UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T J.160

(02/2002)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

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

IPCablecom

Cadre architectural pour l'acheminement de services à temps critique sur les réseaux de télévision par câble utilisant des câblo-modems

Recommandation UIT-T J.160

RECOMMANDATIONS UIT-T DE LA SÉRIE J

RÉSEAUX CÂBLÉS ET TRANSMISSION DES SIGNAUX RADIOPHONIQUES, TÉLÉVISUELS ET AUTRES SIGNAUX MULTIMÉDIAS

Recommandations générales	J.1–J.9
Spécifications générales des transmissions radiophoniques analogiques	J.10–J.19
Caractéristiques de fonctionnement des circuits radiophoniques analogiques	J.20–J.29
Equipements et lignes utilisés pour les circuits radiophoniques analogiques	J.30–J.39
Codeurs numériques pour les signaux radiophoniques analogiques	J.40–J.49
Transmission numérique de signaux radiophoniques	J.50–J.59
Circuits de transmission télévisuelle analogique	J.60–J.69
Transmission télévisuelle analogique sur lignes métalliques et interconnexion avec les faisceaux hertziens	J.70–J.79
Transmission numérique des signaux de télévision	J.80–J.89
Services numériques auxiliaires propres aux transmissions télévisuelles	J.90–J.99
Prescriptions et méthodes opérationnelles de transmission télévisuelle	J.100–J.109
Services interactifs pour la distribution de télévision numérique	J.110–J.129
Transport des signaux MPEG-2 sur les réseaux par paquets	J.130–J.139
Mesure de la qualité de service	J.140–J.149
Distribution de la télévision numérique sur les réseaux locaux d'abonnés	J.150–J.159
IPCablecom	**J.160–J.179**
Divers	J.180–J.199
Application à la télévision numérique interactive	J.200–J.209

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

Recommandation UIT-T J.160

Cadre architectural pour l'acheminement de services à temps critique sur les réseaux de télévision par câble utilisant des câblo-modems

Résumé

La présente Recommandation offre le cadre architectural qui permettra aux opérateurs de télévision par câble de fournir des services à temps critique sur leurs réseaux qui ont été améliorés afin de prendre en charge les câblo-modems.

Source

La Recommandation J.160 de l'UIT-T, élaborée par la Commission d'études 9 (2001-2004) de l'UIT-T, a été approuvée le 13 février 2002 selon la procédure définie dans la Résolution 1 de l'AMNT.

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.

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 responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

Page

Recommandation UIT-T J.160

Cadre architectural pour l'acheminement de services à temps critique sur les réseaux de télévision par câble utilisant des câblo-modems

1 Domaine d'application

La présente Recommandation fait l'objet d'un complément d'étude visant à adapter l'évolution de l'architecture aux nouveaux besoins.

2 Références normatives

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée.

– Recommandation UIT-T G.711 (1988), *Modulation par impulsions et codage (MIC) des fréquences vocales*.

– Recommandation UIT-T J.83 (1997), *Systèmes numériques multiprogrammes pour la distribution par câble des services de télévision, son et données*.

– Recommandation UIT-T J.112, *Systèmes de transmission pour services interactifs de télévision par câble, Annexes A, B et C*.

– Recommandation UIT-T J.161 (2001), *Caractéristiques des codecs audio destinés au service audio bidirectionnel sur les réseaux de télévision par câble utilisant des câblo-modems*.

– Recommandation UIT-T J.162 (2001), *Protocole réseau de signalisation d'appel pour la fourniture de services à temps critique sur les réseaux de télévision par câble de câblo-modems*.

– Recommandation UIT-T J.163 (2001), *Qualité de service dynamique pour la fourniture de services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems*.

– Recommandation UIT-T J.164 (2001), *Prescriptions relatives aux messages d'événement pour la prise en charge des services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems*.

– Recommandation UIT-T J.165 (2002), *Protocole de transport de signalisation IPCablecom*.

– Recommandation UIT-T J.166 (2001), *Structure des bases d'informations de gestion (MIB) IPCablecom*.

– Recommandation UIT-T J.167 (2002), *Prescriptions pour les adaptateurs de terminal multimédia utilisés pour la fourniture de services en temps réel dans les réseaux de télévision par câble utilisant de câblo-modems*.

– Recommandation UIT-T J.168 (2001), *Caractéristiques de la base d'informations de gestion (MIB) de l'adaptateur de terminal de support du système IPCablecom*.

– Recommandation UIT-T J.169 (2001), *Caractéristiques de la base MIB de signalisation d'appel de réseau dans le système IPCablecom*.

– Recommandation UIT-T J.170 (2002), *Spécifications de sécurité IPCablecom*.

– Recommandation UIT-T J.171 (2002), *Protocole de commande de passerelle pour jonctions (TGCP) IPCablecom*.

– Recommandation UIT-T Q.704 (1996), *Fonctions et messages du réseau sémaphore*.

– IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation*.

3 Termes et définitions

La présente Recommandation définit les termes suivants:

3.1 nœud d'accès: dans le cadre de la présente Recommandation dispositif de terminaison de couche 2 formant l'extrémité réseau de la connexion J.112. Dépend de la technique employée. Appelé INA *[adaptateur de réseau interactif (interactive network adapter)]* dans l'Annexe A/J.112 et CMTS *[système de terminaison de câblo-modem (cable modem termination system)]* dans l'Annexe B.

3.2 IPCablecom: projet UIT-T comprenant une architecture et une série de Recommandations permettant la fourniture de services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems.

3.3 câblo-modem: dispositif terminal de couche 2 formant l'extrémité client de la connexion J.112.

3.4 réseau IP géré: réseau IP, géré par une entité unique aux fins du transport de trames de signalisation et d'éléments d'information IPCablecom.

3.5 réseau fédérateur IP géré: réseau IP géré qui est utilisé pour interconnecter des domaines IPCablecom.

4 Abréviations et conventions

4.1 Abréviations

La présente Recommandation utilise les abréviations suivantes:

AN nœud d'accès (*access node*)

ANC contrôleur d'annonces (*announcement controller*)

ANP reproducteur d'annonces (*announcement player*)

ANS serveur d'annonces (*announcement server*)

CM câblo-modem

CMS serveur de gestion d'appels (*call management server*)

CPE équipement des locaux client (*customer premises equipment*)

DHCP protocole de configuration de serveur dynamique (*dynamic host configuration protocol*)

DNS système de noms de domaine (*domain name system*)

DTMF multifréquence à deux tonalités (*dual tone multi-frequency*)

FQDN nom de domaine complet (*fully qualified domain name*)

GC portier (*gate controller*)

HFC hybride fibre/coaxial (*hybrid fibre/coax*)

HTTP protocole de transfert hypertexte (*hypertext transfer protocol*)

IEEE Institut des ingénieurs électriciens et électroniciens (*Institute of Electrical and Electronics Engineers*)

IETF Groupe de travail d'ingénierie Internet (*Internet engineering task force*)

IP protocole Internet (*Internet protocol*)

IPsec sécurité IP (*IP security*)

ISTP protocole de transport de signalisation Internet (*Internet signalling transport protocol*)

ISUP sous-système utilisateur RNIS (*integrated services digital network user part*)

MAC commande d'accès au support physique (*media access control*)

MF multifréquence

MG passerelle média (*media gateway*)

MGC contrôleur de passerelle média (*media gateway controller*)

MIB base d'informations de gestion (*management information base*)

MMH hachage modulaire multilinéaire (*multilinear modular hash*)

MTA adaptateur de terminal de média (*media terminal adapter*)

MTP sous-système transport de messages (*message transfer part*)

NAT traducteur d'adresse de réseau (*network address translator*)

NCS signalisation d'appel par le réseau (*network-based call signalling*)

OSS système d'assistance à l'exploitation (*operational support system*)

QS qualité de service

RKS serveur d'archivage (*record keeping server*)

RTP protocole de transfert en temps réel (*real-time transfer protocol*)

RTPC réseau téléphonique public commuté

SA adresse de source (*source address*)

SCCP sous-système commande de connexions sémaphores (*signalling connection control part*)

SG passerelle sémaphore; passerelle de signalisation (*signalling gateway*)

SID numéro d'identification de système (*system identification number*)

SNMP protocole simple de gestion de réseau (*simple network management protocol*)

TCAP sous-système application pour la gestion des transactions (*transaction capabilities application part*)

TFTP protocole trivial de transfert de fichiers (*trivial file transfer protocol*)

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

TGS serveur-distributeur de tickets (*ticket granting server*)

ToS type de service (*type of service*)

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

4.2 Conventions

Si la présente Recommandation est implémentée, les mots clés "DOIT" (MUST ou SHALL, en anglais) et "REQUIS" doivent être interprétés comme indiquant un aspect obligatoire de la présente spécification.

Les mots clés indiquant un certain niveau d'importance de telle ou telle prescription utilisée dans la présente Recommandation sont résumés:

"doit"	Ce mot ainsi que l'adjectif "REQUIS" indiquent que l'article est une prescription absolue de la présente spécification.
"ne doit pas"	Cette expression indique que l'article est une interdiction absolue de la présente spécification.
"il convient de"	Cette expression ainsi que l'adjectif "RECOMMANDÉ" indiquent qu'il peut, dans des circonstances particulières, exister des raisons valables pour ignorer cet article, mais qu'il convient, avant de faire ce choix, de prendre en considération la totalité des incidences et d'étudier soigneusement le cas.
"il ne convient pas de"	Cette expression indique qu'il peut, dans des circonstances particulières, exister des raisons valables pour que le comportement indiqué soit acceptable ou même utile, mais qu'il convient, avant de faire ce choix, de prendre en considération la totalité des incidences et d'étudier soigneusement le cas.
"peut"	Ce mot ainsi que l'adjectif "FACULTATIF" indiquent que cet article est effectivement facultatif. Un fournisseur peut choisir d'inclure l'article par exemple parce qu'il est requis sur un marché particulier ou parce qu'il améliore le produit, alors qu'un autre fournisseur peut choisir d'omettre ce même article.

5 IPCablecom

5.1 Cadre architectural Cablecom

A un niveau très élevé, l'architecture IPCablecom contient trois réseaux: le "réseau d'accès HFC J.112", le "réseau IP géré" et le RTPC. Le nœud d'accès (AN, *access network*) assure la connexité entre le "réseau d'accès HFC J.112" et le "réseau IP géré". La passerelle sémaphore (SG, *signalling gateway*) et la passerelle média (MG, *media gateway*) assurent la connexité entre le "réseau IP géré" et le RTPC. L'architecture de référence pour l'architecture IPCablecom est décrite dans la Figure 1.

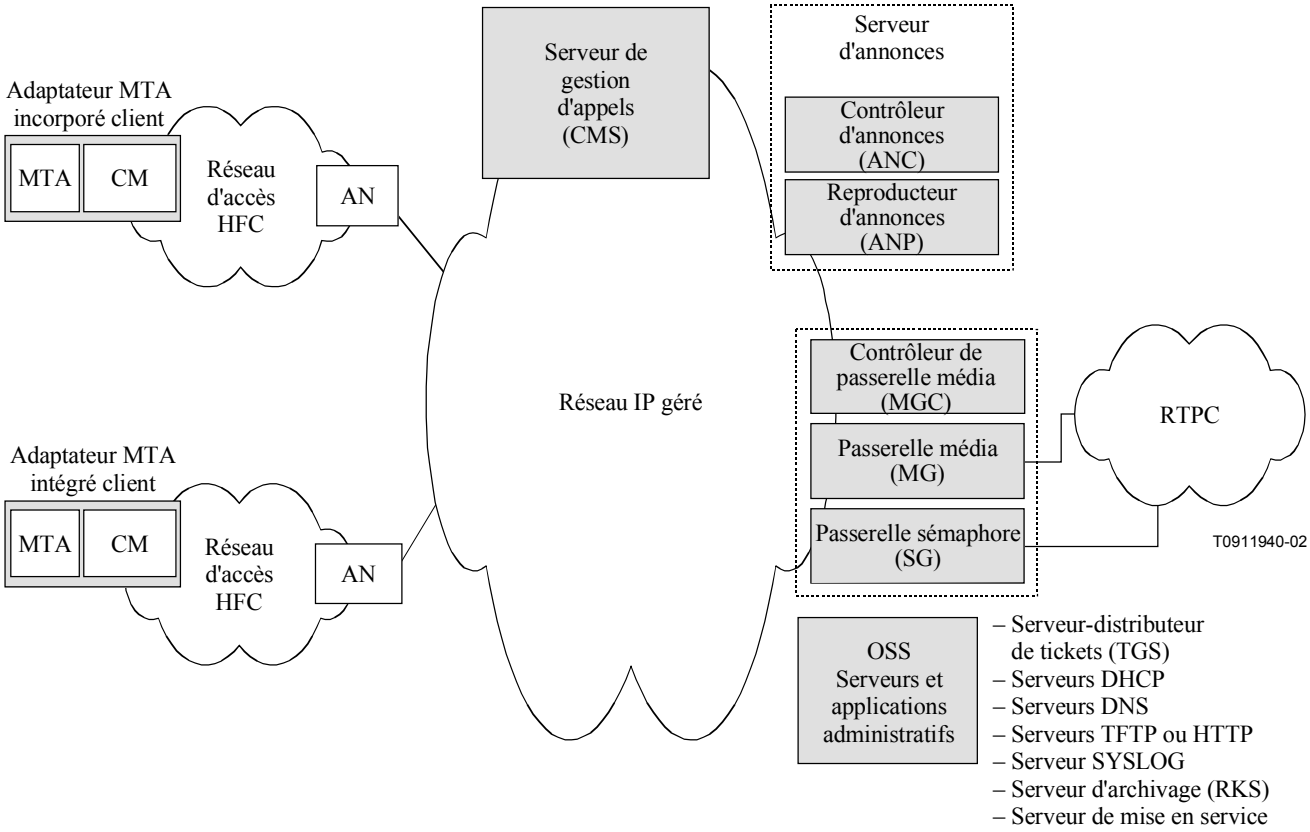


Figure 1/J.160 – Architecture de référence IPCablecom

Le réseau d'accès HFC J.112 assure un transport fiable et sûr à grande vitesse entre les locaux d'abonné et la tête du réseau câblé. Ce réseau d'accès peut offrir toutes les capacités J.112 y compris la qualité de service.

Le réseau IP géré remplit plusieurs fonctions. Premièrement, il assure l'interconnexion entre les composants fonctionnels de base IPCablecom chargés de la signalisation, de la transmission multimédia, de la fourniture et de l'établissement de la qualité de service. Par ailleurs, le réseau IP géré assure la connexité IP à longue distance entre d'autres réseaux IP gérés et les réseaux HFC J.112. Le réseau IP géré comprend les composants fonctionnels suivants: serveur de gestion d'appels (CMS, *call management server*), serveur d'annonces (ANS, *announcement server*), plusieurs serveurs administratifs du système d'assistance à l'exploitation (OSS, *operational support system*), passerelle sémaphore (SG, *signalling gateway*), passerelle média (MG, *media gateway*) et contrôleur de passerelle média (MGC, *media gateway controller*).

Les éléments de réseau indiqués individuellement dans la Figure 1 sont décrits en détail au § 6.

5.2 Zones et domaines IPCablecom

Une zone IPCablecom se compose de l'ensemble des adaptateurs MTA contenus dans un ou plusieurs réseaux d'accès HFC J.112, qui sont gérés par un même serveur CMS, comme indiqué dans la Figure 2. Les interfaces entre composants fonctionnels dans une même zone sont définies dans les spécifications IPCablecom. Les interfaces entre zones (par exemple, CMS-CMS) n'ont pas été définies et seront traitées lors de futurs développements de l'architecture IPCablecom.

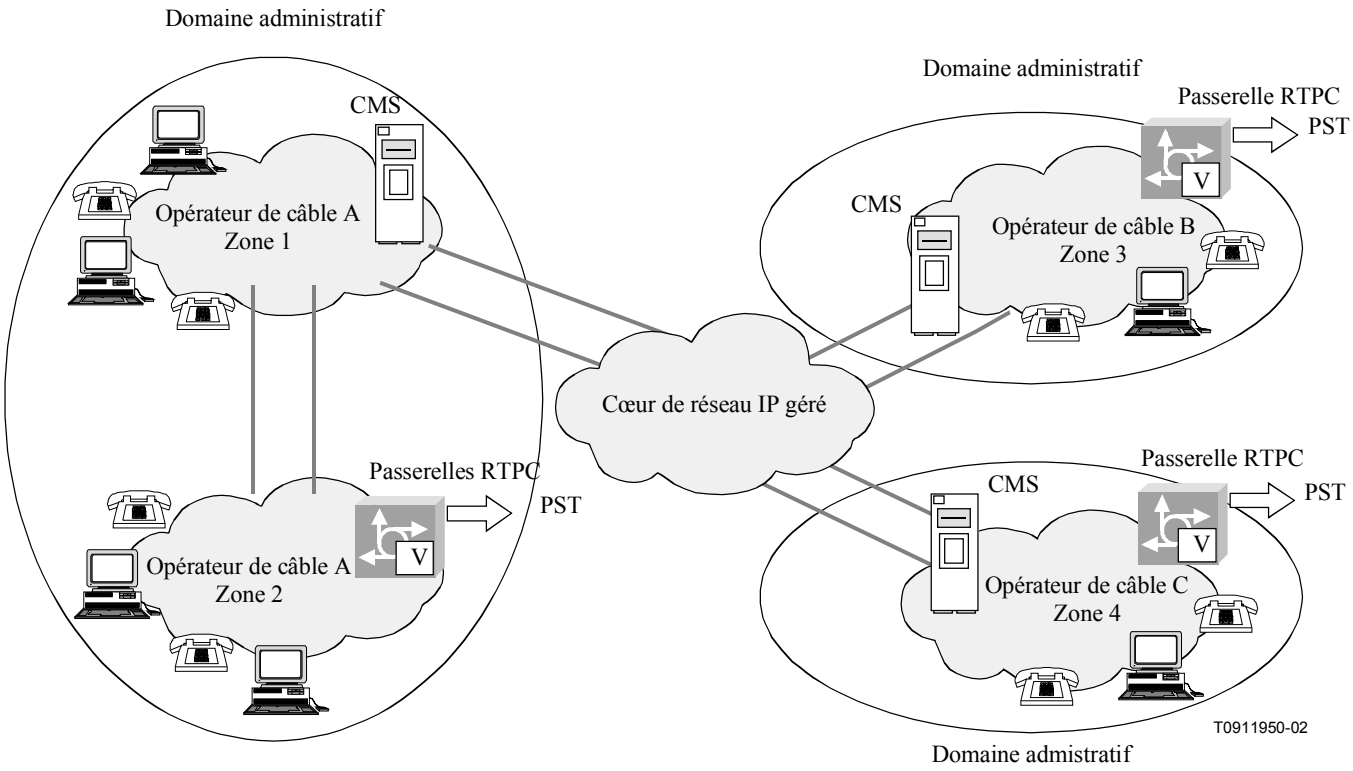


Figure 2/J.160 – Zones et domaines administratifs

Un domaine IPCablecom est constitué d'une ou de plusieurs zones IPCablecom qui sont exploitées et gérées par une seule entité administrative. Un domaine IPCablecom peut également être considéré comme étant un domaine administratif. Les interfaces entre domaines n'ont pas été définies dans l'architecture IPCablecom.

