

Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

J.292

(11/2006)

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

Câblo-modems

**Boîtiers adaptateurs de prochaine génération –
Architecture indépendante du support**

Recommandation UIT-T J.292

Recommandation UIT-T J.292

Boîtiers adaptateurs de prochaine génération – Architecture indépendante du support

Résumé

La présente Recommandation décrit une architecture de base indépendante du support de transport et applicable aux boîtiers adaptateurs de prochaine génération, l'objectif étant de permettre aux fournisseurs de services d'offrir des services perfectionnés, actuels ou futurs, indépendamment du support de transport qui sera adopté à l'avenir. Dans la présente Recommandation, on suppose que tous les contenus sont acheminés sur des paquets IP, avec un mécanisme approprié de commande de la qualité de service. La présente Recommandation contient une description des aspects fonctionnels principaux des boîtiers adaptateurs de la prochaine génération: adaptabilité de la ressource du réseau, gestion des ressources session et de communications bidirectionnelles authentifiées et sécurisées et mécanisme de commande de la qualité de service.

Source

La Recommandation UIT-T J.292 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

	Página
1	Domaine d'application 1
2	Références normatives..... 1
3	Définitions 1
4	Abréviations et acronymes 2
5	Conventions 3
6	Architecture des boîtiers adaptateurs de prochaine génération, indépendante du support 4
6.1	Architecture de référence 4
6.2	Attributs des boîtiers adaptateurs de prochaine génération pour un environnement indépendant du support..... 5
7	Équipement des locaux client 7
7.1	Fonctionnalité des dispositifs CPE..... 7
7.2	Architecture de protocole des applications de transport vidéo et de données 8
7.3	Protocole de signalisation entre segments CPE et CDN 9
7.4	Corrélation entre les flux multidiffusion et les flux de transport TS..... 9
7.5	Rétablissement en cas de perte de paquets 10
7.6	Synchronisation d'horloge de flux TS 10
7.7	Régulation du zapping 11
7.8	Connaissance de l'emplacement 11
8	Multidiffusion IP 11
8.1	Multidiffusion IP 11
8.2	IGMP 12
8.3	Surveillance IGMP 12
8.4	Protocole de routage de multidiffusion 12
9	Priorité en matière de qualité de service et mappage de la politique..... 13
9.1	Priorité en matière de qualité de service..... 13
9.2	Mappage de la politique de QS 16
10	Diffusion IP et point de commutation des canaux..... 17
	Bibliographie..... 18

Recommandation UIT-T J.292

Boîtiers adaptateurs de prochaine génération – Architecture indépendante du support

1 Domaine d'application

La présente Recommandation décrit une architecture de base de boîtiers adaptateurs de prochaine génération STB qui est indépendante du support de transport. Les opérateurs et les équipementiers PEUVENT choisir de continuer à prendre des décisions visant à investir dans des réseaux et des produits. Cette architecture définit plus précisément l'adaptabilité de la ressource du réseau, la gestion des ressources session et de communications bidirectionnelles authentifiées et sécurisées ainsi qu'un mécanisme de commande de la qualité de service sur des environnements tout IP. L'architecture en question permet de faire face à la croissance de la vidéo à la carte, de la télévision numérique haute définition, de réseaux domestiques gérés reliant un large éventail de dispositifs client et, enfin, de services multimédias IP dont la téléphonie IP, la visiophonie et les jeux entre plusieurs joueurs. La présente Recommandation a pour objet de décrire les fonctionnalités essentielles des boîtiers adaptateurs de prochaine génération, indépendamment du support de transport. Dans la mise en œuvre proprement dite des fonctionnalités de l'architecture NG-STB-A, il convient d'utiliser le mot DOIT avec la Recommandation UIT-T J.290. Enfin, la présente Recommandation offre quelques solutions techniques à titre d'exemple, afin d'aider le lecteur à mieux comprendre le texte mais ne vise pas à établir les prescriptions applicables aux boîtiers adaptateurs STB indépendants du support. Il convient de noter que la future Recommandation définira des solutions techniques applicables à ces boîtiers STB indépendants du support.

2 Références normatives

Aucune.

3 Définitions

La présente Recommandation définit les termes suivants:

3.1 réseau de distribution du contenu (CDN): le réseau CDN comprend un réseau central et un réseau d'accès où la fourniture du contenu est contrôlée par un mécanisme de routage par paquets et de commande de la qualité du service.

3.2 équipement des locaux client (CPE): l'équipement CPE comprend des dispositifs vidéo d'abonné (SVD), une passerelle résidentielle (RGW) et des dispositifs facultatifs de réseautage domestiques.

3.3 multidiffusion IP: est utilisée pour la diffusion IP du point de vue de l'efficacité d'utilisation de la largeur de bande sur les segments tête de réseau, CDN (réseau de distribution du contenu) et CPE.

3.4 canaux bidirectionnels de communication authentifiée: ces canaux sont utilisés pour la gestion des clés d'accès conditionnel renouvelable, la gestion à distance des unités SVD, des mises à jour de microprogrammes téléchargeables, des données d'applications interactives privées et la reconfiguration des algorithmes de chiffrement entre la tête de réseau et une unité SVD.

3.5 flux de transport (TS, *transport stream*): le flux de transport décrit dans la présente Recommandation utilise un certain flux multidiffusion qui est identifié par l'adresse de groupe multidiffusé, le numéro de port UDP, etc.

3.6 service de portail (PS, *portal services*): élément fonctionnel qui assure les fonctions de gestion et de traduction entre le réseau HFC et le réseau domestique.

3.7 régulation du zapping: mécanisme de régulation permettant de rejoindre et de quitter un groupe multidiffusé, sachant que la séquence de protocole IGMP/MLD est nécessaire dans les dispositifs CPE conformes aux boîtiers adaptateurs de prochaine génération.

3.8 passerelle domestique: dispositif qui fournit des fonctionnalités d'interconnexion entre le réseau d'accès et le réseau domestique [b-UIT-T J.190].

NOTE – Les modalités d'application de la fonctionnalité de passerelle domestique conforme à la Rec. UIT-T J.190 à divers réseaux DEVRAIENT être examinées dans un proche avenir.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations suivantes:

ARQ	demande automatique de répétition (<i>automatic repeat request</i>)
BE	service au mieux (<i>best effort</i>)
BGP	protocole de passerelle frontière (<i>border gateway protocol</i>)
CA	accès conditionnel (<i>conditional access</i>)
CAS	système d'accès conditionnel (<i>conditional access system</i>)
CDN	réseau de distribution du contenu (selon la définition de [b-Rec. UIT-T J.282] (<i>content distribution network</i>))
CoS	classe de service (<i>class of service</i>)
CPE	équipement des locaux client (<i>customer premises equipment</i>)
DB	base de données (<i>database</i>)
DHCP	protocole de configuration dynamique du serveur (<i>dynamic host configuration protocol</i>)
DiffServ	architecture de services différenciés pour le trafic du réseau (<i>differentiated services architecture for network traffic</i>)
DOCSIS	spécification d'interface du service de transmission de données par câble (<i>data over cable service interface specification</i>)
DSCP	point de code DiffServe (<i>DiffServcode point</i>)
DSLAM	multiplexeur d'accès DSF (<i>digital subscriber line access multiplexer</i>)
DTV	télévision numérique (<i>digital TV</i>)
EMM	message de gestion d'habilitation (<i>entitlement management message</i>)
FEC	correction d'erreur directe (<i>forward error correction</i>)
GigE	Ethernet gigabit (<i>gigabit Ethernet</i>)
HE	tête de réseau (<i>headend</i>)
HGW	passerelle domestique (<i>home gateway</i>)
IGMP	protocole de gestion de groupe Internet (<i>Internet group management protocol</i>)
IP	protocole Internet (<i>Internet protocol</i>)
Couche 3	couche de réseau 3 dans la pile OSI (<i>network layer 3 in OSI stack</i>)
LDPC	codage de contrôle de parité à faible densité (<i>low-density parity check</i>)
MAC	commande d'accès au support physique (<i>media access control</i>)
MLD	protocole Multicast Listener Discovery (<i>multicast listener discovery</i>)

