Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

J.290

(11/2006)

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

Câblo-modems

Architecture centrale de boîtier adaptateur de nouvelle génération

Recommandation UIT-T J.290

Recommandation UIT-T J.290

Architecture centrale de boîtier adaptateur de nouvelle génération

Résumé

La présente Recommandation décrit les fonctions d'architecture centrale de la nouvelle génération de boîtiers adaptateurs que les opérateurs et équipementiers PEUVENT choisir de suivre en prenant des décisions d'investissement en réseau et en produits. Cette architecture définit une plate-forme économique avec des capacités et une souplesse d'adaptation à la croissance de la vidéo à la carte, de la télévision numérique haute définition, de réseaux à gestion résidentielle connectant une large gamme d'appareils fournis par le consommateur et de futurs services multimédias sur IP comprenant la voix sur IP, la vidéo téléphonie et les jeux à plusieurs joueurs. L'objectif de la présente Recommandation est de fournir les fonctions centrales et de servir de fondement aux environnements spécifiques des réseaux. On DEVRAIT noter que la partie résidentielle de cette architecture se fonde sur la Rec. UIT-T J.190. Dans l'implémentation effective des fonctionnalités NG-STB-A, la présente Recommandation DOIT être utilisée avec la Rec. UIT-T J.292 ou la Rec. UIT-T J.291 selon la disponibilité de l'accès réseau.

Source

La Recommandation UIT-T J.290 a été approuvée le 29 novembre 2006 par la Commission d'études 9 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

AVANT-PROPOS

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

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

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

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

NOTE

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

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

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

© UIT 2007

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

			Page
1	Domaine d'application		1
2	Références		1
3	Définitions		1
4	Abréviations et acronymes		3
5	Conventions		5
6	Architecture multimédia intégrée		6
	6.1	Description de l'architecture de référence	7
	6.2	Attributs d'une architecture multimédia intégrée	8
	6.3	Architecture de services vidéo	10
	6.4	Architecture de services IP multimédia	19
	6.5	Architecture de réseau domestique	23
	6.6	Publicité numérique évoluée	31
7	Locaux de l'abonné		31
	7.1	Aperçu général	31
	7.2	Appareils vidéo d'abonné (SVD)	32
	7.3	Autres appareils de CPE	36
8	Sécurité		37
	8.1	Elément matériel de sécurité	37
	8.2	Authentification	38
	8.3	Clés de chiffrement	38
	8.4	Adresse d'unité	38
	8.5	Résistance aux altérations	38
	8.6	Gestion de clés	38
	8.7	Protection de copie	40
9	Architecture d'en-tête de réseau		40
	9.1	Architecture de livraison d'en-tête de réseau	40
	9.2	Architecture de gestion de session et de ressource	41
10	Qualité de service		43
	10.1	IntServ et DiffServ	44
	10.2	Qualité de service de bout en bout et applications de service	44
	10.3	Exigences de pont de qualité de service	45
Appendice I – Relations entre service de type indépendant du support, de type câble et de type de QS			49
Bibliographie			50

Recommandation UIT-T J.290

Architecture centrale de boîtier adaptateur de nouvelle génération

1 Domaine d'application

La présente Recommandation décrit une fonction d'architecture centrale des boîtiers adaptateurs de la prochaine génération que les opérateurs et les équipementiers PEUVENT choisir de suivre en prenant les décisions d'investissement du réseau et des produits. Cette architecture définit une plate-forme économique ayant la capacité et la souplesse de prendre en charge la croissance de la vidéo à la carte, de la télévision numérique haute définition, de réseaux domestiques gérés connectant une large gamme d'appareils fournis par l'abonné et de futurs services IP multimédias incluant la voix sur IP, la vidéo téléphonie et les jeux en ligne à plusieurs. L'objectif de la présente Recommandation est de fournir les fonctions centrales et de servir de fondement aux environnements spécifiques des réseaux. On DEVRAIT noter que la portion domestique de cette architecture de réseau se fonde sur la Rec. UIT-T J.190. Dans les mises en œuvre réelles des fonctionnalités de NG-STB-A, la présente Recommandation DOIT être utilisée soit avec la Rec. UIT-T J.292 soit avec la Rec. UIT-T J.291 selon la disponibilité de l'accès réseau.

2 Références

Aucune.

3 Définitions

La présente Recommandation définit les termes suivants:

3.1 domaine de service autorisé (ASD, *authorized service domain*): dans ce domaine, les appareils sont capables de s'authentifier et de prendre en charge des droits d'utilisation de contenu comme défini par l'opérateur du réseau.

3.2 identifiant d'application: c'est un champ qui indique un identifiant numérique pour une application fonctionnant sur le boîtier adaptateur.

3.3 domaine de sortie autorisée (AOD, *authorized output domain*): dans ce domaine, les appareils sont connectés à l'ASD en utilisant des interfaces de sortie approuvées par l'opérateur.

3.4 domaine au mieux (BED, *best effort domain*): ce sont les appareils et les segments de couche Physique qui ne se conforment pas aux exigences de ASD, AOD, GSD. Dans ce domaine, les appareils n'exigent pas de protection de contenu ou de garantie de qualité de service.

3.5 CA_system_ID: c'est un champ qui indique le type de système d'accès conditionnel applicable aux flux associés ECM et/ou EMM. Le champ CA_system_ID peut être utilisé comme identifiant de client DSG en mode DSG avancé.

3.6 client DSG: le client DSG (*DOCSIS Set-top Gateway*, passerelle de boîtier adaptateur DOCSIS) termine le tunnel DSG et reçoit du contenu du serveur DSG.

3.7 message de contrôle d'habilitation (ECM, *entitlement control message*): un ECM est un message chiffré qui contient des critères d'accès à divers liants de service et un mot de contrôle (CW).

3.8 service portail incorporé: élément de service de portail qui n'utilise pas une interface autonome pour se connecter à un appareil de boîtier adaptateur.

3.9 boîtier adaptateur incorporé: c'est une entité fonctionnelle d'application de service incorporée. Il inclut le ou les clients DSG, un contrôleur de client DSG, un processeur incorporé pour un environnement d'application et un module incorporé ou amovible pour l'accès conditionnel.

3.10 message de gestion d'habilitation (EMM, *entitlement management message*): le message EMM contient les données réelles d'autorisation et doit être envoyé par une méthode sécurisée à chaque équipement d'abonné.

3.11 domaine de service garanti (GSD, *guaranteed service domain*): les appareils dans le GSD seront capables de recevoir des services à contenu sensible à la qualité de service tels que la téléphonie utilisant le protocole Internet, les jeux interactifs multijoueurs et la visiophonie sur IP.

3.12 appareil d'accès résidentiel: groupement d'éléments logiques utilisés pour réaliser l'accès en HFC pour le ou les réseaux IPCable2Home.

3.13 appareil de pont résidentiel (HB, *home bridge*): groupe d'éléments logiques utilisés pour raccorder des réseaux IPCable2Home.

3.14 appareil de client résidentiel (HC, *home client*): groupe d'éléments logiques utilisés pour fournir des fonctions à des applications client.

3.15 appareil IP de LAN: c'est un appareil représentatif de l'appareil IP typique qu'on s'attend à trouver sur les réseaux résidentiels et il est supposé contenir une pile TCP/IP ainsi qu'un client DHCP.

3.16 service portail (PS, *portal services*): élément fonctionnel qui fournit des fonctions de gestion et de traduction entre le câblage HFC et le réseau domestique.

3.17 unidirectionnel: cette expression infère que la voie aval (descendante, du réseau vers l'abonné) est opérationnelle, et que la voie amont (montante, de l'abonné vers le réseau) n'est pas opérationnelle. Cela peut arriver parce que la voie amont n'est pas disponible, que le boîtier adaptateur n'est pas enregistré, ou que le boîtier adaptateur ne prend pas en charge le mode de fonctionnement bidirectionnel.

3.18 ensemble de paramètres de qualité de service: ensemble des codages de flux de service qui décrit les attributs de qualité de service d'un flux de service ou d'une classe de service.

3.19 passerelle domestique: c'est l'appareil qui fournit les fonctions d'interconnexion entre le réseau d'accès et le réseau domestique, comme décrit dans la Rec. UIT-T J.190.

NOTE – La façon d'appliquer la fonctionnalité de passerelle domestique de la Rec. UIT-T J.190 à divers réseaux DEVRAIT être prise en considération dans un avenir proche.

3.20 classe de service: ensemble d'attributs de mise en file d'attente et de programmation qui a reçu un nom et qui est configuré dans l'équipement d'en-tête de réseau. Une classe de service est identifiée par un nom de classe de service. Une classe de service a un ensemble de paramètres de qualité de service associés.

3.21 contrôleur d'adaptateur: c'est le système de calcul qui est responsable de la gestion des boîtiers adaptateurs au sein d'un système câblé. Il gère les boîtiers adaptateurs au moyen de messages de commande et d'information via le canal hors bande.

3.22 appareil adaptateur: récepteur qui contient une fonction de service portail incorporée pour la connectivité du réseau domestique et un boîtier adaptateur incorporé.

3.23 bidirectionnel: cette expression infère que la voie aval et la voie amont sont opérationnelles.

3.24 adresse MAC bien connue: ceci se réfère à l'adresse MAC du client au sein de l'appareil adaptateur. Cette adresse MAC a été allouée par le fabricant du système d'accès conditionnel au sein de l'appareil adaptateur.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et les acronymes suivants:

AES	norme de chiffrement évoluée (*advanced encryption standard*)
API	interface de programmation d'application (*application programming interface*)
ASD	domaine de service autorisé (*authorized service domain*)
BED	domaine au mieux (*best effort domain*)
BP	point limite (IPCable2Home) (*boundary point*)
CA	accès conditionnel (*conditional access*)
CAS	système d'accès conditionnel (*conditional access system*)
CBC	chaînage de bloc de chiffrement (*cipher block chaining*)
CE	électronique client (*consumer electronics*)
CMTS	système de terminaison de câblo-modem (*cable modem termination system*)
Codec	codec (*coder/decoder*)
CPE	équipement des locaux d'abonné (*customer premises equipment*)
CSA	algorithme de brouillage commun (*common scrambling algorithm*)
CSP	processeur de sécurité configurable (*configurable security processor*)
CW	mot de contrôle (*control word*)
DES	norme de chiffrement des données (*data encryption standard*)
DHCP	protocole de configuration de serveur dynamique (*dynamic host configuration protocol*)
DiffServ	architecture de services différenciés pour le trafic réseau (*differentiated services architecture for network traffic*)
DLNA	alliance pour l'animation des réseaux numériques (*digital living network alliance*)
DRM	gestion des droits numériques (*digital rights management*)
DSCP	point de code des services différenciés (*diffserv code point*)
DSL	ligne d'abonné numérique (*digital subscriber line*)
DTCP	protection du contenu de transmissions numériques (*digital transmission content protection*)
DTV	télévision numérique (*digital TV*)
DVB	diffusion vidéo numérique (*digital video broadcast*)
DVI	interface vidéo numérique (*digital video interface*)
DVR	enregistrement vidéo numérique (*digital video recording*)
ECB	répertoire électronique (*electronic code book*)
ECM	message de commande d'habilitation (*entitlement control message*)
EMM	message de gestion d'habilitation (*entitlement management message*)
EPG	guide électronique de programme (*electronic program guide*)
FIPS	norme fédérale de traitement de l'information (*federal information processing standards*)

FTTH	fibre jusqu'au domicile (*fibre to the home*)
GigE	gigabit Ethernet
GSD	domaine de service garanti (*guaranteed service domain*)
HDCP	protection du contenu numérique en bande passante haute (*high-bandwidth digital content protection*)
HDMI	interface multimédia à haute définition (*high definition multimedia interface*)
HFC	hybride fibre optique – câble coaxial (*hybrid fibre coaxial*)
ID	identifiant
IETF	Groupe de travail d'ingénierie Internet (*Internet engineering task force*)
IP	protocole Internet (*Internet protocol*)
Layer 3	couche 3 (couche réseau dans la pile OSI; couche du pare-feu dans laquelle l'acheminement se fonde sur l'adresse IP)
MAC	commande d'accès au support physique (*media access control*)
MGCP	protocole de commande de passerelle média (*media gateway control protocol*)
MIB	base de données d'informations de gestion (*management information base*)
MPEG	groupe d'experts des images animées (*motion picture experts group*)
MPTS	flux de transport multiprogrammes (*multiple program transport streams*)
MTA	adaptateur de terminal multimédia (*multimedia terminal adapter*)
NAT	traduction d'adresse de réseau (*network address translation*)
NCS	signalisation d'appel par le réseau (*network call signalling*)
NE	élément de réseau (*network element*)
NG-STB-A	architecture STB de prochaine génération (*next generation STB architecture*)
NIU	unité d'interface de réseau (*network interface unit*)
OCAP	plateforme d'applications OpenCable (*opencable applications platform*)
OEM	fabricant d'équipement d'origine (*original equipment manufacturer*)
OSS	système support d'exploitation (*operations support system*)
PC	ordinateur personnel (*personal computer*)
PHY	couche Physique
PID	identificateur de paquet (*packet identifier*)
PS	services portail (*portal services*)
QAM	modulation d'amplitude en quadrature (*quadrature amplitude modulation*)
QPSK	modulation par déplacement de phase quadrivalente (*quadrature phase shift keying*)
QS	qualité de service
RAN	réseau de zone régionale (*regional area network*)
RMS	système de gestion des droits (*rights management system*)
RSA	Rivest, Shamir, Adleman (système de chiffrement à clés publiques développé par Rivest, Shamir, Adleman); aussi compagnie de commercialisation de techniques de clés publiques (*resource reservation protocol*)

RSVP	protocole de réservation de ressources (*resource reservation protocol*)
RTP	protocole de transport en temps réel (*real time protocol*)
RTSP	protocole d'écoulement en temps réel (*real time streaming protocol*)
SCTE	Société des ingénieurs en télécommunication par câble (*Society of Cable Telecommunications Engineers*)
SD	numérique sécurisé (*secure digital*)
SHA-1	algorithme de hachage sécurisé n° 1 (*secure hash algorithm 1*)
SNMP	protocole simple de gestion de réseau (*simple network management protocol*)
SOC	système sur puce (*system-on-chip*)
SPTS	flux de transport de programme simple (*single program transport streams*)
STB	boîtier adaptateur (*set-top box*)
SVD	appareil vidéo d'abonné (*subscriber video device*)
TCP	protocole de commande de transmission (*transmission control protocol*)
TOS	type de service (aussi séquence codée de services différenciés, DSCP) (*type of service*)
TS	flux de transport (*transport stream*)
TVHD	télévision à haute définition
UDP	protocole datagramme d'utilisateur (*user datagram protocol*)
UI	interface d'utilisateur (*user interface*)
UPnP	prêt à l'emploi universel (*universal plug and play*)
USB	bus en série universel (*universal serial bus*)
VLAN	réseau local virtuel (*virtual local area network*)
VoD	vidéo à la carte (*video-on-demand*)
VoIP	téléphonie utilisant le protocole Internet (*voice over IP*)
XML	langage de balisage extensible (*extensible markup language*)

5 Conventions

Tout au long de la présente Recommandation, les mots qui sont utilisés pour définir la signification d'une exigence particulière sont en majuscules. Ces mots sont:

"DOIT"	Ce mot ou l'adjectif "EXIGÉ" signifie que l'élément est une exigence absolue de la présente Recommandation.
"NE DOIT PAS"	Cette phrase signifie que l'élément est une interdiction absolue de la présente Recommandation.
"DEVRAIT"	Ce mot ou l'adjectif "RECOMMANDÉ" signifie qu'il peut exister des raisons valides dans des circonstances particulières d'ignorer cet élément, mais toutes leurs implications devraient être comprises et le cas soigneusement évalué avant de choisir une voie différente.

"NE DEVRAIT PAS" Cette phrase signifie qu'il peut exister des raisons valides dans des circonstances particulières où le comportement cité est acceptable ou même utile, mais toutes les implications devraient en être comprises et le cas soigneusement évalué avant d'implémenter tout comportement décrit de cette façon.

"PEUT" Ce mot ou l'adjectif "FACULTATIF" signifie que cet élément est réellement facultatif. Un fabricant peut choisir d'inclure l'élément à cause d'exigences particulières du marché ou parce qu'il améliore le produit, par exemple, un autre fabricant peut omettre le même élément.

6 Architecture multimédia intégrée

Ci-après figurent les attributs clés de NG-STB-A pour une *Architecture multimédia intégrée*:

– *Capacité étendue*: fournit une capacité étendue qui ne sera pas une limitation à l'introduction de nouveaux services. Elle permet aux câblo-opérateurs l'option d'utiliser plus efficacement le spectre grâce à l'utilisation de: la conversion de canaux analogiques en services vidéo à compression numérique; d'algorithmes de compression évolués; de schémas de modulation plus évolués; une gestion intégrée des ressources du spectre à l'en-tête de réseau; et la vidéo numérique commutée.

– *Transition tout numérique*: prend en charge une transition vers les services tout numérique tout en continuant économiquement à prendre en charge télévision et VCR analogiques ordinaires.

– *Accès conditionnel (CA) sécurisé, souple*: met en place l'accès conditionnel au moyen d'un matériel interne (le processeur de sécurité configurable NG-STB-A, ou CSP) qui peut être configuré à distance ou renouvelé par des téléchargements de logiciels. La prise en charge de plusieurs options d'accès conditionnel, y compris l'accès conditionnel ordinaire et de nouveaux accès conditionnels privés ou non privés, permet ainsi l'intégration d'équipements de CPE de fournisseurs multiples. Fournit la souplesse à des prix inférieurs à ceux de contrôles d'accès physiquement amovibles. En même temps, les réseaux câblés peuvent continuer à prendre en charge physiquement une sécurité séparable via l'utilisation d'appareils à carte de sécurité.

– *Prise en charge de la distribution au détail*: facilite la vente au détail d'appareils vidéo d'abonnés (SVD) en fournissant des capacités d'activation par l'abonné, soutenues par la configuration à distance par l'opérateur grâce à la compatibilité avec tous les systèmes par câble NG-STB-A.

– *Réseautage domestique sécurisé*: prend en charge les technologies et normes de réseautage domestique ouvert, les systèmes de gestion de droits numériques (DRM, *digital rights management*), et l'usage universel de IP (protocole Internet) pour la distribution de contenus au foyer. Permet aux opérateurs de réseau d'offrir des services réseau domestiques multimédias gérés de l'en-tête du réseau. Prend en charge l'utilisation de systèmes de divertissement multilocalisation qui utilisent des appareils de mémorisation au foyer pour servir des contenus à divers appareils à faible technicité ou technicité supérieure, mis en réseau. Intègre des services multimédias entre des appareils adaptateurs anciennement dédiés à la vidéo et des ordinateurs personnels dédiés aux données.

– *Canaux authentifiés bidirectionnels sécurisés*: tout équipement CPE de la prochaine génération fournit des canaux de communication bidirectionnels authentifiés et sécurisés entre l'en-tête de réseau et l'équipement CPE. Cela accroît la sécurité par rapport à la sécurité réalisable sur les systèmes unidirectionnels. De tels canaux sont utilisés pour la gestion de clés d'accès conditionnel renouvelables, la gestion à distance de l'équipement CPE, les mises à jour de micrologiciels téléchargeables, les données d'application interactives privées, et la reconfiguration des algorithmes de chiffrement.

– *Options souples de transport*: prise en charge de transport de vidéo en diffusion, en diffusion groupée et/ou en diffusion individuelle sur IP.

– *CPE équipés pour de futures normes de transmission et de compression*: permet des augmentations futures de la capacité effective des systèmes avec un accroissement minimal des investissements sans exiger des investissements préalables sur les équipements CPE, que de tels investissements soient faits par les opérateurs ou au détail par les consommateurs.

– *Environnement d'applications bien défini dans le CPE*: inclut des capacités pour qu'un logiciel médiateur de plateforme d'applications des Recommandations UIT-T de la série J.200 prenne en charge des applications téléchargeables, permettant la création rapide de services, et de nouveaux modèles commerciaux, avec l'idée d'appliquer les Recommandations UIT-T de la série J.200 sur tous les sujets relatifs aux SVD avec des conditions de licence raisonnables. Fournir les économies découlant d'une plateforme standard sans limiter la capacité d'innover des câblo-opérateurs sur l'interface d'utilisateur et l'aspect pratique et esthétique des services.

– *Approvisionnent rapide des nouveaux services*: prise en charge de l'auto-installation et de l'approvisionnement rapide des nouveaux services grâce à l'autodécouverte, la gestion à distance, et des dispositifs de configuration à distance de CPE conformes à NG-STB-A.

– *Gestion de ressource améliorée par des interfaces d'en-tête de réseau ouvertes*: restructurer les éléments d'en-tête de réseau avec des interfaces ouvertes permet une utilisation plus efficace des ressources des systèmes, un accroissement effectif de la capacité et de la souplesse des systèmes utilisables, la réduction des coûts, et l'expansion du nombre des fournisseurs de composants d'en-tête de réseau, tout en assurant les capacités d'interconnexion.

6.1 Description de l'architecture de référence

L'architecture de référence est définie en termes d'ensemble d'éléments de réseau qui sont utilisés pour satisfaire des besoins spécifiques. Ces éléments de réseau opèrent au sein des segments majeurs du réseau qui comprennent les applications administratives, l'en-tête de réseau, les installations extérieures et les locaux de l'usager, comme exposé à la Figure 1.