5.3 Recommandations IPCablecom

On trouvera au § 2 une liste des Recommandations IPCablecom. Au cas où un détail technique contenu dans l'une de ces Recommandations serait en contradiction avec la présente Recommandation, ce sont les Recommandations IPCablecom du § 2 qui auraient priorité.

5.4 Considérations relatives à la conception de l'architecture IPCablecom

Le présent paragraphe donne un aperçu général des objectifs et concepts de haut niveau qui ont servi à élaborer les spécifications définissant l'architecture IPCablecom de référence.

5.4.1 Objectifs architecturaux généraux

- Possibilité de capacités de qualité vocale comparables ou supérieures à celles qui sont perçues par l'utilisateur final dans le RTPC.
- Offre d'une architecture de réseau modulable et capable de prendre en charge des millions d'abonnés.
- Assurance que le temps de propagation dans un seul sens pour l'accès IP local et pour la sortie IP (c'est-à-dire à l'exclusion du cœur de réseau IP) puisse répondre aux exigences de temps de propagation pour tous les services IPCablecom en temps réel, y compris la voix.
- Assurance que le taux de perte de paquets, la gigue et le temps de passage (délai) dans le réseau IP géré puissent répondre aux exigences pour tous les services IPCablecom en temps réel, y compris la voix.

- Prise en charge des capacités de communication vocale résidentielle sur ligne primaire et/ou secondaire.
- Amplification des normes existantes. L'architecture IPCablecom s'efforce de spécifier des normes industrielles ouvertes et agréées qui ont été largement adoptées dans les réseaux de communication du marché. Ces normes incluent celles qui ont été approuvées par l'UIT, par l'IETF, par l'IEEE et par d'autres organisations de normalisation des communications.
- Amplification et prise en charge des capacités de transport de données et de qualité de service offertes par l'infrastructure J.112.
- Définition d'une architecture permettant à des vendeurs multiples de mettre au point rapidement des solutions compatibles à coût réduit afin de répondre aux délais imposés de mise sur le marché.
- Assurance que la probabilité de bloquer un appel puisse être aménagée de façon à répondre aux exigences du fournisseur de services.
- Veiller à ce que les coupures de communication et les dérangements téléphoniques puissent être ramenés à un taux inférieur à 1/10 000 appels efficaces.
- Prise en charge des modems (jusqu'au débit V.90 de 56 kbit/s) et des télécopieurs (jusqu'au débit de 14,4 kbit/s).
- Assurance que les glissements de trames dus à des horloges d'échantillonnage non synchronisées ou à des pertes de paquets se produiront à un taux inférieur à 0,25/min de signalisation d'appel.
- Définition d'un paradigme de signalisation fondé sur le réseau.
- Assurance d'une signalisation d'appel de bout en bout pour les modèles d'appel suivants:
  - appels provenant du RTPC et aboutissant au réseau câblé;
  - appels provenant du réseau câblé et aboutissant à une certaine zone IPCablecom dans ce réseau câblé;
  - appels provenant du réseau câblé et aboutissant au RTPC;
  - appels provenant d'une certaine zone IPCablecom et aboutissant à une autre zone IPCablecom (pour étude complémentaire);
  - appels provenant du RTPC, transitant par le réseau IPCablecom et aboutissant au RTPC: ces appels ne sont pas spécifiquement pris en compte dans la présente architecture.
- Assurance d'une signalisation prenant en charge les éléments de service suivants:
  - appel en attente;
  - annulation d'appel en attente;
  - renvoi d'appel (sur non-réponse, sur occupation, variable);
  - conférence à trois;
  - indicateur de message vocal en attente;
  - acheminement du numéro appelant;
  - acheminement du nom de l'appelant;
  - acheminement de l'identité de l'appelant en attente;
  - blocage de l'acheminement de l'identité de l'appelant;
  - rejet des appels anonymes;
  - rappel automatique de l'appelant;
  - rappel automatique de l'appelé;
  - sonnerie spéciale/appel en attente;

– suivi demandé par un client

- Prise en charge d'un paradigme compatible avec les normes de téléphonie IP existantes pour usage dans un réseau IPCablecom d'opérateur de câble et lors d'une connexion au RTPC.
- Capacité de composer directement tout numéro téléphonique national ou international (adresse UIT-T Rec. E.164).
- Capacité de recevoir un appel provenant de tout numéro téléphonique national ou international pris en charge par le RTPC.
- Assurance qu'un nouvel abonné sera en mesure de conserver son numéro téléphonique actuel au moyen de la portabilité du numéro local (LNP, *local number portability*).
- Capacité d'utiliser l'opérateur de son choix pour les communications à grande distance, ce qui inclut la présélection et la sélection appel par appel.
- Prise en charge du blocage d'appel et des restrictions d'accès à l'interurbain par blocage d'appel (par exemple, blocage des appels à destination de préfixes spécifiques).

5.4.2 Qualité de service

- Offre d'un riche assortiment de mécanismes contractuels de fourniture et de gestion de QS pour les services IPCablecom sur le réseau d'accès.
- Offre de mécanismes de contrôle d'admission dans les deux sens (amont et aval).
- Possibilité de modifications dynamiques de la QS au milieu de communications IP IPCablecom.
- Garantie d'un accès transparent à tous les mécanismes de QS définis dans la Rec. UIT-T J.112. Les clients IPCablecom n'auront pas besoin d'être informés des primitives et paramètres spécifiques de QS J.112.
- Réduction au minimum et prévention d'une utilisation abusive de la QS, y compris les attaques par vol de service et par refus de service. Garantie que la politique de QS est fixée et appliquée par des éléments de réseaux IPCablecom habilités.
- Mise en service d'un mécanisme de priorités pour les services d'urgence et pour les autres services de signalisation fondés sur les priorités.

5.4.3 Codecs et flux médias

- Réduction au minimum des effets du délai, de la perte de paquets et de la gigue sur la qualité vocale dans l'environnement de téléphonie IP.
- Définition d'un assortiment minimal de codecs audio qui doivent toujours être pris en charge par tous les dispositifs d'extrémité (MTA) IPCablecom. Les critères d'évaluation des codecs obligatoires sont choisis comme étant les plus efficaces en termes de qualité vocale, de taux d'utilisation de la largeur de bande et de complexité d'implémentation.
- Prise en compte des technologies évolutives des codecs à bande étroite et à large bande.
- Spécification de mécanismes d'annulation d'écho et de détection d'activité vocale.
- Prise en charge de la transmission et de la détection transparente et sans erreur des fréquences DTMF.
- Prise en charge de dispositifs terminaux pour les sourds et malentendants.
- Mise en service de mécanismes pour la commutation du codec lorsque des services de télécopie et de modem sont requis.

5.4.4 Mise en service de dispositifs et de systèmes logistiques

- Prise en charge de la mise en service dynamique ou statique d'équipement des locaux client (adaptateurs MTA et CM).

- Absence de nécessité de réinitialiser les adaptateurs MTA lors de modifications de mise en service.
- Possibilité d'attribution et de gestion dynamiques d'adresses IP pour les dispositifs d'abonné.
- Garantie que la mise en service et la configuration en temps réel des logiciels d'adaptateurs MTA n'ont pas d'incidence défavorable sur le service à l'abonné.
- Définition de bases MIB du protocole SNMP pour la gestion de l'équipement des locaux client (MTA).

5.4.5 Sécurité

- Possibilité d'offrir des capacités téléphoniques résidentielles avec un niveau de confidentialité perçu égal ou supérieur à celui du RTPC.
- Protection contre les attaques visant les adaptateurs MTA.
- Protection de l'opérateur de câble contre diverses attaques par refus de service, interruption du réseau et vol de service.
- Caractéristiques de conception incluant la confidentialité, l'authentification, l'intégrité, la non-répudiation et le contrôle d'accès.

5.4.6 Réseau IP géré

Il est nécessaire de fixer au réseau des limites relatives aux objectifs de QS, comme la perte de paquets traversant le réseau.

6 Composants fonctionnels de l'architecture IPCablecom

Les composants fonctionnels qui sont présents dans un réseau IPCablecom (voir Figure 3) seront décrits dans le présent paragraphe. Ces descriptions ne visent pas à définir ou à impliquer des exigences d'implémentation de produit mais seulement à indiquer le rôle fonctionnel de chacun de ces composants dans l'architecture de référence. Noter que des implémentations de produit spécifiques pourront combiner ces composants fonctionnels selon les besoins. Il n'est pas obligatoire que tous les composants soient présents dans un réseau IPCablecom.

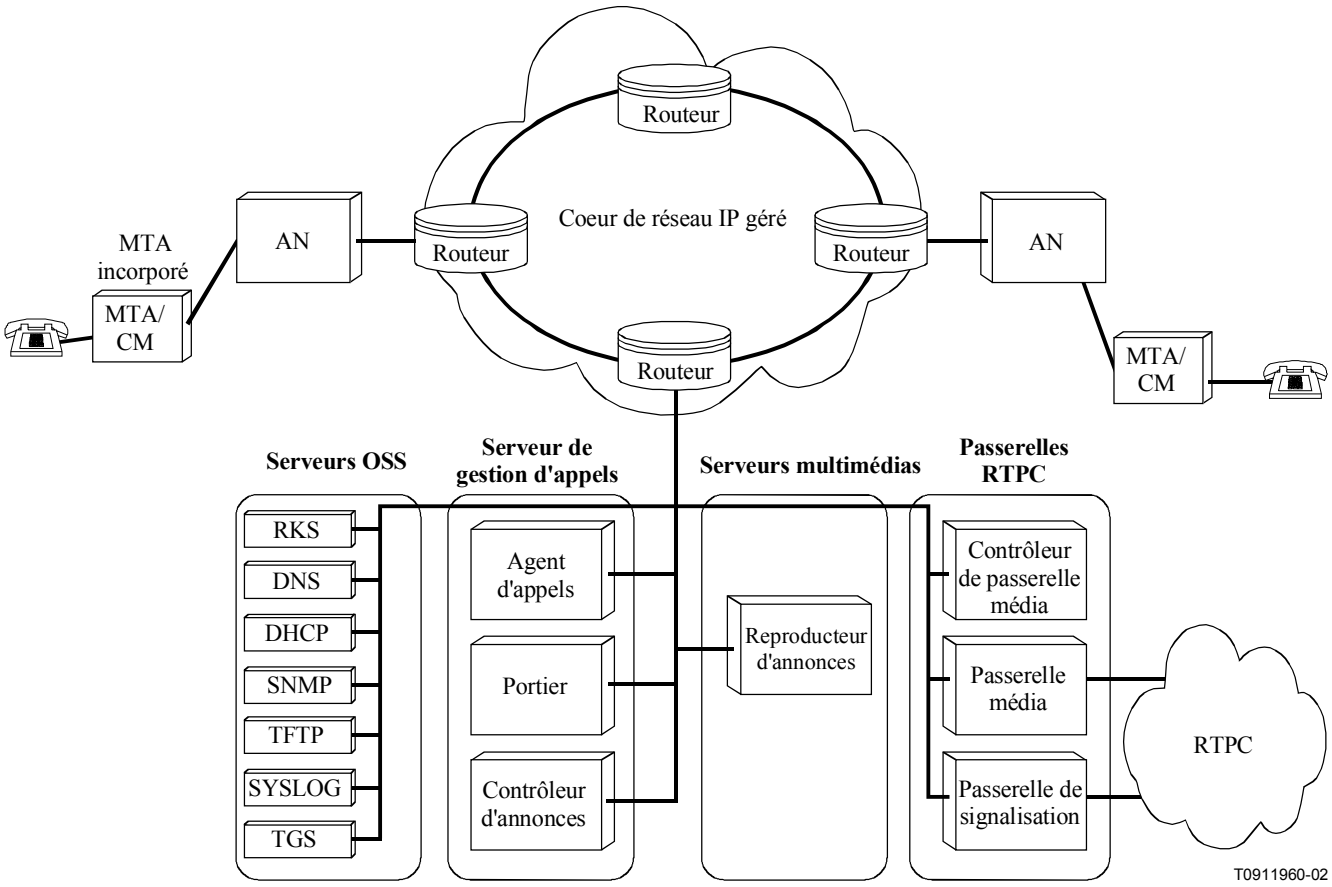


Figure 3/J.160 – Modèle de référence des composants IPCablecom

L'architecture IPCablecom contient des éléments de réseau sécurisés et non sécurisés. Normalement, les éléments de réseau sécurisés sont situés dans le cœur de réseau géré d'un opérateur de câble. Les éléments de réseau non sécurisés, comme les câblo-modems et les adaptateurs MTA, sont normalement situés chez l'abonné et en dehors des installations de l'opérateur de câble.

6.1 Adaptateur de terminal multimédia (MTA)

Un adaptateur MTA est un dispositif client IPCablecom qui contient une interface du côté abonné avec l'équipement local d'abonné (comme un poste téléphonique) et une interface de signalisation du côté réseau avec des éléments de commande d'appel situés dans le réseau. Un adaptateur MTA fournit des codecs et toutes les fonctions de signalisation et d'encapsulation requises pour le transport multimédia et la signalisation d'appel.

Les adaptateurs MTA résident du côté client et sont connectés à d'autres éléments de réseau IPCablecom par l'intermédiaire du réseau d'accès HFC (J.112). Les adaptateurs MTA de l'architecture IPCablecom sont nécessaires pour prendre en charge le protocole de signalisation d'appel par le réseau (NCS, *network call signalling*).

Un adaptateur MTA intégré (E-MTA) est un dispositif matériel isolé qui comporte un câblo-modem ainsi qu'un composant MTA IPCablecom. La Figure 4 montre un schéma fonctionnel représentatif d'un adaptateur E-MTA.

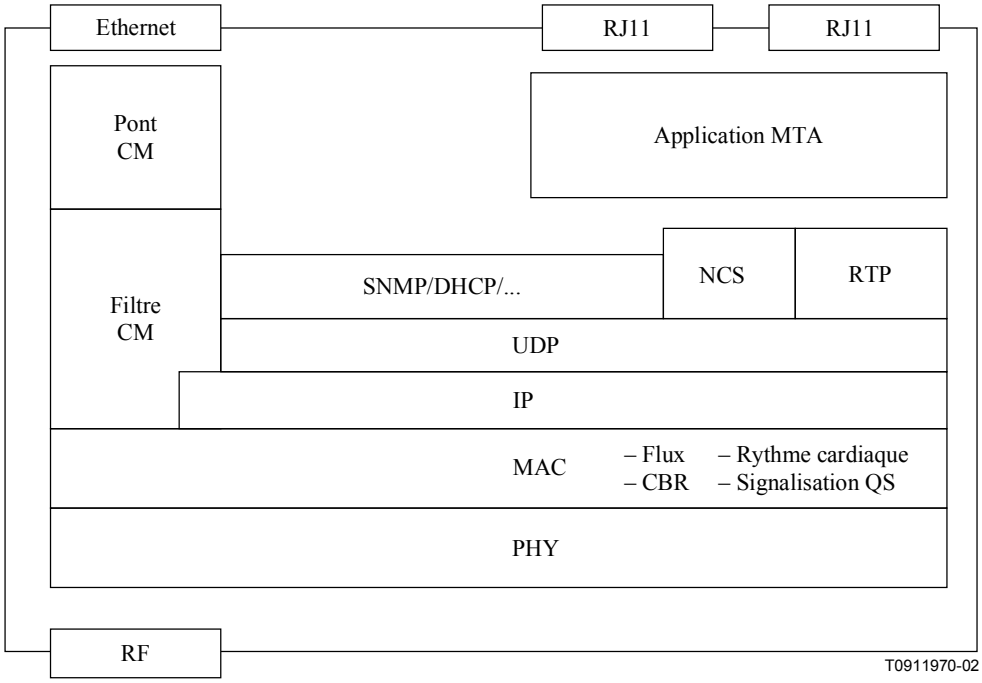


Figure 4/J.160 – Architecture fonctionnelle conceptuelle de l'adaptateur MTA incorporé

Les spécifications IPCablecom ne nécessitent que la prise en charge des adaptateurs MTA incorporés. Dans tout le texte de la présente Recommandation, le terme adaptateur MTA désignera un adaptateur MTA incorporé, sauf indication contraire.

6.1.1 Exigences fonctionnelles relatives aux adaptateurs MTA

Un adaptateur MTA est chargé des fonctions suivantes:

- signalisation d'appels par le protocole NCS au moyen du serveur CMS.
- signalisation de QS avec le serveur CMS et le réseau d'accès.
- authentification, confidentialité et intégrité de certains messages entre l'adaptateur MTA et d'autres éléments de réseau IPCablecom.
- mappage de flux médias sur les services de commande MAC du réseau d'accès J.112.
- codage/décodage de flux média.
- fourniture de multiples indicateurs audio relatifs aux téléphones, comme les tonalités de sonnerie, les tonalités d'appel en attente, la tonalité de bégaiement, la tonalité d'invitation à numéroter, etc.
- signalisation de ligne analogique RTPC normale pour tonalités audio, transport de signaux vocaux, signalisation d'identité de l'appelant, tonalités DTMF et indicateurs de message en attente.
- codec audio G.711.
- une ou plusieurs interfaces analogiques et/ou BRI du RNIS.

D'autres fonctions d'adaptateur MTA sont définies dans d'autres spécifications IPCablecom.

6.1.2 Identificateurs d'adaptateur MTA

Les identificateurs suivants caractérisent les adaptateurs E-MTA:

- un adaptateur MTA incorporé possède deux adresses de commande MAC: l'une pour le câblo-modem, l'autre pour l'adaptateur MTA.

- un adaptateur MTA incorporé possède deux adresses IP: l'une pour le câblo-modem, l'autre pour l'adaptateur MTA.
- un adaptateur MTA incorporé possède deux noms de domaine complets (FQDN, *fully qualified domain names*): l'un pour le câblo-modem, l'autre pour l'adaptateur MTA.
- au moins un numéro téléphonique par accès physique configuré.
- les capacités du dispositif.
- le serveur CMS associé à l'adaptateur MTA.

6.2 Câblo-modem (CM)

Modulateur-démodulateur situé dans le local d'abonné, qui assure la transmission de données dans le réseau câblé au moyen du protocole J.112. Dans l'architecture IPCablecom, le câblo-modem joue un rôle clé pour traiter le flux média. Il fournit des services tels que la classification du trafic en flux de service, conformation du débit et mise en attente selon les priorités.

6.3 Réseau d'accès HFC

Les services de type IPCablecom sont acheminés par le réseau d'accès hybride fibre/coaxial (HFC, *hybrid fibre/coax*). Le réseau d'accès est un système à partage de média dans les deux sens qui se compose du câblo-modem, du nœud d'accès et des couches d'accès MAC et PHY de la Rec. UIT-T J.112.

