CSCF utiliseront tous deux les valeurs de temporisation SIP [IETF RFC 3261] standards. Il est à noter qu'il s'agit d'une exigence supplémentaire par rapport aux modifications figurant dans la version 7 du sous-système IMS 3GPP.

Il est à noter que la solution décrite dans la version 7 du sous-système IMS 3GPP pourra faire l'objet d'un complément d'étude dans le cadre du 3GPP afin d'examiner s'il existe de meilleures méthodes pour déterminer les délais au niveau de l'accès et s'il convient de modifier les valeurs de

temporisation SIP. L'architecture IPCablecom2 pourra ensuite être modifiée afin de tenir compte des futures modifications qui pourront être apportées dans ce domaine.

I.6.14.2 Composants affectés

Les modifications requises sont identifiées et incorporées dans la version 7.

Il existe une exigence supplémentaire: étant donné que l'équipement d'utilisateur et la fonction P-CSCF ont besoin d'utiliser un ensemble cohérent de valeurs de temporisation SIP, si l'équipement d'utilisateur ne fournit pas d'en-tête P-Access-Network-Info, l'équipement d'utilisateur et la fonction P-CSCF utiliseront les valeurs de temporisation SIP [IETF RFC 3261] standards.

I.6.14.2.1 Equipement d'utilisateur

Seuls les équipements d'utilisateur utilisant la technologie d'accès sans fil 3GPP utilisent les valeurs de temporisation SIP modifiées dans le cadre du 3GPP. Les autres équipements d'utilisateur utilisent les valeurs de temporisation SIP [IETF RFC 3261] standards.

I.6.14.2.2 Fonction P-CSCF

La fonction P-CSCF applique les valeurs de temporisation SIP modifiées dans le cadre du 3GPP en direction des équipements d'utilisateur qui utilisent des technologies d'accès sans fil 3GPP. Pour les équipements d'utilisateur utilisant d'autres technologies d'accès, la fonction P-CSCF applique les valeurs de temporisation SIP [IETF RFC 3261] standards. La fonction P-CSCF détermine les valeurs à appliquer sur la base du type d'accès indiqué dans l'en-tête P-Access-Network-Info. Lorsque l'équipement d'utilisateur ne fournit pas d'en-tête P-Access-Network-Info, les valeurs de temporisation [IETF FC 3261] standards s'appliquent.

I.6.14.3 Spécification delta relative au sous-système IMS IPCablecom2

La spécification delta relative au sous-système IMS IPCablecom2 suivante contient les exigences concernant les temporisations SIP: voir paragraphe 7.7 de [UIT-T J.366.4].

I.6.15 Modifications générales

I.6.15.1 Description

Le présent paragraphe décrit un certain nombre de modifications diverses du sous-système IMS afin de respecter les exigences IPCablecom2, y compris des précisions terminologiques, et la prise en charge des deux adressages IPv4 et IPv6.

- La terminologie employée dans [UIT-T J.366.4] se rapporte parfois à une technologie d'accès particulière. Les termes "en provenance d'un mobile", "à destination d'un mobile " et "à l'initiative d'un mobile" sont employés dans l'ensemble du document TS 24.229. Dans le cadre de la prise en charge du "large bande fixe" dans la version 7 du sous-système IMS 3GPP, la terminologie employée dans la spécification 3GPP [UIT-T J.366.4] a été modifiée, les termes "en provenance d'un équipement d'utilisateur", "à destination d'un équipement d'utilisateur" et "à l'initiative d'un équipement d'utilisateur" étant désormais employés. Dans l'architecture IPCablecom2, ce changement de terminologie est implicitement adopté.
- [UIT-T J.366.4] spécifie des procédures permettant de déterminer l'identité publique, l'identité privée et le nom de domaine du réseau domestique lorsque l'équipement d'utilisateur contient une carte UICC mais pas de module ISIM. (Voir les § 4.2 et 5.1.1.1A et l'Annexe C de [UIT-T J.366.4].) Il est possible que certains équipements d'utilisateur utilisés dans l'architecture IPCablecom2 ne contiennent ni carte UICC ni module ISIM. Dans ce cas, l'équipement d'utilisateur sera configuré avec les informations requises. Pour plus d'informations concernant ce cas, on se reportera à l'Appendice III.

Il convient d'avoir à l'esprit ce qui suit:

- certaines procédures [UIT-T J.366.4] sont décrites explicitement comme étant applicables à l'accès 3GPP. Elles ne s'appliquent donc pas aux clients large bande. Par exemple le § 5.2.8.1 de "Libération d'appel à l'initiative de la fonction P-CSCF" contient des scénarios liés à la "couverture radioélectrique" et aux "ressources à l'interface radioélectrique".
- [UIT-T J.366.4] contient aussi des annexes qui s'appliquent explicitement à l'accès GPRS. Il va de soi que ces annexes ne s'appliquent pas à l'accès large bande IPCablecom2, les spécifications correspondantes applicables à l'architecture IPCablecom2 pouvant être contenues dans d'autres documents IPCablecom2.

I.6.15.2 Composants affectés

Les modifications à apporter pour remplacer les termes spécifiques par des termes généraux en ce qui concerne l'accès (remplacement de "mobile" par "équipement d'utilisateur") ont été identifiées. Ces modifications, qui permettent d'élargir le domaine d'application de [UIT-T J.366.4], n'ont pas d'incidence sur les procédures. Le présent paragraphe ne contient donc pas de description détaillée des incidences sur chacun des différents composants.

I.6.15.3 Spécification delta relative au sous-système IMS IPCablecom2

Les modifications à apporter pour remplacer les termes spécifiques par des termes généraux en ce qui concerne l'accès (remplacement de "mobile" par "équipement d'utilisateur") sont adoptées implicitement et, dans un souci de simplicité, [UIT-T J.366.4] n'est pas mis à jour pour intégrer ces modifications.

I.6.16 Interfonctionnement avec les versions IPCablecom précédentes

Un équipement d'utilisateur doit pouvoir établir des sessions vocales avec les points d'extrémité conformes aux versions IPCablecom précédentes. Par exemple, les équipements d'utilisateur et les adaptateurs E-MTA appartenant à un même réseau d'opérateur doivent pouvoir s'appeler sans que les appels doivent être routés par le biais d'un autre opérateur IP ou par le biais du RTPC. En outre, les équipements d'utilisateur doivent pouvoir établir des appels à destination de passerelles média TGCP afin d'assurer l'interfonctionnement avec le RTPC.

La commande de service pour les équipements d'utilisateur n'est aucunement intégrée avec la commande de service pour les adaptateurs E-MTA. Pour un équipement d'utilisateur, la commande de service est partagée entre l'équipement d'utilisateur et la fonction S-CSCF qui le dessert ainsi que les serveurs d'application associés. Pour un adaptateur E-MTA, les services sont fournis et commandés par le serveur CMS par le biais de la signalisation NCS. Les équipements d'utilisateur et les adaptateurs E-MTA se voient simplement comme des entités appelables distinctes présentes dans le réseau.

L'établissement d'appels entre les équipements d'utilisateur et les autres points d'extrémité conformes aux versions IPCablecom précédentes est rendu possible par l'interface pkt-sig-2 fondée sur le protocole SIP, qui raccorde les fonctions S-CSCF, I-CSCF et BGCF au serveur CMS et au contrôleur MGC (voir la Figure I.3). Les spécifications applicables au serveur CMS et au contrôleur MGC concernant la prise en charge de cette interface sont définies dans [UIT-T J.178].

Appendice II

Aperçu technique de l'architecture de qualité de service

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

II.1 Introduction

Le présent appendice contient un aperçu de l'architecture de qualité de service (QS) IPCablecom2. En particulier, il décrit l'utilisation qui est faite de l'architecture IPCablecom multimédia pour assurer des applications de qualité de service élaborées sur la base de l'architecture IPCablecom. Pour aider le lecteur à comprendre l'architecture de qualité de service IPCablecom2, le présent appendice énonce les exigences de haut niveau et décrit les composants logiques et interfaces spécifiques qui sont définis.

II.1.1 Aperçu de l'architecture IPCablecom multimédia

L'architecture IPCablecom multimédia définit une plate-forme IP permettant de fournir des services multimédias avec une qualité de service améliorée sur des réseaux d'accès DOCSIS de version 1.1 (UIT-T J.112) ou supérieure (dans le reste du présent document, le terme DOCSIS renvoie à des réseaux DOCSIS de version 1.1 ou supérieure). Cette plate-forme s'appuie sur les capacités de base de l'architecture IPCablecom (par exemple, autorisation et contrôle d'admission fondés sur la qualité de service, messages d'événement pour la facturation et autres fonctions d'arrière et sécurité) pour prendre en charge un large éventail de services IP en plus de la téléphonie. En d'autres termes, tandis que l'architecture IPCablecom est personnalisée pour la fourniture de services de téléphonie aux particuliers, l'architecture IPCablecom multimédia constitue une plate-forme polyvalente qui permet aux câblo-opérateurs de fournir différents services multimédias IP nécessitant un traitement de la qualité de service. C'est pourquoi aucun service spécifique n'est défini ni examiné.

Bien que la plate-forme IPCablecom multimédia repose sur l'architecture IPCablecom, il n'est pas indispensable de disposer de l'infrastructure de communication vocale complète définie dans le cadre de cette architecture pour déployer des services multimédias. Au contraire, l'objectif est qu'un câblo-opérateur donné puisse choisir de déployer au départ des services vocaux ou des services multimédias tout en étant assuré que ces plates-formes s'intégreront et interfonctionneront de façon transparente si elles sont déployées en parallèle.

II.2 Références

Le présent appendice utilise les références informatives supplémentaires ci-après:

[UIT-T J.163] Recommandation UIT-T J.163 (2005), *Qualité de service dynamique pour la fourniture de services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems*.

[UIT-T J.179 App.I] Recommandation UIT-T J.179 (2005), *Prise en charge du multimédia par IPCablecom. Appendice I: Informations de base*.

[UIT-T J.179] Recommandation UIT-T J.179 (2005), *Prise en charge du multimédia par IPCablecom*.

[UIT-T J.362] Recommandation UIT-T J.362 (2006), *Découverte de point de contrôle IPCablecom2*.

[UIT-T J.365] Recommandation UIT-T J.365 (2006), *Interface de gestion des applications IPCablecom2*.

[UIT-T J.366.4] Recommandation UIT-T J.366.4 (2006), *IPCablecom2 IP Multimedia Subsystem (IMS): Session Initiation Protocol (SIP) and Session Description Protocol (SDP) – Stage 3 Specification.* (3GPP TS 24.229)

[IETF RFC 3264] IETF RFC 3264 (2002), *An Offer/Answer Model with the Session Description Protocol (SDP)*.

[IETF RFC 3890] IETF RFC 3890 (2004), *A Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP)*.

II.3 Termes et définitions

Le présent appendice utilise les termes supplémentaires ci-après:

II.3.1 version 6 du sous-système IMS: Série de spécifications du sous-système multimédia IP 3GPP – Version 6 approuvée.

II.4 Abréviations et acronymes

Le présent appendice utilise les abréviations supplémentaires suivantes:

DQoS qualité de service dynamique (*dynamic quality of service*)

DSCP code des services différenciés (*differentiated services code point*)

P-CSF fonction CSCF proxy (*proxy CSCF*)

WS services Web (*web services*)

II.5 Exigences et portée concernant la qualité de service

Le présent appendice vise à définir une architecture permettant à un équipement d'utilisateur d'avoir accès aux ressources de réseau IPCablecom. En particulier, il décrit un mécanisme détaillé permettant à un réseau IPCablecom de demander des ressources de qualité de service spécifiques nécessaires pour prendre en charge les médias associés aux sessions SIP sur un réseau DOCSIS.

Cette architecture tient également compte du fait que l'architecture IPCablecom assurera une certaine qualité de service pour des applications et services très divers (voix, vidéo, etc.); en tant que telle, elle offre un mécanisme générique permettant de demander des ressources de réseau d'accès et ne nécessite pas que les applications connaissent la topologie du réseau d'accès.

II.5.1 Exigences

On trouvera ci-après la liste des exigences qui sont jugées essentielles pour élaborer une architecture de qualité de service polyvalente permettant de prendre en charge les services envisagés pour l'architecture IPCablecom2:

- l'architecture de qualité de service doit offrir la création de flux pour les équipements d'utilisateur qui ne sont pas sensibles à la qualité de service grâce à un mécanisme de poussée de politique déclenché par le réseau;
- il convient de définir un gestionnaire d'application IPCablecom (IPAM), qui assurera la communication relative à la qualité de service entre la fonction P-CSCF et l'infrastructure multimédia;
- le marquage et la classification des paquets doivent être pris en charge à partir du réseau d'accès de telle sorte qu'un mécanisme de qualité de service (par exemple, services différenciés) puisse être utilisé dans le réseau dorsal;
- le gestionnaire IPAM doit recevoir suffisamment de données de la fonction P-CSCF concernant chacun des flux d'une session pour pouvoir:
  - établir un classificateur approprié tout en prenant en charge les mécanismes de traversée des dispositifs NAT;

  - établir une spécification de flux ou un autre profil de trafic qui tient compte de la limite supérieure minimale des besoins en ressources de tout autre codec qui peut être autorisé pour le flux, y compris la largeur de bande, la vitesse de mise en paquet et le type de programmation;
  - déterminer le type de média de manière à pouvoir choisir un code des services différenciés approprié.
- Le gestionnaire IPAM doit recevoir suffisamment de données de la fonction P-CSCF pour chaque session afin de pouvoir:
  - établir un identificateur de corrélation convenable pour les relevés de comptabilité;
  - identifier l'abonné afin de pouvoir accéder aux données relatives à son profil;
  - reconnaître si la session doit être prioritaire (par exemple, appel d'urgence).
- L'interface doit permettre de réserver et d'engager des ressources selon des étapes distinctes.

II.5.2 Portée

Actuellement, l'architecture de qualité de service IPCablecom ne concerne que les éléments d'accès DOCSIS du réseau d'un câblo-opérateur et les modalités permettant au réseau IPCablecom de demander des ressources de qualité de service du cadre IPCablecom multimédia. L'architecture décrite dans le présent appendice ne s'applique donc pas aux équipements d'utilisateur nomades qui peuvent être raccordés au réseau IPCablecom à partir de réseaux d'accès non DOCSIS.

En outre, cette architecture n'interdit pas l'utilisation des capacités de qualité de service dans les réseaux IPCable2Home. Toutefois, la fourniture de la qualité de service dans ce type de réseau n'entre pas dans le domaine d'application du présent appendice.

II.6 Cadre applicable à l'architecture de qualité de service

L'objectif général étant de tirer le meilleur profit des normes de l'industrie existantes, on vise en particulier à assurer une certaine harmonisation avec l'architecture et les spécifications IMS mises au point dans le cadre du 3GPP. En particulier, l'architecture IPCablecom2 sera harmonisée avec la version 6 du sous-système IMS et réutilisera bon nombre de ses principaux éléments et points de référence. Autre but tout aussi important: utiliser les nombreuses capacités de qualité de service qu'offre l'architecture IPCablecom multimédia.

L'architecture IPCablecom2 doit prendre en charge un modèle de poussée de politique afin d'assurer la liaison avec l'architecture IPCablecom multimédia. La version 6 du sous-système IMS contient deux mécanismes associés permettant d'assurer la qualité de service et de taxer les flux de service IP qui composent les sessions multimédias. La politique locale fondée sur le service (SBLP, *service-based local policy*) constitue un mécanisme permettant d'autoriser, d'établir et de modifier des supports IP à l'aide d'un jeton d'autorisation analogue à celui utilisé dans l'architecture de qualité de service dynamique IPCablecom [UIT-T J.163]. Comme dans le cas de la qualité de service dynamique, pour mettre en place des contextes de protocole PDP en utilisant le mécanisme SBLP, il faut une participation active d'un équipement d'utilisateur sensible à la qualité de service.

Le second mécanisme est la taxation fondée sur les flux (FBC, *flow-based charging*), qui permet d'identifier, de surveiller et de taxer les flux IP qui composent une session à l'aide d'un mécanisme de poussée déclenché par le réseau analogue à celui utilisé dans l'architecture IPCablecom multimédia. Toutefois, le mécanisme FBC ne permet pas d'établir de nouveaux supports (ou flux de service). Ni le mécanisme SBLP, ni le mécanisme FBC tels qu'ils sont définis dans la version 6 du sous-système IMS ne fournissent toutes les informations requises pour prendre en charge l'établissement de flux de service en utilisant l'architecture IPCablecom multimédia. Dans l'avenir, une harmonisation sera possible avec la commande de politique et de taxation définie dans la version 7 du sous-système IMS.

II.6.1 Modèle de référence de l'architecture de qualité de service

L'architecture de qualité de service IPCablecom2 est présentée dans la Figure II.1. L'infrastructure de qualité de service définie dans la version 6 du sous-système IMS n'est pas suffisamment indépendante de l'accès pour respecter les exigences relatives à l'architecture IPCablecom2. L'architecture IPCablecom2 utilise donc les éléments IPCablecom multimédia, y compris le serveur de politique, le système de terminaison de câblo-modem (CMTS) et le câblo-modem. Le gestionnaire d'application IPCablecom2 est un gestionnaire d'application spécialisé qui reçoit de la fonction P-CSCF des demandes de qualité de service au niveau de la session via le protocole simplifié d'accès aux objets (SOAP); en outre il crée et gère des portes IPCablecom multimédia pour chaque flux de la session en utilisant l'interface pkt-mm-3 IPCablecom multimédia.

L'architecture de qualité de service n'interdit pas l'utilisation du point de référence Gq défini dans le sous-système IMS pour les équipements d'utilisateur qui peuvent accéder aux services via un réseau GPRS. La Figure II.1 montre comment l'architecture de qualité de service définie dans le sous-système IMS pour les équipements GPRS coexiste avec l'architecture de qualité de service IPCablecom2 multimédia utilisée pour les équipements d'utilisateur qui accèdent aux services via un réseau DOCSIS.

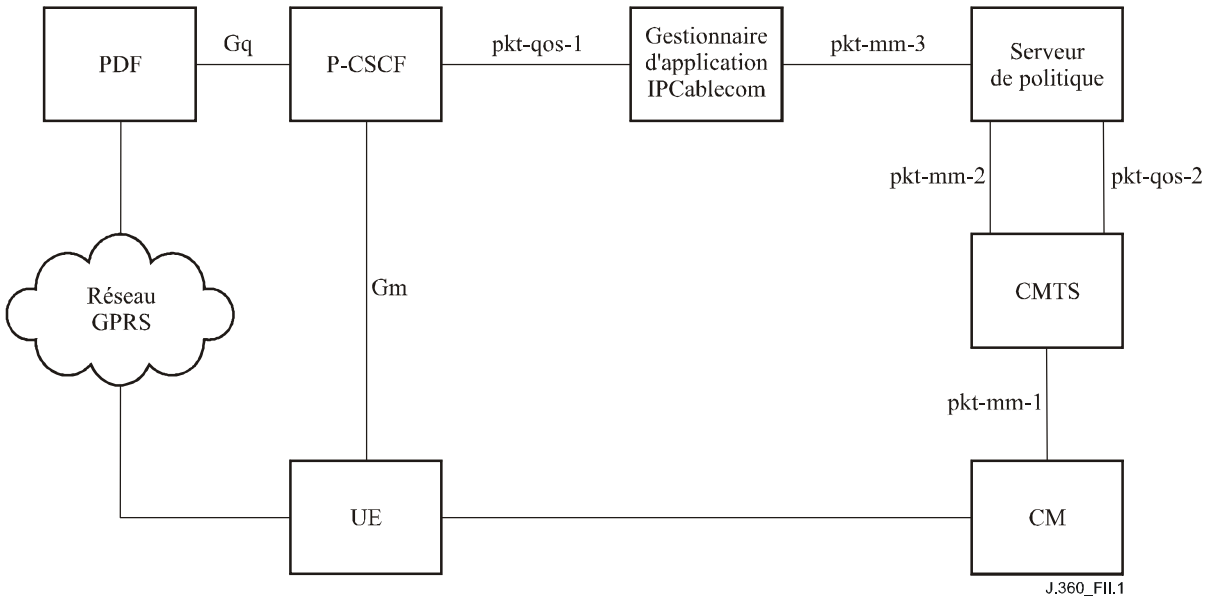


Figure II.1 – Points de référence pour la signalisation de la qualité de service

Les points de référence pkt-mm-1 à pkt-mm-3 sont définis dans l'architecture IPCablecom multimédia. L'architecture IPCablecom2 introduit les nouveaux points de référence pour la qualité de service pkt-qos-1 et pkt-qos-2. Les Tableaux II.1 et II.2 contiennent respectivement une brève description de ces interfaces et une brève description de chaque élément de réseau.

Tableau II.1 – Points de référence pour la qualité de service

Point de référence	Eléments de réseau IPCablecom	Description du point de référence
pkt-mm-1	CMTS – CM	Le système CMTS utilise la signalisation DSX définie dans les spécifications DOCSIS pour charger le câblo-modem d'établir, de libérer ou de modifier un flux de service DOCSIS afin de répondre à une demande de qualité de service.
pkt-mm-2	Serveur de politique – CMTS	L'interface prend en charge les demandes de qualité de service du proxy pour le compte d'un équipement d'utilisateur. Cette interface est essentielle pour le cadre de gestion de politique. Elle commande les décisions de politique qui sont poussées par le serveur de politique (PS) dans le système CMTS et elle est définie dans [UIT-T J.179]. Dans certains cas, cette interface sert également à informer le serveur de politique du moment où les ressources de qualité de service sont devenues inactives.
pkt-mm-3	IPAM-PS	Cette interface permet au gestionnaire d'application IPCablecom (IPAM), qui est un gestionnaire d'application spécialisé défini dans l'architecture IPCablecom, de demander au serveur de politique de pousser une décision de politique dans le système CMTS pour le compte de l'équipement d'utilisateur. Elle est définie dans [UIT-T J.179]. Cette interface peut également servir à informer le gestionnaire IPAM des modifications de l'état des ressources de qualité de service.
Gm	UE – P-CSCF	Permet à l'équipement d'utilisateur de communiquer avec la fonction P-CSCF concernant l'enregistrement et la commande de session. Ce point de référence, qui est fondé sur le protocole SIP, est décrit dans [UIT-T J.366.4].
Mw	CSCF – CSCF	Permet de communiquer et de faire suivre des messages de signalisation entre fonctions CSCF pour permettre l'enregistrement et la commande de session. Ce point de référence est fondé sur le protocole SIP.
Gq	P-CSCF – PDF	L'interface Gq est utilisée pour les échanges de données d'établissement de politique fondés sur la session entre la fonction de décision politique (PDF) et la fonction P-CSCF.
pkt-qos-1	P-CSCF – IPAM	Cette interface entre la fonction P-CSCF et le gestionnaire d'application IPCablecom, fondée sur le protocole SOAP/XML, transporte des informations de qualité de service au niveau de la session. Le gestionnaire IPAM utilise ces informations pour composer des messages adaptés pour l'interface pkt-mm-3 et il est défini dans [UIT-T J.365].
pkt-qos-2	Serveur de politique – CMTS	Le serveur de politique utilise le protocole de découverte de point de commande pour déterminer quel système CMTS dans le réseau dessert un équipement d'utilisateur donné. Ce point de référence repose sur la spécification IPCablecom [UIT-T J.362].

Tableau II.2 – Eléments de réseau pour la qualité de service

Elément de réseau IPCablecom	Brève description
UE	Un équipement d'utilisateur est un client qui interagit avec le réseau pour accéder à des services et fournit des interfaces à des utilisateurs ou entités.
P-CSCF	La fonction P-CSCF analyse les paramètres SDP des messages SIP et implémente l'interface client de service web pour assurer la qualité de service en communiquant avec le gestionnaire d'application. Elle réserve, engage et supprime des ressources de qualité de service dans le réseau d'accès.
Gestionnaire d'application IPCablecom (IPAM)	Le gestionnaire d'application IPCablecom est chargé de gérer les ressources de qualité de service dans le réseau d'accès comme le demande la fonction P-CSCF. Il reçoit des messages de qualité de service au niveau de la session en provenance de la fonction P-CSCF, et formule et envoie des messages de qualité de service IPCablecom multimédia au serveur de politique.
Serveur de politique (PS)	Le serveur de politique est un intermédiaire entre le ou les gestionnaires d'application et le ou les systèmes CMTS. Il applique les politiques de réseau aux messages du gestionnaire d'application puis transmet ces messages au système CMTS.
Système de terminaison de câblo-modem (CMTS)	Le système CMTS est un dispositif qui est situé dans une tête de réseau câblée et implémente le protocole DOCSIS RFI MAC; il se connecte aux câblo-modems via un réseau HFC.
Câblo-modem (CM)	Câblo-modem de type DOCSIS.

