Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

G.9980

(11/2012)

SÉRIE G: SYSTÈMES ET SUPPORTS DE TRANSMISSION, SYSTÈMES ET RÉSEAUX NUMÉRIQUES

Réseaux d'accès – Réseaux intérieurs

Télégestion d'équipements des locaux client sur des réseaux large bande – Protocole de gestion d'équipements des locaux client sur un réseau étendu

Recommandation UIT-T G.9980

RECOMMANDATIONS UIT-T DE LA SÉRIE G

SYSTÈMES ET SUPPORTS DE TRANSMISSION, SYSTÈMES ET RÉSEAUX NUMÉRIQUES

CONNEXIONS ET CIRCUITS TÉLÉPHONIQUES INTERNATIONAUX	G.100–G.199
CARACTÉRISTIQUES GÉNÉRALES COMMUNES À TOUS LES SYSTÈMES ANALOGIQUES À COURANTS PORTEURS	G.200–G.299
CARACTÉRISTIQUES INDIVIDUELLES DES SYSTÈMES TÉLÉPHONIQUES INTERNATIONAUX À COURANTS PORTEURS SUR LIGNES MÉTALLIQUES	G.300–G.399
CARACTÉRISTIQUES GÉNÉRALES DES SYSTÈMES TÉLÉPHONIQUES INTERNATIONAUX HERTZIENS OU À SATELLITES ET INTERCONNEXION AVEC LES SYSTÈMES SUR LIGNES MÉTALLIQUES	G.400–G.449
COORDINATION DE LA RADIOTÉLÉPHONIE ET DE LA TÉLÉPHONIE SUR LIGNES	G.450–G.499
CARACTÉRISTIQUES DES SUPPORTS DE TRANSMISSION ET DES SYSTÈMES OPTIQUES	G.600–G.699
EQUIPEMENTS TERMINAUX NUMÉRIQUES	G.700–G.799
RÉSEAUX NUMÉRIQUES	G.800–G.899
SECTIONS NUMÉRIQUES ET SYSTÈMES DE LIGNES NUMÉRIQUES	G.900–G.999
QUALITÉ DE SERVICE ET DE TRANSMISSION MULTIMÉDIA – ASPECTS GÉNÉRIQUES ET ASPECTS LIÉS À L'UTILISATEUR	G.1000–G.1999
CARACTÉRISTIQUES DES SUPPORTS DE TRANSMISSION	G.6000–G.6999
DONNÉES SUR COUCHE TRANSPORT – ASPECTS GÉNÉRIQUES	G.7000–G.7999
ASPECTS RELATIFS AUX PROTOCOLES EN MODE PAQUET SUR COUCHE TRANSPORT	G.8000–G.8999
RÉSEAUX D'ACCÈS	G.9000–G.9999
	G.9700–G.9799
	G.9800–G.9899
Réseaux intérieurs	**G.9900–G.9999**

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

Recommandation UIT-T G.9980

Télégestion d'équipements des locaux client sur des réseaux large bande – Protocole de gestion d'équipements des locaux client sur un réseau étendu

Résumé

La présente Recommandation définit les spécifications applicables à la télégestion, par un fournisseur de services, de dispositifs en réseau situés au domicile d'un consommateur. Elle donne un aperçu d'une famille de spécifications techniques et fournit les références normatives associées. Elle décrit les relations entre les diverses spécifications techniques de cette famille. Les paragraphes 3 et 4 contiennent un glossaire de termes et définitions employés dans les spécifications techniques.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T G.9980	2012-11-23	15

Mots clés

CWMP, TR-069.

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 avait 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

La présente Recommandation a pour base le protocole de gestion d'équipements des locaux client sur un réseau étendu (CWMP, *CPE WAN management protocol*) du Broadband Forum, communément appelé TR-069.

Ce protocole est destiné à être utilisé pour les communications entre un équipement des locaux client (CPE, *customer premises equipment*) et un serveur de configuration automatique (ACS, *auto-configuration server*). Il comporte un mécanisme de configuration automatique sécurisée d'un équipement CPE ainsi que d'autres fonctions de gestion d'équipement CPE dans un cadre commun.

Le rapport technique TR-069 définit les spécifications génériques du protocole de gestion et les méthodes applicables à tout équipement CPE TR-069. D'autres rapports techniques (TR, *technical report*) du Broadband Forum spécifient les objets gérés, ou modèles de données, pour des types spécifiques de dispositifs ou de services.

Le protocole peut être utilisé pour gérer divers types d'équipement CPE, y compris les routeurs autonomes et les dispositifs client côté réseau local. Il est indépendant de la technologie d'accès spécifique utilisée par le fournisseur de services, même s'il dépend de la connectivité de couche IP qui a été établie initialement par le dispositif.

Recommandation UIT-T G.9980

Télégestion d'équipements des locaux client sur des réseaux large bande – Protocole de gestion d'équipements des locaux client sur un réseau étendu

1 Domaine d'application

La présente Recommandation spécifie la télégestion, par un fournisseur de services, de dispositifs en réseau situés au domicile d'un consommateur. Elle donne un aperçu d'une famille de spécifications techniques et fournit les références normatives associées (voir la Figure 1). Elle décrit les relations entre les diverses spécifications techniques de cette famille.

Les équipements CPE tels que les unités ONU G-PON peuvent être en partie gérés par l'interface OMCI, comme spécifié dans [b-UIT-T G.988], qui définit des options pour la gestion en partage de ces dispositifs. Ces options, et la gestion OMCI des équipements CPE, sortent du cadre de la présente Recommandation.

Le protocole est conçu pour offrir une certaine souplesse dans le modèle de connectivité.

- Le protocole permet à la fois aux équipements CPE et aux serveurs ACS de lancer l'établissement d'une connexion, ce qui évite de devoir maintenir une connexion persistante entre chaque équipement CPE et un serveur ACS.
- Les interactions fonctionnelles entre le serveur ACS et un équipement CPE devraient être indépendantes de la question de savoir quelle extrémité a lancé l'établissement de la connexion. En particulier, même si le lancement de connectivité par le serveur ACS n'est pas pris en charge, toutes les transactions lancées par le serveur ACS devraient pouvoir avoir lieu sur une connexion lancée par l'équipement CPE.
- Le protocole permet à un ou plusieurs serveurs ACS de desservir un ensemble d'équipements CPE. Chaque équipement CPE ne peut être associé qu'à un seul serveur ACS, tandis que chaque serveur ACS peut être associé à un ou plusieurs fournisseurs de services. Toutefois, un même dispositif physique peut comporter plusieurs dispositifs CPE logiques, chacun d'entre eux pouvant être associé à un serveur ACS différent.
- Le protocole comporte des mécanismes permettant à un équipement CPE de découvrir le serveur ACS approprié pour un fournisseur de services donné.
- Le protocole comporte des mécanismes permettant à un serveur ACS d'identifier en toute sécurité un équipement CPE et de l'associer à un utilisateur/client.

Les processus destinés à prendre en charge une telle association peuvent soit faire intervenir une interaction de l'utilisateur soit être entièrement automatiques.