6.4 Nœud d'accès (AN)

Le nœud d'accès assure la connexité des données et remplit une fonction complémentaire de celle des câblo-modems dans le réseau d'accès HFC. Il assure également la connexité avec les réseaux de zone étendue. Le nœud d'accès est situé dans la tête du réseau de télévision par câble ou dans le concentrateur-répartiteur.

Le nœud d'accès est chargé des fonctions suivantes:

- assurer au câblo-modem la QS requise sur la base de la configuration contractuelle;
- attribuer la largeur de bande amont conformément aux demandes du câblo-modem et aux politiques de QS dans le réseau;
- classifier chaque paquet arrivant de l'interface côté réseau et lui attribuer un niveau de QS fondé sur des spécifications de filtrage définies;
- application de la politique relative au champ de type de service (TOS) dans les paquets reçus du réseau câblé afin d'appliquer les réglages de ce champ conformément à la politique de l'opérateur de réseau;
- modification du champ de type TOS dans les en-têtes IP aval sur la base de la politique de l'opérateur de réseau;
- application de la conformation de trafic et de la politique conformément à la spécification du flux;
- renvoi des paquets aval au réseau J.112 avec la QS assignée;
- renvoi des paquets amont aux dispositifs du cœur de réseau avec la QS assignée;
- conversion et classification des paramètres de porte QS en paramètres de QS J.112;
- signalisation et réservation de l'éventuelle QS de cœur de réseau qui serait nécessaire pour effectuer la réservation de service;
- enregistrement du taux d'utilisation des ressources appel par appel au moyen de messages événementiels IPCablecom.

6.4.1 Porte AN

Composant fonctionnel du nœud d'accès qui effectue la classification du trafic et qui met en œuvre la politique de QS dans les flux médias comme indiqué par le portier (GC, *gate controller*).

6.5 Serveur de gestion d'appels (CMS)

Le serveur de gestion d'appels fournit les services associés à la commande et à la signalisation d'appel à l'adaptateur MTA, au nœud d'accès et aux passerelles RTPC dans le réseau IPCablecom. Le serveur CMS est un élément de réseau sécurisé qui réside dans la partie IP gérée du réseau IPCablecom.

Un serveur CMS du réseau IPCablecom se compose des composants logiques suivants de l'architecture IPCablecom:

– **agent d'appel (CMS/CA)** – terme souvent utilisé comme synonyme de serveur CMS, surtout dans le protocole MGCP. Dans un réseau IPCablecom, l'agent d'appel (CA) est le composant de commande du serveur CMS qui est chargé de fournir à l'adaptateur MTA des services de signalisation au moyen du protocole NCS. A ce propos, les tâches de l'agent d'appel sont, entre autres, les suivantes:
  - implémentation des éléments d'appel;
  - maintien de l'état d'avancement de l'appel;
  - utilisation de codecs dans l'adaptateur MTA de l'abonné;
  - collecte et prétraitement des chiffres composés;
  - collecte et classification des actions d'utilisateur.

– **portier (CMS/GC)** – composant logique de gestion QS implanté dans le serveur CMS, qui coordonne toutes les autorisations et commandes de qualité de service. La fonction de portier est définie dans la spécification relative à la qualité de service dynamique;

Le serveur CMS peut également contenir les composants logiques suivants:

– **contrôleur de passerelle média (MGC)** – composant logique de gestion de signalisation servant à commander les passerelles médias du RTPC. La fonction de contrôleur MGC sera définie en détail dans le présent paragraphe;

– **contrôleur d'annonces (ANC)** – composant logique de gestion de signalisation servant à commander des serveurs d'annonces du réseau. La fonction de contrôleur ANC est définie en détail au § 6.8.

Le serveur CMS peut également remplir les fonctions suivantes:

- gestion d'appel et caractéristiques améliorées;
- services d'annuaire et conversion d'adresse;
- routage d'appel;
- enregistrement du taux d'utilisation des services de portabilité de numéro local;
- signalisation d'appel de zone à zone (pour étude complémentaire) et commande d'admission de QS.

Dans le cadre de la présente Recommandation, les protocoles qui implémentent les capacités du serveur CMS sont spécifiées comme aboutissant à ce serveur. Les implémentations proprement dites pourront répartir ces capacités entre un ou plusieurs serveurs situés "derrière" le serveur de gestion d'appels.

6.6 Passerelle RTPC

L'architecture IPCablecom permet aux adaptateurs MTA d'interfonctionner avec le RTPC actuel au moyen de passerelles RTPC.

Afin que les opérateurs puissent minimiser les coûts et optimiser leurs configurations d'interconnexion, la passerelle RTPC se subdivise en trois composants fonctionnels comme suit:

- **contrôleur de passerelle média (MGC)** – maintient l'état d'appel et commande le comportement général de la passerelle RTPC;
- **passerelle sémaphore (SG)** – remplit une fonction d'interconnexion de signalisation entre le réseau de signalisation C7 du RTPC et le réseau IP;
- **passerelle média (MG)** – termine les conduits supports et transcode les médias entre le RTPC et le réseau IP.

6.6.1 Contrôleur de passerelle média (MGC)

Le contrôleur de passerelle média reçoit et soumet à médiation les informations de signalisation d'appel entre le réseau IPCablecom et le RTPC. Il maintient et commande l'état d'appel général des communications nécessitant une interconnexion avec le RTPC.

Le contrôleur MGC commande les passerelles MG en leur donnant l'ordre de créer, de modifier et de supprimer des connexions prenant en charge le flux média dans le réseau IP. Le contrôleur MGC donne également aux passerelles médias l'ordre de détecter et de produire des événements et signaux tels que les ondes pilotes de continuité pour jonctions de l'ISUP ou signalisation multifréquence pour jonctions MF, chacune de celles-ci étant représentée par une extrémité.

Les fonctions remplies par le contrôleur MGC sont énumérées ci-après:

- **commande d'appel** – maintient et commande l'état d'appel général de la passerelle RTPC pour la partie d'un appel qui traverse cette passerelle RTPC. Cette fonction interfonctionne avec des éléments externes du RTPC selon les nécessités de la commande d'appel par passerelle RTPC, par exemple en produisant des interrogations du sous-système TCAP;
- **signalisation IPCablecom** – termine et produit la signalisation d'appel à destination ou en provenance du côté IPCablecom du réseau;
- **commande de passerelle média** – cette fonction exerce un contrôle général des extrémités situées dans la passerelle média:
  - la détection d'événement donne à la passerelle média l'ordre de détecter des événements, par exemple des tonalités intrabande et des états de prise de ligne, concernant l'extrémité et éventuellement des connexions;
  - la production de signaux donne à la passerelle média l'ordre de produire des tonalités et des signaux intrabande concernant l'extrémité et éventuellement des connexions;
  - la commande de connexion donne à la passerelle média des consignes relatives au traitement de base des connexions à destination ou en provenance d'extrémités dans la passerelle média;
  - la commande d'attribut donne à la passerelle média des consignes relatives aux attributs à appliquer à une extrémité et/ou à une connexion, par exemple une méthode de codage, l'utilisation de l'annulation d'écho, des paramètres de sécurité, etc;
- **surveillance de ressources externes** – maintient la visibilité externe, par le contrôleur MGC, de ressources MG et de ressources de réseau en mode paquet, par exemple la disponibilité des extrémités;
- **routage d'appel** – prend des décisions de routage d'appel;
- **sécurité** – fait en sorte que toute entité communiquant avec le contrôleur MGC observe les exigences de sécurité;

- **enregistrement de taux d'utilisation au moyen de messages événementiels** – enregistre le taux d'utilisation de ressources appel par appel.

6.6.2 Passerelle média (MG)

La passerelle média assure la connexité des supports entre le RTPC et le réseau IPCablecom en protocole IP. Chaque support est représenté par une extrémité et le contrôleur MGC donne consigne à la passerelle média d'établir et de contrôler des connexions médias vers d'autres extrémités du réseau IPCablecom. Le contrôleur MGC donne également consigne à la passerelle média de détecter et de produire des événements et des signaux relatifs à l'état d'appel dont le contrôleur MGC est informé.

6.6.2.1 Fonctions de passerelle média

Les fonctions remplies par la passerelle média sont les suivantes:

- termine et contrôle des circuits physiques sous la forme de canaux supports issus du RTPC;
- établit la distinction entre informations de signalisation média et informations de signalisation voie par voie intrabande, issues du circuit RTPC;
- détecte les événements relatifs aux extrémités et aux connexions selon les demandes du contrôleur MGC, ce qui inclut les événements nécessaires pour prendre en charge la signalisation intrabande, multifréquence par exemple;
- produit des signaux relatifs aux extrémités et aux connexions, par exemple des essais de continuité, des sonneries, etc., selon instructions du contrôleur MGC, ces signaux comprenant ceux qui sont nécessaires pour prendre en charge la signalisation intrabande;
- crée, modifie et supprime les connexions à destination ou en provenance d'autres extrémités, selon instructions du contrôleur MGC;
- commande et assigne des ressources internes de traitement média à des connexions spécifiques dès réception d'une demande générale issue du contrôleur MGC;
- effectue un transcodage de médias entre le RTPC et le réseau IPCablecom, ce qui inclut tous les aspects du transcodage comme les codecs, l'annulation d'écho, etc;
- fait en sorte que toute entité communiquant avec la passerelle média observe les exigences de sécurité;
- détermine le taux d'utilisation des ressources correspondantes et des attributs associés à ces ressources, par exemple le nombre d'octets de flux médias envoyés et reçus;
- signale au contrôleur MGC le taux d'utilisation des ressources.

6.6.3 Passerelle sémaphore (SG)

La fonction de passerelle sémaphore envoie et reçoit la signalisation de réseau à commutation de circuits à la frontière du réseau IPCablecom. Pour celui-ci, la fonction de passerelle sémaphore ne prend en charge que la signalisation autre que service par service sous la forme de signaux C7. La signalisation service par service est prise en charge directement par la fonction MG sous la forme de signaux multifréquences.

6.6.3.1 Fonctions de passerelle sémaphore

Les fonctions remplies par une passerelle sémaphore sont énumérées ci-dessous:

- termine physiquement les canaux sémaphores C7 issus du RTPC (canaux A et F);
- implémente des éléments de sécurité afin de garantir que la sécurité de la passerelle est conforme aux exigences de sécurité du réseau IPCablecom et du réseau C7;
- termine les niveaux 1, 2 et 3 du sous-système transport de message (MTP);

- implémente les fonctions de gestion de réseau du sous-système MTP selon les besoins de tout point sémaphore du réseau C7;
- effectue un mappage d'adresses ISUP pour prendre en charge la conversion flexible des codes de point sémaphore (codes de point de destination comme d'origine) et/ou des combinaisons de code de point sémaphore/d'indicatif CIC contenus dans des messages ISUP du réseau C7, afin de les transmettre au contrôleur MGC approprié (sous forme de nom de domaine ou d'adresse IP). Le contrôleur MGC adressé sera chargé de contrôler la passerelle média qui termine les jonctions interurbaines correspondantes;
- effectue un mappage d'adresses du sous-système TCAP avec des combinaisons de code de point sémaphore/numéro de sous-système SCCP contenues dans des messages TCAP du réseau C7 afin de les transmettre au contrôleur MGC ou au serveur CMS approprié;
- offre un mécanisme à certaines entités sécurisées ("utilisateurs TCAP") contenues dans le réseau IPCablecom, telles que des agents d'appel, afin d'interroger des bases de données externes du RTPC au moyen de messages TCAP envoyés dans le réseau C7;
- implémente le protocole de transport requis pour transporter les informations de signalisation entre la passerelle sémaphore et le contrôleur MGC.

6.7 Composants administratifs du système OSS

La partie administrative du système OSS contient des composants de gestion d'entreprise, de service et de réseau prenant en charge les processus commerciaux essentiels. Comme défini par le cadre RGT de l'UIT, les principaux domaines fonctionnels du système OSS sont la gestion des dérangements, la gestion de la performance, la gestion de la sécurité, la gestion de la comptabilité et la gestion de configuration. Ces sujets seront étudiés en détail dans une future Recommandation relative au cadre OSS de l'architecture IPCablecom.

L'architecture IPCablecom défini un ensemble limité de composants fonctionnels et d'interfaces OSS pour prendre en charge la mise en service d'adaptateurs MTA et de messages événementiels transportant des informations de facturation.

6.7.1 Serveur-distributeur de tickets (TGS, *ticket granting server*)

Dans l'architecture IPCablecom, le terme "TGS" (serveur-distributeur de tickets) est utilisé pour désigner un serveur de type Cerbère (*Kerberos*). On utilise le protocole Cerbère avec l'extension PKINIT de clé publique pour la gestion des clés à l'interface MTA-CMS.

Le serveur TGS accorde des tickets Cerbère à l'adaptateur MTA. Chaque ticket contient les informations utilisées pour établir l'authentification, la confidentialité, l'intégrité et le contrôle d'accès de la signalisation d'appel entre l'adaptateur MTA et le serveur CMS. Ce ticket est émis dans trois scénarios différents:

- au cours de la mise en service du dispositif, l'adaptateur MTA demande un ticket au serveur TGS. Il est fortement recommandé que l'adaptateur MTA sauvegarde ses tickets dans une mémoire permanente. Si l'adaptateur MTA réinitialise et que le ticket sauvegardé soit encore valide, l'adaptateur MTA n'aura pas besoin d'exécuter le protocole PKINIT pour demander un nouveau ticket au serveur TGS;
- en fonctionnement normal, l'adaptateur MTA demandera au serveur TGS un nouveau ticket après chaque expiration de ticket au cours du délai de grâce. Noter qu'en cas de panne d'alimentation dans le serveur CMS, l'adaptateur MTA ne sera plus associé à ce serveur CMS. Celui-ci, lors de son redémarrage, demandera à l'adaptateur MTA des informations de "réveil". Si le ticket détenu à ce moment par l'adaptateur MTA a dépassé le délai d'expiration et est ainsi devenu ce qu'on appelle un "ticket périmé", l'adaptateur MTA demandera un nouveau ticket au serveur TGS. Si l'adaptateur MTA détient encore un ticket valide, il doit l'envoyer au serveur CMS sans en demander de nouveau au serveur TGS;

- si le serveur TGS n'est pas disponible dans le réseau et que l'adaptateur MTA ne puisse pas obtenir de nouveau ticket au cours de la période de grâce, cet adaptateur MTA doit conserver son ticket actuel mais périmé jusqu'à ce qu'un serveur TGS soit disponible pour concéder un nouveau ticket. La demande émise par l'adaptateur MTA au cours de cet état sera spécifiée dans une future Recommandation de sécurité IPCablecom.

6.7.2 Protocole de configuration de serveur dynamique (DHCP, *dynamic host configuration protocol*)

Elément de réseau administratif qui est utilisé au cours du processus de mise en service de l'adaptateur MTA afin d'attribuer dynamiquement des adresses IP et d'autres informations de configuration du client.

6.7.3 Serveur de système noms de domaine (DNS, *domain name system*)

Elément de réseau administratif qui est utilisé afin de mettre des noms de domaine ASCII en mappage avec des adresses IP.

6.7.4 Serveur de protocole trivial de transfert de fichiers (TFTP, *trivial file transfer protocol server*) ou serveur de protocole de transfert hypertexte (HTTP, *hypertext transfer protocol server*)

Elément de réseau administratif qui est utilisé au cours du processus de mise en service de l'adaptateur MTA afin de téléimporter dans celui-ci des fichiers de configuration. Un serveur de protocole HTTP peut être utilisé en remplacement d'un serveur de protocole TFTP pour téléimporter des fichiers de configuration dans l'adaptateur MTA.

6.7.5 Serveur SYSLOG (SYSLOG)

Elément de réseau administratif utilisé pour collecter des événements tels que des filtres de piégeage et des erreurs issus d'un adaptateur MTA.

6.7.6 Serveur d'archivage (RKS, *record keeping server*)

Elément de réseau sécurisé qui reçoit les messages événementiels IPCablecom en provenance d'autres éléments de réseau IPCablecom sécurisés, comme le serveur CMS, le nœud AN et le contrôleur MGC. Le serveur RKS est également au moins un dépôt à court terme pour les messages événementiels IPCablecom, qu'il peut regrouper en ensembles cohérents ou en journaux détaillés des communications (CDR, *call detail record*) qui sont ensuite mis à la disposition d'autres systèmes administratifs comme la facturation, la détection des fraudes, etc.

6.8 Serveur d'annonces (ANS, *announcement server*)

Elément de réseau qui gère et reproduit des tonalités et des messages informationnels en réponse à des événements se produisant dans le réseau. Un serveur d'annonces (ANS) est une entité logique composée d'un contrôleur d'annonces (ANC) et d'un reproducteur d'annonces (ANP).

6.8.1 Contrôleur d'annonces (ANC, *announcement controller*)

Le contrôleur ANC lance et gère tous les services d'annonces offerts par le reproducteur d'annonces (ANP) auquel il demande de reproduire des annonces sur la base d'états d'appel déterminés par le serveur CMS. Lorsque des informations sont collectées par l'ANP auprès de l'utilisateur final, l'ANC est chargé d'interpréter ces informations et de gérer la session en conséquence. Le contrôleur ANC peut donc gérer également les états d'appel.

6.8.2 Reproducteur d'annonces (ANP, *announcement player*)

Serveur de ressource média qui est chargé de recevoir et d'interpréter les commandes issues du contrôleur ANC ainsi que d'acheminer les annonces appropriées jusqu'à l'adaptateur MTA. Le

reproducteur ANP est également chargé d'accepter et de signaler les saisies de l'utilisateur (comme les tonalités DTMF). Les fonctions ANP sont sous le contrôle du contrôleur ANC.

7 Interfaces entre protocoles

Des spécifications de protocole ont été définies pour la plupart des interfaces élémentaires dans l'architecture IPCablecom. On trouvera ci-après un aperçu général des diverses interfaces entre protocoles. Il y a lieu de consulter chaque spécification IPCablecom individuelle concernant les exigences de protocole complètes.

Il se peut que certaines de ces interfaces n'existent pas dans une implémentation particulière d'un produit du marché. Par exemple, si plusieurs composants fonctionnels IPCablecom sont combinés, il est possible que certaines de ces interfaces soient intégrées à ces composants.

7.1 Interfaces de signalisation d'appel

La signalisation d'appel nécessite plusieurs interfaces à l'intérieur de l'architecture IPCablecom. Ces interfaces sont indiquées sur le diagramme de la Figure 5, chacune étant étiquetée et décrite plus en détail dans le Tableau 1 suivant.

