Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

J.160

(11/2005)

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

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 contient un cadre de référence de haut niveau qui identifie les composants fonctionnels et définit les interfaces nécessaires pour fournir des services de téléphonie numérique. Une famille de Recommandations (Recommandations UIT-T J.161-J.178) a été élaborée pour implémenter cette architecture.

Source

La Recommandation UIT-T J.160 a été approuvée le 29 novembre 2005 par la Commission d'études 9 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

AVANT-PROPOS

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

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

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

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

NOTE

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

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

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

Le projet IPCablecom définit une famille de Recommandations à utiliser pour mettre au point des équipements interopérables capables de fournir des services vocaux et vidéo en mode paquet et autres services multimédias à haut débit en mode paquet sur des systèmes hybrides par fibres optiques et par câbles coaxiaux (HFC, *hybrid fiber coax*) utilisant des câblo-modems conformes à la famille de Recommandations DOCSIS. Cette architecture sera élargie dans l'avenir afin d'inclure les applications multimédias.

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. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

– 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 (1998), *Systèmes de transmission pour services interactifs de télévision par câble* plus Annexe A (2001), *Diffusion vidéonumérique: canal d'interaction pour les systèmes de télédistribution par câble,* Annexe B (2004), *Spécifications de l'interface du service de transmisssion de données par câble: interface radioélectrique* et Annexe C (2002), *Spécifications de l'interface du service de transmission de données par câble: interface radiofréquence utilisant la technique de modulation en quadrature.*

– 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 (2005), *Protocole réseau de signalisation d'appel pour la fourniture de services à temps critique sur les réseaux de télévision par câble utilisant des cablo-modems*.

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

– Recommandation UIT-T J.164 (2005), *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.166 (2005), *Structure des bases d'informations de gestion (MIB) IPCablecom*.

– Recommandation UIT-T J.167 (2005), *Prescriptions d'installation des adaptateurs MTA pour la fourniture de services en temps réel sur les réseaux de télévision par câble au moyen de câblo-modems*.

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

– Recommandation UIT-T J.171.0 (2005), *Protocole de commande de passerelle de jonction (TGCP) du système IPCablecom: aperçu général des profils*.

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

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

– Recommandation UIT-T T.38 (2005), *Procédures de communication de télécopie du Groupe 3 en temps réel sur les réseaux à protocole Internet*.

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

– IETF RFC 1119 (1989), *Network Time Protocol*.

– IETF RFC 1889 (1996), *RTP: A Transport Protocol for Real-Time Applications*.

– IETF RFC 1890 (1996), *RTP Profile for Audio and Video Conferences with Minimal Control*.

– IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.

– IETF RFC 3168 (2001), *The Addition of Explicit Congestion Notification (ECN) to IP*.

– IETF RFC 3260 (2002), *New Terminology and Clarifications for Diffserv*.

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

– IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.

– IETF RFC 3415 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*.

– IETF RFC 3611 (2003), *RTP Control Protocol Extended Reports (RTCP XR)*.

3 Termes et définitions

La présente Recommandation définit les termes suivants:

3.1 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.

3.2 câblo-modem: dispositif terminal de couche 2 formant l'extrémité client de la connexion DOCSIS.

3.3 réseau IP géré: réseau IP, géré par une entité unique aux fins du transport de paquets de signalisation et de paquets de médias IPCablecom.

3.4 réseau dorsal 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:

ANC contrôleur d'annonces (*announcement controller*)

ANP lecteur 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 contrôleur de porte (*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 (*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 support d'exploitation (*operations 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 d'origine (*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 Recommandation.

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

"DOIT" ce mot ou l'adjectif "REQUIS" signifie que l'élément est une exigence absolue de la présente Recommandation.

"NE DOIT PAS" cette expression signifie que l'élément est une interdiction absolue de la présente Recommandation.

"DEVRAIT" ce mot ou l'adjectif "RECOMMANDÉ" signifie qu'il peut exister, dans des circonstances particulières, des raisons valables pour ignorer cet élément, mais il faut en comprendre toutes les implications et peser attentivement les choses avant de choisir une voie différente.

"NE DEVRAIT PAS" cette expression signifie qu'il peut exister, dans des circonstances particulières, des raisons valables pour que le comportement indiqué soit acceptable voire utile, mais il faut en comprendre toutes les implications et peser attentivement les choses avant d'implémenter tout comportement décrit avec cette mention.

"PEUT" ce mot ou l'adjectif "OPTIONNEL" signifie que cet élément est véritablement optionnel. Un fabricant peut choisir d'inclure l'élément, par exemple parce qu'un marché particulier le requiert ou parce qu'il améliore le produit ; un autre fabricant peut omettre le même élément.

5 IPCablecom

5.1 Cadre architectural IPCablecom

A un niveau très élevé, l'architecture IPCablecom contient trois réseaux: le "réseau d'accès HFC DOCSIS", le "réseau IP géré" et le RTPC. Le système de terminaison de câblo-modem (CMTS, *cable modem termination system*) assure la connexité entre le "réseau d'accès HFC DOCSIS" 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 IPCablecom est décrite sur la Figure 1.

Le réseau d'accès HFC DOCSIS assure un transport fiable et sûr à grande vitesse entre les locaux d'abonné et la tête du réseau câblé. Ce réseau d'accès offre toutes les capacités DOCSIS y compris la qualité de service. Le réseau d'accès HFC DOCSIS comprend les composants fonctionnels suivants: le câblo-modem (CM), l'adaptateur de terminal multimédia (MTA) et le système de terminaison de câblo-modem (CMTS).

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 mise en service et de l'établissement de la qualité de service sur le réseau d'accès. Par ailleurs, le réseau IP géré assure la connexité IP à longue distance entre d'autres réseaux IP gérés et les réseaux HFC DOCSIS. Le réseau IP géré comprend les composants fonctionnels suivants: serveur de gestion d'appels (CMS, *call management server*), plusieurs serveurs du système d'assistance à l'exploitation (OSS, *operation support system*), passerelle sémaphore (SG, *signalling gateway*), passerelle média (MG, *media gateway*) et contrôleur de passerelle média (MGC, *media gateway controller*).

Les différents éléments de réseau représentés sur la Figure 1 sont décrits en détail au § 6.

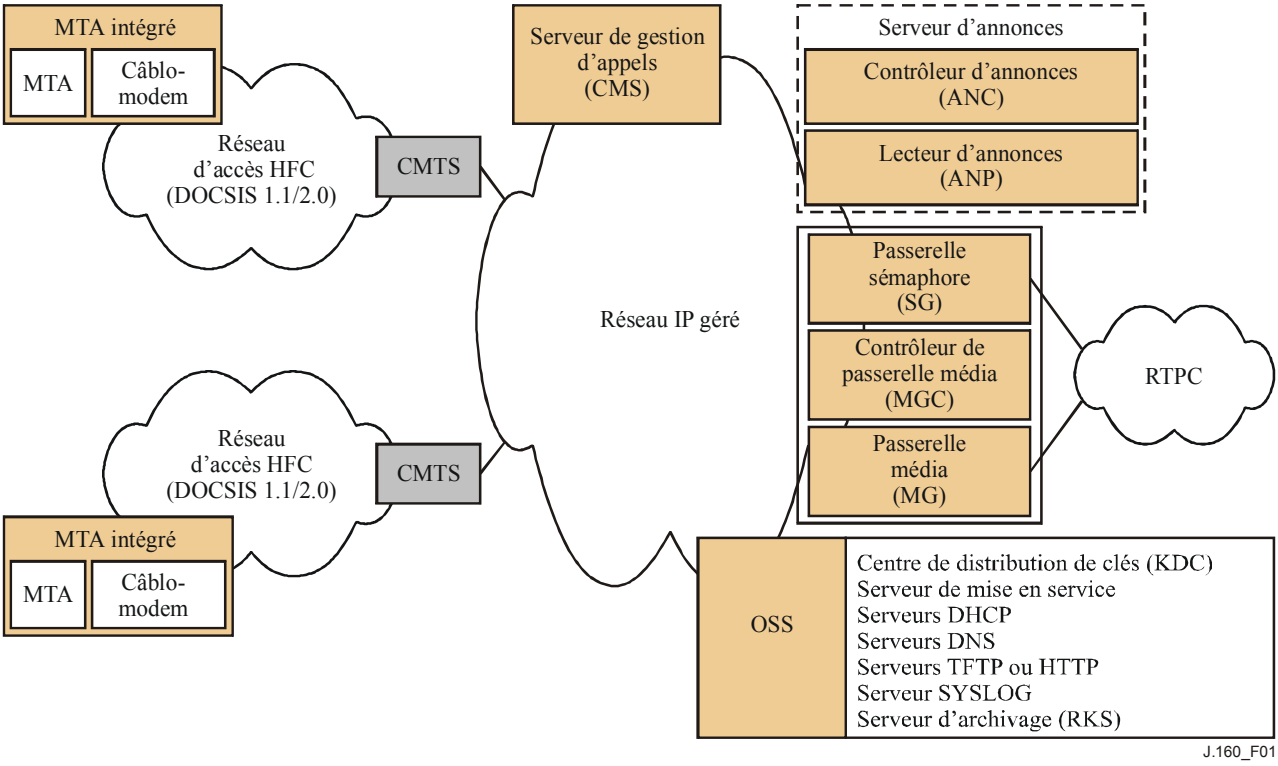


Figure 1/J.160 – Architecture de référence IPCablecom

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 DOCSIS, qui sont gérés par un même serveur CMS, comme indiqué sur la Figure 2. Les interfaces entre composants fonctionnels dans une même zone et les interfaces entre zones (par exemple CMS ↔ CMS) sont définies dans les Recommandations IPCablecom.

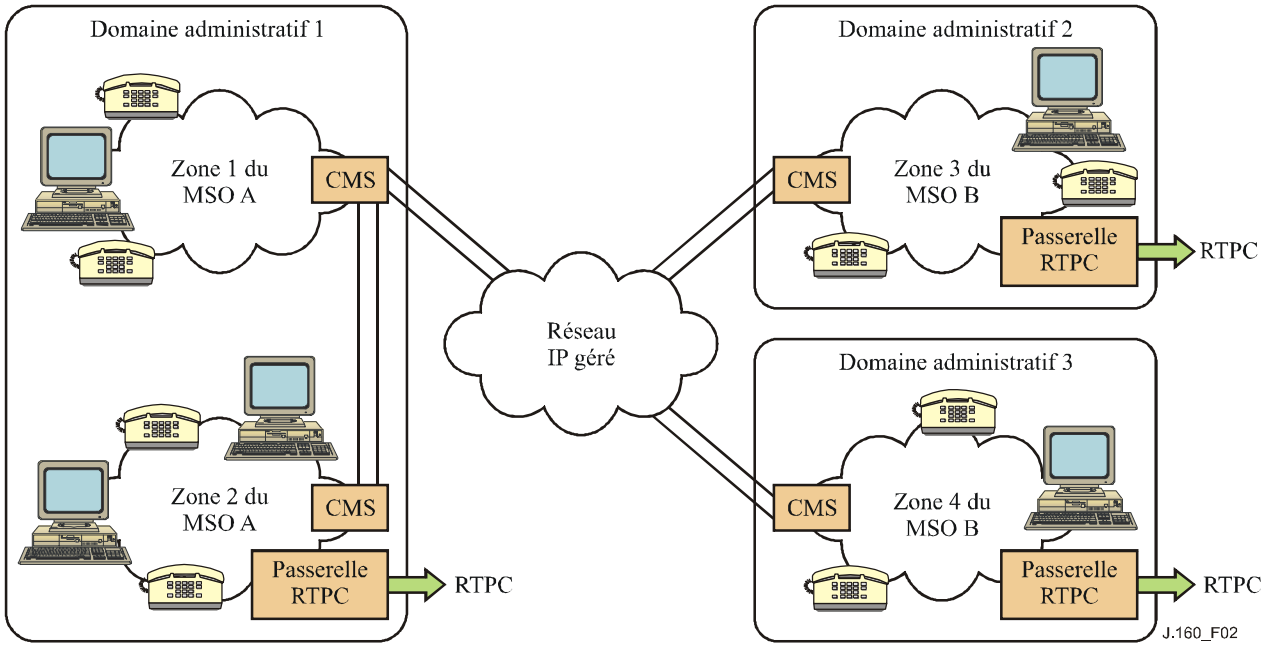


Figure 2/J.160 – Zones et domaines administratifs

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.