Le protocole permet à un serveur ACS de commander et de surveiller divers paramètres associés à un équipement CPE. Les mécanismes d'accès à ces paramètres reposent sur les principes suivants:

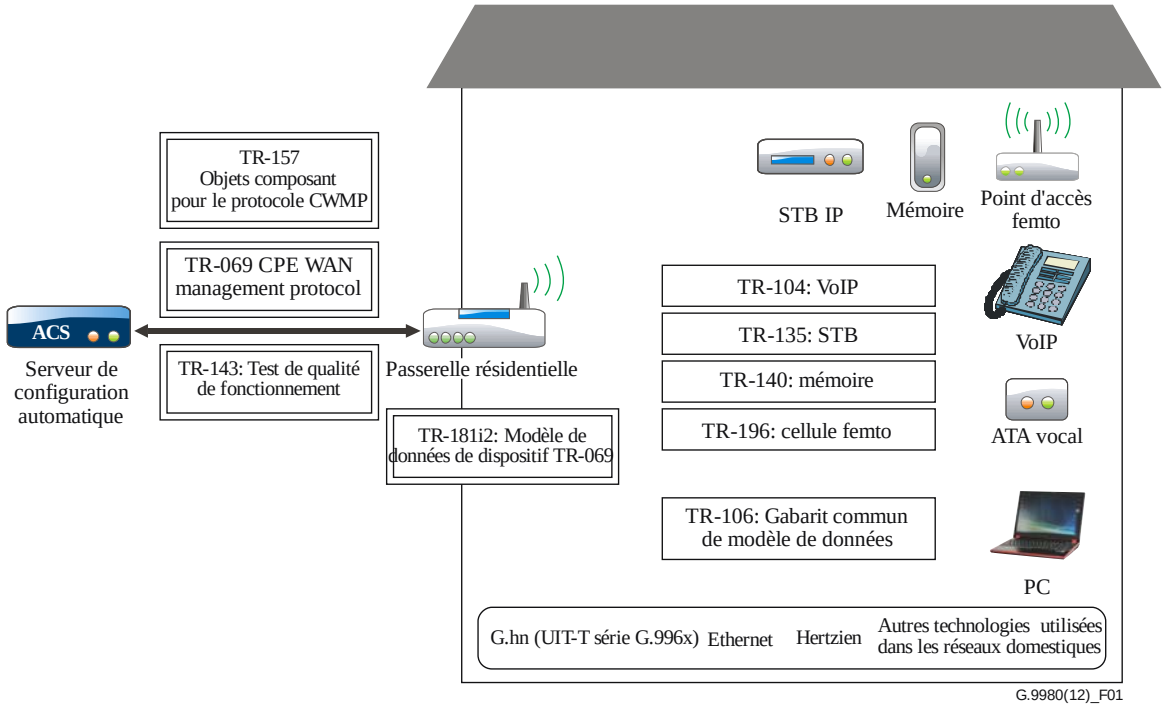
- Des équipements CPE différents peuvent avoir des niveaux de capacité différents, correspondant à la mise en œuvre de sous-ensembles différents de fonctionnalités facultatives. Quant au serveur ACS, il peut gérer différents types de dispositifs prenant en charge différents services. Par conséquent, un serveur ACS doit pouvoir découvrir les capacités d'un équipement CPE particulier.
- Un serveur ACS doit pouvoir commander et surveiller la configuration existante d'un équipement CPE.

- Outre un serveur ACS, il se peut que d'autres entités puissent commander certains paramètres de la configuration d'un équipement CPE (par exemple via la configuration automatique côté réseau local). Par conséquent, le protocole doit permettre à un serveur ACS de tenir compte des modifications externes apportées à la configuration d'un équipement CPE. Le serveur ACS devrait aussi pouvoir déterminer, parmi les paramètres de configuration, ceux qui peuvent être commandés par des entités autres que lui-même.
- Le protocole devrait permettre de définir des paramètres propres au fabricant et d'y accéder.

Le protocole est conçu de manière à ce que les mises en œuvre soient les moins complexes possible, tout en laissant une certaine marge de manœuvre pour l'établissement du compromis entre complexité et fonctionnalités. Il comporte un certain nombre d'éléments facultatifs qui ne sont mis en œuvre que si une fonctionnalité spécifique est requise. Il repose, le cas échéant, sur des normes existantes, ce qui permet de tirer parti de mises en œuvre existantes.

Le protocole est indépendant du réseau d'accès sous-jacent.

Le protocole est également extensible. Il inclut des mécanismes permettant de prendre en charge de futures extensions de la norme, ainsi que des mécanismes explicites pour les extensions propres au fabricant.



Le protocole CWMP et les modèles de données (voir les § 6.1 et 6.2) sont présentés dans des encadrés doubles.
Les rapports techniques qui définissent les modèles de données de service (voir le § 6.2.1) sont présentés dans des encadrés simples.

Figure 1 – Protocole de gestion d'équipements des locaux client sur un réseau étendu et spécifications techniques associées

Tout protocole décrivant une configuration à distance ou la modification de logiciels/micrologiciels d'équipements CPE doit présenter les fonctionnalités permettant de respecter toutes les législations, réglementations et politiques nationales et régionales applicables. La mise en œuvre de mécanismes visant à garantir l'accord explicite du client en obtenant son autorisation expresse avant d'initier à distance toute procédure sur les équipements CPE peut être exigée par les législations, réglementations ou politiques spécifiques nationales et régionales. Les responsables chargés de la mise en œuvre et les utilisateurs du protocole CWMP décrit doivent se conformer à toutes les législations, réglementations et politiques nationales et régionales applicables.

Les responsables chargés de la mise en œuvre et les utilisateurs de toutes les Recommandations de l'UIT-T, y compris de la Recommandation UIT-T G.9980 et des techniques sous-jacentes, doivent respecter toutes les législations, réglementations et politiques nationales et régionales applicables

2 Références

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

[BBF TR-069] Amendement 2 au rapport technique TR-069 du Broadband Forum (2007), *CPE WAN management protocol (CWMP)*.
<http://www.broadband-forum.org/technical/download/TR-069_Amendment-2.pdf>

[BBF TR-104] Rapport technique TR-104 du Broadband Forum (2005), *DSLHome provisioning parameters for VOIP CPE*.
<http://www.broadband-forum.org/technical/download/TR-104.pdf>

[BBF TR-106] Amendement 4 au rapport technique TR-106 du Broadband Forum (2010), *Data model template for TR-069-enabled devices*.
<http://www.broadband-forum.org/technical/download/TR-106_Amendment-4.pdf>

[BBF TR-135] Rapport technique TR-135 du Broadband Forum (2007), *Data model for a TR-069 enabled STB*.
<http://www.broadband-forum.org/technical/download/TR-135.pdf>

[BBF TR-140] Version 1.1 du rapport technique TR-140 du Broadband Forum (2007), *TR-069 data model for storage service enabled device*.
<http://www.broadband-forum.org/technical/download/TR-140_Issue1.1.pdf>

[BBF TR-143] Corrigendum 1 au rapport technique TR-143 du Broadband Forum (2008), *Enabling network throughput performance tests and statistical monitoring*.
<http://www.broadband-forum.org/technical/download/TR-143_Corrigendum-1.pdf>

[BBF TR-157] Amendement 1 au rapport technique TR-157 du Broadband Forum (2009), *Component objects for CWMP – Amendment 1*.
<http://www.broadband-forum.org/technical/download/TR-157_Amendment-1.pdf>

[BBF TR-181 version 2] Version 2 du rapport technique TR-181 du Broadband Forum (2010), *Device data model for TR-069*.
<http://www.broadband-forum.org/technical/download/TR-181_Issue-2.pdf>

[BBF TR-196] Rapport technique TR-196 du Broadband Forum (2009), *Femto access point service data model*.
<http://www.broadband-forum.org/technical/download/TR-196.pdf>

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 équipement des locaux client (CPE, *customer premises equipment*) [b-ITU-T Y.101]: système d'utilisateur final, y compris les éléments de réseaux privés connectant les applications client à la ligne d'accès.

3.1.2 rapport technique (TR, *technical report*): spécification technique approuvée par le Broadband Forum conformément à [b-BBF01].