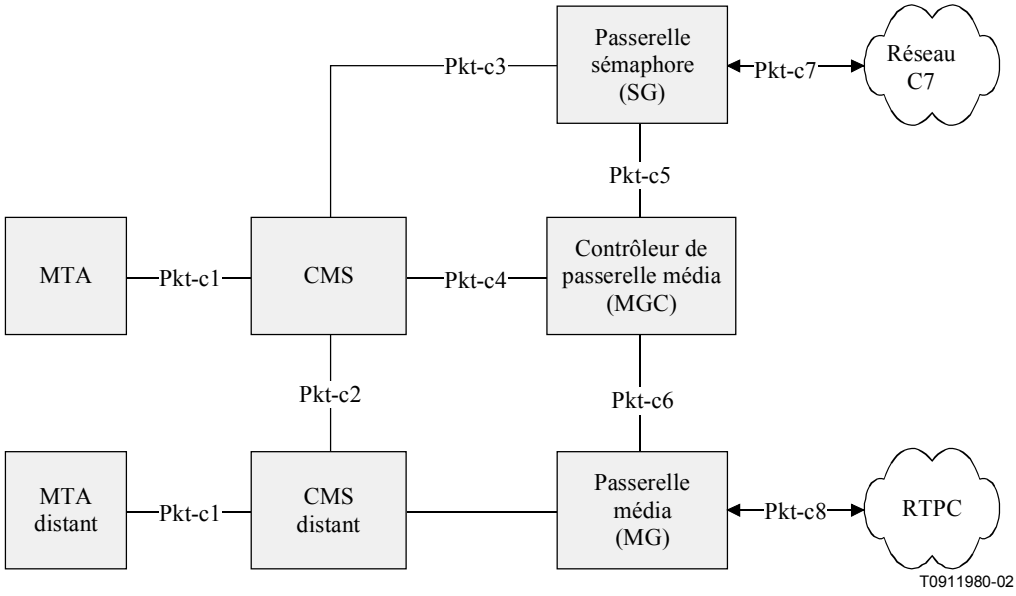


Figure 5/J.160 – Interfaces de signalisation d'appel

Tableau 1/J.160 – Interfaces de signalisation d'appel

Interface	Composants fonctionnels IPCablecom	Description
Pkt-c1	MTA ⟷ CMS	Messages de signalisation d'appel échangés entre l'adaptateur MTA et le serveur CMS au moyen du protocole NCS, qui est un profil du protocole MGCP.
Pkt-c2	CMS ⟷ CMS	Messages de signalisation d'appel échangés entre serveurs CMS. Le protocole pour cette interface n'est pas défini.
Pkt-c3	CMS ⟷ SG	Messages de signalisation d'appel échangés entre CMS et SG au moyen du protocole ISTP/TCAP.
Pkt-c4	CMS ⟷ MGC	Messages de signalisation d'appel échangés entre le serveur CMS et le contrôleur MGC. Le protocole pour cette interface n'est pas défini.
Pkt-c5	SG ⟷ MGC	Messages de signalisation d'appel échangés entre MGC et SG au moyen des protocoles ISTP/ISUP et ISTP/TCAP.
Pkt-c6	MGC ⟷ MG	Interface de commande média de la passerelle média et, éventuellement, signalisation intrabande au moyen du protocole TGCP, qui est un profil du MGCP, semblable au protocole de signalisation NCS.
Pkt-c7	SG ⟷ C7	La passerelle SG prend en charge les canaux sémaphores C7 physiques issus du RTPC (canaux A, F). Les protocoles suivants sont pris en charge: • interface utilisateur ISUP: offre une interface de signalisation C7 ISUP aux porteuses RTPC extérieures; • interface utilisateur TCAP: offre un mécanisme pour certaines entités sécurisées ("utilisateurs TCAP") à l'intérieur du réseau IPCablecom, comme les agents d'appel, afin d'interroger des bases de données RTPC externes au moyen de messages TCAP envoyés dans le réseau C7.
Pkt-c8	MG ⟷ RTPC	Cette interface définit la connexité des canaux supports allant de la passerelle média au RTPC. Elle prend également en charge la connexité des canaux supports allant de la passerelle média au RTPC, ainsi que les protocoles de signalisation d'appel suivants: • signalisation multifréquence intrabande. Une future version de l'architecture IPCablecom pourra prendre en charge les interfaces PRI du RNIS. NOTE – Cette fonction peut être considérée comme faisant partie de la fonction de passerelle sémaphore.

7.1.1 Cadre de signalisation d'appel par le réseau (NCS, *network-based call signalling*)

Le protocole (Pkt-c1) IPCablecom de signalisation d'appel par le réseau (NCS) est une variante élargie du protocole de signalisation d'appel MGCP du groupe IETF. L'architecture NCS implante la réalisation des états d'appel et des éléments de service dans un composant centralisé, le serveur de gestion d'appels (CMS) tandis que la logique de commande des dispositifs est implantée dans l'adaptateur MTA. Celui-ci transmet au serveur CMS les événements relatifs aux dispositifs et répond aux commandes émises par le serveur CMS. Celui-ci, qui peut se composer de plusieurs systèmes répartis géographiquement ou administrativement, est chargé d'établir et de libérer les

communications en fournissant des services évolués (éléments de service d'appel améliorés), en assurant l'autorisation d'appel et en produisant les comptes rendus d'événements de facturation, etc.

Un exemple de répartition des fonctions est le cas dans lequel le serveur CMS donne à l'adaptateur MTA l'ordre de l'informer lorsque le téléphone a été décroché et que le nombre approprié de chiffres a été composé en DTMF. Lorsque cette séquence d'événements se produit, l'adaptateur MTA le signale au serveur CMS qui peut alors donner à l'adaptateur MTA l'ordre de créer une connexion, de réserver des ressources de QoS par l'intermédiaire du réseau d'accès pour la connexion vocale en instance, ainsi que de reproduire une sonnerie produite localement. Le serveur CMS communique à son tour avec un homologue CMS (ou MGC) distant afin d'établir l'appel. Lorsque le serveur CMS détecte une réponse en provenance de l'extrémité distante, il donne à l'adaptateur MTA l'ordre d'arrêter la sonnerie, d'activer la connexion média entre l'adaptateur MTA local et l'adaptateur MTA distant, puis de commencer l'envoi et la réception de paquets de flux média.

La centralisation dans le serveur CMS du traitement des états d'appel et des éléments de service permet au fournisseur de services de gérer de façon centralisée la fiabilité du service fourni. Par ailleurs, le fournisseur de services obtient un accès total à tous les logiciels et à tous les matériels en cas de dérangement affectant les services d'abonné. Les logiciels peuvent être contrôlés de façon centralisée et mis à jour par cycles rapides de mise au point et de résolution n'exigeant pas le déploiement d'agents de terrain jusque dans les locaux d'abonné. Par ailleurs, le fournisseur de services peut contrôler directement les services introduits ainsi que les flux de recettes qui y sont associés.

7.1.2 Cadre de signalisation RTPC

Les interfaces de signalisation RTPC sont résumées dans le Tableau 1 (Pkt-c3 à Pkt-c8). Ces interfaces donnent accès aux services en mode RTPC et aux abonnés RTPC issus du réseau IPCablecom.

Le cadre de signalisation RTPC de l'architecture IPCablecom se compose d'une passerelle RTPC subdivisée en trois composants fonctionnels comme suit:

- contrôleur de passerelle média (MGC);
- passerelle média (MG);
- passerelle sémaphore (SG).

Le contrôleur MGC et la passerelle média sont, respectivement, analogues au serveur CMS et à l'adaptateur MTA dans le cadre de signalisation NCS. La passerelle média assure la connexité des supports et de la signalisation intrabande avec le RTPC. Le contrôleur de passerelle média implémente tous les états d'appel et leur logique. Il contrôle également le fonctionnement de la passerelle média par l'intermédiaire du protocole TGCP (Pkt-c6), ce qui inclut la création, la modification et la suppression de connexions ainsi que d'informations de signalisation intrabande à destination ou en provenance de la passerelle média. Le protocole TGCP est une variante étendue du protocole de signalisation d'appel MGCP du groupe IETF. Cette variante TGCP est étroitement alignée sur le protocole NCS.

Le serveur CMS et le contrôleur MGC peuvent chacun envoyer à un point de commande de services (SCP, *service control point*) du réseau C7, par l'intermédiaire de la passerelle sémaphore [Pkt-c3 et Pkt-c5), des interrogations de routage (par exemple, recherche d'un numéro de libre appel ou recherche de la portabilité (LNP) d'un numéro]. Le contrôleur MGC échange également, par l'intermédiaire de la passerelle sémaphore, des messages de signalisation ISUP avec les entités C7 du RTPC pour la gestion et la commande des jonctions. Le protocole ISTP assure le service d'interconnexion de signalisation entre les éléments de commande d'appel du réseau IPCablecom (serveur CMS et contrôleur MGC) et le réseau de signalisation C7 du RTPC par l'intermédiaire de la passerelle sémaphore C7. Le protocole ISTP contient des capacités d'initialisation, de mappage

d'adresses du domaine C7 au domaine IP, d'acheminement de messages pour les ISUP et TCAP du réseau C7, de gestion des encombrements, de gestion des dérangements, d'opérations de maintenance et de prise en charge des configurations redondantes. Le protocole ISTP comble l'intervalle entre les mécanismes fondamentaux de transport en mode IP et la signalisation dans la couche Application. Bien qu'il n'effectue pas une conversion des protocoles MTP3 et SCCP du système C7, le protocole ISTP implémente des fonctions analogues à certaines de celles des protocoles MTP3 et SCCP d'une manière appropriée à la communication dans un réseau IP entre systèmes répartis. Ces capacités permettent au réseau IP d'interagir avec tous les services du RTPC et de les recevoir. Au fur et à mesure de l'évolution dans le temps des capacités de service, les capacités de signalisation susmentionnées pourront servir à prendre en charge l'accès RTPC aux propres bases de données de routage et de service du réseau IPCablecom.

7.2 Flux médias

La norme RTP du groupe IETF (RFC 1889 – RTP: protocole de transport pour applications en temps réel) est utilisée pour transporter tous les flux médias dans le réseau IPCablecom. Celui-ci utilise le profil RTP pour les flux audio et vidéo définis dans le commentaire RFC 1890 de l'IETF (RTP: profil pour conférences audio et vidéo avec contrôle minimal).

La Figure 6 décrit les principaux trajets de flux médias dans l'architecture de réseau IPCablecom. Ces trajets sont décrits plus en détail ci-après.

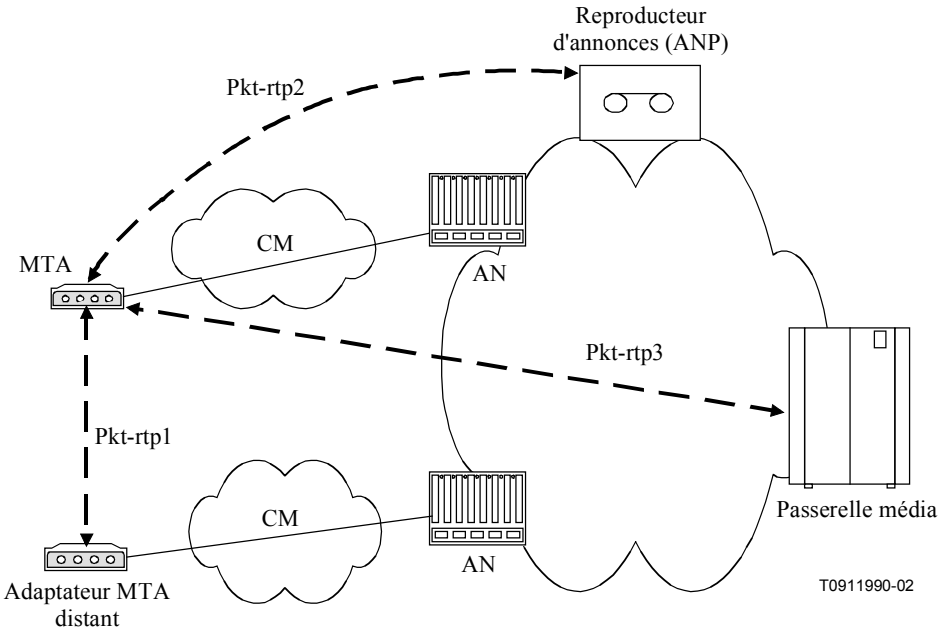


Figure 6/J.160 – Flux médias dans un réseau IPCablecom

Pkt-rtp1: flux média entre adaptateurs MTA, comprenant par exemple des signaux codés de voix, vidéo et télécopie.

Pkt-rtp2: flux média entre le reproducteur ANP et l'adaptateur MTA, comprenant par exemple des tonalités et des annonces envoyées à l'adaptateur MTA par le reproducteur d'annonces.

Pkt-rtp3: flux média entre MG et MTA, comprenant par exemple des tonalités, des annonces et des flux média RTPC envoyés par la passerelle média à l'adaptateur MTA.

Le protocole RTP code une seule voie d'informations multimédias dans un seul sens. La norme prescrit un en-tête de 8 octets dans chaque paquet. Un "type de charge utile" RTP codé sur 1 octet est

défini pour indiquer l'algorithme de codage qui est utilisé. La plupart des algorithmes audio et vidéo normalisés sont attribués à des valeurs de type de charge utile comprises entre 0 et 95. L'étendue de 96 à 127 est réservée aux types de charge utile RTP "dynamique". L'étendue de 128 à 255 est réservée à l'administration privée.

La Figure 7 décrit le format des paquets de données RTP transmis en mode IP sur réseau Ethernet.

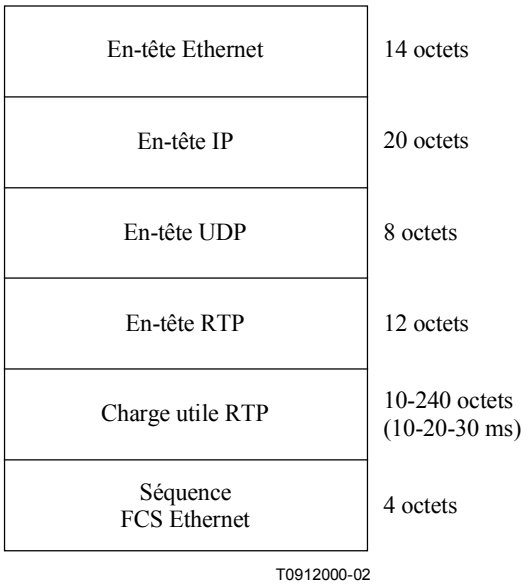


Figure 7/J.160 – Format de paquet RTP

La longueur de la charge utile du protocole RTP, ainsi que la fréquence d'émission des paquets dépendent de l'algorithme défini dans le champ type de charge utile.

Les sessions RTP sont établies dynamiquement par les extrémités impliquées de sorte qu'il n'y a aucun numéro d'accès UDP déjà identifié. Le protocole de description de session (SDP, *session description protocol*) a été élaboré par le groupe IETF afin de communiquer l'adresse IP particulière et l'accès UDP particulier qui sont en cours d'utilisation par une session.

Le surdébit d'en-tête de paquet est, dans les protocoles Ethernet, IP, UDP et RTP, important par rapport à une longueur normale de charge utile RTP, qui peut se réduire à 10 octets pour des signaux vocaux paquetés. La Rec. UIT-T J.112 traite ce problème au moyen d'une fonction de suppression d'en-tête de charge utile afin d'abréger les en-têtes communs.

7.3 Mise en service d'un adaptateur MTA

L'objet de la mise en service d'un adaptateur MTA consiste à permettre qu'un adaptateur MTA enregistre et fournisse des services d'abonné dans le réseau HFC. La mise en service d'un adaptateur MTA couvre les fonctions requises d'initialisation, d'authentification et d'enregistrement. La spécification de mise en service comporte également les définitions d'attribut requises dans le fichier de configuration de l'adaptateur MTA. (Voir Figure 8.)

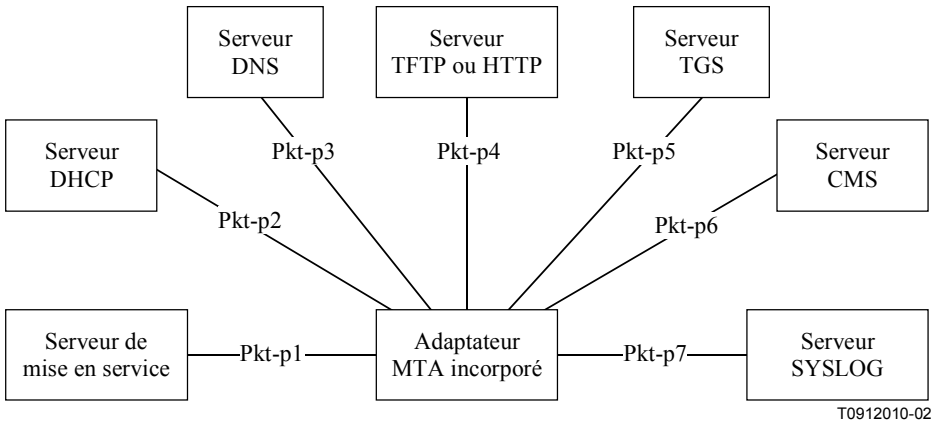


Figure 8/J.160 – Interfaces de mise en service IPCablecom

Le Tableau 2 décrit les interfaces de mise en service indiquées dans la Figure 8.

Tableau 2/J.160 – Interfaces de mise en service de dispositifs

Interface	Composants fonctionnels IPCablecom	Description
Pkt-p1	Serveur MTA ⟷ PROV	Interface d'échange, entre l'adaptateur MTA et le serveur de mise en service au moyen du protocole SNMP, d'informations relatives aux capacités des dispositifs ainsi qu'aux adaptateurs MTA et aux extrémités. L'adaptateur MTA envoie également, au moyen du protocole SNMP, une notification indiquant que la mise en service a été effectuée, assortie d'un état de succès/échec.
Pkt-p2	Serveur MTA ⟷ DHCP	Interface DHCP entre l'adaptateur MTA et le serveur DHCP, utilisée pour attribuer une adresse IP à l'adaptateur MTA. Si un serveur DNS est requis au cours de la mise en service, l'adresse de ce serveur est également incluse.
Pkt-p3	Serveur MTA ⟷ DNS	Interface DNS entre l'adaptateur MTA et le serveur DNS, utilisée pour obtenir l'adresse IP d'un serveur IPCablecom compte tenu de son nom de domaine complet.
Pkt-p4	Serveur MTA ⟷ HTTP ou TFTP	L'adaptateur MTA téléimporte son fichier de configuration à partir du serveur TFTP ou HTTP.
Pkt-p5	MTA ⟷ TGS	L'adaptateur MTA obtient un ticket de type Cerbère auprès du serveur-distributeur de tickets (TGS).
Pkt-p6	MTA ⟷ CMS	L'adaptateur MTA établir un association de sécurité IPSec avec le serveur CMS au moyen du protocole Cerbère.
Pkt-p7	MTA ⟷ SYSLOG	L'adaptateur MTA envoie au serveur SYSLOG, au moyen du protocole UDP, une notification indiquant que la mise en service a été effectuée, assortie d'un état de succès/échec.

7.4 Interfaces avec la couche de gestion d'éléments SNMP

Pour la mise en service des adaptateurs MTA, l'architecture IPCablecom nécessite que la version SNMP3 assure l'interface entre ces adaptateurs MTA et les systèmes de gestion d'élément.