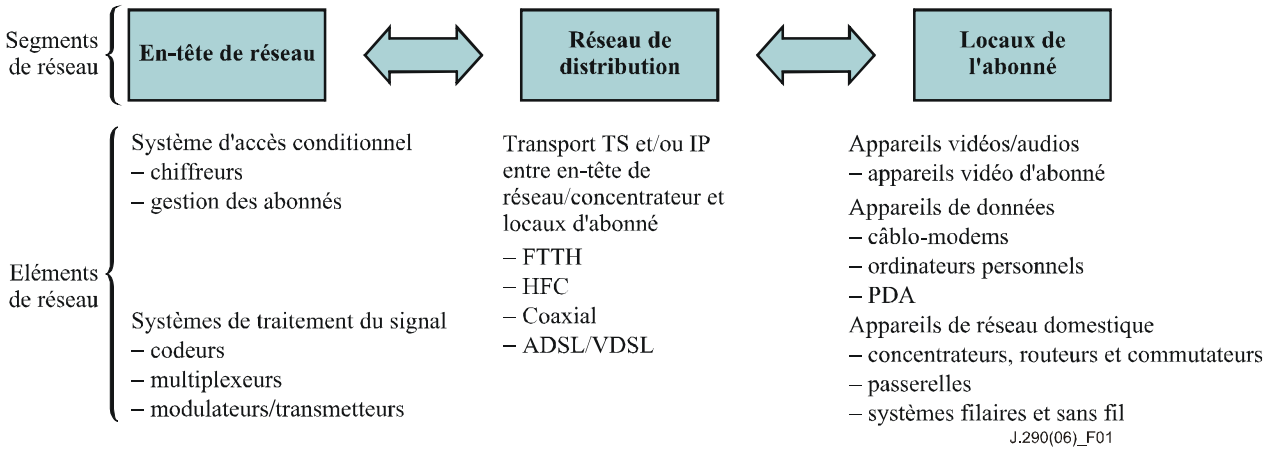


Figure 1 – Segments et éléments majeurs du réseau

6.2 Attributs d'une architecture multimédia intégrée

6.2.1 Architecture des services vidéo

Au minimum, un équipement CPE conforme à NG-STB-A devra avoir les attributs suivants.

– *Accès conditionnel*: employer un accès conditionnel interne reconfigurable fondé sur un hybride de moteur matériel pour le déchiffrement (CSP) et un échange de clés défini par le logiciel. La prise en charge du déchiffrement multiflux pour DVR, des capacités d'insertion d'annonces locales et d'autres applications exigeant des signaux multiples.

– *Transport vidéo*: prise en charge de deux modes:

  • Mode non IP (MPEG de base sur QAM);

  • Mode IP (MPEG encapsulé au sein de IP).

– *Prise en charge d'applications d'appareils vidéo*: tous les équipements CPE de vidéo ont les ressources minimales requises (c'est-à-dire la puissance de mémoire et de processeur) pour prendre en charge [UIT-T J.200], [UIT-T J.201] et [UIT-T J.202].

– *Codecs vidéo*: prise en charge du décodage de H.262 (vidéo MPEG-2) plus des codecs évolués, H.264 (AVC MPEG-4), et facultativement VC-1. L'appareil client DOIT être capable de commuter presque instantanément entre le codec évolué actuellement actif et MPEG-2.

– *Codecs audios*: prise en charge du décodage de MPEG AAC ou du Dolby numérique.

6.2.2 Architecture IP multimédia

– *Protocol Internet*: IP choisi comme couche support de base pour tous les services multimédia de réseau domestique.

– *Qualité de service dans le réseau domestique IP*: {texte pour information: Plan pour se conformer à UPnP (normes de prêt à l'usage universelles) pour activer la gestion à distance, l'approvisionnement et l'observation de service d'appareils UPnP dans les réseaux domestiques.}

– *IPv6*: prise en charge à la fois de IPv4 et IPv6 dans tous les appareils connectés IP, avec l'idée de passer en fin de compte à IPv6.

6.2.3 Réseautage domestique

– *Domaines de réseau domestique*: définir les domaines de réseau domestique comme une fonction de niveau de service et de protection du contenu.

  • GSD (domaine de service garanti): qualité de service gérée de l'en-tête de réseau à l'appareil d'extrémité.

  • ASD (domaine de service autorisé): le contenu peut être transféré aux appareils récepteurs qui ont un des systèmes de DRM certifié, authentifié par l'opérateur du réseau ou d'accès conditionnel.

  • OAD (domaine de sortie autorisée): le contenu peut être transféré à travers une interface de gestion des droits à partir de l'ASD vers des appareils avec un DRM non authentifié par l'opérateur.

  • BED (domaine au mieux): des appareils connectés en dehors de GSD, ASD ou OAD.

    L'équipement CPE PEUT être localisé au sein de n'importe lequel de ces domaines ou dans plusieurs domaines qui se chevauchent.

– *Port USB-2 et/ou Ethernet*: fournit une connexion universelle de CPE avec les réseaux domestiques. Toute couche Physique capable de transporter du trafic IP transparent (par exemple, CAT5 Ethernet) peut être prise en charge au moyen de l'utilisation d'un adaptateur entre le port USB et la couche Physique spécifique.

– *Partage d'applications*: prend en charge le partage d'applications entre les appareils de la série J.200 ainsi que des appareils qui ne sont pas de la série J.200 qui résident dans un ou plusieurs des domaines de réseau domestique définis au § 6.5.1, par exemple, un PC avec un client compatible NG-STB-A. Parmi les exemples d'applications on citera: l'accès distant à un contenu DVR, les jeux multijoueurs, le gestionnaire d'informations personnelles (par exemple, le calendrier de la famille, le carnet d'adresses, le réveil matin).

6.2.4 Insertion de programme

– *Insertion de programme*: les techniques d'insertion de programmes telles que la Rec. UIT T J.181 (Insertion de programme numérique) prennent en charge les besoins de l'opérateur en livraison souple de programmes. La capacité à réunir deux flux chiffrés, par exemple à remplacer un contenu chiffré dans un flux diffusé par un contenu chiffré précédemment mis en mémoire cache sur le pilote matériel local.

6.2.5 Segment réseau: locaux d'abonné

– *Appareil vidéo d'abonné (SVD)*: les SVD sont des appareils de vidéo conformes à NG-STB-A qui comportent un tuner, comme un adaptateur ou une unité de décodage ou des postes de télévision numériques (DTV). Un SVD de base (entrée de gamme) est défini avec la fonctionnalité NG-STB-A minimale requise. Les SVD de haut de gamme incluent diverses options d'amélioration à la discrétion des fournisseurs, des opérateurs des réseaux, et des détaillants. Les fonctions SVD de base et les exemples d'options d'amélioration figurent dans le Tableau 1.

Tableau 1 – Fonctions SVD de base et étendues

Fonctions SVD de base	Fonctions SVD améliorées facultatives (exemples)
• Prise en charge de plusieurs modes de transport. • Prise en charge du décodage MPEG-2 (SD et HD) plus H.264. • Connectivité de réseau domestique comme client. • CA téléchargeable. • Capacité de logiciel médiateur de la série J.200. • Sortie en définition standard. • Sortie en vidéo haute définition. • Interfaces de sortie numérique avec protection de copie. • Contrôle à distance universel fourni par l'OEM capable de contrôler le SVD la TV ordinaire. • Prise en charge en option de la modulation QAM vers l'aval de J.83. • Inclut un accès USB-2 et/ou Ethernet tout venant pour la connectivité du réseautage domestique et une connexion possible de périphériques non spécifiés.	• Interfaces numériques protégées en copie (par exemple, HDMI, DVI). • Fonction de passerelle incorporée (client, serveur, et gestion d'adresse IP) entre les réseaux d'accès et domestique. • Fonctionnalité DVR de base. • Codec VC-1.

– *Gestion des droits*: les équipements CPE respectent et protègent les droits des propriétaires de contenu quant à l'utilisation de leurs contenus de grande valeur.

6.2.6 Segment du réseau: tête de réseau

- *Qualité de service et gestion de ressource de session*: définit la structure logique et traite les flux associés à la qualité de service (demandes, allocations, et assurance de service). Coordonne et se conforme aux processus de qualité de service de l'en-tête de réseau associés à toutes les ressources dans l'en-tête de réseau, installations extérieures et de réseau domestique.
- *Interfaces OSS/BSS*: définit le modèle pour les interfaces avec un système de facturation de l'arrière, un système support d'exploitation (OSS) et un système de soutien commercial (BSS).

6.3 Architecture de services vidéo

Les caractéristiques communes de l'architecture des services vidéo incluent:

- **sécurité**: le processeur de sécurité configurable gère l'accès conditionnel, la protection en copie, prend en charge les services à la demande sécurisés, les téléchargements sécurisés et les fonctions de gestion des droits numériques (DRM) résidentiels;
- **protection en copie**: les mécanismes de protection contre la copie pour la livraison des contenus à travers des sorties protégées;
- **téléchargements de micrologiciels**: permet la configuration des appareils;
- **transport vidéo**: prise en charge du mode non IP (MPEG de base sur QAM) et mode IP (MPEG encapsulé dans IP);
- **codecs vidéo**: prise en charge des codecs H.262 (vidéo MPEG-2) et H.264 (AVC MPEG-4) et prise en charge facultative de SMPTE 421M (VC-1);
- **environnement logiciel de client vidéo**: prise en charge de micrologiciels de la série J.200 dans tous les appareils réseau de la prochaine génération qui acceptent les applications téléchargeables, plus donner de la souplesse dans la prise en charge d'applications à travers des systèmes fondés sur l'en-tête de réseau;
- **téléchargement de logiciel sécurisé**: prise en charge de l'installation et de la mise à niveau d'implémentation d'applications de logiciels, de pilotes, de noyaux et de micrologiciels de la série J.200.

6.3.1 Sécurité

Un SVD va inclure un processeur de sécurité configurable (CSP, *configurable security processor*) interne de prochaine génération pour la gestion des aspects de sécurité pour les services. Les aspects de sécurité peuvent être catégorisés comme suit, avec un certain chevauchement:

- authentification et gestion des appareils;
- accès conditionnel aux services entre l'en-tête de réseau et l'équipement d'abonné;
- téléchargement sécurisé de mises à jour de micrologiciels et d'applications téléchargeables;
- protection contre la copie;
- sécurité du domaine de service autorisé;
- DRM au sein des appareils sur un ou plusieurs réseaux domestiques au sein du domaine de service autorisé;
- le pont de sécurité entre accès conditionnel et DRM est défini dans la Rec. UIT-T J.197.

Le modèle de sécurité de la prochaine génération comporte trois sous-systèmes:

1) *chiffrement/déchiffrement du contenu et des clés*, qui se fonde sur le matériel mais peut être reconfiguré à distance;

2) *gestion de clés*, qui est partiellement fondée sur le logiciel et est donc redéfinissable par un téléchargement de système d'accès conditionnel sécurisé;

3) *authentification*, qui est partiellement fondée sur le logiciel et est donc renouvelable par le téléchargement de systèmes d'accès conditionnel sécurisés.

Ces sous-systèmes prendront en charge la gestion d'opérateur des aspects suivants de l'accès conditionnel:

- la reconfiguration à distance du moteur de déchiffrement pour prendre en charge plusieurs algorithmes d'embrouillage prédéfinis, y compris les algorithmes ordinaires d'accès conditionnel communément utilisés aussi bien que de nouveaux algorithmes d'accès conditionnel;
- le téléchargement initial défini par le logiciel et le renouvellement du mécanisme d'échange de clés d'accès conditionnel.

Dans le modèle de référence CSP, le contenu PEUT être sécurisé par un standard ouvert, un système non propriétaire de CA/DRM et/ou un système CA/DRM privé (ordinaire ou autre).

Le "moteur de déchiffrement flexible" dans le CSP, comme indiqué à la Figure 2, est configurable pour prendre en charge plusieurs algorithmes. Il est assez flexible pour permettre la configuration par une commande à distance de façon à être compatible avec les algorithmes de chiffrement utilisés par le système de contrôle d'accès ainsi qu'avec le ou les systèmes de protection du contenu. Les messages d'habilitation et les messages de contrôle sont codés et distribués sur les canaux hors bande et dans la bande aux équipements CPE de vidéo de telle sorte que les clés puissent être récupérées en toute sécurité par le CSP; ceci est désigné sous l'appellation d'application de gestion de clés d'accès conditionnel défini par micrologiciel.

Les aspects de sécurisation du CSP sont protégés par l'intégration d'un système sur puce (SOC, *system-on-chip*) qui comporte un moteur de déchiffrement configurable et un microcontrôleur pour la gestion de clés. Le SOC inclura les éléments CSP et décodeur de sorte que la vidéo numérique en clair et compressée ne quitte jamais le SOC. La vidéo numérique en clair sera protégée entre les éléments de CSP et de décodeur du SOC en utilisant des techniques de simple hachage ou de chiffrement rapide.

Le CSP sera structuré pour éviter d'encourir une responsabilité en matière de droits de propriété pour les systèmes CA/DRM inactifs ou dormants. On s'attend à ce que les droits de propriété intellectuelle (IPR, *intellectual property rights*) relatifs à un système de CA/DRM ne soient pas utilisés lorsque ce système de CA/DRM n'est pas activé par l'opérateur.

Des exemples de choix possibles d'algorithmes sont donnés dans la Figure 2. Les algorithmes qui seront pris en charge seront décidés en fin de compte lors du développement des spécifications. Pour assurer la transition depuis les accès conditionnels ordinaires, l'appareil client DOIT posséder la capacité à fonctionner dans un environnement simulcrypt ou multicrypt. Dans le cas où simulcrypt est activé, le CSP devra prendre en charge le partage de clés dans le CPE.

Le CSP va employer des technologies de prise en charge du déchiffrement des flux de transport sécurisés propriétaires ou normalisés non propriétaires sur la base des algorithmes de déchiffrement tels que DES, 3-DES, CSA, AES et Multi2.

Le CSP sera capable de générer en toute sécurité des signatures numériques dans des matériels résistants aux altérations sans exposer les clés privées ou le traitement nécessaire pour générer les clés de hachage et de chiffrement. La prochaine génération de réseaux sera capable de signer numériquement les messages utilisés pour l'authentification et de fournir la garantie de l'intégrité en utilisant un hachage sécurisé.

Chaque CSP dans un équipement d'appareil CPE sera identifié par un identifiant univoque. Pour la mise en série privée, chacun pourrait contenir un identifiant unique appelé ID de souche privée. Cet

identifiant de souche est utilisé pour générer la clé unique pour déchiffrer les habilitations pour cet appareil d'équipement CPE spécifique. L'appareil d'équipement CPE sera capable de changer l'identifiant de souche en faveur d'une autre valeur unique d'après une commande sécurisée provenant de l'en-tête du réseau. La clé de chiffrement pourrait alors être générée en utilisant ce nouvel identifiant de souche comme un composant de la clé. Une clé asymétrique pourrait aussi être utilisée pour déchiffrer la clé de catégorie envoyée dans l'EMM (message de gestion d'habilitation).

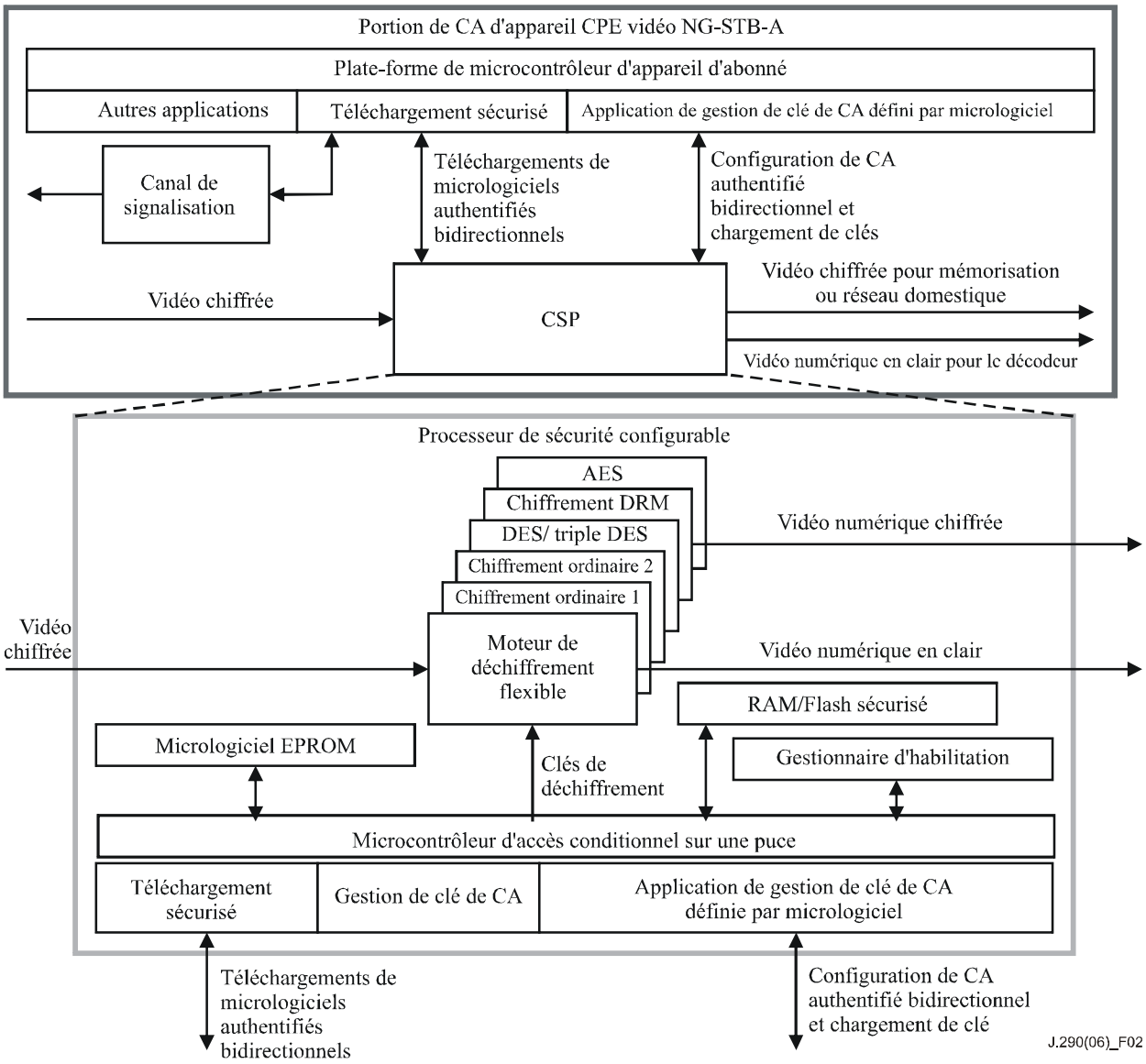


Figure 2 – Exemple de schéma fonctionnel de sécurité

6.3.1.1 Prise en charge de flux multiples

Les CSP seront capables de déchiffrer/rechiffrer simultanément plusieurs flux de contenu. On s'attend à ce que différents CSP soient capables de traiter des quantités différentes de flux en fonction des capacités de l'appareil CPE associé, mais à ce que tous les CSP soient capables de traiter un nombre minimal de flux simultanément. Les CSP DEVRAIENT prendre en charge les scénarios multiflux suivants:

- *Veille et enregistrement*: la capacité, en utilisant deux tuners, à être en veille sur un flux chiffré 'en direct', tout en en enregistrant simultanément un autre sur un pilote matériel. Cela exige vraisemblablement que le CSP retire le chiffrement de contrôle d'accès du réseau et qu'il applique simultanément un chiffrement du pilote matériel aux deux flux.

- *Serveur DVR*: un appareil DVR avec plusieurs tuners et un pilote matériel qui prenne en charge d'autres matériels dans le foyer qui ne possèdent pas de pilote matériel, en livrant du matériel enregistré via le réseau domestique. Un serveur DVR peut prendre en charge plusieurs flux d'enregistrements prêts à l'emploi concurrents, par exemple défilement en continu de contenus concurremment sur plusieurs appareils du foyer tout en enregistrant simultanément plusieurs programmes. Le CSP de l'appareil DVR PEUT avoir à prendre en charge la veille et l'enregistrement tout en servant aussi des flux chiffrés provenant du pilote matériels sur des appareils distants dans un scénario de DVR à multilocalisation.

Les CSP PEUVENT prendre en charge plusieurs flux en employant plusieurs CSP centraux, ou en augmentant le débit d'un seul centre, ou les deux.

6.3.1.2 Accès conditionnel

Le plan NG-STB-A envisage de fournir la prise en charge de plusieurs options d'accès conditionnel (CA) pour le câblo-opérateur, permettant à un opérateur de réseau d'accepter un accès conditionnel propriétaire aussi bien que tout système nouveau d'accès conditionnel normalisé. Le CSP au sein de chaque équipement CPE peut être configuré pour fonctionner sur l'accès conditionnel particulier choisi par le câblo-opérateur.

Comme le choix de l'accès conditionnel peut être fait à tout moment sous le contrôle d'une commande d'en-tête de réseau, un système équipé d'un CSP peut migrer en douceur d'une option d'accès conditionnel à une autre. Le CSP sera compatible avec les cartes de sécurité. Les appareils d'abonné qui ont des interfaces de carte de sécurité DEVRAIENT revenir par défaut au CSP si aucune carte de sécurité n'est installée.

6.3.1.2.1 Renouvellement de logiciel d'accès conditionnel

Certains aspects des algorithmes, des échanges de clé, de la gestion de clé, et des protocoles cryptographiques sont implémentés dans le logiciel ou dans les micrologiciels renouvelables sur le CSP. La capacité de renouvellement dans le logiciel est un aspect important d'un système de sécurité fort et elle est souhaitable dans le système de prochaine génération. Pour des raisons économiques, il est souhaitable d'utiliser aussi souvent que possible la capacité à renouveler le logiciel plutôt que le renouvellement du matériel.

NG-STB-A ne prend pas en charge l'accès conditionnel "tout logiciel" dans lequel les fonctions cryptographiques sont effectuées sur un processeur tout venant. Les éléments de sécurité du matériel sont une exigence essentielle d'un système de sécurité efficace pour les contenus de grande valeur. Les éléments de logiciel et de matériel spécialisés sont complémentaires et PEUVENT fournir des solutions supplémentaires de sécurité sur le logiciel ou seulement sur le matériel.