II.6.2 Relation avec la version 6 du sous-système IMP 3GPP

Les Recommandations relatives à l'architecture IPCablecom2 modifient la version 6 du sous-système IMS 3GPP (document TS 24.229) afin d'énoncer les exigences en matière de qualité de service pour le protocole de commande d'appel fondé sur les protocoles SIP et SDP. Les modifications apportées au document TS 24.229 sont résumées ci-après:

- ajout de la nécessité d'inclure le descripteur de média "b=" et le modificateur de largeur de bande "TIAS" définis dans le document [IETF RFC 3890] pour décrire la largeur de bande requise pour la session.
- Ajout des nouveaux types SDP suivants à la définition du profil SDP pour les agents utilisateur:
  - durée d'un paquet (a=ptime) – ce type doit être inclus par les équipements d'utilisateur afin d'indiquer le temps de mise en paquets prévu aux équipements d'utilisateur qui reçoivent le trafic;
  - le débit maximal de paquets (a=maxprate) – ce type doit être inclus lorsque l'équipement d'utilisateur utilise un codec IPCablecom inhabituel;
  - dispositif NAT (a=Local-Turn) – ce type doit être inclus par l'équipement d'utilisateur lorsque celui-ci utilise un serveur TURN pour traverser un dispositif NAT local.

II.6.3 Relation avec l'interface pkt-mm-11 multimédia

L'architecture IPCablecom multimédia définit également une interface fondée sur les services Web permettant d'assurer la liaison depuis un serveur d'application amont vers le gestionnaire d'application. Cette interface est étiquetée pkt-mm-11 dans le rapport technique [UIT-T J.179 App.I]. Cette interface pourrait être utilisée par la fonction P-CSCF pour assurer la liaison avec le gestionnaire d'application IPCablecom2, toutefois, une nouvelle interface a été élaborée afin d'améliorer l'efficacité de fonctionnement de la fonction P-CSCF. L'interface définie dans la spécification multimédia nécessiterait une double traduction des paramètres de session, ce qui entraînerait une surcharge pour la fonction P-CSCF pour traduire les paramètres de session en

demande de qualité de service générique. L'interface définie dans la spécification IPCablecom permet à la fonction P-CSCF de transmettre simplement tous les paramètres de session au gestionnaire d'application IPCablecom, qui doit alors les traduire en message de qualité de service IPCablecom multimédia valide. Cette approche permet de réduire le nombre de traductions requises et permet à la fonction P-CSCF de conserver une implémentation plus indépendante du réseau d'accès.

II.7 Description de l'architecture

Tandis que le paragraphe II.6 décrit un ensemble d'entités de réseau logiques regroupées par fonctions de service spécifiques (qualité de service), ainsi qu'une série de points de référence qui prennent en charge les flux d'informations échangés entre les groupes fonctionnels et les entités de réseau, le présent paragraphe contient une présentation plus détaillée de ces éléments logiques et des points de référence associés qui sont nouveaux dans l'architecture IPCablecom. Il donne également un aperçu d'autres thèmes relatifs à l'architecture de qualité de service qui ne sont pas abordés ailleurs.

II.7.1 Composants fonctionnels

Le présent paragraphe contient une présentation plus détaillée du gestionnaire d'application IPCablecom2 et de la fonction P-CSCF, ainsi que de leur rôle vis-à-vis de l'architecture de qualité de service.

II.7.1.1 Fonction P-CSCF

En plus de jouer un rôle dans la connectivité de l'équipement d'utilisateur au réseau IPCablecom, la fonction P-CSCF est également chargée de réserver, d'engager et de libérer des ressources de qualité de service pour une session donnée. Il est important de noter qu'elle ne détermine pas véritablement les ressources de qualité de service nécessaires pour la session mais transmet simplement les informations de description de la session au gestionnaire d'application IPCablecom2 et indique s'il faut réserver ou engager des ressources pour la session. Si cette architecture prend en charge une opération d'engagement en deux phases (réserver puis engager), la fonction P-CSCF n'est pas tenue de suivre cette approche. Il est possible d'utiliser un engagement en une seule phase (réserver et engager des ressources en une seule demande).

Une fois la session terminée, la fonction P-CSCF libère les ressources attribuées à la session.

II.7.1.2 Gestionnaire d'application IPCablecom2 (IPAM)

Le gestionnaire d'application IPCablecom2 est avant tout chargé de déterminer les ressources de qualité de service nécessaires pour la session d'après les descripteurs de session reçus et de gérer les ressources de qualité de service attribuées pour une session.

Pour déterminer les ressources de qualité de service requises pour une session, il faut interpréter le descripteur de session et calculer la largeur de bande requise, déterminer le type de programmation du trafic et renseigner les classificateurs de trafic. Il faut en outre déterminer le nombre de flux nécessaires pour la session (voix uniquement ou voix et vidéo) et gérer l'association des flux à la session.

II.7.1.3 Relation entre la fonction P-CSCF et le gestionnaire IPAM

L'architecture IPCablecom multimédia prévoit une relation bien établie entre le gestionnaire IPAM et le serveur de politique. La relation entre la fonction P-CSCF et le gestionnaire IPAM est décrite ci-après. L'architecture de qualité de service n'a pas été élaborée selon une relation préconçue entre ces deux éléments de réseau. Si le choix du mode de déploiement des fonctions P-CSCF et des gestionnaires IPAM et de leur cardinalité associée est essentiellement motivé par des aspects de déploiement, les Figures II.2 et II.3 montrent ce que l'on estime être les scénarios de déploiement les plus courants.

Figure II.2 – Point à point

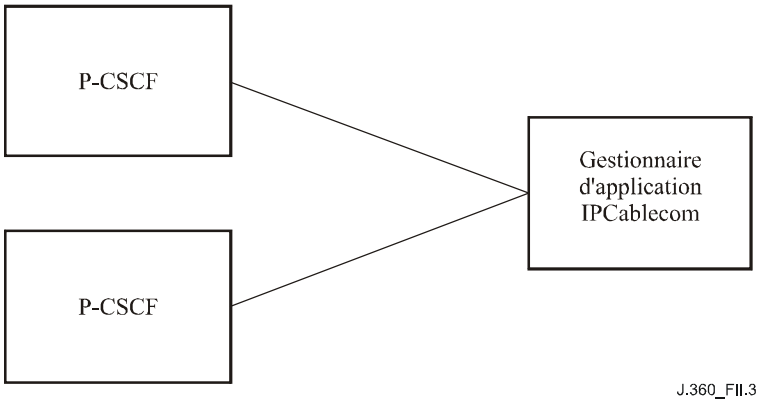


Figure II.3 – Multipoint à point

La Figure II.2 montre une relation point à point entre la fonction P-CSCF et le gestionnaire IPAM. S'il est extrêmement simple à gérer, ce type de scénario de déploiement risque de ne pas correspondre à la manière la plus efficace d'utiliser les ressources. La Figure II.3 montre une relation multipoint à point entre la fonction P-CSCF et le gestionnaire IPAM. Ce scénario reste aussi simple qu'une relation point à point (puisque la fonction P-CSCF n'a pas à déterminer à quel gestionnaire IPAM elle doit envoyer sa demande) mais peut permettre d'utiliser plus efficacement les ressources du gestionnaire IPAM.

Autre scénario possible: relation point à multipoint (ou multipoint à multipoint). Dans ce cas, la fonction P-CSCF peut communiquer avec plusieurs gestionnaires IPAM. Si ce scénario est possible, aucune indication n'est donnée concernant la façon dont la fonction P-CSCF détermine à quel gestionnaire IPAM elle doit envoyer ses demandes. Un tel scénario peut devenir nécessaire à mesure que le réseau évolue et que différents gestionnaires d'application sont invoqués pour différents réseaux d'accès ou dans certains cas d'itinérance.

II.7.2 Interfaces de protocole et points de référence

Le présent appendice a recensé plusieurs interfaces, ou points de référence, dans l'architecture de qualité de service IPCablecom2. La majorité de ces points de référence sont des interfaces existantes définies dans l'architecture IPCablecom multimédia. Le présent paragraphe donne une vue d'ensemble de l'interface de protocole assurant la liaison depuis la fonction P-CSCF vers le gestionnaire IPAM car cette interface est la seule définie dans l'architecture IPCablecom.

Il se peut que cette interface ne soit pas implémentée dans un produit donné. Par exemple, si un fabricant choisit d'intégrer le gestionnaire IPAM dans la fonction P-CSCF l'interface entre la fonction P-CSCF et le gestionnaire IPAM sera interne à ce produit.

II.7.2.1 Description de l'interface entre la fonction P-CSCF et le gestionnaire IPAM

L'interface assurant la liaison depuis la fonction P-CSCF vers le gestionnaire IPAM repose sur des services web. Elle permet à la fonction P-CSCF de demander et de supprimer des ressources de

qualité de service à l'intérieur d'un réseau DOCSIS compatible avec l'architecture IPCablecom multimédia.

L'interface de services Web du gestionnaire d'application IPCablecom2 permet à une fonction P-CSCF de demander la gestion de la qualité de service dans le réseau d'accès sur la base des paramètres du protocole de description de session (SDP, *session description protocol*) contenus dans l'offre et la demande telles qu'elles sont définies dans le document [IETF RFC 3264]. Le gestionnaire IPAM utilise l'interface pkt-mm-3 IPCablecom multimédia pour communiquer ces besoins à un serveur de politique IPCablecom multimédia.

II.7.3 Application de la politique de qualité de service dans l'architecture IPCablecom

Le terme "contrôle de politique" a souvent été utilisé pour décrire le processus grâce auquel un nouveau support ou flux de service dynamique est créé dans le réseau d'accès à la demande d'une application. En effet, l'établissement d'un nouveau flux de service dans le réseau d'accès passe par l'installation d'une nouvelle politique dynamique au point d'application de la politique. Cette politique dynamique détermine comment seront traités les paquets qui composent le nouveau flux de service à l'intérieur du réseau d'accès pendant toute la durée de la session.

Le présent paragraphe porte sur des politiques à des niveaux élevés qui peuvent affecter la disposition d'une demande d'utilisateur lors de son traitement dans le réseau. De telles politiques pourraient être mises en œuvre à plusieurs niveaux dans le réseau afin de répondre aux besoins commerciaux des opérateurs de réseaux. Une politique peut être appliquée aux niveaux suivants:

- applications: les applications peuvent utiliser une politique pour forcer l'utilisation d'une application selon un abonnement ou d'autres informations;
- réseau de signalisation: par exemple, des restrictions d'utilisation de certains paramètres de média dans une offre SDP, en fonction du réseau ou de l'abonnement, peuvent être appliquées dans un réseau IPCablecom par la fonction P-CSCF ou S-CSCF, en envoyant une réponse négative au message SIP comme décrit dans les § 6.2 et 6.3 [UIT-T J.366.4];
- réseau support: chacun des éléments du réseau support (gestionnaire d'application IPCablecom, serveur de politique et système CMTS) joue un rôle unique dans le contrôle de politique. On trouvera ci-après une présentation plus détaillée du rôle de chaque élément de réseau:
  - le gestionnaire d'application IPCablecom2 est le point d'entrée depuis le réseau SIP dans le système de qualité de service du réseau d'accès. Le gestionnaire IPAM peut appliquer une politique qui tient compte du service limité assuré par la fonction P-CSCF et éventuellement d'informations fondées sur l'abonnement;
  - le serveur de politique peut recevoir des messages de plusieurs gestionnaires d'application et notamment des gestionnaires d'application IPCablecom. Les politiques appliquées dans ce serveur peuvent permettre d'optimiser l'utilisation des ressources du réseau d'accès par plusieurs applications et plusieurs types de trafic;
  - le système CMTS est chargé du contrôle d'admission et peut comprendre des politiques qui commandent la répartition de l'attribution des ressources entre différents types de trafic selon la classe de session et, éventuellement, selon le modèle d'autorisation utilisé, par exemple l'architecture IPCablecom ou IPCablecom multimédia.

Dans certains cas, des décisions de politique analogues pourraient être prises à plusieurs niveaux dans le réseau. Le choix du niveau auquel implémenter une politique donnée reposera sur des critères comme:

- l'accès aux informations requises;
- les effets qu'aura l'application de la politique à tel ou tel niveau en termes de performance;
- la facilité d'application de la politique à tel ou tel niveau.

En dernier lieu, la politique sera implémentée au niveau du réseau qui permet de répondre le mieux aux besoins commerciaux du câblo-opérateur.

II.7.4 Routage de la demande de qualité de service

Dans l'hypothèse d'une relation entre fonction P-CSCF et gestionnaire IPAM telle que décrite au § II.7.1.3, le routage des demandes de qualité de service est statique, ce qui signifie que chaque fonction P-CSCF est associée à un gestionnaire d'application unique (avec la possibilité d'un gestionnaire secondaire en cas de panne) auquel elle envoie toutes ses demandes de qualité de service. Dans le cas d'une relation entre plusieurs fonctions P-CSCF et plusieurs gestionnaires d'application, le routage des demandes ne relève pas du domaine d'application du présent appendice.

Actuellement, l'architecture multimédia ne contient aucune précision concernant le routage des demandes de qualité de service entre le gestionnaire IPAM et le serveur de politique, d'une part, et entre le serveur de politique et le système CMTS, d'autre part. C'est pourquoi l'architecture IPCablecom a défini un mécanisme dynamique de routage des messages de qualité de service du serveur de politique au système CMTS. Cette procédure est décrite dans [UIT-T J.362] et repose sur une approche de requête associée au trajet dans le cadre de laquelle la requête suit le même trajet dans le réseau que tout autre paquet destiné à un équipement d'utilisateur donné. Ce mécanisme permet au serveur de politique de tirer profit des protocoles de routage sous-jacents afin de veiller à ce que l'adresse IP de l'équipement d'utilisateur concerné permette d'identifier le système CMTS correspondant.

Le routage des demandes de qualité de service depuis le gestionnaire IPAM et vers le serveur de politique n'est pas défini dans l'architecture IPCablecom.

II.8 Exemples de procédure

Le présent paragraphe décrit un exemple de comportement opérationnel fondé sur les interfaces et exigences définies dans l'architecture IPCablecom. Les flux d'appel qui y figurent ne sont donnés qu'à titre d'exemple afin de présenter plus clairement l'architecture de qualité de service IPCablecom2.

II.8.1 Appel efficace en provenance d'un équipement d'utilisateur

La Figure II.4 montre un flux d'appel efficace en provenance d'un équipement d'utilisateur. Dans l'exemple ci-après, la fonction P-CSCF entame le processus de qualité de service lorsqu'elle reçoit un message SIP avec une offre SDP (en général un message INVITE). La fonction P-CSCF transmet l'offre SDP au gestionnaire IPAM via l'interface de qualité de service définie. Le gestionnaire IPAM peut alors traduire les besoins préliminaires pour la session en demandes IPCablecom multimédia, ce qui entraîne, en règle générale, la création de plusieurs portes IPCablecom multimédia (par exemple, un appel audiotype comprendrait une porte amont et une porte aval).

La demande IPCablecom multimédia produite par le gestionnaire IPAM est ensuite transmise au serveur de politique, qui effectue les vérifications de politique. Celles-ci se font en règle générale au niveau du réseau, ce qui signifie que le serveur de politique s'assurera que la demande est conforme aux politiques fondées sur le réseau (la quantité de ressources demandées est dans les limites, le type de programmation est approprié pour le service, etc.). Une fois que le serveur de politique a vérifié leur conformité, ces demandes sont transmises au système CMTS, qui les traite.

Après réception de la demande de ressources, le système CMTS est chargé du contrôle d'admission et de l'attribution des ressources. Ce processus permet de s'assurer que le système CMTS dispose des ressources adéquates pour satisfaire la demande. Une fois que la demande a franchi l'étape du contrôle d'admission et de l'attribution des ressources, le système CMTS établit les flux nécessaires et en informe le câblo-modem desservant l'équipement d'utilisateur via l'interface de messagerie d'échange de service dynamique (DSX) DOCSIS. A ce stade, les ressources sont seulement

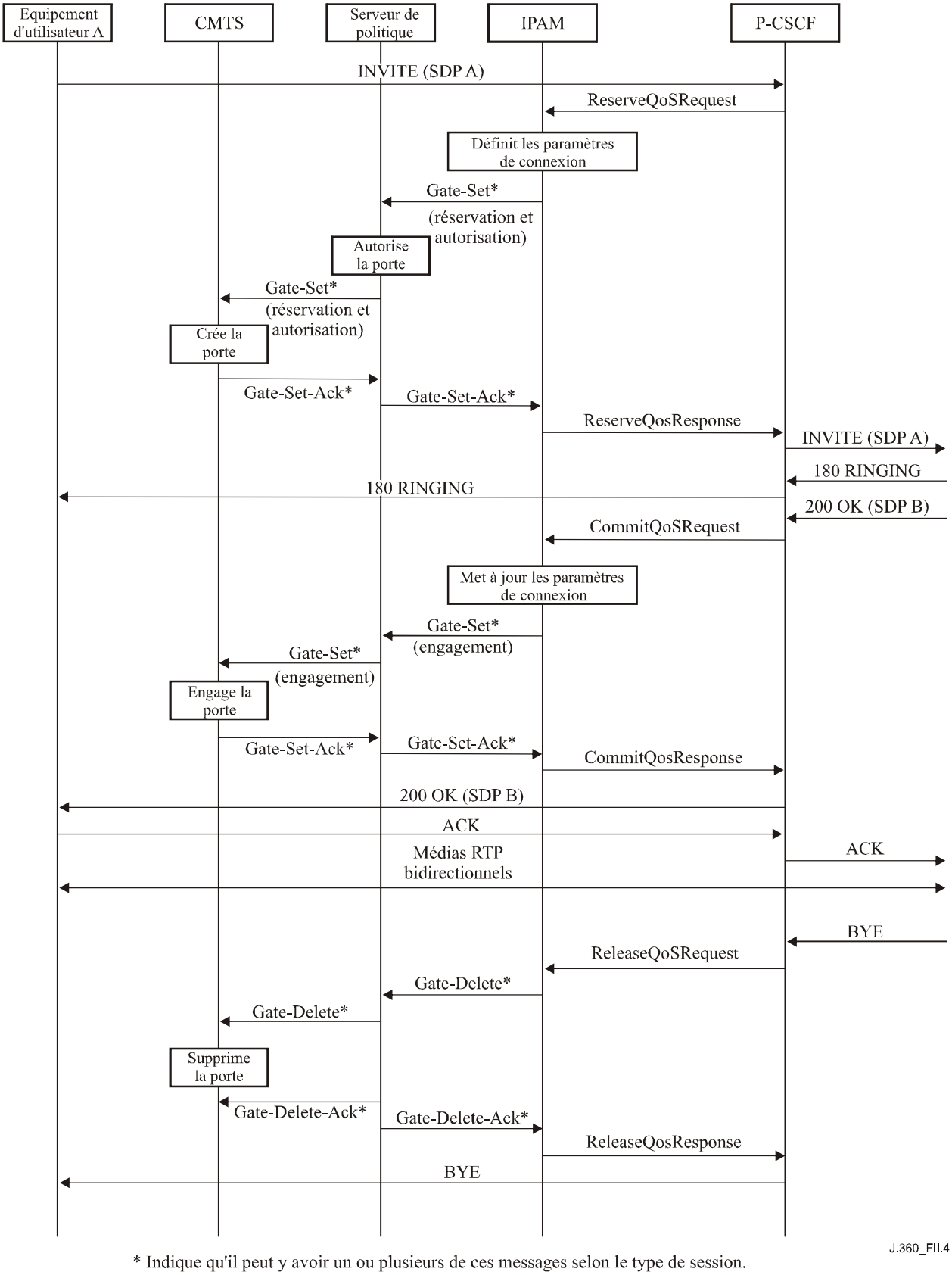
réservées; elles ne sont pas véritablement disponibles pour l'utilisation. Elles ont en fait été attribuées par le système CMTS et ne peuvent plus être attribuées à d'autres services. Une fois que le câblo-modem a été informé avec succès de l'attribution des ressources, le système CMTS renvoie un identificateur de flux au serveur de politique, qui le transmet alors au gestionnaire IPAM à l'origine de la demande.

Une fois qu'elle a reçu la réponse SDP, la fonction P-CSCF dispose de suffisamment d'information sur la partie distante pour engager les ressources pour la session. Pour ce faire, elle transmet la réponse SDP au gestionnaire IPAM, lequel (conjointement avec l'offre SDP) la traduit alors en une nouvelle demande IPCablecom multimédia qui met à jour les ressources réservées précédemment. Tant que la demande mise à jour ne dépasse pas les ressources réservées, il est en principe assuré que la demande sera honorée.

Une fois les ressources engagées, la session peut commencer grâce aux flux établis et la qualité de service souhaitée est reçue.

Après réception d'un message BYE, la fonction P-CSCF libère les ressources associées à la session grâce à une demande ReleaseQoSResources.

La Figure II.4 montre un exemple d'un appel efficace en provenance d'un équipement d'utilisateur.



* Indique qu'il peut y avoir un ou plusieurs de ces messages selon le type de session.

Figure II.4 – Exemple d'appel efficace en provenance d'un équipement d'utilisateur

Appendice III

Aperçu de la sécurité IPCablecom2

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

III.1 Introduction

L'architecture de sécurité IPCablecom2 protège les données, les interfaces et les composants de l'architecture IPCablecom2. Le présent appendice décrit les relations de sécurité entre les éléments de l'architecture IPCablecom2.

Les objectifs nominaux de l'architecture de sécurité IPCablecom2 sont les suivants:

- prise en charge de la confidentialité, de l'authentification, de l'intégrité et des mécanismes de commande d'accès;
- protection du réseau contre les attaques par refus de service, interruption du réseau et vol de service;
- protection des équipements UE (c'est-à-dire des clients) contre les attaques par refus de service, les failles de sécurité et l'accès non autorisé (en provenance du réseau);
- prise en charge du respect de la vie privée de l'utilisateur final par l'intermédiaire du chiffrement et de mécanismes de commande d'accès aux données de l'abonné telles que les informations de présence;
- mécanismes d'authentification des dispositifs, des équipements UE et des utilisateurs et mise en service, signalisation et téléchargement logiciel sécurisés;
- exploitation et extension de l'architecture de sécurité du sous-sytème IMS pour promouvoir les objectifs énoncés précédemment.

III.2 Références

Le présent appendice utilise les références additionnelles à caractère informatif indiquées ci-après:

[UIT-T J.366.4] Recommandation UIT-T J.366.4 (2006), *IPCablecom2 IP Multimedia Subsystem (IMS): Session Initiation Protocol (SIP) and Session Description Protocol (SDP) – Stage 3 specification*. (3GPP TS 24.229)

[UIT-T J.366.7] Recommandation UIT-T J.366.7 (2006), *IPCablecom2 IP Multimedia Subsystem (IMS): Access security for IP-based services*. (3GPP TS 33.203)

[UIT-T J.366.8] Recommandation UIT-T J.366.8 (2006), *IPCablecom2 IP Multimedia Subsystem (IMS): Network domain security specification.* (3GPP TS 33.210)

[UIT-T J.366.9] Recommandation UIT-T J.366.9 (2006), *IPCablecom2 IP Multimedia Subsystem (IMS): Generic authentication architecture specification.* (3GPP TS 33.220)

[IETF RFC 1750] IETF RFC 1750 (1994), *Randomness Recommendations for Security*.

[IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

[IETF RFC 2617] IETF RFC 2617 (1999), *HTTP Authentication: Basic and Digest Access Authentication*.

[IETF RFC 3268] IETF RFC 3268 (2002), *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*.

[IETF RFC 3280] IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile*.

[IETF RFC 3310] IETF RFC 3310 (2002), *Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)*.

[IETF RFC 3329] IETF RFC 3329 (2003), *Security Mechanism Agreement for the Session Initiation Protocol (SIP)*.

[IETF RFC 3489] IETF RFC 3489 (2003), *STUN – Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)*.

[ID SIP-OUTBOUND] *Managing Client Initiated Connections in the Session Initiation Protocol (SIP)*, http://www.ietf.org/internet-drafts/draft-ietf-sip-outbound 02.txt.

[ID TURN] *Obtaining Relay addresses from Simple Traversal of UDP Trough NAT (STUN)*, draft-ietf-behave-turn-00, March 2006.

[TS 23.002] 3GPP TS 23.002 v6.10.0 (2005), *Network architecture*.

[TS 33.222] 3GPP TS 33.222 v6.5.0 (2005), *Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)*.

III.3 Termes et définitions

Le présent appendice utilise les termes et définitions additionnels suivants:

III.3.1 module d'identité des services multimédias IP (ISIM, *IM services identify module*): l'ensemble des données et fonctions relatives à la sécurité d'un sous-système IMS sur une carte à circuit intégré universelle (UICC) peut constituer une application distincte.

III.3.2 IPCablecom multimédia: architecture de qualité de service ignorant tout de l'application pour les services fournis sur les réseaux d'accès DOCSIS.

III.4 Abréviations et acronymes

Le présent appendice utilise les abréviations et acronymes additionnels suivants:

AKA authentification et concordance de clés (*authentication and key agreement*)

BSF aonction du serveur d'amorçage (*bootstrapping server function*)

DDoS attaque par refus de service réparti (*distributed denial of service attack*)

DNSSEC sécurité du système DNS (*DNS security*)

DoS refus de service (*denial of service*)

GBA architecture d'amorçage générique (*generic bootstrapping architecture*)

IDS système de détection des intrusions (*intrusion detection system*)

MiM agressions par entremetteur (*man in the middle*)

PKI infrastructure de clé publique (*public key infrastructure*)

SA association de sécurité (*security association*)

UICC carte à circuit intégré UMTS (*UMTS integrated circuit card*)

USIM module d'identité universelle d'abonné (*universal subscriber identity module*)

III.5 Sécurité IPCablecom2

L'architecture de sécurité IPCablecom2 décrit les points de référence et les composants logiques ainsi que les flux de données entre ces composants.