Les messages "traps" et "informs" de la version SNMP3 sont pris en charge pour le traitement des événements, ainsi que les messages "sets" et "gets" pour la mise en service. Les bases MIB de l'architecture IPCablecom seront définies dans de futures Recommandations relatives aux bases MIB d'adaptateurs MTA.

La base MIB de la signalisation NCS contient, dans l'architecture IPCablecom, des informations de signalisation d'appel par le réseau en vue de la mise en service aussi bien dispositif par dispositif qu'extrémité par extrémité. La base MIB des adaptateurs MTA contient des données pour la mise en service de dispositifs et pour la prise en charge de fonctions mises en service comme la journalisation des événements. L'on pourra trouver dans la spécification correspondante des informations plus détaillées sur le cadre de bases MIB dans l'architecture IPCablecom.

7.5 Interfaces avec les messages événementiels

7.5.1 Cadre des messages événementiels

Un message événementiel est une fiche contenant des informations sur le taux d'utilisation et les activités du réseau. Chaque message événementiel peut contenir un ensemble complet de données concernant le taux d'utilisation ou peut ne contenir qu'une partie des informations totales d'utilisation. Mises en corrélation par le système serveur d'archivage (RKS), les informations contenues dans plusieurs messages événementiels offrent un enregistrement complet du service qui est souvent appelé relevé détaillé des communications (CDR, *call detail record*). Des messages événementiels ou des journaux CDR peuvent être envoyés à une ou plusieurs applications administratives comme un système de facturation, un système de détection de fraude ou un processeur de services prépayés.

La présente spécification de messages événementiels IPCablecom définit la structure de la fiche de message événementiel et définit son protocole de transport (RADIUS). La fiche de message événementiel est conçue de façon à être flexible et extensible afin de transporter des informations sur le taux d'utilisation du réseau pour une large gamme de services. Des protocoles de transport additionnels pourront être recommandés dans de futures versions de la présente Recommandation. Bien que le domaine d'application de la présente Recommandation soit limité à la définition de messages événementiels pour les capacités de base de téléphonie résidentielle, l'on s'attend qu'elle sera étendue à la prise en charge de services additionnels dans l'architecture IPCablecom. La Figure 9 montre une architecture représentative des messages événementiels.

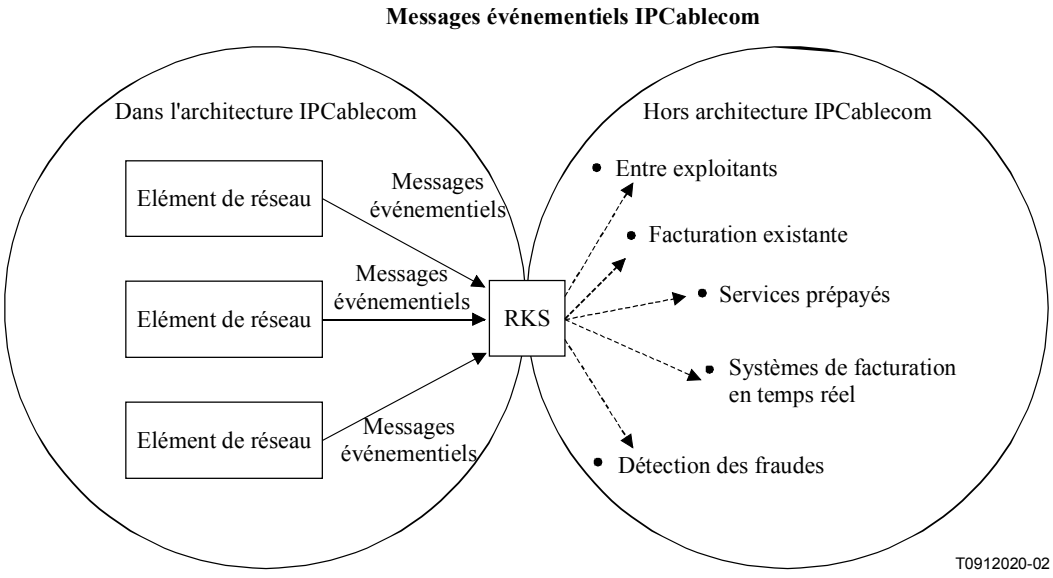
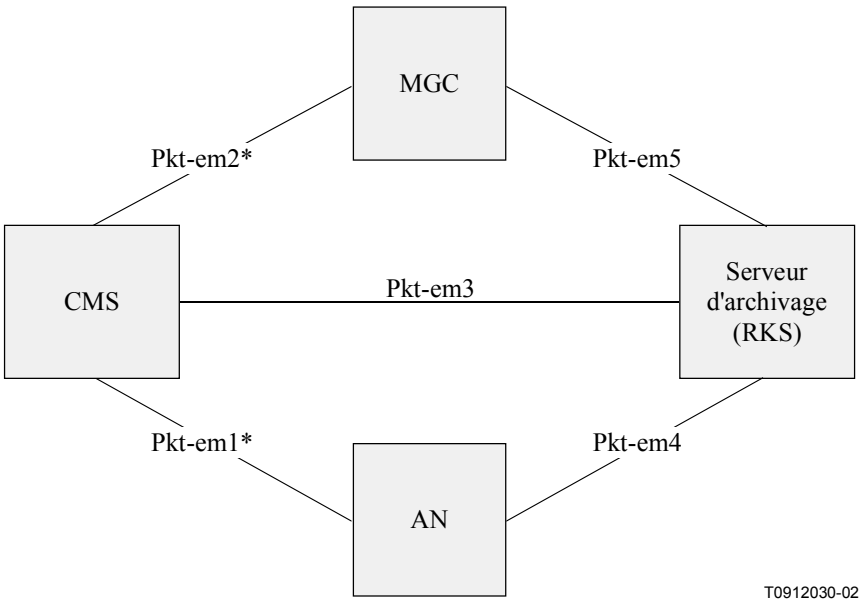


Figure 9/J.160 – Architecture représentative des messages événementiels

Le Tableau 3 décrit les interfaces avec les messages événementiels décrites dans la Figure 10.

Tableau 3/J.160 – Interfaces avec les messages événementiels

Interface	Composant fonctionnel IPCablecom	Description
Pkt-em1	CMS ⟷ AN	Message de choix de porte DQoS acheminant l'identificateur de corrélation avec la facturation et d'autres données requises par un nœud d'accès afin d'envoyer des messages événementiels à un serveur RKS.
Pkt-em2	CMS ⟷ MGC	Interface de vendeur exclusif acheminant un identificateur de corrélation avec la facturation ainsi que d'autres données requises pour la facturation. Soit le serveur CMS soit le contrôleur MGC peut émettre un appel et avoir donc besoin de créer l'identificateur de corrélation avec la facturation puis d'envoyer ces données à l'autre partie.
Pkt-em3	CMS ⟷ RKS	Protocole RADIUS acheminant des messages événementiels IPCablecom.
Pkt-em4	AN ⟷ RKS	Protocole RADIUS acheminant des messages événementiels IPCablecom.
Pkt-em5	MGC ⟷ RKS	Protocole RADIUS acheminant des messages événementiels IPCablecom.



NOTE – L'astérisque indique que l'identificateur de corrélation avec la facturation et les autres données de facturation sont acheminés par une interface de signalisation existante.

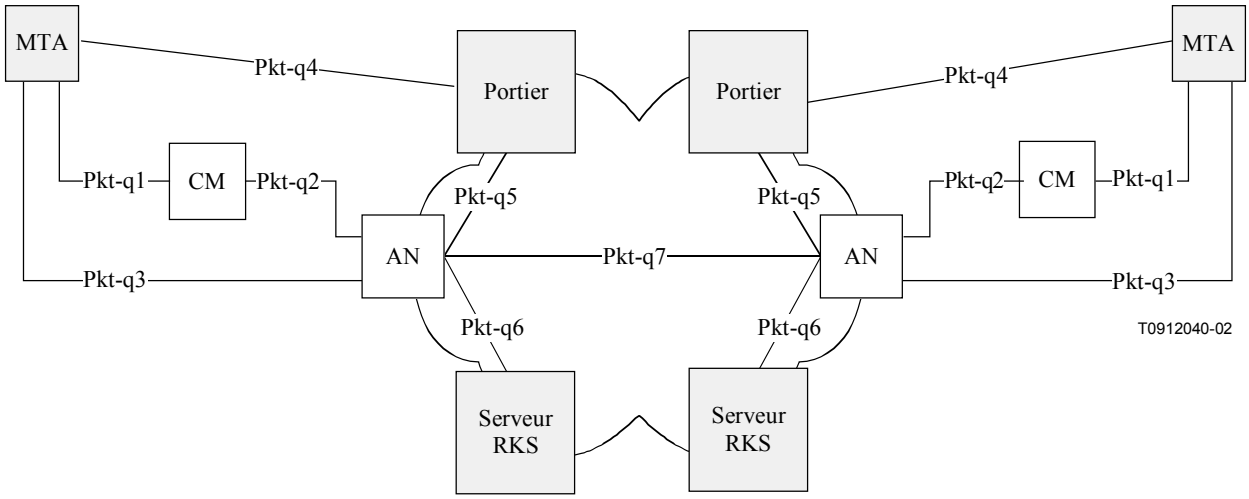
Figure 10/J.160 – Interfaces avec les messages événementiels

7.6 Qualité de service (QS)

7.6.1 Cadre de QS

Des interfaces de signalisation de la qualité de service sont définies entre un grand nombre de composants du réseau IPCablecom. La signalisation peut être manipulée au niveau de la couche Application (par exemple, les paramètres SDP), de la couche Réseau (par exemple, RSVP) ou de la couche Liaison de données (par exemple, QS selon Rec. UIT-T J.112).

Du point de vue de l'adaptateur MTA et de son réseau d'accès, le cadre QS IPCablecom est représenté par la Figure 11:



NOTE – La fonction de portier est contenue dans un nœud serveur CMS.

Figure 11/J.160 – Interfaces de signalisation QS dans l'architecture IPCablecom

Le Tableau 4 décrit brièvement chaque interface et la façon dont elle est utilisée dans la spécification de QS dynamique (DQoS, *dynamic QoS*). Deux variantes sont indiquées pour cette spécification: d'abord une interface générale qui est applicable aux adaptateurs MTA incorporés ou autonomes; ensuite une interface facultative qui n'est applicable qu'aux adaptateurs MTA incorporés.

Tableau 4/J.160 – Interfaces de QS pour adaptateurs MTA autonomes et incorporés

Interface	Composant fonctionnel IPCablecom	Adaptateur MTA incorporé/autonome DQoS	Adaptateur MTA incorporé DQoS
Pkt-q1	MTA ⟷ CM	N/A	Interface de service de commande MAC pour E-MTA
Pkt-q2	CM ⟷ AN	J.112, à l'initiative du nœud d'accès	J.112, à l'initiative du CM
Pkt-q3	MTA ⟷ AN	RSVP+[a)]	N/A
Pkt-q4	MTA ⟷ GC/CMS	NCS/DCS	NCS
Pkt-q5	GC ⟷ AN	Gestion de porte	Gestion de porte
Pkt-q6	AN ⟷ RKS	Facturation	Facturation
Pkt-q7	AN ⟷ AN	Gestion de porte	Gestion de porte

a) Pour l'architecture IPCablecom, seules les interfaces d'adaptateur MTA incorporé sont requises, telles que définies au § 7 de la spécification DQoS. Le système CMTS n'est pas tenu de prendre en charge le protocole RSVP de part et d'autre de l'interface MTA-CMTS, comme défini dans le § 6 de la spécification DQoS.

La fonction de chaque interface de QS est décrite plus en détail dans le Tableau 5.

Tableau 5/J.160 – Interfaces de QoS

Interface	Composant fonctionnel IPCablecom	Description
Pkt-q1	MTA ⟷ CM	Cette interface n'est définie que pour les adaptateurs MTA incorporés. Elle se décompose en trois sous-interfaces comme suit: *commande:* sous-interface utilisée pour gérer des flux de service J.112 et leurs paramètres de trafic QS associés, avec leurs règles de classification; *synchronisation:* sous-interface utilisée pour synchroniser les paquets et pour la planification afin de minimiser le temps de propagation et la gigue; *transport:* sous-interface utilisée pour traiter des paquets dans le flux média et pour appliquer aux paquets le traitement de QS approprié. L'interface MTA/CM est définie théoriquement dans la Rec. UIT-T J.112.

Interface	Composant fonctionnel IPCablecom	Description
Pkt-q2	CM ⟷ AN	Il s'agit de l'interface de QS selon la Rec. UIT-T J.112 (commande, planification et transport). Il convient de noter que, sur le plan de l'architecture, les fonctions de commande peuvent être lancées soit par le câblo-modem soit par le nœud d'accès. Celui-ci est cependant l'arbitre ultime de la politique et le décideur d'admission dans le réseau d'accès J.112. Les capacités suivantes de la commande MAC J.112 sont utilisées dans l'architecture IPCablecom: • flux de service multiples, possédant chacun sa propre classe de trafic amont, sur des connexions vocales aussi bien simples que multiples selon le flux de service J.112; • classification priorisée des flux de trafic en fonction des flux de service; • service de planification de débit minimal/constant garanti; • planification de débit constant avec service de détection d'activité de trafic (planification de ralentissements, d'accélérations, d'arrêts et de redémarrage); • suppression d'en-tête de paquet J.112 pour augmenter la densité d'appels; • classification J.112 des flux vocaux en fonction du flux de service; • synchronisation J.112 de l'horloge entre CODEC et AN ainsi que de l'intervalle de distribution; • activation en deux phases des ressources QS; • marquage des paquets TOS dans la couche Réseau; • garantie de temps de propagation et de gigue; • signalisation de sous-couche interne entre adaptateur MTA (incorporé) IPCablecom et le câblo-modem; Cette interface est définie plus en détail dans la Rec. UIT-T J.112.
Pkt-q3	MTA ⟷ AN	Cette interface est utilisée pour demander des ressources de largeur de bande et de QS associée. Cette interface travaille au sommet des protocoles de couche 4 qui contournent le câblo-modem. Les échanges de messages entre l'adaptateur MTA et le nœud d'accès ont pour résultat que des flux de service sont activés par signalisation issue du nœud d'accès à l'interface Pkt-q2. Une version améliorée du protocole RSVP est utilisée pour cette signalisation.
Pkt-q4	MTA ⟷ CMS/GC	Interface de signalisation entre l'adaptateur MTA et CMS/GC. De nombreux paramètres sont signalés de part et d'autre de cette interface, comme les flux médias, les adresses IP et la sélection de codec. Mais il est possible que certains protocoles extraient la sémantique QS de la signalisation ou que le protocole de signalisation de la couche Application soit étendu de façon à contenir des paramètres de signalisation QS explicites.

Interface	Composant fonctionnel IPCablecom	Description
Pkt-q5	CMS/GC ⟷AN	Cette interface sert à gérer les portes dynamiques pour les canaux supports de flux média. Cette interface permet au réseau IPCablecom de demander et d'autoriser des changements de QS sans exiger de fonctions de commande de QS par réseau d'accès J.112 dans l'adaptateur MTA. Aucun nouveau protocole de signalisation de QS côté client n'a besoin d'être conçu pour prendre en charge les adaptateurs MTA autonomes. Le serveur GC/CMS se charge de demander la politique et le nœud d'accès se charge du contrôle d'accès et du réglage rapide de la QS dans la liaison d'accès J.112.
Pkt-q6	AN ⟷ RKS	Cette interface est utilisée par le nœud d'accès pour signaler au serveur RKS toutes les modifications d'autorisation d'appel et de taux d'utilisation. Elle est définie dans la spécification des messages événementiels.
Pkt-q7	AN ⟷ AN	Cette interface sert à la coordination des ressources entre le nœud d'accès de l'adaptateur MTA local et le nœud d'accès de l'adaptateur MTA distant. Le nœud d'accès est chargé de l'attribution et de l'application des ressources QS locales.

7.6.2 Signalisation de QS par adaptateur MTA dans la couche deux ou dans la couche trois

La signalisation de QS par l'adaptateur MTA peut être effectuée soit dans la couche deux (J.112) soit dans la couche trois (RSVP). La signalisation dans la couche deux est accessible aux dispositifs CM et AN qui existent à la frontière RF du réseau d'accès J.112. La signalisation dans la couche trois est requise pour les dispositifs qui sont éloignés d'un ou de plusieurs bonds de la frontière RF du réseau d'accès J.112.

Si la signalisation de QS dans la couche deux est lancée par l'adaptateur MTA, celui-ci doit être de type incorporé et doit utiliser l'interface implicite de commande MAC des flux de service J.112 comme suggéré dans la Rec. UIT-T J.112.

Si la signalisation de QS dans la couche trois est lancée par l'adaptateur MTA, celui-ci peut être du type incorporé ou du type autonome. Le protocole RSVP en version améliorée est utilisé pour cette signalisation et est intercepté par le nœud d'accès, qui utilise la signalisation de couche deux pour communiquer au câblo-modem les modifications de signalisation de QS.

7.6.3 Qualité de service dynamique (DQoS)

Dans l'architecture IPCablecom, la qualité de service dynamique (DQoS) utilise les informations de signalisation d'appel au moment où celui-ci est établi pour autoriser dynamiquement les ressources correspondantes. La DQoS empêche diverses attaques de type vol de service en intégrant les messages de QS dans d'autres protocoles et éléments de réseau. La Figure 11 décrit les éléments de réseau qui sont nécessaires pour la commande de DQoS.

