Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

G.9980

(11/2012)

SERIE G: SISTEMAS Y MEDIOS DE TRANSMISIÓN, SISTEMAS Y REDES DIGITALES

Redes de acceso – Redes internas

Gestión a distancia de los equipos en los locales del cliente por redes de banda ancha – Protocolo de gestión de equipos en los locales del cliente por redes de área extensa (WAN)

Recomendación UIT-T G.9980

UIT-T

ITU Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE G

SISTEMAS Y MEDIOS DE TRANSMISIÓN, SISTEMAS Y REDES DIGITALES

CONEXIONES Y CIRCUITOS TELEFÓNICOS INTERNACIONALES	G.100–G.199
CARACTERÍSTICAS GENERALES COMUNES A TODOS LOS SISTEMAS ANALÓGICOS DE PORTADORAS	G.200–G.299
CARACTERÍSTICAS INDIVIDUALES DE LOS SISTEMAS TELEFÓNICOS INTERNACIONALES DE PORTADORAS EN LÍNEAS METÁLICAS	G.300–G.399
CARACTERÍSTICAS GENERALES DE LOS SISTEMAS TELEFÓNICOS INTERNACIONALES EN RADIOENLACES O POR SATÉLITE E INTERCONEXIÓN CON LOS SISTEMAS EN LÍNEAS METÁLICAS	G.400–G.449
COORDINACIÓN DE LA RADIOTELEFONÍA Y LA TELEFONÍA EN LÍNEA	G.450–G.499
CARACTERÍSTICAS DE LOS MEDIOS DE TRANSMISIÓN Y DE LOS SISTEMAS ÓPTICOS	G.600–G.699
EQUIPOS TERMINALES DIGITALES	G.700–G.799
REDES DIGITALES	G.800–G.899
SECCIONES DIGITALES Y SISTEMAS DIGITALES DE LÍNEA	G.900–G.999
CALIDAD DE SERVICIO Y DE TRANSMISIÓN MULTIMEDIOS – ASPECTOS GENÉRICOS Y ASPECTOS RELACIONADOS AL USUARIO	G.1000–G.1999
CARACTERÍSTICAS DE LOS MEDIOS DE TRANSMISIÓN	G.6000–G.6999
DATOS SOBRE CAPA DE TRANSPORTE – ASPECTOS GENÉRICOS	G.7000–G.7999
ASPECTOS RELATIVOS A LOS PROTOCOLOS EN MODO PAQUETE SOBRE LA CAPA DE TRANSPORTE	G.8000–G.8999
REDES DE ACCESO	G.9000–G.9999
	G.9700–G.9799
	G.9800–G.9899
Redes internas	**G.9900–G.9999**

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T G.9980

Gestión a distancia de los equipos en los locales del cliente por redes de banda ancha – Protocolo de gestión de equipos en los locales del cliente por redes de área extensa (WAN)

Resumen

La Recomendación UIT-T G.9980 define los requisitos de gestión a distancia de los dispositivos conectados en el hogar del cliente por parte del proveedor. Se hace una presentación general de una familia de especificaciones técnicas y de las referencias normativas conexas. Se describe cómo están relacionadas las distintas especificaciones técnicas de esta familia. En las cláusulas 3 y 4 se incluye un glosario de los términos y definiciones empleados en las especificaciones técnicas.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T G.9980	2012-11-23	15	11.1002/1000/11019-en

Palabras clave

CWMP, TR-069.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Introducción

La base de esta Recomendación es el protocolo de gestión CPE WAN (CWMP) del Foro de la Banda Ancha, comúnmente denominado TR-069.

Este protocolo está previsto para la comunicación entre un CPE y un servidor de autoconfiguración (ACS). El protocolo de gestión CPE WAN define un mecanismo que comprende la autoconfiguración segura de un CPE, además de otras funciones de gestión del CPE en un marco común.

TR-069 especifica los requisitos genéricos del protocolo de gestión y los métodos que pueden aplicarse a cualquier CPE TR-069. En otros Informes técnicos (TR) del Foro de la Banda Ancha se especifican los objetos gestionados, o modelos de datos, de cada tipo de dispositivo o servicio específico.

Este protocolo puede emplearse para gestionar diversos tipos de CPE, incluidos los encaminadores autónomos y los dispositivos de cliente LAN. El protocolo es independiente del medio de acceso concreto utilizado por el proveedor de servicios, aunque depende de que el dispositivo haya establecido previamente una conexión en la capa IP.

Recomendación UIT-T G.9980

Gestión a distancia de los equipos en los locales del cliente por redes de banda ancha – Protocolo de gestión de equipos en los locales del cliente por redes de área extensa (WAN)

1 Alcance

En esta Recomendación se definen los requisitos de gestión a distancia de dispositivos conectados a la red en el hogar del cliente por parte del proveedor de servicios. Se hace una presentación general de una familia de especificaciones técnicas (véase la Figura 1) y de las referencias normativas conexas. Se describen cómo se relacionan las distintas especificaciones técnicas de esta familia.

Los equipos en los locales del cliente (CPE), como por ejemplo ONU G-PON ONU, pueden estar parcialmente gestionados por una OMCI, como se especifica en [b-UIT-T G.988]. En la Recomendación UIT-T G.988 se definen las opciones de gestión compartida de estos dispositivos. Tales opciones, así como la gestión del CPE por parte de la OMCI, quedan fuera del alcance de la presente Recomendación.

El protocolo está previsto para dar flexibilidad al modelo de conexión.

- El protocolo permite que tanto el CPE como el ACS inicien el establecimiento de la conexión, evitando así tener que mantener una conexión permanente entre cada CEP y el ACS.
- La interacción funcional entre el ACS y el CPE no debe depender de qué lado haya iniciado el establecimiento de la conexión. En concreto, incluso cuando no se soporta que el ACS inicie la conexión, todas las transacciones iniciadas por el ACS tendrán que poder realizarse en una conexión iniciada por el CPE.
- El protocolo permite que uno o más ACS sirvan a una población de CPE. Un CPE sólo podrá estar asociado a un ACS, mientras que el ACS podrá estar asociado a uno o más proveedores de servicio. Sin embargo, un único dispositivo físico podrá presentar más de un dispositivo CPE lógico, cada uno de los cuales podrá estar asociado a un ACS distinto.
- El protocolo contiene mecanismos para que el CPE descubra al ACS adecuado para un proveedor de servicios dado.
- El protocolo contiene mecanismos que permiten al ACS identificar de manera segura al CPE y asociarlo con un usuario/cliente.