Le présent paragraphe contient:

- une description des relations entre les versions des systèmes IPCablecom2 et IMS 3GPP;
- un aperçu de l'architecture IPCablecom2;
- une description des menaces qui pèsent sur l'architecture IPCablecom2;
- une description des mécanismes de sécurité IPCablecom2.

III.5.1 Relation avec le sous-système IMS 3GPP

L'architecture IPCablecom2 est fondée sur le sous-système IMS défini dans le cadre du projet de partenariat pour la troisième génération (3GPP). Le projet 3GPP est un accord de collaboration entre différents organismes de normalisation visant à élaborer des spécifications et des rapports techniques relatifs aux réseaux GSM et aux réseaux de systèmes mobiles de la troisième génération (3G).

Dans le cadre général de l'objectif de l'architecture IPCablecom, qui est d'exploiter, chaque fois que possible, les normes de l'industrie actuelles, un objectif consiste plus particulièrement à procéder à une harmonisation avec l'architecture et les spécifications IMS élaborées dans le cadre du projet 3GPP. L'architecture IPCablecom2 réutilisera notamment bon nombre des entités fonctionnelles et des interfaces de base définies dans le sous-système IMS. Bien que le présent Appendice traite du sous-système IMS, l'objectif principal est de décrire les perfectionnements et modifications apportés aux spécifications 3GPP. Voir la norme [TS 23.002] pour obtenir plus de renseignements sur l'architecture IMS 3GPP.

III.5.2 Architecture de référence IPCablecom2

La Figure III.1 donne un aperçu des éléments architecturaux et des groupements fonctionnels IPCablecom2.

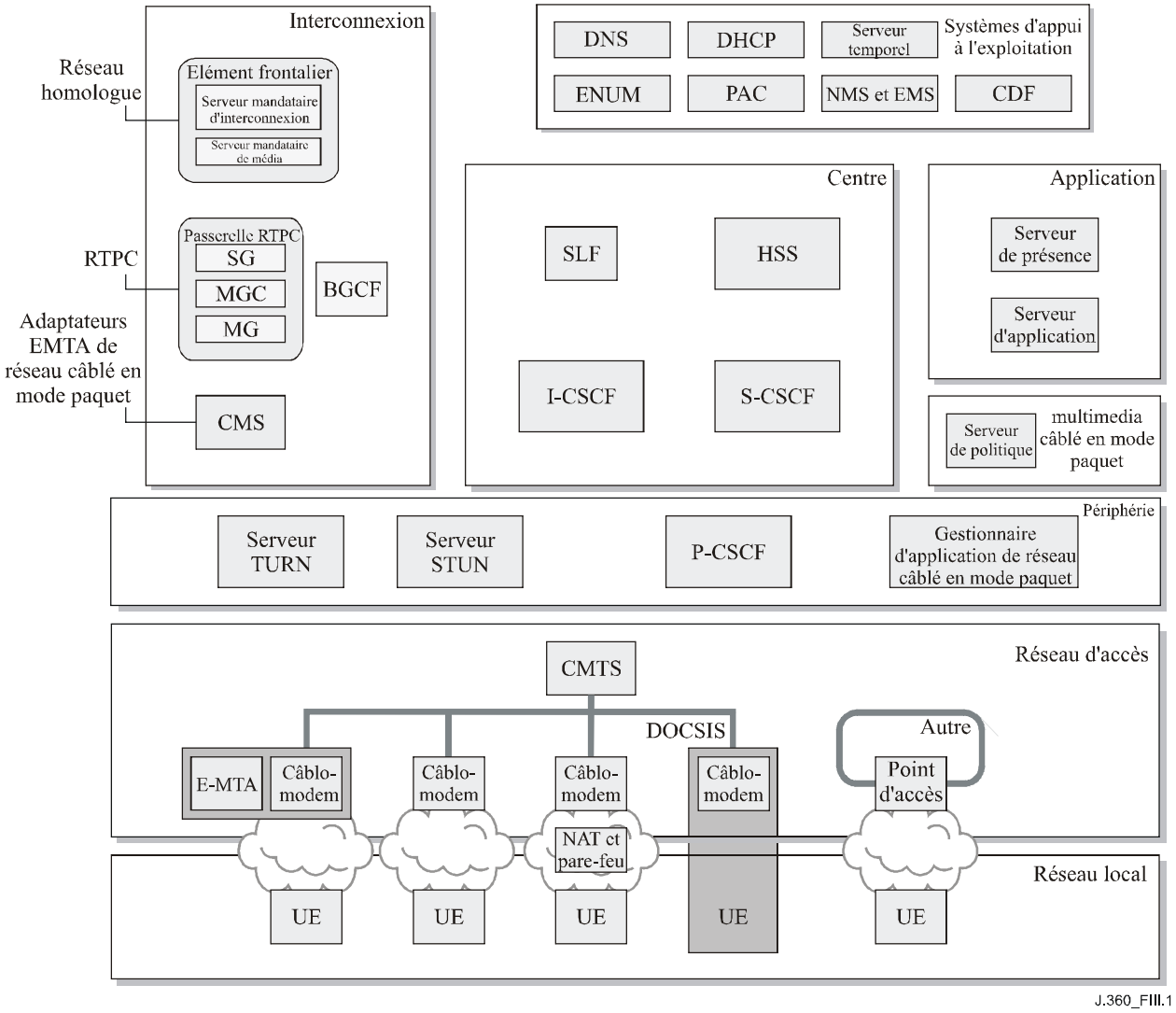


Figure III.1 – Architecture de référence IPCablecom

L'architecture IPCablecom2 est fondée sur l'architecture IMS et comporte certaines extensions visant à prendre en charge les réseaux câblés. Ces extensions prévoient l'utilisation de composants additionnels ou de remplacement et des perfectionnements des capacités offertes par les composants fonctionnels IMS.

Les principaux perfectionnements que l'architecture IPCablecom2 apporte au sous-système IMS sont les suivants:

- prise en charge de la qualité de service (QS) pour les applications fondées sur le sous-système IMS dans les réseaux d'accès câblés, sur la base de l'architecture IPCablecom multimédia;
- prise en charge de la traversée des dispositifs de traduction d'adresse réseau (NAT) et des pare-feu (FW) par la signalisation et les médias sur la base des mécanismes de l'IETF;
- prise en charge de la capacité d'identifier sans ambiguïté un individu et de communiquer avec lui lorsque plusieurs équipements d'utilisateur (UE) sont enregistrés sous la même identité publique;
- prise en charge de mécanismes additionnels relatifs à la sécurité de la signalisation dans le réseau d'accès et à l'authentification des équipements UE pour les équipements UE d'IPCablecom;

- prise en charge de la fourniture de services, de l'activation, de la configuration et de la gestion des équipements UE d'IPCablecom.

L'architecture IPCablecom2 comprend à la fois les composants logiques et les points de référence existants du sous-système IMS et les éléments logiques ainsi que les points de référence ajoutés pour prendre en charge les exigences d'IPCablecom2.

III.5.3 Menaces contre la sécurité de l'architecture IPCablecom2

III.5.3.1 Menaces générales: classification et analyse

On trouvera ci-après un aperçu des menaces générales dans le contexte d'une architecture générique de communication multimédia IP.

III.5.3.1.1 Menaces concernant le domaine de confiance

Un domaine de confiance est un groupement logique d'éléments de réseau qui sont accrédités pour communiquer conformément à un ensemble de politiques de sécurité. On peut délimiter les domaines de confiance au moyen de limites physiques ou logiques. La communication entre les domaines de confiance doit toujours être examinée à des fins d'authentification et d'autorisation. Les interfaces présentant de l'intérêt pour une infrastructure multimédia IP sont les suivantes:

- interfaces dans le domaine intraréseau, qui connectent des éléments du réseau à l'intérieur d'un domaine de fournisseur de services. Une mise en danger d'un élément quelconque du réseau risque de nuire au bon fonctionnement du réseau lui-même. Les menaces concernent presque tous ceux mentionnés dans le présent paragraphe;
- interfaces dans le domaine interréseaux, qui connectent deux domaines. Les domaines peuvent être différents fournisseurs de services ou un même fournisseur. Les niveaux de confiance interdomaines peuvent dicter le niveau de confiance qui peut exister à l'intérieur d'un domaine (intradomaine), de sorte qu'il est impératif de sécuriser ces interfaces. De plus, la sécurité de deux domaines connectés de cette manière dépend de toutes les autres connexions établies par chaque domaine individuel;
- interfaces dans le domaine d'accès, qui permettent à des équipements UE de se connecter avec un fournisseur de services. Cet ensemble d'interfaces est extrêmement vulnérable à une multitude de menaces contre la sécurité, principalement parce que les domaines d'accès contiennent en général des équipements UE et des éléments de réseau sécurisés et non sécurisés. L'authentification renforcée pour tout type d'accès au réseau serait indispensable pour un fournisseur de services. Si l'on est amené à renoncer à l'authentification, les services offerts et les éléments de réseau auxquels cet accès non authentifié est fourni doivent être réduits au minimum.

III.5.3.1.2 Vol de service

On entend par "vol de service" une multitude de menaces, notamment, sans que cette liste soit exhaustive:

- la manipulation des équipements UE – les équipements UE, notamment les équipements UE logiciels, sont vulnérables aux attaques par chevaux de Troie et aux manipulations du comportement. Parmi les techniques de protection vis-à-vis de ces attaques figurent les codes signés et les équipements UE intégrés;
- l'exploitation des failles des protocoles – l'exploitation de mesures cryptographiques défaillantes peut avoir une incidence importante, car elle suppose généralement un redéploiement de grande ampleur. Parmi les techniques de protection vis-à-vis de ces attaques figure l'architecture de défense renforcée;
- l'usurpation d'identité – consiste à se faire passer pour un autre utilisateur afin d'avoir accès à des services, ce qui risque de provoquer une perte de crédibilité et de recettes. Parmi les

mesures de protection visant à lutter contre ce phénomène figurent l'utilisation d'une authentification renforcée et la formation des utilisateurs;

- le clonage des équipements UE – consiste à imiter un équipement UE légitime. Cela pose généralement un problème lorsque les identités des équipements UE sont considérées comme suffisantes pour offrir des services, par exemple dans les architectures où aucune distinction n'est faite entre un "utilisateur" et un "client". La recommandation devrait consister à exiger l'accréditation des équipements UE, à authentifier les utilisateurs avant la fourniture de services et à mettre en place des infrastructures capables d'identifier le clonage et de déjouer les menaces;
- la fraude au moment de l'abonnement et non-paiement de services – les abonnements établis avec des renseignements falsifiés et la détection du non-paiement sortent du cadre de la présente spécification.

III.5.3.1.3 Interruption et refus de service

En général, les attaques par refus de service visent à provoquer une interruption du service en désactivant la totalité ou une partie des entités fournissant des services dans le réseau. Ces attaques surviennent de la couche 2 à la couche 4 du modèle de référence OSI. Les attaques par refus de service ont pour but de rendre indisponible un élément donné du réseau, au moyen d'un ou plusieurs mécanismes différents. Elles comprennent:

- des attaques par messages mal formés – une personne malveillante émet des messages mal formés qui visent à exploiter une faille dans la robustesse d'une pile. Parmi les failles figurent les débordements de mémoire tampon, ou un traitement insuffisant des erreurs ou des effets secondaires. Pour déjouer ces attaques, il faut disposer de piles de protocoles logiciels bien conçues et procéder à des essais de robustesse;
- des attaques par réduction de la couche quatre – une personne malveillante provoque une consommation excessive d'informations d'état sur un dispositif victime, souvent dans le contexte de piles de protocoles avec connaissance de l'état. A titre d'exemple, on peut citer les attaques au niveau du protocole TCP, par exemple une avalanche de requêtes SYN, qui visent à épuiser les ressources de piles qui suivent l'état de la session. On peut remédier à ces attaques au moyen de systèmes de détection des intrusions (IDS, *intrusion detection system*) et de pare-feu, en utilisant des piles de protocoles logiciels bien conçues et en procédant à des essais de robustesse;
- des agressions par submersion au niveau de la couche support – attaques par refus de service qui visent à rendre indisponible un élément donné du réseau, généralement en dirigeant une quantité excessive de trafic média dans le réseau au niveau de ses interfaces. Pour empêcher ces attaques, il faut disposer de pare-feu avec connaissance de l'état, qui ouvrent des microtrous réservés aux médias si le côté sécurisé du pare-feu lance en premier lieu la connexion. Les agressions par submersion utilisent souvent des adresses source falsifiées pour ouvrir des microtrous dans le pare-feu. La vérification de l'adresse source par l'intermédiaire de prises de contact à trois voies permet d'atténuer cette menace. La qualité de service (QS) permet également d'empêcher le passage de flux excessifs par l'intermédiaire d'un routeur.

En général, les agressions par submersion utilisent des paquets IP avec des adresses source falsifiées. On peut déjouer certaines de ces agressions par submersion en empêchant les paquets comprenant des adresses falsifiées. Plusieurs mécanismes permettent d'empêcher la simulation d'adresse, à savoir:

- l'utilisation d'un mécanisme de mise à l'épreuve/réponse tel que le serveur STUN ou TURN;
- l'utilisation du protocole TCP facilite la vérification de l'adresse source (prise de contact à trois voies);

- la retransmission par trajet inverse en monodiffusion (uRPF) – utilisation de tables de routage pour déterminer si le trajet vers la source du paquet (trajet inverse) pointe vers l'interface par laquelle est entré le paquet.

Les attaques par PC "zombies" comprennent tout type d'attaque par refus de service qui est lancée à partir d'un point d'extrémité authentifié. En outre, la plupart des attaques par PC "zombies" utilisent un grand nombre de zombies, ce qui entraîne une attaque par refus de service réparti (DDoS). En général, un cheval de Troie met en danger un point d'extrémité afin d'exploiter l'authentification du point d'extrémité. Il est très difficile de se prémunir contre une attaque par PC zombie, étant donné que le point d'extrémité est authentifié et autorisé. On peut déjouer ces attaques en détectant tout comportement anormal du trafic et en filtrant le trafic malveillant.

III.5.3.1.4 Menaces contre le canal de signalisation

Dans un environnement multimédia tel qu'une architecture SIP, les messages de signalisation comprennent des données relatives à l'identité, aux services et au routage et d'autres données sensibles et critiques. Il existe des composants multimédias comme les serveurs mandataires dans le domaine d'accès, ce qui les expose à un nombre accru de menaces.

Les attaques contre la sécurité de la signalisation sont les suivantes:

- confidentialité compromise – les informations de signalisation comme l'identité de l'appelant et les services auxquels un client est abonné risquent d'être repérées. Les informations relatives à l'identification de l'appelant peuvent également servir à localiser l'appelant si celui-ci souhaite que son emplacement reste confidentiel;
- agressions par entremetteur (MiM, *man in the middle*) – agressions résultant de l'interception et de la modification possible du trafic transitant dans une communication entre deux parties. Ces attaques aboutissent si les parties qui communiquent ne peuvent différencier les communications avec le destinataire prévu de celles avec la personne malveillante. Parmi ces attaques, dont certaines sont décrites dans d'autres paragraphes, figurent l'usurpation d'identité d'un serveur mandataire, le réacheminement non souhaité et la perte de confidentialité résultant de l'intervention d'un entremetteur;
- attaques par refus de service – les attaques par refus de service dans le canal de signalisation vont de la création de fausses demandes, qui aboutissent à des attaques par amplification, à la falsification d'en-têtes de routage. L'utilisation du mode multidiffusion pour transmettre des demandes SIP augmente considérablement les risques d'attaques par refus de service.

Il est possible de déjouer bon nombre de ces attaques en exigeant l'authentification mutuelle, la validation d'identité, la confidentialité et l'intégrité sur le plan de signalisation.

III.5.3.1.5 Menaces contre le canal support

Les menaces contre le canal support concernent le trafic média transféré entre les parties qui communiquent entre elles.

Les attaques contre la sécurité du support sont les suivantes:

- confidentialité compromise – par confidentialité, on entend ici la protection des messages médias eux-mêmes, qui pourraient être une session audio, la messagerie électronique ou d'autres transferts de messages multimédias. En fonction du mécanisme de sécurité qui a été négocié, la confidentialité de bout en bout peut ou non être sous le contrôle de l'expéditeur;
- intégrité compromise – la modification, la suppression et la réexécution sont autant d'attaques qui peuvent être lancées contre le canal support;
- attaques par interruption – comme avec toute technique reposant sur un média, la capacité qu'ont les parties de communiquer crée des communications non souhaitées. On trouve dans cette catégorie toutes les attaques "normales" dont fait l'objet le réseau téléphonique

public à commutation (RTPC), tel que le harcèlement, ainsi que certaines nouvelles menaces relatives à la dégradation et à l'interruption de service dans le modèle IP.

On peut contrecarrer les attaques contre le canal support en exigeant l'authentification mutuelle, la confidentialité et l'intégrité sur le plan support pour empêcher la manipulation des données sur ce plan et garantir la confidentialité des informations sensibles.

III.5.3.1.6 Reconnaissance

Les attaques soigneusement planifiées contre les fournisseurs de services consistent généralement à obtenir en premier lieu la reconnaissance sur un réseau. On peut se prémunir contre ces attaques en utilisant des mécanismes de dissimulation de la topologie, notamment la mise en œuvre d'éléments frontaliers. L'application de techniques de filtrage dans le domaine d'accès permet d'appliquer une politique en matière de trafic à l'extrémité du réseau.

III.5.3.1.7 Considérations relatives au modèle d'itinérance

Les modèles d'itinérance peuvent limiter au maximum ou au contraire accentuer les menaces contre la sécurité. Les équipements UE qui ont accès à des services par l'intermédiaire d'environnements étrangers peuvent exposer à des risques accrus les équipements UE eux-mêmes et le réseau de rattachement. La relation de confiance entre le réseau de rattachement et le réseau visité est mise en œuvre à la limite de la sécurité interdomaines.

III.5.3.2 Menaces contre la sécurité propres au protocole

Les menaces qui pèsent sur les protocoles multimédias sont traitées dans les paragraphes qui suivent. Cette liste ne comprend pas tous les protocoles multimédias, mais inclut les principaux protocoles examinés dans l'architecture et dans d'autres paragraphes.

III.5.3.2.1 Messages SIP

On trouvera ci-après des exemples d'attaques qui peuvent être lancées à partir d'informations obtenues au moyen de la saisie de messages SIP sur le réseau:

- agression par altération des corps de messages (par exemple, envoi de messages SIP mal formés pour perturber un élément de réseau SIP, envoi de messages REGISTER falsifiés pour provoquer le réacheminement de messages de signalisation et empêcher ainsi les équipements UE piratés de lancer ou d'accepter des sessions);
- libération de sessions (par exemple, envoi de message BYE ou CANCEL pour mettre fin prématurément à une session);
- usurpation de l'identité d'un serveur (envoi de messages INVITE falsifiés, par exemple);
- usurpation d'identité et falsification des réponses du serveur qui provoquent une indisponibilité ou un refus de service (par exemple, le réseau est submergé de messages "302 Redirect" ou "401 Unauthorized").

Les vulnérabilités importantes sont présentées dans les paragraphes qui suivent:

III.5.3.2.1.1 Détournement d'enregistrement

Le détournement d'enregistrement met en jeu un point d'extrémité malveillant qui modifie l'enregistrement d'un autre point d'extrémité existant, afin de le pointer en retour vers l'attaquant ou vers une position différente. Il peut prendre plusieurs formes, à savoir:

- clonage de point d'extrémité SIP – un agent d'utilisateur (UA) malveillant peut essayer de s'enregistrer en tant qu'équipement UE victime existant. L'équipement UE malveillant devient un "clone" de l'agent UA victime, s'appropriant ainsi l'identité de la victime;
- exploitation d'une identité faible – si un registre évalue l'identité d'un agent UA, l'en-tête "From:" d'une demande SIP peut être modifié de manière arbitraire et donner lieu par conséquent à un enregistrement malveillant;

- les personnes malveillantes pourraient annuler l'enregistrement de la totalité ou d'une partie des utilisateurs dans un domaine administratif, ce qui empêcherait d'inviter ces utilisateurs à de nouvelles sessions et constituerait ainsi une sorte d'attaque par refus de service.

Voir la section 26.1.1 de [IETF RFC 3261] pour en savoir plus sur le détournement d'enregistrement. La méthode généralement utilisée pour se prémunir contre ce type de piratage d'enregistrement consiste à utiliser la validation d'identité sécurisée.

III.5.3.2.1.2 Falsification de l'identité de l'utilisateur

A moins qu'ils ne soient authentifiés, les messages SIP sont vulnérables à l'usurpation d'identité. Des champs tels que 'From' n'ont pas à être remplis et il est possible de manipuler le champ 'P-Asserted-Identity', sauf s'il contient un élément dûment sécurisé.

Les solutions possibles pour parer à cette menace sont les suivantes:

- utilisation de justificatifs d'identité renforcés et établissement de tunnels sécurisés pour les flux de messages;
- utilisation d'un mécanisme d'identité SIP approprié, tel que "SIP identity", qui prend en charge les validations vérifiables sur le plan cryptographique.

III.5.3.2.1.3 Messages SIP mal formés

Une personne malveillante peut émettre des messages SIP mal formés visant à exploiter une faille dans la robustesse d'une pile de protocoles SIP ou dans le protocole lui-même. Parmi ces failles figurent le lancement non justifié d'un refus de **service**, les débordements de mémoire tampon ou le traitement insuffisant des effets secondaires. Pour contrer de telles attaques, il faut procéder à des essais de robustesse des piles. Les scénarios particuliers qui conduisent à des attaques par refus de service sont les suivants:

- utilisation de champs d'en-tête "Via" falsifiés qui identifient un serveur cible en tant qu'expéditeur de la demande et envoient ces demandes à un grand nombre d'éléments de réseau SIP;
- utilisation d'en-têtes "Route" falsifiés dans une demande qui identifient le serveur cible et envoient ces messages à des serveurs mandataires de bifurcation qui amplifieront les messages envoyés à la cible.

Les serveurs mandataires SIP acceptent par nature les demandes provenant de divers points d'extrémité IP et sont en conséquence exposés à un nombre accru de menaces.

III.5.3.2.1.4 Tempêtes de messages SIP

Les tempêtes de messages SIP peuvent consister à envoyer des messages SIP aléatoires afin d'épuiser la mémoire ou la puissance de traitement en épuisant le stockage d'état ou en exigeant des opérations de chiffrement. Les tempêtes de messages SIP peuvent provenir de l'intérieur ou de l'extérieur d'un réseau. Les techniques visant à déjouer de telles attaques sont les suivantes:

- élimination des piles susceptibles de conduire à un épuisement des ressources;
- utilisation de contremesures antiréexécution;
- éviter les réponses multiples à un seul événement (par exemple messages "401" multiples pour la mise à l'épreuve d'authentification);
- déceler les tempêtes et utiliser des filtres appropriés pour désactiver les équipements UE à comportement erroné.

Les tempêtes de messages peuvent être dues à des déversements d'enregistrement dans lesquels un grand nombre de points d'extrémité tentent de s'enregistrer, mais ne réussissent pas à s'authentifier à la périphérie du réseau et contaminent les serveurs mandataires périphériques. En outre, ces serveurs mandataires périphériques peuvent autoriser l'enregistrement de points d'extrémité sans

authentification et renvoyer la mise à l'épreuve de l'équipement UE aux serveurs internes du réseau, auquel cas ces serveurs risquent d'être submergés par des refus de service. Il existe plusieurs manières de déjouer les attaques de ce genre, à savoir:

- exiger l'authentification au niveau des serveurs mandataires périphériques de façon à répartir la charge de l'authentification et à assurer une meilleure protection contre les déversements de refus de service lors de l'enregistrement;
- imposer des mesures visant à lutter contre les déversements, remettre un mot de circonstance aux équipements UE qui s'authentifient pour la première fois qui pourra être utilisé ultérieurement dans des conditions moins strictes de limitation du débit;
- autoriser la fonction P-CSCF à établir des priorités en matière de signalisation, sur la base de mises à l'épreuve antérieures réussies émanant du même équipement UE.

III.5.3.2.1.5 Piratage de session

Les méthodes utilisées pour lancer une attaque par piratage de session sont les suivantes:

- modification des informations SDP;
- utilisation de messages comme "301 déplacé en permanence" pour rediriger les messages INVITE vers une autre position (à supposer que l'attaquant connaisse les champs Call-ID, To, From, Cseq).

En général, la méthode permettant d'empêcher le détournement de session consiste à exiger l'authentification de tous les messages SIP.

III.5.3.2.1.6 Usurpation d'identité d'un serveur

Un attaquant peut usurper l'identité de serveurs SIP dans le réseau. L'usurpation d'identité de serveurs SIP peut aboutir à un refus de service ou à une violation de la confidentialité. Le problème peut être encore plus grave lorsque la mobilité SIP est prise en compte. L'authentification du serveur par les agents (UA) constitue la méthode à appliquer pour contrer l'usurpation d'identité.

Voir la section 26.1.2 de [IETF RFC 3261] pour plus de renseignements.

III.5.3.2.1.7 Altération avec corps de message

Voir la section 26.1.3 de [IETF RFC 3261] pour plus de renseignements.

III.5.3.2.1.8 Libération de sessions

Voir la section 26.1.4 de [IETF RFC 3261] pour plus de renseignements.

III.5.3.2.1.9 Menaces contre la reconnaissance

Certains messages et champs SIP facilitent les menaces contre la reconnaissance. On peut se prémunir contre ces menaces en empêchant l'utilisation de certains champs (par exemple OPTIONS) dans les messages.