5.3 Recommandations IPCablecom

Tableau 1/J.160 – Recommandations IPCablecom

J.160	Cadre architectural pour l'acheminement de services à temps critique sur des réseaux de télévision par câble utilisant des câblo-modems
J.161	Caractéristiques des codecs audio destinés au service audio bidirectionnel sur les réseaux de télévision par câble utilisant des câblo-modems
J.162	Protocole réseau de signalisation d'appel pour la fourniture de services à temps critique sur les réseaux de télévision par câble utilisant des câblo-modems
J.163	Qualité de service dynamique pour la fourniture de services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems
J.164	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
J.165	Protocole de transport de signalisation Internet IPCablecom
J.166	Structure des bases d'informations de gestion (MIB) IPCablecom
J.167	Prescriptions pour la mise en service des adaptateurs de terminal de média pour la fourniture de services en temps réel sur les réseaux de télévision par câble au moyen de câblo-modems
J.168	Non utilisée – l'ancienne Rec. J.168 a été transformée en Annexe E/166

Tableau 1/J.160 – Recommandations IPCablecom

J.169	Non utilisée – l'ancienne Rec. J.169 a été transformée en Annexe C/166
J.170	Spécification de la sécurité sur IPCablecom
J.171.1	Protocole de commande de passerelle de jonction (TGCP) du système IPCablecom: profil 1
J.171.2	Protocole de commande de passerelle de jonction (TGCP) du système IPCablecom: profil 2
J.172	Mécanisme d'événement de gestion IPCablecom
J.173	Prise en charge du service de ligne principal par un adaptateur MTA IPCablecom intégré
J.174	Qualité de service interdomaniale IPCablecom
J.175	Protocole de serveur audio
J.176	Non utilisée – l'ancienne Rec. J.176 a été transformée en Annexe D/166
J.177	Spécification de la fourniture de service à l'abonné par le serveur de gestion d'appels IPCablecom
J.178	Signalisation entre serveurs de gestion d'appel IPCablecom
J.179	Prise en charge du multimédia par IPCablecom

5.4 Considérations relatives à la conception de l'architecture IPCablecom

Pour que l'infrastructure de réseau câblé puisse prendre en charge des communications multimédias en temps réel, les Recommandations IPCablecom définissent des protocoles dans les domaines suivants:

– signalisation d'appel;
– qualité de service;
– transport et codage de flux de média;
– mise en service des dispositifs;
– échange de messages d'événement;
– sécurité;
– surveillance électronique;
– systèmes d'assistance à l'exploitation.

Le présent paragraphe donne un aperçu général des objectifs et concepts de haut niveau qui ont servi à élaborer les Recommandations définissant l'architecture IPCablecom de référence. Il convient de consulter les différentes Recommandations IPCablecom pour obtenir les caractéristiques détaillées des protocoles pour chacun de ces domaines.

5.4.1 Objectifs architecturaux généraux

- Possibilité de capacités de qualité vocale analogues 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 réseau dorsal IP) sera inférieur à 45 ms.
- 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 fabricants 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 sera inférieure à 1% pendant l'heure la plus chargée de la journée (HDBH, *high day busy hour*).
- Assurance que le nombre de coupures de communication et de dérangements téléphoniques sera inférieur à 1 pour 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 la fréquence des glissements de trames dus à des horloges d'échantillonnage non synchronisées ou à des pertes de paquets sera inférieur à 0,25/min de signalisation d'appel.

5.4.2 Signalisation d'appel

- Définition d'une architecture de signalisation fondée sur le réseau.
- Fourniture 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 au réseau câblé;
  - appels provenant du réseau câblé et aboutissant au RTPC;
  - appels traversant des zones (intradomaine) ou des domaines (interdomaines).
- Fourniture 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'une signalisation compatible avec les normes de téléphonie IP existantes pour usage dans un réseau IPCablecom de câblo-opérateur 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 un abonnement préalable 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).

5.4.3 Qualité de service

- Offre d'un riche ensemble 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 IPCablecom.
- Réduction au minimum et prévention d'une utilisation abusive de la QS, y compris les attaques par vol de service et par déni de service. Garantie que la politique de QS est fixée et appliquée par des éléments de réseaux IPCablecom de confiance.
- Offre d'un mécanisme de priorités pour les services d'urgence et pour les autres services de signalisation fondés sur les priorités.

5.4.4 Codecs et flux médias

- Réduction au minimum des effets du temps de transmission, de la perte de paquets et de la gigue sur la qualité vocale dans l'environnement de téléphonie IP.
- Définition d'un ensemble minimal de codecs audio qui doivent toujours être pris en charge par tous les dispositifs d'extrémité (MTA et MG) 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 transparentes et sans erreur des fréquences DTMF par transmission dans la bande et relais de fréquences DTMF.
- Prise en charge de dispositifs terminaux pour les sourds et malentendants.
- Offre de mécanismes de commutation du codec lorsque des services de télécopie et de modem sont requis.
- Prise en charge d'un relais de télécopie pour la transmission fiable de télécopies sur les réseaux IP.
- Prise en charge du calcul de paramètres de téléphonie IP et de la communication de ces paramètres calculés afin de contrôler la qualité vocale.

5.4.5 Mise en service de dispositifs et système OSS

- Prise en charge de la mise en service dynamique ou statique des équipements des locaux client (MTA et CM).
- Absence de nécessité de réinitialiser les adaptateurs MTA lors de modifications générales 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 modules MIB de gestion de l'équipement des locaux client (MTA) au moyen du protocole simple de gestion de réseau (SNMP) de l'IETF.

5.4.6 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 du câblo-opérateur contre diverses attaques par refus de service, interruption du réseau et vol de service.
- Mise en œuvre d'aspects incluant la confidentialité, l'authentification, l'intégrité et le contrôle d'accès.

5.4.7 Surveillance électronique

- Prise en charge de la capacité d'opérer une surveillance électronique grâce à la communication des données d'appel et du contenu des appels.

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.

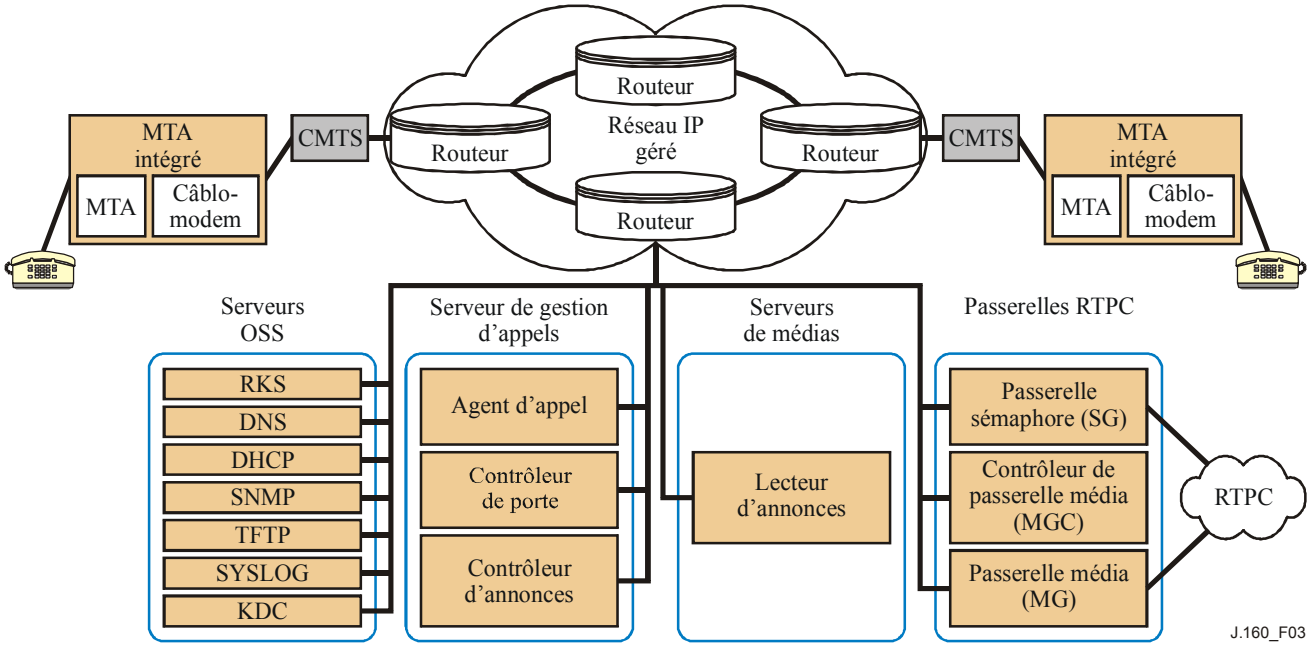


Figure 3/J.160 – Modèle de référence des composants IPCablecom

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 câblo-opérateur. 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 du câblo-opérateur.

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 (Rec. UIT-T 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*) (Rec. UIT-T J.162).

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.

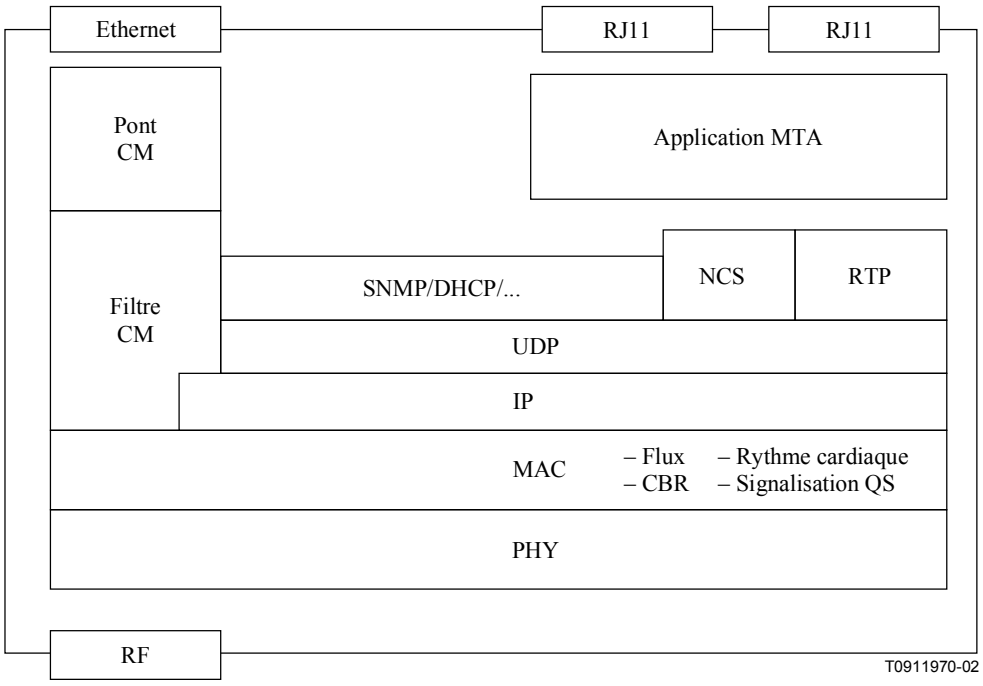


Figure 4/J.160 – Architecture fonctionnelle conceptuelle de l'adaptateur MTA intégré

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 système CMTS;
- 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 DOCSIS;

- 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 et codecs à faible débit;
- une ou plusieurs interfaces analogiques et/ou BRI du RNIS.