MPEG	groupe d'experts pour les images animées (<i>motion picture experts group</i>)
NAT	traduction des adresses de réseau (<i>network address translation</i>)
NG-STB	boîtiers adaptateurs de prochaine génération (<i>next generation set-top box</i>)
NG-STB-MI-A	architecture indépendante du support des boîtiers adaptateurs de prochaine génération (<i>next generation set-top box media independent architecture</i>)
NIT	table d'informations sur le réseau (<i>network information table</i>)
OLT	terminaison de ligne optique (<i>optical line terminal</i>)
OSPF	plus court chemin ouvert en premier (<i>open shortest path first</i>)
PCR	référence temporelle du programme (<i>program clock reference</i>)
PID	identificateur de paquet (<i>packet identifier</i>)
PIMSM	mode de multidiffusion épars indépendant du protocole (<i>protocol independent multicast sparse mode</i>)
QS	qualité de service
RGW	passerelle domestique (<i>residential gateway</i>)
RTP	protocole de transport en temps réel (<i>real time protocol</i>)
RTSP	protocole de diffusion directe en temps réel (<i>real-time streaming protocol</i>)
SI	information sur les services (<i>service information</i>)
STB	boîtier adaptateur (<i>set-top-box</i>)
SVD	unités vidéo de l'abonné (<i>subscriber video device</i>)
TCP	protocole de commande de transmission (<i>transmission control protocol</i>)
TLS	sécurité de la couche transport (<i>transport layer security</i>)
TVHD	télévision à haute définition (<i>high definition TV</i>)
ToS	type de service (<i>type of service</i>)
UPnP	(dispositif) universel prêt à fonctionner (<i>universal plug and play</i>)
VCO	oscillateur à commande par tension (<i>voltage-controlled oscillator</i>)
VoD	vidéo à la carte (<i>video on demand</i>)
VoIP	téléphonie utilisant le protocole Internet (<i>voice over Internet protocol</i>)

5 Conventions

Les mots ci-après, qui sont employés dans l'ensemble de la présente Recommandation pour indiquer la signification de certaines prescriptions, figurent en MAJUSCULES, à savoir:

DOI(VEN)T"	Ce mot ou l'adjectif "REQUIS(E)(S)" indiquent l'absolue prescription de l'élément dans la présente Recommandation.
"NE DOI(VEN)T PAS"	Cette phrase indique l'absolue interdiction de l'élément dans la présente Recommandation.
"DEVRAI(EN)T"	Ce mot ou l'adjectif "RECOMMANDE(E)(S)" indiquent qu'il peut exister des raisons valables, dans certaines circonstances, de ne pas tenir compte de cet élément, mais que toutes les implications devraient être comprises et que le cas devrait être soigneusement soupesé avant de faire un choix différent.

"NE DEVRAI(EN)T PAS"	Ce libellé indique qu'il peut exister des raisons valables, dans des circonstances particulières, de considérer le comportement énoncé comme étant acceptable ou même utile, mais que toutes les implications devraient être bien comprises et que le cas devrait être soigneusement soupesé avant d'implémenter un quelconque comportement décrit par ce libellé.
"PEU(VEN)T"	Ce mot ou l'adjectif "FACULTATIF(VE)(S)" indiquent que l'élément est véritablement en option. Un vendeur peut choisir de l'inclure parce qu'une place de marché l'exige ou parce qu'il améliore le produit, par exemple, tandis qu'un autre vendeur peut omettre ce même élément.

6 Architecture des boîtiers adaptateurs de prochaine génération, indépendante du support

Environnement

Outre les points figurant au § 6 de [b-UIT-T J.290], il y a lieu de signaler les points ci-après qui sont des attributs essentiels obligatoires de l'architecture des boîtiers adaptateurs de prochaine génération (NGSTB) dans un environnement de réseau IP indépendant du support:

- *adaptabilité de la ressource du réseau.* Permet à l'opérateur de réseau d'utiliser plus efficacement la largeur de bande du réseau, cela grâce à des systèmes de rétablissement en cas de perte de paquets, à la suppression du trafic résiduel dû à un zappage des canaux, à la gestion unifiée de la qualité de service de bout en bout entre la tête du réseau et une unité vidéo d'abonné (SVD) conformément à l'architecture des boîtiers adaptateurs NGSTB indépendante du support (NG-STB-MI-A), conjointement avec le codec audio/vidéo évolué décrit dans [b-UIT-T J.290].
- *Transfert de flux de transport TS MPEG-2 sur le réseau IP.* Permet à l'opérateur de réseau de répartir les flux de transport dans un environnement indépendant du support, moyennant l'utilisation d'une suite de protocoles Internet normalisés avec des informations de description des flux spécifiées pour la multidiffusion IP.
- *Synchronisation d'horloge résiliente des flux de transport TS avec la tête du réseau.* Permet à toutes les unités SVD conformes à l'architecture NG-STB-MI-A d'éviter l'excès ou le défaut de remplissage des tampons de reproduction dans l'environnement de réseau IP.
- *Moteur commun de présentation.* Permet à une unité SVD conforme à l'architecture NG-STB-MI-A de prendre en charge les moteurs de présentation définis dans [b-UIT-T J.200] et [b-UIT-T J.201].
- *Connaissance de l'emplacement.* Permet à l'opérateur de réseau de contrôler la zone de distribution des flux de transport en fonction de l'emplacement des unités SVD. La connaissance de l'emplacement de l'unité SVD est facultative.
- *Canaux bidirectionnels authentifiés et sécurisés via le réseau IP.* Conformément à la sécurité de la couche de transport (TLS, *transport layer security*) 1.0 assurée dans une unité SVD conforme à l'architecture NG-STB-MI-A, des canaux bidirectionnels authentifiés et sécurisés sont mis en place entre la tête du réseau et une unité SVD. Ils sont utilisés pour la gestion des clés d'accès conditionnel renouvelable, la gestion à distance des unités SVD, des mises à jour de microprogrammes téléchargeables, des données d'applications interactives privées et la reconfiguration des algorithmes de chiffrement.

6.1 Architecture de référence

L'architecture de référence de l'infrastructure d'un service de distribution de contenu IP est représentée à l'aide du diagramme de la Figure 1. On y trouvera également un résumé des relations

entre les principaux segments du réseau, par exemple, l'équipement CPE (équipement des locaux client), y compris l'unité vidéo de l'abonné (SVD, *subscriber video device*) et les dispositifs de réseau domestique comme la passerelle domestique (RGW, *residential gateway*), le réseau de fourniture du contenu (CDN, *content delivery network*) qui PEUT être défini séparément sous la forme de réseaux de base et de réseaux métropolitains, l'Internet et la tête de réseau (HE, *headend*). Dans un environnement indépendant du support, tous les services de distribution du contenu sont assurés par un support de transmission du trafic monodiffusion ou multidiffusion IP. La multidiffusion IP DEVRAIT être utilisée pour la diffusion IP du point de vue de l'efficacité de la largeur de bande sur les segments tête du réseau, réseau CDN et équipement CPE.