III.5.3.2.2 Serveur STUN

Les attaques contre le serveur STUN peuvent généralement être classées en attaques par refus de service ou en attaque par interception. Les attaques par refus de service peuvent être lancées contre le serveur STUN lui-même ou contre d'autres éléments utilisant le protocole STUN.

Bon nombre de ces attaques exigent de la personne malveillante qu'elle génère une réponse à une demande STUN légitime, de manière à fournir à l'équipement UE un message MAPPED-ADDRESS falsifié. Les attaques qui peuvent être lancées au moyen de l'une de ces techniques sont les suivantes:

- refus de service réparti (DDoS) contre une cible;
- désactivation d'un équipement UE;

- supposition de l'identité d'un équipement UE;
- interception.

On trouvera dans [IETF RFC 3489] des renseignements plus détaillés sur ces attaques et la manière dont elles sont traitées par le protocole STUN lui-même.

III.5.3.2.3 Serveur TURN

Un serveur TURN assume une fonction de réacheminement en vue d'acheminer des flux de média par l'intermédiaire d'un dispositif NAT vers une destination. Il peut donc devenir une source pour une attaque par refus de service utilisant des flux de média à grande largeur de bande. Pour empêcher l'utilisation à mauvais escient d'un serveur TURN, il est indispensable de disposer d'un moyen vérifiable, sur le plan cryptographique, d'établir un mécanisme d'authentification et d'autorisation permettant aux destinataires de flux de média d'autoriser le serveur TURN à transmettre des médias.

III.5.3.2.4 Sécurité TLS

Etant donné que la sécurité de la couche Transport (TLS, *transport layer security*) est assurée bond par bond, elle peut être compromise dans un serveur qui fait aboutir et lance à nouveau la signalisation.

La sécurité TLS s'appuie également sur un mécanisme permettant d'établir la confiance entre deux entités de communication telles que l'infrastructure de clé publique (PKI, *public key infrastructure*) à l'intérieur d'un domaine administratif. L'établissement de la sécurité TLS entre les serveurs devrait faire intervenir une authentification mutuelle.

Le protocole TLS s'appuie généralement sur la fiabilité transitive pour la sécurité bond par bond. Si chaque point d'extrémité dispose de son propre serveur local et que les serveurs se font mutuellement confiance, les points d'extrémité peuvent présumer, par l'intermédiaire de la fiabilité transitive, que la communication de bout en bout est sécurisée.

III.5.3.2.5 Protocole HTTP de type *Digest*

La principale menace qui pèse sur l'authentification HTTP de type *Digest* fait intervenir une agression par un entremetteur (MiM). Le protocole HTTP de type *Digest* fonctionne en vérifiant qu'un utilisateur dispose d'un mot de passe prépartagé. Une fois que l'équipement UE demande un accès à une ressource, le serveur demande à l'équipement UE de fournir un mot de passe. Dans cette demande, le serveur renvoie un mot de circonstance dans la libération, qui devrait être utilisé par l'équipement UE pour générer un hachage du mot de passe formé de manière sécurisée. Le mot de passe haché est envoyé au serveur dans la libération. Cette méthode d'authentification est sensible aux agressions par un entremetteur (MiM) de type dictionnaire visant à trouver un mot de passe qui donne la même valeur de hachage sécurisée que la valeur renvoyée au serveur. En conséquence, le protocole HTTP de type *Digest* devrait être utilisé sur les trajets de données sécurisés.

III.5.3.2.6 Système DNS

En général, le système de noms de domaine n'est pas sécurisé sans l'utilisation de la sécurité DNSSEC. Parmi les menaces possibles contre la sécurité figurent la manipulation des interrogations de demande ou de réponse qui entraîne la réorientation ou le refus de service et l'utilisation de la fonctionnalité dynamique DNS, si elle est permise, pour manipuler des serveurs DNS et refléter des topologies incorrectes.

Pour parer à certaines de ces menaces, le serveur DNS ne devrait être utilisé que pour des mécanismes d'information générale et d'autres mécanismes de configuration tels que l'authentification, qui servent à valider des éléments de réseau.

III.5.3.2.7 Equipements d'utilisateurs fondés sur des logiciels

L'architecture IPCablecom prend en charge les équipements UE fondés sur des logiciels pour authentifier et utiliser les services offerts par le réseau. Ces équipements posent des problèmes qui conduisent à des vulnérabilités, à savoir:

- même si les équipements UE fondés sur un logiciel disposent d'une fonction leur permettant de se connecter à un magasin de clés matériel sécurisé, par exemple une carte à mémoire, ils stockent généralement les justificatifs dans une mémoire non protégée;
- l'image logicielle sur un équipement UE commutable n'est pas infraudable;
- les applications fournies sur des équipements UE fondés sur des logiciels peuvent mémoriser le mot de passe d'un usager en vue d'une entrée automatisée ultérieure.

III.5.4 Aperçu de l'architecture de sécurité IPCablecom2

Le présent paragraphe décrit l'architecture de sécurité IPCablecom2, y compris les perfectionnements apportés au sous-système IMS. Les domaines de confiance décrits au § III.5.3 servent à décomposer l'architecture IPCablecom2. Chaque domaine de confiance est examiné de manière plus approfondie dans les paragraphes ci-après.

III.5.4.1 Domaine d'accès

Les équipements UE se connectent au réseau par l'intermédiaire du domaine d'accès. Les interfaces et les composants présents dans le domaine d'accès sont indiqués sur la Figure III.2.

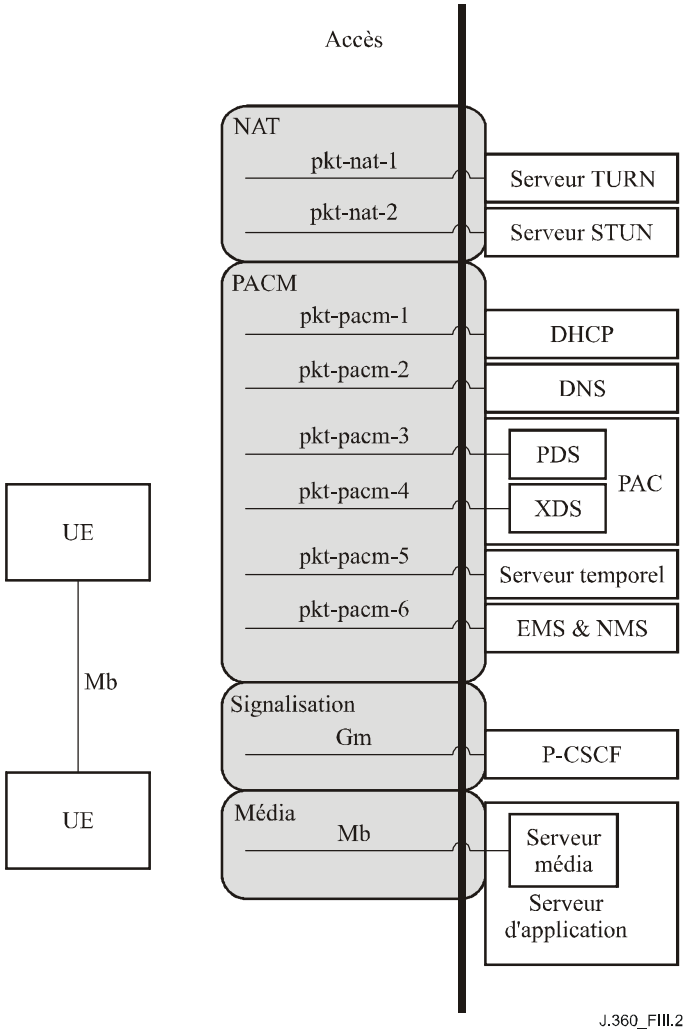


Figure III.2 – Points de référence situés dans le domaine d'accès

Les interactions entre les équipements UE et le réseau se produisent dans le domaine d'accès. Dans ce domaine, diverses méthodes d'accès sont employées, par exemple la spécification de passerelle de décodeur DOCSIS et l'accès sans fil. Du fait de ces caractéristiques, le domaine d'accès est exposé à une multitude de menaces, comme indiqué au § III.5.3.

Le Tableau III.1 donne un aperçu de haut niveau de l'architecture de sécurité résultant des améliorations IPCablecom2 apportées au sous-système IMS. Chaque point de référence situé dans le domaine d'accès, ainsi que le mécanisme de sécurité employé pour cette interface, est indiqué.

Tableau III.1 – Description des points de référence situés dans le domaine d'accès

Point de référence	Eléments de réseau IPCablecom2	Description de la sécurité au point de référence
pkt-nat-1	UE – Serveur TURN	TURN: les demandes TURN sont authentifiées et autorisées dans le cadre du protocole TURN lui-même.
pkt-nat-2	UE – Serveur STUN externe	STUN: l'intégrité des messages est assurée par les mécanismes STUN.
pkt-pacm-1	UE – Serveur DHCP	DHCP: l'architecture IPCablecom2 ne définit pas la sécurité concernant le protocole DHCP.
pkt-pacm-2	UE – Serveur DNS	DNS: l'architecture IPCablecom2 ne définit pas la sécurité concernant le protocole DNS.
pkt-pacm-3	UE – Serveur PDS	SIP: l'intégrité et la confidentialité des messages se font par l'intermédiaire du protocole IPSec ou TLS.
pkt-pacm-4	UE – Serveur XDS	XCAP: intégrité et confidentialité des messages via le protocole HTTP sur TLS.
pkt-pacm-5	UE – Serveur temporel	SNTP: l'architecture IPCablecom2 ne définit pas la sécurité concernant le protocole SNTP.
pkt-pacm-6	UE – Serveur EMS et NMS	La sécurité de l'interface de gestion sort du cadre de la présente spécification.
Gm	UE – P-CSCF	SIP: intégrité et confidentialité des messages via IPSec ou TLS. STUN: l'intégrité des messages est assurée par des mécanismes STUN (étant donné que les demandes STUN sont envoyées à l'accès SIP type, le protocole P-CSCF doit logiquement contenir la fonctionnalité STUN).
Mb	UE – UE UE – Serveur média UE – MG UE – E-MTA	RTP: la sécurité des médias sort du cadre de la présente spécification.

III.5.4.2 Domaine intraréseau

Les points de référence et les composants situés dans le domaine intraréseau sont contenus dans un réseau de fournisseur de services et, par conséquent, appliquent une politique de sécurité intrinsèque.

Le sous-système IMS définit la sécurité des connexions situées dans le domaine intraréseau avec l'interface Zb, telle qu'elle est décrite dans [UIT-T J.366.8]. Dans le sous-système IMS, l'intégrité est requise et la confidentialité est facultative lorsque l'interface Zb est implémentée. La charge utile de sécurité d'encapsulation (ESP) IPsec est utilisée pour assurer des services de sécurité pour l'interface Zb entre les composants situés dans le domaine intraréseau.

L'architecture IPCablecom améliore l'interface Zb en ajoutant le protocole TLS, afin de fournir des services de sécurité destinés aux flux de données TCP situés dans le domaine intraréseau. Le

paragraphe III.6.6 décrit les exigences en matière de protocole TLS applicables au point de référence Zb.

III.5.4.3 Domaine interréseaux

Les points de référence situés dans le domaine interréseaux connectent le domaine de la sécurité de l'opérateur avec les partenaires et les réseaux externes. Ces connexions assurent l'interfonctionnement entre le réseau de l'opérateur et les autres fournisseurs de services et de réseaux, y compris le RTPC. La Figure III.3 indique la frontière délimitant les éléments sécurisés du domaine interréseaux.

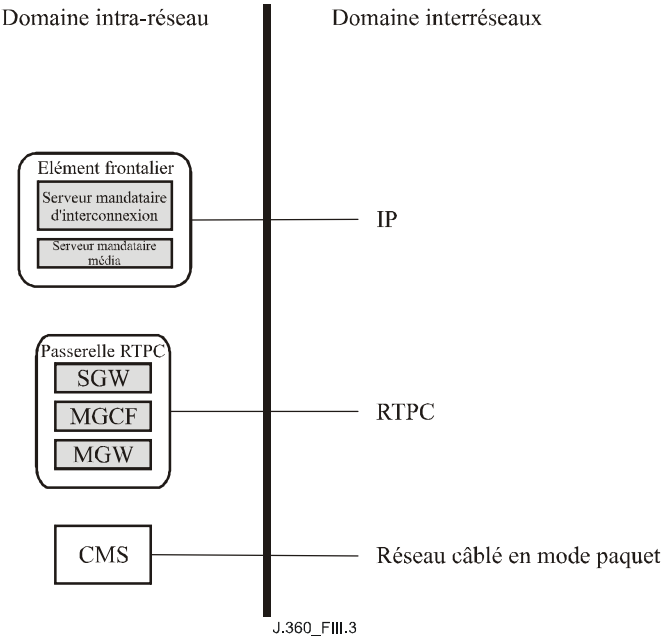


Figure III.3 – Points de référence situés dans le domaine interréseaux

Le sous-système IMS définit la sécurité des connexions situées dans le domaine interréseaux avec l'interface Za, telle qu'elle est décrite dans [UIT-T J.366.8]. L'intégrité et la confidentialité sont requises pour l'interface Za, sur la base de la charge utile ESP IPSec. Le trafic interdomaines dans le sous-système IMS doit obligatoirement passer par une passerelle de sécurité (SEG, *security gateway*). Celle-ci fait aboutir les tunnels IPSec du point de référence Za et applique la politique de sécurité aux flux de trafic interdomaines. La Figure III.3 représente une architecture comportant la fonctionnalité de passerelle de sécurité, dans l'élément frontalier, mais la passerelle de sécurité peut être un élément à part entière.

La passerelle entre le RTPC et le point de référence RTPC est sécurisée au moyen de mécanismes de sécurité du RTPC.

L'architecture IPCablecom2 ajoute la prise en charge de l'interfonctionnement avec les réseaux IPCablecom. Le serveur de gestion d'appels (CMS) fournit la traduction pour la messagerie IPCablecom. La sécurité applicable au point de référence CMS est traitée dans [UIT-T J.170].

III.6 Exigences de sécurité applicable à l'architecture IPCablecom

Les paragraphes qui suivent décrivent les améliorations apportées par l'architecture IPCablecom2 à l'architecture de sécurité du sous-système IMS.

III.6.1 Authentification de l'utilisateur et de l'équipement UE

Le sous-système IMS 3GPP s'appuie entièrement sur les justificatifs d'identité stockés dans une carte à circuit intégré universelle UMTS (UICC, *UMTS integrated circuit card*) aux fins de la sécurité de l'accès. La carte UICC est une plate-forme destinée aux applications de sécurité utilisées pour l'authentification et la concordance de clés. L'architecture IPCablecom doit prendre en charge de multiples types d'équipements UE, tels que les équipements UE logiciels, qui ne contiendront pas de cartes UICC ou n'auront pas accès à ces cartes.

[UIT-T J.366.7] décrit l'approche suivie par le sous-système IMS en matière d'authentification et l'établissement de la sécurité de transport entre les équipements UE et la fonction P-CSCF. Le sous-système IMS utilise à la fois IPSec pour l'intégrité et la confidentialité facultative et IMS-AKA pour l'authentification. Afin de satisfaire aux exigences du sous-système IMS, qui imposent le plus petit nombre possible d'aller-retour, les éléments de sécurité de la négociation procèdent au "portage" sur le flux de messages du registre SIP. On utilise la norme [IETF RFC 3329] pour négocier la sécurité entre l'équipement UE et la fonction P-CSCF et IMS-AKA (norme [IETF RFC 3310]) entre l'équipement UE et la fonction S-CSCF pour procéder à l'authentification mutuelle. La norme [IETF RFC 2617] est développée pour transmettre les données d'authentification de l'équipement UE à la fonction S-CSCF. Les communications entre l'équipement UE et la fonction P-CSCF et celles entre l'équipement UE et la fonction S-CSCF sont reliées en ce sens que les données de clé pour les associations de sécurité entre l'équipement UE et la fonction P-CSCF sont calculées à partir du secret partagé à long terme mémorisée dans le serveur d'abonnés résidentiels (HSS, *home subscriber server*) et la carte UICC de l'équipement UE. La Figure III.4 représente les flux de messages de haut niveau destinés à l'authentification au cours de l'enregistrement. Certains éléments et messages ne sont pas affichés afin de simplifier les discussions.

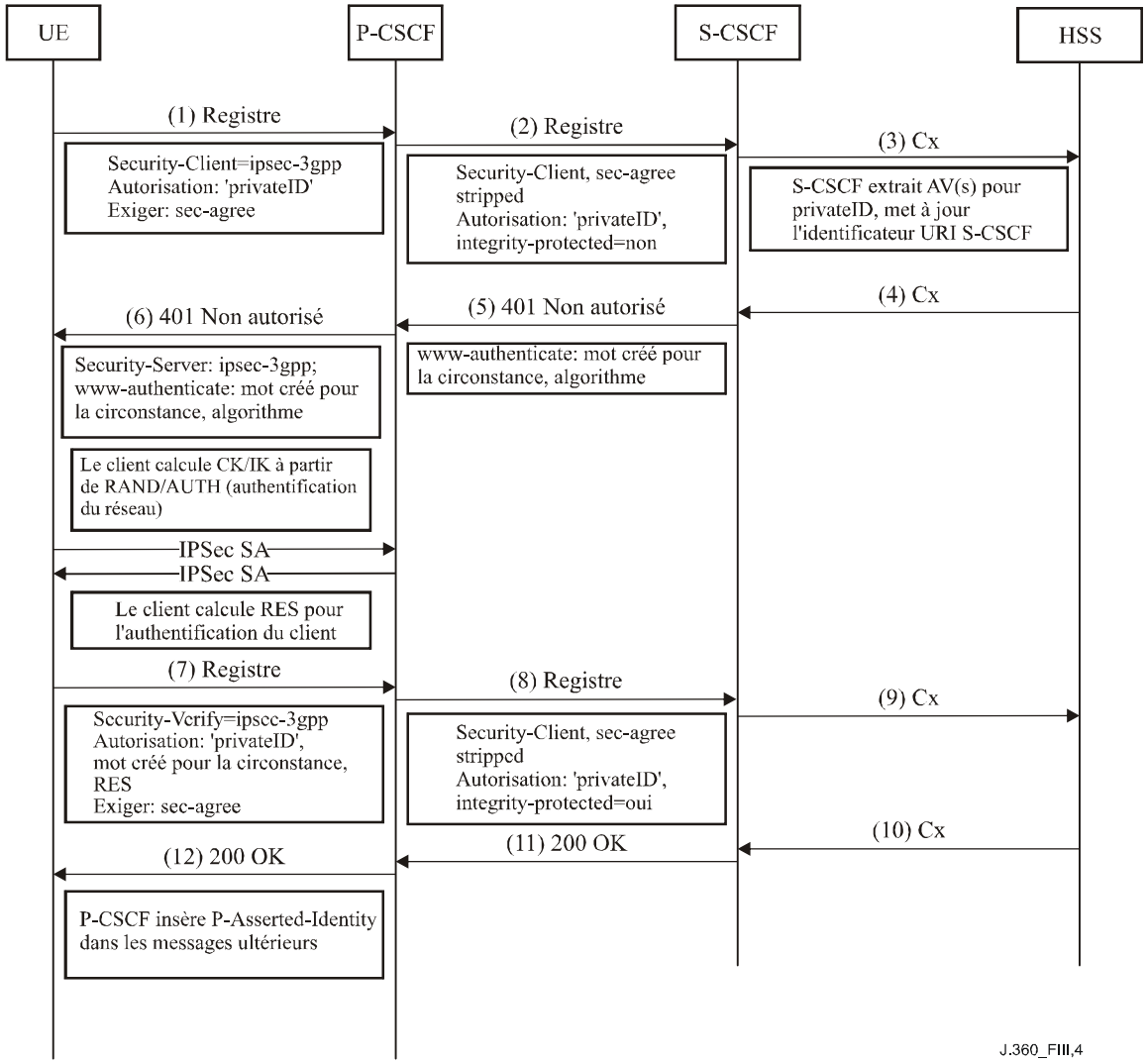


Figure III.4 – Flux de messages d'enregistrement IMS

Aux fins de l'authentification pendant l'enregistrement, les principales mesures suivantes sont prises:

1) L'équipement UE envoie une demande d'enregistrement à la fonction P-CSCF. Le message contient un en-tête de security-client [IETF RFC 3329] qui comprend les mécanismes de sécurité pris en charge par l'équipement UE. Le sous-système IMS impose "ipsec-3gpp". Ce message comprend également un en-tête d'autorisation qui inclut l'identité privée de l'abonné.

2) La fonction P-CSCF enlève les en-têtes de l'accord de sécurité, insère "integrity-protected=no" dans l'en-tête autorisé et transmet la demande d'enregistrement à la fonction I-CSCF appropriée, laquelle retransmet la demande à la fonction S-CSCF appropriée du réseau d'abonnés résidentiels.

3) La fonction S-CSCF contacte le serveur HSS pour mettre à jour l'identificateur URI de la fonction S-CSCF pour cet utilisateur et, le cas échéant, demande un ou plusieurs vecteurs d'authentification.

4) Le serveur HSS retourne un ou plusieurs vecteurs d'authentification s'il est invité à le faire. Les vecteurs d'authentification fournissent les données nécessaires à la fonction S-CSCF pour créer un en-tête www-authenticate et mettre à l'épreuve l'utilisateur.

5) La fonction S-CSCF crée et envoie une réponse SIP 401 (non autorisé) contenant un en-tête www-authenticate qui inclut une mise à l'épreuve. Cette réponse est réacheminée vers la fonction P-CSCF.

6) La fonction P-CSCF enlève la clé d'intégrité (IK) et la clé de confidentialité (CK) de la réponse 401 à l'usage des associations de sécurité (SA, *security association*) IPSec entre la fonction P-CSCF et l'équipement UE et envoie le reste de la réponse à l'équipement UE.

7) Lorsqu'il reçoit le message de mise à l'épreuve, l'équipement UE détermine la validité de l'épreuve d'authentification reçue. L'équipement UE crée des associations de sécurité avec la fonction P-CSCF au moyen des clés IK et CK obtenues à partir des données envoyées par le serveur HSS, en utilisant la clé partagée à long terme figurant dans sa carte UICC. L'équipement UE calcule ensuite une réponse (RES) et envoie une deuxième demande d'enregistrement avec un en-tête Authorization comprenant la réponse de mise à l'épreuve. Ce message contient des en-têtes Security-Verify conformément à [IETF RFC 3329].

8) La fonction P-CSCF enlève les en-têtes de l'accord de sécurité, insère le message "*integrity-protect=yes*" dans l'en-tête autorisé et le transmet à la fonction I-CSCF appropriée, laquelle la retransmet à la fonction S-CSCF appropriée.

9) La fonction S-CSCF compare la réponse de mise à l'épreuve d'authentification reçue de l'équipement UE avec la réponse attendue reçue du serveur HSS. Si ces réponses correspondent, la fonction S-CSCF met à jour les données du serveur HSS en utilisant l'interface Cx.

10) Le serveur HSS communique à la fonction S-C SCF les données de l'abonné sur l'interface Cx, y compris les profils de service, qui contiennent les critères de filtrage initiaux.

11) La fonction S-CSCF transmet une réponse "200 OK" à l'équipement UE. La réponse "200 OK" contient un en-tête P-Associated-URI qui comprend la liste des identités d'utilisateur public associé à l'identité d'utilisateur public en cours d'enregistrement.

12) La fonction P-CSCF transmet le message "200 OK" à l'équipement UE. Etant donné que l'utilisateur a désormais été authentifié et qu'il y a une association de sécurité existante entre la fonction P-CSCF et l'équipement UE, la fonction P-CSCF insère un en-tête P-Asserted-Identify dans tous les messages ultérieurs émanant de cet équipement UE.

L'architecture IPCablecom est tenue de prendre en charge les équipements UE et les systèmes d'authentification qui ne sont pas pris en compte dans l'architecture IMS, ainsi que des mécanismes de sécurité de transport additionnels. L'architecture IP Cablecom2 améliore les spécifications du sous-système IMS dans plusieurs domaines afin de prendre en charge ces exigences.

III.6.1.1 Description

L'architecture IPCablecom2 prend en charge les mécanismes d'authentification suivants:

- AKA-IMS (Authentification et concordance de clés du sous-système IMS);
- procédure d'authentification "*Digest*" du protocole SIP;
- authentification fondée sur des certificats.

Cette architecture doit également admettre les équipements UE comportant plusieurs justificatifs d'authentification. Ainsi, un équipement UE peut disposer d'un certificat permettant d'avoir accès à des services sur un réseau câblé et une carte UICC pour avoir accès à des services sur un réseau cellulaire.

Un abonné peut disposer de plusieurs justificatifs pour la même identité privée. Il peut disposer de plusieurs équipements UE, avec des capacités différentes relatives à ces justificatifs. Un abonné peut par exemple disposer d'un adaptateur MTA ayant un certificat à usage domestique et un équipement UE basé sur une carte UICC pour les déplacements.

III.6.1.1.1 Authentification AKA-IMS

L'authentification AKA (Authentification et concordance de clés) du sous-système IMS avec des justificatifs UICC continuera de fonctionner comme indiqué dans les spécifications 3GPP.