6.3.1.2.2 Renouvellement de matériel d'accès conditionnel

Bien que la capacité à renouveler le logiciel soit plus efficace d'un point de vue économique et plus facile à implémenter, certains niveaux de renouvellement des matériels sont souhaitables dans le domaine des techniques de gestion de clés et de déchiffrement du transport au sein du CSP.

La capacité à renouveler le matériel à la fois de la gestion de clé et du déchiffrement du transport peut être réalisée de plusieurs façons en utilisant des matériels amovibles capables d'accepter les exigences de bande passante des flux de transport. Par exemple, pour les appareils NG-STB-A qui prennent en charge une interface de carte de sécurité multiflux, l'insertion d'une carte de sécurité permettrait une capacité de renouvellement totale. Autrement, un port de communication tel que USB 2.0 pourrait être utilisé pour héberger un nouvel appareil qui pourrait être développé pour une pleine capacité de renouvellement du matériel si la sécurité de l'appareil se trouvait compromise.

6.3.2 Protection de copie

Si un appareil NG-STB-A emploie une carte de sécurité, l'interface doit implémenter la capacité à renouveler et à configurer. Des méthodes supplémentaires de la prochaine génération de protection contre la copie seront aussi prises en compte.

6.3.3 Téléchargements de microcodes et/ou logiciels

Les SVD sont supposés prendre en charge trois types de téléchargement sécurisé de micrologiciels:

- des micrologiciels de contrôle général qui contrôlent l'interface d'utilisateur, le fonctionnement de l'appareil et la prise en charge des applications (par exemple, VoD, EPG, les Recommandations UIT-T de la série J.200);
- des micrologiciels internes qui gèrent et communiquent avec le CSP;
- des messages hautement sécurisés destinés à être passés au CSP, qui reconfigurent le moteur matériel et/ou installent le micrologiciel de gestion de clé d'accès conditionnel dans le CSP.

Les téléchargements sécurisés sont codés pour la transmission au SVD sur un canal sécurisé. Tous les chemins de signal de téléchargement sécurisé exigent des échanges bidirectionnels authentifiés et il est de plus supposé que les chemins de signal physiquement accessibles entre les blocs de la Figure 2 sont chiffrés.

6.3.4 Transport de vidéo

Les flux numériques vidéo et audio sont normalement transportés sur des flux de transport MPEG-2. Les flux de transport programme unique (SPTS, *single program transport stream*) et les flux de transport de programme multiple (MPTS, *multiple program transport stream*) PEUVENT être livrés à divers segments du système. Les informations spécifiques de programme MPEG-2 et les informations de service (SI de J.94) sont utilisées à la couche de transport MPEG.

6.3.4.1 Cœur de réseau

Le transport audio/vidéo de cœur de réseau (en diffusion et à la demande) est normalement du transport MPEG-2 sur le protocole datagramme d'utilisateur (UDP)/IP porté sur du Gigabit Ethernet. SPTS et MPTS PEUVENT tous deux être utilisés. Un exemple de SPTS est un flux de vidéo à la carte à la sortie Gigabit Ethernet du serveur de flux. Un exemple de MPTS est le flux de diffusion multiplexé provenant d'un multiplexeur. L'encapsulation IP dans le cœur de réseau est habituellement terminée à la bordure du réseau (au QAM ou au CMTS).

Les cœurs de réseau de l'avenir PEUVENT faire usage de RTP ou d'autres protocoles pour restaurer la synchronisation affectée par la gigue et la latence du réseau. L'utilisation d'un en-tête supplémentaire tel que RTP PEUT permettre d'ajouter des informations spécifiques de la vidéo pour les transporter dans le paquet, comme un identifiant de session VoD ou un identifiant de programme.

6.3.4.2 De la périphérie aux locaux d'abonné

L'architecture de référence NG-STB-A envisage deux moyens de remplacement pour porter les données audio/vidéo entre la bordure d'en-tête de réseau et les locaux de l'usager. Les données vidéo seront compressées via MPEG-2 ou un schéma de codage évolué décrit ci-dessous. Les données audio seront dans la couche 3 de MPEG-1, ou dans un schéma de codage audio évolué. Les deux méthodes de transport possibles sont:

- **Méthode de base: transport MPEG-2 sur QAM**

  Le flux de transport de programme multiple (MPTS) MPEG-2 sur QAM est l'approche conventionnelle utilisée dans les systèmes de câble numérique d'aujourd'hui. Afin de maintenir la compatibilité vers l'amont, l'appareil vidéo numérique d'abonné

(SVD, *subscriber video device*), ou l'équipement CPE vidéo de prochaine génération, devra être capable de traiter le transport MPEG-2 sur QAM pour les applications aussi bien en diffusion qu'à la demande. La charge utile du flux de transport PEUT être un flux audio/vidéo MPEG-2 ou un flux compressé de codec évolué.

- **Méthode améliorée: vidéo sur IP**

  Dans cette approche, la vidéo est transportée sur IP et livrée sur divers supports tels que des canaux FTTH, DSL, HFC, coaxiaux. Cela permet des services futurs allant des supports en continu fondés sur IP aux SVD numériques. L'audio et la vidéo PEUVENT être transportés dans n'importe lequel des formats suivants:

  – paquets de transport MPEG-2 sur IP;

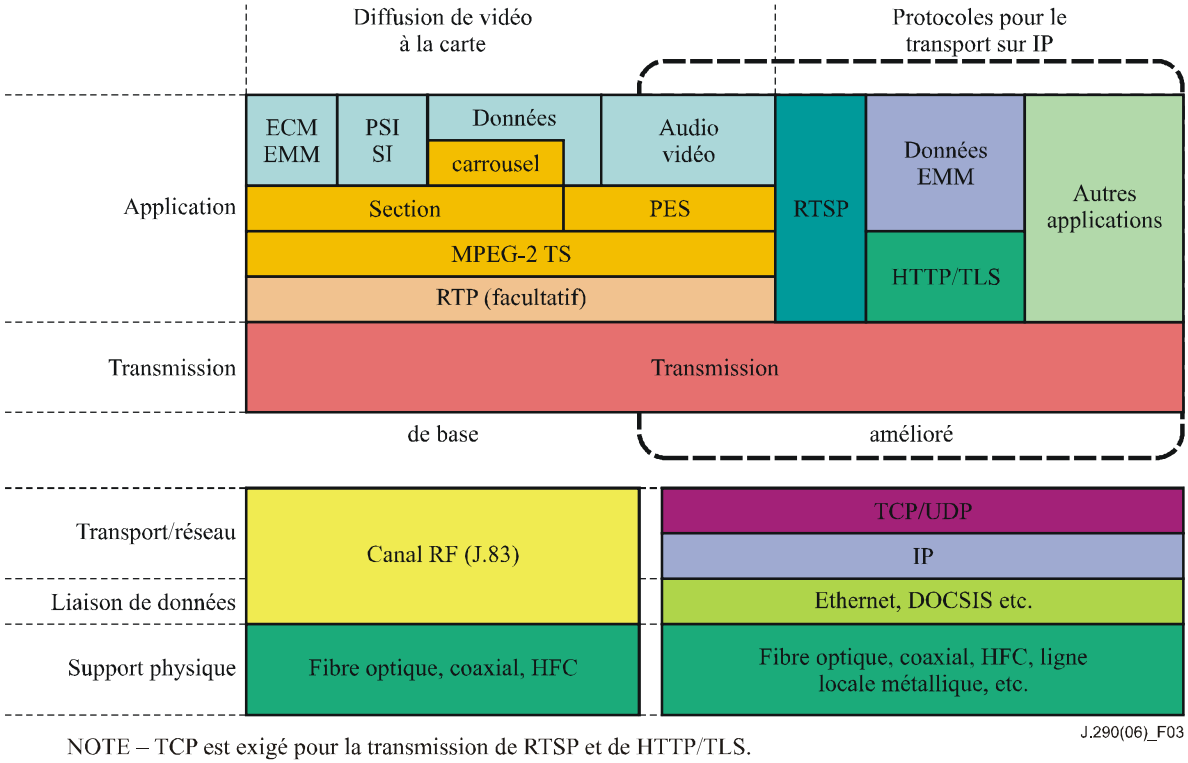
  – paquets de transport MPEG-2 dans des charges utiles RTP sur IP;

  – charge utile RTP (ou autre protocole de synchronisation IP en temps réel) sur IP.

L'équipement CPE de réception DEVRAIT être capable de traiter des flux délivrés dans n'importe lequel des trois formats ci-dessus.

De plus, les données et messages EMM PEUVENT être portés sur HTTP avec TLS. Pour les applications de vidéo à la carte, le protocole RTSP PEUT être utilisé pour la commande de session. L'équipement CPE de réception DEVRAIT aussi prendre en charge ces protocoles. Pour les applications de vidéo à la carte, le protocole RTSP est utilisé pour la commande de sessions telles que SETUP, PLAY, PAUSE, TEARDOWN.

Il est exigé que le terminal de l'abonné prenne en charge deux méthodes de transport, la méthode de base et la méthode améliorée. La Figure 3 montre les approches de transport vidéo fondées sur les deux méthodes de transport.



NOTE – TCP est exigé pour la transmission de RTSP et de HTTP/TLS.

Figure 3 – Approches de transport vidéo de remplacement

6.3.5 Codec vidéo

Les systèmes par câble NG-STB-A délivreront les contenus vidéo sous deux formats de compression: MPEG-2 (à la fois en haute définition et en définition standard) comme délivré sur les systèmes actuels, et un format de compression évolué. Le choix de MPEG-2 ou d'un codec évolué sera fait programme par programme, ou service par service (y compris le passage à/ d'un contenu de programme et de publicité). Donc, le SVD DOIT être capable de commuter rapidement entre le décodage d'un contenu MPEG-2 compressé et un contenu de codec évolué. La transition d'un décodage de contenu MPEG-2 à un décodage de codec évolué DOIT être aussi insensible pour l'auditeur que les transitions actuelles entre les programmes MPEG-2.

Le format de compression évolué sera celui de la Rec. UIT-T H.264 (MPEG-4 Partie 10, codage vidéo évolué) et facultativement VC-1.

L'opérateur choisira quel format de compression évolué utiliser. On ne s'attend pas à ce qu'un opérateur utilise les deux formats de compression évolués simultanément sur ses installations. Donc, on s'attend à ce que le SVD soit capable de décoder à la fois MPEG-2 et seulement un des codecs évolués à la fois. On suppose que le SVD voudra découvrir quel codec évolué est nécessaire pour le système auquel il est rattaché et qu'il configure de façon appropriée le décodeur au moment de l'amorçage. Cela pourrait impliquer le téléchargement du micrologiciel approprié ou l'activation du micrologiciel résident approprié.

On s'attend à ce qu'aucun aspect caché du codec évolué non utilisé (c'est-à-dire, des structures matérielles ou du code du micrologiciel) n'enfreigne les droits de propriété intellectuelle (IPR) qui se rapportent à ce codec. Les IPR ne seraient utilisés que lorsque et pour autant que le codec évolué serait activé par l'opérateur. Cette exigence est nécessaire pour que les fournisseurs d'OEM de SVD conformes à NG-STB-A ainsi que les câblo-opérateurs qui développent de tels appareils ne soient pas obligés de payer des redevances de licences de IPR à moins qu'ils n'utilisent réellement les algorithmes de codec évolués de remplacement.

En plus des techniques de codage vidéo évoluées, on considérera aussi des schémas de codage audio évolués avec des améliorations significatives par rapport au schéma de codage audio actuellement déployé.

6.3.6 Environnement logiciel de client vidéo

Tous les SVD conformes à NG-STB-A seront fournis avec une mémoire et des ressources de processeur suffisantes pour être capables de faire fonctionner le micrologiciel des Recommandations UIT-T de la série J.200. Le micrologiciel PEUT être résident ou être téléchargé sur l'appareil. Il est prévu que le micrologiciel fonctionne sur les SVD sous réserve de la négociation de termes de licence raisonnables. Les Recommandations UIT-T de la série J.200 fournissent un environnement cohérent pour des applications libres ou liées; celles-là (les applications libres) sont indépendantes de tout canal de programmation particulier, comme un jeu, et celles-ci (les applications liées) sont liées à des canaux de programmation spécifiques tels qu'un lien cliquable sur un affichage d'un film en cours de vision.

Les Recommandations UIT-T de la série J.200 comprennent un ensemble d'API pour le composant de micrologiciel d'une solution logicielle. Les Recommandations UIT-T de la série J.200 spécifient un ensemble de fichiers de demande de permission, une image de code à signature numérique et une application de surveillance pour diverses questions de sécurité et de conflit de ressources.

La Figure 4 décrit l'architecture logicielle dans les Recommandations UIT-T de la série J.200 qui hébergent des équipements CPE de vidéo.

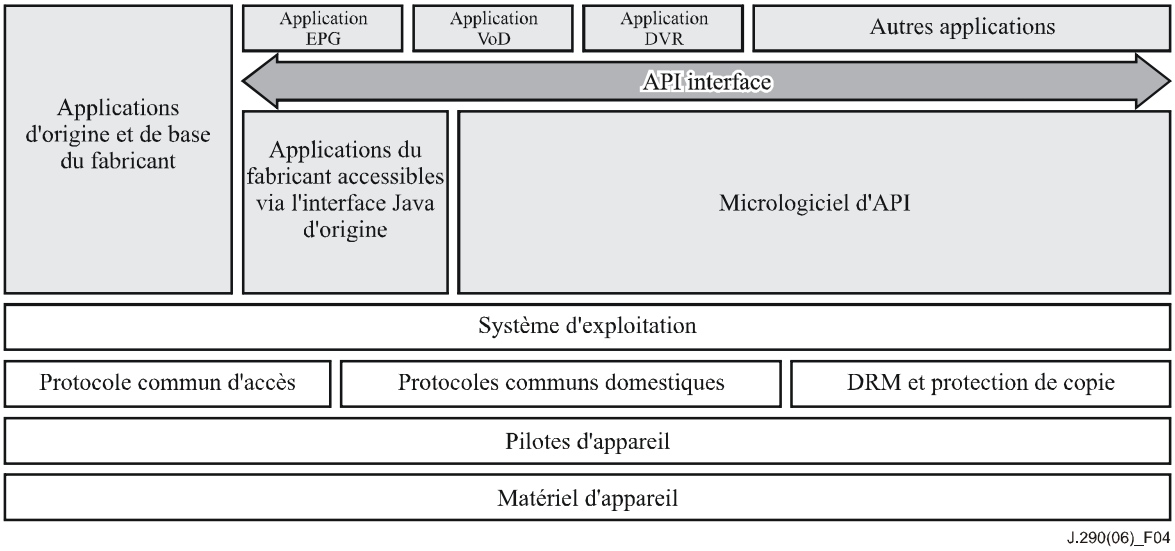


Figure 4 – Architecture de logiciel d'équipement CPE vidéo

Le modèle de référence identifie deux catégories d'applications d'origine que le fabricant de l'appareil inclura vraisemblablement dans son produit. Les applications de fabricant décrites comme "d'origine et de base" auront un accès direct au système de fonctionnement et outrepassent la couche de micrologiciel des Recommandations UIT-T de la série J.200 pour s'interfacer directement à l'interface d'hôte et d'utilisateur; par exemple, cela pourrait inclure de donner à l'utilisateur la capacité à choisir entre les modes de fonctionnement en diffusion sur le câble et par ondes hertziennes. L'autre catégorie d'applications de fabricants est conçue comme "accessible via l'interface native Java" (JNI, *Java native interface*). Ces applications seraient aussi fournies par le fabricant et seraient mappées par l'intermédiaire de la couche micrologicielle des Recommandations UIT-T de la série J.200.

Le comportement par défaut pour les Recommandations UIT-T de la série J.200 serait de passer ces applications à travers l'interface d'hôte et d'utilisateur; cependant, les Recommandations UIT-T de la série J.200 devraient avoir la capacité de modifier le comportement par défaut ou même de supplanter l'application OEM par une nouvelle application, par exemple, par une application téléchargée par un utilisateur final par dessus les Recommandations UIT-T de la série J.200. Un exemple de telles applications d'origine par défaut pourrait être la commande d'augmentation/diminution du volume sonore sur un DTV. Normalement, les Recommandations UIT-T de la série J.200 devraient permettre que l'application du fabricant ait le contrôle, mais dans l'éventualité d'une alerte pour un sinistre, le micrologiciel d'application d'alerte aux sinistres de l'opérateur du réseau fonctionnant au sommet des Recommandations UIT-T de la série J.200 pourrait reprendre le contrôle du volume sonore.

Les applications téléchargeables fonctionnent dans l'environnement des micrologiciels des Recommandations UIT-T de la série J.200. Des exemples d'applications qu'un opérateur de réseau PEUT choisir de télécharger incluraient le plus vraisemblablement un noyau dur d'applications essentielles: guide électronique des programmes (EPG), vidéo à la carte (VoD) et autres applications du câble comme la prise en charge d'applications d'en-tête de réseau. Avec cette dernière option, l'affichage visuel de l'interface de sortie de l'utilisateur est utilisé comme une image vidéo de trame fixe à l'en-tête de réseau pour geler l'affichage des trames par l'équipement CPE, ou autrement cela PEUT être implémenté comme un flux vidéo en envoi individuel si la bande passante le permet et si l'interface d'utilisateur implique des composants mobiles. La prise en charge de l'interface d'entrée d'utilisateur consisterait à relayer l'interaction d'utilisateur avec la commande

à distance vers l'en-tête de réseau pour communiquer un choix de menu, ou une sélection par un curseur, à partir de l'affichage.

{texte pour information: à côté des API de la série J.200, des API fondées sur Internet telles que html, java et flash DEVRAIENT être applicables pour des applications assez simples. Ces API DEVRAIENT faire l'objet de négociations pour des conditions de licence raisonnables. Le travail en cours de définition des relations du format de contenu, par exemple HTML, FLASH avec l'architecture J.200, pourra être ajouté par la suite.}

On s'attend à ce qu'il y ait des différences entre les appareils d'équipement CPE en termes d'applications et de capacités prises en charge. Par exemple, les appareils de haut de gamme prendront en charge certaines applications, telles que DVR, qui sont absentes sur les équipements CPE d'entrée de gamme.

6.3.6.1 Améliorations de la sécurité

Le logiciel client de la prochaine génération sera un composant critique de l'architecture de sécurité globale du système. Dans la mesure où le système de sécurité pour l'authentification au moment de l'amorçage, l'authentification du pilote de l'appareil et la sécurité du noyau du système ne sont pas couvertes dans les spécifications des Recommandations UIT-T de la série J.200, et dans la mesure où cela crée un risque de compromettre la sécurité, il sera important de spécifier les autres exigences de sécurité pour toute la solution de logiciel client de la prochaine génération. La solution suggérée comporte un chargeur d'amorce de confiance non modifiable qui est le fondement de tous les téléchargements et toutes les mises à jour de logiciel. Elle comporte aussi l'authentification de tous les éléments de logiciel y compris la mise en œuvre des Recommandations UIT-T de la série J.200, du noyau du système des pilotes d'appareils, des applications des Recommandations UIT-T de la série J.200 et de tous les autres logiciels au moment de l'amorçage et durant le téléchargement. De plus, elle inclut la technologie de noyau de confiance qui crée un environnement de confiance pour la commutation du contexte de tâche. Toute la sécurité de logiciel client fournie par le câble dans l'équipement CPE DEVRAIT être liée à la confiance dans le système d'accès conditionnel plutôt que de créer un modèle de confiance autonome séparé.

6.3.6.2 Interface évoluée d'utilisateur

Les Recommandations UIT-T de la série J.200 et les applications fondées sur l'en-tête de réseau peuvent être employées ensemble avec d'autres éléments de NG-STB-A pour fournir des interfaces d'utilisateur évoluées avec les nouveaux services. Comme l'architecture de réseau de la prochaine génération prendra en charge une variété beaucoup plus grande de services ainsi qu'une introduction de service rapide, il sera important d'avoir des interfaces d'utilisateur intuitives qui soient pratiques et dont l'utilisation soit facile à apprendre.

Le modèle de référence NG-STB-A est destiné à prendre en charge des concepts élargis d'interface d'utilisateur de matériel et de logiciel au-delà du clavier de commande à distance de base, tels que:

- des commandes à distance évoluées avec de nouveaux appareils d'entrée tels que des blocs à effleurement, des appareils de pointage et des claviers définis par logiciel;
- des commandes à distance, ou autres appareils auxiliaires avec des écrans s'ajoutant à l'écran d'affichage principal pour permettre les messages, les pages de la toile, la navigation, l'aide, ou des informations de contrôle à afficher à une ou plusieurs personnes dans la même pièce;
- des appareils d'entrée/sortie atypiques tels qu'un rétrocontrôle de puissance sur les commandes de jeux, des appareils vibrants pour taper un contenu de programme, et des générateurs d'effets spéciaux qui présentent des effets sonores en trois dimensions.

Afin de prendre en charge de tels ajouts, on définira un port d'expansion standard (voir le paragraphe 7) qui puisse être employé comme interface avec un appareil d'interface d'utilisateur évolué externe.

6.4 Architecture de services IP multimédia

Le cœur des services IP multimédia inclut des services de données à grande vitesse et de la téléphonie fondée sur la voix sur IP. On prévoit que les offres multimédias interactives fondées sur IP fournies par le câble vont croître de façon à inclure, à titre d'exemples représentatifs: le partage et l'affichage de photographies fixes de haute qualité, de la visiophonie et de la visioconférence animées, de la présence améliorée pour les supports de communication émergeants, des outils de partage d'applications et de collaboration et des jeux multijoueurs en ligne. L'architecture de services multimédia sur IP de la prochaine génération servira de plateforme d'activation d'une large série d'applications visant une plus large gamme d'appareils d'équipement CPE et un ensemble plus riche de services.