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

6.1.2 Attributs d'adaptateur MTA

Les attributs suivants caractérisent les adaptateurs E-MTA:

- un adaptateur MTA intégré possède deux adresses MAC: l'une pour le câblo-modem, l'autre pour l'adaptateur MTA;
- un adaptateur MTA intégré possède deux adresses IP: l'une pour le câblo-modem, l'autre pour l'adaptateur MTA;
- un adaptateur MTA intégré 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 port 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 DOCSIS. 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 système CMTS et des couches d'accès MAC et PHY DOCSIS.

6.4 Système de terminaison de câblo-modem (CMTS)

Le système CMTS 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 étendus. Le système CMTS est situé dans la tête du réseau de télévision par câble ou dans le concentrateur-répartiteur.

Le système CMTS est chargé des fonctions suivantes:

- assurer au câblo-modem la QS requise sur la base des demandes DOCSIS validées;
- 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 DOCSIS avec la QS assignée;
- renvoi des paquets amont aux dispositifs du réseau dorsal avec la QS assignée;
- conversion des paramètres de porte QS en paramètres de QS DOCSIS;
- enregistrement du taux d'utilisation des ressources appel par appel au moyen de messages événementiels IPCablecom.

6.4.1 Porte CMTS

Le système CMTS est chargé d'attribuer et de programmer la largeur de bande amont et aval conformément aux demandes de l'adaptateur MTA et aux autorisations de QS établies par le contrôleur de porte.

Le système CMTS implémente une porte QS dynamique IPCablecom ou porte CMTS entre le réseau câblé DOCSIS et un réseau dorsal IP. La porte CMTS est un composant fonctionnel du système CMTS qui effectue la classification du trafic et qui met en œuvre la politique de QS dans les flux médias comme indiqué par le contrôleur de porte (GC, *gate controller*). La porte CMTS est commandée par le contrôleur de porte (GC), composant logique de gestion de QS implanté dans le serveur CMS, qui coordonne toutes les autorisations et commandes de qualité de service.

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 système CMTS et aux passerelles RTPC dans le réseau IPCablecom. Le serveur CMS est un élément de réseau de confiance qui réside dans la partie IP gérée du réseau IPCablecom.

Un serveur CMS du réseau IPCablecom comprend les composants logiques IPCablecom suivants:

– **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 (Rec. UIT-T J.162). A ce propos, les tâches de l'agent d'appel sont, entre autres, les suivantes:
  - implémentation des éléments de service;
  - 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;
  - contrôle de l'utilisation des paramètres vocaux par l'adaptateur MTA.
– **contrôleur de porte (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 contrôleur de porte est définie dans la Recommandation 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;

Le serveur CMS peut également remplir les fonctions suivantes:

- gestion d'appel et éléments de service améliorés;
- services d'annuaire et conversion d'adresse;
- routage d'appel;
- enregistrement du taux d'utilisation des services de portabilité de numéro local.

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 avec le RTPC, 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 SS7 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 transmet 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 tonalités d'essai de continuité pour jonctions de l'ISUP. Chaque jonction est représentée sous la forme d'un point d'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 communique 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 points d'extrémité situés dans la passerelle média:
  - la détection d'événement donne à la passerelle média l'ordre de détecter des événements, par exemple des tonalités dans la bande, concernant le point d'extrémité et éventuellement des connexions;

– la production de signaux donne à la passerelle média l'ordre de produire des tonalités et des signaux dans la bande concernant le point d'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 de points d'extrémité dans la passerelle média;

– la commande d'attribut donne à la passerelle média des consignes relatives aux attributs à appliquer à un point d'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 points d'extrémité;
- **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 les connexions supports entre le RTPC et le réseau IPCablecom. Chaque support est représenté par un point d'extrémité et le contrôleur MGC donne consigne à la passerelle média d'établir et de contrôler des connexions médias vers d'autres points d'extrémité 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;
- détecte les événements relatifs aux points d'extrémité et aux connexions selon les demandes du contrôleur MGC;
- produit des signaux relatifs aux points d'extrémité et aux connexions, par exemple des essais de continuité, selon les instructions du contrôleur MGC;
- crée, modifie et supprime les connexions à destination ou en provenance d'autres points d'extrémité, selon instructions du contrôleur MGC;
- commande et assigne des ressources internes de traitement média à des connexions spécifiques dès réception de demandes issues 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 de réseau.

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 SS7.

6.6.3.1 Fonctions de passerelle sémaphore SS7

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

- termine physiquement les canaux sémaphores SS7 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 SS7;
- termine les niveaux 1, 2 et 3 du sous-système transport de message (MTP, *message transfer part*);
- implémente les fonctions de gestion de réseau du sous-système MTP selon les besoins de tout point sémaphore du réseau SS7;
- 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 SS7, 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 SS7 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 SS7;
- implémente le protocole de transport requis pour transporter les informations de signalisation entre la passerelle sémaphore et le contrôleur MGC.

6.7 Composants du système OSS

Le système OSS contient des composants de gestion d'entreprise, de service et de réseau prenant en charge les processus d'entreprise 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.

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 l'échange de messages événementiels transportant des informations de facturation.

6.7.1 Serveur de sécurité – centre de distribution de clés (KDC, *key distribution center*)

Dans l'architecture IPCablecom, le terme "centre KDC" est utilisé pour désigner un serveur de sécurité Kerberos. On utilise le protocole Kerberos avec l'extension PKINIT de clé publique pour la gestion des clés aux interfaces entre l'adaptateur MTA d'une part et le serveur CMS et le serveur de mise en service d'autre part.

Après l'authentification de l'adaptateur MTA au moyen du protocole PKINIT, le centre KDC accorde des tickets Kerberos à l'adaptateur MTA. Chaque ticket contient les informations servant à configurer la sécurité pour la signalisation d'appel entre l'adaptateur MTA et le serveur CMS (si l'adaptateur MTA doit communiquer avec le serveur CMS par le biais d'une interface sécurisée) et pour l'interface de gestion entre l'adaptateur MTA et le serveur de mise en service (si l'adaptateur MTA doit être géré par le biais d'une interface sécurisée). Un ticket est émis:

- au cours de la mise en service du dispositif. Si l'adaptateur MTA est réinitialisé et qu'un ticket sauvegardé est encore valide, l'adaptateur MTA n'aura pas besoin d'exécuter l'échange PKINIT pour demander un nouveau ticket au centre KDC;

- lorsqu'un ticket arrive à expiration. En fonctionnement normal, les tickets expirent approximativement au bout d'une semaine.

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

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

6.7.5 Serveur SYSLOG (SYSLOG)

Elément de réseau facultatif du système OSS utilisé pour collecter les messages de notification d'événement indiquant que des événements tels que des erreurs au niveau de dispositifs se sont produits.

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

Elément de réseau de confiance qui reçoit les messages événementiels IPCablecom en provenance d'autres éléments de réseau IPCablecom de confiance, comme le serveur CMS, le système CMTS 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 ou corréler dans des ensembles cohérents ou dans des journaux détaillés des communications (CDR, *call detail record*) qui sont ensuite mis à la disposition d'autres fonctions du système OSS comme la facturation ou la détection des fraudes.

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 lecteur 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 lecteur 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 Lecteur 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 lecteur 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 convient de consulter chaque Recommandation 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 2 suivant.

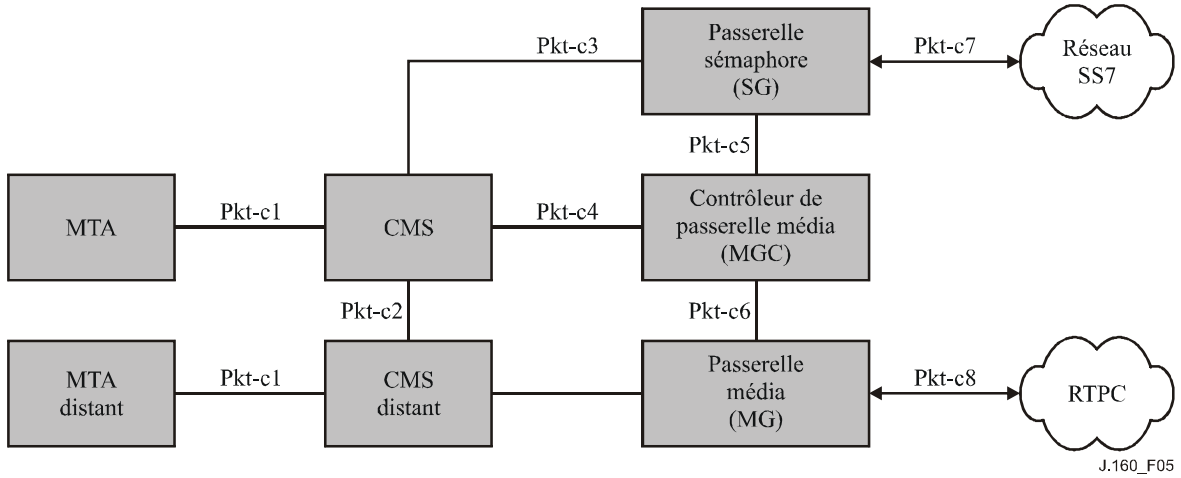


Figure 5/J.160 – Interfaces de signalisation d'appel

Tableau 2/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. A cette interface, on utilise le protocole de signalisation CMSS (Rec. UIT-T J.178).
Pkt-c3	CMS ↔ SG	Messages de signalisation d'appel échangés entre le serveur CMS et la passerelle sémaphore.
Pkt-c4	CMS ↔ MGC	Messages de signalisation d'appel échangés entre le serveur CMS et le contrôleur MGC. A cette interface, on utilise le protocole de signalisation CMSS.
Pkt-c5	SG ↔ MGC	Messages de signalisation d'appel échangés entre le contrôleur MGC et la passerelle sémaphore.

Tableau 2/J.160 – Interfaces de signalisation d'appel

Interface	Composants fonctionnels IPCablecom	Description
Pkt-c6	MGC ↔ MG	Interface de commande de la passerelle média au moyen du protocole TGCP, qui est un profil du MGCP, semblable au protocole de signalisation NCS.
Pkt-c7	SG ↔ SS7	La passerelle sémaphore termine les canaux sémaphores SS7 physiques issus du RTPC (canaux A, F). Les protocoles suivants sont pris en charge: • interface utilisateur ISUP: offre une interface de signalisation SS7 ISUP aux exploitants de RTPC extérieurs; • interface utilisateur TCAP: offre un mécanisme pour certaines entités de confiance ("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 SS7.
Pkt-c8	MG ↔ RTPC	Cette interface définit la connexité des canaux supports allant de la passerelle média au RTPC.

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 du point d'extrémité distant, 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 2 (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 dans la bande 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 (Rec. UIT-T J.171) (Pkt-c6), ce qui inclut la création, la modification et la suppression de connexions. 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 SS7, 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 SS7 du RTPC pour la gestion et la commande des jonctions.

7.1.3 Cadre de signalisation entre serveurs CMS

L'architecture IPCablecom prend en charge la signalisation CMS-CMS et CMS-MGC interdomaines et intradomaine comme défini dans la Recommandation relative à la signalisation CMSS (Rec. UIT-T J.178). L'architecture de signalisation CMSS est fondée sur le protocole d'ouverture de session (SIP) de l'IETF (IETF RFC 3261). La signalisation CMSS définit un protocole de signalisation d'appel. Elle ne porte pas sur le routage dans le réseau.

Un serveur CMS contient un client d'agent d'utilisateur (UAC, *user agent client*) et un serveur d'agent d'utilisateur (UAS, *user agent server*) SIP. L'agent d'utilisateur maintient l'état d'appel pendant la durée de vie de l'appel et surveille l'adaptateur MTA concernant les changements d'état qui ont une incidence sur l'appel. L'interface entre le serveur CMS et l'adaptateur MTA est assurée au moyen de la signalisation NCS. Les messages de signalisation CMSS destinés à l'établissement d'un nouvel appel ou à la modification des attributs ou des participants pour un appel actif, sont lancés par le serveur CMS. Celui-ci est généralement amené à lancer de tels messages par suite d'une signalisation issue de l'adaptateur MTA, par exemple par suite de la réception d'un message NCS l'informant des chiffres composés. Un serveur CMS inclut une fonction de contrôleur de porte (GC). La partie agent d'utilisateur du serveur CMS participe à la signalisation CMSS et la partie contrôleur de porte participe à la signalisation DQoS. Ensemble, elles assurent la coordination de la signalisation pour l'établissement d'appel et la gestion des ressources.