III.6.1.1.2 Authentification "*Digest*" du protocole SIP

L'architecture IPCablecom2 prend en charge l'authentification du protocole SIP comme indiqué dans [IETF RFC 3261]. L'authentification du protocole SIP utilise un cadre de réponse mise à l'épreuve pour l'authentification des messages SIP et l'accès aux services. Selon cette approche, un utilisateur est mis à l'épreuve afin de prouver son identité, soit au cours de l'enregistrement, soit au cours d'autres lancements de dialogues SIP.

Dans l'architecture IPCablecom2, l'authentification du protocole SIP est gérée de la même manière que pour l'authentification IMS AKA et est conforme aux [IETF RFC 3261] et [IETF RFC 2617]. Cette approche atténue le plus possible les incidences pour le flux d'authentification existant du sous-système IMS en maintenant les en-têtes et les aller et retour existants. A la différence de l'authentification IMS AKA, les mises à l'épreuve ne sont pas calculées au préalable. Afin de garantir au maximum la sécurité de l'authentification "*Digest*" du protocole SIP, on utilise les paramètres cnonces et qop et des directives *"auth-int*", ce qui nécessite le calcul des mises à l'épreuve en temps réel au niveau de la fonction S-CSCF.

La Figure III.5 représente le flux de messages pour l'authentification basée sur le protocole SIP au cours d'un enregistrement.

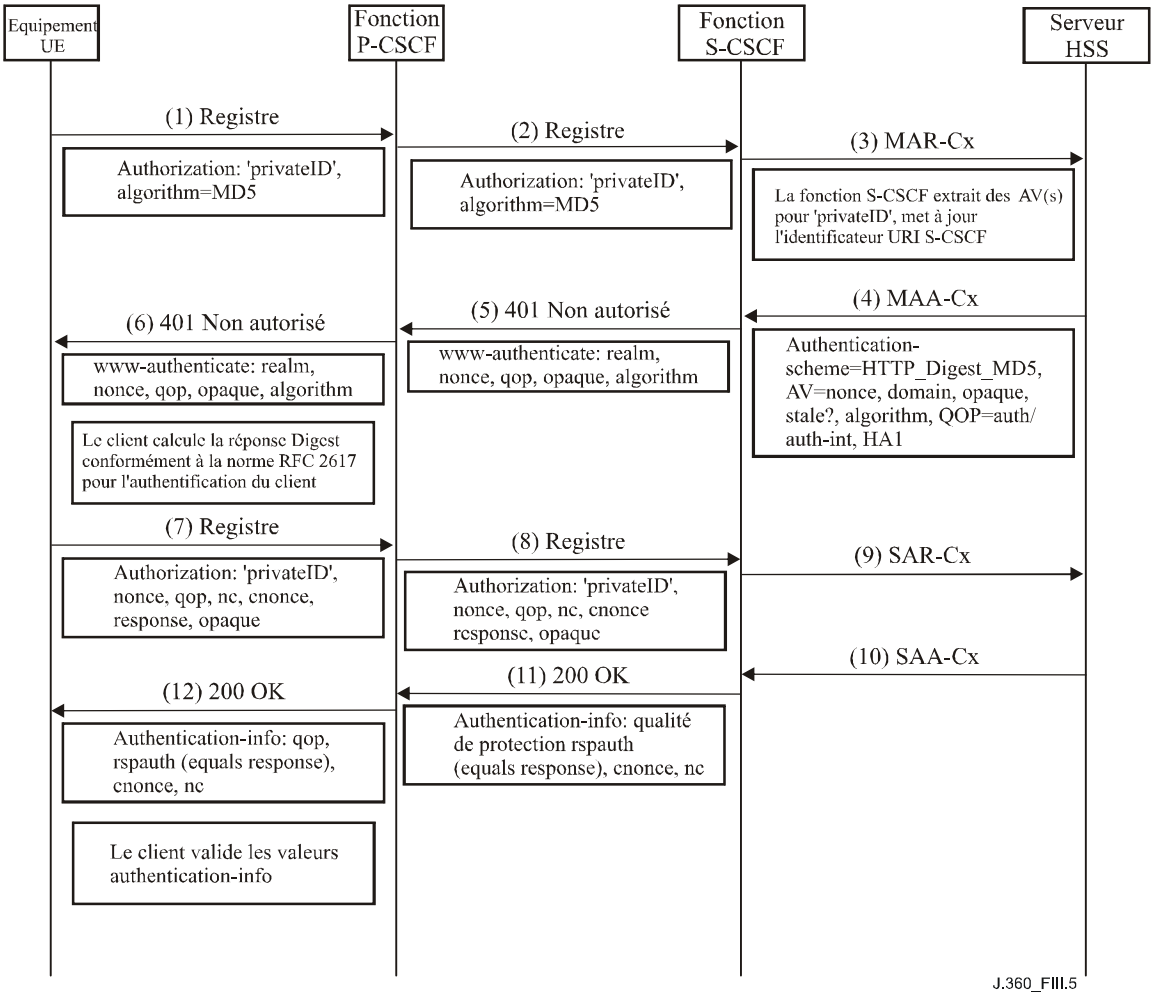


Figure III.5 – Authentification de type Digest du protocole SIP

Aux fins de l'authentification de type *Digest* du protocole SIP pendant l'enregistrement, les principales opérations suivantes sont effectuées. Dans un souci de simplicité, les en-têtes et autres contenus d'en-tête du protocole SIP de [IETF RFC 3329] ne sont pas indiqués.

1) L'équipement UE envoie une demande d'enregistrement à la fonction P-CSCF. Ce message comprend un en-tête Authorization qui contient l'identité privée de l'abonné. On trouvera ci-dessous un exemple d'en-tête d'autorisation:

```
REGISTER sip:home.atlanta.com SIP/2.0
Authorization: Digest username="alice_private@atlanta.com",
      realm=" atlanta.com", nonce="", uri="sip:home.atlanta.com",
      response="", algorithm="MD5"
```

L'architecture IPCablecom ajoute le paramètre de l'algorithme au message d'enregistrement initial du sous-système IMS afin d'informer le réseau du type d'épreuve à créer. L'objectif est de prendre en charge plusieurs types de justificatifs d'identité pour chaque utilisateur.

2) La fonction P-CSCF envoie la demande d'enregistrement à la fonction I-CSCF appropriée, laquelle retransmet la demande à la fonction S-CSCF appropriée du réseau de l'abonné résidentiel.

3) La fonction S-CSCF contacte le serveur HSS en utilisant une commande AMR en direction du serveur HSS sur l'interface Cx. Le message MAR contient l'identité privée de l'abonné, les informations de la fonction S-CSCF et le nombre de vecteurs d'identification demandé. Ces informations sont utilisées par le serveur HSS pour mettre à jour l'identificateur URI de

la fonction S-CSCF concernant l'identité privée et pour fournir les informations correctes du vecteur d'authentification à la fonction S-CSCF.

4) Le serveur HSS retourne un message MAA sur l'interface Cx. Ce message MAA contient les identités publiques et les vecteurs d'authentification correspondant à cet abonné. Le contenu du vecteur d'identification relatif à l'authentification de type *Digest* du protocole SIP est présenté en détail dans un autre paragraphe. Les principales différences ont trait à l'absence de clés CK et IK et au contenu de l'élément de donnée "SIP-Authenticate". Au lieu des données AKA, le profil AVP "SIP-Authenticate" contient les données dont la fonction S-CSCF a besoin pour calculer une réponse de type Digest, essentiellement HA1.

5) La fonction S-CSCF créé une réponse "SIP 401" (non autorisé), qui comprend une mise à l'épreuve dans le champ de l'en-tête www-authenticate et d'autres champs [IETF RFC 3261]. On trouvera ci-après un exemple d'en-tête.

```
SIP/2.0 401 Unauthorized
      WWW-Authenticate: Digest realm="atlanta.com",
        nonce="CjPk9mRqNuT25eRkajM09uTl9nM09uTl9nMz5OX25PZz==",
        qop=auth,auth-int, opaque="5ccc069c403ebaf9f0171e9517f40e41",
              algorithm="MD5"
```

On trouvera des renseignements sur la création de mots de circonstance dans un autre paragraphe. En fonction de la politique locale, le serveur renvoie les paramètres qop parmi lesquels doit choisir le client.

6) Cette réponse est retransmise à la fonction P-CSCF, puis à l'équipement UE.

7) Une fois que l'équipement UE reçoit l'épreuve, il calcule la réponse sur la base des éléments figurant dans l'en-tête WWW-Authenticate et d'autres éléments (par exemple le paramètre cnonce) qu'il a générés. Les valeurs figurant dans l'en-tête Authorize sont calculées conformément à [IETF RFC 3261] et, par conséquent, à [IETF RFC 2617]. La valeur du paramètre qop est choisie parmi les valeurs possibles offertes par la fonction S-CSCF. Les valeurs du paramètre cnonce sont calculées comme indiqué dans un paragraphe ultérieur. L'équipement UE envoie une deuxième demande d'enregistrement avec l'en-tête Authorization. On trouvera ci-dessous un exemple d'en-tête Authorization:

```
REGISTER sip:home.atlanta.com SIP/2.0
      Authorization: Digest
              username="alice_private@atlanta.com", realm="atlanta.com",
              nonce="CjPk9mRqNuT25eRkajM09uTl9nM09uTl9nMz5OX25PZz==",
              uri="sip:home.atlanta.com", qop=auth-int, nc=00000001,
              cnonce="0a4f113b",
              response="6629fae49393a05397450978507c4ef1",
              opaque="5ccc069c403ebaf9f0171e9517f40e41", algorithm="MD5"
```

8) La fonction P-CSCF transmet le message à la fonction I-CSCF appropriée, laquelle la retransmet à son tour à la fonction S-CSCF appropriée.

9) Lorsqu'elle reçoit le deuxième enregistrement de la part de l'équipement UE, la fonction S-CSCF calcule l'épreuve de la même manière que l'équipement UE, afin de comparer les deux résultats et, en conséquence, d'authentifier l'abonné. A l'aide de paramètres fournis par le serveur HSS, tels que HA1, et des paramètres fournis par l'en-tête Autorization tel que le paramètre cnonce, la fonction S-CSCF calcule la réponse/mise à l'épreuve conformément à [IETF RFC 3261] et, par conséquent, à [IETF RFC 2617]. Ce calcul est effectué conformément au paramètre qop envoyé par l'équipement UE.

Si les deux résultats de mise à l'épreuve sont identiques, la fonction S-CSCF met en œuvre une procédure SAR (segmentation et réassemblage) sur l'interface Cx, en informant le serveur HSS que l'utilisateur est enregistré et en demandant le profil de cet utilisateur.

10) Le serveur HSS retourne à la fonction S-CSCF un message SAA contenant le profil de l'utilisateur, qui contient notamment l'ensemble de toutes les identités d'utilisateur public attribuées à des fins d'authentification de l'identité de l'utilisateur privé ainsi que les critères de filtrage initiaux.

11) La fonction S-CSCF envoie une réponse "200 OK" à la demande d'enregistrement. Cette réponse contient un en-tête Authentication-Info, qui permet à l'équipement UE d'authentifier le réseau ou la fonction S-CSCF. La valeur "rspauth" est calculée conformément à [IETF RFC 2617]. L'en-tête contient aussi une valeur "nextnonce". Le message "200 OK" est transmis à l'équipement UE. On trouvera ci-dessous un exemple d'en-tête Authentication-Info:

```
SIP/2.0 200 OK
        Authentication-Info:
        qop=auth-int, rspauth="7729fae49393a05397450978507c4ef1",
        cnonce="0a4f113b",nc=00000001,
        nextnonce="8829fae49393a05397450978507c4ef1"
```

12) Le message "200 OK" est acheminé vers la fonction P-CSCF appropriée, puis vers l'équipement UE.

13) L'équipement UE valide la valeur "rspauth", afin d'authentifier le réseau ou la fonction S-CSCF.

Etant donné que l'utilisateur a désormais été authentifié et qu'il y a une association de sécurité existante entre la fonction P-CSCF et l'équipement UE, la fonction P-CSCF insère un en-tête "P-Asserted-Identity" dans tous les messages ultérieurs provenant de cet équipement UE.

Le fait d'ajouter la prise en charge de l'authentification de type *Digest* du protocole SIP a les incidences suivantes sur les spécifications du sous-système IMS:

- de nouveaux algorithmes du résumé peuvent être présents dans les en-têtes www-authenticate et Authorization;
- le serveur HSS doit calculer et stocker de nouveaux types de réponses de résumé;
- les équipements UE doivent pouvoir prendre en charge et calculer de nouveaux types de réponses de résumé;
- le réseau domestique (ou fonction S-CSCF) s'authentifie auprès de l'équipement UE en incluant un en-tête Authentication-Info dans la réponse "2xx" à la suite d'une authentification réussie de l'équipement UE.

Les conséquences pour les différents composants sont examinées au § III.6.1.2.

III.6.1.1.3 Authentification fondée sur des certificats

L'authentification fondée sur des certificats sort du cadre de la présente version du présent appendice.

III.6.1.2 Composants affectés

On trouvera dans les paragraphes qui suivent les conséquences pour les composants du sous-système IMS afin de tenir compte des exigences en matière d'authentification IPCablecom.

III.6.1.2.1 Equipement UE

Afin de prendre en charge de nouvelles formes d'authentification, les équipements UE de l'architecture IPCablcom doivent envoyer le paramètre "algorithm" approprié dans les demandes d'enregistrement initiales.

Les équipements UE IPCablecom qui prennent en charge l'authentification de type *Digest* (résumé) doivent être conformes à [IETF RFC 3261] et, par conséquent, à [IETF RFC 2617]. Les équipements UE doivent envoyer le paramètre 'algorithm' fixé à la valeur de l'algorithme de résumé

approprié dans la demande d'enregistrement initiale. Dès réception d'une mise à l'épreuve de la part de la fonction S-CSCF dans un message "401 Unauthorized", les équipements UE doivent créer un en-tête "Authorization" comprenant une réponse/mise à l'épreuve comme indiqué dans [IETF RFC 2617], sur la base du paramètre de l'algorithme figurant dans l'en-tête "www-Authenticate". Les paramètres "Cnonce" et "nc" doivent être inclus dans la réponse de mise à l'épreuve. Le paramètre "cnonce" doit être de 32 octets et être codé en format hexadécimal ASCII conformément à [IETF RFC 2617] et aux lignes directrices figurant dans [IETF RFC 1750]. La valeur du paramètre qop utilisée pour les calculs de la réponse et retournée dans l'en-tête Authorization doit être l'une des valeurs reçues dans l'en-tête 401 "www-Authenticate" provenant de la fonction S-CSCF. Les équipements UE doivent pouvoir valider les valeurs de l'en-tête Authentication-Info retournées par la fonction S-CSCF avec le message 200 OK.

Les équipements UE doivent être à même de stocker en toute sécurité les noms d'utilisateur et les mots de passe de manière à réduire le plus possible les risques. A titre facultatif, les équipements UE peuvent inciter les utilisateurs à fournir un nom d'utilisateur et un mot de passe.

III.6.1.2.2 Fonction S-CSCF

Afin de prendre en charge de nouvelles formes d'authentification, la fonction S-CSCF doit comprendre de nouvelles valeurs du paramètre algorithme dans les en-têtes "Authorization" envoyés par les équipements UE. Cette valeur doit ensuite être utilisée pour le profil AVP "Authentication-Scheme" dans les procédures Cx.

Afin de prendre en charge l'authentification de type *Digest* du protocole SIP, la fonction S-CSCF doit être en mesure de calculer les réponses *Digest* comme indiqué dans [IETF RFC 3261] et [IETF RFC 2617]. La fonction S-CSCF recevra la valeur HA1 du serveur HSS sur l'interface Cx et devra utiliser cette valeur pour créer la réponse de résumé concernant cette identité privée. Cette réponse est comparée à celle qui est reçue par l'équipement UE, de sorte qu'elle doit être calculée de la même manière. La valeur du paramètre "qop" reçue de la part de l'équipement UE doit être utilisée pour le calcul de la réponse. Si la réponse calculée par la fonction S-CSCF est identique à celle reçue de l'équipement UE, la fonction S-CSCF envoie un message 200 OK contenant un en-tête "Authentication-Info", conformément à [IETF RFC 2617]. Le paramètre "nextnonce" doit être utilisé dans l'en-tête "Authentication-Info".

Etant donné que la sécurité de l'authentification de type *Digest* dépend fortement du calcul du mot de circonstance, la fonction S-CSCF doit se conformer à ces lignes directrices lorsqu'elle envisage la création et l'utilisation de mots de circonstance:

- le mot de circonstance doit être de 32 octets et être codé au format hexadécimal ASCII conformément à [IETF RFC 2617];
- le mot de circonstance doit être généré conformément à la création de nombres pseudo-aléatoires, par exemple à [IETF RFC 1750];
- le paramètre "nextnonce" est toujours envoyé dans les réponses "Authentication-Info" (par exemple, les réponses 2xx) aux fins de l'authentification réussie de l'équipement UE.

En fonction de la politique locale, la fonction S-CSCF devrait:

- accepter un mot de circonstance utilisé précédemment avec un paramètre nonce-count valable, par exemple pour permettre la réception de demandes PRACK et d'autres types de demandes avant une réponse 2xx;
- accepter uniquement un mot de circonstance utilisé antérieurement pour une période précise. Il est recommandé d'utiliser une valeur temporelle de 10 min au maximum;
- accepter uniquement un mot de circonstance utilisé antérieurement pour un certain nombre de fois. Il est recommandé d'utiliser une valeur de 5 fois au maximum;

- accepter un mot de circonstance ancien sur la base des règles de la politique précitée, même si le paramètre nextnonce a été envoyé.

Les règles de politique précitées se rapportent essentiellement au cas dans lequel la sécurité de la signalisation est désactivée dans le réseau.

III.6.1.2.3 Serveur HSS

Afin de prendre en charge de nouveaux systèmes d'authentification, il faut étendre les interfaces et les procédures Cx. L'authentification de type *Digest* ajoute de nouveaux paramètres à l'interface Cx, notamment le profil AVP "SIP-Auth-Data-Item" présent dans les procédures MAR et MAA. Le vecteur d'authentification fournit à la fonction S-CSCF l'élément HA1 et d'autres éléments pour permettre à cette fonction de calculer les réponses. Pour plus de précisions, voir l'Appendice IV.

III.6.1.3 Sécurité de signalisation

Le sous-système IMS définit le protocole IPSec afin de sécuriser la signalisation entre les équipements UE et les serveurs mandataires périphériques. La carte UICC fournit des justificatifs d'identité aux fins de l'authentification et du protocole IPSec. Le mécanisme de sécurité est négocié au moyen d'un accord de sécurité SIP conforme à [IETF RFC 3329], mais le seul mécanisme autorisé pour la négociation dans le sous-système IMS est le mécanisme ipsec-3gpp.

L'architecture IPCablecom2 ajoute le protocole TLS en tant qu'option pour assurer la sécurité de la signalisation entre l'équipement UE et la fonction P-CSCF. L'utilisation du protocole TLS par l'équipement UE est facultative et offre les avantages suivants:

- le protocole TLS est le mécanisme de sécurité recommandé dans [IETF RFC 3261];
- d'une manière générale, la tendance est à l'utilisation du protocole TCP pour mieux gérer les messages longs;
- le protocole TLS prend en charge la traversée de dispositifs NAT au niveau de la couche protocole;
- le protocole TLS est implémenté au niveau de l'application et non pas au niveau du noyau, ce qui offre certains avantages tels qu'une prise en charge plus facile dans les environnements multiples.

Le fait que le protocole TLS soit pris en charge pour la signalisation amène à prendre en considération les justificatifs d'identité TLS.

- Authentification mutuelle TLS – Les équipements et le serveur fournissent des certificats lors de l'établissement de la sécurité de signalisation. Le serveur doit valider le certificat UE et l'équipement UE doit valider le certificat du serveur. L'authentification mutuelle offre un degré de sécurité élevé.
- Authentification côté serveur – Seul le serveur fournit un certificat lors de l'établissement de la sécurité de signalisation. Cette approche évite les surcoûts de calculs liés à une opération PKI sur l'équipement UE, assure un niveau de sécurité moyen, impose moins d'exigences au niveau de l'unité centrale à l'équipement UE et peut servir à sécuriser les sessions de type HTTP *Digest*.

Ces deux modèles obligent la fonction P-CSCF et l'équipement UE à prendre en charge des fonctionnalités PKI telles que la validation et la gestion des certificats.

Le fait que le protocole TLS soit pris en charge amène également à examiner les assignations d'accès TLS et la gestion des connexions TLS. L'architecture IPCablecom2 utilisera les accès SIP normalisés pour les protocoles UDP, TCP et TLS. Les équipements UE ayant négocié le protocole TLS facultatif avant des messages SIP se connectent à l'accès SIPS du message 5061, sinon ils utilisent l'accès type UDP/TCP du protocole SIP (message 5060). Les demandes et les réponses sont effectuées conformément aux procédures décrites dans [ID SIP-OUTBOUND].

L'architecture IPCablecom2 prend en charge une session TLS facultative avant la signalisation SIP, si l'équipement UE et la fonction P-CSCF la prennent en charge, ce qui assure la sécurité sur le message d'enregistrement initial. Les en-têtes [IETF RFC 3329] sont encore utilisés pendant le processus d'enregistrement, afin d'assurer la sécurité contre les attaques par sous-enchère et de garantir la conformité aux flux de messages d'enregistrement IMS existants.

La Figure III.6 représente une négociation de sécurité de signalisation pendant un dialogue d'enregistrement réussi. Seuls les en-têtes de sécurité de signalisation sont indiqués dans un souci de simplicité.

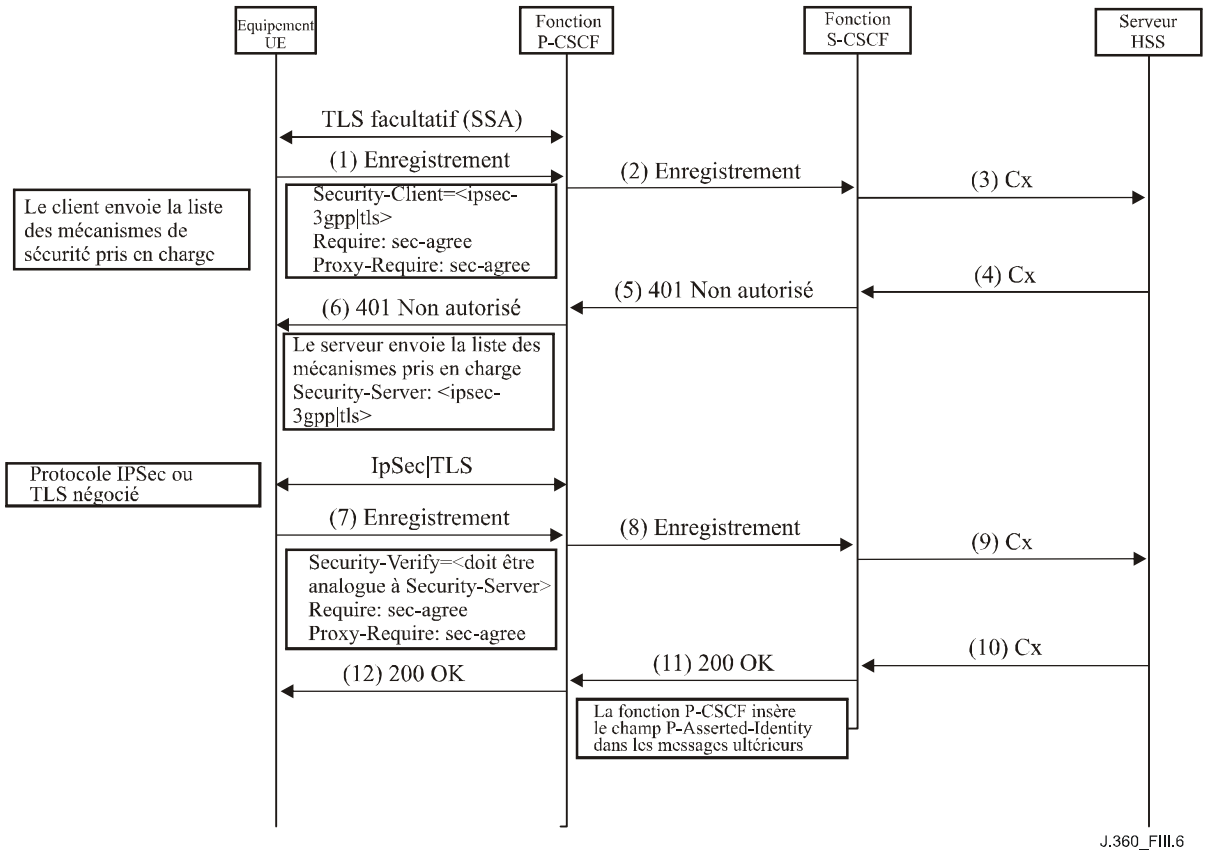


Figure III.6 – Sécurité de transport

Pour prendre en charge le protocole TLS aux fins de la sécurité de signalisation entre l'équipement UE et la fonction P-CSCF, il faut améliorer les spécifications IMS afin que le protocole TLS puisse être négocié en tant que mécanisme de sécurité SIP facultatif. [IETF RFC 3329] fait figurer le protocole TLS au nombre des mécanismes de sécurité pouvant être négociés, de sorte que la seule modification concerne les spécifications IMS.