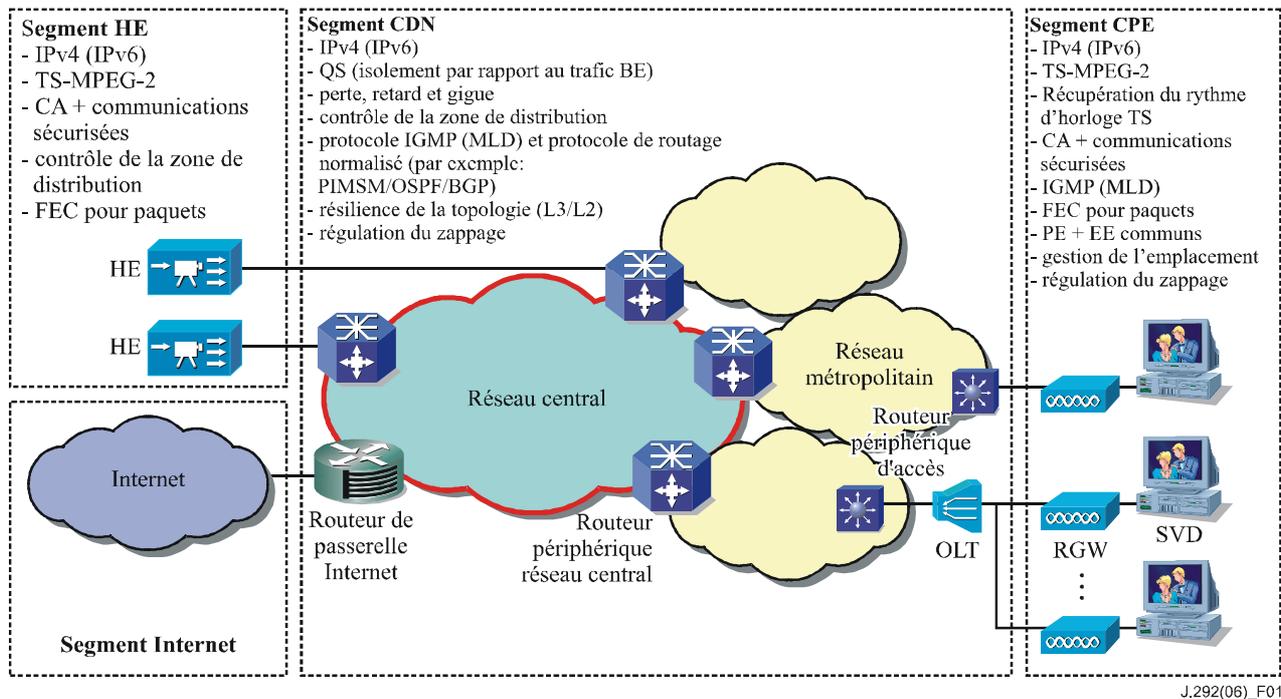


Figure 1– Architecture de référence de l'infrastructure d'un service de distribution de contenu IP

6.2 Attributs des boîtiers adaptateurs de prochaine génération pour un environnement indépendant du support

6.2.1 Architecture des services de distribution du contenu

L'architecture NG-STB-MI-A DEVRAIT, au minimum, posséder les attributs ci-après, en plus de ceux indiqués au § 6.2.1 de [UIT-T J.290].

- *Distribution du contenu fondée sur le protocole Internet.* Le protocole IP est choisi comme couche de support de base pour tous les services de distribution du contenu. Tous les dispositifs conformes à l'architecture NG-STB-MI-A sont nécessaires pour la prise en charge du protocole IPv4 et de ses possibilités d'extension vers l'IPv6. Il est également possible d'utiliser la configuration de pile double IPv4/v6. Des mécanismes d'autoconfiguration comme le protocole DHCP sont également requis pour offrir une connectivité IP sans pour autant nécessiter une configuration manuelle.
- *Corrélation entre le flux multidiffusion et le flux de transport (TS).* Le flux de transport utilise un certain flux multidiffusion, identifié par une adresse de groupe multidiffusé, un numéro de port UDP, etc. Il est recommandé d'attribuer une adresse de groupe différente à chaque flux de transport. Toutes les unités SVD conformes à l'architecture NG-STB-MI-A

sont nécessaires pour obtenir des informations de flux multidiffusion correspondant au flux de transport que l'unité SVD veut reproduire.

- *Régulation du zapping.* Il faut un mécanisme de régulation dans les équipements CPE conformes à l'architecture NG-STB-MI-A pour les scénarios de zapping du contenu, où l'unité SVD change successivement les groupes multidiffusés (c'est-à-dire des flux de transport) à grande vitesse. De ce fait, le trafic résiduel des groupes qui sont déjà sortis PEUT causer un encombrement dans le segment CPE.
- *Rétablissement en cas de perte de paquets.* Afin d'assurer la qualité de transmission des flux de transport (TS, *transport stream*), il faut que toutes les unités SVD conformes à l'architecture NG-STB-MI-A offrent un mécanisme de rétablissement en cas de perte de paquets.
- *Synchronisation d'horloge des flux de transport (TS).* Pour synchroniser la temporisation de reproduction audio/vidéo avec le codeur dans le segment tête du réseau, il faut un mécanisme robuste de régénération d'horloge des flux TS, même si l'on constate une gigue de réception des paquets et/ou des pertes de paquets avec les informations de référence temporelle du programme (PCR) dans le support de transmission IP.
- *Sortie vidéo haute définition.* Elle est obligatoire, même pour l'unité SVD de base dans un environnement indépendant du support.

6.2.2 Segment du réseau: CPE

Le segment CPE comprend des unités vidéo de l'abonné (SVD), une passerelle domestique (RGW) et des dispositifs facultatifs de réseau domestique auxquels les unités SVD et la passerelle RGW sont rattachées. L'unité SVD est un dispositif vidéo conforme à l'architecture NG-STB-MI-A qui compte un syntoniseur, par exemple des boîtiers adaptateurs ou des postes de télévision numérique autonomes (DTV, *standalone digital TV*). La passerelle RGW est située à la périphérie du segment CPE et logée dans un dispositif de desserte d'accès du segment CDN. Elle assure aussi l'accès Internet aux autres équipements CPE. La passerelle RGW différencie et protège le flux de transport entrant du trafic Internet fourni "au mieux". Elle doit aussi différencier, sur le plan du service, le trafic sortant qui va du réseau domestique au segment CDN. Elle PEUT aussi gérer la qualité de service de ce réseau. S'agissant du dispositif de desserte d'accès au réseau CDN auquel une passerelle RGW est connectée, les équipements ci-après PEUVENT être utilisés mais pas exclusivement: la terminaison de ligne optique (OLT, *optical line terminal*), le multiplexeur DSLAM et le commutateur de la couche 2/3.

6.2.3 Segment du réseau: CDN

Les flux de transport sont répartis par l'intermédiaire du segment CDN. Le trafic Internet "au mieux" PEUT être multiplexé via des routeurs de passerelle Internet. Le segment CDN DEVRAIT ménager une largeur de bande suffisante pour accueillir tous les flux de transport et l'utilisation de cette largeur de bande DEVRAIT être garantie même si le trafic Internet "au mieux" augmente. On se reportera au [b-UIT-T J.282] pour le mécanisme de garantie de la largeur de bande. De plus, le segment CDN DEVRAIT être résilient et éviter de présenter un point de défaillance isolé. On se reportera au [b-UIT-T J.283] pour les moyens d'accroître la résilience du réseau IP.

En plus des prescriptions indiquées dans [UIT-T J.290], les dispositifs du réseau conformes à l'architecture NG-STB-MI-A dans le segment CDN DEVRAIENT prévoir un mécanisme de contrôle de la qualité si les dispositifs assurent à la fois le trafic Internet "au mieux" et le trafic du flux de transport à haute priorité provenant du segment tête du réseau. A titre d'exemple de mécanismes du contrôle de la qualité, IEEE 802.1p spécifie l'identificateur de priorité inséré dans des trames Ethernet.

6.2.4 Segment du réseau: tête du réseau

Le segment tête du réseau DEVRAIT être élaboré sur la base du protocole IP. Il faut une largeur de bande GbE ou supérieure au niveau des interfaces de réseau pour assurer la distribution du contenu TVHD multicanal. La technique de FEC pour paquets DEVRAIT être implémentée conformément à l'application de cette même technique dans une unité SVD. Voir [UIT-T J.290] pour d'autres caractéristiques concernant le segment tête du réseau.

6.2.5 Segment du réseau: Internet

On peut considérer que le trafic du segment Internet est un trafic entrant dans le segment CDN, acheminé via des routeurs de passerelle Internet et vice versa. Ces routeurs sont nécessaires si l'on veut disposer d'une capacité suffisante pour bloquer toute anomalie du trafic de l'Internet à destination des dispositifs présents dans les segments tête du réseau et CDN.

7 Equipement des locaux client

7.1 Fonctionnalité des dispositifs CPE

- *Unités vidéo de l'abonné (SVD)*. On trouvera au Tableau 1 la liste des fonctions des unités SVD de base ainsi que des exemples d'options évolutives. Une unité SVD de base (non professionnelle) est définie comme ayant les fonctionnalités minimales requises dans l'architecture NG-STB-MI-A. Dans les unités SVD professionnelles on trouve diverses options évolutives dont le choix est laissé à l'appréciation des fournisseurs, des opérateurs de réseau et des détaillants.

