Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

J.261
(10/2009)

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

IPCablecom

Cadre applicable à la mise en œuvre des télécommunications à traitement préférentiel sur les réseaux IPCablecom et IPCablecom2

Recommandation UIT-T J.261

Recommandation UIT-T J.261

Cadre applicable à la mise en œuvre des télécommunications à traitement préférentiel sur les réseaux IPCablecom et IPCablecom2

Résumé

Cette Recommandation décrit un cadre applicable à la mise en œuvre des capacités de traitement préférentiel sur les réseaux IPCablecom et IPCablecom2.

Elle définit un cadre applicable aux capacités qui peuvent être utilisées pour observer les prescriptions contenues dans le document UIT-T J.260 et constitue la base de Recommandations détaillées relatives aux réseaux IPCablecom et IPCablecom2 pour la prise en charge des télécommunications à traitement préférentiel.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T J.261	2009-10-30	9

AVANT-PROPOS

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

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

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

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

NOTE

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

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

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

TABLE DES MATIÈRES

Introduction

Les télécommunications en cas d'urgence/de catastrophe pour les utilisateurs autorisés sont d'une importance vitale pour la santé, la sécurité et le bien-être de la population dans tous les pays. Habituellement, pour faciliter les opérations en cas d'urgence/de catastrophe, on utilise des capacités garanties pour la fourniture de services de télécommunication à traitement préférentiel faciles à utiliser, ces capacités pouvant être assurées par des solutions techniques et/ou par une politique administrative. Les infrastructures IPCablecom et IPCablecom2 constituent une ressource importante pour prendre en charge des services garantis de télécommunication à traitement préférentiel.

Les deux aspects essentiels des télécommunications à traitement préférentiel sur les réseaux câblés qui sont abordés dans la présente Recommandation cadre sont l'authentification et la priorité. Ces aspects sont indispensables pour accéder aux ressources des réseaux câblés lorsqu'un traitement préférentiel est nécessaire. D'autres aspects comme la politique, l'ingénierie du trafic, le routage alternatif, la fourniture d'une capacité de rétablissement, etc., sont en dehors du domaine d'application de la présente Recommandation ou ne sont pas abordés dans cette version.

L'évolution des réseaux de télécommunication en général et des réseaux câblés en particulier conduit à une approche par étapes pour la prise en charge du traitement préférentiel. Cette approche par étapes doit tenir compte de l'évolution des Recommandations relatives aux réseaux IPCablecom: l'ensemble initial de Recommandations relatives aux réseaux IPCablecom, les Recommandations relatives aux réseaux IPCablecom révisées en 2005 et l'ensemble de Recommandations relatives aux réseaux IPCablecom2.

Recommandation UIT-T J.261

Cadre applicable à la mise en œuvre des télécommunications à traitement préférentiel sur les réseaux IPCablecom et IPCablecom2

1 Domaine d'application

L'objectif de la présente Recommandation est d'établir un cadre pour la mise en œuvre de services de télécommunication à traitement préférentiel dans les réseaux câblés décrits dans les documents [UIT-T J.160] et [UIT-T J.360]. Ce cadre fait partie de la série de Recommandations portant sur ces services.

Les deux aspects essentiels des services de télécommunication à traitement préférentiel abordés dans ce cadre sont la priorité et l'authentification. Pour étudier les différences architecturales concernant ces deux aspects, on s'appuie sur les entités fonctionnelles logiques définies respectivement dans les documents [UIT-T J.160] et [UIT-T J.360].

Cette version du cadre porte sur les deux aspects essentiels, à savoir la priorité et l'authentification, nécessaires à la prise en charge du traitement préférentiel dans les services de télécommunication. D'autres aspects comme la politique, l'ingénierie du trafic, le routage alternatif, la fourniture de capacités, etc., sont en dehors du domaine d'application de la présente Recommandation ou feront l'objet d'un complément d'étude. A titre d'exemple, on prévoit, dans de futures versions, d'examiner la fourniture de services à traitement préférentiel pour des utilisateurs particuliers et/ou pour des dispositifs (adaptateurs de terminal média) situés dans des endroits particuliers.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

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

[ITU-T J.163] Recommandation ITU-T J.163 (2007), *Qualité de service dynamique pour la fourniture de services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems*.