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.

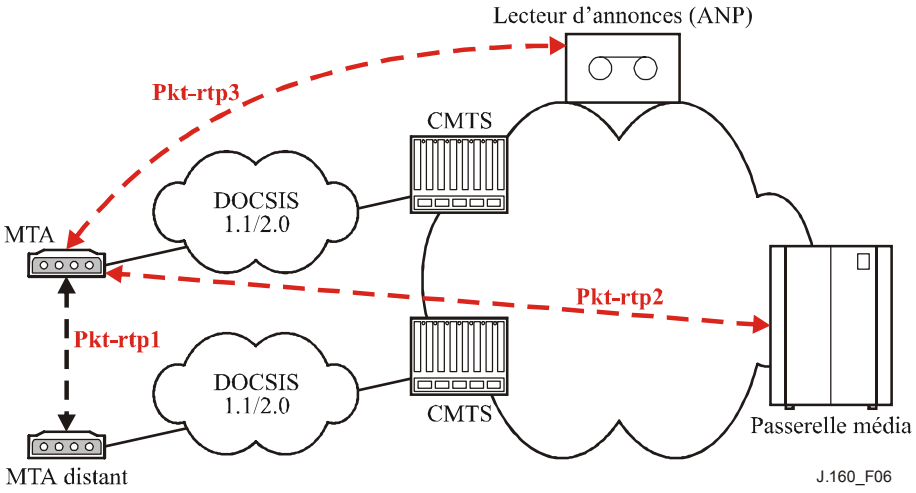


Figure 6/J.160 – Flux médias RTP dans un réseau IPCablecom

Tableau 3/J.160 – Flux médias RTP

Interface	Composants fonctionnels IPCablecom	Description
pkt-rtp1	MTA ↔ MTA	Flux média entre adaptateurs MTA, comprenant par exemple des signaux codés de voix et télécopie.
pkt-rtp2	MTA ↔ MG	Flux média entre la passerelle média et l'adaptateur MTA, comprenant par exemple des tonalités, des annonces et un flux média RTPC.
pkt-rtp3	MTA ↔ ANP	Flux média entre le lecteur ANP et l'adaptateur MTA, comprenant par exemple des tonalités et des annonces envoyées à l'adaptateur MTA par le lecteur d'annonces.

Le protocole RTP code une seule voie d'informations multimédias dans un seul sens. Dans chaque en-tête RTP, un "type de charge utile" (PT) de 7 bits indique l'algorithme de codage (par exemple G.711) qui est utilisé dans le paquet de charge utile. Pour la plupart des algorithmes audio courants, une valeur de type de charge utile comprise entre 0 et 95 est attribuée. L'intervalle de 96 à 127 est réservé aux types de charge utile RTP "dynamique" pour lesquels le lien entre l'algorithme de codage et le type de charge utile est établi par le biais de la signalisation.

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

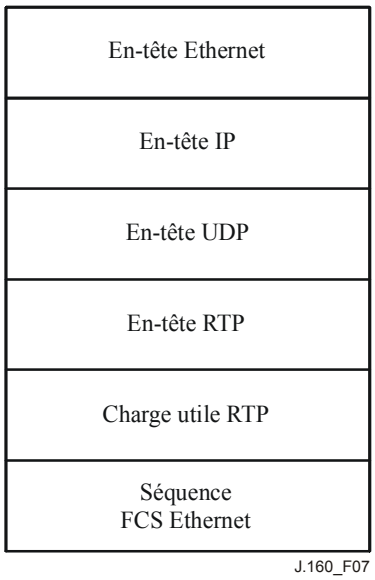


Figure 7/J.160 – Format de paquet RTP

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

Les sessions RTP sont établies dynamiquement par les points d'extrémité impliqués de sorte qu'aucun numéro de port UDP "bien connu" n'est utilisé pour recevoir les informations RTP. 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 le port UDP particulier utilisés par une session RTP particulière. Le protocole SDP est utilisé à la fois par le protocole NCS et par le protocole TGCP.

Les en-têtes de paquet Ethernet, IP, UDP et RTP sont importants par rapport à une longueur normale de charge utile RTP, qui peut se réduire à 10 octets pour des signaux vocaux paquetés. Les Recommandations DOCSIS règlent ce problème au moyen d'une fonction de suppression d'en-tête de charge utile afin d'abréger les en-têtes communs.

La Rec. UIT-T T.38 est également utilisée pour transporter des médias de télécopie dans les réseaux IPCablecom (voir le § 8.7 pour plus de détails).

7.2.1 Protocole de commande de transport en temps réel (RTCP)

Le protocole RTCP est défini dans la norme IETF RFC 1889. Il est fondé sur la transmission périodique de paquets de commande à tous les participants de la session considérée, au moyen du même mécanisme de distribution que celui utilisé pour les paquets de données. Le protocole RTCP donne des indications sur la qualité de la distribution des données. Il fait partie intégrante du rôle du protocole RTP en tant que protocole de transport et est lié aux fonctions de commande de flux et de gestion des encombrements des autres protocoles de transport. L'architecture IPCablecom prend en charge l'utilisation du protocole RTCP à tous les points d'extrémités.

Il existe des extensions au protocole RTCP permettant de mieux évaluer la qualité d'une communication vocale et de diagnostiquer plus efficacement les problèmes sur le réseau. Ces extensions sont appelées rapports étendus RTCP (XR RTCP) et sont définies dans le document IETF RFC 3611. Les rapports étendus RTCP contiennent de nombreux ensembles de paramètres. L'architecture IPCablecom prend uniquement en charge les paramètres vocaux des rapports étendus RTCP à tous les points d'extrémité.

7.3 Mise en service d'un adaptateur MTA

La mise en service d'un adaptateur MTA permet à un adaptateur MTA de s'enregistrer auprès du réseau de l'opérateur et de fournir 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 Recommandation relative à la mise en service comporte également les définitions d'attribut requises dans le fichier de configuration de l'adaptateur MTA. (Voir Figure 8.)

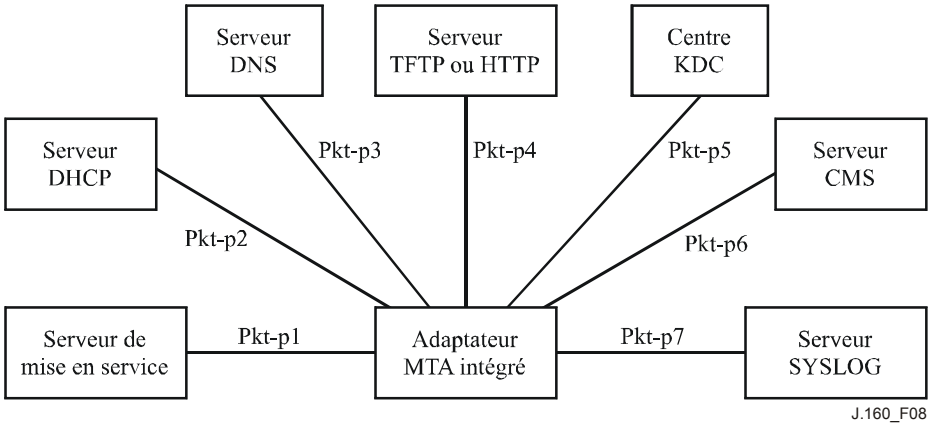


Figure 8/J.160 – Interfaces de mise en service IPCablecom

Le Tableau 4 décrit les interfaces de mise en service indiquées dans la Figure 8.

Tableau 4/J.160 – Interfaces de mise en service de dispositifs

Interface	Composants fonctionnels IPCablecom	Description
Pkt-p1	MTA ↔ Serveur de mise en service	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 points d'extrémité. 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	MTA ↔ Serveur DHCP	Interface DHCP entre l'adaptateur MTA et le serveur DHCP, utilisée pour attribuer une adresse IP à l'adaptateur MTA et pour fournir d'autres informations de bas niveau utilisées par l'adaptateur MTA lors de son rattachement au réseau.
Pkt-p3	MTA ↔ Serveur 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	MTA ↔ Serveur HTTP ou TFTP	L'adaptateur MTA téléimporte son fichier de configuration à partir du serveur TFTP ou HTTP.

Tableau 4/J.160 – Interfaces de mise en service de dispositifs

Interface	Composants fonctionnels IPCablecom	Description
Pkt-p5	MTA ↔ KDC	L'adaptateur MTA obtient un ticket Kerberos auprès du centre de distribution de clés (KDC) au moyen du protocole Kerberos.
Pkt-p6	MTA ↔ CMS	L'adaptateur MTA établit une association de sécurité IPsec avec le serveur CMS au moyen du protocole Kerberos.
Pkt-p7	MTA ↔ SYSLOG	Interface utilisée par l'adaptateur MTA pour envoyer des notifications d'événement de réseau au serveur SYSLOG, y compris des informations liées au statut de la mise en service de dispositif.

7.4 Interfaces avec la couche de gestion d'éléments SNMP

Pour la mise en service des adaptateurs MTA, l'architecture IPCablecom nécessite que le protocole SNMP assure l'interface entre ces adaptateurs MTA et les systèmes de gestion d'élément. Les messages "traps" et "informs" de la version 3 du protocole SNMP sont pris en charge pour le traitement des événements, ainsi que les messages "sets" et "gets" pour la mise en service. 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 que point d'extrémité par point d'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. On trouvera dans la Recommandation relative à la structure des bases d'informations de gestion (MIB) IPCablecom (Rec. UIT-T J.166) des informations plus détaillées sur ces bases MIB.

7.5 Interfaces liées aux 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 serveur d'archivage (RKS), les informations contenues dans plusieurs messages événementiels offrent un enregistrement complet du service rendu dans le cadre d'un appel. Cet enregistrement 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 de systèmes OSS comme un système de facturation, un système de détection de fraude ou un processeur de services prépayés.

La Recommandation relative aux messages événementiels IPCablecom (Rec. UIT-T J.164) définit la structure de la fiche de message événementiel et définit son protocole de transport (RADIUS). Le format de la fiche de message événementiel est conçu 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. La Figure 9 montre une architecture représentative des messages événementiels.