De nombreux services IP multimédias sont sensibles au délai du réseau, à la gigue et au débit; le NG-STB-A active le traitement de la qualité de service de bout en bout pour le trafic des données associé aux services IP multimédias livrés aux appareils dans les domaines de réseau domestique. En plus de la prise en charge de la qualité de service, il répond aux besoins d'approvisionnement et de surveillance de service, à la gestion des droits numériques et à la traversée des traductions d'adresse de réseau (NAT, *network address translation*).

Les services IP multimédias sont livrés sur des canaux IP transparents, à la fois:

i) entre l'en-tête de réseau et les locaux d'abonné;

ii) au sein des domaines de réseau domestique qui impliquent un contenu protégé (Domaine de service autorisé, ou ASD) et qualité de service gérée (Domaine de service garanti, ou GSD).

Les couches de réseau physiques ne sont pas définies par NG-STB-A mais pourraient inclure le trafic IP sur des réseaux domestiques coaxiaux ou non coaxiaux, par exemple, CAT5, HomePlug, ou sans fil. Alors que NG-STB-A pourrait pour les différents types de services prendre en charge toutes les couches Physiques, il y a en général une préférence pour les couches PHY qui prennent en charge la qualité de service et offrent des capacités de plusieurs canaux haute définition (HD).

Les points de terminaison IP multimédias potentiels pourraient inclure des appareils d'abonné des Recommandations UIT-T de la série J.200 connectés au réseau coaxial, des ordinateurs personnels partageant une connexion de données DOCSIS à haut débit sur le réseau de données domestique et des appareils personnels sans fil assurant des fonctions de mobilité et de confort au sein du domicile. Un échantillonnage des applications IP multimédias prospectives hébergées sur ces équipements CPE permet de noter:

- les ordinateurs personnels sur le réseau de données IP domestique configurés comme serveurs de support physique auxquels accèdent les équipements CPE de vidéo sur le réseau IP domestique pour une présentation de musique, vidéo, ou images fixes de haute fidélité;
- l'interface de consoles de jeu avec à la fois les équipements CPE de vidéo et les réseaux domestique et d'accès de données facilitant la participation à des sessions de jeu à plusieurs joueurs;
- des terminaux de visiophonie et des appareils de communication mobiles et sans fil recevant un soutien réseau fondé sur la qualité de service améliorée tout en partageant l'infrastructure avec d'autres services au sein du domicile;
- des applications Internet fournissant l'affichage de l'identifiant de l'appelant téléphonique, la localisation d'appel et la restitution de messages sur les appareils vidéo et ordinateurs personnels de l'abonné.

NG-STB-A prendra en charge les extensions au réseau par câble qui permettront aux câblo-opérateurs d'entrer en partenariat et/ou en compétition avec les fournisseurs de services de voix et de données sans fil, offrant des services tels que:

- des services d'échange de messages unifiés qui intègrent la ligne filaire avec la numérotation universelle sans fil, la messagerie vocale, la télécopie, le renvoi d'appel vocal, la messagerie électronique, l'échange de message support enrichi et les réseaux privés virtuels;
- la mobilité IP et l'itinérance entre les services par câblo-modem et les bornes d'accès sans fil WiFi des réseaux publics;
- déployer des points d'accès sur des implantations extérieures pour fournir une couverture en WiFi ou autres technologies sans fil dans des locaux publics.

6.4.1 Transport

La livraison de services multimédias se fera sur IPv4 en utilisant à la fois l'envoi individuel et la distribution. La prise en charge de IPv6 sera nécessaire pour assurer les capacités futures de NG-STB-A alors que plus d'appareils de réseau seront connectés au réseau.

Les réseaux de zone régionale seront fondés sur IP et on prévoit qu'ils seront portés sur des technologies de Gigabit Ethernet, par exemple, 1GigE et 10GigE. Il est vraisemblable qu'une infrastructure de réseau de zone régionale courante sera partagée entre les architectures de services vidéo et IP multimédias.

Le plan de NG-STB-A ne prescrit pas de couches Physiques (PHY) spécifiques de réseau de données domestique. Cependant, toute couche Physique convenable DOIT satisfaire à deux exigences:

- La couche Physique DOIT fournir la transparence IP pour les services dans tous les domaines de réseau domestique.
- Pour les services qui au sein du domaine de réseau domestique, impliquent la qualité de service, la couche Physique DOIT être aussi capable de gérer la qualité de service.

Les abonnés PEUVENT sélectionner tous les choix qui sont transparents au regard d'IP. Cependant, les combinaisons PHY/MAC qui peuvent avoir la qualité de service gérée par les protocoles NG-STB-A fourniront une meilleure relation à l'utilisateur. Et aussi, tous les choix de couche Physique n'auront pas la capacité de prendre en charge les applications à forte bande passante comme les flux multiples à haute définition. Des exemples de couche Physique IP transparente qui pourraient être utilisés avec les systèmes NG-STB-A incluent la ligne téléphonique WiFi 802.11a/b/g sans fil, les courants porteurs en ligne, le câblage par paire coaxiale et torsadée (CAT5).

6.4.2 Qualité de service de bout en bout

L'expérience globale qu'éprouvera un utilisateur dépend du traitement de bout en bout subi par le trafic que reçoit un service du réseau. Par conséquent, il est important de viser les frontières entre les segments du réseau pour s'assurer que la coordination appropriée est apportée à la gestion de la qualité globale de la session.

Une approche pour considérer le réseau multimédia de la prochaine génération est de distinguer trois grands segments du réseau: le réseau de zone régionale (RAN, *regional area network*), défini comme le cœur de réseau, qui consiste en un pont entre la source du contenu ou du service et le réseau d'accès; le réseau d'accès, défini comme le segment HFC qui connecte les éléments CMTS et câblo-modem (CM); et finalement le réseau domestique, grossièrement défini comme la topologie de réseau tout entière (ignorante de la couche Physique) derrière le câblo-modem au sein du foyer.

NG-STB-A incorpore par référence les mécanismes développés dans les projets IPCablecom et IPCable2Home; IPCablecom multimédia (IPCMM) se focalise sur le segment d'accès, alors que IPCable2Home vise le segment du réseau domestique. De plus, NG-STB-A définit un pont ou une passerelle entre le réseau coaxial du foyer (normalement une extension à partir du cordon coaxial qui connecte les télévisions et les autres appareils de vidéo à l'intérieur du foyer) et les réseaux de données domestiques (normalement propriété de l'abonné, souvent différents du coaxial, qui prennent en charge des applications centrées sur l'ordinateur individuel).

6.4.2.1 Qualité de service de réseau de zone régionale

De nombreux réseaux de zone régionale (RAN) sont en train d'évoluer pour distinguer et acheminer les paquets sur des chemins divergents (avec les mesures de qualité associées) sur la base du marquage des paquets. IPCablecom multimédia prend en charge les stratégies DiffServ sur le RAN en permettant à l'opérateur de réseau d'associer un point de code des services différenciés (DSCP, *DiffServ code point*) particulière à chaque flux de service amont. Tous les paquets sortant de ce flux seront marqués avec ce DSCP avant d'entrer dans le RAN. De même, IPCablecom multimédia inclut la capacité à distinguer le trafic vers l'aval entrant reçu en provenance du RAN et à placer ce trafic sur un flux de service approprié sur la base des marquages DSCP (aussi bien que les mécanismes conventionnels d'adresse d'origine et de terminaison IP et de couche MAC). Les architectures respectives ont été décrites dans la Rec. UIT-T J.174.

Bien que les architectures de réseau hors des RAN soient en dehors du domaine d'application du projet NG-STB-A, il y a des bénéfices potentiels reconnus dans les normes d'échange de trafic entre opérateurs pour les contenus et les services au delà des arrangements actuels d'échange de trafic pour le trafic de données à haut débit. Par exemple, la capacité à garder les appels VoIP "en interne" de bout en bout pourrait procurer des économies significatives. Ceci est particulièrement vrai dans les zones géographiques où les câblo-opérateurs ont des RAN adjacents. De tels arrangements d'échange de trafic entre opérateurs incluraient des interfaces matérielles et de protocole et des systèmes de "règlement" convenables.

6.4.2.2 Qualité de service de réseau d'accès

La condition préalable fondamentale de la qualité de service du réseau d'accès est la capacité à fournir la gestion de la bande passante pour le trafic prioritaire.

Une approche de la gestion est de garantir la bande passante nécessaire pour les services spécifiques sur les segments d'accès; une portion de la bande passante disponible est constamment allouée au trafic prioritaire. Le trafic est distingué par le marquage du paquet de qualité de service et passé à travers les canaux alloués individuellement. La méthode de mise en file d'attente en fonction de la priorité est aussi une solution efficace pour s'assurer de la qualité de service du réseau d'accès.

Le trafic affecté de priorités reçoit la priorité pour l'utilisation des ressources de bande passante, ce qui conduit à prévenir la latence du réseau, la gigue et la dégradation du débit.

Alors que plusieurs éléments et interfaces clés du réseau ont été identifiés et profilés dans la spécification IPCablecom multimédia, Rec. UIT-T J.179, aucun protocole d'établissement de session n'est défini. NG-STB-A reconnaît la prévalence de SIP dans nombre des applications multimédias d'aujourd'hui. Un des objectifs de l'architecture est de prendre en charge une large variété d'applications et leurs mécanismes d'établissement de session associés. NG-STB-A prendra implicitement en charge SIP en plus des autres mécanismes d'établissement de session spécifiques des applications.

6.4.2.3 Qualité de service de réseau domestique

Les spécifications IPCable2Home sont destinées à fournir une architecture fondée sur le protocole Internet (IP, *Internet protocol*) pour les services de réseau domestique gérés.

L'architecture de réseau domestique NG-STB-A est partiellement définie par les aspects existants de [b-UIT-T J.192] sur IPCable2Home. Cependant, la version actuelle de [b-UIT-T J.192] n'inclut que la qualité de service à priorité à travers le réseau domestique vers les appareils qui incluent le logiciel de point de limite de qualité de service IPCable2Home. {texte pour information: Afin de pleinement prendre en charge les objectifs de qualité de service de NG-STB-A, [b-UIT-T J.192] aura besoin d'une extension pour fournir un contrôle des paramètres de qualité de service en établissant un pont entre UPnP et IPCablecom multimédia.}

Les capacités de qualité de service PEUVENT être fournies OU PAS au client terminal, selon les technologies de couche deux employées et la localisation du client dans le réseau. Du point de vue de la qualité de service, le client peut résider dans un des deux domaines de réseau domestique, dans le domaine de service garanti (GSD) ou en dehors du GSD. Lorsqu'un client réside dans le GSD, il a les capacités de qualité de service à sa disposition pour établir non seulement la qualité de service du réseau domestique, mais aussi la qualité de service résidentielle sur le réseau d'accès pour le traitement de la QS de bout en bout. Pour les clients qui sont en dehors du GSD, la qualité de service résidentielle n'est pas disponible; cependant, le client PEUT encore recevoir le traitement de la qualité de service d'accès et de RAN à travers la signalisation de niveau application. Ce type de client est très vraisemblablement un appareil ordinaire insensible à la qualité de service qui peut encore bénéficier d'un traitement de la qualité de service de niveau accès.

Pour faire un pont entre les réseaux d'accès et domestique, l'appareil IPCable2Home peut tirer parti du mécanisme robuste de classification de paquets introduit dans DOCSIS 1.1 et transporté dans IPCablecom multimédia. Il est possible d'identifier et de transmettre les paquets sortant du segment de réseau domestique sur la base d'un certain nombre de caractéristiques distinctives, y compris des adresses et ports d'origine et de terminaison IP et de couche MAC, des marquages DiffServ/ToS et des étiquettes de VLAN 802.1q.

IPCable2Home 1.1 [b-UIT-T J.192] a actuellement adopté un schéma de marquage des paquets et de mise en file d'attente en fonction de la priorité fondé sur 802.1q. {texte pour information: à l'avenir, on prévoit l'alignement entre les capacités de qualité de service de IPCable2Home et celles définies par UPnP.}

Pour les appareils qui résident dans le GSD, les liens du réseau domestique entre la passerelle et l'appareil du GSD devront prendre en charge la qualité de service paramétrée. {texte pour information: De plus, l'appareil client devra se conformer aux exigences de point frontière de qualité de IPCable2Home (qui sont un surensemble des exigences des appareils UPnP).}

NG-STB-A fournira des interfaces de niveau application permettant aux services clients de demander des ressources de bande passante et de contenu. Le segment de réseau spécifique au sein duquel résident ces ressources déterminera quelle interface recevra l'accès. Il est souhaitable de conserver un langage commun afin de simplifier les exigences d'application. {texte pour information: des exemples de ces interfaces PEUVENT inclure IPCablecom multimédia avec des extensions SOAP/XML, IPCable2Home avec la prise en charge de la qualité de service UPnP, et les extensions d'application de réseautage domestique des Recommandations UIT-T de la série J.200.} Ces améliorations fourniront un mécanisme standard pour l'interface d'application.

6.4.3 IPv6

Pour assumer les développements de grande échelle envisagés, la prise en charge d'IPv6 sera nécessaire pour les clients réseaux. Cette exigence est nécessaire pour empêcher le naufrage des investissements en capital et pour assurer un espace d'adresse assez large pour accepter des services de télémétrie fondés sur des utilitaires en plus d'autres services de plus petit marché. Alors qu'une stratégie de coexistence et de transition pour IPv6 n'a pas encore été définie, la prise en charge d'IPv6 peut être interprétée comme améliorable par le logiciel. La mise à jour de matériel NE DEVRAIT PAS être nécessaire pour la prise en charge de IPv6 pour les appareils NG-STB-A (ceci PEUT n'être pas vrai pour les appareils ordinaires existants).

6.4.4 Sécurité et confidentialité

Dans le but de fournir un service de télémétrie, il est impératif de prendre en considération la protection de la confidentialité de l'utilisateur et donc de sécuriser les données de l'utilisateur. NG-STB-A fournira des mécanismes pour permettre à un point d'extrémité d'authentifier la demande et de sécuriser la réponse du point d'extrémité à de telles demandes. Les caractéristiques suivantes sont exigées pour les applications de télémétrie et de contrôle sécurisées:

- tous les points d'extrémité doivent avoir des identités définies en usine;
- les mécanismes de chiffrement sécurisés (c'est-à-dire, AES, 3DES) doivent être conservés à travers tous les éléments réseau et client de réglage et de passerelle;
- toutes les communications de gestion (XML, SNMP) doivent pouvoir être sécurisées.

6.5 Architecture de réseau domestique

Le présent paragraphe se rapporte au "réseautage domestique" au sein de et entre les réseaux qui vont exister dans le foyer.

Alors que de nos jours de nombreux foyers ont un ou plusieurs réseaux domestiques, ils ne sont en général pas bien intégrés avec le système du câble et ne fournissent qu'un soutien limité au multimédia (par exemple, la livraison au mieux de vidéos de faible qualité par opposition à la livraison garantie de vidéo de haute définition). L'extension des services fournis par le câblo-opérateur et des contenus sur les réseaux domestiques permettra à une plus grande variété d'appareils de participer et de fournir de nouvelles opportunités de modèles de services et d'affaires originaux.

L'architecture de réseau de la prochaine génération inclura une architecture résidentielle complète qui prendra en charge le transfert sans rupture du trafic entre les appareils sur le câble en dehors de l'implantation (par exemple, DOCSIS, MPEG-TS) et divers segments/technologies de réseau domestique. NG-STB-A prendra en charge divers modèles d'application au sein du réseau domestique. Un de ces modèles a les Recommandations UIT-T de la série J.200 à la fois sur les appareils client et serveur (par exemple, un SVD de bas de gamme communiquant avec un SVD de haut de gamme). {texte pour information: De plus, NG-STB-A PEUT aussi définir des interfaces d'application, telles que des interfaces d'utilisateur UPnP distantes, qui seraient indépendantes du système d'exploitation et du micrologiciel sur certains appareils.}

Des exemples de services et d'applications qu'une telle architecture de réseautage domestique prendrait en charge incluent:

- un appareil vidéo d'abonné (SVD) de bas de gamme pourrait accéder à un SVD de haut de gamme fonctionnant comme magnétoscope numérique (DVR) sur le réseau coaxial pour regarder le contenu mémorisé sur le pilote matériel du SVD de haut de gamme. Et donc, le SVD de bas de gamme accèderait à la fonction application DVR de l'appareil de haut de gamme sans supporter le coût d'un pilote matériel supplémentaire et fournirait aussi une vision unifiée des contenus mémorisés dans les multiples localisations du foyer;
- un SVD d'entrée de gamme avec une mémoire et une puissance de traitement limitées pourrait accéder aux applications prises en charge par les Recommandations UIT-T de la série J.200 qui fonctionnent sur un SVD de haut de gamme et obtenir les fonctionnalités d'application comme si l'application résidait sur le SVD d'entrée de gamme;
- un SVD sur le réseau coaxial domestique pourrait accéder à des contenus de supports vidéo ou multimédias résidents sur un ordinateur personnel situé sur le réseau domestique non coaxial, ou vice versa;

- le trafic de messages pourrait passer entre les réseaux domestiques coaxial et non coaxial pour prendre en charge des applications telles que l'affichage de l'identifiant de l'appelant sur une télévision connectée à un SVD ou peut-être afficher le sommaire de la boîte de réception de la messagerie électronique sur l'écran d'une télévision connectée à un SVD.

Le trafic le plus exigeant du réseau domestique en termes de bande passante est vraisemblablement le contenu de télévision en haute définition (TVHD). Il y a une préférence pour que les couches Physiques fournissent la capacité de lecture en continu en temps réel de plusieurs canaux TVHD simultanés au sein de et entre divers segments et technologies de réseau domestique.

Le projet IPCable2Home a défini un élément de passerelle de réseautage domestique pour établir un pont entre le réseau DOCSIS du câblo-opérateur et le ou les réseaux domestiques de l'abonné. Cette passerelle est destinée à être approvisionnée et gérée de façon sécurisée et, de plus, elle peut affecter une priorité aux paquets qui passent entre les segments DOCSIS et le réseau domestique. L'architecture de réseau domestique de la prochaine génération sera le complément des éléments de base définis par le projet IPCable2Home avec les considérations nécessaires pour transporter des contenus de haute qualité (par exemple, des contenus exigeant la gestion des droits et une mise en application stricte de la qualité de service) au sein de et entre chaque réseau, pour gérer les divers segments de LAN, et pour admettre les appareils clients sur le réseau.

6.5.1 Eléments et domaines d'architecture générale

Un élément de passerelle étend les fonctionnalités des services de portail de IPCable2Home. Cet élément de passerelle adapte le ou les segments de réseau domestique à la couche MAC et éventuellement au réseau MPEG-TS; sa fonction inclut de transférer du trafic parmi et entre les divers segments et technologies de réseau domestique. La passerelle PEUT avoir de nombreuses implémentations physiques, du modem ou câblo-modem xDSL incorporé aux combinaisons modem/NAT, jusqu'aux implémentations au sein d'un SVD haut de gamme.

Comme le montre la Figure 5, la passerelle donne la capacité de prendre en charge plusieurs technologies de transport, ce qui permet au trafic de se déplacer sans rupture tout autour des locaux dans un environnement IP qui ignore le transport. Le trafic sur le réseau domestique PEUT inclure diverses combinaisons de contenu, de contrôle de contenu, de navigation, et de partage d'applications pour permettre les interactions entre les données, la vidéo et les services IP multimédias.

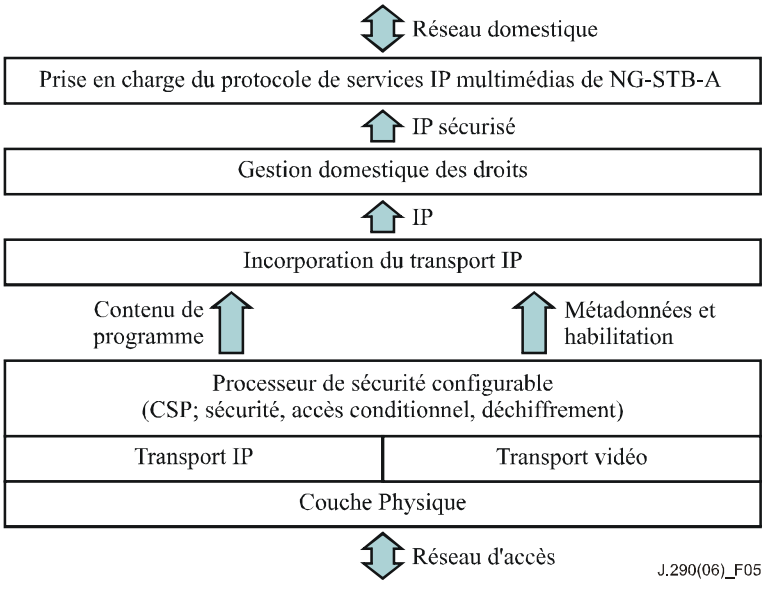


Figure 5 – Architecture de communications de passerelles

Les diverses technologies de réseau domestique ne sont pas spécifiées à la couche de commande de moyen d'accès (MAC) et à la couche Physique. Les candidats pour ces couches incluent toute couche connue ou future, capable de prendre en charge le protocole Internet (IP) à grande vitesse. {texte pour information: Des exemples de telles couches incluent Ethernet sur CAT5, le courant porteur en ligne HomePlug, PNA domestique, MoCA, et 802.11a/b/g/n.} Il est vraisemblable que de nombreux foyers vont utiliser plusieurs technologies de réseau domestique pour satisfaire différents besoins.

Les divers segments de réseau domestique sont supposés être fondés sur IP; en plus de fournir une prise en charge continue d'applications de données à grande vitesse, IP fournit une couche d'interfonctionnement normalisée et omniprésente à travers de nombreux appareils et technologies du réseau.

Comme le montre la Figure 6, au sein de l'architecture de communications du réseau domestique, il y a des domaines fonctionnels qui diffèrent à la fois par la gestion de la qualité de service et en termes de gestion des droits (protection du contenu).