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

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

[ITU-T J.260] Recommandation ITU-T J.260 (2005), *Prescriptions relatives aux communications à traitement préférentiel sur les réseaux IPCablecom*.

[ITU-T J.360] Recommandation ITU-T J.360 (2006), *Architecture générale IPCablecom2*.

[ITU-T J.368] Recommandation ITU-T J.368 (2008), *IPCablecom2: spécification de la qualité de service*.

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

[IETF RFC 4412] IETF RFC 4412 (2006), *Communications Resource Priority for the Session Initiation Protocol (SIP)*.

3 Définitions

3.1 Termes définis dans d'autres documents

La présente Recommandation utilise les termes suivants définis dans d'autres documents.

3.1.1 capacités garanties [UIT-T J.260]: capacités assurant avec une haute probabilité ou avec certitude, la fourniture et le fonctionnement fiable de communications critiques.

3.1.2 authentification [UIT-T J.260]: acte ou méthode appliqués pour vérifier une identité déclarée.

3.1.3 habilitation, autorisation [UIT-T J.260]: acte consistant à déterminer si un privilège particulier, tel que l'accès à des ressources de télécommunication, peut être accordé au détenteur d'un mandat.

3.1.4 câblo-modem [UIT-T J.160]: dispositif terminal de couche 2 formant l'extrémité client de la connexion DOCSIS.

3.1.5 situation d'urgence [UIT-T J.260]: situation grave, survenue subitement et de manière inattendue. Des efforts immédiats importants peuvent être nécessaires, facilités par les télécommunications, pour rétablir une situation normale et empêcher que les personnes ou les biens subissent de nouveaux dommages. Si la situation s'aggrave, elle peut se transformer en crise ou en catastrophe.

3.1.6 situation d'urgence internationale [UIT-T J.260]: situation d'urgence affectant plusieurs pays.

3.1.7 IPCablecom[UIT-T J.160]: projet UIT-T comprenant une architecture et une série de Recommandations permettant la fourniture de services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems.

3.1.8 étiquette [UIT-T J.260]: identificateur faisant partie des éléments de données ou attachés à ceux-ci. Dans le contexte de communications à traitement préférentiel, il s'agit d'une indication de priorité. Cet identificateur peut être utilisé comme un mécanisme de mappage entre différents niveaux de priorité de réseau.

3.1.9 réseau IP géré [UIT-T J.160]: réseau IP, géré par une entité unique aux fins du transport de paquets de signalisation et de paquets de médias IPCablecom.

3.1.10 préférentiel [UIT-T J.260]: qualifie une capacité accordant certains privilèges par rapport au service régulier.

3.1.11 capacités de traitement prioritaire [UIT-T J.260]: capacités permettant d'accéder aux ressources d'un réseau de télécommunication et/ou de les utiliser de manière prioritaire.

3.1.12 abonné [UIT-T J.360]: entité (comportant un ou plusieurs utilisateurs) ayant souscrit un abonnement auprès d'un fournisseur de services.

3.1.13 agent d'utilisateur (UA) [UIT-T J.360]: agent d'utilisateur SIP, au sens du document [IETF RFC 3261].

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit le terme suivant:

3.2.1 équipement d'utilisateur: tout dispositif utilisé directement par un utilisateur pour communiquer.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

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

ATM guichet automatique *(automatic teller machine)*

AVP paire attribut-valeur *(attribute value pair)*

CM câblo-modem

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

CMTS système de terminaison de câblo-modem *(cable modem termination system)*

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

E-DVA adaptateur vocal numérique intégré *(embedded digital voice adapter)*

E-MTA adaptateur de terminal de média intégré *(embedded media terminal adapter)*

IPSec sécurité du protocole Internet *(internet protocol security)*

KDC centre de distribution de clés *(key distribution centre)*

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

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

P-CSCF fonction relais de commande de session d'appel *(proxy call session control function)*

PIN numéro d'identification personnel *(personal identification number)*

PKI infrastructure de clés publiques *(public key infrastructure)*

PKINIT authentification initiale par cryptographie à clé publique *(public key cryptography for initial authentication)*

QoS qualité de service *(quality of service)*

RTPC réseau téléphonique public commuté

RTP protocole de transport en temps réel *(real time transport protocol)*

SIP protocole d'utilisation de session *(session initiation protocol)*

TGT ticket d'attribution de ticket *(ticket granting ticket)*

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

UE équipement d'utilisateur *(user equipment)*

5 Conventions

Aucune.