Tableau 1– Fonctionnalités des unités SVD de base et évoluées

Fonctionnalités de l'unité SVD de base	Fonctions évolutives facultatives de l'unité SVD (Exemples)
<ul style="list-style-type: none">• IPv4;• Possibilités d'extension future IPv4 – IPv6;• IGMPv2;• Possibilités d'extension future IGMPv2 – MLDv2;• Client DHCP;• Sortie haute définition;• Corrélation flux multidiffusion/TS;• Régulation du zapping;• TLS 1.0;• Technique FEC pour paquets;• Synchronisation d'horloge de TS;• Connaissance de l'emplacement.	<ul style="list-style-type: none">• Configuration de pile double IPv4/IPv6, IPv6;• MLDv2;• IGMPv3;• Technique FEC avancée pour paquets et/ou ARQ/FEC pour paquets au niveau local.

- *Passerelle domestique (RGW)*. La méthode de routage de la couche 3 ou encore la méthode de routage par pont de la couche 2 PEUT être utilisée pour implémenter une passerelle RGW. Afin d'offrir l'accès Internet à d'autres dispositifs CPE, il convient de recourir à la méthode de la couche 3 avec une traduction des adresses de réseau (NAT, *network address translator*), qui est plus générale, car il faut assurer la protection des autres dispositifs CPE contre l'accès malveillant des hôtes en dehors du segment CPE. Toutefois, les fonctions ci-après (voir le Tableau 2) sont nécessaires en tant que passerelle RGW de la couche 3.

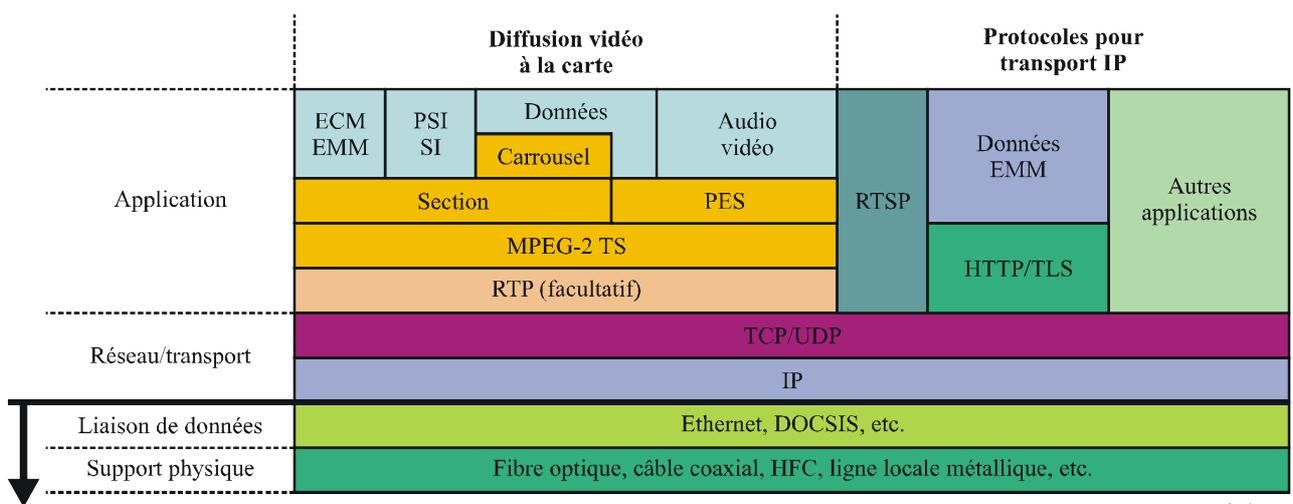
Tableau 2– Fonctionnalités des passerelles RGW de base et évoluées (couche 3)

Fonctionnalités de la passerelle RGW de base	Fonctions évolutives facultatives de la passerelle RGW (Exemples)
<ul style="list-style-type: none"> • IPv4; • Possibilités d'extension future IPv4 – IPv6; • Mode proxy IGMPv2; • Possibilités d'extension future du mode proxy IGMPv2 vers le mode proxy MLDv2; • Client/serveur DHCP; • Connectivité Internet; • Franchissement NAT pour IPv4; • Connaissance de l'emplacement. 	<ul style="list-style-type: none"> • Configuration de pile double IPv4/IPv6, IPv6; • Mode proxy MLDv2; • Mode proxy IGMPv3; • ARQ/FEC pour paquets au niveau local vers l'unité SVD.

– *Dispositif de réseau domestique facultatif.* Un réseau domestique PEUT être mis en place à l'intérieur du segment CPE avec d'autres dispositifs qui contiennent des fonctions de commutation comme les commutateurs Ethernet. Pour obtenir davantage d'informations concernant le réseau domestique, par exemple sur la commande de la qualité de service, on se reportera au [UIT-T J.290].

7.2 Architecture de protocole des applications de transport vidéo et de données

L'architecture de protocole des applications de transport vidéo et de données est représentée à la Figure 2. Tous les dispositifs conformes à l'architecture NG-STB-MI-A utilisent le protocole IP comme support de transmission de base pour assurer l'indépendance du support dans tous les segments du réseau. Les applications de transport vidéo, comme la diffusion et la vidéo à la carte, utilisent des flux de transport TS MPEG-2 et un ou plusieurs paquets de flux TS sont transférés comme messages RTP/UDP. A noter qu'il est possible d'utiliser le protocole TCP au lieu du protocole UDP pour des services de monodiffusion IP comme la vidéo à la carte. Toutefois, dans les services de diffusion IP, il est recommandé d'utiliser le protocole RTP/UDP avec la multidiffusion IP, compte tenu de l'efficacité de la largeur de bande sur les segments de réseau tête de réseau, CDN et CPE, où une seule copie des paquets est nécessaire sur les liaisons de transmission entre dispositifs de réseaux adjacents.



J.292(06)_F02

NOTE – Le protocole TCP est nécessaire pour la transmission des protocoles RTSP et HTTP/TLS.

Figure 2– Architecture de protocole des applications de transport vidéo et de données

Il existe deux versions du protocole IP, IPv4 et IPv6, la principale différence entre ces deux versions étant la longueur des adresses. Des procédures concernant la distribution en mode multidiffusion, la signalisation et la gestion des adresses ont été définies pour chaque protocole. Tous les dispositifs CPE conformes à l'architecture NG-STB-MI-A doivent, au minimum, prendre en charge la version IPv4 et les possibilités d'extension future à la version IPv6. Il est également possible d'utiliser la configuration de pile double IPv4/v6. Il est recommandé de fournir en ligne une reconfiguration des versions du protocole IP, par exemple avec le téléchargement de microprogrammes via le segment CDN.

S'il est nécessaire d'assurer une protection plus sécurisée du contenu que celle fournie par le système CAS existant, on chiffrera un groupe de paquets de flux TS MPEG-2 dans une charge utile RTP/UDP. Ainsi, la Figure 3 donne un exemple de message RTP/UDP avec des paquets de flux TS MPEG-2 chiffrés. Cet exemple contient des paquets de flux TS MPEG-2 chiffrés, un identificateur de clé de chiffrement et des informations de mise à jour essentielles.

En-tête RTP	ID clé	Groupe chiffré de paquets de flux TS MPEG-2	Informations de mise à jour essentielles
-------------	--------	---	--

Figure 3– Exemple de message RTP/UDP avec des paquets de flux TS MPEG-2

7.3 Protocole de signalisation entre segments CPE et CDN

On utilise le protocole IGMP et/ou MLD comme mécanisme de sélection de programmes des unités SVD. S'agissant du protocole homologue IGMP/MLD, il est possible d'utiliser une passerelle RGW ou un routeur périphérique d'accès du segment CDN. Dans le cas de la passerelle RGW de la couche 3, il DEVRAIT assumer les fonctions de proxy IGMP/MLD comme routeur (interrogateur) IGMP/MLD pour les unités SVD et comme hôte IGMP/MLD pour le routeur périphérique d'accès.

Il est recommandé d'utiliser le protocole IGMPv2, ou à titre facultatif, le protocole IGMPv3 pour un environnement IPv4 et le protocole MLDv2 pour un environnement IPv6. A noter qu'en cas d'utilisation du protocole IGMPv3, l'interopérabilité du protocole IGMPv2 DOIT être garantie comme cela est indiqué dans le Document RFC 3376.

7.4 Corrélation entre les flux multidiffusion et les flux de transport TS

On trouvera ci-après la liste des informations de corrélation nécessaires pour obtenir un certain flux de transport.