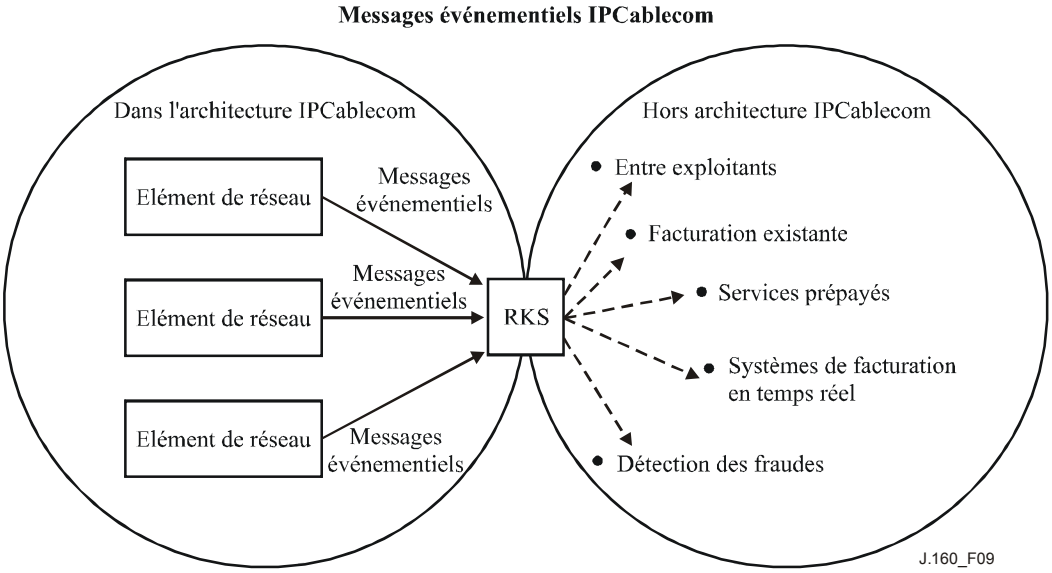
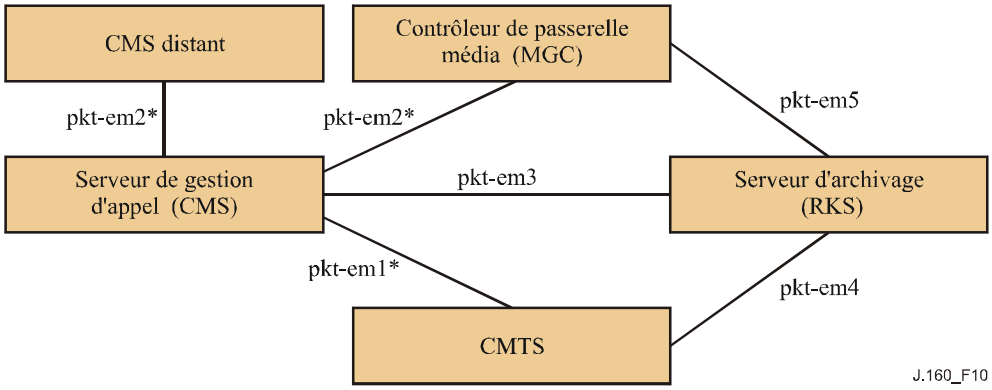


Figure 9/J.160 – Architecture représentative des messages événementiels

Le Tableau 5 décrit les interfaces liées aux messages événementiels représentées sur la Figure 10.

Tableau 5/J.160 – Interfaces liées aux messages événementiels

Interface	Composant fonctionnel IPCablecom	Description
Pkt-em1	CMS ↔ CMTS	Message Gate-Set DQoS acheminant l'identificateur de corrélation avec la facturation et d'autres données requises par le système CMTS afin d'envoyer des messages événementiels à un serveur RKS.
Pkt-em2	CMS ↔ MGC CMS ↔ CMS	A cette interface, on utilise le protocole de signalisation CMSS, qui est utilisé pour acheminer un identificateur de corrélation avec la facturation ainsi que d'autres données requises pour la facturation.
Pkt-em3	CMS ↔ RKS	Protocole RADIUS pour le transport des messages événementiels IPCablecom.
Pkt-em4	CMTS ↔ RKS	Protocole RADIUS pour le transport des messages événementiels IPCablecom.
Pkt-em5	MGC ↔ RKS	Protocole RADIUS pour le transport des messages événementiels IPCablecom.



NOTE – * Indique que l'interface de signalisation existante est utilisée pour transporter les données utilisées pour d'autres interfaces liées aux messages événementiels.

Figure 10/J.160 – Interfaces liées aux messages événementiels

7.6 Qualité de service (QS)

7.6.1 Cadre de QS

Le cadre de QS IPCablecom est représenté sur la Figure 11:

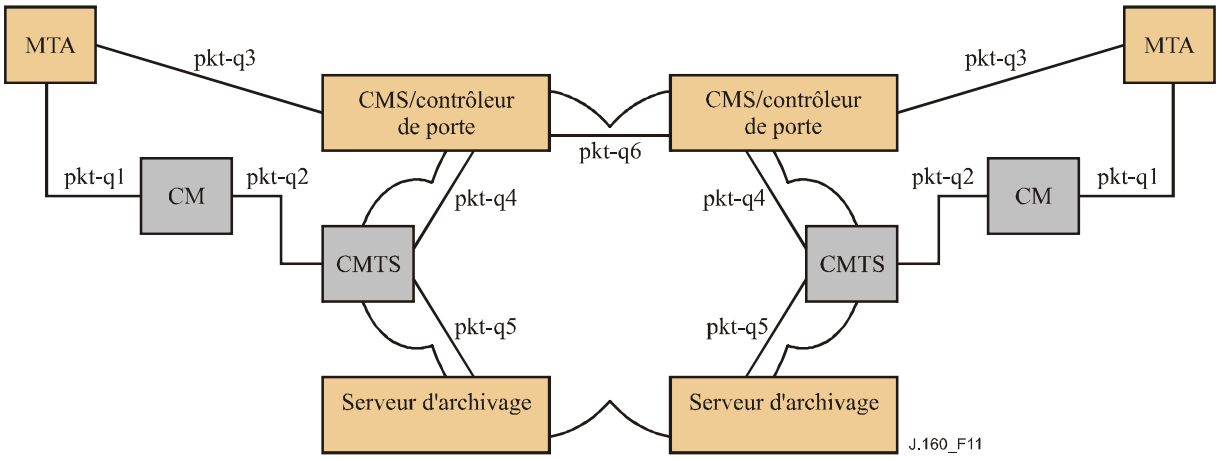


Figure 11/J.160 – Interfaces de signalisation de QS dans l'architecture IPCablecom

Le Tableau 6 décrit brièvement chaque interface et la façon dont elle est utilisée dans la Recommandation relative à la QS dynamique (DQoS, *dynamic QoS*, Rec. UIT-T J.163).

Tableau 6/J.160 – Interfaces liées à la QS

Interface	Composant fonctionnel IPCablecom	Description D-QoS
Pkt-q1	MTA ↔ CM	Interface de service de commande MAC pour E-MTA
Pkt-q2	CM ↔ CMTS	J.112, à l'initiative du CM
Pkt-q3	MTA ↔ CMS	NCS
Pkt-q4	GC ↔ CMTS	Gestion de porte
Pkt-q5	CMTS ↔ RKS	Facturation
Pkt-q6	CMS ↔ CMS	Etablissement de session

La fonction de chaque interface de QS est décrite plus en détail dans le Tableau 7.

Tableau 7/J.160 – Interfaces liées à la QS

Interface	Composant fonctionnel IPCablecom	Description
Pkt-q1	MTA ↔ CM	Cette interface se décompose en trois sous-interfaces comme suit: *commande:* sous-interface utilisée pour gérer des flux de service DOCSIS 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.
Pkt-q2	CM ↔ CMTS	Il s'agit de l'interface de QS DOCSIS (commande, planification et transport). Il convient de noter que, sur le plan de l'architecture, les fonctions de commande peuvent être lancées uniquement par le câblo-modem. Le système CMTS est l'arbitre ultime de la politique et le décideur d'admission dans le réseau d'accès DOCSIS. Les capacités suivantes de la commande MAC DOCSIS 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 DOCSIS; • classification priorisée des flux de trafic en fonction des flux de service; • service de planification de débit minimal/constant garanti;

Tableau 7/J.160 – Interfaces liées à la QS

Interface	Composant fonctionnel IPCablecom	Description
		• 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 DOCSIS pour augmenter la densité d'appels; • classification DOCSIS des flux vocaux en fonction du flux de service; • synchronisation DOCSIS de l'horloge entre CODEC et système CMTS ainsi que de l'intervalle de distribution; • activation en deux phases des ressources de QS; • marquage des paquets TOS dans la couche Réseau; • garantie de temps de propagation et de gigue; • signalisation de sous-couche interne entre l'adaptateur MTA IPCablecom et le câblo-modem (adaptateur MTA intégré); Cette interface est définie plus en détail dans la Rec. UIT-T J.112.
Pkt-q3	MTA ↔ CMS	Interface de signalisation entre l'adaptateur MTA et le serveur CMS. De nombreux paramètres sont signalés de part et d'autre de cette interface, comme les flux médias, les adresses IP, les numéros de port, la sélection de codec et la paquétisation.
Pkt-q4	CMS ↔ CMTS	Cette interface sert à gérer les portes dynamiques pour les sessions de flux média. Cette interface permet au réseau IPCablecom de demander et d'autoriser une certaine QS.
Pkt-q5	CMTS ↔ RKS	Cette interface est utilisée par le système CMTS pour signaler les modifications dans les ressources de QS utilisées par un appel. Elle est définie dans la Recommandation relative aux messages événementiels.
Pkt-q6	CMS ↔ CMS	Cette interface est utilisée pour établir des sessions intradomaine et des sessions interdomaines. Elle inclut une fonctionnalité permettant de garantir que des ressources de QS sont disponibles aux deux extrémités de la connexion avant que l'appel ne soit autorisé à aboutir.

7.6.2 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.

L'entité logique qui définit, à l'intérieur du système CMTS, la classification du trafic et la politique de QS relative aux flux médias est appelée "porte". L'élément de contrôleur de porte du serveur CMS gère les portes pour les flux médias IPCablecom. Les informations clés suivantes sont incluses dans la signalisation entre le contrôleur de porte (GC) et le système CMTS:

enveloppe de QS maximale autorisée – l'enveloppe de QS maximale autorisée définit la ressource de QS maximale (par exemple, "2 attributions de 160 octets toutes les 10 ms") que l'adaptateur MTA est autorisé à demander 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 points d'extrémité de flux média – le GC/CMS autorise les parties qui sont impliquées dans un flux support de média. Au moyen de ces informations, le système CMTS peut régler le flux de données de façon que l'origine et la destination de ce flux correspondent aux parties qui sont autorisées;

destination des informations de facturation – le GC/CMS communique au système CMTS l'identité des serveurs d'archivage primaire et secondaire pour l'appel et fournit un identificateur de facturation unique pour pouvoir corréler les enregistrements dans plusieurs éléments de réseau;

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

serveur de gestion d'appels/contrôleur de porte – le 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. Le CMS/GC utilise également la signalisation CMSS pour garantir que des ressources de QS sont disponibles aux deux extrémités d'un appel dans le cas d'un appel intradomaine ou interdomaines.

système CMTS – au moyen des informations fournies par le CMS/GC, le système CMTS applique un contrôle d'admission aux demandes de QS puis règle le flux de données admis de façon que l'origine et la destination de ce flux correspondent aux parties qui ont été autorisées en tant que points d'extrémité du flux. Le système CMTS interagit avec la partie câblo-modem de l'adaptateur MTA et avec le serveur RKS. Les tâches du système CMTS par rapport à chacun de ces éléments sont les suivantes:

- **système CMTS par rapport au serveur RKS** – le système CMTS envoie une notification au serveur d'archivage (RKS) chaque fois que la QS est modifiée entre le système CMTS et l'adaptateur MTA pour un appel donné;
- **système CMTS par rapport à l'adaptateur MTA** – l'adaptateur MTA formule dynamiquement des demandes de création ou de modification des paramètres de trafic QS associés aux flux de service dynamiques DOCSIS qui acheminent le trafic support. Lorsque le système CMTS reçoit une demande, il vérifie si les caractéristiques demandées sont contenues dans l'enveloppe de QS autorisée et si les points d'extrémité des flux médias sont autorisés à acheminer ce trafic. Si le résultat de la vérification est positif, le système CMTS crée ou modifie le flux de service dynamique en conséquence;

serveur d'archivage (RKS) – le serveur RKS reçoit chaque événement (sous la forme de message événementiel) envoyé par le système CMTS. Il présente généralement une interface avec un ou plusieurs composants du système OSS et reformatte et retransmet les informations reçues du système CMTS à ces composants;

adaptateur MTA – l'adaptateur MTA est l'entité à laquelle l'accord sur le niveau de service (SLA) est offert par le système CMTS. L'adaptateur MTA est chargé de l'emploi approprié de la liaison de QS (et le système CMTS est chargé de faire en sorte que cet emploi soit approprié, étant donné que l'adaptateur MTA n'est pas un dispositif de confiance). Si l'adaptateur MTA tente de dépasser l'enveloppe de trafic autorisée par l'accord SLA, le système CMTS fait en sorte que l'adaptateur MTA ne reçoive pas la QS excédentaire qu'il a demandée.