La fonction qui effectue, à l'intérieur du nœud d'accès, la classification du trafic et qui applique la politique de QS aux flux médias est appelée "porte". L'élément de portier gère les portes pour les flux médias IPCablecom. Les informations clés suivantes sont incluses dans la signalisation entre le portier (GC) et le nœud d'accès (AN):

enveloppe de QS maximale autorisée – l'enveloppe maximale de QS autorisée indique la ressource de QS maximale (par exemple, "2 attributions de 160 octets toutes les 10 ms") que l'adaptateur MTA est autorisé à admettre pour un flux support de média déterminé. Si l'adaptateur MTA demande une valeur supérieure aux paramètres contenus dans l'enveloppe, cette demande est rejetée;

identité des extrémités de flux média – le serveur GC/CMS autorise les parties qui sont impliquées dans un flux support de média. Au moyen de ces informations, le nœud d'accès peut régler le flux de données de façon que celui-ci soit à destination ou en provenance des parties autorisées;

informations de facturation – le serveur GC/CMS crée des informations de facturation opaques, que le nœud d'accès n'a pas à décoder. Ces informations peuvent se réduire à l'identité de facturation ou à la nature de l'appel. Le nœud d'accès retransmet ces informations de facturation au serveur RKS lorsque l'appel est activé ou terminé;

Le rôle de chaque composant IPCablecom dans l'implémentation de la DQoS est le suivant.

serveur de gestion d'appels/portier – le serveur CMS/GC est chargé de l'autorisation de QS, qui peut dépendre du type d'appel, du type d'utilisateur ou d'autres paramètres définis par la politique.

nœud d'accès – au moyen des informations fournies par le serveur GC/CMS, le nœud d'accès applique un contrôle d'admission aux demandes de QS tout en réglant le flux de données de façon que celui-ci soit à destination ou en provenance de parties autorisées en termes de flux média. Le nœud d'accès interagit avec le câblo-modem, le serveur RKS, l'adaptateur MTA et le nœud d'accès terminal. Les tâches du réseau d'accès concernant chacun de ces éléments sont les suivantes:

- **AN par rapport à CM** – le nœud d'accès est chargé d'établir et de libérer les flux de service conformément à la convention sur le niveau de service (SLA, *service level agreement*) conclue avec l'adaptateur MTA. S'il ne compte pas sur le câblo-modem pour régler le trafic, le nœud d'accès effectue ce réglage de façon que le câblo-modem travaille de la façon demandée;
- **AN par rapport à serveur RKS** – le nœud d'accès met à jour le serveur d'archivage (RKS) à chaque changement de la convention SLA entre le nœud d'accès et l'adaptateur MTA. Il utilise les informations de facturation qui sont données par le serveur GC/CMS afin d'identifier chaque liaison de QS autorisée. Le nœud d'accès insère des informations de rythme dans le message qu'il envoie et met en tampon les messages si la connexion avec le serveur RKS est interrompue;
- **AN par rapport à adaptateur MTA** – l'adaptateur MTA formule dynamiquement des demandes de modification des paramètres de trafic QS. Lorsque le nœud d'accès reçoit une telle demande, il effectue un contrôle d'autorisation afin de déterminer si les caractéristiques demandées sont contenues dans l'enveloppe de QS autorisée et si les extrémités des flux médias sont autorisées. Il met ensuite en service les attributs de QS pour la liaison d'interface RFI avec le nœud d'accès et active les paramètres de trafic QS appropriés par signalisation avec le câblo-modem. Lorsque tous les contrôles de mise en service et d'autorisation ont été effectués avec succès, le nœud d'accès envoie un message de succès au serveur GC/CMS afin d'indiquer que l'adaptateur MTA et le nœud d'accès sont engagés dans une convention SLA;
- **AN par rapport à AN terminal** – le nœud d'accès envoie des messages à son homologue terminal (ou à un autre dispositif terminal d'accès réseau) afin de veiller à ce que la largeur de bande convenue des deux côtés soit la même. Si ce n'est pas le cas, les deux côtés ferment la connexion;

câblo-modem (CM) – bien qu'il soit une entité non sécurisée, le câblo-modem est chargé du fonctionnement correct de la liaison de QS entre lui-même et le nœud d'accès. Ce dernier veille à ce que le câblo-modem ne puisse pas abuser de la liaison d'interface RFI mais il appartient au câblo-modem d'utiliser la liaison d'interface RFI de façon à fournir les services qui sont définis par la Rec. UIT-T J.112;

serveur d'archivage (RKS) – le serveur RKS joue le rôle de base de données et mémorise tous les événements envoyés par le réseau d'accès. Le serveur RKS mémorise les messages en y joignant les informations relatives à l'heure de réception et à l'élément de réseau. Le serveur RKS doit posséder

une capacité d'interface et/ou de traitement suffisante pour qu'un traitement additionnel puisse être effectué;

adaptateur MTA – l'adaptateur MTA est l'entité à laquelle la convention sur le niveau de service (SLA) est offerte par le réseau d'accès. L'adaptateur MTA est chargé de l'emploi approprié de la liaison de QS. Si cette liaison dépasse le trafic autorisé par la convention SLA, l'adaptateur MTA ne recevra pas les caractéristiques de QS qu'il a demandées. L'adaptateur MTA utilise une attribution de largeur de bande en deux temps: les ressources de QS sont admises pendant que l'appel est en cours d'établissement au point d'origine, puis ces ressources sont activées lorsque l'appel est connecté.

7.7 Services d'annonce

Les annonces sont normalement nécessaires pour les appels qui n'aboutissent pas. Elles peuvent aussi servir à fournir des services d'information améliorés à l'appelant. Les interfaces de signalisation prenant en charge les services d'annonce IPCablecom sont indiquées sur la Figure 12 et résumées dans le Tableau 6.

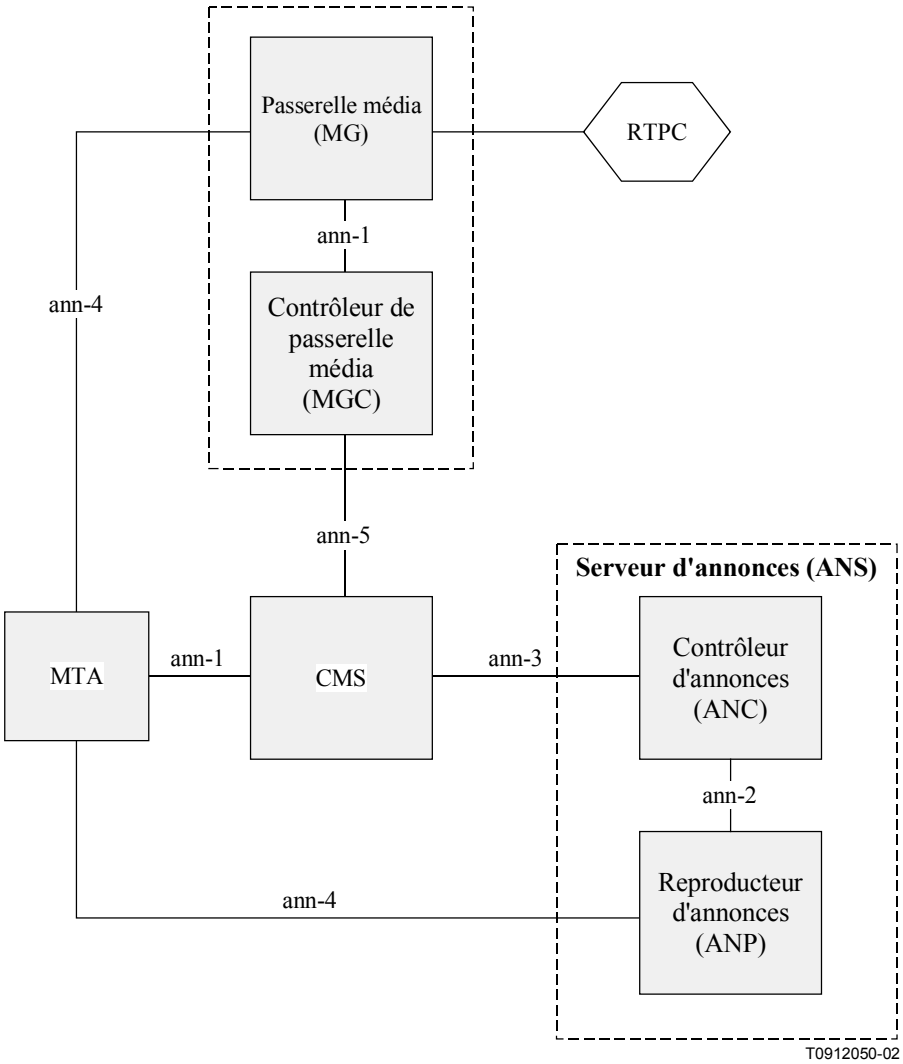


Figure 12/J.160 – Composants et interfaces des services d'annonce

Tableau 6/J.160 – Interfaces d'annonce

Interface	Composant fonctionnel IPCablecom	Protocole
Pkt-ann1	MTA ⟷ CMS MGC ⟷ MG	L'interface entre serveur CMS et adaptateur MTA offre un mécanisme permettant au serveur CMS de signaler à l'adaptateur MTA qu'il doit reproduire localement des annonces mémorisées. La mémorisation d'annonces dans l'adaptateur MTA permet de fournir à l'utilisateur final des tonalités donnant des informations de progression d'appel, indépendamment de l'état du réseau (par exemple, encombrement). Un progiciel d'annonce en mode NCS a été défini pour usage aux interfaces aussi bien CMS-MTA que MGC-MG. Des annonces simples et à contenu fixe (par exemple, "toutes les lignes sont occupées") peuvent aussi être mémorisées dans la passerelle média afin de fournir des annonces aux utilisateurs du RTPC. L'interface MGC-MG offre un mécanisme permettant à la passerelle média de reproduire des annonces à contenu fixe chez des utilisateurs finals du RTPC dans des communications avec accès de l'extérieur à l'intérieur du réseau.
Pkt-ann2	ANC ⟷ ANP	Le protocole de signalisation pour l'interface entre ANC et ANP est NCS avec un progiciel d'annonce. Lorsque le serveur CMS détecte la nécessité d'une annonce par serveur ANS, il envoie une demande au contrôleur ANC par l'interface Pkt-ann-3. Dès qu'il reçoit une demande issue du serveur CMS, le contrôleur ANC ouvre une session avec le reproducteur d'annonces au moyen du progiciel NCS.
Pkt-ann3	CMS ⟷ ANC	Le protocole de l'interface Pkt-ann-3 est indéfini dans l'architecture IPCablecom.
Pkt-ann4	ANP ⟷ MTA	Cette interface définit le format de flux média (RTP) pour l'acheminement de l'annonce entre le reproducteur d'annonce et l'adaptateur MTA au moyen du protocole RTP.
Pkt-ann5	CMS ⟷ MGC	Le protocole de l'interface Pkt-ann-5 est indéfini dans l'architecture IPCablecom.

7.7.1 Configuration physique ou configuration logique du serveur ANS

Le contrôleur ANC et le reproducteur ANP sont des composants logiques qui peuvent résider dans les mêmes entités physiques, auquel cas leurs interfaces deviennent facultatives. Par ailleurs, les composants autonomes utilisant les interfaces Pkt-ann-2 et Pkt-ann-3 peuvent être partagés par de nombreuses entités de réseau.

7.8 Sécurité

7.8.1 Aperçu général

Chacune des interfaces de protocole IPCablecom est exposée à des menaces qui pourraient compromettre la sécurité de l'abonné comme du fournisseur de services. L'architecture IPCablecom traite ces menaces en spécifiant, pour chaque interface de protocole définie, les mécanismes de sécurité sous-jacents (comme IPsec) qui offrent à cette interface les services de sécurité qu'elle exige, par exemple, l'authentification, l'intégrité, la confidentialité.

Le trajet du flux média peut par exemple traverser un grand nombre de lignes de fournisseurs de services Internet et de services infrastructurels qui peuvent être inconnus. En conséquence, le flux média est parfois vulnérable à des interceptions illicites se traduisant par une perte de la

confidentialité des communications. Les services essentiels de sécurité IPCablecom comportent un mécanisme assurant le chiffrement de bout en bout des flux médias en protocole RTP, ce qui réduit considérablement les atteintes possibles à la confidentialité des communications.

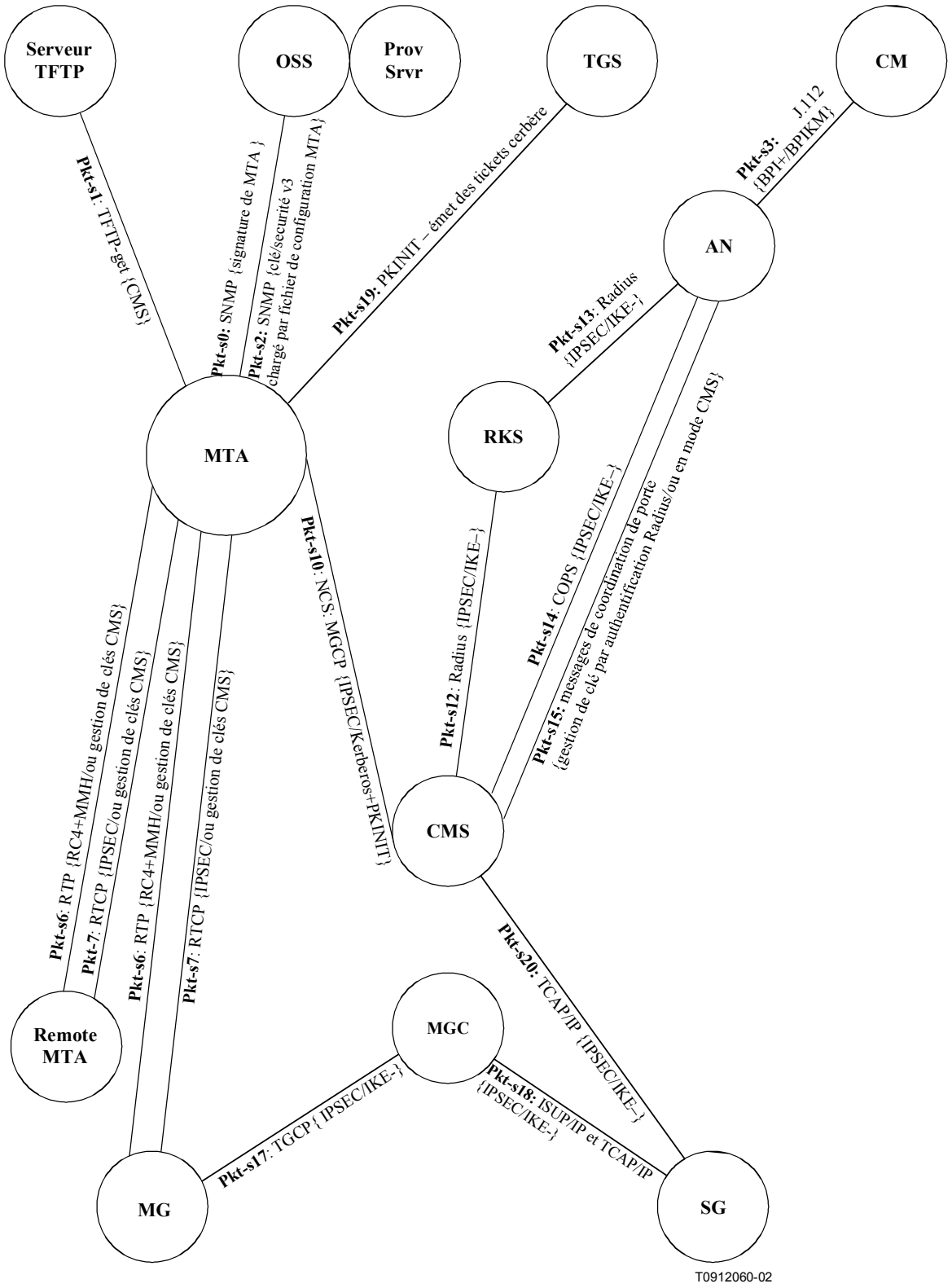
Les services de sécurité disponibles par l'intermédiaire de la couche des services essentiels de l'architecture IPCablecom sont l'authentification, le contrôle d'accès, l'intégrité, la confidentialité et la non-répudiation. Une interface de protocole IPCablecom peut employer zéro, un ou plusieurs de ces services afin de répondre à ses exigences de sécurité particulières.

La sécurité IPCablecom répond comme suit aux exigences de sécurité de chaque interface de protocole constituante:

- en identifiant le modèle de menace propre à chaque interface de protocole constituante;
- en identifiant les services de sécurité (authentification, autorisation, confidentialité, intégrité et non-répudiation) requis pour répondre aux menaces identifiées;
- en spécifiant le mécanisme de sécurité particulier qui assure les services de sécurité requis.

Les mécanismes de sécurité comprennent aussi bien le protocole de sécurité (par exemple, IPsec, sécurité de couche RTP et sécurité SNMPv3) que le protocole de gestion de clé sous-jacent (par exemple, IKE, PKINIT/Cerbère).

La Figure 13 présente un résumé de toutes les interfaces de sécurité IPCablecom.



IKE – échange IKE de clés prépartagées
IKE+ échange IKE nécessitant des certificats de clé publique
KM de type CMS production et distribution aléatoires des clés par serveur CMS

Figure 13/J.160 – Interfaces de sécurité IPCablecom

Dans la Figure 13, chaque interface est étiquetée comme suit:

<étiquette>:<protocole> { <protocole de sécurité> / <protocole de gestion de clés> }

Si le protocole de gestion de clés fait défaut, cela signifie qu'il n'est pas nécessaire pour l'interface considérée. Les interfaces IPCablecom qui n'exigent pas de sécurité ne sont pas représentées dans la Figure 13.

Le Tableau 7 décrit chacune des interfaces indiquées dans la Figure 13.

Tableau 7/J.160 – Interfaces de sécurité

Interface	Composant fonctionnel IPCablecom	Description
Pkt-s0	MTA ⟷ Application de mise en service	Un message INFORM du protocole SNMPv3 est envoyé par l'adaptateur MTA au gestionnaire SNMP, suivi de message(s) GET facultatif(s) par le gestionnaire SNMP afin de connaître les capacités d'adaptateur MTA. Cela se produit au moment où des clés SNMPv3 ne peuvent pas être fournies et la sécurité est assurée par une signature en code RSA, formatée conformément à la syntaxe de message cryptographique (CMS, *cryptographic message syntax*).
Pkt-s1	MTA ⟷ serveur TFTP ou HTTP	Téléimportation de fichier de configuration d'adaptateur MTA. Celui-ci téléimporte un fichier de configuration (par message TFTP-get) qui est signé par le serveur TFTP et scellé avec la clé publique de l'adaptateur MTA par un enveloppeur de syntaxe de message cryptographique (CMS). Ce flux apparaît immédiatement après un message INFORM de la version SNMPv3, suivi d'un ou de plusieurs messages GET facultatif(s) du protocole SNMP; voir flux Pkt-s0.
Pkt-s2	MTA ⟷ Application de mise en service	Sécurité SNMPv3 normale. Les clés SNMPv3 sont téléimportées avec le fichier de configuration MTA au moyen de l'interface Pkt-s1.
Pkt-s3	CM ⟷ AN	Couche de confidentialité par interface BPI+ dans la liaison HFC. La gestion de sécurité et la gestion de clé sont toutes les deux définies dans la Rec. UIT-T J.112.
Pkt-s6	MTA ⟷ MTA	Paquets médias de bout en bout entre deux adaptateurs MTA ou entre un adaptateur MTA et une passerelle MG. Les paquets RTP sont chiffrés directement par algorithme RC4, sans aucune couche de sécurité supplémentaire. Un code d'authentification de message (MAC, *message authentication code*) utilisant le hachage MMH assure facultativement l'intégrité des messages. Les clés sont distribuées par le serveur CMS aux deux extrémités.
Pkt-s7	MTA ⟷ MTA	Protocole de commande RTCP pour protocole RTP, défini ci-dessus. L'intégrité et le chiffrement des messages sont assurés par IPsec. La gestion des clés est la même que dans le protocole RTP. Les clés sont distribuées par le serveur CMS.
Pkt-s10	MTA ⟷ CMS	Signalisation MTA-CMS du protocole NCS. Intégrité et confidentialité des messages par IPsec. La gestion des clés est assurée par le protocole Cerbère avec l'extension PKINIT (authentification initiale de clé publique).