- 1) ID de service;
- 2) ID de flux de transport;
- 3) ID de réseau;
- 4) Version IP (v4 ou v6);
- 5) Protocole de transport (TCP ou UDP);
- 6) Groupe multidiffusé ou adresse de destination;
- 7) Numéro du port de destination;
- 8) Utilisation de l'en-tête RTP;
- 9) Type de FEC;
- 10) Format de trame.

Les informations indiquées ci-après ne sont pas obligatoires mais sont souhaitables du point de vue de la sécurité, de l'application générale et de la facilité d'exploitation des unités SVD.

- 11) Adresse IP source;
- 12) Numéro de port source;

- 13) Taille de paquets IP;
- 14) Taille de paquets de flux TS;
- 15) Débit du flux TS;
- 16) Informations de flux FEC, y compris les adresses IP de source/destination et les numéros de port, si des informations de flux différentes du flux de transport sont utilisées pour les paquets FEC.

Il existe plusieurs systèmes pour distribuer les informations de corrélation décrites plus haut: on distingue la diffusion sélective et la recherche active. En mode de diffusion sélective, il est possible que l'information soit toujours diffusée sous forme de table d'information sur le réseau (NIT, *network information table*), à l'aide d'un flux multidiffusion dans la bande des flux de transport ou d'un certain type de flux multidiffusion bien connu et hors bande que toutes les unités SVD doivent écouter. En revanche, dans le mode de recherche active, un serveur fournissant l'information de corrélation PEUT être utilisé lorsque toutes les unités SVD doivent accéder à ce serveur.

7.5 Rétablissement en cas de perte de paquets

Une méthode de correction d'erreur est utile pour le rétablissement en cas de perte de paquets. Compte tenu des scénarios de perte de paquets en rafale, certaines techniques d'entrelacement sont efficaces, le calcul de la FEC étant réalisé entre des paquets dont les ordres de transmission sont différents entre eux. Comme le montre la Figure 4 qui fournit un exemple de calcul de la FEC, on voit que le rétablissement de 25 paquets consécutifs perdus est possible.

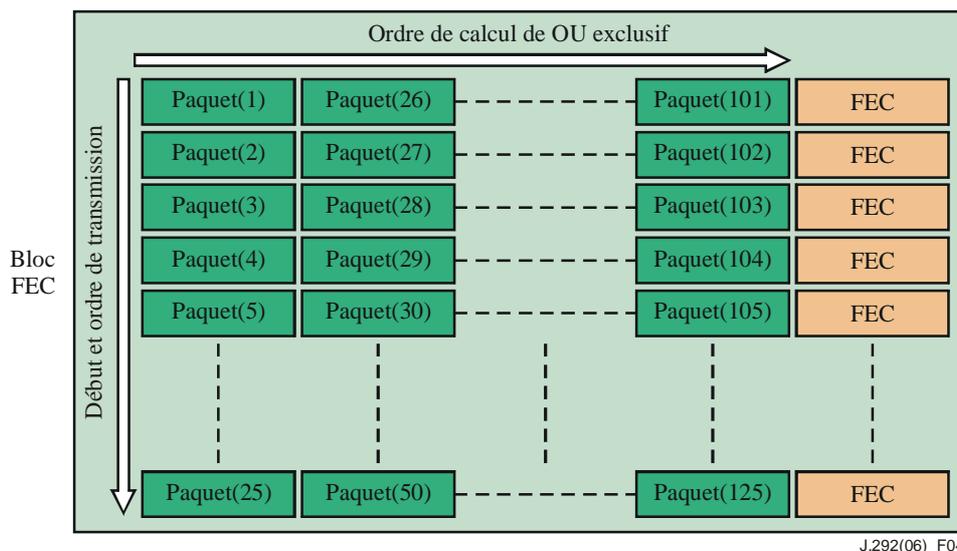


Figure 4– Exemple de calcul de la FEC

Certaines techniques de FEC perfectionnées comme le codage de contrôle de parité à faible densité (LDPC) PEUVENT permettre une meilleure performance du rétablissement en cas de perte de paquets. De plus, la retransmission de paquets au niveau local entre la passerelle RGW et l'unité SVD est importante.

7.6 Synchronisation d'horloge de flux TS

L'horloge de référence du décodeur est contrôlée de façon à permettre une synchronisation avec l'horloge du codeur dans le segment tête de réseau à l'aide d'un mécanisme à bouclage de phase (PLL, *phase-locked loop*) entre les paquets PCR transmis et un oscillateur à commande par tension réglable (VCO, *voltage-controlled loop*) à l'intérieur du décodeur. Toutefois, dans une unité SVD,

le décodeur ne DEVRAIT pas utiliser directement les paquets PCR transmis par l'intermédiaire du segment CDN car les giges d'un réseau IP type sont beaucoup plus importantes que la gigue tolérée de la référence PCR (500 ns), définie dans le système MPEG-2. Par conséquent, il faut un mécanisme de compensation de la gigue pour satisfaire à la tolérance de gigue du système MPEG-2. La méthode de compensation de la gigue dépend de l'implémentation et sort du cadre de la présente Recommandation.

7.7 Régulation du zapping

Le zapping, c'est-à-dire les changements fréquents de groupes multidiffusés, entraîne une augmentation du trafic occasionnel et, dans le même temps, un gaspillage de la largeur de bande. Afin de favoriser l'utilisation la plus efficace de la largeur de bande, un mécanisme de régulation du zapping DEVRAIT être implémenté dans des dispositifs appropriés conformes à l'architecture NG-STB-MI-A qui prennent en charge un protocole de commande multidiffusion hôte-routeur c'est-à-dire, le protocole IGMP et/ou MLD.

Il existe deux façons de parvenir à la régulation du zapping. La première consiste à restreindre le nombre de demandes de canaux émanant d'une unité SVD pendant une période de temps spécifiée, ce qui signifie que l'unité SVD ne demande pas les canaux inutiles. Cette méthode est classée dans la catégorie commande côté récepteur du trafic multidiffusion.

L'autre méthode consiste à restreindre le nombre d'inscriptions possibles d'adresses de groupes multidiffusés sur une table de transfert multidiffusion dans des dispositifs de réseau intermédiaire acceptant des messages de commande IGMP et/ou MLD en provenance de l'unité SVD. Les dispositifs de réseau ci-après sont possibles: une passerelle RGW et des dispositifs de desserte d'accès CDN comme un commutateur de couche 2/3 avec une capacité IGMP/MLD (surveillance). Dans ces dispositifs, le transfert multidiffusion est géré avec la table de transfert multidiffusion qui établit des associations entre une adresse de groupes multidiffusés et un ensemble de ports de destination. En limitant le nombre d'inscriptions possibles d'adresses de groupes multidiffusés par port de destination ou adresse MAC de l'unité SVD, il est possible de réguler le zapping. Cette méthode limite sensiblement la largeur de bande maximale admissible du trafic multidiffusion par port de destination ou adresse MAC de l'unité SVD, de sorte que cette méthode est classée dans la catégorie commande côté émetteur du trafic multidiffusion.

7.8 Connaissance de l'emplacement

Etant donné que le réseau CDN IP PEUT couvrir une zone relativement étendue, c'est-à-dire de niveau national ou même mondial, il est à craindre qu'une unité SVD, dans une région donnée, puisse avoir accès à des flux de transport destinés à d'autres régions. Par conséquent, un mécanisme de connaissance de l'emplacement PEUT être nécessaire pour contrôler la zone de distribution des flux de transport en fonction de l'emplacement régional des unités SVD.

L'emplacement régional des dispositifs de desserte d'accès client dans le segment CDN peut être géré par l'opérateur du réseau CDN et il faut connaître l'emplacement de la passerelle RGW et des unités SVD pour assurer un lien avec ces dispositifs. Il PEUT être nécessaire d'appliquer certains mécanismes d'authentification des ports comme la Norme IEEE 802.1X entre chaque paire de dispositifs adjacents, par exemple, la passerelle RGW et le dispositif de desserte d'accès client correspondant, la passerelle RGW et les unités SVD, etc.