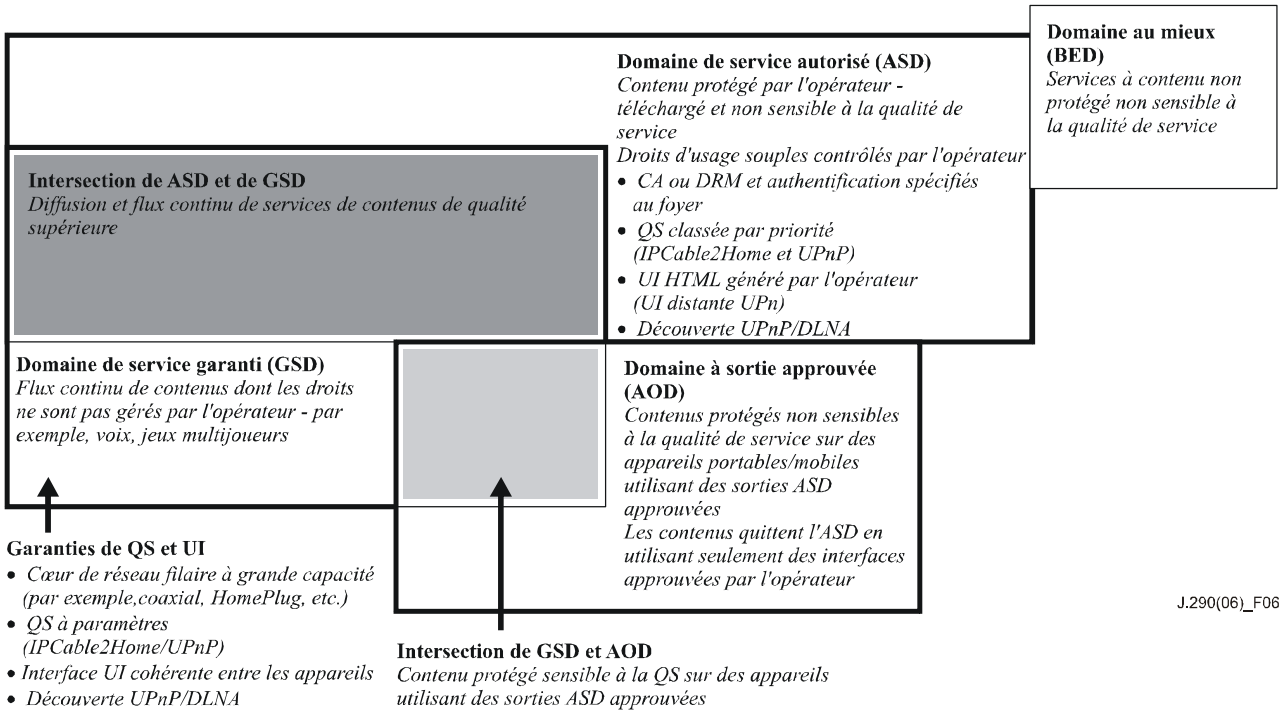


Figure 6 – Domaines du réseau domestique – Aperçu général

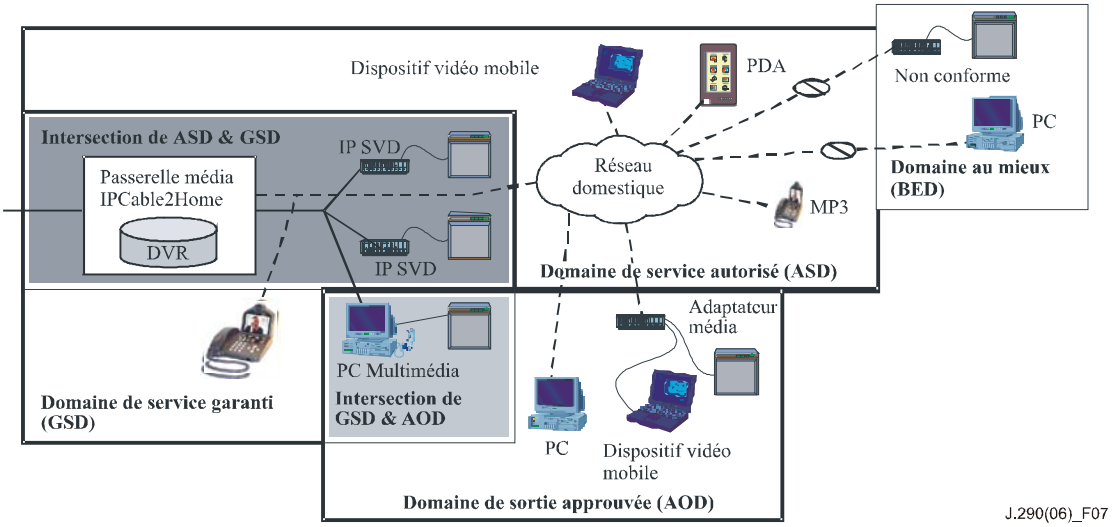


Figure 7 – Domaines du réseau domestique – Exemples

Domaine de service garanti (GSD, *guaranteed service domain*)

Si les garanties de qualité de service peuvent être maintenues depuis l'en-tête de réseau jusqu'à un client, le client est considéré comme faisant partie du domaine de service garanti.

Pour assurer la qualité de service garantie, le client DOIT prendre en charge la signalisation de qualité de service appropriée: la technologie de réseautage domestique à laquelle est connecté le client DOIT être capable de fournir la garantie pour les paramètres de qualité de service nécessaires, tels que la bande passante, la gigue et le délai, et il DOIT avoir suffisamment de capacités pour porter plusieurs flux de haute définition. {texte pour information: des exemples de technologies qui sont destinées à satisfaire ces exigences à l'avenir sont des technologies filaires fondées sur le coaxial (MoCA), les courants porteurs (HomePlug) et la ligne téléphonique (HPNA 2.0).}

{texte pour information: la passerelle domestique DOIT prendre en charge la signalisation de qualité de service appropriée et les raccords nécessaires pour faire le pont entre la qualité de service domestique et la qualité de service du réseau d'accès, et elle DOIT implémenter la fonction de qualité de service d'IPCable2Home tandis que l'appareil client DOIT implémenter la qualité de service UPnP. La fonction de qualité de service de IPCable2Home est un superensemble de la qualité de service de UPnP.} Et donc, un client donné PEUT être dans le GSD lorsqu'il est connecté à un segment de réseau dans le foyer et n'être pas dans le GSD lorsqu'il est connecté à un autre. De même, un segment donné aura vraisemblablement certains clients qui sont dans le GSD et certains autres ne le seront pas, sur la base du niveau de prise en charge de la qualité de service dans chaque appareil et application client.

{texte pour information: tous les appareils et le contenu mémorisé dans ce domaine peuvent être découverts en utilisant un mécanisme défini par UPnP/DLNA *(digital living network alliance*, précédemment appelé *digital home working group* ou DHWG). La passerelle domestique agit comme un serveur de découverte centralisé pour le LAN domestique. Le câblo-opérateur peut accéder à ces informations à travers une interface de MIB définie par IPCable2Home.}

Les appareils dans le GSD seront capables de recevoir des services de contenu sensibles à la qualité de service tels que la voix sur IP, des jeux interactifs à plusieurs joueurs et la visiophonie sur IP. Ces contenus PEUVENT contenir ou non une protection de contenu contre les tiers fondée sur DRM.

Domaine de service autorisé (ASD, *authorized service domain*)

Les appareils dans ce domaine sont capables de s'authentifier et de prendre en charge les droits d'utilisation du contenu selon ce qui est défini par l'opérateur du réseau. Ce segment inclut des appareils qui se conforment à la gestion des droits numériques domestiques, comme décrit ci-dessous.

Il n'est pas nécessaire de fournir la qualité de service aux appareils dans le domaine ASD. {texte pour information: cependant, les appareils clients PEUVENT être capables de prendre en charge de la qualité de service classée par priorité et DEVRAIENT donc implémenter la signalisation de qualité de service de UPnP.} La technologie de réseautage domestique DEVRAIT être capable de prendre en charge la qualité de service classée par priorité, en particulier dans les segments où sont lus en continu des contenus sensibles au délai de latence et à la bande passante.

{texte pour information: tous les appareils et les contenus mémorisés dans ce domaine peuvent être découverts en utilisant le mécanisme de découverte défini par UPnP/DLNA.}

Les appareils dans le domaine ASD seront capables de recevoir des services protégés à contenu non sensible à la qualité de service comme de la musique et des vidéos en différé ou à bas débit.

Domaine de sortie approuvée (AOD, *approved output domain*)

Dans ce domaine, les appareils sont connectés à l'ASD en utilisant des interfaces de sortie approuvées par l'opérateur. Lorsque le contenu circule de l'ASD vers l'AOD, les règles d'utilisation spécifiées par l'opérateur de réseau sont imposées à travers l'interface. Actuellement, 5C sur 1394 et HDCP sur DVI (ou HDMI, Interface multimédia haute définition) sont des interfaces de sortie numérique approuvées pour le développement du câble en Amérique du Nord. Par exemple, une interface possible qui PEUT être établie est une interface DRM qui permet la communication des règles de contenu et d'usage à un système DRM tiers, séparé du DRM de l'opérateur de réseau.

Un câblo-opérateur abandonne le contrôle direct sur le contenu une fois qu'il est transféré sur l'AOD. C'est une différence clé entre le domaine de service autorisé et le domaine de sortie approuvée.

Un appareil PEUT recevoir du contenu provenant de l'ASD sur une interface approuvée. Il n'y a pas d'obligation que l'appareil satisfasse aucune autre exigence en rapport avec la qualité de service et la découverte des appareils. Cependant, certains appareils d'AOD seront capables de participer au domaine de service garanti car il se rapporte à la découverte d'appareil et à la qualité de service. Tous les appareils dans l'AOD seront capables de recevoir des contenus protégés non sensibles à la qualité de service qui ont des restrictions d'utilisation mises en application par l'opérateur dépendantes de l'interface de sortie approuvée.

Des supports amovibles tels que des DVD enregistrables, des cartes flash et des CD-R seront normalement trouvés dans l'AOD.

Domaine au mieux (BED, *best effort domain*)

Les appareils et segments de couche Physique qui ne se conforment pas aux exigences des trois domaines définis ci-dessus PEUVENT toujours être découverts et participer à des services qui n'exigent pas de protection du contenu ou de qualité de service garantie.

Intersection de GSD et ASD

Les domaines GSD et ASD sont indépendants; un appareil peut n'appartenir à aucun des deux, à l'un ou à l'autre ou à tous les deux. Les appareils qui appartiennent à la fois à GSD et ASD peuvent fournir les garanties de qualité de service et peuvent s'authentifier et prendre en charge la DRM domestique. De tels appareils représentent un plus haut niveau de conformité et PEUVENT être capables de recevoir des contenus de valeur élevée avec des restrictions d'utilisation mises en application par l'opérateur du réseau.

Intersection de GSD et AOD

Les domaines GSD et AOD sont indépendants; un appareil peut n'appartenir à aucun des deux, à l'un ou à l'autre ou à tous les deux. Les appareils qui appartiennent à la fois à GSD et AOD peuvent fournir les garanties de qualité de service pour le contenu qui s'écoule de l'ASD vers l'AOD sur des interfaces approuvées. De tels appareils seront capables de recevoir des contenus protégés sensibles à la qualité de service avec des restrictions d'utilisation mises en application par l'opérateur du réseau selon les interfaces approuvées.

Exclusivité de ASD et AOD

ASD et AOD s'excluent mutuellement. Un appareil ne peut appartenir qu'à ASD, ou AOD, ou aucun des deux.

Le Tableau 2 résume les diverses exigences fonctionnelles pour les appareils dans les différents domaines.

Tableau 2/J.290 – Exigences fonctionnelles des différents domaines et services offerts

Fonctionnalité[a]	**ASD – Droits d'usage souples contrôlés par l'opérateur de réseau**	**GSD – Garanties de QS, UI cohérente**	**AOD**	**ASD+GSD**	**AOD+GSD**	**BED**
Sécurité	Authentification plus CA ou DRM domestique fondé sur CSP NG-STB-A	Aucune	Sécurité d'interface de sortie approuvée	Authentification et CA ou DRM domestique	Sécurité d'interface de sortie approuvée	Aucune
QS	QS à priorité (QS UPnP) – **Facultative**	QS à paramètres (IPCable2Home ou UPnP)	Aucune	QS à paramètres (IPCable2Home ou UPnP)	QS à paramètres (IPCable2Home ou UPnP)	Aucune
UI cohérent	Souhaité	Oui	Aucune	Oui	Oui	Aucune
Gestion	PS[b] IPCable2Home (pour passerelle) ou BP[c] IPCable2Home (pour client) – **Facultatif**	PS IPCable2 Home (pour passerelle) ou BP IPCable2Home (pour client)	Contrôle de sortie à choix	PS IPCable2Home (pour passerelle) ou BP IPCable2Home (pour client)	PS IPCable2 Home (pour passerelle) ou BP IPCable2Home (pour client)	Contrôle de sortie à choix
Découverte	UPnP/DLNA	UPnP/DLNA	Aucune	UPnP/DLNA	UPnP/DLNA	Aucune
Services	Services de contenu protégé, non sensible à la QS avec toute liberté pour établir les droits d'usage	Services de contenu non protégé, sensible à la QS, par exemple, jeu interactif, voix, visiophone	Services de contenu protégé, non sensible à la QS avec liberté limitée pour établir les droits d'usage	Services de contenu de haute valeur avec pleine liberté pour établir les droits d'usage	Services de contenu protégé, sensible à la QS avec liberté limitée pour établir les droits d'usage	Contenu non protégé, non sensible à la QS

[a] Ce tableau suppose que tous les appareils dans ces domaines ont une interface de réseautage domestique.

[b] PS IPCable2Home inclut les fonctionnalités d'un point de contrôle UPnP.

[c] BP IPCable2Home est un surensemble de la QS UPnP et des autres fonctionnalités UPnP.

[d] Toutes les descriptions d'UPnP et DLNA dans le Tableau 2 sont pour information.

Si la gestion de réseau domestique NG-STB-A est indisponible, les appareils d'équipement CPE NG-STB-A DEVRAIENT être conçus pour continuer à fonctionner, éventuellement à un niveau réduit. Les appareils programmables PEUVENT être conformes en faisant fonctionner certaines applications, et non conformes pour d'autres applications.

Cette structure NG-STB-A proposée anticipe le fonctionnement de clients sécurisés sur ordinateur personnel de sorte que les contenus à gestion des droits puissent être échangés entre les SVD et les PC. Un exemple d'application pourrait être de regarder une vidéo de PC à partir d'un DVR hébergé dans un SVD. Autrement, un PC pourrait jouer le rôle d'un serveur de vidéo ou de musique en permettant l'accès du SVD au contenu du PC. Par exemple, un PC pourrait servir de répondeur domestique évolué, ou des informations sur l'identité d'un appelant pourraient être affichées sur une télévision.

6.5.2 Gestion des droits numériques

Les contenus sont délivrés à chaque SVD au sein du domaine de service autorisé en utilisant le contrôle d'accès géré par l'en-tête de réseau. Chaque SVD inclut la prise en charge d'un protocole d'homologue à homologue avec la protection de copie fournie par la gestion des droits numériques (DRM) du réseautage domestique. Le plan NG-STB-A suppose que chaque appareil comporte des clients sécurisés qui peuvent s'authentifier mutuellement en utilisant des signatures numériques ou une technique d'échange de clés normalisée. Le CSP PEUT fournir des capacités de pontage entre le contrôle d'accès du réseau câblé et la DRM du réseau domestique.

Dans la structure NG-STB-A domestique proposée, un SVD sur le réseau accéderait aux caractéristiques et aux contenus sur n'importe quel autre appareil sur le réseau GSD ou ASD. En employant des algorithmes normalisés pour le chiffrement de contenu au système de gestion des droits (RMS), le RMS doit être capable de prendre en charge plusieurs flux de vidéo pour des sessions d'enregistrement, de lecture en temps réel et de multivision.

Le RMS NG-STB-A sera capable de traduire les états d'habilitation et de protection contre la copie et de transporter ces droits tout au long du réseau domestique. Le RMS NG-STB-A emploiera de nouveaux concepts et technologies dans le domaine de la gestion de clé tout en fonctionnant avec les systèmes ordinaires existants en utilisant les critères de partage de clés ou de reconfiguration. Les clés et les habilitations PEUVENT être traduites à partir des informations de contrôle de copie (CCI, *copy control information*), des ECM et des EMM du flux vidéo pour être chargées directement dans les moteurs de déchiffrement sans exposition dans le moteur de déchiffrement de contenu sur l'appareil du réseau domestique.

Dans le système proposé de gestion des droits domestiques de NG-STB-A, un fichier des droits qui contient les critères d'accès aux divers liants de service et une clé de déchiffrement de contenu seront normalement signés et chiffrés. La clé de contenu serait la clé utilisée pour déchiffrer le contenu et PEUT devoir être changée selon une périodicité variable. Les restrictions d'habilitation et de protection contre la copie devraient être déchiffrées et vérifiées dans l'équipement de CPE par rapport aux critères d'accès du consommateur afin de fournir l'autorisation. Si l'autorisation est accordée, la clé de contenu sera produite par l'élément d'accès conditionnel et utilisée pour déchiffrer le contenu à l'appareil d'équipement de CPE sur le réseau domestique.

Le RMS de NG-STB-A effectuera tous les traitements de génération de clé, de chiffrement, déchiffrement, traitement de signature numérique et algorithmes d'échange de clé à l'intérieur de matériel/logiciel inviolable, qui seront conçus pour empêcher complètement la modification ou la découverte/analyse non autorisée du traitement, des paramètres critiques de sécurité et des clés privées.

6.5.2.1 Liaison CA-DRM

L'accès conditionnel du réseau sera responsable de la gestion du RMS de NG-STB-A. Tous les DRM tiers DOIVENT être approuvés comme sortie acceptable avant que le RMS de NG-STB-A n'effectue le transfert du contenu et des droits. Les DRM tiers seront traités au titre du domaine de sortie approuvée, comme défini plus haut. Pour prendre en charge tout système DRM tiers non associé à l'accès conditionnel du réseau, le RMS NG-STB-A sera utilisé pour traduire les droits dans le DRM tiers. De plus, le RMS NG-STB-A sera utilisé pour authentifier tout appareil DRM tiers avant de partager les informations de contenu et de droits. Le CSP devra soutenir ce processus de transfert.

6.5.3 Sources de contenu et clients

L'architecture de réseau domestique est spécifiée pour aider à l'interopérabilité sans rupture des sources et des clients du contenu. Les mémorisations de contenu (c'est-à-dire, la musique, les bibliothèques de photos et de vidéos) qui existent chez les clients en réseau PEUVENT être découvertes, cataloguées, et envoyées aux autres appareils sur le réseau domestique, et même facultativement offertes aux appareils autorisés en dehors du réseau domestique.

Un objectif clé pour l'architecture de réseau domestique est de rendre possible une plate-forme de réseau domestique pratique et facile à comprendre pour l'utilisateur tout en maintenant l'intégrité des contenus protégés (interdits) au sein du domaine de service autorisé (ASD). Plusieurs hypothèses clé sont incorporées dans ce cadre:

- tout transport de contenu entre les appareils connectés au réseau domestique est via IP;
- l'architecture de réseau transportera de nombreux types différents de supports, y compris la vidéo, l'audio, des "fixes" (par exemple, JPEG) et des données;
- l'architecture de réseau fournira la prise en charge simultanée de contenus et services protégés fournis par l'opérateur de réseau, des contenus protégés provenant d'autres sources (par exemple, une solution DRM de musique tierce) et des contenus non protégés (indépendamment d'une source).

Alors qu'il PEUT y avoir plusieurs architectures de réseau domestique qui réalisent les objectifs recherchés, un certain nombre de points techniques clés DOIVENT être pris en considération:

- seuls les appareils autorisés (c'est-à-dire, certifiés) PEUVENT faire partie de l'ASD;
- l'architecture DOIT prendre en charge la transmission et la mémorisation aussi bien des contenus livrés par l'opérateur de réseau que des contenus livrés par d'autres que l'opérateur de réseau;
- les contenus protégés livrés par l'opérateur du réseau PEUVENT être mémorisés et consommés au sein de l'ASD;
- les contenus protégés livrés par l'opérateur du réseau PEUVENT sortir de l'ASD seulement par des sorties approuvées;
- les contenus protégés et livrés par d'autres que l'opérateur PEUVENT être consommés et mémorisés au sein de l'ASD;
- si la liaison de communications avec le réseau par câble est interrompue, l'architecture de réseau domestique DEVRAIT toujours fonctionner pendant une certaine durée, avec une limite de durée fixée par l'opérateur du câble.

6.6 Publicité numérique évoluée

NG-STB-A prendra en charge des insertions de programme et des technologies de dévidage sur divers supports allant de l'encart publicitaire analogique au numérique, et il permettra une grande variété de modèles de publicité évolués[1] tels que:

- publicité numérique sur numérique;
- publicité ciblée et adressable;
- publicité interactive (sur tous les services);
- publicité sur DVR:
  - contenu de forme longue, distribué et mémorisé localement sur le DVR;
  - remplacement – rafraîchissement d'un contenu de publicité précédemment enregistré sur le DVR;
  - DVR réseau – rafraîchissement d'une publicité précédemment enregistrée sur un nDVR.
- Publicité sur VoD:
  - prise en charge d'une publicité sur un contenu de VoD – contenu de publicité tampon ou interstitiel;
  - insertion de publicité dans une VoD locale – prise en charge de l'insertion d'une publicité locale dans un contenu de VoD pris en charge par la publicité;
  - publication de VoD pour un publicitaire;
- collecte des données à travers tous les services de publicité pour inclure un contenu synchronisé;
- insertion de publicités nationales, régionales et locales en tous les points de l'implantation physique du câble ainsi qu'à partir de sources en dehors de l'implantation, telles que l'Internet.