Los procesos que soportan tal asociación también soportan modelos que incorporan la interacción del usuario y modelos plenamente automáticos.

El protocolo permite que el ACS controle y supervise diversos parámetros asociados con un CPE. Los mecanismos previstos para acceder a estos parámetros están diseñados en función de las siguientes premisas:

- CPE distintos pueden tener distintos niveles de capacidad, aplicar diferentes subconjuntos de funcionalidades opcionales. Además, un ACS puede gestionar una gama de distintos tipos de dispositivos que prestan una gama de diferentes servicios. Por consiguiente, un ACS ha de poder descubrir las capacidades de cada CPE concreto.
- Un ACS ha de poder controlar y supervisar la configuración del CPE vigente.
- Además del ACS, otras entidades podrán controlar algunos parámetros de la configuración del CPE (por ejemplo, a través de la autoconfiguración desde LAN). Así, el protocolo ha de permitir que un ACS tenga en cuenta las modificaciones de la configuración del CPE

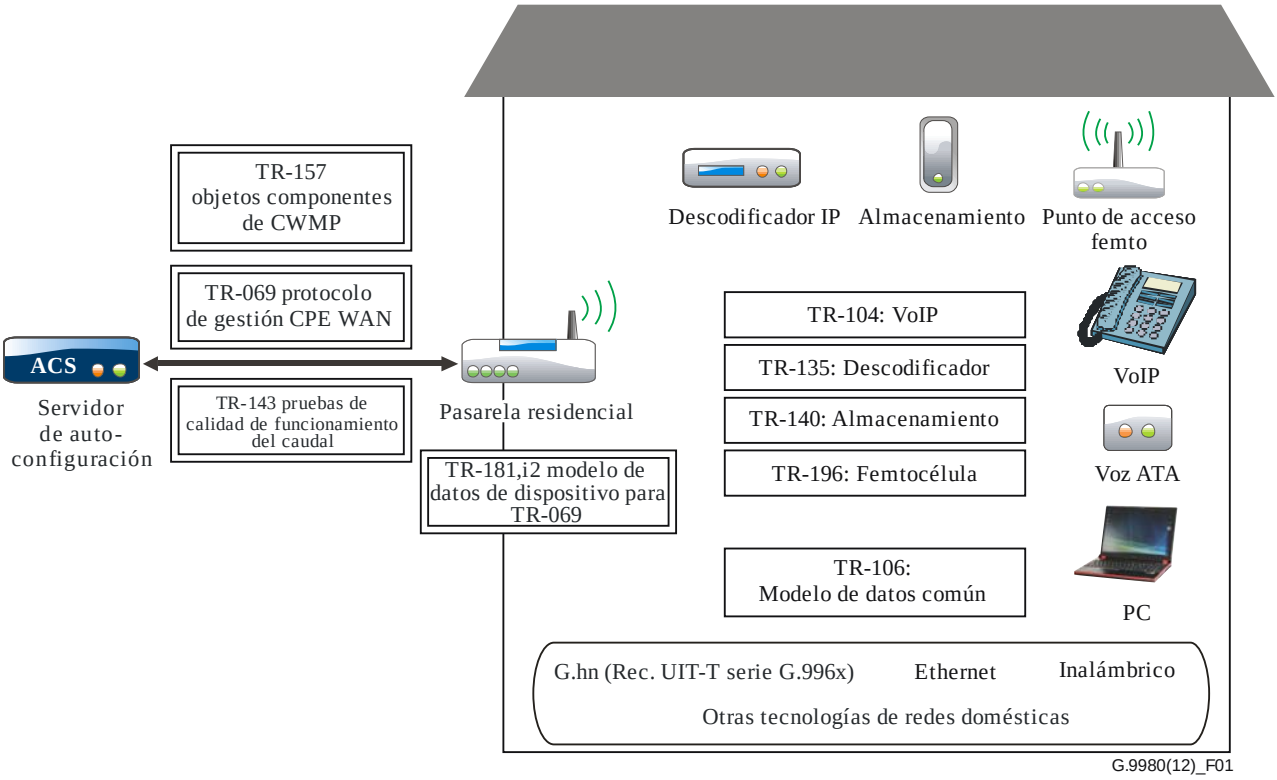
realizadas desde el exterior. Un ACS también deberá poder controlar qué parámetros de la configuración se pueden controlar por otros medios distintos del ACS.

- El protocolo debe permitir la definición de parámetros propios de fabricante y el acceso a los mismos.

Este protocolo pretende minimizar la complejidad de aplicación, dando al mismo tiempo flexibilidad al equilibrio entre complejidad y funcionalidad. El protocolo incorpora una serie de componentes opcionales que entran en juego sólo si se necesita una funcionalidad específica. El protocolo incorpora las normas existentes, cuando procede, permitiendo así utilizar aplicaciones comercializadas.

El protocolo es independiente de la red de acceso subyacente.

Este protocolo es también extensible. Comprende mecanismos para soportar futuras ampliaciones de la norma, así como mecanismos explícitos para las ampliaciones específicas del fabricante.



Los informes técnicos del Foro de la banda ancha para CWMP y modelos de datos (véanse las cláusulas 6.1 y 6.2) aparecen en los rectángulos con dobles líneas.
Los informes técnicos del Foro de la Banda Ancha que definen modelos de datos de servicio (véase la cláusula 6.2.1) aparecen en los rectángulos con una sola línea.