8 Multidiffusion IP

8.1 Multidiffusion IP

La multidiffusion IP est la transmission d'un datagramme IP à un "groupe d'hôtes", c'est-à-dire un ensemble de zéros ou de plusieurs hôtes identifiés par une adresse de destination IP unique. Un datagramme de multidiffusion est remis à tous les membres de son groupe d'hôtes de destination

comme datagrammes IP monodiffusion normaux. L'appartenance à un groupe d'hôtes est dynamique; cela signifie que les hôtes peuvent rejoindre ou quitter les groupes à tout moment. Il n'existe aucune restriction quant à l'emplacement ou au nombre de membres dans un groupe d'hôtes mais l'appartenance à un groupe PEUT être limitée à ces seuls hôtes. Un groupe d'hôtes PEUT être permanent ou transitoire. Un groupe permanent comporte une adresse IP bien connue, attribuée par l'administrateur. En revanche, un groupe transitoire reçoit une adresse attribuée dynamiquement lors de la création du groupe, à la demande d'un hôte.

La prise en charge intégrale de la multidiffusion IP permet à un hôte de créer, rejoindre et quitter des groupes d'hôtes ainsi que d'envoyer à ces derniers des datagrammes IP. Cela exige l'implémentation du protocole de gestion de groupe Internet (IGMP, *Internet group management protocol*) ainsi que l'extension des interfaces de service de réseaux IP et local au sein de l'hôte.

8.2 IGMP

Le protocole IGMP (protocole de gestion de groupe Internet) est utilisé entre des hôtes et des routeurs multidiffusion sur un réseau physique unique afin de créer des membres d'hôtes dans des groupes multidestinataires précis. Les routeurs multidiffusion utilisent ces informations, conjointement avec un protocole de routage multidiffusion, pour prendre en charge l'envoi multidiffusion IP sur l'Internet. Un routeur DEVRAIT implémenter la partie routeur multidiffusion du protocole IGMP.

On utilise le protocole IGMP pour rejoindre et quitter un groupe multidiffusé. Au moment d'envoyer une demande d'adhésion à un groupe multidiffusé, le protocole IGMP envoie un message de rapport d'adhésion IGMP aux routeurs du sous-réseau et notifie la demande d'adhésion au groupe multidiffusé. Ce rapport est appelé message de demande d'adhésion IGMP. Un routeur envoie le message de requête IGMP une fois par minute pour confirmer la présence de l'unité SVD dans un groupe multidiffusé. L'unité SVD renvoie le message de rapport d'adhésion IGMP à ce message de requête. Ce faisant, le routeur peut détecter l'unité SVD qui est présente sur l'interface et envoyer un paquet multidiffusion à la seule interface nécessaire.

Dans le cas du protocole IGMPv2, l'unité SVD envoie un message de sortie explicite pour indiquer à quel moment elle quitte le groupe multidiffusé. Toutefois, elle ne peut éviter que des paquets de multidiffusion provenant de sources spécifiques soient remis à des réseaux lorsqu'il n'existe aucune unité SVD intéressée.

Le protocole IGMPv3 permet en outre un "filtrage de la source", c'est-à-dire qu'un système a la possibilité d'indiquer qu'il souhaite recevoir uniquement des paquets envoyés d'adresses source spécifiques à destination d'une adresse multidiffusion donnée. Ces informations PEUVENT être utilisées par des protocoles de routage multidiffusion pour éviter que des paquets de multidiffusion provenant de sources spécifiques soient remis à des réseaux dans lesquels il n'existe aucune unité SVD intéressée.

8.3 Surveillance IGMP

La surveillance IGMP est un protocole utile pour contrôler l'inondation dans le mode multidiffusion. Lorsqu'une unité SVD envoie un message d'adhésion IGMP, un commutateur le transmet à des routeurs. A ce moment-là, un commutateur analyse le message et enregistre l'adresse MAC du groupe multidiffusé où l'unité SVD rejoint le groupe. Le commutateur peut relayer la trame de multidiffusion vers l'interface uniquement si l'unité SVD existe, évitant ainsi l'inondation du paquet de multidiffusion.

8.4 Protocole de routage de multidiffusion

Les routeurs ou les commutateurs ne se trouvent pas toujours dans le même sous-réseau que l'unité SVD. Pour localiser cette unité, on utilise le protocole de routage de multidiffusion. Un routeur de premier bond est placé au point d'interface entre la source de multidiffusion et le réseau de

transmission par paquets, alors que le routeur du dernier bond est situé au point d'interface entre le groupe multidiffusé et le segment CDN (voir la Figure 1). Le protocole de routage de multidiffusion s'applique généralement dans la section située entre le routeur du premier bond et le routeur du dernier bond.

Dans un protocole de routage de multidiffusion, on distingue deux modes: un mode dense et un mode épars. Le mode dense consiste à créer une configuration arborescente de distribution répartie par source et à remettre des paquets fondés sur la configuration en mode inondation. La remise des paquets cesse lorsqu'elle n'est pas nécessaire. Dans ce mode, la demande de remise de paquets des unités SVD aux routeurs en amont n'est pas notifiée. Le mode épars permet la transmission des paquets avec des configurations arborescentes pour une source de multidiffusion donnée et pour des sources multiples. Dans ce mode, un routeur central de réseau et des routeurs appelés points de rendez-vous (RP, *rendez-vous point*) sont définis. Un point RP est obligatoire par groupe multidiffusé. Une configuration arborescente répartie par source est appliquée à la section située entre la source de multidiffusion et le point RP, une autre configuration du groupe multidiffusé s'appliquant à la section située entre le point RP et l'unité SVD. Contrairement au mode dense, le mode épars possède la fonction explicite de demande de remise de paquet de multidiffusion aux routeurs en amont. On parle de message d'adhésion explicite. Dans ce mode, si une nouvelle unité SVD rejoint le groupe, le routeur peut envoyer la demande de remise de paquet aux routeurs en amont, élargir la configuration arborescente de remise et la remise de paquets de multidiffusion à un nouveau membre devient possible. Le mode dense PEUT influencer fortement sur le réseau avec une inondation des paquets. Lorsque le réseau de distribution en mode multidiffusion est étendu, le mode épars est recommandé.

9 Priorité en matière de qualité de service et mappage de la politique

9.1 Priorité en matière de qualité de service

Chaque unité SVD appartenant à l'architecture conforme à [UIT-T J.292] DEVRAIT pouvoir fournir une qualité de service contrôlée par la passerelle domestique (RGW).

NOTE 1 informative – Dans la présente Recommandation, on suppose que le dispositif terminal ou équipement CPE DOIT être conforme aux spécifications appropriées qui s'appliquent au réseau domestique comme le dispositif UPnP.

La description fournie dans le présent paragraphe est un exemple de routage par pont en fonction de la qualité de service. Le protocole proprement dit sera détaillé dans la spécification qui fait suite au présent document consacré à l'architecture des STB. La méthode de commande de la qualité de service, y compris la commande d'admission de la passerelle RGW vers l'unité SVD, DEVRAIT faire référence aux spécifications relatives au réseau domestique.

NOTE 2 informative – Dans le cas de l'architecture du dispositif UPnP, les messages de commande sont envoyés à partir des éléments du point de commande UPnP et une réponse est fournie par les éléments de service du dispositif UPnP.

L'architecture se caractérise également par une architecture répartie dans laquelle de multiples instanciations d'un service donné appartenant au réseau domestique (HN) PEUVENT être utilisées de façon interchangeable.

NOTE 3 informative – La présente Recommandation décrit certains services de QS de dispositifs UPnP qui DEVRAIENT figurer dans le service PS de la passerelle RGW.

La présente Recommandation définit trois catégories de priorité de QS pour la transmission de paquets entre une passerelle RGW et une unité SVD.

- Chiffre correspondant à l'importance du trafic;
- Priorité de mise en file d'attente;
- Priorité d'accès au support.

9.1.1 Chiffre correspondant à l'importance du trafic

NOTE informative – Dans la présente Recommandation, le trafic du dispositif UPnP est acheminé sous la forme d'un paquet bilatéral entre la passerelle RGW et l'unité SVD. Le chiffre correspondant à l'importance du trafic (TIN, *traffic importance number*) du dispositif UPnP est indiqué au Tableau 3. A noter que le dispositif UPnP évalue de 0 à 7 l'importance du trafic, les chiffres 1 et 2 ayant une faible priorité par rapport au zéro attribué au trafic du service "au mieux". Le gestionnaire de la qualité de service attribue le chiffre TIN à la fonction de commande du trafic qui est une fonction du service de portail (PS, *portal service*) dans la passerelle RGW, en fonction de la prescription de QS applicable à chaque dispositif terminal.