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit le terme suivant:

3.2.1 télégestion: gestion d'un équipement CPE sur un réseau étendu par un fournisseur de services.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ACS serveur de configuration automatique (*auto-configuration server*)

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

CWMP protocole de gestion d'équipements des locaux client sur un réseau étendu (*CPE WAN management protocol*)

FAP point d'accès femto (*femto access point*)

FDD duplexage par répartition en fréquence (*frequency-division duplexing*)

NAS mémoire rattachée au réseau (*network attached storage*)

NAT traduction d'adresse réseau (*network address translation*)

PVR enregistreur vidéo personnel (*personal video recorder*)

QoE qualité d'expérience (*quality of experience*)

QoS qualité de service (*quality of service*)

RG passerelle résidentielle (*residential gateway*)

RPC appel de procédure à distance (*remote procedure call*)

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

SSL/TLS couche de correcteurs sécurisés/sécurité de la couche transport (*secure socket layer/transport layer security*)

STB boîtier-adaptateur (*set-top box*)

TR rapport technique (*technical report*)

TVIP télévision IP

UMTS système de télécommunications mobiles universelles (*universal mobile telecommunication system*)

VoIP téléphonie IP (*voice over internet protocol*)

WAN réseau étendu (*wide area network*)

5 Conventions

Dans la présente Recommandation, il n'est pas fait usage de notations, de styles, de présentations, etc. particuliers.

6 Télégestion d'équipements CPE sur des réseaux large bande

Le présent paragraphe décrit les éléments du protocole de gestion d'équipements CPE sur un réseau étendu (voir le § 6.1) et les modèles de données pour des dispositifs spécifiques (voir le § 6.2), tous figurant à titre normatif dans la présente Recommandation.

6.1 Eléments du protocole de gestion d'équipements CPE sur un réseau étendu

Les spécifications du protocole de gestion d'équipements CPE sur un réseau étendu sont définies dans [BBF TR-069].

Il est admis que les politiques des fournisseurs de services ou les réglementations locales peuvent restreindre l'utilisation de la gestion d'équipements CPE sur un réseau étendu et des spécifications associées pour des raisons de sécurité et de respect de la vie privée. Ces restrictions peuvent être les suivantes:

- Communications CWMP uniquement via des canaux SSL/TLS mutuellement authentifiés.
- Restrictions sur le type d'équipement CPE à télégérer.
- Obligation d'obtenir l'accord individuel explicite de l'abonné, avant la mise en place de la télégestion, concernant l'extraction d'informations sur la configuration de l'équipement CPE.
- Obligation de demander l'accord explicite de l'abonné avant de lancer une modification de la configuration de l'équipement CPE.
- Autre.

6.1.1 TR-069: protocole de gestion d'équipements CPE sur un réseau étendu (CWMP)

Le rapport technique [BBF TR-069] est destiné à être utilisé pour les communications entre un équipement CPE et un serveur ACS. Le protocole CWMP comporte un mécanisme de configuration automatique sécurisée d'un équipement CPE ainsi que d'autres fonctions de gestion d'équipement CPE dans un cadre commun.

Pour faciliter l'harmonisation technique de la Recommandation et du rapport [BBF TR-069], la structure du reste du présent paragraphe (présenté dans un encadré) suit celle de ce rapport. Les numéros des titres renvoient aux numéros de paragraphe du rapport technique [BBF TR-069].

1 Introduction

Les spécifications génériques des méthodes du protocole CWMP sont applicables à tout équipement CPE compatible CWMP.

D'un point de vue purement fonctionnel, le protocole CWMP prend en charge diverses fonctionnalités pour gérer un ensemble d'équipements CPE, les principales étant les suivantes:

- configuration automatique et approvisionnement en services dynamique;
- gestion d'image logicielle/micrologicielle;
- surveillance de l'état et de la qualité de fonctionnement;
- diagnostic.

1.2 Positionnement dans l'architecture de bout en bout

Le serveur ACS réside dans le réseau. Il gère des dispositifs situés dans les locaux d'abonné via le protocole CWMP. Ce protocole est indépendant de la technologie d'accès spécifique utilisée par le fournisseur de services, même s'il dépend de la connectivité de couche IP qui a été établie.

1.3 Objectifs de sécurité

La sécurité CWMP est censée être modulable afin de tenir compte d'une large gamme d'équipements CPE, du plus simple au plus sophistiqué. Les objectifs de sécurité sont les suivants:

- éviter toute altération des fonctions de gestion d'un équipement CPE ou du serveur ACS, ou des transactions qui ont lieu entre un équipement CPE et le serveur ACS;
- assurer la confidentialité des transactions entre un équipement CPE et le serveur ACS;
- permettre une authentification appropriée pour chaque type de transaction;
- éviter le vol de service.

2 Architecture

2.1 Eléments du protocole

Les applications CWMP sont définies au niveau supérieur d'une pile, dont les autres niveaux sont respectivement les suivants: méthodes RPC, SOAP, HTTP, SSL/TLS, TCP et IP, comme spécifié dans le rapport [BBF TR-069].

2.2 Mécanismes de sécurité

Les mécanismes pris en charge par le protocole CWMP incluent les secrets partagés HTTP et SSL/TLS.

2.3 Eléments architecturaux

Le protocole CWMP repose sur la définition et l'extraction à distance de variables nommées, la création et la suppression d'objets distants et l'invocation d'un petit ensemble de méthodes prédéfinies, afin de prendre en charge les mécanismes de découverte automatique, de notification et de transfert de fichier.

Les modèles d'information CWMP standard sont spécifiés au § 6.2 de la présente Recommandation. Ils peuvent aussi être étendus avec des spécifications propres au fabricant.

Les sessions CWMP peuvent être lancées soit par le serveur ACS soit par un équipement CPE. Au moment de son initialisation, l'équipement CPE peut contacter un serveur ACS pour obtenir une partie ou la quasi-totalité de sa configuration, y compris éventuellement son micrologiciel.

3 Procédures et spécifications

3.1 Découverte du serveur ACS

L'équipement CPE peut avoir une adresse URL de serveur ACS par défaut intégrée dans sa configuration ou peut obtenir l'identité du serveur ACS par le biais de la configuration locale ou d'une option DHCP. Le protocole DHCP peut aussi fournir un code d'approvisionnement, à utiliser par l'équipement CPE pour poursuivre son identification auprès du serveur ACS. Le serveur ACS peut lui-même modifier l'adresse URL à utiliser par l'équipement CPE, qui contactera alors un autre serveur ACS.

Si l'adresse URL du serveur ACS contient HTTPS, l'équipement CPE doit utiliser les protocoles SSL/TLS pour établir la session avec le serveur ACS.

3.2 Etablissement de la connexion

L'équipement CPE peut lancer une session avec le serveur ACS au moment de son initialisation, ou au moment périodique ou programmé configuré par le serveur ACS pour l'envoi d'un message d'information, ou lorsque, conformément à son approvisionnement, il doit envoyer une notification de changement de valeur ou d'état, ou encore pour rétablir une session antérieure qui s'est terminée prématurément. L'équipement CPE ne garde pas une session ouverte lorsqu'il n'a pas d'information à échanger avec le serveur ACS.

Le serveur ACS peut lancer indirectement une session avec l'équipement CPE en demandant à ce dernier, via une demande HTTP, d'ouvrir une session avec lui.

3.3 Utilisation des protocoles SSL/TLS et TCP

Pour toutes les sessions, il est recommandé, mais pas obligatoire, d'utiliser les protocoles SSL/TLS. En cas d'utilisation, l'équipement CPE doit authentifier le serveur ACS au moyen d'une authentification fondée sur un certificat. Le serveur ACS est également encouragé à authentifier l'équipement CPE.

Les autres sous-paragraphes du paragraphe 3 décrivent en détails les opérations de codage de message (SOAP), d'établissement de session, d'exploitation et de terminaison ainsi que de transfert de fichier. D'autres procédures d'authentification sont définies, notamment l'authentification HTTP de l'équipement CPE par le serveur ACS, si l'équipement CPE n'a pas encore été authentifié pendant la négociation SSL/TLS.

Annexe A – Méthodes RPC

Les types de données et les messages définis pour les appels de procédure à distance (RPC) CWMP sont définis dans l'Annexe A du rapport [BBF TR-069]. Outre la syntaxe de chaque message et de la réponse associée, cette annexe spécifie les contraintes comportementales spéciales susceptibles de s'appliquer au serveur ACS ou à l'équipement CPE.

Cette annexe contient un schéma XML générique.