Figura 1 – Protocolo de gestión CPE WAN y especificaciones técnicas conexas

Todo protocolo que describa la configuración a distancia o la modificación de software/firmware del CPE debe proporcionar las capacidades necesarias para cumplir el conjunto de leyes, normativas y políticas nacionales y regionales aplicables. Algunas leyes, normativas y políticas nacionales y regionales específicas pueden requerir la aplicación de mecanismos que garanticen el apoyo explícito del cliente por medio de autorizaciones *opt-in* antes de iniciar cualquier procedimiento a distancia en el CPE. Los implementadores y usuarios del protocolo de gestión CPE WAN (*CPE WAN management protocol-CWMP*) descrito deberán cumplir el conjunto de leyes, normativas y políticas nacionales y regionales aplicables.

Los implementadores y usuarios de todas las Recomendaciones del UIT-T, incluida la Rec. UIT-T G.9980 y sus técnicas subyacentes, deberán cumplir el conjunto de leyes, normativas y políticas nacionales y regionales aplicables.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[BBF TR-069] Broadband Forum TR-069 Amendment 2 (2007), *CPE WAN Management Protocol v1.1*.
<http://www.broadband-forum.org/technical/download/TR-069_Amendment-2.pdf>

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

[BBF TR-106] Broadband Forum TR-106 Amendment 4 (2010), *Data Model Template for TR-069-Enabled Devices*.
<http://www.broadband-forum.org/technical/download/TR-106_Amendment-4.pdf>

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

[BBF TR-140] Broadband Forum TR-140 (2007), *TR-069 Data Model for Storage Service Enabled Devices*.
<http://www.broadband-forum.org/technical/download/TR-140_Issue1.1.pdf>

[BBF TR-143] Broadband Forum TR-143 Corrigendum 1 (2008), *Enabling Network Throughput Performance Tests and Statistical Monitoring*.
<http://www.broadband-forum.org/technical/download/TR-143_Corrigendum-1.pdf>

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

[BBF TR-181 Issue 2] Broadband Forum TR-181 Issue 2 (2010), *Device Data Model for TR-069*.
<http://www.broadband-forum.org/technical/download/TR-181_Issue-2.pdf>

[BBF TR-196] Broadband Forum TR-196 (2009), *Femto Access Point Service Data Model*.
<http://www.broadband-forum.org/technical/download/TR-196.pdf>

3 Definiciones

3.1 Términos definidos en otros documentos

En esta Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 equipo en los locales del cliente (CPE, *customer premises equipment*) [b-UIT-T Y.101]: Sistema de usuario extremo que comprende elementos de red privada que conectan las aplicaciones del cliente a la línea de acceso.

3.1.2 informe técnico (TR, *technical report*): Especificación técnica aprobada del Foro de la Banda Ancha, de conformidad con [b-BBF01].

3.2 Términos definidos en esta Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 gestión a distancia: Gestión del CPE por parte del proveedor de servicios a través de una WAN

4 Abreviaturas y acrónimos

En esta Recomendación se emplean las siguientes abreviaturas y acrónimos:

ACS Servidor de autoconfiguración (*auto-configuration server*)

CPE Equipo en los locales del cliente (*customer premises equipment*)

CWMP Protocolo de gestión CPE WAN (*CPE WAN management protocolo*)

DDF Dúplex por división de frecuencia

FAP Punto de acceso femto (*Femto access point*)

TVIP Televisión por protocolo Internet

NAS Almacenamiento anexo a la red (*network attached storage*)

NAT Traducción de direcciones de red (*network address translation*)

PVR Grabador de video personal (*personal video recorder*)

QoE Calidad percibida (*quality of experience*)

QoS Calidad de servicio (*quality of service*)

RG Pasarela residencial (*residential gateway*)

RPC Llamada de procedimiento a distancia (*remote procedure call*)

SIP Protocolo de inicio de sesión (*session initiation protocol*)

SSL/TLS Capa de zócalos segura/Seguridad de capa de transporte (*secure socket layer/transport layer security*)

STB Descodificador (*set-top box*)

TR Informe técnico (*technical report*)

UMTS Sistema de telecomunicaciones móviles universal (*universal mobile telecommunication system)*

VOIP Voz por el protocolo Internet (*voice over internet protocolo*)

WAN Red de área extensa (*wide area network*)

5 Convenios

En la presente Recomendación no se utilizan notaciones, estilos, presentaciones, etc. particulares.

6 Gestión a distancia del CPE por redes de banda ancha

En esta cláusula se enumeran los elementos del protocolo de gestión CPE WAN (véase la cláusula 6.1) y los modelos de datos para dispositivos específicos (véase la cláusula 6.2), que constituyen la parte normativa de esta Recomendación.

6.1 Elementos del protocolo de gestión CPE WAN

Los requisitos del protocolo de gestión CPE WAN se definen en [BBF TR-069].

Es bien sabido que las políticas del proveedor de servicios o los reglamentos locales pueden restringir la utilización de la gestión CPE WAN y sus especificaciones asociadas por motivos de privacidad y seguridad. Estas restricciones pueden implicar uno o más de los siguientes elementos:

- las comunicaciones CWMP sólo se efectuarán a través de canales SSL/TLS mutuamente autentificados;
- restricciones relativas al tipo de CPE que puede gestionarse a distancia;
- exigencia de que el abonado dé su consentimiento individual explícito necesariamente antes de que se establezca la gestión a distancia para extraer información sobre la configuración del CPE;
- exigencia de solicitar el consentimiento explícito del abonado obligatoriamente antes de iniciar la modificación de la configuración del CPE;
- otros.

6.1.1 TR-069: protocolo de gestión CPE WAN (CWMP)

[BBF TR-069] está previsto para la comunicación entre un CPE y un servidor de autoconfiguración (ACS, *auto-configuration server*). El protocolo de gestión CPE WAN define un mecanismo que comprende la autoconfiguración segura de un CPE e incorpora otras funciones de gestión del CPE en un marco común.

Para la equiparación técnica de la Recomendación con [BBF TR-069], esta cláusula (enmarcada) se estructura de conformidad con [BBF TR-069]. Los números de los títulos son los de las cláusulas de [BBF TR-069].