Il ressort de la figure que les équipements UE pouvant fournir le protocole TLS peuvent négocier l'authentification TLS côté serveur avant l'échange de messages SIP, par exemple lorsqu'un utilisateur exige la confidentialité. Les en-têtes [IETF RFC 3329] servent à négocier la sécurité de signalisation pendant l'enregistrement du protocole SIP, de façon à assurer une protection contre les attaques par sous-enchère et à garantir la conformité aux flux de messages IMS actuels.

A un niveau supérieur, les conséquences pour les composants IMS sont les suivantes:

- l'équipement UE doit prendre en charge la capacité de négocier le protocole TLS à l'aide de [IETF RFC 3329];
- l'équipement UE peut établir le protocole TLS avant l'échange de messages SIP;

- la fonction P-CSCF doit prendre en charge la capacité de négocier le protocole TLS à l'aide de [IETF RFC 3329];
- la fonction P-CSCF peut prendre en charge le protocole TLS avant l'échange de messages SIP.

III.6.1.3.1 Composants affectés

Les paragraphes suivants décrivent les incidences pour les composants IMS afin de négocier la sécurité de signalisation.

III.6.1.3.1.1 Equipement UE

Afin de prendre en charge la négociation de la sécurité de signalisation, les équipements UE de l'architecture IPCablecom doivent prendre en charge le protocole TLS tel que défini dans [IETF RFC 2246].

Les équipements UE doivent prendre en charge la construction et l'interprétation des en-têtes de [IETF RFC 3329] contenant le paramètre "mechanism-name" du champ 'tls'.

III.6.1.3.1.2 Fonction P-CSCF

La fonction P-CSCF doit être à même d'établir des sessions TLS sur la base d'une demande émanant d'un équipement UE. Elle devrait toujours demander des certificats UE, mais si elle n'en reçoit aucun, elle devrait établir un protocole TLS authentifié côté serveur. Si le protocole TLS mutuellement authentifié est établi, la fonction P-CSCF doit fixer le paramètre integrity-protected=yes dans les en-têtes "Authorization". Si le protocole TLS authentifié mutuellement n'est pas établi, la fonction P-CSCF fixe le paramètre integrity-protected=no. Ces règles s'ajoutent aux règles existantes applicables à l'établissement du protocole IPSec. Si le protocole TLS authentifié côté serveur assure l'intégrité, le protocole TLS authentifié mutuellement s'apparente davantage au cas 3GPP du protocole IPSec combiné à l'authentification AKA.

La fonction P-CSCF doit prendre en charge le paramètre "mechanism-name" du champ 'tls' de [IETF RFC 3329]. Cela peut être négocié sous la forme d'une authentification TLS mutuelle ou côté serveur, selon les fonctionnalités de l'équipement UE. Les mêmes règles que celles qui sont décrites ci-dessus s'appliquent à l'attribution des valeurs integrity-protected.

Il convient de valider les certificats conformément à [IETF RFC 3280].

III.6.1.3.1.3 Fonction S-CSCF

La fonction S-CSCF peut mettre à l'épreuve tout message SIP. Les messages contenant des en-têtes Authorize avec un paramètre integrity-protected fixé à 'no' devraient toujours être mis à l'épreuve, étant donné que ce fanion indique l'absence de sécurité de signalisation entre l'équipement UE et la fonction P-CSCF sur les demandes d'enregistrement non initiales. Si la fonction S-CSCF met à l'épreuve, avec succès un abonné, elle doit insérer l'en-tête "P-Asserted-Identity" dans les messages ultérieurs provenant de cet abonné si l'en-tête "P-Asserted-Identity" n'existe pas.

III.6.1.3.2 Désactivation de la sécurité de signalisation

Bien que cela ne soit pas recommandé, il est possible de désactiver la sécurité de signalisation au niveau de la fonction P-CSCF. Du fait de cette désactivation, les équipements UE et le réseau sont exposés à un grand nombre des menaces décrites au § III.5.3, notamment lorsqu'ils sont utilisés conjointement avec une forme d'authentification plus faible telle que l'authentification de type *Digest* du protocole SIP.

L'Appendice I sur la signalisation des messages SIP de l'architecture IPCablecom2 et la spécification delta de l'architecture IPCablecom2 [UIT-T J.366.4] donnent des informations détaillées sur les procédures à suivre pour désactiver la sécurité de signalisation. La principale

différence entre les procédures de désactivation de la sécurité de signalisation est que les demandes de dialogue autres que d'enregistrement doivent à présent être mises à l'épreuve.

III.6.2 Validation de d'identité

Dans les environnements IPCablecom, il faut trouver un moyen, pour les éléments de réseau sécurisés, de transmettre l'identité des abonnés à d'autres éléments ou services et de supprimer l'identité lorsqu'ils communiquent avec des réseaux non fiables. La validation de l'identité constitue le mécanisme qui permet aux éléments et aux services de sécuriser l'identité d'un utilisateur.

Comme indiqué dans [UIT-T J.366.4], le sous-système IMS confie la tâche de la validation de l'identité à la fonction P-CSCF pour tous les messages SIP, en se fondant sur le flux strict décrit au § III.6.1. Une fois que les associations de sécurité (SA) IPSec sont établies et que l'abonné est authentifié, la fonction P-CSCF valide l'identité de l'abonné. En surveillant l'échange de messages SIP en direction de l'équipement UE, la fonction P-CSCF constate que le message "200 OK" provient des abonnés S-CSCF. Ces informations, auxquelles s'ajoute la présence d'associations SA vers l'équipement UE, permet à la fonction P-CSCF de justifier l'authentification réussie de l'équipement UE.

L'architecture IPCablecom2 améliore le sous-système IMS du fait des exigences suivantes:

- une fonction P-CSCF comportant une session TLS établie avec un équipement UE qui constate qu'une réponse 200 OK émane de la fonction S-CSCF pour cet abonné peut valider l'identité de l'identité publique utilisée par cet équipement;
- une fonction P-CSCF ne comportant aucune session TLS établie qui constate une réponse 200 OK émane de la fonction S-CSCF de l'équipement UE pendant l'authentification SIP, ne peut valider l'identité de cet équipement, auquel cas la fonction S-CSCF valide l'identité après l'authentification réussie de l'abonné.

III.6.3 Sécurité de la traversée du dispositif NAT

Les paragraphes ci-après décrivent la sécurité des serveurs STUN et TURN.

III.6.3.1 Serveur STUN

Le protocole STUN [IETF RFC 3489] définit les contremesures à prendre pour se prémunir contre les attaques décrites au § III.5.3.2.2. Il s'agit notamment de recommandations relatives à l'architecture du réseau et de mécanismes d'intégrité des messages fournis par le protocole STUN lui-même. Aucun mécanisme additionnel n'est proposé pour la présente version du présent appendice.

III.6.3.2 Serveur TURN

Le serveur TURN représente une ressource de réseau qui est utilisée pendant la durée d'une connexion, d'où l'importance de la sécurité relative à cette ressource.

Le protocole TURN [ID TURN] définit les contremesures à prendre contrecarrer les attaques décrites au § III.5.3.2.3. Il s'agit notamment de recommandations relatives à l'architecture du réseau et de mécanismes d'intégrité des messages fournis par le protocole TURN lui-même. Aucun mécanisme additionnel n'est proposé.

NOTE – La sécurité relative au serveur TURN est en cours de mise à jour. Des précisions seront fournies une fois que le projet de protocole TURN sera disponible.

III.6.4 Sécurité de la configuration

III.6.4.1 Architecture d'amorçage générique

Il a été reconnu que l'infrastructure d'authentification 3GPP permettait de mettre en œuvre des fonctions d'application dans le réseau et côté utilisateur, en vue d'établir des clés partagées. En conséquence, le projet 3GPP a conçu "l'amorçage de la sécurité d'application" afin d'authentifier

l'abonné en définissant une architecture d'amorçage générique (GBA, g*eneric bootstrappping architecture*) fondée sur le protocole AKA. Les points de référence et les composants de l'architecture GBA sont représentés sur la Figure III.7.

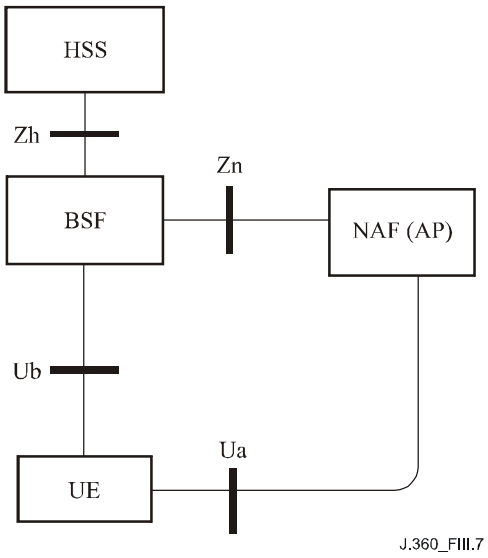


Figure III.7 – Points de référence et composants de l'architecture GBA

Le sous-système IMS décrit actuellement l'architecture d'amorçage générique (GBA) sur la base du protocole AKA. Cette architecture offre à un équipement UE un moyen d'effectuer un amorçage avec un serveur, afin de recevoir des informations sur la configuration et d'obtenir des clés pouvant être utilisées par l'équipement UE et les serveurs d'application en vue de sécuriser les communications sur l'interface UA.

Conformément à [UIT-T J.366.9], une fonction du serveur d'amorçage générique (BSF) et l'équipement UE doivent s'authentifier mutuellement à l'aide du protocole AKA et se mettre d'accord sur des clés de session qui seront utilisées par la suite entre l'association UA et la fonction d'application de réseau (NAF, *network application function*). A cette fin, la fonction BSF doit acquérir les réglages de sécurité de l'utilisateur de l'architecture GBA auprès du serveur HSS et restreindre l'applicabilité des données de clé à une fonction NAF spécifique au moyen d'une procédure d'obtention de la clé. Comme indiqué dans [UIT-T J.366.9], le sous-système IMS utilise l'architecture GBA pour authentifier et recevoir des informations de configuration sur le protocole IPSec. Le sous-système IMS a besoin d'un module ISIM basé sur une carte UICC pour ce processus, étant donné qu'il s'appuie sur le protocole AKA du sous-système IMS pour l'authentification et sur le protocole IPSec pour le transport sécurisé.

Etant donné que l'architecture IPCablecom2 étend le sous-système IMS pour prendre en charge des scénarios de déploiements ne reposant pas sur une carte UICC, le protocole AKA ne peut pas être utilisé par tous les clients IPCablecom pour l'authentification mutuelle entre l'équipement UE et la fonction BSF. En conséquence une nouvelle procédure est nécessaire. L'architecture IPCablecom ajoute une option pour que l'interface Ub prenne en charge l'authentification HTTP de type *Digest* sur le protocole TLS pour l'authentification et l'obtention de clés GBA.

A noter que dans l'architecture IPCablecom2, la fonction NAF est un serveur XCAP, qui fournit la configuration avec l'équipement UE.

Dans le cas d'équipements UE qui ne prennent pas en charge les protocoles IPSec et AKA, lorsque l'équipement UE commence à communiquer avec la fonction NAF, il doit établir un tunnel TLS avec cette fonction. La fonction NAF est authentifiée auprès de l'équipement UE au moyen d'un certificat de clés publiques. L'équipement UE doit vérifier que le certificat du serveur correspond au

nom de domaine complet (FQDN, *fully qualified domain name*) de la fonction NAF avec laquelle il a établi le tunnel. Aucune authentification UE n'est effectuée dans le cadre de la sécurité TLS (c'est-à-dire qu'aucun certificat UE n'est nécessaire). Les interfaces Zh, Zn et Ua sont des interfaces normalisées définies dans [UIT-T J.366.9].

L'interface Ub utilise le mécanisme HTTP de type *Digest* pour établir les justificatifs d'identité (par exemple, la ou les clés de session entre l'équipement UE et la fonction BSF).

Le nouvel échange d'amorçage sur l'interface Ub est illustré sur la Figure III.8.

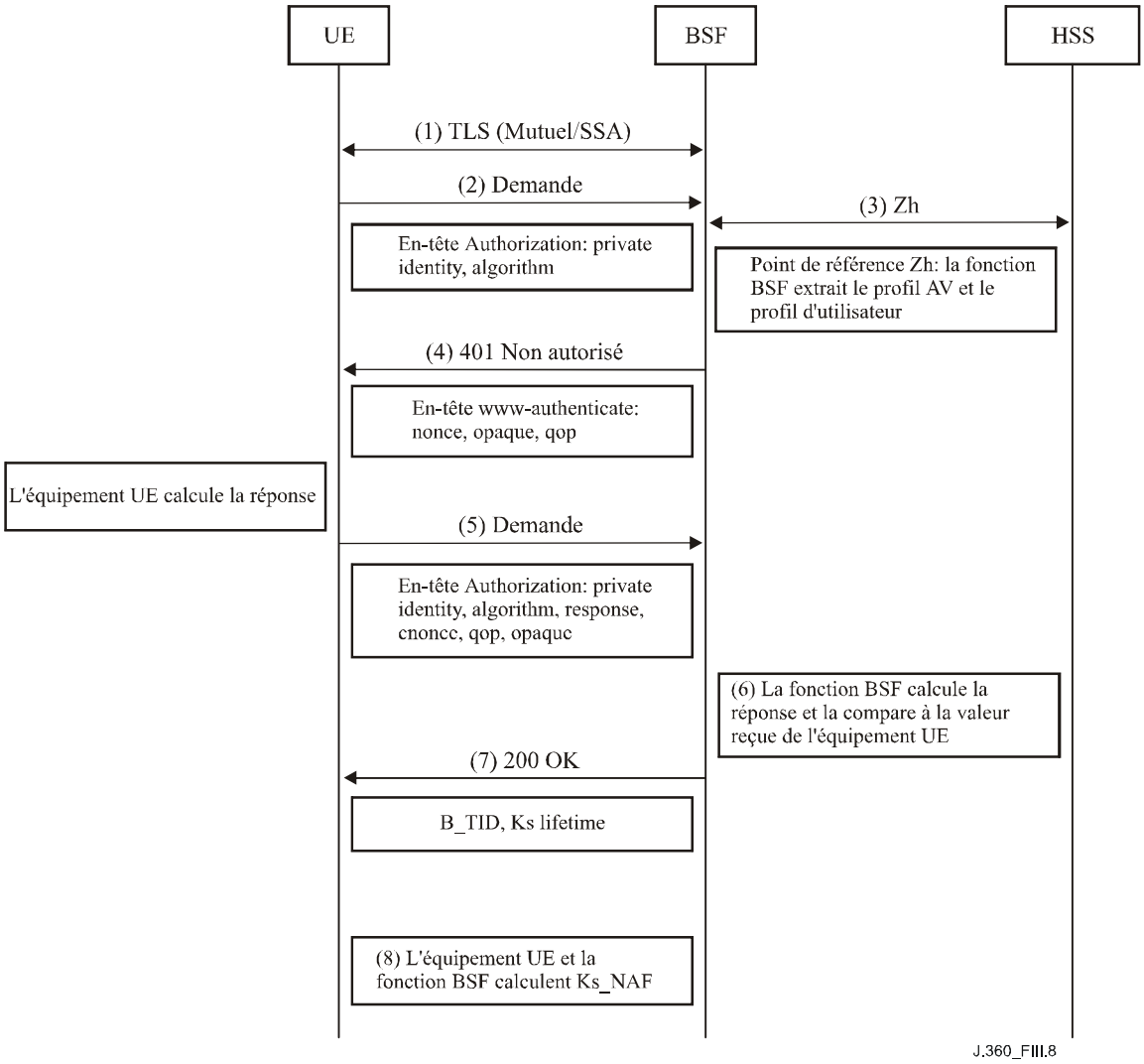


Figure III.8 – Flux de messages de l'architecture GBA

Les mesures suivantes décrivent la procédure d'amorçage applicable au protocole HTTP de type Digest sur le protocole TLS.

1) L'équipement UE engage la procédure d'amorçage en lançant une session TLS avec la fonction BSF. L'équipement UE et la fonction BSF négocient l'authentification TLS côté serveur. L'équipement UE authentifie la fonction BSF au moyen du certificat présenté par cette fonction. La fonction BSF n'impose pas l'authentification de l'équipement UE à ce stade.

2) L'équipement UE engage la procédure d'amorçage en envoyant un message de demande HTTP à la fonction BSF contenant l'identité privée dans un en-tête Authorization. L'équipement UE indique l'algorithme qu'il prend en charge dans le paramètre "algorithm" de l'en-tête Authorization.

3) La fonction BSF envoie une commande MAR au serveur HSS pour extraire un vecteur d'authentification pour cet utilisateur. Le serveur HSS répond avec le vecteur d'authentification approprié pour cet utilisateur et un algorithme dans un message MAA. Le contenu du vecteur d'authentification est amélioré comme dans SIP *Digest* pour permettre à la fonction BSF de calculer une mise à l'épreuve auprès de l'équipement UE, comme indiqué dans [IETF RFC 2617].

NOTE 1 – Dans un environnement comportant plusieurs serveurs HSS, la fonction BSF peut être amenée à obtenir l'adresse du serveur HSS lorsque l'abonnement de l'utilisateur est mémorisé au moyen d'une interrogation de la fonction SLF, avant l'étape 3.

4) La fonction BSF répond à la demande de l'UE en envoyant un message "401 Unauthorized" contenant un en-tête "www-authenticate", afin de contraindre l'UE à s'authentifier. L'en-tête "www-authenticate" comprend un mot créé pour la circonstance conformément aux lignes directrices décrites précédemment dans le présent appendice (c'est-à-dire un mot de 32 octets codé en format hexadécimal ASCII). Le paramètre algorithm informe l'UE de l'algorithme qu'il devrait utiliser pour calculer sa réponse.

5) Lorsqu'il reçoit la mise à l'épreuve, l'équipement UE utilise les données reçues dans l'en-tête "www-authenticate" pour créer une deuxième demande HTTP avec la réponse de mise à l'épreuve dans un en-tête Authorization. La réponse de mise à l'épreuve est calculée conformément à [IETF RFC 2617]. Un paramètre cnonce doit être inclus. L'équipement UE doit sélectionner une valeur du paramètre qop dans la liste des valeurs de paramètres qop envoyée par la fonction BSF. Le message est envoyé à la fonction BSF sur la session TLS.

6) La fonction BSF vérifie la validité de la réponse de mise à l'épreuve envoyée par l'équipement UE en calculant elle-même la réponse et en comparant les valeurs. Cette fonction calcule la réponse conformément à [IETF RFC 2617] et utilise la valeur HA1 fournie par le serveur HSS sur le point de référence Zh.

7) Si la réponse de mise à l'épreuve envoyée par l'équipement UE est identique à la réponse calculée par la fonction BSF, celle-ci doit envoyer à l'équipement UE un message "200 OK" comprenant la valeur B-TID pour indiquer que l'authentification a été fructueuse. En outre, dans un message "200 OK", la fonction BSF doit fournir la durée de vie de la clé Ks.

La valeur B-TID doit être générée au format de l'identificateur d'accès au réseau (NAI, n*etwork access identifier*), en prenant la valeur du paramètre nonce base64 encoded provenant de l'étape 4 et le nom du serveur BSF, c'est-à-dire le paramètre base64encode(nonce)@BSF_servers_domain_name.

NOTE 2 – Avant le codage base64 du mot de circonstance provenant de l'étape 4, le mot de circonstance doit d'abord être converti d'une valeur codée au format hexadécimal ASCII à une valeur codée en binaire.

8) L'équipement UE et la fonction BSF doivent utiliser le secret maître du protocole TLS provenant de la session TLS existante pour la clé Ks. L'équipement UE et la fonction BSF doivent utiliser la clé Ks pour obtenir les données de clé Ks_NAF. Les données de clé Ks_NAF doivent être utilisées pour sécuriser le point de référence Ua.

Les données de clé Ks_NAF sont calculées comme Ks_NAF=KDF(Ks, "gba-h", RAND, IMPI, NAF_Id), où la fonction KDF est la fonction d'obtention de la clé décrite dans l'Annexe B de [UIT-T J.366.9]. Le mot de circonstance codé en binaire est remplacé par la variable RAND basée sur le protocole AKA lors du calcul de Ks_NAF. Ks est le secret maître provenant de la session TLS existante.

L'équipement UE et la fonction BSF doivent mémoriser la clé Ks avec la valeur B-TID associée en vue d'une utilisation ultérieure, jusqu'à ce que la durée de vie de Ks ait expiré ou que la clé soit mise à jour.

La clé Ks sert à obtenir des clés pour les communications avec des serveurs d'application tels que l'élément mise en service, activation et configuration (PAC), en utilisant le point de référence Ua.

III.6.4.2 Téléchargement logiciel sécurisé

Le téléchargement logiciel sécurisé sort du cadre de la présente version du présent appendice.

III.6.5 Sécurité des médias

La sécurité des médias sort du cadre de la présente version du présent appendice.

III.6.6 Utilisation du protocole TLS pour la sécurité intradomaine

Ainsi qu'il est défini dans [UIT-T J.366.8] relative à la spécification IMS-delta, le point de référence Zb connecte d'une manière sécurisée les composants du sous-système IMS à l'intérieur d'un même domaine de confiance. L'implémentation de l'interface Zb est facultative. Si elle est implémentée, cette interface doit utiliser la charge utile ESP du protocole IPSec pour l'authentification et l'intégrité. La confidentialité (chiffrement) est facultative.

L'architecture IPCablecom2 ajoute la prise en charge du protocole TLS pour la sécurité intra-domaine pour les raisons suivantes:

- le protocole TLS constitue le mécanisme de sécurité recommandé spécifié dans [IETF RFC 3261];
- le protocole TLS prend en charge la traversée du dispositif NAT au niveau de la couche du protocole;
- le protocole TLS est implémenté au niveau de l'application et non pas au niveau du noyau, ce qui offre certains avantages comme une prise en charge plus facile dans des environnements multiples.

Les composants de l'architecture IPCablecom2 ayant des interfaces SIP sont tenus de prendre en charge le protocole TLS aux fins de la sécurité intradomaine, en plus du protocole IPSec défini par le sous-système IMS.

Sauf indication contraire dans ce paragraphe, les interfaces SIP exigeant le protocole TLS DOIVENT être conformes à la spécification TLS [IETF RFC 2246] et avec les exigences éventuelles spécifiées dans [IETF RFC 3261] concernant son utilisation dans le protocole SIP.

Le protocole TLS [IETF RFC 2246] prend en charge la négociation et l'utilisation de méthodes de compression, mais comme ces méthodes ne sont pas spécifiées dans TLS [IETF RFC 2246], la compression NE DOIT PAS être utilisée.

III.6.6.1 Algorithmes d'authentification TLS

L'algorithme HMAC-SHA-1 (avec une clé de 160 bits) doit être pris en charge afin de fournir des services d'authentification de l'origine des données et d'intégrité des données dans le protocole TLS. L'algorithme AES-XCBC n'est pas requis.

III.6.6.2 Algorithmes d'échange de clés pour le protocole TLS

On trouvera ci-après les prescriptions relatives aux méthodes d'échange de clés dans le protocole TLS:

- l'algorithme Rivest Shamir Adleman (RSA) doit être pris en charge;
- l'algorithme de Diffie Hellman (DH) doit être pris en charge.

III.6.6.3 Utilisation de certificats X.509 dans le protocole TLS

Les certificats X.509 sont utilisés aux fins de l'authentification dans le protocole TLS et doivent tous être signés par un tiers de confiance. Les certificats autosignés peuvent être utilisés.

III.6.6.4 Générateur de nombres aléatoires pour le protocole TLS

Les mises en œuvre de génération de nombres aléatoires constituent généralement une faiblesse. Un grand nombre de constructeurs de semi-conducteurs ajoutent des générateurs de nombres aléatoires sécurisés dans leurs circuits intégrés, qui doivent être utilisés s'ils sont disponibles. Si aucun matériel n'est disponible, on peut utiliser facultativement un logiciel de générateur de nombres pseudo-aléatoires renforcé conformément à [IETF RFC 1750].

Les prescriptions relatives à la génération de nombres aléatoires sont les suivantes:

- un générateur de nombres aléatoires matériel peut être pris en charge;
- un logiciel de générateur de nombres pseudo aléatoires doit être pris en charge si un générateur de nombres aléatoires matériel n'est pas pris en charge.

III.6.6.5 Algorithmes de chiffrement TLS

Les prescriptions applicables au client TLS et au serveur TLS en ce qui concerne les algorithmes cryptographiques utilisés pour fournir les services de chiffrement à l'association TLS-SA sont les suivantes:

- le mode 3DES CBC (avec 3 clés indépendantes de 56 bits) doit être pris en charge;
- le mode AES CBC (avec une clé de 128 bits) doit être pris en charge;
- le chiffrement néant peut être pris en charge.

III.6.6.6 Suites de chiffres pour le protocole TLS

Le protocole TLS spécifie plusieurs suites de chiffres à utiliser dans le cadre de ce protocole, comme indiqué en détail dans [IETF RFC 3268]. Les suites de chiffres représentent les combinaisons d'algorithmes d'échange de clés et d'authentification de chiffrement recommandées à utiliser dans le cadre du protocole TLS.

Les prescriptions relatives aux suites de chiffres sont les suivantes:

- le champ "TLS_RSA_WITH_NULL_SHA" peut être pris en charge;
- le champ "TLS_RSA_WITH_3DES_EDE_CBC_SHA" devrait être pris en charge;
- le champ "TLS_RSA_WITH_AES_128_CBC_SHA, doit être pris en charge;
- le champ "TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA" devrait être pris en charge;
- le champ "TLS_DH_RSA_WITH_AES_128_CBC_SHA" doit être pris en charge.