Annexe B – Supprimée

(supprimée de cette édition du rapport TR-069)

Annexe C – Bons signés

Annexe D – Gestion d'identité sur le web

Annexe E – Format de paquetage signé

Annexe F – Association dispositif-passerelle

Le protocole CWMP peut être utilisé pour télégérer des dispositifs CPE qui sont connectés dans un réseau local par une passerelle. Lorsqu'un serveur ACS gère à la fois un dispositif et la passerelle par laquelle le dispositif est connecté, il peut être utile pour le serveur ACS de pouvoir déterminer l'identité de cette passerelle particulière.

Les procédures définies dans cette annexe permettent à un serveur ACS de déterminer l'identité de la passerelle par laquelle un dispositif donné est connecté. Le mécanisme repose sur l'utilisation du protocole DHCP à la fois par le dispositif et par la passerelle.

Dans un cas d'utilisation modèle, il se peut qu'un serveur ACS établissant la qualité de service pour un service particulier doive approvisionner à la fois le dispositif et la passerelle par laquelle ce dispositif est connecté. Pour cette dernière, le serveur ACS devra en déterminer l'identité.

Pour pouvoir prendre en charge cette fonctionnalité, la passerelle et le dispositif doivent tous deux être gérés au moyen du protocole CWMP et ce, par le même serveur ACS ou par des serveurs ACS distincts couplés de façon appropriée.

Annexe G – Demande de connexion via une passerelle NAT

La fonction de traduction d'adresse réseau (NAT) dans une passerelle sépare l'espace d'adresses IP côté réseau local de l'espace IP côté réseau étendu. Un équipement CPE situé derrière une passerelle NAT peut utiliser les méthodes définies précédemment pour lancer des sessions, mais les procédures définies dans cette annexe sont nécessaires pour permettre au serveur ACS de demander une connexion à l'équipement CPE. Il n'est pas nécessaire que la passerelle NAT prenne en charge le protocole CWMP.

6.1.2 Configuration automatique et approvisionnement en services dynamique

Le protocole CWMP permet à un serveur ACS d'approvisionner un équipement CPE ou un ensemble d'équipements CPE sur la base de divers critères.

Le mécanisme d'approvisionnement permet d'approvisionner un équipement CPE au moment de la connexion initiale au réseau d'accès large bande, et de procéder à un réapprovisionnement ou à une reconfiguration ultérieurement. Est notamment pris en charge le réapprovisionnement asynchrone d'un équipement CPE lancé par le serveur ACS.

Les mécanismes d'identification inclus dans le protocole permettent d'approvisionner un équipement CPE sur la base soit des spécifications propres à cet équipement soit d'un ensemble de critères tels que le fabricant, le modèle ou la version logicielle de l'équipement CPE.

Le protocole comporte aussi des outils facultatifs pour gérer les éléments d'applications ou de services facultatifs propres à l'équipement CPE pour lesquels un niveau supplémentaire de sécurité est nécessaire, par exemple ceux qui font intervenir un paiement.

Le mécanisme d'approvisionnement permet de prendre en charge directement des extensions futures relatives à l'approvisionnement en services et en capacités non inclus dans cette version.

6.1.3 Gestion d'image logicielle/micrologicielle

Le protocole CWMP offre un cadre pour la gestion du téléchargement de fichiers d'image logicielle/micrologicielle d'équipement CPE. Il comporte des mécanismes pour l'identification de version, le lancement du téléchargement d'un fichier (téléchargement lancé par le serveur ACS ou, éventuellement, par l'équipement CPE) et la notification au serveur ACS du succès ou de l'échec du téléchargement du fichier.

6.1.4 Surveillance de l'état et de la qualité de fonctionnement

Le protocole CWMP permet à un équipement CPE de fournir des informations que le serveur ACS peut utiliser pour surveiller l'état et la qualité de fonctionnement de l'équipement CPE. Par ailleurs, un ensemble de mécanismes permettent à l'équipement CPE de notifier activement tout changement de son état au serveur ACS. Le rapport [BBF TR-143] décrit des tests permettant d'évaluer l'expérience des abonnés en termes de débit large bande.

6.1.5 Diagnostic

Le protocole CWMP permet à un équipement CPE de fournir des informations que le serveur ACS peut utiliser pour diagnostiquer et résoudre des problèmes de connectivité ou de service et permet d'exécuter des tests de diagnostic définis.

6.1.6 Sécurité

Le protocole CWMP est conçu pour offrir un degré élevé de sécurité. Le modèle de sécurité est par ailleurs conçu pour être modulable, avec une sécurité de base pour les équipements CPE les moins robustes et une meilleure sécurité pour les équipements CPE qui peuvent prendre en charge des mécanismes de sécurité plus avancés. Les objectifs de sécurité du protocole CWMP sont les suivants:

- Eviter toute altération des fonctions de gestion d'un équipement CPE ou du serveur ACS, ou des transactions qui ont lieu entre un équipement CPE et le serveur ACS.
- Permettre une authentification mutuelle forte entre un équipement CPE et le serveur ACS.
- Assurer la confidentialité des transactions entre un équipement CPE et le serveur ACS.
- Permettre une authentification appropriée pour chaque type de transaction.
- Eviter le vol de service.

6.2 Modèles de données

Dans le protocole CWMP, un concept essentiel est celui du modèle de données. Un modèle de données comporte des objets et des paramètres qui peuvent être utilisés par les appels de méthode générique CMWP. Ces objets et paramètres exposent des données de configuration, de diagnostic ou d'état pour divers types de services et de dispositifs. Par exemple, le modèle de données d'un dispositif de VoIP expose des paramètres concernant la configuration SIP, et notamment les capacités liées à la VoIP. Les modèles de données définissent un superensemble de fonctionnalités qui peuvent être gérées pour un dispositif ou un service particulier; les dispositifs mettent en œuvre les parties des modèles de données qui correspondent à leurs fonctionnalités spécifiques.

Les spécifications des modèles de données de gestion d'équipements CPE sur un réseau étendu sont définies dans [BBF TR-106], [BBF TR-143], [BBF TR-157], [BBF TR-181 version 2], [BBF TR-104], [BBF TR-135], [BBF TR-140] et [BBF TR-196].

[BBF TR-106] contient des informations génériques pour la définition des modèles de données CWMP, notamment des spécifications concernant la hiérarchie, les règles applicables aux items obsolètes ou déconseillés, les types de données, et le schéma XML des modèles de données CWMP, qui sert à définir tous les modèles de données.

Les équipements CPE, par exemple les passerelles résidentielles (RG), les boîtiers-adaptateurs (STB) et les mémoires rattachées su réseau (NAS), sont approvisionnés et gérés au moyen d'un ensemble commun de paramètres, qui fait que ces dispositifs sont reconnaissables par le serveur ACS de réseau et qui permet un approvisionnement automatique et une gestion continue.

Les rapports techniques qui établissent ces paramètres sont les suivants:

- [BBF TR-181 version 2]: *Device data model for TR-069*
- [BBF TR-157]: *Component objects for CWMP*
- [BBF TR-143]: *Enabling network throughput performance tests and statistical monitoring*

Les rapports techniques qui définissent les modèles de données de service sont les suivants:

- [BBF TR-104]: *DSLHome provisioning parameters for VOIP CPE*
- [BBF TR-135]: *Data model for a TR-069 enabled set-top box*
- [BBF TR-140]: *TR-069 data model for storage service enabled devices*
- [BBF TR-196]: *Femto access point service data model*

6.2.1 TR-181 version 2: modèle de données de dispositif TR-069

Le rapport [BBF TR-181 version 2] définit la version 2 du modèle de données de dispositif TR-069. Le modèle de données s'applique à tous les types de dispositifs compatibles TR-069, y compris les dispositifs d'extrémité, les passerelles Internet et d'autres dispositifs de l'infrastructure de réseau. Il s'agit d'une nouvelle version qui annule et remplace à la fois la version 1 du rapport [b-BBF TR-181 version I] (non inclus dans la présente Recommandation) et l'amendement 2 au rapport [b-BBF TR-098] (non inclus dans la présente Recommandation). Les installations existantes peuvent continuer à utiliser les modèles de données InternetGatewayDevice:1 et Device:1, qui sont toujours valables.