1 Introducción

Los requisitos genéricos CWMP de los métodos del protocolo de gestión pueden aplicarse a cualquier CPE con capacidad CWMP.

Desde una perspectiva puramente funcional, CWMP soporta diversas funcionalidades para gestionar una serie de CPE, incluidas las siguientes capacidades primarias:

- autoconfiguración y configuración de servicio dinámica;
- gestión de imágenes de software/firmware;
- supervisión de estado y calidad de funcionamiento;
- diagnóstico.

1.2 Posicionamiento en la arquitectura de extremo a extremo

El ACS es un servidor que reside en la red y gestiona dispositivos en los locales del cliente a través del protocolo de gestión CPE WAN. El CWMP es independiente del medio de acceso específico utilizado por el proveedor de servicio, aunque depende de que se haya establecido una conexión en la capa IP.

1.3 Objetivos de seguridad

Está previsto que la seguridad CWMP pueda adaptarse a una gama de CPE, desde el más simple al más sofisticado. Los objetivos de seguridad son los siguientes:

- impedir la intervención no autorizada en las funciones de gestión de un CPE o un ACS, o en las transacciones que se realizan entre un CPE y un ACS;
- otorgar confidencialidad a las transacciones que se realizan entre el CPE y el ACS;
- permitir la autentificación adecuada para cada tipo de transacción;
- impedir el robo del servicio.

2 Arquitectura

2.1 Componentes del protocolo

Las aplicaciones CWMP se definen por encima de una pila que respectivamente comprende los métodos RPC, SOAP, HTTP, SSL/TLS, TCP e IP, como se especifica en [BBF TR-069].

2.2 Mecanismos de seguridad

Los mecanismos disponibles para CWMP incluyen SSL/TLS y secretos compartidos HTTP.

2.3 Componentes arquitectónicos

El CWMP está diseñado alrededor de la idea fundamental de determinar y extraer a distancia variables nombradas, creando y eliminando objetos distantes, e invocando un pequeño conjunto de métodos predefinidos. Esta es la base para soportar el autodescubrimiento, las notificaciones y los mecanismos de transferencia de ficheros.

Los modelos de información CWMP normalizados se especifican en la cláusula 6.2 de la presente Recomendación. El modelo de información también puede soportar ampliaciones propias del fabricante.

Las sesiones CWMP pueden estar iniciadas por el ACS o el CPE. Cuando un CPE inicia la sesión, puede contactar con un ACS para obtener parte de su configuración o casi toda ella, incluida posiblemente la carga de su firmware.

3 Procedimientos y requisitos

3.1 Descubrimiento ACS

El CPE puede llevar en su configuración una URL ACS por defecto. El CPE también puede aprender la identidad del ACS gracias a la configuración local o a una opción DHCP. DHCP también puede dar el código de configuración, que utilizará el CPE al identificarse ante el ACS. El ACS puede modificar la URL que utilizará el CPE para posteriores contactos con otros ACS.

Si la URL ACS especifica HTTPS, el CPE ha de utilizar SSL/TLS para establecer la sesión con el ACS.

3.2 Establecimiento de la conexión

El CPE puede iniciar una sesión con el ACS cuando se inicializa, cuando llega un informe periódico o planificado configurado por el ACS, cuando necesita enviar un valor configurado o una notificación de cambio de estado, o para recuperar una sesión terminada prematuramente. El CPE no mantiene una sesión abierta cuando no tiene información que intercambiar con el ACS.

El ACS podrá indirectamente iniciar una sesión con el CPE a través de una petición HTTP para que el CPE abra una sesión con el ACS.

3.3 Utilización de SSL/TLS y TCP

Se recomienda utilizar SSL/TLS para todas las sesiones, aunque no es obligatorio. Si se utiliza SSL/TLS, el CPE habrá de autentificar al ACS mediante autentificación por certificado. También es conveniente que el ACS autentifique al CPE.

En la cláusula 3 se describen los detalles de la codificación de mensajes (SOAP), el establecimiento de sesión, el funcionamiento y la terminación, y las operaciones de transferencia de ficheros. Se definen otros requisitos de autentificación, incluida la autentificación HTTP ACS del CPE, si no se ha autentificado ya al CPE durante la negociación SSL/TLS.

Anexo A – Métodos RPC

Los tipos de datos y mensajes definidos para las llamadas de procedimiento a distancia (RPC) CWMP se definen en el Anexo A de [BBF TR-069]. Al igual que la sintaxis de cada mensaje y su respuesta, en esa cláusula se especifican todas las restricciones de comportamiento especiales que pueden aplicarse al ACS o el CPE.

En esta cláusula se incluye un esquema XML genérico.

Anexo B – Eliminado

(Eliminado de esta edición de TR-069.)

Anexo C – Comprobantes firmados

Anexo D – Gestión de la identidad en la web

Anexo E – Formato de lote firmado

Anexo F – Asociación dispositivo-pasarela

CWMP puede utilizarse para gestionar a distancia dispositivos del CPE conectados por una LAN a través de una pasarela. Cuando el ACS gestiona tanto el dispositivo como la pasarela a través de la cual está conectado el dispositivo, puede resultar útil al ACS poder determinar la identidad de esa pasarela.

Los procedimientos definidos en este anexo permiten al ACS determinar la identidad de la pasarela a través de la cual está conectado un dispositivo concreto. El mecanismo depende de la utilización de DHCP tanto por el dispositivo como por la pasarela.

En un ejemplo práctico, un ACS que establece la QoS de un servicio concreto podrá necesitar configurar tanto el dispositivo como la pasarela a través de la cual está conectado. Para esto último, el ACS necesitará determinar la identidad de esa pasarela.

Para soportar esta característica, se supone que tanto el dispositivo como la pasarela se gestionarán con el CWMP, y que ambos estarán gestionados por el mismo ACS o por ACS distintos que estén adecuadamente acoplados.