6 Cadre commun pour la priorité

Le document [UIT-T J.260] énumère un certain nombre de prescriptions pour garantir un traitement prioritaire dans les réseaux IPCablecom et IPCablecom2. Il existe des différences architecturales entre le réseau IPCablecom décrit dans le document [UIT-T J.160] et le réseau IPCablecom2 décrit dans le document [UIT-T J.360], mais le présent paragraphe porte sur un cadre applicable aux deux réseaux. Trois aspects sont à prendre en considération lorsqu'on envisage le traitement prioritaire de services de télécommunication à traitement préférentiel: classification ou étiquetage de la session ou de l'appel comme nécessitant un traitement prioritaire, signalisation de la priorité et mécanismes permettant de prendre en charge la priorité demandée. Le choix des mécanismes et des politiques, ainsi que leurs mises en œuvre respectives, sont en dehors du domaine d'application de la présente Recommandation.

Le Tableau 1 classe les prescriptions en trois catégories correspondant à ces trois aspects: classification, signalisation et mécanismes. Pour certaines prescriptions, plusieurs aspects sont indiqués car la classification de priorité de l'appel doit être maintenue et les mécanismes effectifs de préservation de la classification peuvent varier.

Tableau 1 – Correspondance entre les prescriptions et les aspects relatifs à la priorité

Prescription [UIT-T J.260]	Catégorie
Accès prioritaire aux réseaux IPCablecom et IPCablecom2 (1a)	Classification
Activation et caractéristiques de l'appel (1b)	Signalisation
Attribution de ressources de réseau (1c)	Mécanismes
Priorité donnée aux appels étiquetés au niveau des passerelles (1d)	Signalisation et mécanismes
Attribution d'étiquettes au moment du lancement de l'appel (2)	Classification
Priorité donnée aux appels étiquetés dans les réseaux IPCablecom et IPCablecom2 (3)	Mécanismes
Correspondance entre les étiquettes utilisées du réseau câblé à la passerelle de réseau de connexion et dans l'autre sens (4 et 5)	Mécanismes
Préservation de l'étiquette de priorité dans le réseau câblé (6)	Signalisation et mécanismes
Traitement des appels prioritaires en transit dans un réseau câblé en fonction des capacités de ce réseau (7)	Classification et mécanismes
Nombre de niveaux de priorité: au moins 1 et possibilité d'autres niveaux en fonction des options nationales (8)	Classification
Traitement prioritaire assuré dans un réseau câblé aux appels avec étiquette de priorité provenant d'un réseau fiable (9)	Mécanismes

Par priorité d'un appel ou d'une session, on entend l'obtention d'une plus grande probabilité d'aboutissement de cet appel ou de cette session. En d'autres termes, une fois que le trafic est identifié comme correspondant à un service de télécommunication à traitement préférentiel, les politiques doivent offrir une plus grande probabilité de succès pour l'admission d'appel, le routage et l'acheminement du trafic. Cette capacité doit exister sur la liaison d'accès ainsi que dans toutes les

entités de réseau appropriées comme les serveurs de gestion d'appels (CMS) et les contrôleurs de passerelle média (MGC) ou les entités de l'infrastructure de protocole d'initiation de session (SIP).

Même si les mécanismes d'activation de la priorité et l'attribution d'une qualité de service sont différents, on peut, dans les réseaux IPCablecom, utiliser les classes de session DQoS pour accorder un traitement prioritaire à une session. L'une des prescriptions pour l'attribution de ressources qui peut être prise en charge dans les réseaux IPCablecom repose sur le concept de portes multimédias décrit dans les documents [UIT-T J.163] et [UIT-T J.179]. On s'intéresse ci-après au document [UIT-T J.163], qui porte spécifiquement sur IPCablecom. Les portes servent à contrôler l'accès d'un flux IP à une qualité de service améliorée depuis le réseau DOCSIS. Elles sont installées dans le système de terminaison de câblo-modem (CMTS) pour permettre de créer des flux de service avec une qualité de service garantie grâce à une réservation des ressources nécessaires. Le contrôle d'admission au niveau du système CMTS sert à vérifier que les ressources disponibles sont supérieures aux ressources engagées et réservées. Dans le cas d'un réseau IPCablecom fondé sur le document [UIT-T J.163], un client, par exemple un adaptateur de terminal média intégré (E-MTA), lance la réservation et l'activation des ressources, tandis que dans le cas du document [UIT-T J.179] avec prise en charge du multimédia, un proxy peut réaliser ces étapes pour le compte du client du point d'extrémité.