NOTE – Le passage au modèle de données Device:2 était nécessaire pour pouvoir surmonter certaines limitations inhérentes au modèle de données InternetGatewayDevice:1, qui s'est avéré peu souple et qui causait des problèmes lorsqu'il s'agissait de représenter des configurations de dispositifs complexes. Toutefois, lors de la définition de ce modèle de données nouvelle génération, il a été pris soin de bien prendre en compte toutes les fonctionnalités des modèles de données InternetGatewayDevice:1 et Device:1.

Le modèle de données Device:2 défini dans la version 2 du rapport [BBF TR-181 version 2] comporte un ensemble d'objets de données ayant trait notamment à des informations de base relatives au dispositif, à la configuration de l'heure du jour, à la configuration des interfaces de réseau et de la pile de protocoles, à la gestion du routage et du pontage et aux tests de diagnostic. Est également défini un profil de base qui spécifie un niveau minimal de prise en charge du modèle de données.

Le modèle de données Device:2 est articulé autour du mécanisme d'empilage d'interfaces. Les interfaces de réseau et les couches de protocole sont modélisées sous la forme d'objets de données indépendants qui peuvent être empilés, l'un au-dessus de l'autre, dans n'importe laquelle des configurations qu'un dispositif peut prendre en charge.

Pour faciliter l'harmonisation technique de la Recommandation et de la version 2 du rapport [BBF TR-181 version 2], la structure du reste du présent paragraphe (présenté dans un encadré) suit celle de ce rapport. Les numéros des titres renvoient aux numéros de paragraphe de la version 2 du rapport technique [BBF TR-181 version 2].

4 Architecture

4.1 Couches d'interfaces

Ce rapport technique modélise les interfaces de réseau et les couches de protocole sous la forme d'objets de données indépendants, généralement appelés objets interface (ou interfaces). Les objets interface peuvent être empilés, l'un au-dessus de l'autre, en utilisant des références de trajet afin de définir dynamiquement les relations entre les interfaces.

L'objet interface et la pile d'interfaces sont des concepts issus du document [b-IETF RFC 2863].

Dans le modèle de données Device:2, les objets interface sont restreints arbitrairement à des définitions valables au niveau de la couche de réseau IP ou en dessous (à savoir au niveau des couches 1 à 3 du modèle OSI). Toutefois, des objets interface propres au fabricant qui sortent de ce cadre restreint PEUVENT être définis.

4.2 Objets interface

Un objet interface est un type d'interface de réseau ou de couche de protocole. Chaque type d'interface est modélisé par une table du modèle de données Device:2, avec une ligne pour chaque instance d'interface (par exemple IP.Interface.{i} pour les interfaces IP).

Chaque objet interface contient un ensemble principal de paramètres et d'objets, qui sert de gabarit pour définir les objets interface dans le modèle de données. Les objets interface peuvent aussi contenir d'autres paramètres et sous-objets propres au type d'interface.

4.3 Table InterfaceStack (pile d'interfaces)

Bien que la pile d'interfaces puisse être traversée via des paramètres LowerLayers (décrits au § 4.2.1 Lower Layers), un autre mécanisme est défini afin de faciliter la visualisation de l'ensemble des relations d'empilage et d'accéder rapidement aux objets à l'intérieur de la pile.

La table InterfaceStack est un objet du modèle de donnés Device:2 (Device.InterfaceStack.{i}). Il s'agit d'une table en lecture seule dont les lignes sont générées automatiquement par l'équipement CPE sur la base des relations existantes qui sont configurées entre les objets interface (via le paramètre LowerLayers de chaque instance d'interface). Chaque ligne de la table représente un "lien" entre un objet interface de couche supérieure (désigné par le paramètre HigherLayer) et un objet interface de couche inférieure (désigné par le paramètre LowerLayer). Autrement dit, les paramètres HigherLayer et LowerLayer d'une ligne de la table InterfaceStack auront toujours tous les deux une valeur significative.

NOTE – En conséquence, les instances d'interface qui ont été bloquées ne seront pas représentées dans la table InterfaceStack. Par ailleurs, il est probable que plusieurs groupes distincts d'objets interface empilés coexisteront dans la table (par exemple, chaque interface IP sera la racine d'un groupe distinct; les "fragments" inutilisés, par exemple un canal DSL secondaire ayant un circuit PVC ATM configuré qui n'est rattaché à rien au-dessus, subsisteront s'ils restent interconnectés; et, enfin, des "fragments" partiellement configurés peuvent être présents au moment de l'établissement d'une pile d'interfaces).

5 Définition des paramètres

La définition normative du modèle de données Device:2 est répartie dans plusieurs documents relatifs aux instances de modèle de données (voir l'Annexe A du rapport TR-069). Le Tableau 3 présente les versions du modèle de données Device:2 et les instances de modèle de données qui avaient été définies au moment de la rédaction. Il indique en outre les rapports techniques correspondants et donne les liens vers les fichiers XML et HTML associés. Le document XML TR-181i2 définit le modèle Device:2 proprement dit, et importe des éléments supplémentaires des autres documents XML énumérés. Le document HTML TR-181i2 est un rapport généré à partir des fichiers XML, qui contient la totalité du modèle de données Device:2 sous forme lisible par l'homme.

Annexe A – Pontage et mise en file d'attente

Cette annexe définit le modèle de mise en file d'attente et de pontage (classification des paquets, mise en file d'attente et programmation, et pontage), le mappage par défaut de la qualité de service entre les couches 2 et 3 ainsi que les notations URN pour les tables App et Flow (App ProtocolIdentifier, Flow Type et Flow TypeParameters).

6.2.2 TR-157: objets composant pour le protocole CWMP

Le rapport [BBF TR-157] définit les objets composant à utiliser dans les dispositifs gérés CWMP pour tous les modèles de données racine. Un objet composant est défini comme étant un objet et les paramètres qu'il contient, et il est destiné à être utilisé dans n'importe quel modèle de données racine CWMP applicable. Les objets peuvent se trouver au niveau supérieur ou à un sous-niveau approprié.

Afin de prendre en charge les fonctionnalités définies dans le rapport [BBF TR-157], une extension au modèle de données Device et au modèle de données InternetGatewayDevice est spécifiée dans le Tableau 1 du rapport [BBF TR-157]. Pour le modèle de données Device, cette extension est considérée comme faisant partie de Device:1.4 (version 1.4 du modèle de données Device), qui étend la version 1.3 du modèle de données Device défini dans la version 1 du rapport [BBF TR-157]. Pour le modèle de données InternetGatewayDevice, cette extension est considérée comme faisant partie de InternetGatewayDevice:1.6 (version 1.6 du modèle de données InternetGatewayDevice), qui étend la version 1.5 du modèle de données InternetGatewayDevice défini dans la version 1 du rapport TR-157.

6.2.3 TR-143: tests de qualité de fonctionnement du réseau et surveillance statistique

Le rapport [BBF TR-143] définit une série de tests de surveillance active que les fournisseurs de services de réseau peuvent utiliser pour surveiller et/ou diagnostiquer l'état des trajets dans leur réseau large bande desservant des populations d'abonnés qui disposent d'équipements CPE compatibles TR-069. La surveillance active prend en charge à la fois les diagnostics lancés par le réseau et les diagnostics lancés par les équipements CPE en vue de surveiller et de caractériser les trajets de service, soit en permanence, soit sur demande. Ces outils génériques servent de plate-forme pour la validation des objectifs de qualité de service et des accords de niveau de service.

Pour faciliter l'harmonisation technique de la Recommandation et du rapport [BBF TR-143], la structure du reste du présent paragraphe suit celle de ce rapport. Les numéros des titres renvoient aux numéros de paragraphe du rapport [BBF TR-143].