Anexo G – Petición de conexión por pasarela NAT

La traducción de direcciones de red (NAT, Network address translation) en una pasarela aísla el espacio de dirección IP en el lado LAN del espacio IP en el lado WAN. El CPE tras la pasarela NAT puede emplear los métodos definidos anteriormente para iniciar sesiones, pero los procedimientos definidos en este anexo son necesarios para que el ACS pueda pedir una conexión al CPE. La pasarela NAT no necesita soportar CWMP.

6.1.2 Autoconfiguración y configuración de servicio dinámica

El CWMP permite que un ACS configure un CPE o una serie de CPE en función de un conjunto de criterios.

El mecanismo de configuración permite configurar el CPE en el momento de la conexión inicial a una red de acceso de banda ancha y la posibilidad de reconfigurarlo en cualquier momento posterior. Esto incluye el soporte de la reconfiguración asíncrona del CPE iniciada por el ACS.

Los mecanismos de identificación incluidos en el protocolo permiten la configuración del CPE basada en los requisitos de cada CPE específico o en criterios colectivos, como el fabricante, el modelo o la versión del software del CPE.

Este protocolo también ofrece herramientas opcionales para gestionar componentes de aplicaciones o servicios opcionales específicos del CPE para los que se necesita un nivel de seguridad adicional, como los que se utilizan para realizar pagos.

El mecanismo de configuración permite la ampliación futura directa a fin de poder configurar servicios y capacidades que aún no se incluyen en esta versión.

6.1.3 Gestión de imágenes de software/firmware

El CWMP establece un marco para gestionar la descarga de ficheros de imagen de software/firmware del CPE. El protocolo ofrece mecanismos para la identificación de versión, el inicio de descarga de ficheros (descargas iniciadas por el ACS y descargas iniciadas por el CPE opcionales) y la notificación de éxito o fracaso de la descarga de un fichero por parte del ACS.

6.1.4 Supervisión de estado y calidad de funcionamiento

El CWMP soporta que un CPE facilite información que el ACS puede utilizar para supervisar el estado y las estadísticas de calidad de funcionamiento del CPE. También define un conjunto de mecanismos que permiten al CPE notificar activamente al ACS las modificaciones de su estado. [BBF TR-143] facilita las pruebas de caudal para poder evaluar la percepción de los abonados en términos de velocidad de banda ancha.

6.1.5 Diagnóstico

El CWMP soporta que el CPE facilite información que el ACS puede utilizar para realizar un diagnóstico y resolver problemas de conectividad o servicio. También soporta la capacidad de ejecutar pruebas de diagnóstico definidas.

6.1.6 Seguridad

El CWMP está diseñado para dar un alto grado de seguridad. El modelo de seguridad también está previsto para ser adaptable. Prevé una seguridad básica para acomodar los CPE menos robustos, mientras que da una mayor seguridad para los CPE que pueden soportar mecanismos de seguridad más avanzados. Los objetivos de seguridad del protocolo de gestión CPE WAN son los siguientes:

- impedir la intervención no autorizada en las funciones de gestión de un CPE o un ACS, o en las transacciones que tienen lugar entre el CPE y el ACS;
- permitir una fuerte autentificación mutua del CPE y el ACS;
- aportar confidencialidad a las transacciones entre el CPE y el ACS;
- permitir la autentificación adecuada a cada tipo de transacción;
- impedir el robo de servicio.

6.2 Modelos de datos

Un concepto clave del CWMP es el modelo de datos. Un modelo de datos determina los objetos y parámetros sobre los que se puede actuar con las llamadas de método genérico CMWP. Estos objetos y parámetros exponen la configuración, el diagnóstico o los datos de estado de diversos tipos de servicios y dispositivos. Por ejemplo, el modelo de datos para un dispositivo VoIP expone parámetros relacionados con la configuración SIP, entre otras capacidades VoIP. Los modelos de datos definen un superconjunto de funcionalidades que pueden gestionarse en un dispositivo o servicio concreto: los dispositivos aplican las partes de los modelos de datos pertinentes para su funcionalidad específica.

Los requisitos de los modelos de datos de gestión CPE WAN se definen en [BBF TR-106], [BBF TR-143], [BBF TR-157], [BBF TR-181 Issue 2], [BBF TR-104], [BBF TR-135], [BBF TR-140] y [BBF TR-196].

En [BBF TR-106] se define la información genérica para definir los modelos de datos CWMP, incluidos los requisitos de jerarquía, las normas de obsolescencia y depreciación, los tipos de datos y el esquema CWMP-DM XML, que se utiliza para definir todos los modelos de datos.

Los CPE, como las pasarelas residenciales (RG, *residential gateways*), los descodificadores (STB, *set-top boxes*) y los dispositivos de almacenamiento anexo a la red (NAS, *network attached storage*), se configuran y gestionan utilizando un conjunto común de parámetros, que hacen que el ACS de red pueda reconocer el dispositivo y permiten la autoconfiguración y la gestión continua.

Los Informes técnicos donde se definen estos parámetros son los siguientes:

- [BBF TR-181 Issue 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*.

Los Informes técnicos donde se definen los modelos de datos de servicio son los siguientes:

- [BBF TR-104]: *DSLHome provisioning parameters for VOIP CPE*
- [BBF TR-135]: *Data model for a TR-069 enabled set-top box (STB)*
- [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 Issue 2: *Device data model for TR-069* (Modelo de datos de dispositivo para TR-069)

En [BBF TR-181 Issue 2] se define la versión 2 del modelo de datos de dispositivo de TR-069. El modelo de datos se aplica a todos los dispositivos con capacidad TR-069, incluidos los dispositivos extremos, los dispositivos de pasarela Internet y otros dispositivos de infraestructura de red. Representa la evolución de la próxima generación que sustituye tanto a [b-BBF TR-181 Issue 1] (no incluido en la Recomendación) como a [b-BBF TR-098] Enmienda 2 (no incluido en la Recomendación). Las instalaciones anteriores podrán seguir utilizando los modelos de datos InternetGatewayDevice:1 y Device:1, que siguen siendo válidos.