La liste des chiffres TIN DEVRAIT être enregistrée dans la base de données du service (PS) de la passerelle RGW.

Tableau 3– Chiffre correspondant à l'importance du trafic

Chiffre correspondant à l'importance du trafic
7 (le plus élevé)
6
5
4
3
0 (au mieux/existant)
2
1 (le plus bas)

9.1.2 Priorité de mise en file d'attente

On suppose que des paquets provenant de plusieurs interfaces arrivent jusqu'aux fonctions du service PS de la passerelle RGW qui appartient au réseau conforme au [UIT-T J.292]. Toutefois, les paquets DOIVENT être envoyés vers une seule interface à destination de l'unité SVD. Afin de garantir une QS totale du service, il FAUT procéder à une mise en file d'attente des paquets sur cette interface. La présente Recommandation décrit un mécanisme de mise en file d'attente priorisée qui vise à traiter les paquets de QS avec la priorité voulue. Les méthodes de mise en file d'attente indiquées ci-après sont largement répandues et le choix relève de l'opérateur.

NOTE informative – Un service ou une application (c'est-à-dire, le chiffre correspondant à l'importance du trafic du dispositif UPnP) DEVRAIT se prononcer sur le mécanisme de mise en file d'attente à appliquer.

La combinaison des méthodes de mise en file d'attente DOIT être enregistrée dans la base de données du service PS de la passerelle RGW.

– *Gestion équitable pondérée des files (WFQ, weighted fair queuing)*

Cette méthode permet de gérer dynamiquement les files par flux d'application et les paquets sont mis en file d'attente. La largeur de bande est attribuée de manière équitable en fonction de la priorité IP de chaque paquet. Cette méthode permet d'éviter que de gros paquets n'entravent la remise des petits paquets.

– *Gestion équitable pondérée des files en fonction de la catégorie (CBWFQ, class-based weighted fair queuing)*

Dans cette méthode, des paquets sont attribués à la catégorie d'opérateur de file d'attente définie et les paquets sont mis en file d'attente. Une largeur de bande appropriée est attribuée explicitement par file d'attente de chaque catégorie. La méthode précédente gère automatiquement les files par flux alors que la présente méthode peut attribuer de la largeur

de bande en fonction de la catégorie fixée explicitement par l'opérateur, ce qui suppose une commande souple du mécanisme de mise en file d'attente.

– *Desserte prioritaire (PQ, priority queuing)*

Cette méthode consiste à créer des files d'attente de quatre niveaux: élevé, intermédiaire, normal et moyen, en fonction de la priorité requise. Dans cette méthode, les paquets figurant dans la file de priorité "élevée" sont programmés avec la plus haute priorité. Les paquets placés dans d'autres files d'attente ne sont pas remis tant que la transmission des paquets à priorité "élevée" n'est pas totalement achevée. Cette méthode permet de traiter les paquets d'urgence critique comme la téléphonie IP ou les trames principales dans des files d'attente de priorité "élevée".

– *Mise en file d'attente avec latence faible (LLQ, low latency queuing)*

Dans cette méthode, des paquets sont attribués à la catégorie d'opérateur de file d'attente définie, tout comme la méthode CBWFQ, et il peut être décidé de remettre le paquet qui a la plus haute priorité dans la file d'attente. Une largeur de bande est attribuée à la file d'attente de très haute priorité ainsi qu'à d'autres files d'attente. Cette méthode permet de remettre des paquets de téléphonie IP jugés prioritaires ainsi que d'autres paquets applicables avec une largeur de bande garantie.

– *Pondération comparative (WRR, weighted round robin)*

Cette méthode s'appuie sur quatre files d'attente dans l'interface de sortie et le mécanisme de mise en file d'attente applique la priorité configurée des paquets. La priorité des paquets et les files d'attente sont préétablies, chaque file d'attente étant assortie d'une valeur de pondération. Cette méthode permet une mise en file d'attente avec pondération et le contrôle de la remise des paquets. Une file d'attente peut recevoir la plus haute priorité parmi les quatre files d'attente. La méthode commence par la file d'attente de très haute priorité et d'autres paquets prioritaires peuvent être remis une fois que la remise du paquet de très haute priorité est terminée. Le paquet de téléphonie IP est généralement placé dans la file d'attente de très haute priorité.

9.1.3 Priorité d'accès au support

Il s'agit ici de décrire un mécanisme de QS priorisée par flux de paquets priorisés dans un support partagé. La Figure 5 donne un exemple de diffusion par multidiffusion avec largeur de bande préconfigurée et QS priorisée.

NOTE informative – La section située entre la passerelle RGW et l'unité SVD correspond à la section QS du dispositif UPnP, chaque paquet étant priorisé et la mise en file d'attente est contrôlée dans cette section.

Par ailleurs, la largeur de bande est préassignée dans la section d'accès et les paquets sont contrôlés au niveau de la QS des services DiffServ par l'intermédiaire du champ ToS avec priorité IP, DSCP ou CoS.

Dès lors que la largeur de bande du segment CDN est bien configurée et que la largeur de bande attribuée est supérieure à la largeur de bande totale de tous les paquets priorisés, la qualité de ces paquets est garantie s'ils sont remis en premier avec une QS priorisée. Par exemple, si la largeur de bande totale de tous les paquets priorisés est de 100 Mbit/s et qu'une largeur de bande supérieure à 100 Mbit/s est attribuée au segment CDN, les paquets en question doivent pouvoir être remis sans causer d'encombrement grâce à l'adoption de la QS priorisée. Sur le plan de la qualité, la QS priorisée avec largeur de bande préconfigurée est considérée comme étant équivalente à la version paramétrique de la QS.

Le mappage de la QS DOIT être assuré dans une passerelle RGW pour permettre l'échange de signalisation de QS dans chaque section.

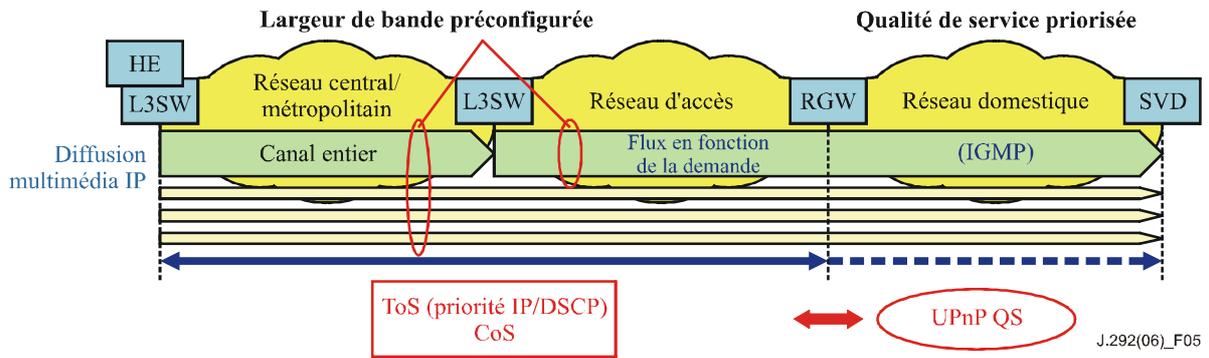


Figure 5– Diffusion par multidiffusion

La description détaillée du mappage de la QS sort du cadre de la présente Recommandation mais quelques indications sur ce type de mappage sont données dans le § 9.2.

9.2 Mappage de la politique de QS

Le flux de paquets DEVRAIT être contrôlé avec des paquets de QS priorisée et une mise en file d'attente selon les priorités entre la passerelle RGW et l'unité SVD.

NOTE informative – Le détenteur de la politique de QS et le gestionnaire de la QS jouent un rôle central dans le système de contrôle de la QS du dispositif UPnP QS.

Le détenteur de la politique de QS DEVRAIT enregistrer la politique de QS et assurer l'interface nécessaire pour y accéder mais ne DEVRAIT pas contrôler les ressources de QS. Le gestionnaire de la QS travaille conjointement avec le détenteur de la politique de QS et contrôle les ressources de QS dans un segment de réseau LAN. L'unité SVD DOIT offrir une capacité de QS avec des informations sur les ressources et assurer l'interface nécessaire pour le contrôle des ressources. La Figure 6 décrit un exemple de relation entre les mappages de la politique de QS.