Interface	Composant fonctionnel IPCablecom	Description
Pkt-s12	CMS ⟷ RKS	Evénements de facturation du service radius envoyés par le serveur CMS au serveur RKS. Les clés d'authentification du service radius sont à codage fixe par 0. En revanche, le protocole IPsec est utilisé pour l'intégrité comme pour la confidentialité des messages. La gestion des clés est IKE–.
Pkt-s13	AN ⟷ RKS	Evénements du service radius envoyés par le réseau d'accès au serveur RKS. Les clés d'authentification du service radius sont à codage fixe par 0. En revanche, le protocole IPsec est utilisé pour l'intégrité comme pour la confidentialité des messages. La gestion des clés est de type IKE–.
Pkt-s14	CMS ⟷ AN	Protocole du service COPS entre GC et AN, utilisé pour téléimporter l'autorisation de QS dans le nœud d'accès. Intégrité et confidentialité des messages assurés par IPsec. Gestion de clés: IKE–.
Pkt-s15	CMS ⟷ AN	Messages de coordination de porte pour DQoS. L'intégrité des messages est assurée par un authentificateur de couche Application (service radius). Les clés sont distribuées par serveur CMS local avec service COPS.
Pkt-s16	N/A	N/A
Pkt-s17	MGC ⟷ MG	Interface IPCablecom avec la passerelle média du RTPC. Le protocole IPsec est utilisé pour l'intégrité comme pour la confidentialité des messages. La gestion des clés est de type IKE–.
Pkt-s18	MGC ⟷ SG	Interface IPCablecom avec la passerelle sémaphore du RTPC. Le protocole IPsec est utilisé pour l'intégrité comme pour la confidentialité des messages. La gestion des clés est de type IKE–.
Pkt-s19	MTA ⟷ TGS	Protocole de gestion de clés Cerbère/PKINIT, dans lequel le serveur TGS envoie des tickets CMS aux adaptateurs MTA.
Pkt-s20	CMS ⟷ SG	Le serveur CMS interroge la passerelle RTPC quant à la portabilité du numéro local (LNP) et d'autres services téléphoniques. Le protocole IPsec est utilisé pour l'intégrité comme pour la confidentialité des messages. La gestion des clés est de type IKE–.

7.8.2 Sécurité de mise en service des dispositifs

L'architecture de sécurité IPCablecom subdivise la mise en service des dispositifs en trois activités distinctes: l'enrôlement d'abonné, la mise en service de dispositif et l'autorisation de dispositif.

7.8.2.1 Enrôlement d'abonné

Le processus d'enrôlement d'abonné établit un compte permanent de facturation d'abonné qui identifie de façon unique l'adaptateur MTA auprès du serveur CMS au moyen du numéro de série de l'adaptateur MTA ou de son adresse MAC. Le compte de facturation sert également à identifier les services auxquels l'abonné est inscrit pour l'adaptateur MTA.

L'enrôlement d'abonné peut s'effectuer dans la bande ou hors bande. La spécification proprement dite du processus d'enrôlement d'abonné est hors du domaine d'application de l'architecture IPCablecom et peut être différente selon chaque fournisseur de services.

7.8.2.2 Mise en service de dispositif

Le dispositif MTA vérifie l'authenticité du fichier de configuration qu'il téléimporte du serveur de démarrage. La confidentialité des données de configuration est également assurée. Ces données seront "signées et scellées" par encapsulation dans un objet scellé PKCS #7.

7.8.2.3 Mise en service dynamique

La sécurité SNMPv3 sera utilisée pour la mise en service dynamique des capacités de communication vocale d'un adaptateur MTA incorporé.

7.8.2.4 Autorisation de dispositif

Un dispositif est autorisé lorsqu'un adaptateur MTA mis en service s'authentifie auprès du serveur de gestion d'appels et établit une association de sécurité avec ce serveur avant de devenir pleinement opérationnel. L'autorisation de dispositif permet de protéger la signalisation d'appel subséquente aux termes de l'association de sécurité établie.

7.8.2.5 Sécurité de signalisation

Tout le trafic de signalisation, y compris de QS, d'appel et d'interface de passerelle RTPC, sera sécurisé par IPsec. La gestion des associations de sécurité IPsec sera effectuée au moyen de deux protocoles de gestion de clés: Cerbère/PKINIT et IKE. Le protocole Cerbère/PKINIT servira à échanger des clés entre des clients d'adaptateur MTA et leur serveur CMS. Le protocole IKE servira à gérer toutes les autres associations de sécurité à signalisation IPsec.

7.8.2.6 Sécurité des flux médias

Chaque paquet RTP de flux média est chiffré pour assurer la confidentialité. Les adaptateurs MTA ont la capacité de négocier un algorithme de chiffrement particulier, bien que le seul qui soit actuellement spécifié soit RC4. Le chiffrement est appliqué à la charge utile du paquet et non à son en-tête.

Chaque paquet RTP peut contenir un code d'authentification de message (MAC) facultatif. L'algorithme MAC peut également être négocié, bien que le seul qui soit actuellement spécifié soit le hachage MMH. Le calcul de code MAC recouvre l'en-tête non chiffré et la charge utile chiffrée du paquet.

Les clés de calcul de chiffrement et de codage MAC sont extraites du secret de bout en bout qui est échangé entre adaptateurs MTA émetteurs et récepteurs dans le cadre de la signalisation d'appel. Les échanges de clés pour la sécurité des flux médias sont donc eux-mêmes sécurisés par la protection de la signalisation d'appel.

7.8.2.7 Sécurité du système logistique et du système de facturation

Les agents SNMP contenus dans les dispositifs IPCablecom mettent en œuvre la version SNMPv3. Le modèle de sécurité d'utilisateur SNMPv3 [RFC 2274] fournit les services d'authentification et de confidentialité pour le trafic SNMP. Le contrôle d'accès de type vue SNMPv3 [RFC 2275] peut être utilisé pour le contrôle d'accès à des objets de base MIB.

Le protocole de gestion de clés IKE sert à établir des clés de chiffrement et d'authentification entre le serveur d'archivage (RKS) et chaque élément de réseau IPCablecom produisant des messages événementiels. Lorsque des associations de sécurité de réseau IPsec sont établies, ces clés doivent être créées entre chaque serveur RKS (primaire, secondaire, etc.) et chaque serveur CMS et réseau d'accès. L'échange de clés entre le contrôleur MGC et le serveur RKS peut avoir lieu. Il relève de l'implémentation du vendeur dans la phase 1 de l'architecture IPCablecom. Les messages événementiels sont envoyés par le serveur CMS et par le nœud d'accès au serveur RKS au moyen du protocole de transport RADIUS, qui est lui-même sécurisé par IPsec.

8 Considérations relatives à la conception du réseau

8.1 Synchronisation et comptes rendus

Afin de maintenir la qualité de service, il est fortement recommandé que toutes les horloges équipant le réseau soient calées à ±200 ms du temps universel coordonné (UTC, *universal time coordinated*).

Il est recommandé que les réseaux IPCablecom maintiennent un serveur temporel dont la précision s'inscrive dans un intervalle spécifié du temps universel coordonné (UTC). Il est recommandé que ce serveur soit en mesure d'échanger des informations chronologiques avec d'autres équipements de réseau de façon que les récepteurs puissent être synchronisés avec l'horloge du serveur temporel dès la fin de l'échange du protocole de synchronisation.

Le protocole temporel de réseau (NTP, *network time protocol*) est celui qui est recommandé pour la synchronisation dans l'architecture IPCablecom.

Tous les systèmes qui produisent des messages événementiels de facturation doivent synchroniser leurs horloges avec une référence temporelle du réseau. Il convient d'effectuer la synchronisation de façon que l'horloge propre du dispositif de compte rendu reste à ±100 ms de la dernière valeur de synchronisation.

8.2 Synchronisation d'alignement du tampon de reproduction avec le débit de codage

L'équipement de production et de traitement des paquets fonctionne généralement avec des horloges non synchronisées. Des problèmes peuvent se poser lors de l'offre de services isochrones en raison de la nature plésiochrone de ces horloges. La différence de vitesse d'horloge entre ces entités plésiochrones se manifeste généralement par un excès ou un défaut de remplissage des tampons de reproduction.

Afin de minimiser l'apparition de ces conditions, tous les nœuds d'accès devraient caler leur débit de transmission aval sur un rythme issu d'une référence reflétant une horloge de strate 3. Les adaptateurs MTA incorporés doivent utiliser le débit de transmission aval afin de déterminer le rythme utilisé pour déterminer la période de mise en paquets. Il convient également que les adaptateurs MTA utilisent ce rythme pour déterminer le débit de reproduction à la sortie du tampon de réception. Les adaptateurs MTA non incorporés devront utiliser l'intervalle moyen entre arrivées de paquets[1] comme base de détermination de leur horloge de mise en paquets et de reproduction.

8.3 Adressage IP

Un adaptateur MTA intégré est une entité multifonctionnelle dont une fonction est requise pour l'administration du câblo-modem et dont la deuxième fonction est celle de l'adaptateur MTA proprement dite. Toutes les adresses IP d'un réseau IPCablecom sont de type IPv4.

Tous les adaptateurs MTA incorporés de l'architecture IPCablecom doivent posséder deux adresses. l'une pour le câblo-modem, l'autre pour l'adaptateur MTA. Tous les adaptateurs MTA incorporés de l'architecture IPCablecom doivent posséder deux adresses MAC: l'une pour le câblo-modem, l'autre pour l'adaptateur MTA proprement dit.

Les exigences suivantes peuvent être satisfaites au moyen de cette double configuration d'adresses IP:

- un adaptateur MTA incorporé contenant une double adresse IP peut attribuer une adresse IP privée à la fonction de serveur-modem, si la conversion de table NAT n'est pas assurée ailleurs dans le réseau IPCablecom;

---

[1] C'est-à-dire entre l'arrivée du premier bit du paquet N et l'arrivée du premier bit du paquet N+1, sans tenir compte des intervalles dans lesquels aucun paquet n'arrive dans la périodicité prévue ±5 ms.

- avec deux adresses IP par adaptateur MTA, l'opérateur IPCablecom peut acheminer les paquets de service vocal sur une infrastructure vocale et tous les autres paquets (données) sur une infrastructure non vocale. L'infrastructure de routage doit surtout être configurée de façon que différents trajets de routage soient suivis pour chacune des deux adresses IP de destination;
- l'opérateur du réseau IPCablecom peut simplifier les fonctions d'administration et de gestion du côté réseau en utilisant des adresses IP distinctes. Par exemple, des filtres de politique peuvent être instanciés afin d'admettre ou d'interdire le trafic issu du composant MTA du nœud. Par ailleurs, les fournisseurs de services de réseau peuvent fournir des services de sélection d'adresse d'origine et des statistiques ou diagnostics de trafic réseau peuvent être collectés sur la base de l'adresse IP de l'adaptateur MTA.

Les doubles adresses IP relèvent de considérations particulières qui ont une incidence sur ce qui suit:

- implémentation d'une pile de protocoles IP dans l'adaptateur MTA;
- implémentation d'un système d'assistance à l'exploitation (OSS) et de protocoles de mise en service de dispositifs IPCablecom;
- implémentations de tables de routage dans le réseau.

8.4 Attribution dynamique d'adresses IP

Un problème d'exploitation se pose au sujet de l'attribution dynamique d'adresses IP aux adaptateurs MTA. Le modèle de signalisation NCS spécifié dans l'architecture IPCablecom est fondé sur l'association, par un serveur de gestion d'appels, d'un service d'abonné avec un identificateur d'extrémité et une adresse IP. Les opérations de traitement d'appel seront donc affectées si l'adresse IP de l'adaptateur MTA est modifiée au cours d'une communication active. Il existe cependant certaines recommandations que les opérateurs de réseau et vendeurs d'adaptateurs MTA peuvent appliquer afin de résoudre ce problème:

1) lors de la configuration des options de protocole DHCP pour un adaptateur MTA, il y a lieu que l'opérateur de réseau configure la durée de location d'adresse IP (code d'option 51) de façon à spécifier une durée de location très longue. Cette option est détaillée dans le protocole de configuration dynamique de serveur (DHCP) [RFC 2131] et dans les options DHCP et extensions de vendeur BOOTP [RFC 2132]. Conformément au § 3.3 du commentaire RFC 2131, une durée de location réglée à la valeur "0xffffffff" représente une durée infinie. L'emploi de longues durées de location minimisera la probabilité qu'un adaptateur MTA ne soit pas en mesure de renouveler sa location d'adresse IP attribuée.
2) il y a lieu également que les opérateurs de réseau configurent les valeurs T1 et T2 d'un temporisateur DHCP d'adaptateur MTA (codes d'option 58 et 59 respectivement) de façon qu'elles ne dépassent pas les valeurs par défaut spécifiées au § 4.4.5 du commentaire RFC 2131. Le fait de configurer un adaptateur MTA de façon qu'il commence son processus de renouvellement de durée de location d'adresse IP à 50 % au plus de la durée de location attribuée, combiné à l'utilisation de très grandes valeurs de durée de location, garantira également qu'un adaptateur MTA sera en mesure de renouveler sa location d'adresse IP.
3) il y a lieu que les vendeurs d'adaptateurs MTA implémentent des mécanismes empêchant un adaptateur MTA d'entrer dans l'état "RENEWING" (renouvellement, comme spécifié dans RFC 2131) alors que le traitement d'appel est actif. Il relèvera de l'implémentation du vendeur de déterminer la façon exacte dont cette capacité pourra être le mieux implémentée dans son produit.

8.5 Attribution de noms FQDN

On trouvera ci-dessous les problèmes d'exploitation éventuels qui sont censés être résolus par des implémentations spécifiques de vendeur.

L'on part du principe que l'administration du système d'assistance à l'exploitation (OSS) produira les noms FQDN appropriés à tous les dispositifs IPCablecom et transmettra ces données aux dispositifs IPCablecom et aux autres éléments de réseau appropriés. Ces interfaces ne sont pas définies dans l'architecture IPCablecom (phase 1).

Un problème d'exploitation se pose en ce qui concerne la synchronisation des bases de données à l'intérieur du domaine de mise en service. Plus précisément, la base de données DHCP et les tables de système DNS nécessitent des mises à jour concomitantes lorsqu'une fiche d'abonné est modifiée (ce qui inclut sa création). Le commentaire RFC 2131 offre un mécanisme permettant à un serveur (client de protocole DHCP) d'acquérir certaines informations de configuration, en particulier son ou ses adresses IP. Le protocole DHCP n'offre cependant pas de mécanismes permettant de mettre à jour les fiches de ressources DNS qui contiennent les informations relatives au mappage entre le nom FQDN du serveur et son ou ses adresses IP (c'est-à-dire les fiches de ressource d'adresse et de pointeur). Les informations conservées par le système DNS pour un client DHCP peuvent donc être incorrectes car un serveur (le client) peut obtenir son adresse au moyen du protocole DHCP mais la fiche de ressource d'adresse correspondant au nom FQDN de ce serveur ne reflétera pas l'adresse obtenue par le serveur et la fiche de ressource de pointeur correspondant à l'adresse obtenue ne reflétera pas le nom FQDN du serveur.

Le problème comporte deux éléments principaux: premièrement comment mettre à jour le système DNS lorsqu'une nouvelle adresse IP est attribuée et d'autre part quelle durée attribuer aux valeurs de fiche de ressource. Ces deux éléments relèvent de l'implémentation du vendeur et se trouvent donc hors du domaine d'application des spécifications IPCablecom. Certaines recommandations "modèles" sont cependant décrites dans le commentaire RFC 2131.

8.6 Marquage de priorité dans les paquets de flux de signalisation et de flux média

Aussi bien le flux média que le flux de signalisation pour services de type IPCablecom nécessitent des méthodes appropriées de marquage et de transport des paquets à un niveau de qualité de service suffisamment élevé, tant dans le réseau d'accès J.112 que dans l'infrastructure IP gérée.

Le principal mécanisme permettant d'offrir une qualité de service à faible retard pour les flux médias dans le réseau d'accès est le service de classification de flux J.112, qui classe les paquets en flux spécifiques sur la base de champs de paquet comme les adresses de source et de destination IP et les paramètres de numéro d'accès UDP. Vers l'amont, ces paquets classifiés sont transportés par un service approprié à débit constant (pour les codecs actuels), qui est planifié dynamiquement dans le temps par le nœud d'accès. Vers l'aval, les paquets sont transportés par un mécanisme approprié de mise en files d'attente à haute priorité et de planification dans le temps. Les mécanismes de signalisation DQoS (entre CMS et AN) et J.112 (entre AN et CM) servent à fixer dynamiquement les règles de classification des flux médias et les paramètres de trafic QS des services.

En plus de la classification des flux, il est utile de marquer les paquets de flux média avec des priorités appropriées. Ces marquages de priorité peuvent être utilisés à l'intérieur de systèmes de mise en file d'attente aux interfaces AN/CM ainsi qu'à l'intérieur des infrastructures de QS à gestion Diff-serv (qui peuvent ne pas contenir de mécanismes de classification de flux) afin d'assurer un traitement de QS à haute priorité de tels paquets. Il y a lieu de noter que si aucune définition n'est donnée quant à la façon dont la QS est gérée dans l'infrastructure IP gérée de l'architecture actuelle, il est prévu que les mécanismes définis pour la QS de l'architecture IPCablecom seront utilisables dans une telle infrastructure gérée.

Les paquets de signalisation peuvent également bénéficier de services QS priorisés. Lorsqu'en particulier un réseau d'accès arrive à sa limite de capacité, il est sans doute important de retransmettre les paquets de signalisation à un niveau de priorité plus élevé que les paquets de données afin d'éviter un trop grand retard de signalisation. Il convient de noter que, du point de vue de l'ingénierie de trafic réseau, l'on n'a pas encore déterminé si un traitement à haute priorité des paquets de signalisation est requis. Si l'on recherche la priorisation de la signalisation de QS, la

méthode appropriée est fondée sur deux mécanismes: d'abord le marquage de tous les paquets de signalisation à un niveau de priorité élevé; ensuite la mise en œuvre d'un classificateur J.112 rangeant tous les paquets de signalisation à transporter dans un flux de service de priorité supérieure. Ce classificateur peut se réduire à une association de tous les paquets amont ayant une priorité donnée avec l'identificateur SID de haute priorité. Il peut être plus complexe et identifier également l'adresse IP de l'adaptateur (des adaptateurs) MTA émettant la signalisation. Le flux de service de priorité supérieure peut être soit mis en service statiquement ou être créé dynamiquement par l'administrateur du nœud d'accès. Il convient de noter que si l'administrateur cherche à éviter un vol de service dans le flux de service à haute priorité, il peut configurer ce flux de service de façon qu'il ait une priorité élevée (faible retard) mais une largeur de bande étroite.