La signalisation de la priorité est examinée séparément pour IPCablecom et IPCablecom2 en raison des méthodes différentes de connexion au réseau d'accès utilisées par un adaptateur E-MTA et par un équipement d'utilisateur.

Les réseaux IPCablecom et IPcablecom2 utilisent le protocole de transport en temps réel (RTP) pour le transport des paquets audio et vidéo. Comme indiqué dans le document [b-IETF RFC 4190], le protocole RTP ne comporte pas de marquages pour indiquer la priorité du paquet avec une étiquette. Différentes méthodes sont envisagées, parmi lesquelles la définition d'un nouveau comportement par saut pour le trafic à traitement préférentiel, un nouveau protocole de couche de calage (shim) sur IP ou le marquage d'un paquet de couche d'application.

7 Cadre commun pour l'authentification

L'authentification dans les réseaux IPCablecom et IPCablecom2 nécessite la fourniture de justificatifs d'identité, dans un certain format, qui sont utilisés par le système pour vérifier l'intégrité d'un identificateur présenté par un utilisateur souhaitant utilisé le système. La gestion de ces justificatifs d'identité est très importante lorsqu'il s'agit d'examiner le type de mécanismes d'authentification utilisés dans les réseaux câblés. Il faut aussi examiner les mécanismes d'authentification déjà déployés (par exemple pour les abonnés) ainsi que l'acceptabilité et l'utilisabilité de tout mécanisme d'authentification déjà déployé pour les télécommunications à traitement préférentiel dans d'autres réseaux. Les deux formes d'authentification disponibles sont les suivantes:

- authentification fondée sur les justificatifs d'identité de l'utilisateur, pour laquelle l'utilisateur préférentiel doit fournir des informations au dispositif (par exemple adaptateur E-MTA); et
- authentification fondée sur l'équipement, qui repose sur la reconnaissance, par le système de réseau câblé, de l'équipement de l'utilisateur préférentiel.

7.1 Authentification fondée sur les justificatifs d'identité de l'utilisateur

L'authentification fondée sur les justificatifs d'identité de l'utilisateur repose sur une fonctionnalité intégrée dans le dispositif ou dans le réseau qui accepte des données d'entrée dans un certain format permettant à l'utilisateur préférentiel d'authentifier son identificateur. Le dispositif interagit avec un serveur d'authentification présent dans l'infrastructure pour valider l'identificateur et activer le service à traitement préférentiel. Pour réaliser ce type d'authentification, l'utilisateur peut appeler un

numéro spécial et composer son numéro d'identification personnel (PIN). Cette méthode permet d'utiliser n'importe quel équipement d'utilisateur IPCablecom ou IPCablecom2 doté d'un clavier numérique standard à 12 touches. Elle est utile en raison de sa simplicité et de la rétrocompatibilité avec les capacités de service à traitement préférentiel qui existent dans les réseaux déployés.

7.2 Authentification fondée sur l'équipement

L'authentification fondée sur l'équipement repose sur la reconnaissance, par le système IPCablecom ou IPCablecom2, de l'équipement d'un utilisateur de service de télécommunication à traitement préférentiel. Dans cette méthode, on utilise l'identité de l'équipement (par exemple le certificat numérique d'un dispositif) comme constituant tout ou partie de l'identification de l'utilisateur du service de télécommunication à traitement préférentiel. Cette authentification ne sera disponible que sur certains équipements (par exemple téléphones, adaptateurs E-MTA) et pourra nécessiter d'autres mécanismes (par exemple cartes à puce, jetons et/ou un numéro PIN), en plus de ceux qui assurent la sécurité physique de base de l'équipement.

7.3 Mécanismes d'authentification de base

Les mécanismes fondés sur le numéro PIN sont les plus simples et les plus accessibles dans les réseaux IPCablecom actuels, mais des méthodes plus sûres pourront être nécessaires à l'avenir pour certaines applications. Ces méthodes sont examinées dans le présent paragraphe.