NOTA – La evolución a Device:2 respondió a la necesidad de resolver ciertas limitaciones fundamentales del modelo de datos InternetGatewayDevice:1, que demostró ser inflexible y causó problemas para la representación de configuraciones de dispositivo complejas. Sin embargo, al definir este modelo de datos de la próxima generación, se ha tenido cuidado de garantizar que se conservan todas las funcionalidades de InternetGatewayDevice:1 y Device:1.

El modelo de datos Device:2, definido en [BBF TR-181 Issue 2], comprende un conjunto de objetos de datos que abarcan elementos tales como la información básica de dispositivo, la configuración horaria, la configuración de la interfaz de red y la pila de protocolo, la gestión del encaminamiento y el puenteo, y las pruebas de diagnóstico. También define un perfil básico que especifica el nivel mínimo de soporte del modelo de datos.

La piedra angular del modelo de datos Device:2 es el mecanismo de apilamiento de interfaz. Las interfaces de red y las capas de protocolo se modelan como objetos de datos independientes que pueden apilarse, unas encima de otras, para formar cualquier configuración que el dispositivo pueda soportar.

Para la equiparación técnica de la Recomendación con [BBF TR-181 Issue 2], esta cláusula (enmarcada) se estructura de conformidad con [BBF TR-181 Issue 2]. Los números de los títulos denotan los números de las cláusulas de [BBF TR-181 Issue 2].

4 Arquitectura

4.1 Capas de interfaz

En este Informe Técnico se modelan las interfaces de red y las capas de protocolo como objetos de datos independientes, generalmente denominados objetos de interfaz (o interfaces). Los objetos de interfaz pueden apilarse, unos encima de otros, utilizando referencias de trayecto para definir dinámicamente las relaciones entre las interfaces.

El objeto de interfaz y la pila de interfaz son conceptos inspirados en [b-IETF RFC 2863].

Dentro del modelo de datos Device:2, los objetos de interfaz están arbitrariamente restringidos a definiciones que funcionan en la capa de red IP o por debajo de ella (es decir, las capas 1 a 3 del modelo OSI). Sin embargo, se PUEDEN definir objetos de interfaz propios del fabricante que quedan fuera de este alcance restringido.

4.2 Objetos de interfaz

Un objeto de interfaz es un tipo de interfaz de red o capa de protocolo. Cada tipo de interfaz se modela en función de un cuadro del modelo de datos Device:2, donde cada fila corresponde a una instancia de interfaz (por ejemplo, IP.Interface.{i} para las interfaces IP).

Cada objeto de interfaz contiene un núcleo de parámetros y objetos, que se utiliza como modelo para definir los objetos de interfaz del modelo de datos. Los objetos de interfaz también pueden contener otros parámetros y subobjetos específicos del tipo de interfaz.

4.3 Cuadro InterfaceStack

Aunque la pila de interfaz puede atravesarse por los parámetros LowerLayers (como se explica en la cláusula 4.2.1 Capas inferiores), se facilita otro mecanismo que ayuda a visualizar las relaciones generales en la pila y acceder rápidamente a los objetos que están en ella.

El cuadro InterfaceStack es un objeto del modelo de datos Device:2, concretamente Device.InterfaceStack.{i}. Se trata de un cuadro de sólo lectura cuyas filas autogenera el CPE en función de las relaciones vigentes, que se configuran entre los objetos de interfaz (a través de cada parámetro LowerLayers de la instancia de interfaz). Cada fila del cuadro representa un "enlace" entre un objeto de interfaz de capa superior (indicado por su parámetro HigherLayer) y un objeto de interfaz de capa inferior (indicado por su parámetro LowerLayer). Esto significa que los parámetros HigherLayer y LowerLayer de una fila del cuadro InterfaceStack siempre serán distintos de cero.

NOTA – Por consiguiente, las instancias de interfaz perdidas no se representarán en el cuadro InterfaceStack. También es probable que múltiples grupos dispares de objetos de interfaz apilados coexistan dentro del cuadro (por ejemplo, cada interfaz IP será la raíz de un grupo dispar. Los "fragmentos" no utilizados, por ejemplo, un canal DSL secundario con PVC ATM configurado que no está anexo a nada por encima, permanecerán si siguen interconectados. Por último, podrá haber "fragmentos" parcialmente configurados cuando se cree la pila de interfaz).

5 Definiciones de parámetro

La definición normativa del modelo de datos Device:2 se divide entre diversos documentos *DM Instance* (véase el Anexo A a TR-069). En el Cuadro 3 se enumeran las versiones del modelo de datos Device:2 y las *DM Instances* definidas en el momento de preparación del presente documento. También se indican los correspondientes Informes Técnicos y se facilitan enlaces a los ficheros XML y HTML asociados. En el documento TR-181i2 XML se define el modelo Device:2 mismo y se importan otros componentes de los demás documentos XML enumerados. El documento TR-181i2 HTML es un informe generado a partir de los ficheros XML, y expone todo el modelo de datos Device:2 en formato legible para las personas.

Anexo A – Puenteo y puesta en cola

En este anexo se define el modelo de puenteo y puesta en cola (la clasificación de paquetes, la puesta en cola y la programación, y el puenteo), la correspondencia de QoS de capa 2/3 por defecto, las definiciones URN para aplicaciones y cuadros de flujo (Aplicación ProtocolIdentifier, Tipo de Flujo y Flujo TypeParameters).

6.2.2 TR-157: *Component objects for CWMP* (Objetos componentes de CWMP)

En [BBF TR-157] se definen los objetos componentes que utilizarán todos los modelos de datos raíz en los dispositivos gestionados con CWMP. Un objeto componente se define como un objeto y los parámetros que contiene para su utilización en cualquier modelo de datos raíz CWMP aplicable. Los objetos pueden residir en el nivel más alto o en un nivel de subobjeto conveniente.