7 Locaux de l'abonné

Le présent paragraphe du plan NG-STB-A décrit les éléments essentiels des appareils d'équipement CPE vidéo et non vidéo conformes à NG-STB-A. Les fabricants sont invités à développer des variations et combinaisons innovantes de ces éléments. L'intention du plan NG-STB-A est de fournir aux fabricants d'équipements une plate-forme qui soit la moins contraignante possible.

7.1 Aperçu général

Le segment de réseau dans les locaux de l'abonné implique des opportunités et des défis significatifs vis-à-vis des fabricants de produits électroniques, des détaillants de matériel électronique et des réglementations, et il représente aussi le plus gros investissement global étant donné le grand nombre d'appareils en cause. Les équipements CPE varieront dans leurs capacités. Par exemple, les options incluent la prise en charge des services de passerelle dans le réseau de données domestique, et du magnétoscope numérique (DVR). Le Tableau 3 résume les caractéristiques et attributs clé d'une gamme d'appareils d'équipement CPE conformes à NG-STB-A.

---

[1] La publicité numérique évoluée serait un service intéressant pour les opérateurs de service qui veulent développer leurs structures commerciales. Il est nécessaire d'harmoniser les schémas d'affaires entre les opérateurs de service et les diffuseurs.

Tableau 3 – Généralités sur les caractéristiques des équipements chez l'abonné

	SVD de base	SVD étendu (non passerelle)	SVD étendu (passerelle)	Prise en charge client
Prise en charge CSP	✓	✓	✓	✓
Fonctions SVD étendues autres que passerelle (par exemple, DVR, carte de sécurité, affichage)		✓	✓	A déterminer
Passerelle de réseau domestique (service portail IPCable2Home, point de contrôle UPnP)			✓	
Client de réseau domestique (point frontière de IPCable2Home, signalisation UPnP, QS UPnP)	✓	✓		✓
Capacités de la série J.200	✓	✓	✓	Facultatif
USB 2.0 et/ou hôte Ethernet	✓	✓	✓	✓
NOTE – Toutes les descriptions UPnP du Tableau 3 sont pour information.				

7.2 Appareils vidéo d'abonné (SVD)

Les appareils vidéo d'abonné (SVD) incluent des appareils qui ont un cœur minimal de capacités, jusqu'à des appareils qui fournissent en ensemble plus riche de capacités.

Ces équipements seront fournis par l'opérateur ou au détail par des fournisseurs de matériels électroniques. Les SVD fonctionneront comme boîtiers adaptateurs (STB) ou comme boîtiers de détournement (SBB, *set-back boxes*). Les autres SVD pourraient inclure des postes de télévision numériques bidirectionnels.

Ces appareils sont conçus comme des SVD parce que chacun d'eux fournit plus que les fonctions conventionnelles de boîtier adaptateur, comme l'accès conditionnel reconfigurable via un CSP, la prise en charge d'un vidéo codec évolué, la prise en charge de plusieurs options de transport vidéo, et le réseautage sur le réseau domestique. Chaque SVD peut accéder à des ressources situées dans d'autres appareils du réseau ou leur fournir des ressources. En d'autres termes, tous les SVD PEUVENT agir comme source ou destination de contenu au sein du réseau domestique. Et donc, à travers le réseau domestique, l'appareil le moins sophistiqué peut fournir certaines des caractéristiques et capacités des appareils les plus sophistiqués. Le système conforme à la présente Recommandation fournit l'échange de contenus protégés en copie et à gestion des droits entre n'importe lesquels des SVD sur le réseau domestique.

La Figure 8 illustre la capacité des SVD à agir en réseau avec les autres SVD et autres appareils compatibles.

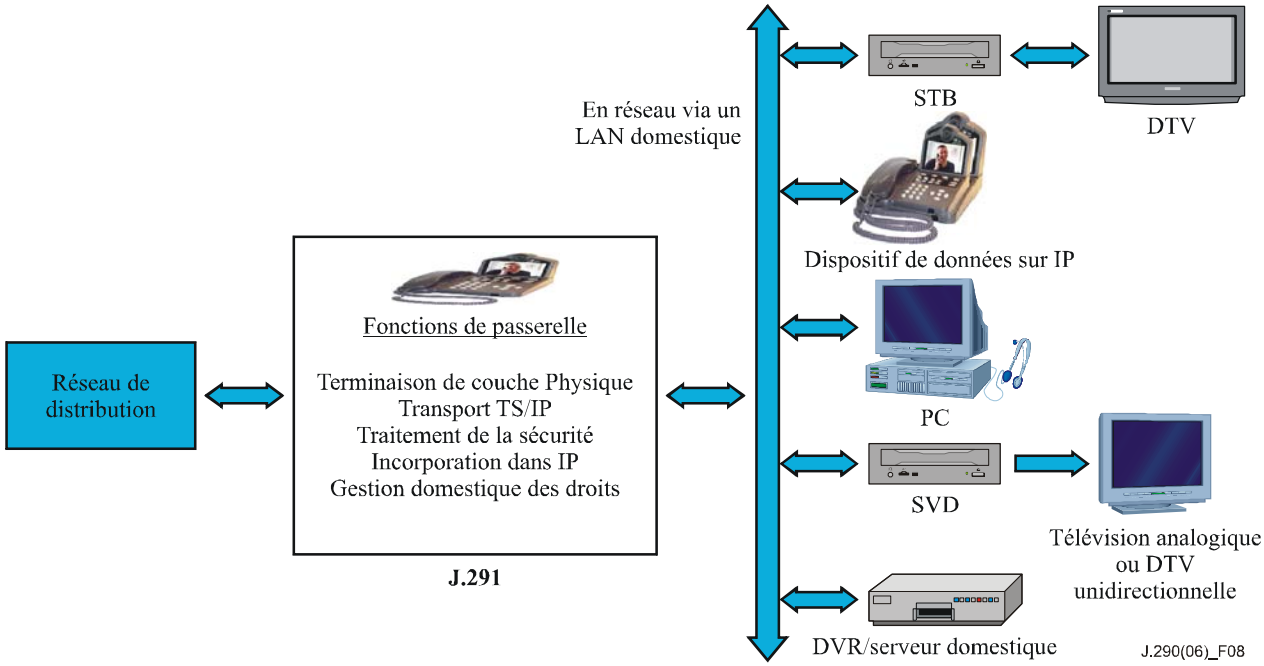


Figure 8 – Exemples de développement de CPE pour abonné avec réseau de données domestique fondé sur IP (en résidentiel, le système DRM est appliqué)

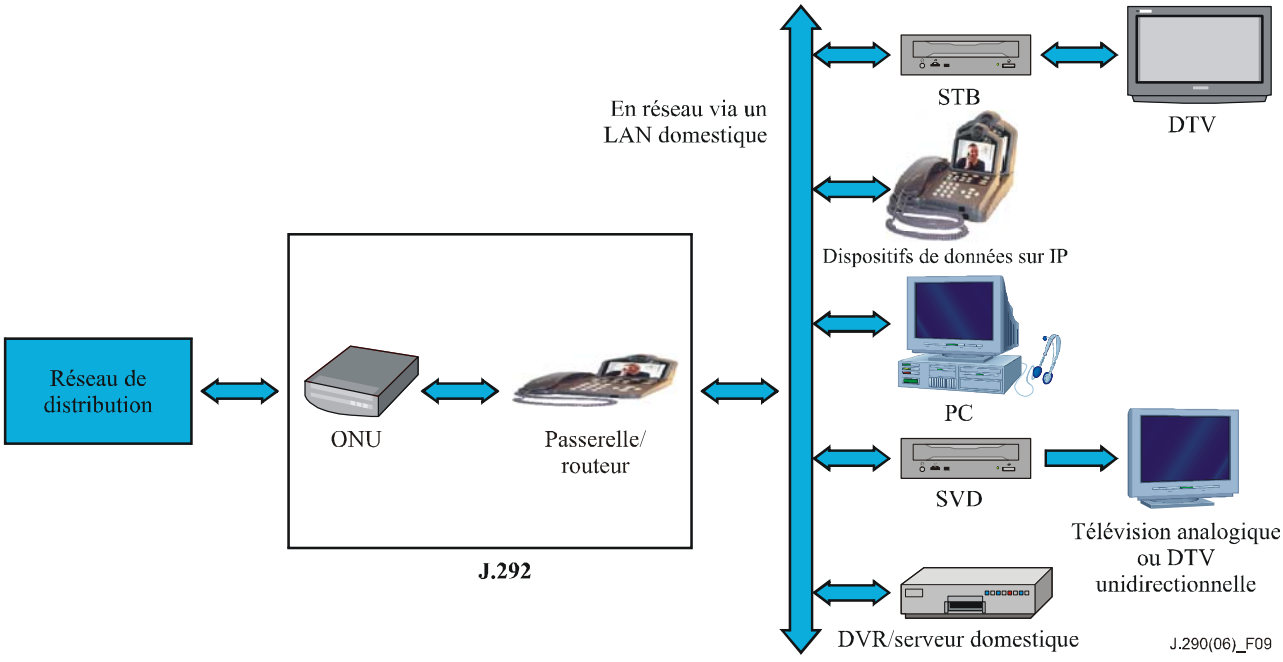


Figure 9 – Exemples de développement de CPE pour abonné avec réseau de données domestique fondé sur IP

Les SVD ont comme fonction principale la livraison de divertissements vidéo. Des appareils supplémentaires PEUVENT offrir des communications vidéo et PEUVENT être en réseau avec des SVD, comme des appareils de visioconférence et autres formes d'applications IP. Ces appareils seront définis par le marché et ne sont pas détaillés dans la présente Recommandation.

Le SVD de base comporte les fonctionnalités suivantes:

- tout numérique, décodage vidéo à définition normalisée (MPEG-2 et codec évolué);
- appareil autonome (ne fonctionne pas comme une télévision;
- accepte à la fois les services mono et bidirectionnel;
- capacités des Recommandation UIT-T de la série J.200 – l'intention est d'avoir des SVD fonctionnant sur les micrologiciels de la série J.200, en fonction de conditions de licence raisonnables de la technologie de la série J.200;
- compatible avec le modèle de sécurité, comme décrit plus haut, avec le CSP interne;
- la vidéo PEUT être délivrée sous forme de paquets de transport MPEG sur QAM, ou sur un réseau fondé sur IP. De plus, la vidéo PEUT être délivrée sur le réseau domestique;
- prise en charge de MPEG-2 ainsi que des codecs vidéo évolués décrits plus haut;
- prise en charge du codage audio, BC (ISO/CEI 13818-3) et/ou AAC (ISO/CEI 13818-7);
- la prise en charge de base du réseautage domestique est fournie par la présence d'un port USB 2.0 et/ou Ethernet (100BASE-TX). Divers adaptateurs de réseautage peuvent être attachés à ce port pour fournir la fonctionnalité de couche PHY/MAC pour différentes architectures de réseautage domestique (par exemple, WiFi, CAT5);
- le SVD de base est un appareil de domaine de service garanti et autorisé, comme défini plus haut;
- {texte pour information: l'appareil fonctionnera comme un client de réseau domestique, qui exige que l'appareil fonctionne comme un point de frontière IPCable2Home et qu'il fournisse la signalisation UPnP et la qualité de service UPnP.};
- l'appareil prendra aussi en charge un accès d'expansion (d'un type à déterminer) qui permette le renouvellement matériel du mécanisme de sécurité interne;
- la sortie vidéo est fournie par un seul port vidéo composite RF, une sortie vidéo de haute définition ou une interface vidéo numérique approuvée.

Les SVD de base PEUVENT aider à la transition vers les services tout numérique. Utilisés dans ce but, les SVD de base permettront aux abonnés qui ont une télévision analogique et d'autres appareils analogiques (par exemple, des VCR) de continuer à recevoir leurs services existants de façon aussi transparente que possible même si les anciens canaux analogiques auront été réalloués pour transporter des signaux numériques compressés.

Les fonctions de base de SVD sont illustrées à la Figure 10.

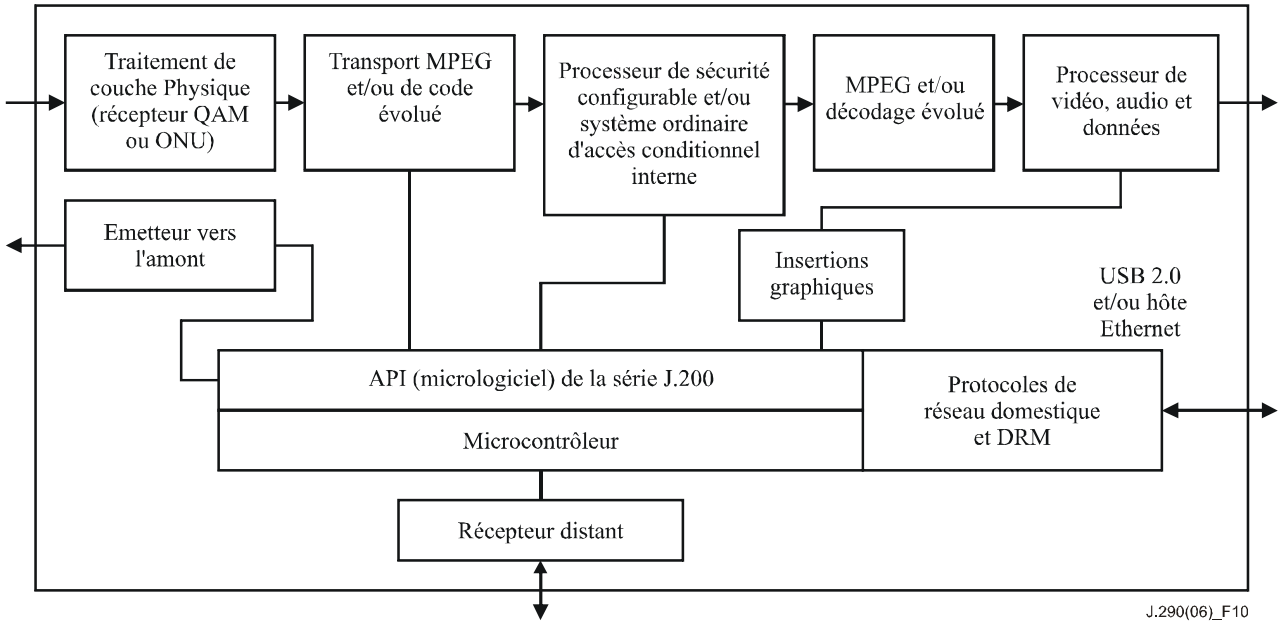


Figure 10 – Fonctions SVD de base

Les fournisseurs de SVD PEUVENT fournir des fonctions étendues supplémentaires dans des appareils de gamme supérieure. Par exemple, ces dispositifs PEUVENT prendre en charge:

- des signaux vidéo de haute définition, y compris les sorties numériques autorisées suivantes: DVI (ou HDMI) avec HDCP et 1394 avec DTCP;
- la prise en charge de la réception et du traitement de plusieurs programmes vidéo;
- des fonctions de DVR, y compris la mémorisation interne et externe;
- {texte pour information: La fonction de passerelle, qui exige que l'appareil prenne en charge les services et fonctions de portail comme un point de contrôle UPnP.} De plus, les appareils qui acceptent la fonction de passerelle doivent prendre en charge la capacité à activer et désactiver cette caractéristique pour éviter les conflits si plusieurs passerelles sont installées sur le même réseau;
- prise en charge de la carte de sécurité;
- prise en charge de la connectivité de réseautage (par exemple, WiFi, CAT5). Ce soutien s'ajoute à l'accès USB-2 basique exigé et au réseau associé;
- affichage associé tel que le SVD fonctionne comme un DTV bidirectionnel.

Alors que la présente Recommandation n'exige pas la prise en charge d'un tuner analogique, un SVD qui comporte ce dispositif aurait à se conformer aux exigences applicables concernant les appareils DTV qui incorporent la télévision analogique.

La Figure 11 montre les capacités d'un SVD de base plus les caractéristiques d'extension qui PEUVENT se trouver dans des SVD de plus haute gamme.

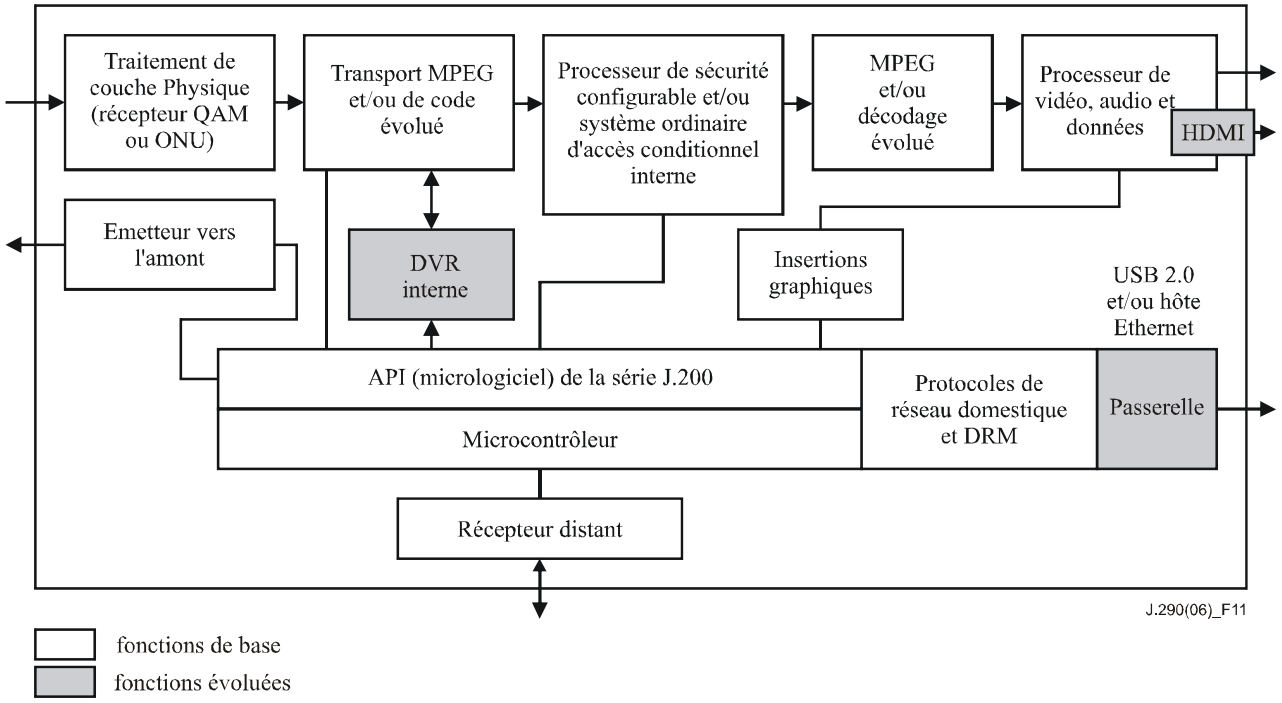


Figure 11 – Fonctions SVD avec extensions possibles

Il sera exigé de tous les SVD qu'ils satisfassent aux règles de conformité appropriées de protection de contenu et autres, pour assurer que les services délivrés dans les domaines de service garanti et autorisé le soient comme prévu par le câblo-opérateur.

7.3 Autres appareils de CPE

Le plan NG-STB-A décrit des exemples d'équipements CPE de réseau de la prochaine génération en plus des options pour les SVD.

7.3.1 Client à support vidéo

Le client de support vidéo est un appareil "sans tuner" qui est spécifiquement conçu pour se connecter aux autres SVD sur le réseau domestique afin de recevoir des contenus de vidéo. Il PEUT fournir un environnement d'application riche à partir de micrologiciels et applications embarqués, ou PEUT au lieu de cela présenter une "interface d'utilisateur distant" qui est pilotée par le SVD qui lui sert son contenu.

Certaines des caractéristiques de base du client de support incluent:

- une définition standard, uniquement numérique;
- la prise en charge du DRM domestique tel que fourni par le CSP;
- la prise en charge du client de réseautage domestique;
- l'appareil PEUT fonctionner comme un appareil ASD ou un appareil GSD/ASD;
- prise en charge du codec MPEG-2 et du codec évolué;
- contrôle à distance universel associé ou contrôlé à distance qui communique avec l'appareil source;
- USB 2.0 pour fournir la connectivité avec le réseau.

Les caractéristiques facultatives du client de support incluent:

- La prise en charge de la vidéo haute définition avec les sorties numériques approuvées associées.

7.3.2 CPE non vidéo

Etant donné la prolifération de nouveaux services de vidéo, données et multimédias, et la convergence croissante entre ces services, il est vraisemblable que des équipements CPE non vidéo supplémentaires de la prochaine génération seront développés, qui se connecteront directement et indirectement au réseau par câble.

Les fabricants d'appareils incorporent déjà plusieurs fonctions dans les câblo-modems, telles que diverses combinaisons de pare-feu, de routeur, de concentrateur de données, d'adaptateurs de téléphonie multimédia et de transport de réseautage domestique (par exemple WiFi, HPNA, HomePlug, etc.) de couche 3, et ils vont vraisemblablement intégrer aussi certaines des fonctions réseau de la prochaine génération dans les futurs câblo-modems et autres appareils d'abonné. Les fonctions réseau de la prochaine génération qui sont les candidates à une intégration créative dans les équipements CPE incluent le réseautage domestique au sein et entre les domaines de service garanti et autorisé, et les fonctions IPCable2Home qui permettent la gestion et la visibilité des appareils d'abonné depuis l'en-tête de réseau.