Pour réaliser l'authentification, l'utilisateur peut appeler un numéro spécial et composer son PIN. Cette méthode permet d'utiliser n'importe quel équipement d'utilisateur IPCablecom doté d'un clavier numérique standard à 12 touches. Elle est utile en raison de sa simplicité et de la rétrocompatibilité avec les capacités de service à traitement préférentiel qui existent dans les réseaux déployés. Toutefois, dans cette méthode fondée sur le numéro PIN, on utilise un seul facteur (quelque chose que l'individu connaît) et non une combinaison de facteurs (par exemple "quelque chose que l'individu possède" ou "quelque chose d'unique qui caractérise l'individu"). Avec la généralisation des communications par paquets, le principe de base communément accepté consiste à utiliser deux facteurs, par exemple:

- La connaissance d'un numéro PIN conjointement avec la possession d'une carte à bande magnétique (par exemple les cartes utilisées dans les guichets automatiques bancaires).
- La connaissance d'un mot de passe conjointement avec la possession d'un jeton limité dans le temps (par exemple les jetons utilisés pour les opérations bancaires et financières en ligne).

Toutefois, la plupart de ces méthodes alternatives ne sont utilisables que si le dispositif a d'autres capacités d'entrée/sortie, en plus du clavier numérique standard à 12 touches.

Il existe peu de mécanismes d'authentification (ou de combinaisons de mécanismes) qui peuvent être utilisés dans les réseaux câblés et qui ne sont pas fondés sur le numéro PIN. Une alternative consisterait, par exemple, à utiliser des phrases de passe (sous réserve que les capacités de reconnaissance vocale donnent des taux de ‘faux positifs' et de ‘faux négatifs' suffisamment faibles). Il existe de nombreux autres mécanismes d'authentification (par exemple mots de passe, cartes à puce, lecteurs biométriques, etc.), mais les architectures des réseaux câblés ne permettent pas de les prendre en charge facilement (par exemple les adaptateurs E-MTA n'ont pas de lecteur de carte à puce).

Pour les services multimédias qui nécessitent une certaine qualité de service, IPCablecom définit des interfaces au niveau desquelles on utilise une authentification fondée sur les protocoles RADIUS et Diameter: RADIUS entre le serveur de gestion d'appels et le système d'archivage et Diameter entre la fonction P-CSCF et la fonction relative aux données de taxation. Les mécanismes suivants ne sont pas définis dans les Recommandations relatives à IPCablecom mais peuvent être envisagés pour l'authentification des utilisateurs des services à traitement préférentiel:

- mots de passe couplés avec une infrastructure d'authentification fondée sur RADIUS;
- mots de passe couplés avec une infrastructure d'authentification fondée sur Diameter;
- mots de passe couplés avec un centre de distribution de clés (KDC), par exemple Kerberos;
- phrases de passe couplées avec une carte à puce; et
- phrases de passe couplées avec une carte à puce et une infrastructure de clés publiques (PKI).

Ces différents types de mécanismes diffèrent par le degré de garantie qu'ils offrent concernant la validité de l'identité assertée et sa présentation par un utilisateur valable du système. Ils diffèrent aussi par l'ampleur de leur déploiement, les capacités opérationnelles et la complexité. Les méthodes énumérées ci-dessus doivent être examinées plus avant de point de vue de leurs capacités d'authentification relatives, du degré d'évolutivité, de la performance, de l'interopérabilité entre les domaines et de l'interopérabilité avec les mécanismes d'authentification existants.

Pour l'authentification dans le cas du traitement préférentiel de certains appels ou de certaines sessions dans les réseaux IPCablecom, le niveau de sécurité doit être élevé. Toutefois, un utilisateur doit aussi pouvoir s'authentifier assez facilement car, dans certains cas, il sera dans une situation d'urgence. Il convient donc, dans la mesure du possible, de choisir une combinaison de mécanismes qui seront faciles à utiliser tout en offrant un niveau de sécurité élevé.

7.4 Mécanismes de gestion des justificatifs d'identité

La gestion des justificatifs d'identité est importante pour faire en sorte que le système utilise des justificatifs d'identité à jour et exacts pour l'authentification des utilisateurs. Cette gestion couvre généralement la mise à jour des justificatifs d'identité, leur révocation et l'échange de justificatifs d'identité entre domaines de fournisseur de service.