7.7 Mise en service du serveur CMS pour l'abonné

La Recommandation relative à la mise en service du serveur CMS pour l'abonné permet d'activer automatiquement le service par la définition d'une interface entre le serveur de mise en service (ou un composant autorisé du système OSS) et le serveur CMS. Le cadre applicable à la mise en service du serveur CMS pour l'abonné est représenté sur la Figure 12.

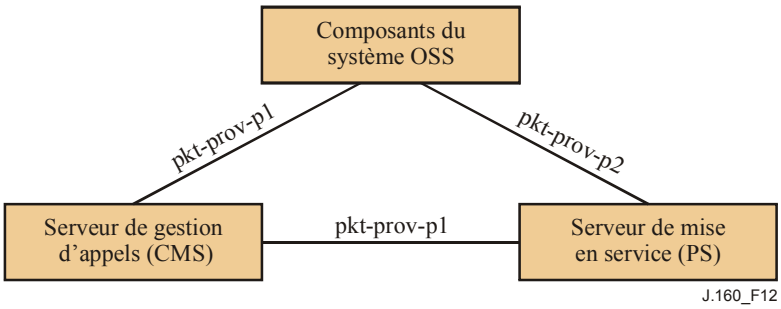


Figure 12/J.160 – Interfaces relatives à la mise en service du serveur CMS pour l'abonné

La fonction de chacune de ces interfaces est décrite en détail dans le Tableau 8.

Tableau 8/J.160 – Interfaces relatives à la mise en service du serveur CMS par l'abonné

Interface	Composants fonctionnels	Description
pkt-prov-p1	PS-CMS Composant du système OSS-CMS	Il s'agit de l'interface relative à la mise en service du serveur CMS pour l'abonné. Les informations concernant l'abonné peuvent être transmises au serveur CMS par le serveur de mise en service ou par un composant autorisé du système OSS.
pkt-prov-p2	Composant du système OSS-PS	Cette interface permet aux composants du système OSS d'échanger des informations avec le serveur de mise en service. Cette interface n'est pas définie dans l'architecture IPCablecom.

La mise en service pour l'abonné comprend les opérations suivantes:

- **Prise en charge d'un enregistrement de l'abonné et de la facturation** – Etablissement d'un enregistrement de l'abonné contenant les informations nécessaires à la fourniture du service, à la facturation et à la collecte du paiement pour cet abonné. La création d'un enregistrement de l'abonné et la facturation sont considérées comme faisant partie du système OSS et sont actuellement hors du domaine d'application de l'architecture IPCablecom.
- **Etablissement et configuration des équipements** – Cela peut comprendre l'installation physique et/ou le raccordement des équipements ainsi que les éventuelles mises à jour de logiciels et/ou de bases de données nécessaires pour fournir effectivement le service à l'abonné. En ce qui concerne l'interface relative à la mise en service du serveur CMS pour l'abonné, l'établissement des équipements a une incidence sur le serveur CMS. La mise en service du serveur CMS proprement dit peut être subdivisée en deux:
  - **Mise en service relative au service téléphonique ordinaire de base (BPP)** – Cette mise en service permet de fournir au serveur CMS l'ensemble minimal de données nécessaires pour le routage du service téléphonique ordinaire (RTC) dans le réseau IPCablecom. Cet ensemble minimal de données comprend un numéro de téléphone mappé vers le nom FQDN de l'adaptateur MTA associé et l'identificateur de point

d'extrémité NCS. Ces données seront utilisées pour établir les tables de conversion qui permettront au serveur CMS de router les appels vers le dispositif/port approprié compte tenu d'un numéro de téléphone donné. La mise en service BPP pour chaque abonné est nécessaire avant que cet abonné puisse recevoir des appels dans un réseau IPCablecom.

– **Mise en service relative aux éléments de service (CFP)** – En plus de la mise en service BPP, la mise en service CFP est réalisée afin de fournir des éléments de service à un abonné. La mise en service CFP est plus compliquée que la mise en service BPP car les paramètres transmis peuvent varier d'un élément de service à l'autre et peuvent aussi dépendre des implémentations de chaque fabricant.

7.8 Surveillance électronique

Le cadre de surveillance électronique IPCablecom permet de procéder à une surveillance électronique autorisée légalement (LAES, *lawfully authorized electronic surveillance*) dans les réseaux IPCablecom. L'architecture IPCablecom prend en charge la remise des données et du contenu d'appels à des organismes d'application des lois (LEA, *law enforcement agency*). Les données et le contenu d'appels sont remis par différents composants du réseau à une fonction de remise (DF, *delivery function*), laquelle est chargée de regrouper ces données et ce contenu et de les remettre à l'organisme LEA approprié. L'organisme LEA comprend une fonction de collecte, chargée de recevoir les données et le contenu d'appels que lui envoie la fonction de remise.

L'architecture IPCablecom définit uniquement les mécanismes permettant de réaliser la surveillance électronique. Elle ne définit pas comment un ordre de surveillance électronique est géré (c'est-à-dire accepté par l'opérateur IPCablecom et mis en service dans le réseau).

Le cadre de surveillance électronique IPCablecom est représenté sur la Figure 13.

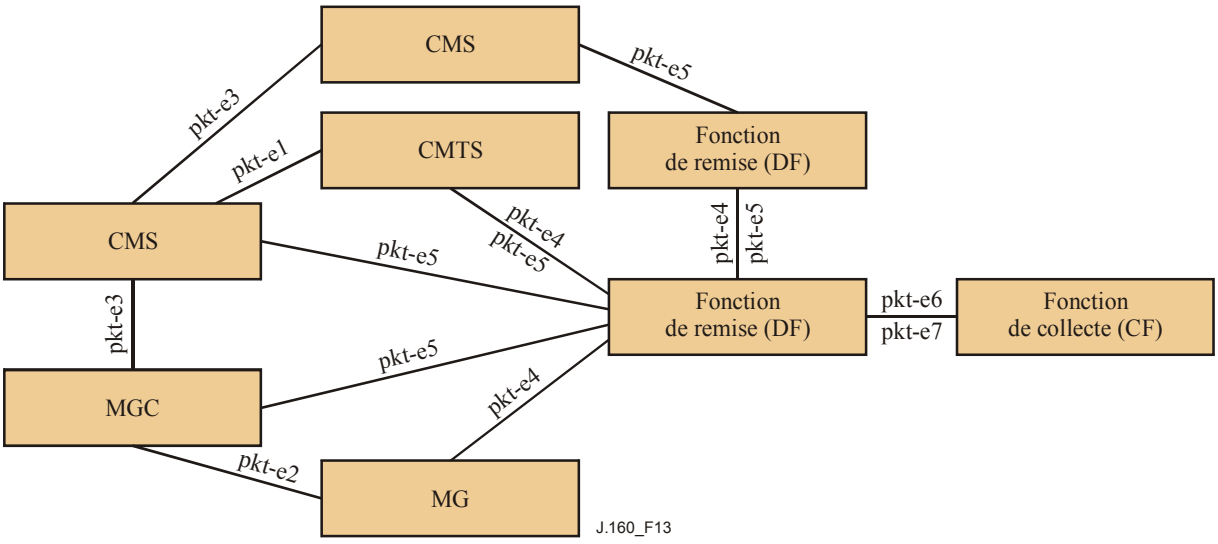


Figure 13/J.160 – Interfaces relatives à la surveillance électronique

La fonction de chacune de ces interfaces est décrite en détail dans le Tableau 9.

Tableau 9/J.160 – Interfaces relatives à la surveillance électronique

Interface	Composants fonctionnels IPCablecom	Description
pkt-e1	CMS ↔ CMTS	Interface DQoS COPS, permettant à un serveur CMS d'activer la surveillance des données et du contenu d'un appel.
pkt-e2	MGC ↔ MG	Interface TGCP, permettant à un contrôleur MGC de commander à la passerelle MG de réaliser une surveillance électronique.
pkt-e3	CMS ↔ CMS CMS ↔ MGC	Interface CMSS, prenant en charge la capacité de communiquer des besoins de surveillance électronique dans le cas de certains scénarios d'appel intradomaine ou interdomaines (par exemple, lorsqu'une certaine entité retransmet un appel).
pkt-e4	CMTS ↔ DF MG ↔ DF DF ↔ DF	Interface fondée sur l'échange de messages événementiels IPCablecom et utilisée pour la remise des données d'appels entre des composants IPCablecom et la fonction DF, ou entre la fonction DF et une autre fonction DF.
pkt-e5	CMTS ↔ DF MGC ↔ DF DF ↔ DF CMS ↔ DF	Interface utilisée pour la remise du contenu d'appels sous la forme de paquets RTP encapsulés entre des composants IPCablecom et la fonction DF, ou entre la fonction DF et une autre fonction DF.
pkt-e6	DF ↔ CF	Interface utilisée pour la remise des données d'appels à la fonction CF.
pkt-e7	DF ↔ CF	Interface utilisée pour la remise du contenu d'appels à la fonction CF.

7.9 Sécurité

7.9.1 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.

Pour la plupart des interfaces, l'architecture IPCablecom nécessite que le ou les mécanismes de sécurité définis soient utilisés. Pour certaines interfaces, l'architecture permet aux opérateurs d'utiliser des liaisons non sécurisées; dans ce cas, toutefois, l'opérateur exposera les abonnés et lui-même à des attaques, qui sont contrecarrées lorsque les liaisons sont sécurisées au moyen des mécanismes définis dans la Recommandation relative à la sécurité IPCablecom (Rec. UIT-T J.170).

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 et la confidentialité. 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 ou sécurité SNMPv3) que le protocole de gestion de clé sous-jacent (par exemple, IKE ou PKINIT/Kerberos).

La Figure 14 récapitule toutes les interfaces relatives à la sécurité IPCablecom.