4 Surveillance active

La surveillance active consiste à introduire un trafic TCP ou UDP fictif dans un réseau, dans ce cas un réseau d'accès large bande qui inclut des équipements CPE compatibles TR-069, afin d'évaluer la qualité de service. Le trafic de test peut provenir du réseau ou d'un équipement CPE compatible [BBF TR-143].

5 Définition des paramètres

Le § 5 définit la syntaxe et la sémantique spécifiques des paramètres d'un service de VoIP. Les paramètres sont regroupés dans des paquetages, qui sont eux-mêmes regroupés dans des profils pour diverses applications (§ 7).

6 Spécifications de notification

7 Définition des profils

7.1 Notation

7.2 Profil de téléchargement

Ce profil configure l'équipement CPE pour exécuter un test de téléchargement et pour enregistrer les résultats. Les champs DSCP et de priorité Ethernet peuvent être configurés dans le cadre du profil.

7.3 Profil de téléchargement avec TCP

Ce profil étend le profil de téléchargement afin d'enregistrer les dates et heures de demande et de réponse TCP, lorsque le téléchargement utilise TCP.

7.4 Profil de téléversement

Ce profil configure l'équipement CPE pour exécuter un test de téléversement et pour enregistrer les résultats. Les champs DSCP et de priorité Ethernet peuvent être configurés dans le cadre du profil.

7.5 Profil de téléversement avec TCP

Ce profil étend le profil de téléversement afin d'enregistrer les dates et heures de demande et de réponse TCP, lorsque le téléversement utilise TCP.

7.6 Profil du service écho UDP

Ce profil configure l'équipement CPE pour exécuter un test d'écho UDP.

7.7 Profil du service écho plus UDP

Ce profil étend le profil du service écho UDP moyennant l'adjonction d'un paramètre d'activation du service écho plus.

Appendice A – Théorie de fonctionnement

A.1 Service écho plus UDP

La fonctionnalité écho plus UDP est une extension de la fonction écho ICMP ordinaire. Elle permet de mesurer à la fois le temps aller et le temps aller-retour des paquets. Le traitement est effectué conformément aux marquages DSCP ou de priorité Ethernet, ce qui permet d'améliorer la mesure de la qualité de fonctionnement telle qu'elle est vue par l'abonné.

A.2 Diagnostic de téléchargement utilisant le transport FTP

Ce test consiste à procéder au transfert FTP d'un fichier test du serveur de test à l'équipement CPE et à enregistrer le nombre d'octets reçus et plusieurs horodates afin d'évaluer la qualité du téléchargement.

A.3 Diagnostic de téléversement utilisant le transport FTP

Ces tests sont similaires au test de téléchargement.

A.4 Diagnostic de téléchargement utilisant le transport HTTP

Ces tests sont similaires au test de téléchargement.

A.5 Diagnostic de téléversement utilisant le transport HTTP

Ces tests sont similaires au test de téléchargement.

6.2.4 TR-104: Paramètres d'approvisionnement DSLHome pour les équipements CPE VoIP

Le rapport [BBF TR-104] définit le modèle de données pour l'approvisionnement d'un dispositif d'équipement CPE de téléphonie IP (VoIP) par un serveur de configuration automatique (ACS) utilisant le mécanisme défini dans le rapport [BBF TR-069].

Pour faciliter l'harmonisation technique de la Recommandation et du rapport [BBF TR-104], la structure du reste du présent paragraphe (présenté dans un encadré) suit celle de ce rapport. Les numéros des titres renvoient aux numéros de paragraphe du rapport [BBF TR-104].

1 Introduction

Le rapport technique TR-104:

- Est compatible avec des dispositifs VoIP qui sont soit intégrés dans un dispositif de passerelle Internet, soit des dispositifs indépendants et autonomes.
- Est compatible avec des dispositifs VoIP qui prennent en charge plusieurs services de VoIP distincts, pouvant chacun être associé à plusieurs lignes distinctes.
- Prend en charge l'utilisation des protocoles de signalisation SIP et MGCP.
- Prend en charge différents types d'équipement CPE VoIP, y compris les points d'extrémités VoIP, les proxies de liaison sortante SIP et les agents d'utilisateur dos à dos SIP.

2 Architecture

Le rapport [BBF TR-104] définit un objet VoiceService comme étant le conteneur associé aux objets d'approvisionnement pour l'équipement CPE VoIP. Dans le contexte du rapport [BBF TR-106], l'objet VoiceService défini dans le rapport [BBF TR-104] est un objet de service. Les différents dispositifs CPE pourront contenir zéro ou plus instances d'objet VoiceService. La présence de plus d'un objet VoiceService pourrait être nécessaire, par exemple lorsqu'un dispositif CPE assure la fonction de mandataire de gestion pour d'autres équipements CPE VoIP non compatibles TR-069. Par exemple, un dispositif de passerelle Internet peut servir de mandataire de gestion pour un ou plusieurs téléphones VoIP non compatibles TR-069.

Chaque objet VoiceService contient un ou plusieurs objets VoiceProfile. Un objet VoiceProfile correspond à une ou plusieurs lignes téléphoniques qui partagent la même configuration de base. Chaque objet VoiceProfile contient un ou plusieurs objets ligne, qui représentent chacun une ligne téléphonique distincte unique.

L'objet VoiceProfile permet à un dispositif téléphonique à multi-lignes de regrouper des lignes ayant des caractéristiques communes sous un seul et même profil. Puisque ce modèle autorise plusieurs objets VoiceProfile, un seul et même dispositif téléphonique à multi-lignes peut disposer de groupes de lignes ayant des configurations différentes. On pourrait utiliser cette structure pour associer des groupes distincts de lignes ayant des fournisseurs de services complètement séparés, chacun avec leur propre serveur VoIP et leurs propres exigences en matière de configuration. Elle pourrait également être utilisée pour faire une distinction entre différents niveaux de service d'un seul et même fournisseur. Par exemple, un dispositif unique pourrait offrir des lignes privées et des lignes professionnelles, chacune associée à un objet VoiceProfile distinct, et se différenciant par ses caractéristiques sur le plan de la qualité.

3 Modèle de données VoiceService version 1.0

Le § 3 définit la syntaxe et la sémantique spécifiques des paramètres d'un service de VoIP. Les paramètres sont regroupés dans des paquetages, qui sont eux-mêmes regroupés dans des profils pour diverses applications (§ 4).

4 Définition des profils

4.1 Notation

4.2 Profil Endpoint

Ce profit rassemble des paramètres qui conviennent pour un point d'extrémité VoIP en plusieurs groupes. Le groupe de fonctionnalités comprend les limites concernant le choix du codec et du débit, le nombre de sessions simultanées, les protocoles de signalisation disponible, la détection et le transfert de télécopie et modem, le plan de numérotage, la tonalité, la sonnerie et la personnalisation du cadran. Le groupe de profils téléphoniques est subdivisé en plusieurs groupes plus petits, se rapportant au protocole RTP, à l'état de la ligne, aux paramètres du codec utilisé, aux temporisateurs de session et aux adresses d'extrémité distante, ainsi qu'aux compteurs pour le contrôle de la qualité de fonctionnement.

Les trois profils présentés ci-après contiennent des informations analogues, mais sous des formes adaptées au protocole de signalisation auquel ils sont associés.

4.3 Profil SIPEndpoint

Ce profil étend le profil Endpoint avec des paramètres spécifiques importants pour la signalisation SIP, comprenant en particulier les informations de mandataire SIP, d'enregistrement et d'authentification de l'abonné.

4.4 Profil MGCPEndpoint

Ce profil étend le profil Endpoint avec des paramètres importants pour la signalisation MGCP, qui comprennent les informations d'identité et d'enregistrement de l'agent et de l'utilisateur local.

4.5 Profil H323Endpoint

Ce profil étend le profil Endpoint avec des paramètres importants pour la signalisation H.323, qui comprennent en particulier les informations d'identité et d'enregistrement du portier et de l'utilisateur local.