La gestion des justificatifs d'identité dépend des justificatifs d'identité proprement dits, par exemple les bases de données de mots de passe, les serveurs RADIUS/Diameter, les serveurs KDC, les cartes à puce, la racine PKI, etc. Les différents types de mécanismes diffèrent par le degré de protection de l'intégrité et de la confidentialité des données relatives aux justificatifs d'identité. Ils diffèrent aussi par l'ampleur de leur déploiement, les capacités opérationnelles et la complexité.

8 Authentification et priorité dans les réseaux IPCablecom

8.1 Authentification dans les réseaux IPCablecom

Les documents [UIT-T J.160] et [UIT-T J.170] décrivent les mécanismes utilisés pour authentifier un client demandant un service. Le protocole utilisé pour authentifier le client est le protocole Kerberos avec l'extension de cryptographie à clé publique pour l'authentification initiale (PKINIT, public key cryptography for initial authentication). Le protocole de sécurité du protocole Internet (IPSec) Kerbérisé est utilisé pour créer une association sécurisée entre le serveur CMS et l'adaptateur MTA (client). Trois phases sont décrites. Dans la première phase, le client envoie un certificat de dispositif au centre de distribution de clés (KDC) pour obtenir un ticket d'attribution de ticket (TGT) qui lui permet d'obtenir un ticket du centre KDC pour un serveur spécifique, par exemple le serveur CMS. Le client peut ne pas passer par la première phase et fournir son certificat de dispositif au centre KDC pour obtenir directement un ticket pour un serveur spécifique. Dans la troisième phase, une paire de paramètres de sécurité est établie avec le serveur d'application pour l'envoi et la réception de données sécurisées sur IPSec.

8.2 Priorité dans les réseaux IPCablecom

Les utilisateurs préférentiels bénéficient d'un traitement prioritaire, qui est assuré au moyen de la méthode définie dans le document [UIT-T J.163].

Dans les réseaux IPCablecom, la réservation de ressources se fait à l'aide de deux composants. Le premier est situé dans la couche de liaison de données et fait en sorte que les flux de service DOCSIS soient plus rapidement disponibles pour les portes d'une certaine classe de session. Le second est situé dans la couche de session et a pour objet de décrire le statut prioritaire d'un appel de manière à ce que l'information puisse être transmise à toutes les entités concernées dans le réseau.

Sur la liaison d'accès par câble, on peut activer une hiérarchisation des priorités en commençant par associer les portes de qualité de service dynamique (DQoS) avec une classe de session particulière réservée spécifiquement à cette fin, puis, en résultat, en demandant au système CMTS de prendre des mesures particulières. Suivant la valeur de la classe de session, un contrôle d'admission différent est appliqué à la demande de ressources résultante. Par exemple, on peut définir une classe de session pour les communications vocales normales et une classe de session chevauchante pour les appels à traitement préférentiel pour permettre d'attribuer jusqu'à, respectivement, 50% et 70% de la totalité des ressources dans le sens montant, le reste (30% à 50%) de la totalité de la largeur de bande amont étant laissé à la disposition des autres services, dont le niveau de priorité est éventuellement moindre.

Le document [b-UIT-T J.162] décrit la signalisation d'appel par le réseau utilisée dans les réseaux IPCablecom entre l'adaptateur E-MTA et l'agent d'appel pour la création et la suppression des connexions. Tandis que l'agent d'appel fournit l'identificateur de porte (GateID) à l'adaptateur MTA pendant l'établissement de l'appel, il convient d'utiliser pour la session un mécanisme – qui n'est pas actuellement disponible – pour communiquer la priorité de trafic DOCSIS souhaitée à l'adaptateur MTA. Le système CMTS utilise la priorité de trafic DOCSIS pour fixer des priorités concernant le trafic pendant les périodes d'encombrement. Un complément d'étude est nécessaire dans ce domaine dans le contexte des télécommunications à traitement préférentiel.

9 Authentification et priorité dans les réseaux IPCablecom2

9.1 Authentification dans les réseaux IPCablecom2

Les réseaux IPCablecom2 prennent en charge à la fois les équipements d'utilisateur intégrés et les équipements d'utilisateur autonomes. Les équipements d'utilisateur utilisent des logiciels et peuvent être dotés de capacités de connexion d'un dispositif physique sécurisé (carte à puce par exemple). Les mécanismes d'authentification disponibles dans les réseaux IPCablecom2 devraient être davantage polyvalents et on obtiendra facilement une authentification adéquate dans ces réseaux.