Para soportar la funcionalidad definida en [BBF TR-157], en el Cuadro 1 de [BBF TR-157] se especifica una extensión del modelo de datos Device y del modelo de datos InternetGatewayDevice. Para el modelo de datos Device, esta extensión se considera parte de Device:1.4 (versión 1.4 del modelo de datos Device), que amplía la versión 1.3 del modelo de datos Device definido en TR-157 Issue 1. Para el modelo de datos InternetGatewayDevice, esta extensión se considera parte de InternetGatewayDevice:1.6 (versión 1.6 del modelo de datos InternetGatewayDevice), que amplía la versión 1.5 del modelo de datos InternetGatewayDevice definido en TR-157 Issue 1.

6.2.3 TR-143: *Enabling network throughput performance tests and statistical monitoring* (Activación de las pruebas de calidad de funcionamiento de caudal de red y supervisión estadística)

En [BBF TR-143] se define una serie de pruebas de supervisión activa que pueden utilizar los proveedores de servicios de red para controlar y/o diagnosticar el estado de sus trayectos de red de banda ancha que dan servicio a abonados con CPE compatibles con TR-069. La supervisión activa soporta tanto el diagnóstico iniciado por la red como el diagnóstico iniciado por el CPE para la supervisión y caracterización de los trayectos de servicio de manera continua o puntual. Estas herramientas genéricas ofrecen una plataforma de validación de los objetivos de QoS y los acuerdos de nivel de servicio.

Para la equiparación técnica de la Recomendación con [BBF TR-143], esta cláusula (enmarcada) se estructura de conformidad con [BBF TR-143]. Los números de los títulos denotan los números de las cláusulas de [BBF TR-143].

4 Supervisión activa

La supervisión activa consiste en introducir tráfico TCP o UDP ficticio en una red, en este caso una red de acceso de banda ancha, con CPE compatible con TR-069 a fin de evaluar la QoS. El tráfico de prueba puede originarse en la red o en el CPE que soporta [BBF TR-143].

5 Definiciones de parámetro

En la cláusula 5 se define la sintaxis y la semántica específicas de los parámetros de un servicio VoIP. Los parámetros se agrupan en lotes, que a su vez se reúnen en perfiles para las diversas aplicaciones de la cláusula 7.

6 Requisitos de notificación

7 Definiciones de perfil

7.1 Notación

7.2 Perfil de descarga

El perfil de descarga configura el CPE para ejecutar una prueba de descarga y registrar los resultados. Como parte del perfil pueden configurarse la prioridad Ethernet y los campos DSCP.

7.3 Perfil TCP de descarga

El perfil TCP de descarga amplia el perfil de descarga para registrar los tiempos de petición y respuesta TCP, cuando la descarga emplea TCP.

7.4 Perfil de telecarga

El perfil de telecarga configura el CPE para ejecutar una prueba de telecarga y registrar los resultados. Como parte del perfil pueden configurarse la prioridad Ethernet y los campos DSCP.

7.5 Perfil TCP de telecarga

El perfil TCP de telecarga amplía el perfil de telecarga para registrar los tiempos de petición y respuesta TCP, cuando la telecarga emplea TCP.

7.6 Perfil eco UDP

El perfil eco UDP configura el CPE para ejecutar una prueba de eco UDP.

7.7 Perfil ecoplus UDP

El perfil ecoplus UDP amplía el perfil eco UDP añadiendo un parámetro que habilita ecoplus.

Apéndice A – Teoría de las operaciones

A.1 Ecoplus UDP

La característica ecoplus UDP es una aplicación de la función eco ICMP ordinaria. Permite mediciones en uno o dos sentidos de la calidad de funcionamiento de los paquetes. Se procesa de acuerdo con la prioridad DSCP o Ethernet marcada, lo que permite una mejor medición de la calidad de funcionamiento desde la perspectiva del abonado.

A.2 Diagnóstico de descarga utilizando el transporte FTP

Esta prueba consiste en la transferencia FTP de un fichero de prueba desde un servidor de prueba a un CPE. Se registran el número de bytes recibidos y los diversos sellos de tiempo que permiten evaluar la calidad de funcionamiento de descarga.

A.3 Diagnóstico de telecarga utilizando el transporte FTP

Estas pruebas son similares a la prueba de descarga.

A.4 Diagnóstico de descarga utilizando el transporte HTTP

Estas pruebas son similares a la correspondiente prueba de descarga FTP.

A.5 Diagnóstico de telecarga utilizando el transporte HTTP

Estas pruebas son similares a la correspondiente prueba de telecarga FTP.

6.2.4 TR-104: *DSLHome provisioning parameters for VOIP CPE* (Parámetros de configuración de DSL doméstica para CPE VoIP)

En [BBF TR-104] se define el modelo de datos para la configuración de un dispositivo CPE de voz por el protocolo Internet (VoIP) por parte de un servidor de autoconfiguración (ACS) utilizando el mecanismo definido en [BBF TR-069].

Para la equiparación técnica de la Recomendación con [BBF TR-104], esta cláusula (enmarcada) se estructura de conformidad con [BBF TR-104]. Los números de los títulos denotan los números de las cláusulas de [BBF TR-104].

1 Introducción

TR-104

- acomoda dispositivos VoIP que están incorporados en un dispositivo de pasarela Internet o que son independientes y autónomos;
- acomoda dispositivos VoIP que soportan múltiples servicios VoIP diferentes, cada uno de ellos posiblemente con múltiples líneas distintas;
- soporta la utilización de los protocolos de señalización SIP y MGCP;
- soporta diversos tipos de CPE VoIP, incluidos los puntos extremos VoIP, los intermediarios SIP externos y los agentes de usuario adosados SIP.

2 Arquitectura

[BBF TR-104] define un VoiceService como contenedor asociado con los objetos de configuración del CPE VoIP. En el contexto de [BBF TR-106], el objeto VoiceService definido en [BBF TR-104] es un objeto de servicio. Cada dispositivo CPE podrá contener cero o más instancias del objeto VoiceService. La presencia de más de un objeto VoiceService podrá convenir, por ejemplo, cuando el dispositivo CPE sirve de intermediario de gestión para otros CPE VoIP no compatibles con TR-069. Por ejemplo, un dispositivo de pasarela Internet podrá ser el intermediario de gestión de uno o más teléfonos VoIP no compatibles con TR-069.