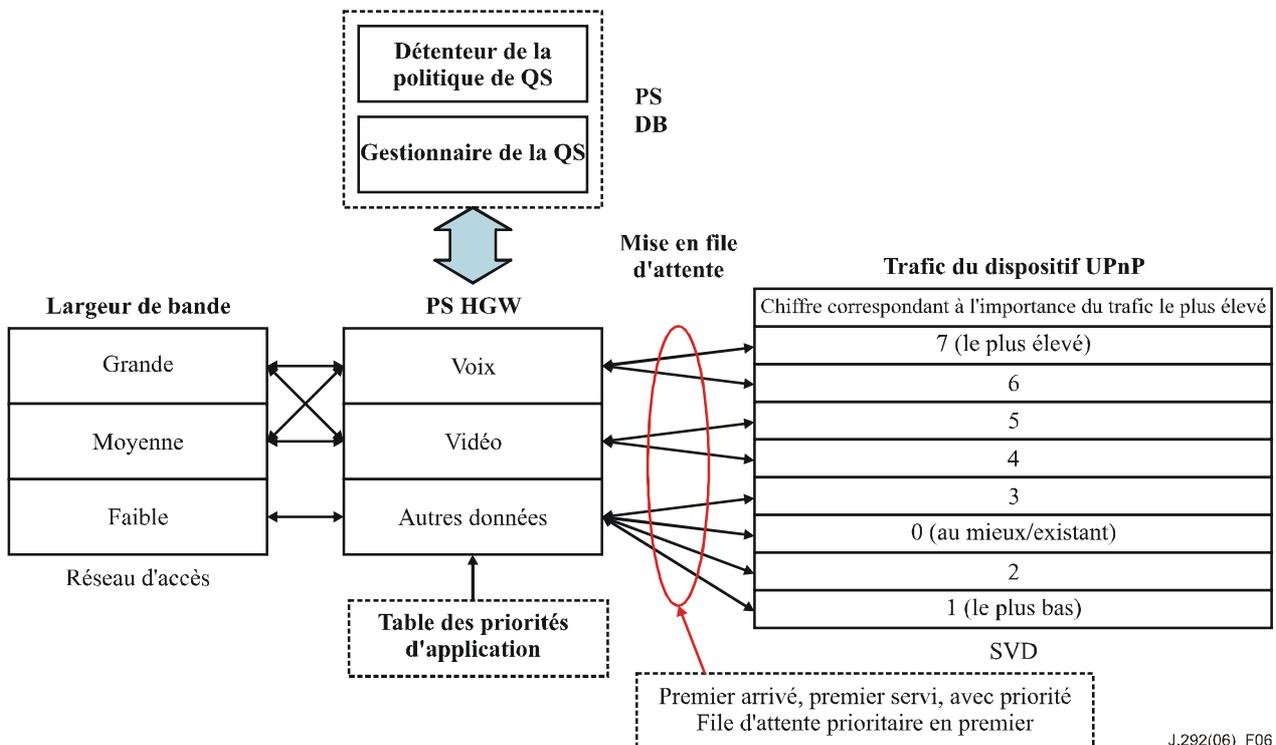


Figure 6– Relation entre les mappages de la politique de QS

Une table de mappages multiples PEUT être nécessaire pour différents services. Ces tables de mappages DEVRAIENT être comparées avec la politique de QS et être placées sous le contrôle du gestionnaire de la QS. La Figure 6 représente un mappage de QS priorisée par service, une autre méthode prioritaire pouvant être appliquée à l'aide d'un numéro de port. La table de mappage DEVRAIT être disponible dans la base de données du service PS.

10 Diffusion IP et point de commutation des canaux

La diffusion exige que la totalité du programme soit acheminée vers le dispositif terminal; toutefois, grâce à l'évolution technologique, la diffusion utilisant une ligne de télécommunication est également considérée aussi comme telle si la totalité du programme parvient à la station la plus proche. Autrement dit, la remise par multidiffusion au routeur du dernier bond est un type de diffusion, c'est-à-dire une diffusion IP. La vidéo à la carte est une application de la diffusion IP et occupe la largeur de bande dont le consommateur a besoin pour transmettre un programme. La Figure 7 illustre la relation existant entre la diffusion IP et un point de commutation des canaux. Tous les contenus de diffusion IP, c'est-à-dire les flux IP (IPS, *IP stream*) sont remis au point de commutation des canaux à partir de la tête du réseau. Un contenu choisi est remis à l'équipement CPE depuis le point de commutation des canaux.

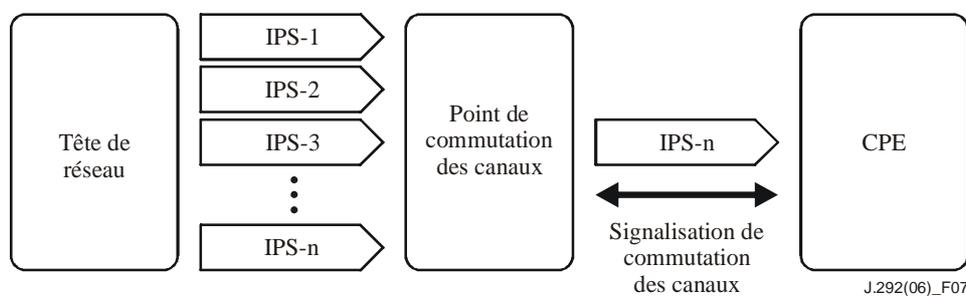


Figure 7– Relation entre la diffusion IP et un point de commutation des canaux

Le flux IPS est un flux de paquets IP identifié par son adresse et son numéro de port. Le point de commutation des canaux, qui n'est pas spécifié dans l'implémentation physique, comporte en principe un commutateur de station avec terminaison OLT/DSLAM, un terminal de réseau avec passerelle RGW et un logiciel dans l'équipement CPE. Le signal de sélection des canaux, information de signalisation destinée à contrôler le point de commutation des canaux à partir de l'équipement CPE, utilise actuellement le protocole de commande de multidiffusion IP comme le protocole IGMP/MLD. Il est nécessaire de développer la fonctionnalité pour répondre aux demandes anonymes.

Le protocole Multicast Listener Discovery (MLD) est utilisé dans la suite de protocoles IPv6 par un routeur pour trouver des auditeurs pour un groupe multidiffusé donné; il s'apparente au protocole IGMP, utilisé dans l'IPv4. On utilise le protocole inséré dans la version 6 du protocole de message de commande Internet (ICMP) plutôt qu'un protocole séparé. Le protocole est décrit dans le Document RFC 2710 de l'IETF.

Les protocoles MLD et MLDv2 équivalent respectivement aux protocoles IGMPv2 et IGMPv3.

Bibliographie

- [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.*
- [b-UIT-T J.282] Recommandation UIT-T J.282 (2006), *Architecture de la distribution vidéo multicanal sur les réseaux IP.*
- [b-UIT-T J.283] Recommandation UIT-T J.283 (2006), *Architecture de réseau IP avec diversité de route dans la couche réseau assurant une distribution vidéo robuste en multidiffusion IP.*
- [b-IETF RFC 768] IETF RFC 768 (1980), *User Datagram Protocol.*
- [b-IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol.*
- [b-IETF RFC 793] IETF RFC 793 (1981), *Transmission Control Protocol.*
- [b-IETF RFC 1889] IETF RFC 1889 (1996), *RTP: A Transport Protocol for Real-Time Applications.*
- [b-IETF RFC 2131] IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol.*
- [b-IETF RFC 2236] IETF RFC 2236 (1997), *Internet Group Management Protocol, Version 2.*
- [b-IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0.*
- [b-IETF RFC 2733] IETF RFC 2733 (1999), *An RTP Payload Format for Generic Forward Error Correction.*
- [b-IETF RFC 3022] IETF RFC 3022 (2001), *Traditional IP Network Address Translator (Traditional NAT).*
- [b-IETF RFC 3376] IETF RFC 3376 (2002), *Internet Group Management Protocol, Version 3.*
- [b-IETF RFC 3810] IETF RFC 3810 (2004), *Multicast Listener Discovery Version 2 (MLDv2) for IPv6.*
- [b-IEEE 802.1] IEEE 802.1: 802.1X – *Port Based Network Access Control.*

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