III.6.6.7 Authentification TLS

Le protocole TLS permet l'authentification unidirectionnelle, lorsque le serveur est identifié auprès du client seulement, ou l'authentification bidirectionnelle, lorsque le client et le serveur s'authentifient tous deux l'un auprès de l'autre. L'authentification unidirectionnelle est la méthode généralement utilisée dans l'Internet public. Toutefois, pour les applications de signalisation et de commande de réseau, l'authentification bidirectionnelle est obligatoire, afin de permettre aux deux parties de savoir si elles communiquent avec le point d'extrémité voulu.

Les prescriptions relatives à l'authentification TLS sont les suivantes:

- l'authentification bidirectionnelle doit être prise en charge pour les applications TLS.

III.6.7 Validation de certificats

Il convient d'utiliser [IETF RFC 3280] pour obtenir des indications sur la validation des certificats.

III.6.8 Révocation de certificat

La révocation de certificat n'entre pas dans le cadre de la présente version du présent appendice.

Appendice IV

Aperçu du serveur d'abonnés résidentiels (HSS) IPCablecom2

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

A étudier.

Appendice V

Aperçu de la traversée de dispositif NAT et de pare-feu IPCablecom2

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

V.1 Introduction

Le présent appendice donne un aperçu de la manière dont l'architecture IPCablecom2 et les équipements d'utilisateur associés prennent en charge la traversée de dispositifs NA(P)T et de pare-feu (généralement appelés dispositifs NAT) pour les flux de média et de signalisation ainsi que pour l'approvisionnement et la gestion. Pour aider le lecteur à mieux comprendre le mécanisme de traversée de dispositif NAT IPCablecom2 et les méthodes associées, le présent appendice énonce les exigences de haut niveau et décrit les composants logiques et interfaces spécifiques qui sont définis.

V.2 Références

Le présent appendice utilise les références informatives supplémentaires suivantes.

[UIT-T J.179] Recommandation UIT J.179 (2005), *Prise en charge du multimédia pour IPCablecom*.

[UIT-T J.364] Recommandation UIT J.364 (2006), *IPCablecom2 provisioning, activation, configuration and management*.

[IETF RFC 2663] IETF RFC 2663 (1999), *IP Network Address Translator (NAT) terminology and considerations*.

[IETF RFC 3489] IETF RFC 3489 (2003), *Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NAT) (STUN)*.

[ID BEHAVE] IETF draft, draft-ietf-behave-nat-udp-04, *Network Address Translation (NAT) Behavioural Requirements for Unicast UDP*, 6 septembre 2005.

[ID ICE] IETF draft, draft-ietf-mmusic-ice-07, *Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offer/Answer Protocols*, 6 mars 2006.

[ID OUTBOUND] IETF draft, draft-ietf-sip-outbound-03, *Managing Client Initiated Connections in the Session Initiation Protocol (SIP)*, 20 mars 2006.

[ID TURN] IETF draft, draft-ietf-behave-turn-00, *Obtaining Relay Addresses from Simple Traversal of UDP Through NAT (STUN)*, février 2005.

V.3 Termes et définitions

Divers termes liés aux dispositifs NAT sont définis dans [IETF RFC 2663]; on pourra se reporter à ce document pour ce qui est des termes et définitions généraux concernant les dispositifs NAT autres que les termes et définitions figurant ci-dessous. En outre, le présent appendice utilise les termes suivants:

V.3.1 ALG: passerelle de couche application (*application layer gateway*) qui est présente dans un dispositif NAT et qui tente de détecter les messages de signalisation d'application et de modifier les adresses d'application de façon appropriée afin de gérer les modifications causées par le dispositif NAT.

V.3.2 NAT, NAPT: les dispositifs NAT traduisent les adresses IP, interconnectant généralement des domaines d'adresses privées et des domaines d'adresses publiques. Les dispositifs NAPT

traduisent aussi les ports, afin d'économiser les adresses IP. Dans le présent appendice, le terme NAT désigne aussi les dispositifs NAPT.

V.4 Abréviations et acronymes

Le présent appendice utilise les abréviations supplémentaires suivantes:

DQoS qualité de service dynamique (*dynamic quality of service*)

UDPTL couche transport UDP (*UDP transport layer*)

VPN réseau privé virtuel (*virtual private network*)

V.5 Exigences et portée concernant les dispositifs NAT IPCablecom2

Le présent appendice a pour objectif de définir une architecture permettant à un équipement d'utilisateur d'accéder au réseau IPCablecom2 lorsqu'un ou plusieurs dispositifs NAT sont présents. Il décrit en particulier un ensemble complet de mécanismes permettant à un équipement d'utilisateur de maintenir les liens de signalisation et de média pour garantir que le trafic de média et de signalisation destiné à l'équipement d'utilisateur puisse traverser le dispositif NAT, et permettant d'approvisionner et de gérer l'équipement d'utilisateur lorsque celui-ci est situé derrière un dispositif NAT.

En outre, cette architecture permet d'assurer un relais en cas de défaillance de trajets de signalisation grâce à une fonction CSCF proxy (P-CSCF) de secours.

Enfin, cette architecture permet l'interfonctionnement des équipements d'utilisateur avec des dispositifs non-IPCablecom2 qui ne prennent pas en charge les mécanismes requis de traversée de dispositif NAT.

Le paragraphe qui suit énonce l'ensemble des exigences relatives à l'architecture afin d'atteindre l'objectif visé.

V.5.1 Exigences

La liste suivante est la liste des exigences qu'une solution générale de traversée de dispositif NAT devrait respecter afin de prendre en charge les services envisagés pour l'architecture IPCablecom2:

- prendre en charge plusieurs équipements d'utilisateur (sur un ou plusieurs dispositifs) derrière un même dispositif NAT;
- ne pas imposer d'exigence aux dispositifs NAT et ne pas exiger que le réseau ait connaissance de la présence d'un dispositif NAT;
- prendre en charge à la fois les demandes entrantes en provenance d'équipements d'utilisateur et les demandes sortantes à destination d'équipements d'utilisateur passant par un ou plusieurs dispositifs NAT;
- maintenir des liens avec plusieurs fonctions P-CSCF afin d'assurer une fourniture fiable des messages entrants en cas de défaillance d'une fonction P-CSCF;
- prendre en charge la traversée des dispositifs NAT entre l'équipement d'utilisateur et le réseau (dispositif NAT domestique, dispositif NAT dans un réseau visité);
- définir une solution indépendante de l'application: la solution ne devrait pas employer de mécanismes propres à une application qui ne puissent pas être utilisés par d'autres solutions non fondées sur le protocole SIP. Pour les solutions effectivement utilisées, un appui peut devoir être assuré par les applications;
- éviter les trajets de média inutilement longs dus à l' "épinglage" des médias;
- rétablir les communications en cas de défaillance (par exemple en cas de réamorçage de dispositif NAT et de perte des liens NAT).

V.5.2 Portée

La solution de traversée de dispositif NAT IPCablecom2 est limitée aux dispositifs NAT situés dans le réseau d'accès. Dans le cas d'un accès câblé, cela signifie que les dispositifs NAT sont situés entre l'équipement d'utilisateur et le système CMTS. Il est à noter que les adaptateurs E-MTA IPCablecom sortent du cadre du présent document. Toutefois, certaines exigences supplémentaires peuvent être imposées aux adaptateurs E-MTA IPCablecom afin de faire en sorte qu'ils interfonctionnent avec les équipements d'utilisateur IPCablecom2 qui suivent les procédures de traversée décrites dans le présent document et dans d'autres spécifications.

V.5.3 Limitations

Le présent appendice ne porte pas sur la traversée de dispositif NAT et de pare-feu par les flux de média de type télécopie UIT-T T.38 sur la couche (UDPTL).

Pour le moment, le rappel opérateur pour les appels d'urgence (numéro 911 par exemple) lancés sans enregistrement préalable n'est pas pris en charge.

V.6 Eléments de base concernant les dispositifs NAT

Les traductions d'adresse réseau (NAT) traduisent les adresses entre un domaine d'adresses IP et un autre. Le plus souvent, ce mappage est effectué entre un espace d'adresses Internet privées utilisant des adresses réservées à cette fin et un espace d'adresses Internet publiques. Ce mappage est souvent appelé lien NAT étant donné que le dispositif NAT a lié ensemble les n-uplets PrivateIP:AdresseIPPrivée:PortPrivé et AdresseIPPublique:PortPublic pour permettre aux paquets de réponse ultérieurs provenant du point d'extrémité externe d'être retransmis correctement côté interne. Dans le présent appendice, le terme NAT désigne aussi les dispositifs de traduction d'adresse réseau et de port (NAPT), qui traduisent aussi les ports afin de réduire le nombre d'adresses publiques utilisées du côté des adresses publiques du dispositif NAT (voir la section 4 du document [IETF RFC 2663] pour plus de détails).

Outre la traduction d'adresses, les dispositifs NAT remplissent aussi une fonction de pare-feu. En d'autres termes, ils bloquent le trafic entrant (le trafic en provenance de l'extérieur et à destination de l'intérieur du dispositif NAT/FW) sur la base de certaines règles de filtrage.

V.6.1 Types de dispositifs NA(P)T et de pare-feu

Les paragraphes qui suivent utilisent les définitions élaborées par le groupe de travail BEHAVE de l'IETF dans le document [ID BEHAVE].

V.6.1.1 Types de dispositifs NAT

Les définitions figurant dans le document [ID BEHAVE] sont incluses ici dans un souci de commodité:

mappage indépendant du point d'extrémité: le dispositif NAT réutilise le mappage de port pour les paquets ultérieurs envoyés depuis la même adresse IP et le même port internes vers une adresse IP et un port externes quelconques.

mappage dépendant de l'adresse: le dispositif NAT réutilise le mappage de port pour les paquets ultérieurs envoyés depuis la même adresse IP et le même port internes vers la même adresse IP externe, quel que soit le port externe. Si les paquets sont envoyés vers une adresse IP externe différente, le mappage sera différent.

mappage dépendant de l'adresse et du port: le dispositif NAT réutilise le mappage de port pour les paquets ultérieurs envoyés depuis la même adresse IP et le même port internes vers la même adresse IP et le même port externes. Si des paquets sont envoyés vers une adresse IP et/ou un port différents, un mappage différent sera utilisé.

Le Tableau V.1 décrit ces différentes transpositions d'adresse sur la base de l'illustration de la Figure V.1.

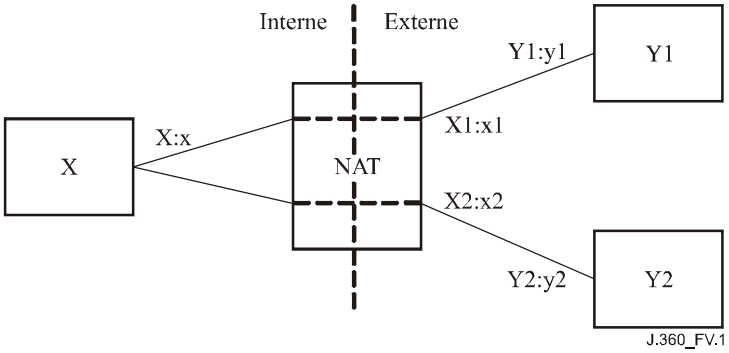


Figure V.1 – Types de dispositifs NAT (mappage d'adresse)

Sur la Figure V.1, l'adresse X:x à l'intérieur du dispositif NAT est traduite en adresse X1:x1 pour les communications avec l'adresse Y1:y1 à l'extérieur du dispositif NAT. La même adresse X:x est traduite en adresse X2:x2 pour les communications avec l'adresse Y2:y2.

Tableau V.1 – Types de dispositifs NAT (mappage d'adresse)

Type de dispositif NAT	Description du mappage
Mappage indépendant du point d'extrémité	X1:x1 est toujours égal à X2:x2 pour toutes les valeurs de Y2:y2
Mappage dépendant de l'adresse	X1:x1 est égal à X2:x2 uniquement si Y1 est égal à Y2
Mappage dépendant de l'adresse et du port	X1:x1 est égal à X2:x2 uniquement si Y1:y1 est égal à Y2:y2

Il est à noter que pour les petits dispositifs NAT (par exemple les dispositifs NAT situés dans les locaux de clients résidentiels), une seule adresse IP (provenant généralement de l'espace d'adresses publiques) est normalement attribuée comme adresse IP externe (X1 = X2). Pour les dispositifs NAT plus grands, l'adresse IP externe attribuée sera choisie dans un ensemble d'adresses IP disponibles.

V.6.1.2 Types de filtrage

Le document [ID BEHAVE] décrit des types de filtrage sur le même schéma:

- filtrage indépendant du point d'extrémité: l'envoi de paquets depuis le côté interne du dispositif NAT à n'importe quelle adresse IP externe suffit pour permettre la réception de paquets quelconques par le point d'extrémité interne;
- filtrage dépendant de l'adresse: pour pouvoir recevoir des paquets provenant d'un point d'extrémité externe particulier, il est nécessaire que le point d'extrémité interne envoie d'abord des paquets à l'adresse IP de ce point d'extrémité externe;
- filtrage dépendant de l'adresse et du port: pour pouvoir recevoir des paquets provenant d'un point d'extrémité externe particulier, il est nécessaire que le point d'extrémité interne envoie d'abord des paquets à l'adresse IP et au port de ce point d'extrémité externe.

Le Tableau V.2 décrit ces types de filtrage sur la base de l'illustration de la Figure V.1.

Tableau V.2 – Types de filtrage

Type de dispositif NAT	Exemple de filtrage
Filtrage indépendant du point d'extrémité	L'envoi de paquets de X:x à Y1:y1 permettra de recevoir les paquets provenant de Y1:y1 ou Y2:y2.
Filtrage dépendant de l'adresse	L'envoi de paquets de X:x à Y1:y1 permettra de recevoir les paquets provenant de Y1:z, quel que soit le port z, mais ne permettra pas de recevoir les paquets provenant d'une autre adresse IP.
Filtrage dépendant de l'adresse et du port	L'envoi de paquets de X:x à Y1:y1 permettra uniquement l'envoi de paquets de Y1:y1 à X:x.

V.6.2 Considérations relatives à la traversée des dispositifs NA(P)T et des pare-feu

Les dispositifs NAT offrent une solution relativement simple à l'épuisement des adresses IP, mais la conséquence est que ces dispositifs affectent de nombreuses applications existantes, en particulier les applications et les protocoles de communication en temps réel (le protocole SIP par exemple), qui dépendent de l'échange d'informations d'adressage dans le protocole proprement dit (parfois dans les lignes d'en-tête SIP ou, plus généralement, à l'intérieur du corps de message SDP de certains messages SIP). En cas d'incapacité à atteindre l'adresse dans le protocole, la réponse envoyée par le destinataire du message ne pourra pas aboutir, ce qui entraînera l'échec de la session. Compte tenu du problème croissant que les dispositifs NAT posent aux protocoles de communication, plusieurs solutions ont été utilisées par le passé et sont proposées pour l'avenir. La liste suivante présente de façon succincte certaines solutions parmi les plus courantes et leurs inconvénients:

- passerelle de couche Application (ALG): une solution consiste pour le dispositif NAT à inclure une passerelle ALG, qui regarde à l'intérieur des messages de protocole et qui les modifie sur la base des liens NAT qu'elle a créés. Toutefois, cela nécessite une mise à jour constante de la passerelle ALG au fur et à mesure de l'évolution des protocoles de manière à préserver le fonctionnement attendu. En outre, cette solution échoue lorsque le protocole inclut un contrôle d'intégrité ou est chiffré;
- une autre solution est celle proposée par le groupe MIDCOM de l'IETF. Dans cette solution, un élément de signalisation commande directement au dispositif NAT d'ouvrir des micro-ouvertures dans le pare-feu pour les médias et d'obtenir les informations de lien NAT nécessaires à la mise à jour des informations d'adressage IP (par exemple SDP) dans le protocole. Toutefois, il faut le concours du dispositif NAT et il faut que le dispositif de signalisation puisse déterminer d'une manière ou d'une autre quel dispositif NAT il doit commander;
- dans le cadre d'autres solutions proposées, un relais de média (un traducteur d'adresse supplémentaire) est inséré directement sur le trajet ou une tunnellisation est assurée à travers le dispositif NAT au moyen de la technologie de VPN. Ces solutions présentent toutes des avantages et des inconvénients mais le principal inconvénient est qu'elles obligent les médias à emprunter le même trajet que la signalisation. Le routage des médias n'est alors pas nécessairement optimal dans certains cas;
- la solution actuellement définie par l'IETF consiste à utiliser la méthode ICE [ID ICE] avec les serveurs STUN [IETF RFC 3489] et TURN [ID TURN] pour les médias, et la méthode Outbound [ID OUTBOUND] pour la signalisation. La méthode ICE permet à un point d'extrémité de découvrir, d'annoncer et de trouver la meilleure adresse de communication en utilisant les mécanismes décrits dans le document [ID ICE] tandis que la méthode Outbound permet au point d'extrémité de gérer activement sa connectivité au réseau SIP en créant et en maintenant des flux vers son ou ses proxys approvisionnés comme décrit dans le document[ID OUTBOUND];

- d'autres solutions sont actuellement examinées par le groupe de travail BEHAVE de l'IETF. Toutefois, elles nécessitent une modification à plus long terme du comportement des dispositifs NAT afin de résoudre les problèmes évoqués.

Outre le problème causé par les protocoles qui imbriquent les informations d'adresse IP dans leur charge utile, les dispositifs NAT causent d'autres problèmes, notamment:

- dans les dispositifs NAT, des temporisations sont associées aux liens NAT et aux micro-ouvertures de pare-feu. Pour les transports UDP, ces liens ont tendance à avoir des durées de vie relativement courtes et si le trafic est absent pendant un certain temps, les liens sont désactivés et les micro-ouvertures sont fermées. Pour éviter cette situation, il faut prévoir des mécanismes permettant de maintenir les liens/micro-ouvertures pour les médias et pour la signalisation;
- l'IETF spécifie que, pour le protocole UDP et des protocoles analogues, le protocole RTP devrait utiliser un numéro de port de destination pair et que le flux RTCP correspondant devrait utiliser le numéro de port de destination immédiatement supérieur (impair). Toutefois, les dispositifs NAT ne respecteront pas cette pratique puisqu'en général, ils ne maintiennent pas ces relations de port;
- un autre problème concerne le routage des messages de signalisation entrants à destination d'équipements d'utilisateur. Ces messages doivent être routés par le biais du dispositif NAT sur une connexion pour laquelle il existe un lien NAT.

Compte tenu des exigences énoncées au § V.5.1, la solution actuelle de l'IETF reposant sur la méthode ICE (pour les médias) et la méthode OUTBOUND (pour la signalisation) a été retenue pour l'architecture IPCablecom2. Non seulement cette solution satisfait les exigences énoncées, mais elle présente aussi l'avantage d'être de plus en plus approuvée par l'industrie.

V.7 Architecture des dispositifs NAT IPCablecom2

La Figure V.2 est un diagramme de référence qui montre les principaux composants et les principales interfaces concernant la traversée de dispositif NAT/FW dans l'architecture IPCablecom2. Le câblo-modem n'est pas représenté car il ne contient pas de fonctions qui se rapportent spécifiquement à la traversée de dispositif NAT ou sur lesquelles cette traversée a une incidence spécifique.

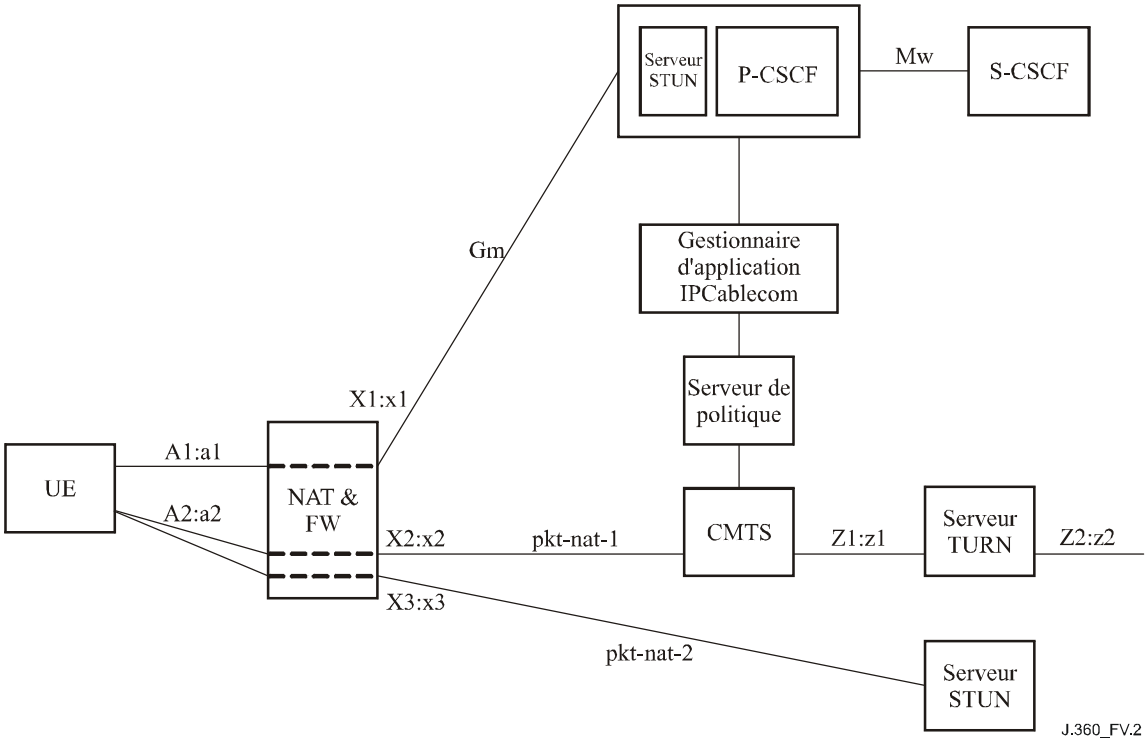


Figure V.2 – Points de référence pour la traversée de dispositifs NAT et FW

Les adresses réseau indiquées dans la Figure V.2 sont de la forme "adresse_IP:port". Il est à noter que:

- pour les équipements d'utilisateur, la même adresse IP est normalement utilisée pour les médias et pour la signalisation: A1 = A2;
- pour les dispositifs NAT/FW situés dans les locaux de clients résidentiels (par exemple déployés dans un environnement résidentiel), normalement X1=X2=X3. Pour les dispositifs NAT plus grands, associés à un plus grand nombre de dispositifs de client, l'adresse IP externe peut être choisie dans un ensemble d'adresses IP.

Il est entendu que d'autres topologies de réseau avec des dispositifs NAT peuvent être rencontrées (dispositif NAT de réseau par exemple). Ces topologies sont actuellement en dehors du domaine d'application de l'architecture IPCablecom2 et ne sont donc pas examinées dans le présent appendice. Certaines topologies de réseau (les points d'interconnexion par exemple) peuvent être considérées comme entrant dans le domaine d'application de l'architecture IPCablecom2 et peuvent être examinées dans d'autres documents.

Tableau V.3 – Points de référence pour les dispositifs NAT IPCablecom2

Points de référence	Eléments de réseau IPCablecom2	Description des points de référence
Gm	UE – P-CSCF	Permet à l'équipement d'utilisateur de communiquer avec la fonction P-CSCF pour l'enregistrement et la commande de session. Ce point de référence, défini dans [UIT-T J.366.4], est fondé sur le protocole SIP.
Mw	CSCF – CSCF	Permet de communiquer et de transmettre des messages de signalisation entre fonctions CSCF pour permettre l'enregistrement et la commande de session. Ce point de référence, défini dans [UIT-T J.366.4], est fondé sur le protocole SIP.

Tableau V.3 – Points de référence pour les dispositifs NAT IPCablecom2

Points de référence	Eléments de réseau IPCablecom2	Description des points de référence
pkt-nat-1	UE – serveur STUN/P-CSCF	Interface de type STUN définie dans le document [IETF RFC 3489] et utilisée par l'équipement d'utilisateur pour déterminer l'adresse IP attribuée au dispositif NAT qui le dessert ou pour garder actifs les liens NAT avec une fonction P-CSCF via un mécanisme de maintien en vie.
pkt-nat-2	UE – serveur TURN	Interface de type TURN définie dans le document [ID TURN] et utilisée par l'équipement d'utilisateur pour demander au serveur TURN des ressources afin de relayer des paquets de média à destination/en provenance de l'équipement d'utilisateur demandeur.

V.7.1 Relation avec l'architecture IPCablecom multimédia

Des éléments fonctionnels issus de l'architecture IPCablecom multimédia [UIT-T J.179] sont également représentés sur la Figure V.2, notamment le gestionnaire d'application (AM) et le serveur de politique (PS). Le présent appendice n'a pas d'incidence sur le fonctionnement de l'architecture IPCablecom multimédia, mais le gestionnaire d'application est tenu de fournir des définitions de classificateur de paquet appropriées pour les flux de média destinés au système CMTS.

Le gestionnaire d'application élabore les classificateurs de paquet pour les flux de média en utilisant l'adresse IP et le port par défaut annoncés dans les lignes "m=" et "c=" du protocole SDP. Lorsqu'un équipement d'utilisateur invoque la procédure ICE et regroupe les adresses possibles, il est tenu d'utiliser l'adresse et le port attribués par le serveur TURN comme adresse par défaut dans le protocole SDP.