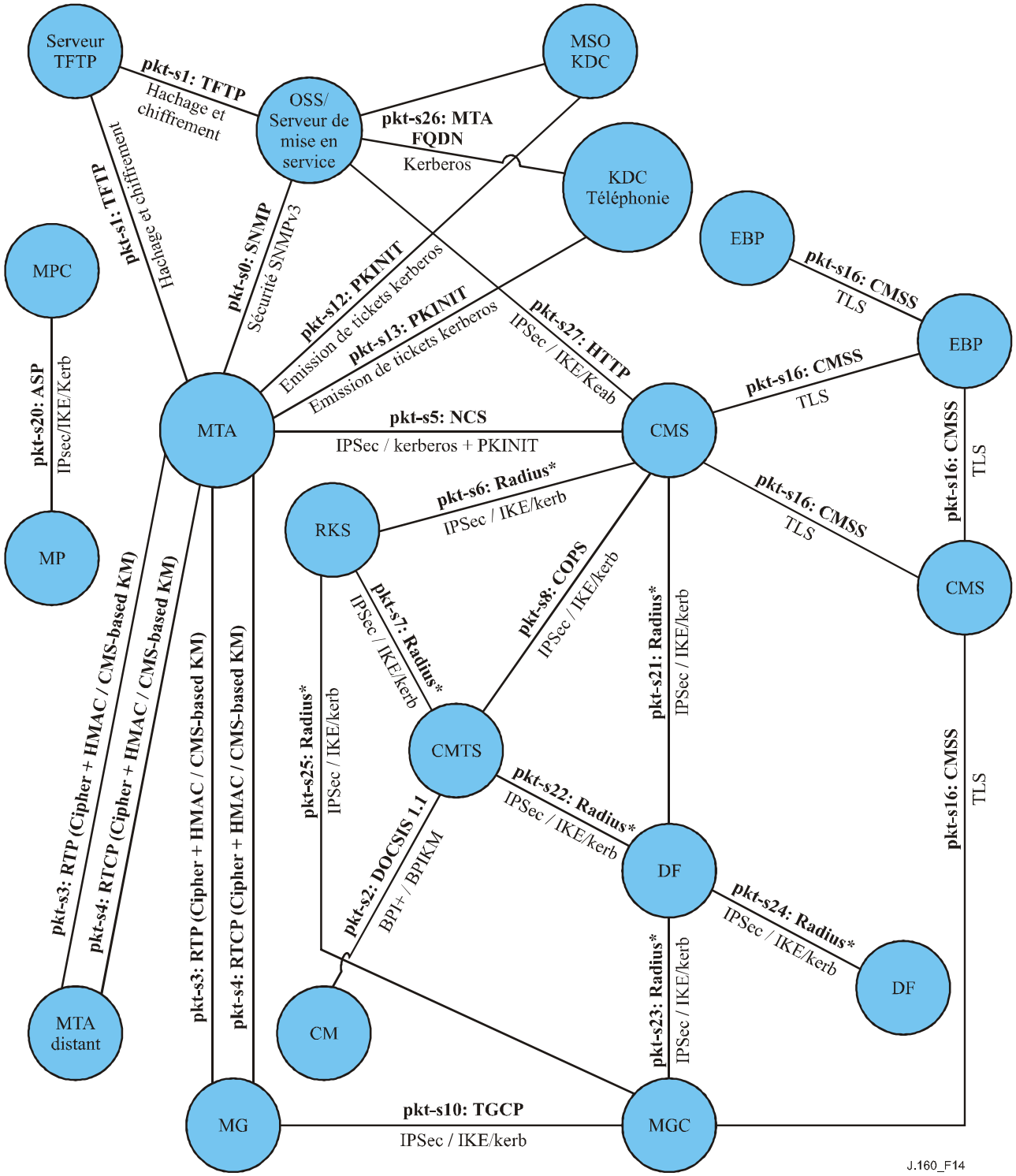


Figure 14/J.160 – Interfaces relatives à la sécurité IPCablecom

Sur la Figure 14, 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 sur la Figure 14.

Le Tableau 10 décrit chacune des interfaces indiquées sur la Figure 14.

Tableau 10/J.160 – Interfaces relatives à la sécurité

Interface	Composant fonctionnel IPCablecom	Description
Pkt-s0	MTA ↔ PS/OSS	Immédiatement après la séquence DHCP dans le flux de mise en service sécurisée, l'adaptateur MTA effectue la gestion de clés fondée sur Kerberos avec le serveur de mise en service pour établir les clés SNMPv3. L'adaptateur MTA ignore le SNMPv3 kerbérisé et utilise le SNMPv2c dans les flux de base et hybride.
Pkt-s1	MTA ↔ TFTP ou PS/OSS	Téléimportation de fichier de configuration d'adaptateur MTA. Lorsque le serveur de mise en service envoie, dans le flux de mise en service sécurisée, une commande SNMP Set à l'adaptateur MTA, il inclut à la fois le nom et la valeur de hachage du fichier de configuration. Ensuite, lorsque l'adaptateur MTA téléimporte le fichier de configuration, il l'authentifie en utilisant la valeur de hachage. Le fichier de configuration peut facultativement être chiffré. Le protocole HTTP peut être utilisé à la place du protocole TFTP.
Pkt-s2	CM ↔ CMTS	Cette interface devrait être sécurisée par le protocole BPI+, la gestion de clés BPI étant utilisée. La confidentialité BPI+ est assurée sur la liaison HFC.
Pkt-s3	MTA ↔ MTA MTA ↔ MG	RTP: 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 au moyen de l'algorithme choisi. L'intégrité des messages est facultativement assurée par un code MAC MMH. Des clés sont générées aléatoirement et échangées par les deux points d'extrémité dans des messages de signalisation par le biais du serveur CMS ou d'un autre serveur d'application.
Pkt-s4	MTA ↔ MTA MTA ↔ MG	Protocole de commande RTCP pour protocole RTP. Intégrité des messages et chiffrement au moyen de l'algorithme choisi. Les clés RTCP sont obtenues à partir du secret négocié au cours de la gestion de clés RTP. Aucun message de gestion de clés additionnel n'est nécessaire et n'est utilisé.

Tableau 10/J.160 – Interfaces relatives à la sécurité

Interface	Composant fonctionnel IPCablecom	Description
Pkt-s5	MTA ↔ CMS	NCS. Intégrité et confidentialité des messages par IPsec. La gestion des clés est assurée par le protocole Kerberos avec l'extension PKINIT (authentification initiale de clé publique).
Pkt-s6	RKS ↔ CMS	RADIUS: IPsec est utilisé pour l'intégrité comme pour la confidentialité des messages. Pour la gestion de clés, on utilise IKE ou Kerberos.
Pkt-s7	CMTS ↔ RKS	Radius, IPsec est utilisé pour l'intégrité comme pour la confidentialité des messages. Pour la gestion de clés, on utilise IKE– ou Kerberos.
Pkt-s8	CMS ↔ CMTS	Protocole COPS entre GC et CMTS, utilisé pour téléimporter l'autorisation de QS dans le CMTS. Intégrité et confidentialité des messages assurés par IPsec. Pour la gestion de clés, on utilise IKE– ou Kerberos.
Pkt-s10	MGC ↔ MG	TGCP: interface IPCablecom avec la passerelle média du RTPC. Le protocole IPsec est utilisé pour l'intégrité comme pour la confidentialité des messages. Pour la gestion de clés, on utilise IKE– ou Kerberos.
Pkt-s12	MTA ↔ KDC MSO	PKINIT: un message AS-REQ est envoyé au centre KDC avec le chiffrement par clé publique utilisé pour l'authentification. Le centre KDC vérifie le certificat et envoie soit un ticket de service soit un ticket d'autorisation de ticket (TGT, ticket granting ticket), suivant le contenu de la demande AS. La réponse AS retournée par le centre KDC contient une chaîne de certificats et une signature numérique qui sont utilisées par l'adaptateur MTA pour authentifier ce message. Dans le cas où le centre KDC retourne un ticket TGT, l'adaptateur MTA envoie alors une demande TGS au centre KDC à laquelle le centre KDC répond par une réponse TGS contenant un ticket de service. Les messages de demande/réponse TGS sont authentifiés au moyen d'une clé de session symétrique figurant dans le ticket TGT.
pkt-s13	MTA ↔ KDC téléphonie	PKINIT: voir pkt-s12. Cette interface est représentée séparément car un centre KDC distinct peut être utilisé pour assurer les services d'authentification concernant le service de téléphonie.
pkt-s16	CMS ↔ CMS CMS ↔ MGC CMS ↔ EBP EBP ↔ EBP	SIP: TLS est utilisé pour l'intégrité comme pour la confidentialité des messages. Des certificats sont utilisés pour l'authentification mutuelle au cours de la prise de contact TLS.
pkt-s20	MPC ↔ MP	ASP: IPsec est utilisé pour l'intégrité comme pour la confidentialité des messages. Pour la gestion de clés, on utilise IKE ou Kerberos.

Tableau 10/J.160 – Interfaces relatives à la sécurité

Interface	Composant fonctionnel IPCablecom	Description
pkt-s21	DF ↔ CMS	RADIUS: IPsec est utilisé pour l'intégrité comme pour la confidentialité des messages. Pour la gestion de clés, on utilise IKE ou Kerberos.
pkt-s22	DF ↔ CMTS	RADIUS: IPsec est utilisé pour l'intégrité comme pour la confidentialité des messages. Pour la gestion de clés, on utilise IKE ou Kerberos.
pkt-s23	DF ↔ MGC	RADIUS: IPsec est utilisé pour l'intégrité comme pour la confidentialité des messages. Pour la gestion de clés, on utilise IKE ou Kerberos.
pkt-s24	DF ↔ DF	RADIUS: IPsec est utilisé pour l'intégrité comme pour la confidentialité des messages. Pour la gestion de clés, on utilise IKE+.
Pkt-s25	RKS ↔ MGC	RADIUS: IPsec est utilisé pour l'intégrité comme pour la confidentialité des messages. Pour la gestion de clés, on utilise IKE ou Kerberos.
pkt-s26	OSS/Serveur de mise en service ↔ KDC MSO OSS/Serveur de mise en service ↔ KDC téléphonie	Le centre KDC utilise Kerberos pour établir un mappage entre l'adresse MAC de l'adaptateur MTA et son nom FQDN pour authentifier l'adaptateur MTA avant de lui envoyer un ticket.
Pkt-s27	CMS ↔ PS/OSS	HTTP: IPsec est utilisé pour l'intégrité comme pour la confidentialité des messages. Pour la gestion de clés, on utilise IKE ou Kerberos.

7.9.2 Sécurité de mise en service des dispositifs

Dans le cadre de l'architecture IPCablecom, la mise en service des dispositifs peut se faire en mode non sécurisé ou en mode sécurisé. En outre, la gestion SNMPv2 peut se faire en mode non sécurisé après que l'adaptateur MTA a été mis en service de façon sécurisée. Comme le présent paragraphe porte sur la sécurité, on part de l'hypothèse que le réseau fonctionne en mode sécurisé.

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.

7.9.2.1 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 de l'adresse MAC de l'adaptateur MTA. 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.

7.9.2.2 Mise en service de dispositif

L'adaptateur MTA s'authentifie auprès du centre KDC au moyen de l'extension PKINIT de Kerberos. Après avoir vérifié les justificatifs d'authentification et avoir vérifié que l'adaptateur MTA est connu du serveur de mise en service du système OSS, le centre KDC émet un

ticket pour le serveur de mise en service. L'adaptateur MTA utilise le ticket pour échanger des clés SNMPv3 de façon sécurisée avec le serveur de mise en service. Une fois qu'une session SNMPv3 sécurisée a été établie, l'adaptateur MTA demande son fichier de configuration (qui est authentifié et peut être chiffré) auprès d'un serveur TFTP ou HTTP.

7.9.2.3 Mise en service dynamique

La sécurité SNMPv3 sera utilisée pour la mise en service dynamique et la gestion des capacités de communication vocale ainsi que d'autres aspects de l'adaptateur MTA.

7.9.2.4 Autorisation de dispositif

Un adaptateur MTA mis en service est autorisé une fois qu'il s'est authentifié auprès du serveur de gestion d'appels et qu'il a établi une association de sécurité avec ce serveur avant de devenir pleinement opérationnel. L'autorisation de dispositif permet de protéger la signalisation d'appel subséquente dans le cadre de l'association de sécurité établie.

L'adaptateur MTA s'authentifie auprès du centre KDC au moyen de l'extension PKINIT de Kerberos. Après avoir vérifié les justificatifs d'authentification et avoir vérifié que l'adaptateur MTA est connu du serveur de mise en service du système OSS, le centre KDC émet un ticket pour le serveur CMS. L'adaptateur MTA utilise le ticket pour établir un tuyau IPsec vers le serveur CMS de façon sécurisée. Le tuyau IPsec peut utiliser le chiffrement néant, auquel cas les messages de signalisation NCS traversent cette interface sans être chiffrés.

7.9.2.5 Sécurité de signalisation

Tout le trafic de signalisation, y compris de QS, d'appel et d'interface de passerelle RTPC, est acheminé dans des tuyaux IPsec. La gestion des associations de sécurité IPsec est effectuée au moyen d'une combinaison de Kerberos et IKE. Le protocole Kerberos, avec les extensions PKINIT, est utilisé pour échanger des clés entre des clients d'adaptateur MTA et leur serveur CMS. Le protocole IKE, ou facultativement le protocole Kerberos, sert à gérer toutes les autres associations de sécurité IPsec de signalisation.

7.9.2.6 Sécurité des flux médias

Pendant l'établissement d'appel, les adaptateurs MTA négocient un algorithme de chiffrement particulier pour le flux support. Les dispositifs sont tenus de prendre en charge au minimum le chiffrement néant et le chiffrement AES. Le chiffrement est appliqué à la charge utile du paquet RTP mais pas à son en-tête.