Exemple d'équipement CPE non vidéo: passerelle multifonction

Le cœur de cet appareil est actuellement disponible, incluant un câblo-modem, un pare-feu routeur de couche 3, et un adaptateur téléphonique multimédia (MTA). Une version de prochaine génération de cet appareil ajouterait des capacités IPCable2Home de visibilité et de gestion à distance à partir de l'en-tête de réseau. Elle devrait aussi inclure un dispositif de pontage permettant l'interaction entre les SVD compatibles avec les protocoles de réseau domestique et l'équipement CPE sur le réseau de données domestique. Un tel appareil devrait prendre en charge des applications telles que:

- permettre aux ordinateurs personnels ayant un pontage approprié d'utiliser le réseau coaxial comme un moyen d'accéder aux services de données à grande vitesse;
- permettre aux ordinateurs personnels ou serveurs qui sont en la possession de l'abonné sur le réseau de données ou coaxial domestique de communiquer les messages affichables ou les messages de commande sur les SVD;
- permettre à l'adaptateur de téléphonie multimédia d'envoyer les messages d'identification de l'appelant (ou autres messages) aux SVD;
- permettre aux SVD d'accéder aux informations de facturation ou de service concernant les services interactifs multimédia/données des abonnés.

8 Sécurité

8.1 Elément matériel de sécurité

L'élément matériel de processeur de sécurité configurable (CSP) de la prochaine génération prendra en charge les algorithmes normalisés suivants pour le chiffrement des flux de transport à l'en-tête de réseau et leur déchiffrement à l'équipement de CPE. Ci-après figure une liste d'exemples des algorithmes normalisés qui PEUVENT éventuellement être pris en charge par le CSP.

- Norme de chiffrement des données (DES) – Répertoire électronique (ECB, *electronic code book*), chaînage de bloc de chiffrement (CBC, *cipher block chaining*) et autres modes pour les blocs résiduels (norme fédérale de traitement de l'information, FIPS 46-2).
- Triple DES – ECB, CBC et autres modes pour les blocs résiduels (FIPS 46-2). Cela inclut la prise en charge à la fois du chiffrement à deux clés et à trois clés.
- Norme de chiffrement évolué (AES, *advanced encryption standard*) (Rijndael).
- DVB – algorithme de brouillage commun (CSA, *common scrambling algorithm*)
- Multi2 (ISO/CEI 9979).

L'élément matériel de CSP sera configurable ("renouvelable") et utilisera les technologies de prise en charge du déchiffrement d'au moins des cinq types suivants de flux de transport sécurisés:

1) triple DES – acceptant ECB et CBC au minimum ainsi que les modes à deux et trois clés;

2) DVB-CSA – comme défini dans DVD;

3) AES – en utilisant une nouvelle architecture de clés normalisée avec ECM normalisé, EMM, le germe d'unité et la méthodologie d'identifiant d'unité;

4) B-CAS – comme défini dans ARIB, qui sera pris en charge par les cartes de sécurité.

Noter que le CSP doit être défini de telle sorte que les fournisseurs de microprocesseurs ne soient pas obligés d'obtenir de licences pour des systèmes de sécurité afin de construire les fonctionnalités de CSP dans leurs produits. Le CSP sera défini d'une manière telle que les microprocesseurs conformes soient capables de faire fonctionner les algorithmes appropriés qui sont téléchargés dans le CSP lors de la connexion au câble ou qui leur sont fournis par la carte de sécurité.

8.2 Authentification

Les composants matériels du CSP devront être capables de mémoriser en toute sécurité et d'effectuer des signatures numériques en utilisant diverses tailles (par exemple, 1024, 2048 et 4096 bits) de clés RSA dans les registres matériels. Les composants de la prochaine génération devront être capables de générer en toute sécurité des signatures numériques à l'intérieur d'un matériel inviolable sans exposer les clés privées ou les processus nécessaires pour générer le hachage et le chiffrement. Le réseau de la prochaine génération doit être capable de signer numériquement les messages utilisés pour l'authentification et de protéger l'intégrité en utilisant un hachage SHA-1 sécurisé.

8.3 Clés de chiffrement

Le matériel CSP devra être capable de mémoriser en toute sécurité les clés de chiffrement de clés qui pourraient être sous la forme d'un chiffrement symétrique ou, de préférence, asymétrique. La capacité à utiliser des paires de clés pour le transport des clés chiffrées parmi les appareils d'équipement de CPE et vers les appareils d'en-tête de réseau est très souhaitable.

8.4 Adresse d'unité

Chaque CSP utilisé dans un appareil d'équipement de CPE devra être identifié de façon univoque avec un identifiant complètement unique. Cet identifiant est utilisé pour donner une adresse à chaque appareil d'équipement de CPE pour la réception des habilitations pour cet appareil de CPE spécifique. Dans certaines implémentations, une adresse MAC PEUT être utilisée pour cet identifiant. L'identifiant d'unité doit pouvoir être aussi fourni par la carte de sécurité.

8.5 Résistance aux altérations

Le CSP doit être conçu de façon à satisfaire la sécurité de niveau 2 de FIPS-140 dans la plupart des zones, avec certaines zones (reconfiguration de matériel et mises à jour de micrologiciels) exigeant la sécurité de niveau 3 de FIPS 140-2 qui a la résistance aux altérations en conformité à certains critères tels que le niveau 2 ou le niveau 3 de FIPS-140. Il doit aussi employer les technologies les plus récentes (par exemple, la distribution de plan de puissance et la fragmentation de cellule) en résistance aux altérations pour empêcher l'analyse au microscope électronique et les attaques de rasage de surface.

8.6 Gestion de clés

La hiérarchie de clés inclut des clés multiples comme illustré dans la Figure 12. De plus, la Figure 13 illustre le schéma de déchiffrement qui utilise la carte de sécurité.

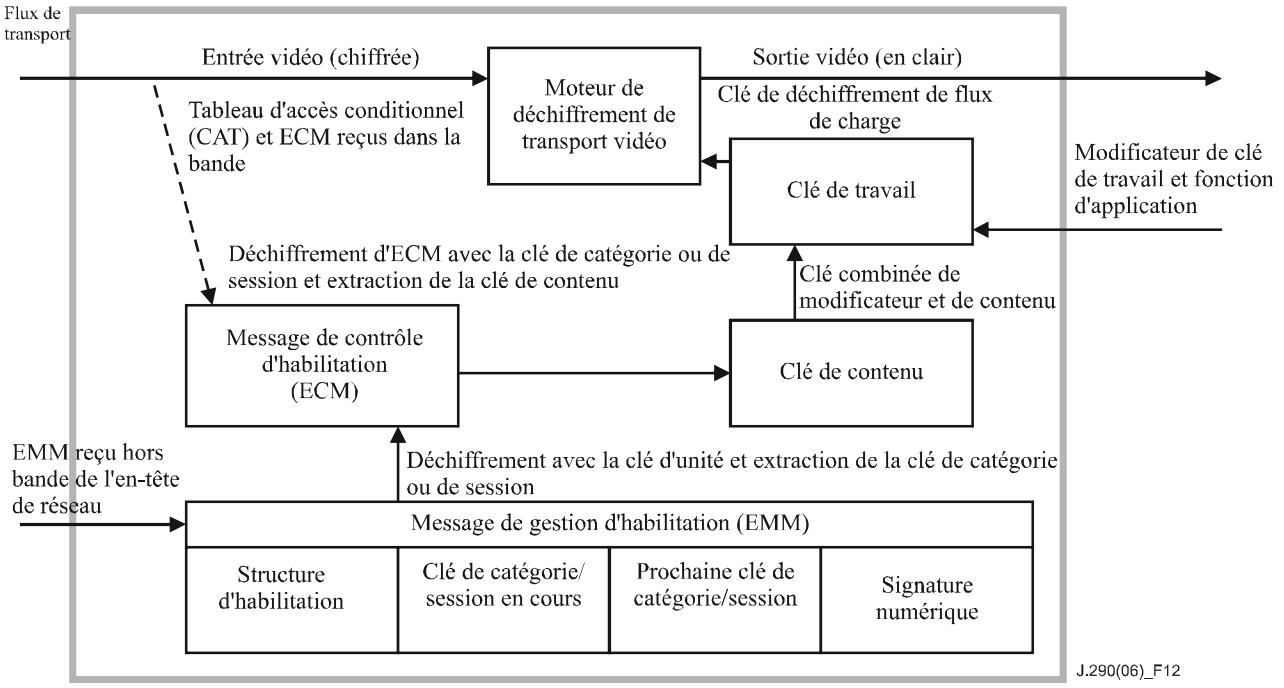


Figure 12 – Hiérarchie des clés

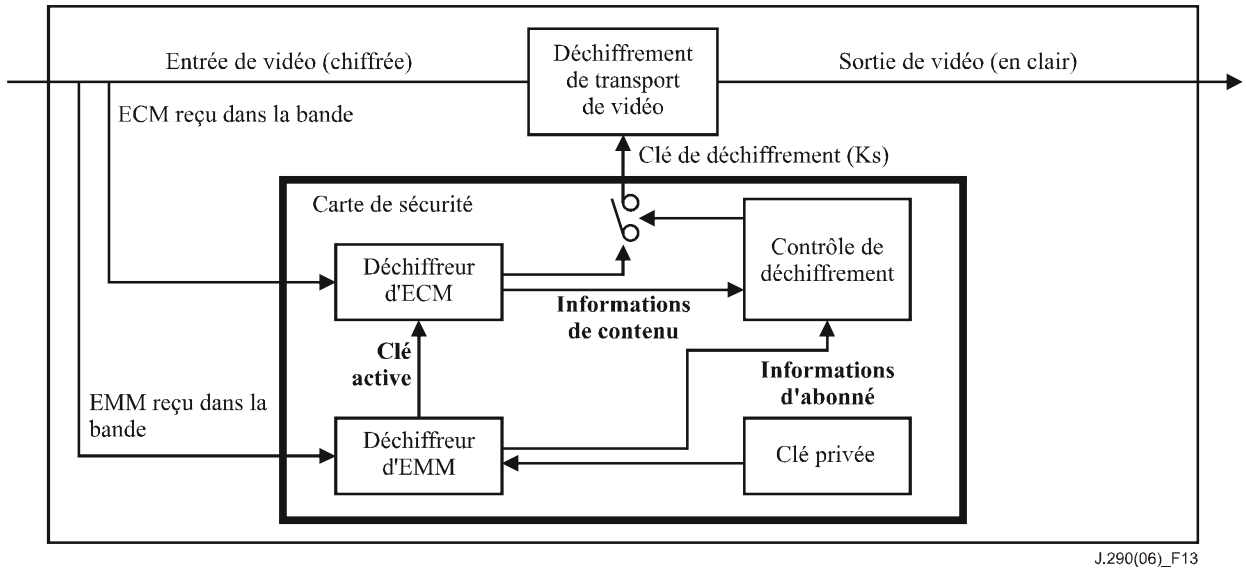


Figure 13 – Flux de signaux utilisant une carte de sécurité

Le logiciel et le matériel de CSP DEVRAIENT être conçus de façon à employer les nouveaux concepts et technologies dans le domaine de la gestion des clés tout en fonctionnant avec les systèmes ordinaires existants qui utilisent le partage des clés ou les critères de reconfiguration. Le module CSP doit prendre en charge les schémas suivants:

1) clés déchiffrées extraites dans l'équipement de CPE à partir du flux vidéo, et les ECM et EMM doivent être chargés directement dans les moteurs de déchiffrement sans passer sur des interfaces externes, y compris les déchiffreurs du transport;

2) les ECM et EMM sont extraits du flux de transport (dans la bande) et ils doivent être transférés directement dans l'appareil de carte de sécurité, où la clé de travail est décodée et où la clé de déchiffrement du flux est calculée.

8.6.1 Messages de contrôle d'habilitation (ECM)

Un ECM, message de contrôle d'habilitation est un message chiffré qui contient des critères d'accès à divers liants de service et un mot de contrôle (CW, *control word*). Le mot de contrôle est le germe de clé qui est modifié et utilisé pour déchiffrer le flux vidéo et doit être capable d'être changé selon une périodicité variable ou converti effectivement en une "clé active". L'ECM est déchiffré et vérifié dans l'équipement CPE par rapport aux critères d'accès afin de fournir l'autorisation. Si l'autorisation est accordée, le CW sera libéré, converti en une clé active et utilisé pour déchiffrer le contenu dans l'appareil d'équipement CPE.

8.6.2 Messages de gestion d'habilitation (EMM)

Les messages chiffrés sont créés dans l'en-tête de réseau et envoyés à l'équipement CPE de la prochaine génération pour autoriser l'appareil d'équipement CPE pour certains critères d'accès au contenu. Les messages EMM, messages de gestion d'habilitation, contiennent les données réelles d'autorisation et ils doivent être envoyés selon une méthode sécurisée à chaque appareil d'équipement CPE. L'EMM est adressé à un seul appareil d'équipement CPE et il est chiffré de façon univoque de sorte que seul cet appareil puisse déchiffrer l'habilitation et la valider. Le CSP doit prendre en charge les mécanismes et formats d'habilitation DigiCipher II, PowerKey, NDS, Nagravision, NCAS et B-CAS.

8.7 Protection de copie

Si un appareil NGNA emploie une carte de sécurité, l'interface doit implémenter la capacité à renouveler et à configurer, conformément à SCTE-41. En plus de la prise en charge des exigences de flux de transport actuelles de SCTE-41, le CSP doit être capable de déchiffrer les trois types de flux de transport sécurisé normalisés suivants. La liste des exemples est la suivante:

1) protection de copie – DES (comme défini dans SCTE-41, avec l'option supplémentaire d'utiliser DES en mode CBC en plus du mode EBC);
2) triple DES – prenant en charge au minimum ECB et CBC;
3) AES – utilisant une nouvelle architecture de clé normalisée avec ECM, EMM, clés de chiffrement de clés, et la méthodologie d'identifiant d'unité, normalisées;
4) Multi2 – prenant en charge ECB et OFB.

9 Architecture d'en-tête de réseau

Parmi les bénéfices de l'intégration de l'en-tête de réseau, qui est cohérente avec la version de NG-STB comme multimédia intégré, on notera:

- une utilisation plus efficace des ressources du système;
- une interopérabilité facilitée des éléments du réseau fournis par des fabricants différents pour activer une concurrence ouverte, pour augmenter la durée de vie de la base installée, pour fournir de la souplesse aux introductions de nouveaux services et pour donner le facteur d'échelle permettant de s'accommoder d'une large gamme de tailles de systèmes;
- fournir une plate-forme pour l'innovation et accélérer la création de service.

9.1 Architecture de livraison d'en-tête de réseau

La Figure 14 décrit l'architecture globale de livraison d'en-tête de réseau.

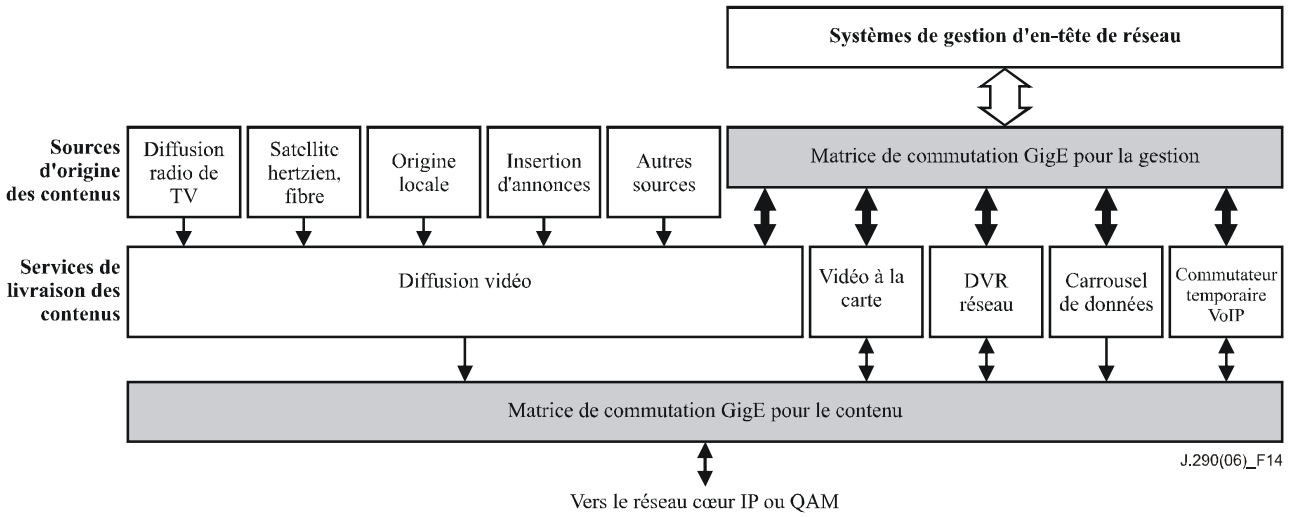


Figure 14 – Architecture de livraison de réseau d'extrémité

Les caractéristiques clé de l'architecture d'en-tête de réseau de la prochaine génération comportent:

- l'en-tête de réseau permet la livraison du trafic vidéo numérique et du trafic générique de datagrammes IP sur une infrastructure commune d'en-tête de réseau;
- les applications sont gérées à travers tous les services par des systèmes de gestion de session et de ressources, qui doivent avoir la capacité de fonctionner de façon autonome dans le cas d'une défaillance des communications avec les systèmes de l'arrière;
- le contrôle des serveurs d'en-tête de réseau est séparé de sorte que les applications de gestion des ressources tierces communes et de fonctionnement du réseau puissent gérer l'en-tête de réseau comme un système intégré plutôt que comme des sous-systèmes autonomes spécifiques des service.
  - *Matrice de commutation GigE pour le contenu*: la matrice de commutation GigE sera sous le contrôle d'un gestionnaire de ressources réseau pour la distribution de contenus et s'assurera que tout serveur peut avoir des données commutées sur toute source de contenus et peut commuter aisément entre les serveurs de contenus.
  - *Système de gestion de session et de ressource*: les gestionnaires d'application, les gestionnaires de session et les gestionnaires de ressources auront les fonctionnalités qui donnent à l'opérateur la capacité à contrôler et surveiller les charges de trafic, les besoins en qualité de service et les habilitations des abonnés.
  - *Matrice de commutation Ethernet ou GigE pour la gestion*: la matrice de commutation fournira une interface standard de plan de gestion au moyen d'une matrice de commutation Ethernet ou GigE de sorte que chaque service puisse être géré et contrôlé par des systèmes de gestion informatiques externes via des API ouvertes.
- IP est utilisé pour le transport réseau des messages de gestion et de contrôle à l'équipement de CPE. L'ensemble des protocoles de signalisation pour les services fondés sur la vidéo inclura vraisemblablement les protocoles DSM-CC (support de mémorisation numérique – commande et contrôle), RTSP, SIP, NCS/MGCP et des protocoles "de services de la toile" qui pourront être fondés sur XML, tels que SOAP.

9.2 Architecture de gestion de session et de ressource

Dans le but de satisfaire le désir de gestion commune des ressources à travers tous les services et applications, il est nécessaire d'avoir un cadre de travail pour la gestion des sessions et des ressources, comme le montre la Figure 15.

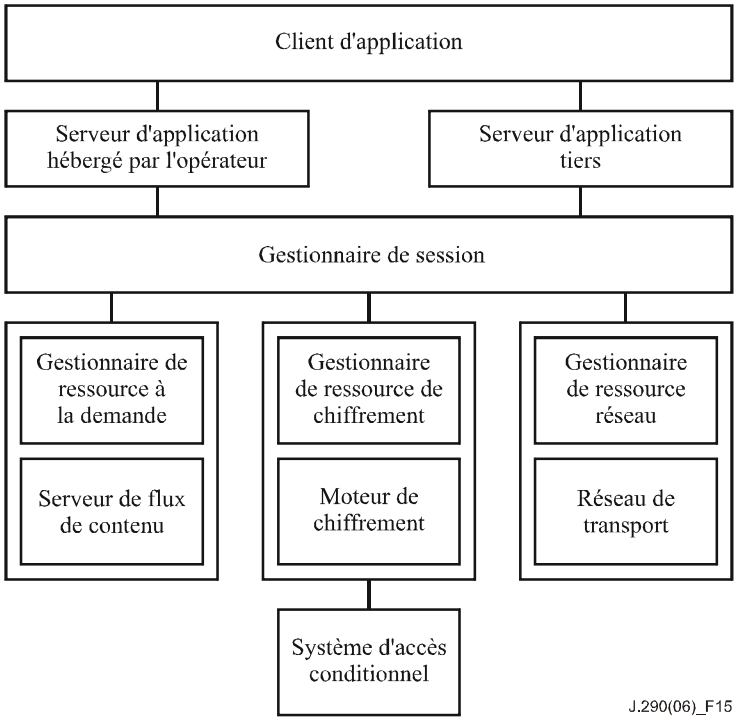


Figure 15 – Cadre de gestion de session et de ressource

Pour augmenter l'efficacité de l'utilisation des ressources, l'en-tête de réseau de la prochaine génération emploie une architecture de gestion des ressources fondée sur la session. La création d'une telle architecture exige un contrôle étroit des ressources pour assurer leur utilisation efficace. Pour essayer de fournir un cadre de travail générique, la fonction de gestion de session et de ressource est partagée en trois domaines: application, session et gestion des ressources. Chacun de ces domaines est exposé en détail dans les paragraphes suivants.

9.2.1 Gestionnaire d'application

Un gestionnaire d'application joue un rôle de coordination qui implique la signalisation des applications aussi bien que l'interaction avec le cadre de travail de gestion de ressources de l'en-tête de réseau via le gestionnaire de session. Dans la plupart des cas, le gestionnaire d'application est supposé être possédé et contrôlé par l'opérateur de service. Cependant, il PEUT y avoir des cas où le gestionnaire d'application est en fait en dehors du contrôle de l'opérateur du service. Un exemple de gestionnaire d'application hébergé par l'opérateur serait celui de services de vidéo à la carte et de services de téléphonie. Un exemple de gestionnaire d'application tiers pourrait être celui de services audio/vidéo et de jeux.

Dans un système de vidéo à la carte, il est de la responsabilité du gestionnaire de session de maintenir et de gérer le cycle de vie de la session plutôt que de celle du gestionnaire d'application. Pour de tels cas, le client peut établir directement une session avec le gestionnaire de session ou passer par l'intermédiaire du gestionnaire d'application. Comme le gestionnaire d'application n'a pas besoin de gérer la session lui-même, cette architecture permet que différentes applications utilisent le même gestionnaire de session pour plusieurs services à la carte.