Lorsqu'un serveur TURN est utilisé, l'adresse par défaut annoncée dans le protocole SDP comme illustré sur la Figure V.2 est "Z2:z2". Toutefois, elle ne sert pas pour la définition d'un classificateur de paquet; un filtre unique doit donc être disponible dans le protocole SDP pour la description des flux provenant des adresses "X2:x2" et "Z1:z1". Comme le client sait où envoyer les paquets, il connaît la valeur de "Z1:z1" et devra donc la fournir via le protocole SDP (nouvel attribut SDP défini dans [UIT-T J.366.4]).

V.7.2 Relation avec la version 6 du sous-système IMS 3GPP

L'architecture IPCablecom2 est fondée sur la version 6 du sous-système multimédia IP (IMS), définie dans le cadre du projet de partenariat pour la troisième génération (3GPP). Le 3GPP est un accord de collaboration conclu entre différents organismes de normalisation. Il vise à fournir des spécifications techniques et des rapports techniques pour les réseaux GSM et les réseaux de systèmes mobiles de la troisième génération (3G).

La traversée de dispositif NAT et de pare-feu n'est pas prise en charge dans la version 6 du sous-système IMS mais elle doit l'être dans l'architecture IPCablecom2. L'architecture IPCablecom2 contient donc les spécifications supplémentaires requises par rapport aux documents existants relatifs à la version 6 du sous-système IMS. Les modifications apportées au sous-système IMS sont énoncées dans deux spécifications techniques: Rec. UIT-T J.366.3 et [UIT-T J.366.4].

Les modifications énoncées dans la Rec. UIT-T J.366.3 ont pour objet de spécifier la prise en charge de la traversée de dispositif NAT et de pare-feu du point de vue de l'architecture.

Les modifications énoncées dans [UIT-T J.366.4] ont pour objet de décrire les procédures liées à la traversée des dispositifs NAT et des pare-feu par les médias et la signalisation, la méthode Outbound décrite dans le document Internet-Draft [ID OUTBOUND] de l'IETF étant prise en charge pour la signalisation et la méthode d'établissement de connectivité interactive décrite dans le

document Internet-Draft [ID ICE] de l'IETF étant prise en charge pour les médias. Le paragraphe V.8 du présent document contient une description de haut niveau du rôle des éléments de réseau et des interfaces associées concernant la traversée de dispositif NAT.

V.7.3 Relation avec les adaptateurs E-MTA IPCablecom

Le présent appendice ne s'applique pas aux adaptateurs E-MTA IPCablecom. Toutefois, la solution proposée impose aux adaptateurs E-MTA IPCablecom de pouvoir accepter un paquet RTP vide (sans charge utile) avec un type de charge utile égale à 20 (paquet de maintien en vie) en vue du maintien des liens NAT pour les médias.

V.7.4 Approvisionnement et gestion

Outre la prise en charge de la traversée des dispositifs NAT par la signalisation et les médias, il est impératif que l'équipement d'utilisateur puisse être approvisionné et géré lorsqu'il est situé derrière un dispositif NAT. L'approvisionnement désigne les processus utilisés pour initialiser les attributs d'utilisateur et les ressources au niveau de l'équipement d'utilisateur et des composants de réseau afin de fournir des services à un utilisateur. La gestion désigne les protocoles, les méthodes et les interfaces permettant de contrôler, réguler et garantir la disponibilité des services offerts dans le réseau d'un fournisseur de services.

V.7.4.1 Approvisionnement

Le processus d'approvisionnement IPCablecom2 est fondé sur la signalisation SIP standard, en particulier sur les méthodes SUBSCRIBE/NOTIFY (abonnement/notification). Il présente la particularité de se produire avant l'enregistrement de l'équipement d'utilisateur, moment auquel les liens NAT sont généralement créés. Ce processus ayant lieu avant l'enregistrement, la fonction P-CSCF doit tirer parti des concepts liés à la méthode Outbound de l'IETF pour pouvoir fournir la réponse à la demande d'abonnement puis la notification. Pour cela, le plus simple est d'imposer à la fonction P-CSCF d'ajouter un en-tête Record-Route et d'insérer un jeton de flux dans la partie utilisateur de l'identificateur URI utilisé dans la valeur de champ de cet en-tête. Le jeton de flux fait office d'identificateur pour le flux sur lequel le message SUBSCRIBE a été reçu. Le flux permet à la fonction P-CSCF de déterminer l'adresse IP et le port d'origine contenus dans l'en-tête IP de la demande SUBSCRIBE.

En outre, l'équipement d'utilisateur doit faire en sorte que les liens NAT restent actifs pendant la durée de vie de l'abonnement de sorte que le message NOTIFY associé puisse être acheminé.

V.7.4.2 Gestion

Pour le moment, la gestion de l'équipement d'utilisateur sort du cadre du présent appendice et aucune procédure n'a donc été élaborée pour la gestion d'un équipement d'utilisateur situé derrière un dispositif NAT.

V.8 description de l'architecture

Le paragraphe V.7 a décrit un ensemble d'entités de réseau logiques regroupées par fonctions de service particulières (NAT) ainsi qu'un ensemble d'interfaces qui prennent en charge les flux d'informations échangés entre les groupes fonctionnels et les entités de réseau. Le présent paragraphe décrit de façon plus détaillée ces éléments logiques et les interfaces associées de l'architecture IPCablecom2. Il donne en outre un aperçu d'autres questions liées à l'architecture des dispositifs NAT qui ne sont pas abordées ailleurs.

V.8.1 Composants fonctionnels

Le présent paragraphe décrit plus en détails les différents éléments fonctionnels de l'architecture IPCablecom2 et leur rôle dans la traversée de dispositif NAT et de pare-feu.

V.8.1.1 Fonction P-CSCF

Le principal rôle de la fonction P-CSCF dans la traversée de dispositif NAT est de faire en sorte que les demandes et les réponses circulent dans un flux pour lequel il existe un lien NAT. Lorsqu'un enregistrement a lieu, la fonction P-CSCF stocke un jeton d'identification de flux dans l'en-tête path SIP de sorte que, pour les demandes entrantes dans lesquelles un identificateur URI contient ce jeton, elle peut déterminer le flux à utiliser.

La fonction P-CSCF prend aussi en charge l'extension 'rport', qui permet de garantir que toutes les réponses destinées à l'équipement d'utilisateur, y compris celles associées à des demandes de demi-dialogue, sont envoyées à l'adresse IP et au port d'origine d'où la demande a été reçue afin qu'elles puissent traverser le dispositif NAT.

La fonction P-CSCF fait également office de serveur STUN pour permettre à l'équipement d'utilisateur d'utiliser ce serveur pour les messages de maintien en vie et pour détecter les modifications apportées aux liens NAT (par exemple pour détecter les réamorçages de dispositif NAT, entraînant en principe une suppression du flux).

V.8.1.2 Fonction S-CSCF/serveur d'enregistrement

La fonction S-CSCF/le serveur d'enregistrement est chargé de produire et d'attribuer l'identificateur URI d'agent d'utilisateur routable à l'échelle mondiale (GRUU) pour l'équipement d'utilisateur et la fonction P-CSCF associée. La fonction S-CSCF/le serveur d'enregistrement stocke l'identificateur instance-id associé à l'identificateur GRUU ainsi que l'identificateur reg-id et l'en-tête Path et les inclut dans les informations de contact.

V.8.1.3 Equipement d'utilisateur

L'équipement d'utilisateur est chargé de gérer l'ensemble du processus de découverte de dispositif NAT et d'invoquer les divers mécanismes de protocole permettant d'implémenter la solution de traversée de dispositif NAT. Suivant le type d'équipement d'utilisateur (autonome, imbriqué, etc.), les protocoles ou mécanismes suivants sont nécessaires:

- méthode Outbound pour la signalisation;
- client et serveur STUN pour le maintien des liens NAT (signalisation et médias), les contrôles de connectivité (ICE) et le regroupement des adresses possibles (ICE);
- client TURN pour le relais de média;
- méthode ICE pour les médias.

Avant que l'équipement d'utilisateur puisse recevoir des demandes de session entrantes (ou des réponses à des demandes de session sortantes), il devra invoquer les procédures définies dans le document [ID OUTBOUND] pendant le processus d'enregistrement pour créer un flux à destination de la fonction P-CSCF qui lui est attribuée. Une fois que les flux ont été créés, l'équipement d'utilisateur peut ouvrir des sessions et recevoir des demandes de session passant par le dispositif NAT.

Pendant le processus d'établissement de session, l'équipement d'utilisateur applique la méthode ICE pour regrouper, annoncer et tester les adresses possibles.

L'équipement d'utilisateur utilise également le paramètre d'extension 'rport' de l'en-tête Via défini dans le document IETF RFC 3581 pour un routage symétrique des réponses aux messages SIP.

V.8.1.4 Serveurs STUN

Les serveurs STUN reçoivent les demandes de lien STUN et fournissent une réponse contenant l'adresse IP et le port d'origine contenus dans l'en-tête IP de la demande de lien STUN. Deux serveurs STUN sont représentés sur la Figure V.2:

- le serveur STUN représenté en tant que composant fonctionnel de la fonction P-CSCF est utilisé par l'équipement d'utilisateur pour maintenir les liens NAT pour la signalisation. Ces messages STUN peuvent aussi jouer le rôle de messages de maintien en vie, permettant à l'équipement d'utilisateur de déterminer la disponibilité de la fonction P-CSCF;
- le serveur STUN externe apparaissant en bas et à droite de la Figure V.2 est utilisé dans le cadre de la méthode ICE [ID ICE] pour déterminer une adresse de média possible parmi d'autres au moyen du protocole STUN [IETF RFC 3489]. Pour le flux de média avec l'adresse IP d'origine "A2:a2" donné en exemple, l'équipement d'utilisateur obtient l'adresse traduite "X3:x3" via le serveur STUN.

V.8.1.5 Serveur TURN

Outre des serveurs STUN, l'architecture contient aussi un serveur TURN. Celui-ci peut être requis si le dispositif NAT n'utilise pas la transposition indépendante du point d'extrémité (voir § V.6.1.1). Lorsqu'il est utilisé pour le transfert de médias, le serveur TURN joue le rôle de relais de média. L'équipement d'utilisateur envoie des paquets provenant de l'adresse "A2:a2" à l'adresse de serveur TURN "Z1:z1". L'adresse d'origine de ces paquets est d'abord traduite par le dispositif NAT en "X2:x2" puis, après relais par le serveur TURN, l'adresse d'origine devient "Z2:z2". Le serveur TURN relaie aussi les paquets de média en sens inverse: les paquets envoyés à l'adresse "Z2:z2" seront envoyés à l'adresse "X2:x2" puis à l'adresse "A1:a2" via le dispositif NAT. Il est à noter que le serveur TURN assure un filtrage indépendant de l'adresse (voir § V.6.1.2), certaines caractéristiques de filtrage étant identiques à celles d'un dispositif NAT, mais les restrictions de port ne sont pas maintenues, à savoir, si du trafic est envoyé à une adresse IP, le trafic provenant de cette adresse est autorisé quel que soit le port d'où il provient.

Il est à noter qu'un seul flux de média est donné en exemple sur la Figure V.2. En réalité, il peut y avoir plusieurs flux de média, chacun pouvant avoir un flux RTP et un canal de commande RTCP. Les traductions NAT et les mécanismes correspondants de communication s'appliquent aux deux.

V.8.2 Interfaces de protocole et points de référence

Le présent appendice a identifié plusieurs interfaces, ou points de référence, dans l'architecture de traversée de dispositif NAT IPCablecom2. Le présent paragraphe donne un aperçu des diverses interfaces de protocole.

V.8.2.1 Traversée de dispositif NAT par les médias

Les équipements d'utilisateur communiquent par le biais d'un réseau qui contient des composants de signalisation ainsi que des serveurs STUN et TURN pour permettre la traversée de dispositif NAT. Ils prennent en charge les protocoles STUN et TURN ainsi que la méthode ICE. Les exigences associées sont énoncées dans les paragraphes qui suivent. Le diagramme de la Figure V.3 est une représentation abstraite de l'architecture.

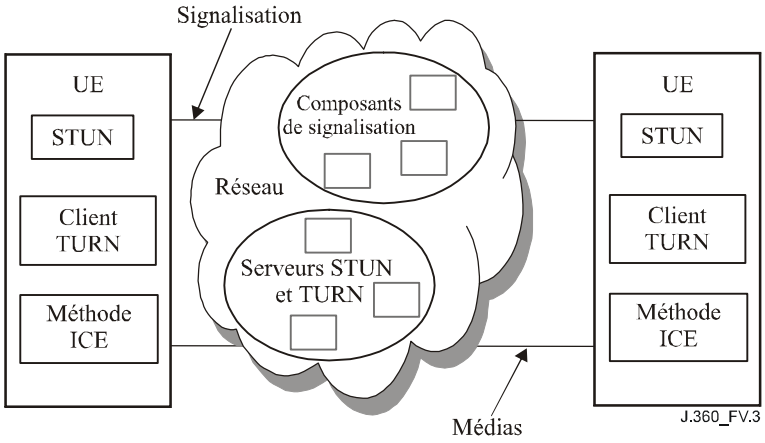


Figure V.3 – Diagramme de référence abstrait

V.8.2.1.1 ICE

La méthode ICE [ID ICE] comporte les étapes suivantes:

- regrouper les adresses possibles pour les communications de média;
- annoncer les adresses possibles ainsi que l'adresse de transport active dans les lignes m/c du protocole SDP;
- procéder à des contrôles de connectivité concernant les adresses possibles afin de choisir une adresse appropriée pour les communications;
- en fonction des résultats des contrôles de connectivité, l'une des adresses possibles peut devenir l'adresse de transport active;
- maintenir les liens pour les médias.

Si l'un des points d'extrémité ne prend pas en charge la méthode ICE, il ignorera tous les attributs "a=candidate" et ne fournira aucun de ces attributs. Dans ce cas, la valeur par défaut figurant dans les lignes m/c sera utilisée et aucun contrôle de connectivité ne sera effectué.

V.8.2.1.2 PKT-NAT-1

La simple traversée d'une traduction NAT par le protocole UDP (STUN) offre un ensemble de fonctions. Ces fonctions permettent aux entités situées derrière un dispositif NAT de connaître les liens d'adresse attribués par le dispositif NAT, de garder ces liens ouverts et de communiquer avec d'autres dispositifs compatibles STUN pour valider la connectivité. Le protocole STUN ne nécessite pas de modifications des dispositifs NAT et fonctionne avec un nombre arbitraire de dispositifs NAT en cascade entre l'entité d'application et l'Internet public.

Le protocole STUN est un protocole client-serveur simple. Un client envoie une demande à un serveur, lequel retourne une réponse. Il existe deux types de demande: les demandes de lien, envoyées sur UDP, et les demandes de secret partagé, envoyées sur TLS sur TCP. Concernant les demandes de secret partagé, le serveur doit retourner un nom d'utilisateur et un mot de passe temporaires, qui sont utilisés dans une demande de lien et une réponse de lien ultérieures aux fins d'authentification et d'intégrité des messages.

Les demandes de lien servent à déterminer les liens attribués par les dispositifs NAT. Le client envoie une demande de lien au serveur, sur UDP. Le serveur examine l'adresse IP et le port d'origine de la demande et les copie dans une réponse qui est retournée au client.

Une fois que le client connaît l'adresse WAN de son dispositif NAT local, il annoncera cette adresse comme adresse possible dans le protocole SDP et les points d'extrémité tenteront de l'atteindre par le biais de la méthode ICE.

V.8.2.1.3 PKT-NAT-2

Le protocole TURN est utile pour les applications qui nécessitent qu'un client place une adresse de transport dans un message de protocole, le but étant que le client puisse recevoir des paquets provenant d'un seul point d'extrémité, qui fera ses envois à cette adresse. Il est par exemple utile pour le protocole SIP, qui utilise le protocole de description de session (SDP). Le protocole SDP achemine une adresse IP à laquelle le client recevra les paquets de média provenant de son homologue. Le protocole TURN est un protocole client-serveur simple. Sa syntaxe et son fonctionnement général sont identiques à ceux du protocole STUN, afin de faciliter une mise en œuvre conjointe des deux protocoles. Le protocole TURN définit un message de demande, appelé Allocate, qui demande au serveur TURN d'attribuer une adresse IP publique et un port. Le protocole TURN peut être exécuté sur UDP et TCP, étant donné qu'il permet à un client de demander des paires adresse/port pour la réception UDP et TCP.

Un client TURN commence par découvrir l'adresse d'un serveur TURN sur la base de la configuration (voir [UIT-T J.364]). Cette adresse peut être préconfigurée sous la forme d'une adresse IP, d'un nom de domaine ou d'un nom FQDN, ce qui permet d'avoir des serveurs TURN différents pour UDP et TCP. Une fois qu'un serveur TURN est découvert, le client lui envoie une demande Allocate TURN. Le protocole TURN offre un mécanisme d'authentification mutuelle et de contrôle d'intégrité pour les demandes et les réponses, sur la base d'un secret partagé. Dans l'hypothèse où la demande est authentifiée et n'a pas été altérée, le serveur TURN attribue une adresse de transport au client TURN, appelée adresse de transport attribuée, et la retourne dans la réponse à la demande Allocate. Normalement, l'adresse de transport attribuée sera située sur l'une des interfaces du serveur TURN proprement dit. Toutefois, le serveur TURN peut aussi se trouver derrière un dispositif NAT, auquel cas l'adresse de transport attribuée peut correspondre au dispositif NAT et est ensuite transposée vers l'adresse privée du serveur TURN. Pour que le serveur TURN fonctionne correctement, de nombreux liens le concernant devront avoir été établis au préalable dans le dispositif NAT; la façon de procéder sort du cadre du présent appendice.

Une fois qu'une adresse TURN est attribuée au client, celui-ci annoncera cette adresse dans la ligne "c=" du protocole SDP. Cette adresse sera donc la première adresse utilisée en attendant de trouver une autre adresse possible correspondant à un meilleur trajet au moyen de la méthode ICE.

V.8.2.2 Gm (traversée de dispositif NAT par la signalisation)

Le présent paragraphe donne un aperçu de haut niveau des procédures définies dans le document "draft-ietf-sip-outbound-03" de l'IETF [ID OUTBOUND] et des rôles des divers éléments de réseau IPCablecom2. Il est à noter que le terme flux est employé dans le document [ID OUTBOUND] et dans les paragraphes qui suivent pour décrire une connexion de couche réseau qui utilise les mêmes adresses IP et ports (UDP ou TCP) à ses deux extrémités.

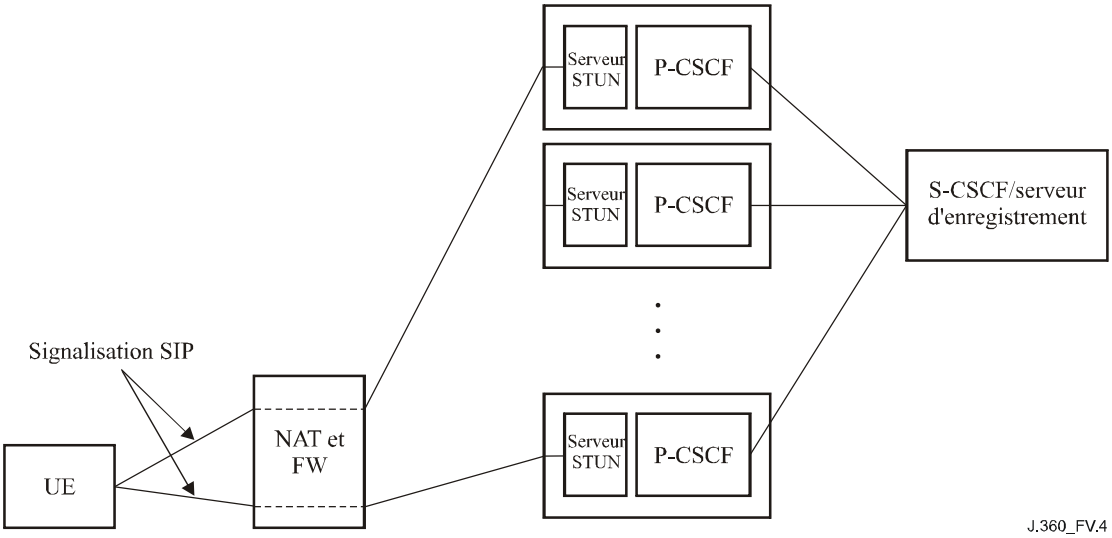


Figure V.4 – Traversée de dispositif NAT par la signalisation SIP

Comme illustré sur la Figure V.4, un équipement d'utilisateur peut se raccorder à un nombre quelconque de fonctions P-CSCF. Toutefois, pour que l'équipement d'utilisateur puisse recevoir des appels entrants, la signalisation doit suivre un trajet pour lequel il existe un lien NAT. Plusieurs liens de ce type peuvent exister sur plusieurs flux à destination de proxys périphériques (par exemple à des fins de redondance). Pour que la signalisation SIP puisse traverser le dispositif NAT, il faut alors:

- établir une connexion sortante: établir un ou plusieurs flux ou connexions de signalisation à destination d'une fonction P-CSCF;
- maintenir les liens NAT et garder ouvertes les micro-ouvertures de pare-feu pour ces flux;
- assurer le routage de la signalisation: pouvoir router les messages de signalisation vers une fonction P-CSCF appropriée ainsi que depuis cette fonction vers l'équipement d'utilisateur sur un flux pour lequel il existe un lien NAT.

V.8.2.2.1 Etablissement d'une connexion sortante

L'enregistrement SIP est utilisé pour établir une connexion sortante et établir des liens NAT pour ce flux. Pendant l'enregistrement:

- l'équipement d'utilisateur établit un identificateur instance-id unique qui reste constant même en cas de réamorçage;
- l'équipement d'utilisateur utilise aussi un identificateur reg-id comme décrit dans le document [ID OUTBOUND] afin d'identifier chaque flux qui est établi avec une fonction P-CSCF. Le protocole STUN est utilisé pour maintenir le flux (à savoir les liens NAT et les micro-ouvertures) en vie;
- l'équipement d'utilisateur inclut les identificateurs instance-id et reg-id lorsqu'il s'enregistre. S'il s'enregistre sur plusieurs flux, il utilise en principe le même identificateur instance-id, mais un identificateur flow-id différent pour des flux différents;
- la fonction P-CSCF retransmet le message REGISTER et inclut un en-tête Path [ID OUTBOUND] afin d'établir un trajet de signalisation entre la fonction P-CSCF située à l'extrémité de la connexion/du flux spécifique et la fonction S-CSCF/le serveur d'enregistrement. La fonction P-CSCF inclut, dans la partie utilisateur d'une route souple dans l'en-tête Path, un identificateur unique afin d'identifier le flux sur lequel l'enregistrement a lieu. La fonction P-CSCF associe ensuite à ce flux toutes les demandes futures qui incluent cet identificateur.

Le serveur d'enregistrement stocke:

- les identificateurs instance-id et reg-id dans les informations de contact en plus de l'heure à laquelle la dernière mise à jour du lien a eu lieu;
- l'en-tête Path.

Il est à noter que plusieurs enregistrements sur différents flux (identificateurs reg-id différents) permettent à l'équipement d'utilisateur de préétablir des canaux de signalisation redondants.

Dans le cas où des équipements d'utilisateur non enregistrés sont autorisés à établir des dialogues (par exemple appels d'urgence, abonnement aux profils de configuration, etc.), toute la signalisation qui a lieu pendant la durée de vie de la session considérée doit être maintenue sur le flux établi pour cette session. Cela suppose que la fonction P-CSCF doive enregistrer la route et faire en sorte que la signalisation pour cette session soit acheminée sur ce flux jusqu'à la fin de la session.

V.8.2.2.2 Maintien des liens NAT

Comme indiqué plus haut, le protocole STUN est utilisé par l'équipement d'utilisateur pour:

- maintenir les liens NAT et garder ouvertes les micro-ouvertures de pare-feu pour la signalisation;
- déterminer si la connexion fait l'objet d'une défaillance;
- déterminer si le lien NAT a changé par suite d'un réamorçage de dispositif NAT.

Le serveur STUN au niveau de la fonction P-CSCF utilise le même port que celui qui est utilisé pour la signalisation associée au flux considéré. L'équipement d'utilisateur envoie des demandes STUN sur le flux afin de maintenir le flux en vie et de déterminer si des liens NAT ont changé par suite d'un réamorçage de dispositif NAT.

V.8.2.2.3 Routage de la signalisation

Il est à noter que la signalisation dans les deux sens doit être établie sur un flux pour lequel il existe des liens NAT. Dans le cas du protocole UDP, cela signifie que les messages SIP sont envoyés et reçus sur le même port UDP.

Par suite des enregistrements, la fonction S-CSCF/le serveur d'enregistrement est capable de mettre à jour les informations de contact (y compris les identificateurs reg-id) et les en-têtes Path, permettant ainsi d'accéder à une instance donnée d'équipement d'utilisateur sur un ou plusieurs flux. Par conséquent, la fonction S-CSCF/le serveur d'enregistrement peut router un appel entrant vers une instance d'équipement d'utilisateur sur un flux donné et, s'il échoue, il peut faire une nouvelle tentative sur un autre flux.

Appendice VI

Aperçu de la stratégie IPv6 et IPv4 IPCablecom2

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

A étudier.

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