Chaque paquet RTP peut contenir un code d'authentification de message (MAC) facultatif fondé sur l'algorithme MMH. Le calcul de code MAC recouvre l'en-tête non chiffré et la charge utile chiffrée (ou non chiffrée) du paquet.

Les clés utilisées pour le chiffrement et le calcul de code MAC sont extraites d'un secret qui est échangé entre les adaptateurs MTA émetteur et récepteur dans le cadre de la signalisation d'appel au moment de l'établissement d'appel. Les échanges de clés pour la sécurité des flux médias sont donc eux-mêmes sécurisés par le niveau de sécurité offert par le transport IPsec qui sécurise la signalisation d'appel.

7.9.2.7 Sécurité du système OSS et du système de facturation

Les agents SNMP contenus dans les adaptateurs MTA IPCablecom implémentent la version SNMPv3 lorsqu'ils fonctionnent en mode sécurisé. Le modèle de sécurité d'utilisateur SNMPv3 (RFC 3414) fournit les services d'authentification et de confidentialité pour le trafic SNMP. Le contrôle d'accès de type vue SNMPv3 (RFC 3415) peut être utilisé pour le contrôle d'accès à des objets de base MIB.

Le protocole de gestion de clés IKE ou Kerberos 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. Les dispositifs conformes à la Recommandation relative à la sécurité PacketCable sont tenus d'implémenter le protocole IKE avec clés prépartagées; ils peuvent aussi implémenter le protocole IKE avec certificats ou le protocole Kerberos, qui permettent aux fabricants d'implémenter des mécanismes de changement de clé entièrement automatiques. Les messages événementiels sont envoyés par le serveur CMS et par le système CMTS 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 des équipements du réseau soient calées à ±200 ms du temps universel coordonné (UTC, *universal time coordinated*). Les dispositifs qui envoient des messages événementiels sont tenus de maintenir leur synchronisation au moyen du protocole relatif au temps dans le réseau (NTP, *network time protocol*) (selon le document RFC 1119).

Il est recommandé que les réseaux IPCablecom maintiennent un serveur NTP dont la précision s'inscrive dans un intervalle spécifié par rapport au temps universel coordonné (UTC).

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 systèmes CMTS devraient caler leur débit de transmission aval sur un rythme issu d'une référence reflétant une horloge de strate 3. Les adaptateurs MTA 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.

8.3 Adressage IP

Un adaptateur MTA 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.

Tous les adaptateurs MTA de l'architecture IPCablecom doivent posséder deux adresses, l'une pour le câblo-modem, l'autre pour l'adaptateur MTA. Tous les adaptateurs MTA intégrés de l'architecture IPCablecom doivent posséder deux adresses MAC: l'une pour le câblo-modem, l'autre pour l'adaptateur MTA proprement dit. L'architecture IPCablecom prend en charge uniquement les adresses de type IPv4.

Les exigences suivantes peuvent être satisfaites au moyen de cette configuration à deux adresses IP:

- l'opérateur du réseau IPCablecom peut attribuer une adresse IP privée à la fonction d'hébergement du câblo-modem, si la traduction NAT n'est pas assurée ailleurs dans le réseau IPCablecom;
- 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 de données. Dans ce cas, l'infrastructure de routage doit être

configurée de façon que différents trajets 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 installés pour admettre ou interdire le trafic issu du composant MTA du dispositif. 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 se traduisent par des 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

Il est nécessaire, sur le plan opérationnel, de pouvoir attribuer dynamiquement des adresses IP aux adaptateurs MTA pour la mise en service et la gestion de dispositif comme pour diverses opérations liées aux protocoles. Le modèle de signalisation d'appel spécifié dans la Recommandation relative à la signalisation NCS (Rec. UIT-T J.162) est fondé sur la capacité pour un serveur de gestion d'appels de mapper un service d'abonné avec un identificateur de point d'extrémité et un nom de domaine complet (FQDN) d'adaptateur MTA. Si l'adresse attribuée à l'adaptateur MTA est changée au cours d'un appel actif (ce qui est susceptible de se produire si la location DHCP expire au cours d'un appel actif), cela aura des incidences sur les opérations de traitement d'appel. Le protocole DHCP n'autorise pas les changements d'adresse IP lors des renouvellements; un changement ne peut avoir lieu que si l'adaptateur MTA est contraint à la réinitialisation (soit explicitement soit par suite d'un refus de renouvellement). Il est recommandé de maintenir la continuité de l'adresse IP de l'adaptateur MTA par le biais de renouvellements DHCP. Pour des opérations telles que le 'renumérotage d'adresse IP', il convient d'examiner les incidences associées.

8.5 Attribution de noms FQDN

On part du principe que les systèmes OSS produiront les noms FQDN pour les dispositifs IPCablecom et transmettront ces données aux dispositifs IPCablecom et aux autres éléments de réseau appropriés. Ces interfaces ne sont pas définies dans l'architecture IPCablecom (phase 1).

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 DOCSIS que dans le réseau dorsal IP géré.

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 DOCSIS, qui classe les paquets en flux spécifiques sur la base de champs de paquet comme les adresses d'origine et de destination IP et le numéro de port UDP. Vers l'amont, ces paquets classifiés sont transportés par un service approprié à débit constant (pour les codecs actuellement pris en charge), qui est planifié dynamiquement dans le temps par le système CMTS. 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 CMTS) et DOCSIS (entre CMTS et CM) servent à configurer 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 CMTS/CM ainsi qu'à l'intérieur des réseaux dorsaux de QS à gestion Diffserv afin d'assurer un traitement de QS à haute priorité de tels paquets. L'architecture IPCablecom ne définit pas les modalités d'application des politiques de QS dans le réseau dorsal géré mais fournit les mécanismes de protocole servant à créer des classes de service spéciales.

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. 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 DOCSIS rangeant tous les paquets de signalisation à transporter dans un flux de service de priorité supérieure. Ce classificateur peut se réduire à un mappage 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 système CMTS. 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.

L'architecture IPCablecom permet l'utilisation du cadre des services différenciés (IETF RFC 3260) afin de différencier les médias et la signalisation IPCablecom des paquets de données haut débit. Le marquage des paquets pour les flux de médias (RTP et RTCP) et le flux de signalisation (NCS, TGCP) est effectué par les MTA/MG et/ou les CMS/MGC. Le marquage des paquets peut être réalisé dans la couche IP au moyen du code Diffserv (DSCP, *diffserv code point*). Il est à noter que dans le document IETF RFC 2474, on essaie de renommer respectivement l'octet TOS de l'en-tête IPv4 et l'octet de classe de trafic de l'en-tête IPv6, en champ DS. Le champ DS comprend un code Diffserv à six bits et deux bits "actuellement non utilisés". Le document IETF RFC 2474 a été mis à jour par le document IETF RFC 3168, qui définit les deux bits "non utilisés" comme des bits de "notification explicite d'encombrement (ECN, *explicit congestion notification*)". Il est fortement recommandé d'utiliser le champ DSCP de préférence à l'octet TOS IPv4.

La configuration des valeurs DSCP pour les flux de média et de signalisation est effectuée au moyen des modules MIB IPCablecom pour l'adaptateur MTA. Il convient de noter que dans le protocole NCS, les paramètres SDP signalés peuvent contenir, connexion par connexion, des valeurs qui annulent et remplacent la valeur configurée de marquage de priorité de flux de média.

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 Rec. UIT-T T.38 pour le relais de télécopie sur les réseaux IP (terminaison locale de télécopie et conversion du flux de télécopie en flux de données de relais de télécopie IP). Si une communication est établie au moyen d'un codec audio, l'adaptateur MTA est chargé de rechercher les tonalités de télécopie. Si des tonalités de télécopie sont détectées, le serveur CMS en reçoit la notification et l'adaptateur MTA est chargé de commuter le flux support sur T.38. L'architecture IPCablecom prend aussi en charge la transmission directe (*pass-through*) de télécopie, pour laquelle les tonalités de télécopie sont transmises dans le réseau IP en tant que flux audio codé G.711. L'annulation d'écho est également prise en charge pour la transmission directe de télécopie.

La prise en charge de la commutation sur télécopie à partir d'un appel vocal est requise. Dans le cas du relais de télécopie, la commutation inverse est également prise en charge.

8.8 Prise en charge des modems analogiques

Les modems analogiques sont pris en charge de façon similaire à la transmission directe de 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. L'annulation d'écho est également prise en charge pour la transmission directe de tonalités de modem.

La commutation sur un codec G.711 à partir d'un codec à faible largeur de bande pour prendre en charge la signalisation de modem analogique à partir d'un appel vocal est prise en charge. La commutation inverse une fois que la signalisation de modem est terminée est également prise en charge.

La terminaison locale des modems et la conversion du flux correspondant en flux de données de relais de modem IP ne sont pas requises.

Appendice I

Glossaire

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.

I.1 Définitions

I.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.

I.1.2 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.

I.1.3 authentification: processus de vérification de l'identité déclarée par une entité auprès d'une autre entité.

I.1.4 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.

I.1.5 autorisation: fourniture de l'accès à un service ou à un dispositif lorsque l'accès est autorisé.

I.1.6 câblo-modem: dispositif de terminaison de couche 2 formant l'extrémité client de la connexion J.112.

I.1.7 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.

I.1.8 chiffrement; cryptage: algorithme ou méthode qui transforme des données en clair en données chiffrées.

I.1.9 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.

I.1.10 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.

I.1.11 aval: sens allant de la tête de réseau aux locaux d'abonné.

I.1.12 chiffrement; cryptage: voir § II.1.8.

I.1.13 point extrémité: terminal, passerelle ou pont MCU.

I.1.14 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.

I.1.15 attribut de message d'événement: élément de données prédéfini qui est décrit par une définition et par un type.

I.1.16 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.

I.1.17 en-tête: information de commande de protocole située au début d'une unité de données protocolaire.

I.1.18 intégrité: moyen de s'assurer que les informations ne sont pas modifiées sauf par ceux qui en ont l'autorisation.

I.1.19 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.

I.1.20 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.

I.1.21 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.

I.1.22 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.

I.1.23 clé: valeur mathématique introduite dans l'algorithme cryptographique choisi.

I.1.24 échange de clés: échange entre entités de clés publiques à utiliser pour le chiffrement de communications entre ces entités.

I.1.25 gestion de clés: processus de distribution de clés symétriques partagées nécessaires à l'application d'un protocole de sécurité.

I.1.26 base d'informations de gestion (MIB): Spécification d'informations d'une manière permettant un accès normalisé au moyen d'un protocole de gestion de réseau.

I.1.27 non-répudiation: capacité permettant d'empêcher un expéditeur de nier ultérieurement avoir envoyé un message ou exécuté une opération.

I.1.28 secret: terme parfois utilisé pour désigner la confidentialité.

I.1.29 clé privée: clé utilisée en cryptographie à clés publiques, qui appartient à une seule entité et doit être tenue secrète.

I.1.30 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.

I.1.31 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.

I.1.32 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.

I.1.33 cryptographie à clé publique: 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.

I.1.34 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.

I.1.35 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.

I.1.36 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.

I.1.37 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 SS7 convertit en particulier les variantes des sous-systèmes ISUP et TCAP contenues dans une passerelle SS7 Internet en une version commune de ces sous-systèmes.

I.1.38 certificat X.509: spécification de certificat de clé publique élaborée dans le cadre des Recommandations UIT de la série T X.500 relatives à l'annuaire.

I.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 lecteur 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*)
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*)
FID	identificateur de flux (*flow identifier*)
FQDN	nom de domaine complet (*fully qualified domain name*)
GC	contrôleur de porte (*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+	échange IKE nécessitant des certificats numériques pour l'authentification
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 (*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 support d'exploitation (*operations 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 de commentaires (*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 parameter index*)
SS7	système de signalisation n^{o} 7 (*signalling system No. 7*)
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 le protocole Internet (*voice over IP*)

BIBLIOGRAPHIE

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

SÉRIES DES RECOMMANDATIONS UIT-T

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

Imprimé en Suisse
Genève, 2006