Le marquage des paquets pour les deux flux – médias et de signalisation (NCS) – est effectué dans la couche IP par l'adaptateur MTA et par le serveur CMS au moyen d'un champ qui est appelé parfois l'octet de type de service (TOS) et parfois la séquence codée Diff-serv (DSCP, *diff-serv code point*). L'octet TOS était la définition initiale de cet octet tandis que la séquence DSCP est la nouvelle définition de l'octet telle qu'utilisée par l'architecture Diff-serv du groupe IETF. Etant donné qu'il y a deux formats pour cet octet, il y a lieu d'effectuer la configuration des valeurs d'une façon indépendante du format et du type (dans les bases MIB pour l'adaptateur MTA et pour l'agent d'appel).

Les bases d'informations de gestion (MIB) sont définies dans l'architecture IPCablecom de façon à attribuer les valeurs mises en service et par défaut pour les marquages de priorité de flux média et de flux de signalisation (par exemple, une valeur de "3" pour la signalisation et de "5" pour le média). Il convient de noter qu'en signalisation NCS, les paramètres SDP signalés peuvent contenir, connexion par connexion, des neutralisations de la valeur configurée du marquage de priorité de flux média. Aucun mécanisme n'existe actuellement pour neutraliser dynamiquement, appel par appel, la valeur de marquage de priorité mise en service dans le flux de signalisation.

8.7 Prise en charge de la télécopie

L'architecture IPCablecom prend en charge la transmission de télécopie en temps réel. A cette fin, la "meilleure" méthode consiste à utiliser la norme G.711 pour le codage/décodage audio. Si une communication est établie au moyen d'un codec comprimé, il faudra donner à l'adaptateur MTA incorporé l'ordre de rechercher les tonalités de télécopie. Si celles-ci sont détectées, le serveur CMS devra en recevoir la notification et l'ordre sera donné à l'adaptateur MTA de commuter sur l'utilisation de la norme G.711. Noter que cela implique une surveillance du flux média et une détection des tonalités de télécopie par le dispositif incorporé.

La prise en charge de la commutation sur télécopie à partir d'un appel vocal est requise mais non l'inverse (c'est-à-dire surveillance du flux média de télécopie pour détecter un signal de fin puis recommutation sur un codec à faible largeur de bande).

La terminaison locale de la télécopie et la conversion du flux correspondant en flux-relais de données IP de télécopie ne sont pas requises dans la présente version de l'architecture.

8.8 Prise en charge des modems analogiques

Les modems analogiques sont pris en charge de façon similaire à la télécopie: consigne sera donnée à un adaptateur MTA de détecter les tonalités de modem puis, lorsque de telles tonalités auront été détectées, le serveur CMS donnera à l'adaptateur MTA la consigne de commuter sur le codec G.711 si celui-ci n'est pas déjà en cours d'utilisation. Noter que cela implique une surveillance du flux vocal et une détection des tonalités de modem analogique par le dispositif incorporé.

La commutation sur le codec G.711 pour prendre en charge la signalisation de modem analogique à partir d'un appel vocal sera assurée mais non l'inverse (c'est-à-dire surveillance du flux média de modem pour détecter un signal de fin puis recommutation sur un codec à faible largeur de bande).

La terminaison locale des modems et la conversion du flux correspondant en flux-relais de données IP de modem ne sont pas requises dans la présente version de l'architecture.

APPENDICE I

Bibliographie

– IETF RFC 1899 (1996), *RTP: A Transport Protocol for Real-Time Applications* (RTP: protocole de transport pour applications en temps réel).

– IETF RFC 1890 (1996), *RTP Profile for Audio and Video Conferences with Minimal Control* (Profil RTP pour conférences audio et vidéo avec contrôle minimal).

– IETF RFC 2131(1997), *Dynamic Host Configuration Protocol* (Protocole de configuration dynamique de serveur).

– IETF RFC 2132 (1997), *DHCP Options and BOOTP Vendor Extensions* (Options DHCP et extensions de vendeur BOOTP).

– IETF RFC 2274 (1998), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)* (Modèle de sécurité selon l'utilisateur (USM) pour la version 3 du protocole simple de gstion de réseau (SNMPv3).

– IETF RFC 2275 (1998), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)* (Obsoleted by RFC 2575) (Modèle de commande d'accès selon la vue (VACM) pour le protocole simple de gestion de réseau (SNMP) (annulé par RFC 2575).

– IETF RFC 2575 (1999), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).* (Obsoletes RFC 2275) (Modèle de commande d'accès selon la vue (VACM) pour le protocole simple de gestion de réseau (SNMP) (annule RFC 2275).

APPENDICE II

Glossaire terminologique

Le présent appendice contient la liste complète des termes, des définitions, des acronymes et des abréviations utilisés dans la série des Recommandations relatives à l'environnement IPCablecom.

II.1 Définitions

II.1.1 contrôle d'accès: limitation du flux d'informations provenant des ressources d'un système aux seuls programmes, processus, personnes ou aux autres ressources de système dans un réseau.

II.1.2 nœud d'accès: dans le cadre de la présente Recommandation, dispositif de terminaison de couche 2 formant l'extrémité réseau de la connexion J.112. Dépend de la technique employée. Appelé INA (adaptateur de réseau interactif) dans l'Annexe A/J.112 et CMTS (système de terminaison de câblo-modem) dans l'Annexe B.

II.1.3 actif: un flux J.112 est dit "actif" lorsqu'il est autorisé à retransmettre des paquets de données. Un flux J.112 doit d'abord être admis avant d'être actif.

II.1.4 authentification: processus de vérification de l'identité déclarée par une entité auprès d'une autre entité.

II.1.5 authenticité: capacité permettant de garantir que les informations données sont exemptes de modification ou de falsification et qu'elles ont bien été produites par l'entité qui déclare les avoir fournies.

II.1.6 autorisation: fourniture de l'accès à un service ou à un dispositif lorsque l'accès est autorisé.

II.1.7 câblo-modem: dispositif de terminaison de couche 2 formant l'extrémité client de la connexion J.112.

II.1.8 appel: demande par un utilisateur de capacités de communication vocale. En téléphonie classique, un appel est généralement considéré comme l'établissement d'une connexion directe entre deux points, l'entité de départ et l'entité d'arrivée. Dans le contexte IPCablecom, la communication entre les entités est, comme indiqué ci-dessus, "en mode sans connexion" au sens traditionnel.

II.1.9 chiffrement; cryptage: algorithme ou méthode qui transforme des données en clair en données chiffrées.

II.1.10 suite de chiffrement: ensemble qui doit contenir un algorithme de chiffrement et un algorithme d'authentification de message (par exemple, MAC ou HMAC). En général, il peut aussi contenir un algorithme de gestion de clés, qui n'est pas applicable dans le contexte IPCablecom.

II.1.11 confidentialité: moyen de s'assurer que des informations ne sont pas divulguées à des personnes autres que celles à qui elles sont destinées. La confidentialité est assurée par le chiffrement des informations.

II.1.12 aval: sens allant de la tête de réseau aux locaux d'abonné.

II.1.13 chiffrement; cryptage: voir II.1.9.

II.1.14 extrémité: terminal, passerelle ou pont MCU.

II.1.15 message d'événement: ensemble de données représentant dans l'architecture IPCablecom un événement qui correspond à l'utilisation d'une ou de plusieurs capacités IPCablecom facturables. Un message d'événement en lui-même n'indique pas nécessairement toutes les activités facturables d'un client mais, en corrélation avec d'autres messages d'événement, il forme la base d'un enregistrement de données des utilisations facturables.

II.1.16 attribut de message d'événement: élément de données prédéfini qui est décrit par une définition et par un type.

II.1.17 passerelle: dispositif servant de pont entre l'environnement IPCablecom de communication vocale IP et le RTPC; par exemple, la passerelle média qui comporte les interfaces des circuits support avec le RTPC et transcode le flux média, ou la passerelle de signalisation qui émet et reçoit une signalisation de réseau à commutation de circuits au niveau de la frontière du réseau IPCablecom.

II.1.18 en-tête: information de commande de protocole située au début d'une unité de données de protocole.

II.1.19 intégrité: moyen de s'assurer que les informations ne sont pas modifiées sauf par ceux qui en ont l'autorisation.

II.1.20 IPCablecom: projet UIT-T comprenant une architecture et une série de Recommandations permettant la fourniture de services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems.

II.1.21 transaction IPCablecom: ensemble d'événements se produisant dans le réseau IPCablecom lors de la fourniture d'un service à un abonné. Les messages d'événement associés à une même transaction sont identifiés par un unique identificateur de corrélation pour facturation. Dans le cas de

certains services, plusieurs transactions peuvent être requises pour fournir les informations nécessaires à la collecte de toutes les données d'utilisation du service. Plusieurs messages d'événement peuvent être nécessaires pour repérer les ressources pour chacun des services utilisés. Une transaction peut durer un certain temps.

II.1.22 flux J.112: flux uni- ou bidirectionnel de paquets de données, qui est soumis à la signalisation de couche MAC et à l'attribution de qualité de service conformément à la Rec. UIT-T J.112.

II.1.23 Cerbère (*Kerberos*): protocole d'authentification de réseau à clé secrète qui fait appel à un ensemble d'algorithmes cryptographiques pour le chiffrement et à une base de données de clés centralisée pour l'authentification.

II.1.24 clé: valeur mathématique introduite dans l'algorithme cryptographique choisi.

II.1.25 échange de clés: échange entre entités de clés publiques à utiliser pour le chiffrement de communications entre ces entités.

II.1.26 gestion de clés: processus de distribution de clés symétriques partagées nécessaires à l'application d'un protocole de sécurité.

II.1.27 MIB: (base d'informations de gestion) – Spécification d'informations d'une manière permettant un accès normalisé au moyen d'un protocole de gestion de réseau.

II.1.28 non-répudiation: capacité permettant d'empêcher un expéditeur de nier ultérieurement avoir envoyé un message ou exécuté une opération.

II.1.29 secret: terme parfois utilisé pour désigner la confidentialité. Voir II.1.11.

II.1.30 clé privée: clé utilisée en cryptographie à clés publiques, qui appartient à une seule entité et doit être tenue secrète.

II.1-31 serveur proxy: équipement qui fournit de manière indirecte certains services ou qui agit comme un représentant pour la fourniture d'informations, évitant ainsi à un serveur hôte de devoir prendre en charge les services proprement dits.

II.1.32 clé publique: clé utilisée en cryptographie à clés publiques, qui appartient à une seule entité et est distribuée publiquement. Les autres entités utilisent cette clé pour chiffrer les données à envoyer au détenteur de la clé.

II.1.33 certificat de clé publique: lien entre la clé publique d'une entité et un ou plusieurs attributs associés à l'identité de celle-ci; également appelé certificat numérique.

II.1.34 cryptographie à clés publiques: procédure, également appelée algorithme asymétrique, faisant appel à une paire de clés (l'une publique et l'autre privée) pour le chiffrement et le déchiffrement. La clé publique d'un utilisateur est mise à disposition publiquement afin que les autres utilisateurs puissent l'utiliser pour envoyer un message au détenteur de la clé. La clé privée d'un utilisateur est tenue secrète. C'est la seule clé qui permette de déchiffrer les messages chiffrés au moyen de la clé publique de l'utilisateur.

II.1.35 clé privée racine: clé de signature privée de l'autorité de certification du niveau le plus élevé. Elle est normalement utilisée pour signer des certificats de clé publique destinés aux autorités de certification de niveau inférieur ou à d'autres entités.

II.1.36 clé publique racine: clé publique de l'autorité de certification du niveau le plus élevé. Elle est normalement utilisée pour vérifier les signatures numériques qui ont été produites avec la clé privée racine correspondante.

II.1.37 service: fonctionnalité ou ensemble de fonctionnalités de communication qu'un abonné peut sélectionner. Un service est identifié par un ensemble d'un ou de plusieurs "appels" ou transactions qui permettent à l'abonné de disposer de la fonctionnalité souhaitée. Exemples de service:

communication vocale entre deux abonnés IPCablecom locaux, conversation à trois, films à la carte et session de navigation sur le Web. Un service peut être ponctuel ou durable.

II.1.38 passerelle de signalisation (SG, *signalling gateway*): Agent de signalisation qui reçoit/émet la signalisation RCC d'origine à la frontière du réseau IP. La fonction SG du système C7 convertit en particulier les variantes des sous-systèmes ISUP et TCAP contenues dans une passerelle C7 Internet en une version commune de ces sous-systèmes.

II.1.39 certificat X.509: spécification de certificat de clé publique élaborée dans le cadre de la série de normes UIT-T X.500 relatives à l'annuaire.

II.2 Abréviations

AH	en-tête d'authentification (*authentication header*)
AMA	comptabilisation automatique des messages (*automated message accounting*)
AN	nœud d'accès (*access node*)
ANC	contrôleur d'annonces (*announcement controller*)
ANP	reproducteur d'annonces (*announcement player*)
ANS	serveur d'annonces (*announcement server*)
API	interface de programmation d'applications (*application programming interface*)
BPI+	interface de confidentialité de base + (*baseline privacy interface plus*)
C7	système de signalisation n^{o} 7 (*signalling system No. 7*)
CA	agent d'appel (*call agent*)
CBC	mode d'enchaînement de blocs chiffrés (*cipher block chaining mode*)
CDR	relevé détaillé des communications (*call detail record*)
CIC	code d'identification de circuit
CID	identificateur de circuit (*circuit ID*)
CM	câblo-modem
CMS	serveur de gestion d'appels (*call management server*)
CMS	syntaxe de message cryptographique (*cryptographic message syntax*)
CMTS	système de terminaison de câblo-modem (*cable modem termination system*)
COPS	service de politique ouverte commune (*common open policy service*)
CPE	équipement des locaux client (*customer premises equipment*)
DCS	signalisation d'appel répartie (*distributed call signalling*)
DHCP	protocole de configuration de serveur dynamique (*dynamic host configuration protocol*)
DNS	système de noms de domaine (*domain name system*)
DPC	code de point de destination (*destination point code*)
DQoS	qualité de service dynamique (*dynamic quality of service*)
DTMF	multifréquence à deux tonalités (*dual tone multi-frequency*)
ESP	sécurité d'encapsulation IPsec (*IPsec encapsulation security*)
F ID	identificateur de flux (*flow identifier*)
FQDN	nom de domaine complet (*fully qualified domain name*)
GC	portier (*gate controller*)
HFC	système hybride fibre optique/câble coaxial (*hybrid fibre/coaxial [cable]*)

HMAC	code d'authentification de message par hachage (*hashed message authentication code*)
HTTP	protocole de transfert hypertexte (*hypertext transfer protocol*)
IANA	Autorité chargée de l'assignation des numéros Internet (*Internet assigned numbers authority*)
IEEE	Institut des ingénieurs électriciens et électroniciens (*Institute of Electrical and Electronics Engineers*)
IETF	Groupe de travail d'ingénierie Internet (*Internet engineering task force*)
IKE	échange de clés Internet (*Internet key exchange*)
IKE–	échange IKE où les clés sont partagées à l'avance pour l'authentification (*IKE with pre-shared keys for authentication*)
IKE+	échange IKE nécessitant des certificats numériques pour l'authentification (*a notation defined to refer to the use of IKE, which requires digital certificates for authentication*)
INA	adaptateur de réseau interactif (*interactive network adapter*)
IP	protocole Internet (*Internet protocol*)
IPsec	sécurité IP (*IP security*)
ISTP	protocole de transport de signalisation Internet (*Internet signalling transport protocol*)
ISUP	sous-système utilisateur de réseau numérique à intégration de services (*integrated services digital network user part*)
LNP	portabilité de numéro local (*local number portability*)
MAC	code d'authentification de message (*message authentication code*)
MAC	commande d'accès au support physique (*media access control*)
MD5	condensé de message 5 (*message digest 5*)
MF	multifréquence
MG	passerelle média (*media gateway*)
MGC	contrôleur de passerelle média (*media gateway controller*)
MGCI	interface de contrôleur de passerelle média (*media gateway controller interface*)
MGCP	protocole de commande de passerelle média (*media gateway control protocol*)
MIB	base d'informations de gestion (*management information base*)
MMH	hachage modulaire multilinéaire (*multilinear modular hash*)
MTA	adaptateur de terminal de média (*media terminal adapter*)
MTP	sous-système transfert de messages (*message transfer part*)
MWD	délai d'attente maximal (*maximum waiting delay*)
NCS	signalisation d'appel par le réseau (*network call signalling*)
NTP	protocole relatif au temps dans le réseau (*network time protocol*)
OSS	système d'assistance à l'exploitation (*operational support system*)
PHS	suppression d'en-tête de charge utile (*payload header suppression*)
PKI	infrastructure de clé publique (*public key infrastructure*)
PKINIT	authentification initiale par cryptographie à clé publique (*public key cryptography initial authentication*)
QS	qualité de service
RADIUS	service d'accès distant pour les utilisateurs entrants (*remote access dial-in user service*)
RAP	protocole d'attribution de ressources (*resource allocation protocol*)

RC4	chiffrement de flux à longueur de clé variable faisant partie de la suite de chiffrement, utilisé pour chiffrer le trafic média dans le réseau IPCablecom
RFC	demande d'observations (*request for comments*)
RFI	interface radioélectrique (*radio frequency interface*)
RKS	serveur d'archivage (*record keeping server*)
RSVP	protocole de réservation de ressources (*resource reservation protocol*)
RTCP	protocole de commande en temps réel (*real-time control protocol*)
RTO	temporisation de retransmission (*retransmission timeout*)
RTP	protocole de transfert en temps réel (*real-time transfer protocol*)
RTPC	réseau téléphonique public commuté
SA	adresse de source (*source address*)
SA	association de sécurité (*security association*)
SCCP	sous-système commande de connexions sémaphores (*signalling connection control part*)
SCP	point de commande de services (*service control point*)
SCTP	protocole de transmission de commande de flux (*stream control transmission protocol*)
SDP	protocole de description de session (*session description protocol*)
SG	passerelle sémaphore; passerelle de signalisation (*signalling gateway*)
SHA – 1	algorithme 1 de hachage sécurisé (*secure hash algorithm 1*)
SID	numéro d'identification de système (*system identification number*)
SIP	protocole d'ouverture de session (*session initiation protocol*)
SIP+	protocole d'ouverture de session + (*session initiation protocol plus*)
SNMP	protocole simple de gestion de réseau (*simple network management protocol*)
SPI	indice des paramètres de sécurité (*security parameters index*)
SSP	point de commutation de signal (*signal switching point*)
TCAP	sous-système application pour la gestion des transactions (*transaction capabilities application part*)
TCP	protocole de commande de transmission (*transmission control protocol*)
TGS	serveur-distributeur de tickets (*ticket granting server*)
TLV	type-longueur-valeur (*type-length-value*)
ToS	type de service (*type of service*)
UDP	protocole datagramme d'utilisateur (*user datagram protocol*)
VAD	détection d'activité vocale (*voice activity detection*)
VoIP	téléphonie utilisant la protocole Internet (*voice over IP*)

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
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	RGT et maintenance des réseaux: systèmes de transmission, circuits téléphoniques, télégraphie, télécopie et circuits loués internationaux
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 et communication entre systèmes ouverts
Série Y	Infrastructure mondiale de l'information et protocole Internet
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

21843

Imprimé en Suisse
Genève, 2002