L'Appendice III du document [UIT-T J.360] décrit trois mécanismes d'authentification pris en charge dans l'architecture IPCablecom2: authentification et concordance de clés (AKA) IMS, authentification Digest SIP et authentification par certificat. Pour chacun de ces mécanismes, des prescriptions sont spécifiées pour les divers composants des réseaux IPCablecom2. A titre d'exemple, pour prendre en charge l'authentification Digest, il est nécessaire de stocker de façon sécurisée les noms d'utilisateur et les mots de passe.

La signalisation entre l'équipement d'utilisateur et la fonction P-CSCF est sécurisée grâce à l'utilisation du protocole IPSec ou TLS. Conformément au document [UIT-T J.360], un équipement d'utilisateur doit prendre en charge la négociation de l'utilisation du protocole TLS. Deux modèles sont définis pour la sécurisation sur TLS, à savoir l'authentification mutuelle, pour laquelle l'équipement d'utilisateur et le serveur (fonction P-CSCF par exemple) valident le certificat de l'autre, et l'authentification côté serveur, pour laquelle seul le serveur fournit un certificat pour établir la sécurité de la signalisation. Le niveau de sécurité est plus élevé dans le premier cas. Dans les réseaux IPCablecom2, la prise en charge de l'authentification côté serveur est obligatoire. Il peut être souhaitable d'envisager l'authentification mutuelle pour les équipements d'utilisateur utilisés pour lancer des services à traitement préférentiel.

Dans les réseaux IPcablecom2, l'assertion d'identité de l'abonné doit être effectuée par la fonction P-CSCF afin d'acheminer l'authenticité de l'utilisateur aux autres éléments de réseau situés dans un réseau fiable et de supprimer l'identité lors des communications avec des éléments de réseau situés dans des réseaux non fiables. L'assertion et la suppression d'identité garantissent que les services de télécommunication à traitement préférentiel sont lancés par un utilisateur autorisé.

Le document [b-UIT-T J.262] définit les prescriptions.

9.2 Priorité dans les réseaux IPCablecom2

L'architecture IPCablecom2, décrite dans le document [UIT-T J.360], est fondée sur l'infrastructure IMS 3GPP. La priorité est établie en trois endroits: la signalisation IMS, le mécanisme d'activation et l'étiquetage de paquet.

9.2.1 Signalisation de la priorité

Au niveau de la signalisation IMS, on utilise les nouveaux en-têtes SIP Resource-Priority (R-P) (priorité de ressource) et Accept-Resource-Priority (acceptation de la priorité de ressource) définis dans le document [IETF RFC 4412]. L'adjonction de ces en-têtes dans les messages de demande et de réponse, respectivement, permet aux proxys et aux agents d'utilisateur SIP de traiter prioritairement les demandes.

Le document [IETF RFC 4412] définit de nouveaux en-têtes, Resource-Priority (R-P) dans les messages de demande SIP, pour demander un accès prioritaire aux ressources, et Accept-Resource-Priority, qui est inclus dans la réponse pour indiquer les valeurs R-P qu'un agent d'utilisateur SIP est prêt à prendre en charge. Les valeurs R-P sont enregistrées auprès de l'IANA et l'en-tête est un champ facultatif. Cinq espaces de noms sont enregistrés par l'IANA et inclus dans le document RFC. La présente Recommandation ne contient pas de proposition d'utilisation d'un espace de noms spécifique. Les espaces de noms supplémentaires requis pour les services de télécommunication à traitement préférentiel pourront être enregistrés conformément aux procédures définies dans le document [IETF RFC 4412]. L'utilisation d'en-têtes R-P permet de prendre en charge la signalisation de la priorité.

Il convient de noter que ces en-têtes n'ont pas d'incidence directe sur le comportement de retransmission des routeurs IP. Cette fonctionnalité, c'est-à-dire dans la couche de réseau ou couche 3, est à l'étude. Le document [b-IETF RFC 3690] définit des prescriptions générales relatives aux systèmes pour la prise en charge de services à traitement préférentiel dans le domaine général de la téléphonie IP en tant que service de bout en bout. Il est utile de tenir compte de ces prescriptions pour la prise en charge du traitement préférentiel dans les réseaux IPCablecom2.