4.6 Profil TAEndpoint

Ce profil est destiné à être utilisé par un point d'extrémité de terminal. Il élargit le profil Endpoint de base avec des listes de ports physiques associés et leurs identifiants qui partagent les mêmes paramètres.

Appendice A – Opérations concernant les éléments de service

L'Appendice A définit les différents éléments de service de signalisation VoIP qui peuvent être déclenchés par les préfixes du plan de numérotation de l'abonné ou l'utilisation des touches du combiné téléphonique, par exemple l'activation ou la désactivation de fonctionnalités comme le transfert d'appel, l'identification de l'appelant ou la sonnerie sélective. Il peut également s'agir par exemple de l'élément de service qui permet de passer d'un appel en attente à l'autre.

Appendice B – Téléchargement de fichiers de tonalité et de sonnerie

L'Appendice B décrit comment utiliser la fonction de téléchargement de fichiers TR-069 dans le but précis de télécharger des tonalités ou des sonneries VoIP.

6.2.5 TR-135: Modèle de données de boîtier-adaptateur compatible TR-069

Le rapport [BBF TR-135] présente les spécifications applicables à la télégestion de la fonctionnalité de télévision numérique (TVIP ou radiodiffusion) sur des dispositifs STB via le protocole SWMP. L'accès au contenu du réseau ou de l'enregistreur PVR est géré par une plate-forme de services de TVIP et ne relève pas du serveur ACS. Celui-ci peut effectuer une partie de la configuration de départ d'un boîtier STB qui vient d'être installé, mais ses fonctions principales sont la configuration des paramètres STB pour la gestion des pannes et la collecte de statistiques pour le contrôle de

la Qos/QoE. La plupart des paramètres définis dans le rapport [BBF TR-135] sont donc en lecture seule pour le serveur ACS.

NOTE – Le rapport [BBF TR-135] définit, d'une part, le modèle de données pour décrire un dispositif STB et, d'autre part, les règles relatives aux notifications de modification de la valeur d'un paramètre, ce qui donne des profils de modèles de données types que l'on verrait normalement pendant la télégestion d'un dispositif de cette nature.

Pour faciliter l'harmonisation technique de la Recommandation et du rapport [BBF TR-135], la structure du reste du présent paragraphe (présenté dans un encadré) suit celle de ce rapport. Les numéros des titres renvoient aux numéros de paragraphe du rapport [BBF TR-135].

5 Architecture

Un boîtier-adaptateur (STB) est modélisé comme étant un ensemble de fonctions et fonctionnalités, pour la plupart facultatives et pouvant exister dans plus d'une instance. Outre l'infrastructure STB de base, les autres composants sont ceux dont les profils sont définis ci-après au § 7.

6 Définitions des paramètres

Le § 6 définit la syntaxe et la sémantique spécifiques des paramètres d'un boîtier STB. Les paramètres sont regroupés dans des paquetages, qui sont eux-mêmes regroupés dans des profils pour diverses applications (§ 7).

7 Définitions des profils

7.1 Notation

7.2 Profil Baseline

Ce profil donne des informations en lecture seule sur les fonctionnalités du boîtier STB, y compris les normes qu'il prend en charge, le nombre maximal de flux de différents types qu'il peut prendre en charge simultanément. Les paramètres modifiables se limitent à la commande silence et au choix des langues pour les flux audio et sous-titres.

7.3 Profil PVR

Ce profil renvoie l'état d'une possible application PVR. Le stockage PVR est pris en charge via une référence à un objet storageService défini dans le rapport [BBF TR-140].

7.4 Profil DTT

Ce profil fournit des paramètres de configuration pour la radiodiffusion vidéonumérique, ainsi que des paramètres de maintenance et de contrôle de la qualité de fonctionnement en lecture seule.

7.5 Profil IPTVbaseline

Ce profil fournit des paramètres concernant la QoS en lecture-écriture pour la mise en tampon et une série de paramètres en lecture seule qui rendent compte des fonctionnalités du boîtier STB et de l'état en cours des fonctions de TVIP.

7.6 Profil RTCP

Ce profil fournit une commande de configuration simple (activation, définition des intervalles) et un rapport d'état.

7.7 Profil RTPAVPF

Ce profil configure la fonctionnalité de retour d'information RTP en temps réel et rend compte de son statut en cours.

7.8 Profil IPTVhomenetwork

Ce profil rend compte de l'état et des capacités des interfaces du réseau domestique du boîtier STB, tels que traduits depuis le flux du côté du réseau étendu.

7.9 Profil IGMP

Ce profil offre un moyen de configurer les paramètres IGMP comme l'étiquetage VLAN, la robustesse et l'intervalle des rapports, et donne des statistiques sur l'état et le contrôle de la qualité de fonctionnement en lecture seule.

7.10 Profil BasicPerfmon

Ce profil prend en charge la configuration des paramètres de contrôle de la qualité de fonctionnement de haut niveau, par exemple Enable, TimeReference, etc. Il contient des statistiques dans le boîtier STB dans son ensemble et de statistiques de haut niveau pour les principaux composants à différents niveaux, par exemple, RTP, MPEC et décodeur vidéo.

7.11 Profil ECPerfmon

Ce profil contient des statistiques relatives à la capacité de correction d'erreur RTP.

7.12 Profil VideoPerfmon

Ce profil donne des statistiques associées à la qualité de lecture vidéo.

7.13 Profil AudioPerfmon

Ce profil contient des statistiques associées à la qualité de lecture audio.

7.14 Profil AudienceStats

Ce profil recueille des statistiques sur le comptage des canaux et la durée.

7.15 Profil AnalogOutput

Ce profil rend compte des fonctionnalités du boîtier STB permettant de prendre en charge des dispositifs externes comme les écrans vidéo.

7.16 Profil Digital Output

Ce profil indique si la protection des contenus numériques à grande largeur de bande (HDCP, high-bandwidth digital content protection) est utilisée sur une sortie vidéo donnée.

7.17 Profil CA

Ce profil indique l'existence d'un accès conditionnel, qui est modélisé via un lecteur de carte intelligent.

7.18 Profil DRM

Ce profil fournit des paramètres en lecture seule sur l'état actuel du flux média en cours.

Appendice I – Théorie de fonctionnement

Cet appendice décrit un grand nombre de cas d'utilisation et explique comment le modèle d'informations STB y est employé.

6.2.6 TR-140: modèle de données de dispositifs compatibles avec le service de stockage TR-069

Le rapport [BBF TR-140] permet à un serveur ACS de gérer un service de stockage de base. On trouvera ci-après la liste des fonctionnalités de prise en charge que peut offrir un serveur ACS utilisant le protocole CWMP:

- Configuration et paramétrage de base pendant l'activation ([BBF TR-140] et [BBF TR-140 version 2]).
- Etablissement des justificatifs d'identité des utilisateurs et accès privilégié au fichier ([BBF TR-140] (accès au dossier)).
- Extraction de l'état du dispositif ([BBF TR-140] (paramètres) et [BBF TR-181 version 2]).

- Configuration du mode sans fil (par exemple sécurité WEP) pour un dispositif de service de stockage avec accès Wi-Fi.
- Diagnostics et dépannage du réseau, par exemple connectivité du réseau avec le dispositif de passerelle Internet et à l'Internet (version 2 de TR-181 (paramètres de connexion)).

NOTE – Ces fonctionnalités ne sont pas toutes traitées avec ce modèle de données; certaines relèvent du protocole CWMP natif et d'autres sont traitées via d'autres modèles de données.

4 Définition des paramètres

Le § 4 définit la syntaxe et la sémantique spécifiques des paramètres d'un boîtier STB. Les paramètres sont regroupés dans des paquetages, qui sont eux-mêmes regroupés dans des profils pour diverses applications (§ 6).

5 Notifications

6 Définition des profiles

6.1 Notation

6.2 Profil Baseline

Ce profil fournit des informations en lecture seule concernant le service de stockage, y compris ses capacités de stockage et d'accès, les dispositifs physiques, les systèmes de fichiers et les dossiers de niveau supérieur. Les paramètres modifiables se limitent à la configuration de l'identité du réseau externe du service de stockage.