Pour les applications et services fondés sur IP, l'implémentation normale intègre en réalité le gestionnaire de session dans le serveur d'application, alors qu'ils PEUVENT résider dans le même boîtier physique, ils sont considérés comme logiquement séparés.

9.2.2 Gestionnaire de session

Le rôle d'un gestionnaire de session est de servir d'intermédiaire pour les demandes de ressources d'en-tête de réseau au nom du gestionnaire d'application. Alors qu'un gestionnaire d'application ne connaît que les besoins en qualité de service de la session, le gestionnaire de session a besoin de comprendre comment traduire ces besoins de qualité de service dans les diverses ressources du système ainsi que d'identifier les ressources qui ne sont pas fondées sur la qualité de service que la session PEUT aussi requérir (c'est-à-dire, les ressources de chiffrement, les ressources de serveur).

Il est important de noter que plusieurs instances de gestionnaire de session PEUVENT exister dans un en-tête de réseau donné et que chaque gestionnaire de session communique avec un ensemble de gestionnaires de ressources. L'ensemble des gestionnaires de ressource avec lesquels communique un gestionnaire de session est déterminé par les applications pour lesquelles le gestionnaire de session est supposé traiter des demandes de ressource. Une telle architecture permet une introduction plus rapide des nouveaux services en n'exigeant pas un 'super' gestionnaire de session central mis à jour chaque fois qu'un nouveau service est essayé. Il est envisagé qu'un gestionnaire d'application donné ne communique avec un gestionnaire de session unique que lorsque des gestionnaires de session redondants sont implémentés. Les gestionnaires de session n'ont pas besoin d'être capables de prendre en charge tous les types de session; en fait, il est vraisemblable que des gestionnaires de session séparés seront développés pour différents types de sessions, par exemple, vidéo à la carte contre diffusion commutée.

Le gestionnaire de session ne prendra pas de décisions de politique à caractère commercial. Il coordonnera plutôt les besoins en ressources d'application en agissant avec l'hypothèse que la demande provient d'un appareil valide et d'un abonné autorisé à demander de tels services. Il PEUT prendre des décisions de politique fondées sur les ressources sur la base de l'état actuel des ressources du système.

9.2.3 Gestionnaire de ressource

Le gestionnaire de ressources traite principalement de l'allocation des ressources nécessaires pour satisfaire une demande de session. Chaque ressource d'en-tête aura un gestionnaire de ressource (logique) associé. C'est la tâche du gestionnaire de ressource de garder la trace de toutes les consommations de ressources et d'allouer de nouvelles ressources en tant que de besoin. Des exemples de gestionnaire de ressource sont:

- gestionnaire de ressources à la demande – ressources de serveur de à flux continu;
- gestionnaire de ressources de chiffrement – ressources de chiffrement de flux;
- gestionnaire de ressources réseau – ressources de réseau IP commuté.

Les exemples suivants sont fournis pour mieux expliquer le cadre de travail de gestion de session et de ressource:

- Un service de vidéo à la carte suit le flux suivant: le client commence la session en faisant une demande d'établissement de vidéo à la carte au gestionnaire d'application. A réception d'une telle requête, le gestionnaire d'application va la transmettre au gestionnaire de session approprié. Le gestionnaire de session va négocier avec plusieurs gestionnaires de ressources pour obtenir les ressources correspondantes. Cela PEUT inclure (pas nécessairement dans cet ordre) des ressources de serveur, des ressources de réseau, des ressources de chiffrement et des ressources d'extrémité.

10 Qualité de service

La qualité de service peut être fournie en surprovisionnant généreusement un réseau de telle sorte que tous les paquets obtiennent une qualité de service suffisante pour prendre en charge les applications sensibles à la qualité de service. Cette approche est relativement simple et elle est économiquement faisable pour de nombreux réseaux à haut débit. La performance est raisonnable,

particulièrement si l'utilisateur est d'accord pour accepter une certaine dégradation. Cependant, pour les réseaux à faible débit plus typiques des entreprises et bureaux locaux, les coûts du haut débit peuvent être substantiels et le surprovisionnement difficile à justifier. Les réseaux exigent généralement les quatre facteurs clés suivants pour établir la qualité de service de bout en bout afin de prendre en charge à la fois les services en temps critique et les services vidéo de haute qualité.

- délai;
- gigue;
- perte de paquet;
- bande passante.

Les fonctions de qualité de service fournies dans les routeurs ou les commutateurs DOIVENT contrôler ces facteurs clés et transmettre les paquets au prochain bond. Dans ces situations, deux philosophies différentes distinctes sont développées pour satisfaire les exigences.

10.1 IntServ et DiffServ

Les travaux antérieurs utilisaient la philosophie "IntServ" de réservation des ressources de réseau. Dans ce modèle, les applications utilisaient le protocole de réservation de ressource (RSVP) pour demander et réserver des ressources à travers un réseau. Bien que les mécanismes IntServ fonctionnent, il faut réaliser que dans un réseau haut débit typique d'un grand fournisseur de service, les routeurs centraux seraient obligés d'accepter, maintenir, et supprimer des milliers ou éventuellement des dizaines de milliers de réservations.

La seconde approche, couramment acceptée, est "DiffServ" ou services différenciés. Dans le modèle DiffServ, les paquets sont marqués conformément au type de service dont ils ont besoin. En réponse à ces marquages, les routeurs et commutateurs utilisent diverses stratégies de mise en file d'attente pour ajuster les performances aux exigences. A la couche IP, les marquages de point de code des services différenciés (DSCP) utilisent les six bits de l'en-tête de paquet IP. A la couche MAC, le VLAN IEEE 802.1Q et IEEE 802.1D peuvent être utilisés pour transporter essentiellement les mêmes informations.

10.2 Qualité de service de bout en bout et applications de service

Au regard des services que les STB de la prochaine génération DEVRAIENT fournir, le mécanisme de qualité de service DOIT satisfaire les exigences de la vidéo de haute qualité et des services en temps critique comme la voix sur IP. Le mécanisme de qualité de service garantie, tel que défini au § 6.5.1, DOIT être implémenté pour le faire.

Le provisionnement du mécanisme de qualité de service garantie diffère dans les zones d'application de service et dans les structures de session entre les divers réseaux. Dans la présente Recommandation les types de qualité de service sont classés en trois types; QS fondée sur la session, QS à bande passante préprovisionnée et QS à classe de priorité. La définition de chaque type de qualité de service est donnée ci-dessous:

- QS fondée sur la session: la signalisation est nécessaire au réglage du routage de la QS. Elle est sécurisée à chaque activation de service et sa bande passante est libérée lorsque le service est clos;
- QS à bande passante préprovisionnée: la signalisation n'est pas toujours nécessaire pour le réglage du routage de la QS. C'est exclusivement le type de QS qui réserve la bande passante requise indépendamment du type de trafic ou de sa présence;

- QS à classe de priorité: dans certains cas, la qualité de service à classe de priorité peut satisfaire les exigences de qualité de service garantie comme défini au § 6.5.1 en surprovisionnant la bande passante. Un tel surprovisionnement satisfait aux contraintes de bande passante, et dans la plupart des cas satisfera aussi aux exigences de gigue et de délai si la priorité des paquets est strictement maintenue sans aucune interruption due à des limitations de bande passante ou de processeur.

Noter que dans la présente Recommandation, service est considéré du point de vue de l'utilisateur et non de celui du fournisseur de service Internet ou de l'opérateur de télécommunication.

Le Tableau 4 montre des services typiques et la qualité de service requise pour une architecture indépendante du support (Rec. UIT-T [J.292]) et de l'architecture du câble (Rec. UIT-T [J.291]).

Les exigences pour chaque service DEVRAIENT être mentionnées dans la Rec. UIT-T J.193 (2004). Comme pour les relations entre service et qualité de service, se reporter à l'Appendice I.

Tableau 4 – Types de services et exigences de qualité de service

Service	Architecture indépendante du support	Architecture du câble
Télévision diffusée	Bande passant préprovisionnée	Bande passante préprovisionnée
Vidéo à la carte	Fondé sur la session	Fondé sur la session
VoIP	Fondé sur la session	Fondé sur la session
Visiophone	Fondé sur la session	Fondé sur la session
Internet	Au mieux	Au mieux

Le Tableau 5 décrit les relations entre le type de QS, la signalisation et l'allocation de bande passante. Signalisation signifie ici toutes transactions de signaux pour le réglage de session entre les appareils concernés.

Tableau 5 – Relations entre type de QS, signalisation et allocation de bande passante

Type de QS	Signalisation	Allocation de bande passante
QS fondée sur la session	Applicable	Déclanché par session, réserve la bande passante
QS à bande passante préprovisionnée	Non applicable	Bande passante fixée
QS à classe de priorité	Non applicable	File d'attente à priorité, indépendamment de la bande passante Facultatif pour la QS de type DiffServ qui a un aspect bande passante

10.3 Exigences de pont de qualité de service

Comme indiqué à la Figure 16, il est exigé de confronter logiquement les mécanismes de qualité de service du segment A (c'est-à-dire du réseau d'accès) et du segment B (c'est-à-dire, du réseau domestique) qui diffèrent habituellement l'un de l'autre. Le pont de qualité de service active les communications entre eux, et son entité logique DEVRAIT être implémentée dans l'appareil d'accès domestique de la Rec. UIT-T J.190 ou dans la passerelle résidentielle.

10.3.1 Objectifs du pont de qualité de service

L'objectif du pont de qualité de service est d'établir la route de qualité de service de bout en bout en mettant logiquement à l'épreuve le mécanisme de qualité de service entre le segment A et le segment B, et de fournir une interface unifiée de qualité de service aux appareils terminaux en cachant les différents mécanismes de qualité de service appliqués au segment A.

10.3.2 Exigences fonctionnelles du pont de qualité de service

- *Lieu d'implémentation*

  La fonction de pont de qualité de service DEVRAIT être implémentée dans l'appareil d'accès domestique spécifié dans la Rec. UIT-T J.190 ou à un point d'interface différent des mécanismes de qualité de service définis dans d'autres architectures de qualité de service.

- *Direction de la signalisation de qualité de service*

  1) Au moins une fonction directionnelle de pont de qualité de service DOIT échanger de la signalisation de qualité de service provenant du segment A vers le segment B. Deux ponts de qualité de service directionnels sont aussi nécessaires lorsque le contrôle de la qualité de service est requis d'un appareil terminal d'extrémité vers le serveur d'application. La Figure 16 montre un aspect de pont de qualité de service.

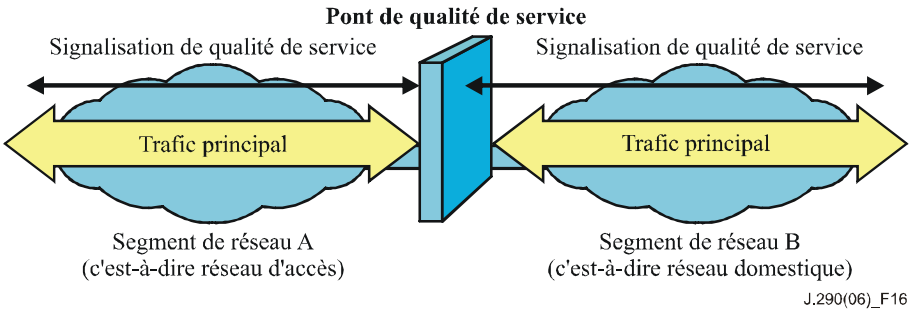


Figure 16 – Aspect du pont de qualité de service

  Le pont de QS, à la différence d'un pont de couche 2, DEVRAIT être situé sur la zone (Segment A/B à la Figure 16) où différents réseaux sont interfacés, et DEVRAIT fournir les sous-fonctions suivantes:

  a) initier, relayer et terminer la signalisation de QS de chaque segment,

  b) marquer, remarquer le trafic de signal principal,

  c) donner forme au trafic de signal principal.

  2) Le pont de QS DEVRAIT notifier aux appareils terminaux son indisponibilité comme pont de qualité de service, si le segment A (réseau d'accès) n'a pas de fonctions de qualité de service dans la direction amont.

- *Gestion*

  1) Le pont de QS DEVRAIT s'assurer que la politique de l'opérateur fonctionne avec la politique de QS du segment B (réseau domestique) éventuellement fournie par l'utilisateur final. Un utilisateur final PEUT fournir une fonction de gestion de politique pour le segment B.

  2) Le pont de QS DEVRAIT notifier aux deux parties le décalage des politiques de qualité de service entre le segment A et le segment B, s'il survient.

- *Fonction de pont*

  1) Le pont de QS DEVRAIT maintenir la priorité de la classe de qualité de service à la fois dans le segment A et le segment B, et fournir les tableaux de mappage entre leurs classes de qualité de service. La Figure 17 montre un aspect du mappage de classe de QS.

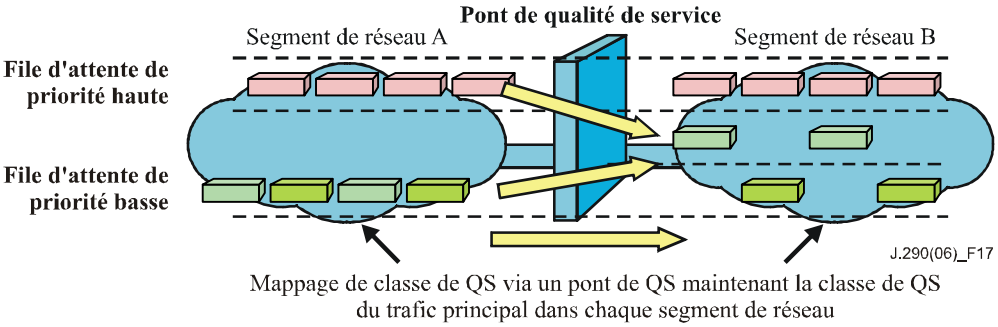


Figure 17 – Aspect de mappage de classe de QS

2) Le pont de QS DEVRAIT avoir des fonctions d'initiation, de relais et de terminaison de signalisation de QS dans les deux segments A et B. La Figure 18 montre un traitement de signalisation de QS.

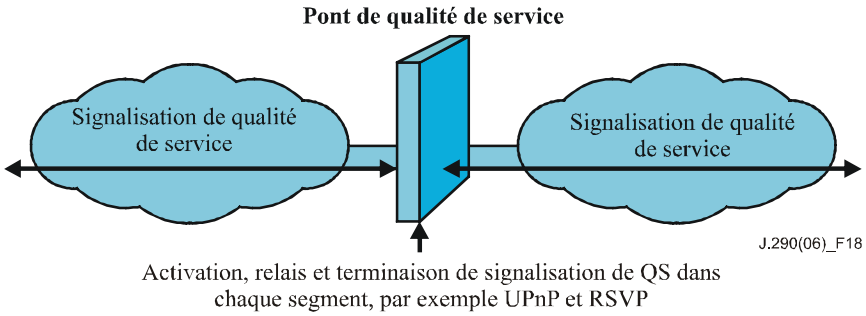


Figure 18 – Traitement de signalisation de QS

- *Politique*

L'approvisionnement de la qualité de service de bout en bout et les exigences du pont de qualité de service sont décrits dans les paragraphes précédents, cependant le mécanisme de priorité des paquets est nécessaire pour le contrôle réel de la qualité de service. La Figure 19 montre un exemple de flux de traitement de QS.

1) Classification:

   pour classer les étiquettes de qualité de service sur la base de la vérification et de l'établissement du paquet. Etablissement signifie ici étiquette de type de service, numéro de port UDP, protocole et adresse IP, etc.

2) Régulation:

   discriminer la confrontation des paquets en comparant le taux de trafic reçu et le régulateur provisionné. Ici le régulateur est une entité de politique, et plus spécifiquement signifie des tableaux de politique fournis par l'opérateur ou le consommateur.

3) Marquage:

   juger si le paquet satisfait aux critères, pour être transmis, sur la base des paramètres établis, pour être marqué (priorité suivante), ou être éliminé.

4) Mise en file d'attente et programmation:

   pour discriminer la sortie de file d'attente des sorties à placer dans le paquet d'étiquette de qualité de service. Procéder ensuite à la mise en file d'attente conformément à la pondération de réglage.

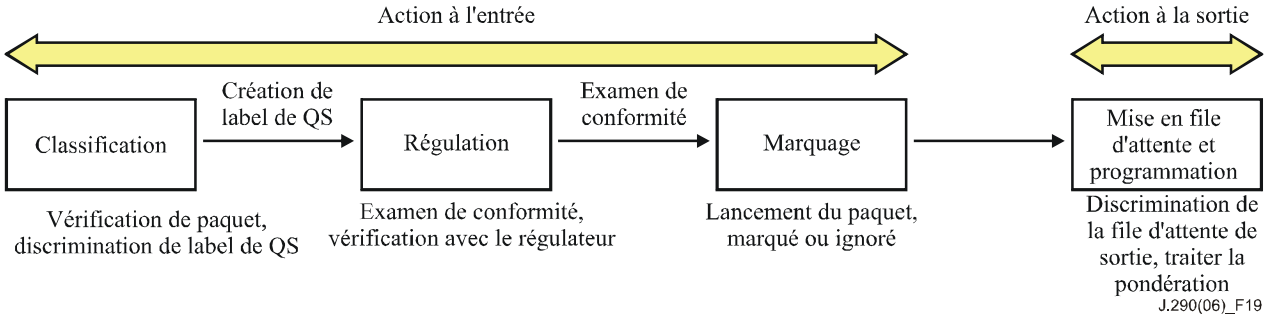


Figure 19 – Exemple de flux de traitement de QS

L'attribution de priorités aux paquets DEVRAIT prendre en charge la préséance IP, DSCP (point de code des services différenciés) dans le mécanisme de qualité de service DiffServ et/ou de classe de service défini dans IEEE802.1Q. La Figure 20 montre un aspect de la priorité de mise en file d'attente entre le cœur de réseau et le réseau d'accès. La politique de mise en file d'attente DOIT être fournie avec la priorité de type de service comme prétraitement de l'allocation de bande passante; pour des précisions sur les priorités de qualité de service, se référer au § 9/J.292.

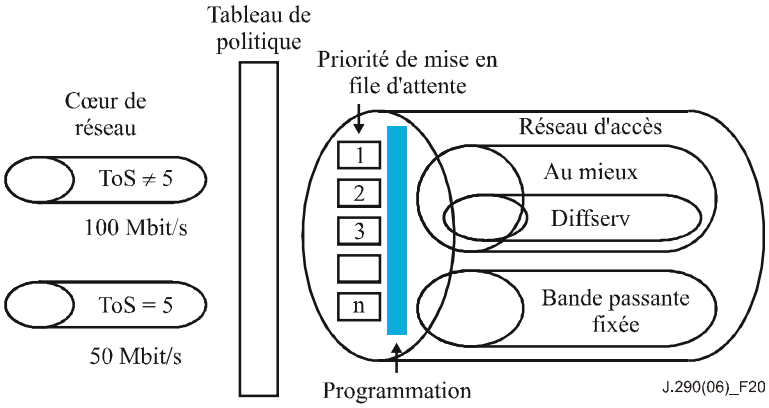


Figure 20 – Aspect de mise en file d'attente de priorité entre cœur de réseau et réseau d'accès

Appendice I

Relations entre service de type indépendant du support, de type câble et de type de QS

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

Le présent appendice est un supplément au Tableau 4 du § 10. Le Tableau I.1 montre les relations entre le service de type indépendant du support et le type de qualité de service pour les services à qualité garantie. Ce tableau montre une combinaison souhaitable entre le service et le type de qualité de service et n'exclut pas d'autres combinaisons possibles.

Tableau I.1 – Relations entre service de type indépendant du support et type de QS

	Bande passante préprovisionnée	**Fondé sur la session**	**DiffServ**	**Au mieux**
Télévision en diffusion	✓			
Vidéo à la carte	✓	✓		
VoIP	✓	✓		
Visiophone	✓	✓	✓	✓
Téléphone sur PC				✓

Le Tableau I.2 montre les relations entre le service de type câble et le type de qualité de service pour les services à qualité garantie. Ce tableau montre une combinaison souhaitable entre le type de service et le type de qualité de service et n'exclut pas d'autres combinaisons possibles.

Tableau I.2 – Relations entre service de type câble et type de QS

	Bande passante préprovisionnée	**Fondé sur la session**	**DiffServ**	**Au mieux**
Télévision en diffusion	✓			
Vidéo à la carte		✓		
VoIP		✓		
Visiophone		✓	✓	✓
Téléphone sur PC				✓

Bibliographie

[b-UIT-T J.112] Recommandation UIT-T J.112 (1998), *Systèmes de transmission pour services interactifs de télévision par câble*.

[b-UIT-T J.122] Recommandation J.122 (2002), *Systèmes de transmission de deuxième génération pour les services interactifs de télévision par câble – Câblo-modems pour protocole IP*.

[b-UIT-T J.125] Recommandation UIT-T J.125 (2004), *Confidentialité des liaisons pour les implémentations de câblo-modems*.

[b-UIT-T J.126] Recommandation UIT-T J.126 (2004), *Spécification de câblo-modem intégré*.

[b-UIT-T J.192] Recommandation UIT-T J.192 (2005), *Passerelle résidentielle assurant la remise des services de données par câble*.

[b-UIT-T J.200] Recommandation UIT-T J.200 (2001), *Architecture noyau mondiale commune – Environnement applicatif des services de télévision numérique interactive*.

[b-UIT-T J.201] Recommandation UIT-T J.201 (2004), *Harmonisation du format des contenus déclaratifs pour les applications de télévision interactive*.

[b-UIT-T J.202] Recommandation UIT-T J.202 (2005), *Harmonisation des formats de contenus procéduraux pour les applications de télévision interactive*.

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, 2007