9.2.2 Mécanisme d'activation

Au niveau du réseau d'accès, on peut utiliser la paire attribut-valeur (AVP) Reservation-Priority (priorité de la réservation) pour indiquer que la demande de ressources du réseau d'accès est prioritaire. Afin de définir la spécification de porte pour la réservation de ressources, la fonction P-CSCF interagit avec le gestionnaire d'application IPCablecom2 via l'interface Rx définie dans le sous-système IMS 3GPP. Cette interface utilise le protocole Diameter avec plusieurs nouvelles paires AVP définies dans le document [UIT-T J.368], portant sur une spécification de qualité de service.

Les messages GateSpec (spécification de porte) utilisés pour demander et activer des ressources du réseau d'accès incluent un identificateur de classe de session qui définit le niveau de priorité de la demande. Tandis que l'agent d'appel fournit l'identificateur GateID à l'adaptateur vocal numérique intégré (E-DVA) pendant l'établissement de l'appel, il convient d'utiliser pour la session un mécanisme – qui n'est pas actuellement disponible – pour communiquer la priorité de trafic DOCSIS souhaitée à l'adaptateur E-DVA. Le système CMTS utilise la priorité de trafic DOCSIS pour fixer des priorités concernant le trafic pendant les périodes d'encombrement. Un complément d'étude est nécessaire dans ce domaine.

Dans le réseau d'accès DOCSIS, une priorité de trafic peut être attribuée pour que certains types de flux de service bénéficient d'un traitement prioritaire.

La définition des valeurs spécifiques à utiliser pour spécifier les niveaux de priorité pour les services de télécommunication à traitement préférentiel est en dehors du domaine d'application de la présente Recommandation.

Des mécanismes existent pour prendre en charge le routage prioritaire dans le réseau central par paquets IP, y compris la signalisation SIP et les paquets de support RTP, mais ils ne sont pas définis dans la présente Recommandation.

9.2.3 Etiquetage

Actuellement, l'étiquetage de la priorité n'est pas pris en charge dans le protocole RTP, qui est le protocole de transfert de médias utilisé dans les réseaux IPCablecom2.

Le document [b-UIT-T J.263] définit en détail les prescriptions.

Bibliographie

[b-UIT-T E.106] Recommandation UIT-T E.106 (2003), *Plan international de priorité en période de crise destiné aux opérations de secours en cas de catastrophe*.

[b-UIT-T J.162] Recommandation UIT-T J.162 (2007), *Protocole réseau de signalisation d'appel pour la fourniture de services à temps critique sur les réseaux de télévision par câble utilisant des câblo-modems*.

[b-UIT-T J.262] Recommandation UIT-T J.262 (2009), *Spécifications relatives à l'authentification pour les télécommunications à traitement préférentiel sur les réseaux IPCablecom2***.**

[b-UIT-T J.263] Recommandation UIT-T J.263 (2009), *Spécifications relatives à la priorité pour les télécommunications à traitement préférentiel sur les réseaux IPCablecom2*.

[b-UIT-T Q-Sup.57] Supplément 57 aux Recommandations UIT-T de la série Q (2008), *Spécifications de signalisation pour la prise en charge du service de télécommunications d'urgence (ETS) dans les réseaux IP*.

[b-UIT-T Y.1271] Recommandation UIT-T Y.1271 (2004), *Cadres généraux applicables aux spécifications et aux capacités de réseau pour la prise en charge des télécommunications d'urgence sur les réseaux à commutation de circuits et à commutation de paquets en cours d'évolution*.

[b-UIT-T Y.2205] Recommandation UIT-T Y.2205 (2008), *Réseaux de prochaine génération – Télécommunications d'urgence – Considérations techniques*.

[b-UIT-T Y.2702] Recommandation UIT-T Y.2702 (2008), *Spécifications d'authentification et d'autorisation pour les réseaux NGN (version 1)*.

[b-IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

[b-IETF RFC 3689] IETF RFC 3689 (2004), *General Requirements for Emergency Telecommunication Service (ETS)*.

[b-IETF RFC 3690] IETF RFC 3690 (2004), *IP Telephony requirements for Emergency Telecommunications Service (ETS)*.

[b-IETF RFC 4190] IETF RFC 3190 (2005), *Framework for supporting Emergency Telecommunications Services (ETS) in IP Telephony*.

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	Terminaux et méthodes d'évaluation subjectives et objectives
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, 2010