6.3 Profil Useraccess

Ce profil permet de configurer le réseau et les utilisateurs locaux, ainsi que leurs droits d'accès et leurs justificatifs d'identité pour l'ouverture d'une session.

6.4 Profil Groupaccess

Ce profil étend le profil Useraccess utilisateur aux groupes d'utilisateurs et permet de définir des privilèges d'accès au niveau du groupe.

6.5 Profil FTPserver

Ce profil permet de configurer un éventuel serveur FTP associé au service de stockage, y compris sa volonté de desservir des utilisateurs anonymes.

6.6 Profil SFTPserver

Ce profil étend le profil FTPserver pour configurer également un éventuel serveur SFTP associé au service de stockage.

6.7 Profil HTTPserver

Ce profil permet de configurer un éventuel serveur HTTP associé au service de stockage, y compris sa politique de sécurité.

6.8 Profil HTTPSserver

Ce profil étend le profil HTTP serveur pour y inclure des paramètres HTTPS supplémentaires.

6.9 Profil Volumeconfig

Ce profil étend le profil Baseline pour gérer la configuration du volume logique et des dossiers de niveau supérieur.

6.10 Profile RAID

Ce profil configure des matrices de stockage et rend compte de l'état et de la capacité actuels de la matrice.

6.11 Profil Folderquota

Ce profil permet de configurer les politiques de capacité des dossiers, y compris le seuil d'alerte de surcapacité.

6.12 Profil Volumethreshold

Ce profil permet de configurer les politiques de capacité au niveau du volume logique.

6.13 Profil Networkserver

Ce profil permet de configurer les protocoles d'accès au réseau pouvant être utilisés pour téléaccéder au service de stockage.

7 Exemples d'utilisation

La vocation première d'un service de stockage géré selon TR-069 est de décharger l'abonné de la responsabilité de gestion du stockage. En même temps, un abonné nomade ou des serveurs externes (par exemple, le serveur ACS lui-même (mise à jour du logiciel) ou l'espace de stockage de l'enregistreur PVR) peut accéder à tout ou partie du stockage depuis l'extérieur et l'utiliser (voir [BBF TR-135]).

Annexe A – Théorie de fonctionnement

L'Annexe A décrit le fonctionnement du dispositif de stockage, y compris la gestion du dispositif amovible et la sécurité de l'accès et donne des exemples d'utilisation.

Annexe B – Description des types RAID

L'Annexe B présente les différentes combinaisons de disques correspondant à l'appellation RAID.

6.2.7 TR-196: modèle de données de service de point d'accès femto

Le rapport [BBF TR-196] définit le modèle de données d'un point d'accès femto (FAP, *femto access point)* pour la télégestion à l'aide du protocole CWMP. L'objectif du rapport [BBF TR-196] est de permettre à un opérateur de proposer aux abonnés un service d'accès femto géré. A ce titre, la plupart des éléments du service sont commandés par le serveur ACS.

Ce modèle de données de point FAP s'applique au nœud domestique B FDD UMTS (3G HNB). Toutefois, sa structure et son organisation peuvent être étendues pour couvrir d'autres types de dispositif FAP utilisant d'autres technologies d'interface radioélectrique.

Pour faciliter l'harmonisation technique de la Recommandation et du rapport [BBF TR-196], la structure du reste du présent paragraphe (présenté dans un encadré) suit celle de ce rapport. Les numéros des titres renvoient aux numéros de paragraphe du rapport [BBF TR-196].

4 Définition du modèle de données

Le § 4 définit la syntaxe et la sémantique spécifiques des paramètres d'un point FAP. Les paramètres sont regroupés dans des paquetages, qui sont eux-mêmes regroupés dans des profils pour diverses applications (§ 5).

5 Définition des profils

TR-196 définit de nombreux profils permettant de regrouper des fonctionnalités FAP. Un profil de base spécifie les détails de la configuration que l'on attend dans tout point FAP. D'autres profils décrivent les politiques d'accès local, la politique de sécurité, les différents protocoles hertziens pouvant être pris en charge et les fonctionnalités de contrôle de la qualité de fonctionnement, d'alerte et de diagnostic.

La liste des profils est la suivante:

2. Profil Baseline
3. Profil ACL
4. Profil Local IP access
5. Profil REM WCDMA FDD
6. Profil REM GSM
7. Profil GPS
8. Profil Transport SCTP
9. Profil Transport real time
10. Profil IPSec tunnel
11. Profil UMTS baseline
12. Profil UMTS self config
13. Profil UMTS self config NL in use intra freq cell
14. Profil UMTS self config NL in use inter freq cell
15. Profil UMTS self config NL in use inter RAT cell
16. Profil UMTS cell config baseline
17. Profil UMTS cell config advanced
18. Profil UMTS cell config freq measurement
19. Profil UMTS cell config UE internal measurement
20. Profil UMTS cell config NL intra freq cell
21. Profil UMTS cell config NL inter freq cell
22. Profil UMTS cell config NL inter RAT cell
23. Profil Fault management supported alarms
24. Profil Fault management active alarms
25. Profil Fault management profile event history
26. Profil Fault management profile expedited delivery
27. Profil Fault management profile queued delivery
28. Profil Performance management

Bibliographie

[b-UIT-T G.988] Recommandation UIT-T G.988 (2010), *Spécification de l'interface de gestion et de commande de l'unité ONU (OMCI)*.

[b-UIT-T Y.101] Recommandation UIT-T Y.101 (2000), *Infrastructure mondiale de l'information: termes et définitions*.

[b-BBF01] Processus d'approbation des rapports techniques du Broadband Forum.
<http://www.broadband-forum.org/about/download/trapprovalprocess.pdf>

[b-BBF TR-098] Amendement 2 au rapport technique TR-098 du Broadband Forum (2008), *Internet gateway device data model for TR-069* (remplacé par BBF TR-181 version 2).
<http://www.broadband-forum.org/technical/download/TR-098_Amendment-2.pdf>

[b-BBF TR-181 version 1] Version 1 du rapport technique TR-181 du Broadband Forum (2010), *LAN-side DSL CPE configuration* (remplacé par TR-181 BBF version 2).
<http://www.broadband-forum.org/technical/download/TR-181_Issue-1.pdf>

[b-IETF RFC 2863] IETF RFC 2863 (2000), *The Interfaces Group MIB*.

Autres documents connexes

[b-BBF TR-064] Rapport technique TR-064 du Broadband Forum (2004), *LAN-side DSL CPE configuration*.
<http://www.broadband-forum.org/technical/download/TR-064.pdf>

[b-BBF TR-68] Rapport technique TR-68 du Broadband Forum (2006), *Base requirements for an ADSL modem with routing*.
<http://www.broadband-forum.org/technical/download/TR-068_Issue-3.pdf>

[b-BBF TR-122] Amendement 1 – Rapport technique TR-122 du Broadband Forum (2006), *Base requirements for consumer-oriented analog terminal adapter functionality*.
<http://www.broadband-forum.org/technical/download/TR-122v1.01.pdf>

[b-BBF TR-124] Rapport technique TR-124 du Broadband Forum (2006), *Functional requirements for broadband residential gateway devices*.
<http://www.broadband-forum.org/technical/download/TR-124.pdf>

[b-BBF TR-131] Rapport technique TR-131 du Broadband Forum (2009), *ACS northbound interface requirements*.
<http://www.broadband-forum.org/technical/download/TR-131.pdf>

[b-BBF TR-133] Rapport technique TR-133 du Broadband Forum (2005), *DSLHome TR-064 extensions for service differentiation*.
<http://www.broadband-forum.org/technical/download/TR-133.pdf>

[b-BBF TR-142 version 2] Version 2 du rapport technique TR-142 du Broadband Forum (2010), *Framework for TR-069 enabled PON devices*.
<http://www.broadband-forum.org/technical/download/TR-142_Issue-2.pdf>

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, 2013