Cada objeto VoiceService contiene uno o más objetos VoiceProfile. Un objeto VoiceProfile corresponde a una o más líneas telefónicas que comparten la misma configuración básica. Cada objeto VoiceProfile contiene uno o más objetos de línea, cada uno de los cuales representa una única línea telefónica concreta.

El objeto VoiceProfile permite a un dispositivo de voz multilínea agrupar líneas con características comunes dentro de un único perfil. Al poder haber más de un VoiceProfile, el modelo permite a un dispositivo de voz multilínea tener grupos de líneas con configuraciones diferentes los unos de los otros. Una posible utilización de esta estructura puede ser la asociación de diferentes grupos de líneas con proveedores de servicio completamente independientes, cada uno con sus propios servidores VoIP y requisitos de configuración. Otra posibilidad puede ser distinguir entre distintos niveles de servicio de un único proveedor de servicios. Por ejemplo, un único dispositivo puede facilitar algunas líneas de consumidor más otras líneas de empresa, cada una de ellas asociada a un VoiceProfile diferente, que se distinguen por sus características de calidad.

3 Modelo de datos VoiceService versión 1.0

En la cláusula 3 se definen la sintaxis y la semántica específicas de los parámetros de un servicio VoIP. Los parámetros se agrupan en lotes, que a su vez se reúnen en perfiles para las diversas aplicaciones de la cláusula 4.

4 Definiciones de perfil

4.1 Notación

4.2 Perfil Endpoint

El perfil de punto extremo reúne parámetros adecuados para un punto extremo VoIP en varios grupos. El grupo de capacidades comprende límites para la elección del códec y la velocidad binaria, el número de sesiones simultáneas, los protocolos de señalización disponibles, la detección de fax y módem y el traspaso, el plan de numeración, y la personalización de tono, timbre y correspondencia de las teclas. El grupo de perfil de voz se subdivide en varios grupos más pequeños encargado de RTP, el estado de la línea, los parámetros del códec utilizado, el temporizador de sesión y las direcciones de extremo distante y los contadores PM.

Los tres perfiles siguientes contienen información similar, pero su forma está adaptada a cada uno de los protocolos de señalización.

4.3 Perfil SIPEndpoint

El perfil de punto extremo SIP amplia el perfil de punto extremo con parámetros específicos importantes para la señalización SIP, y en concreto incluye el intermediario SIP, el registro y la información de autentificación de abonado.

4.4 Perfil MGCPEndpoint

El perfil de punto extremo MGCP amplía el perfil de punto extremo con parámetros importantes para la señalización MGCP, y en concreto incluye la información de identidad y registro del agente y del usuario local.

4.5 Perfil H323Endpoint

El perfil de punto extremo H323 amplía el perfil de punto extremo con parámetros importantes para la señalización H.323, y en concreto incluye la información de identidad y registro del controlador de pasarela y del usuario local.

4.6 Perfil TAEndpoint

El perfil de punto extremo TA está previsto para que lo utilice un punto extremo terminal. Amplía el perfil de punto extremo básico con las listas de los puertos físicos asociados y sus identificadores, que comparten los mismos parámetros.

Apéndice A – Acciones de facilidad

En el Apéndice A se definen las diversas acciones de señalización VoIP que se pueden activar mediante prefijos del plan de marcación del abonado y las teclas del teléfono, por ejemplo, activación o desactivación de características tales como el reenvío de llamada, la identificación de línea llamante, el timbre selectivo, etc. Otras acciones incluyen, por ejemplo, la conmutación entre múltiples llamadas en espera.

Apéndice B – Descarga de ficheros de tono y timbre

En el Apéndice B se detalla la utilización de la característica descarga de ficheros TR-069 específicamente para la descarga de tonos y timbres VoIP.

6.2.5 TR-135: *Data model for a TR-069 enabled set-top box* (Modelo de datos para un descodificador con capacidad TR-069)

En [BBF TR-135] se especifica la gestión a distancia de la funcionalidad de televisión digital (TVIP o radiodifusión) en los descodificadores a través del CWMP. El acceso a la red y el grabador de video personal (PVR) se gestiona desde una plataforma de servicio TVIP y queda fuera del alcance del ACS. El ACS puede realizar parte de la configuración inicial de un descodificador nuevo, pero sus principales funciones son la configuración de los parámetros del descodificador para la gestión de problemas y la recopilación de estadísticas para la supervisión de la QoS /QoE. Por consiguiente, la mayoría de parámetros definidos en [BBF TR-135] son de sólo lectura para el ACS.

NOTA – [BBF TR-135] define el modelo de datos para describir un dispositivo descodificador, así como las normas relativas a la notificación de cambio del valor de un parámetro. Se trata de los perfiles de modelo de datos normalizados que normalmente gestionarán a distancia un dispositivo de este tipo.

Para la equiparación técnica de la Recomendación con [BBF TR-135], esta cláusula (enmarcada) se estructura de conformidad con [BBF TR-135]. Los números de los títulos denotan los números de las cláusulas de [BBF TR-135].

5 Arquitectura

Un descodificador se modela como un conjunto de funciones y capacidades, la mayoría de las cuales son opcionales y pueden estar presentes en más de una instancia. En la siguiente cláusula 7 se definen los perfiles de los componentes distintos de la infraestructura básica del descodificador.

6 Definiciones de parámetros

En la cláusula 6 se definen la sintaxis y la semántica específicas de los parámetros de un descodificador. Los parámetros se agrupan en lotes, que a su vez se reúnen en perfiles para las diversas aplicaciones de la cláusula 7.

7 Definiciones de perfil

7.1 Notación

7.2 Perfil básico

El perfil básico presenta información de sólo lectura sobre las capacidades del descodificador, incluidas las normas que soporta, el número máximo de trenes de distintos tipos que puede soportar. Los parámetros escribibles se limitan al control de silenciamiento y la elección de idioma para los trenes de audio y subtitulado.

7.3 Perfil PVR

El perfil de grabador de video personal devuelve el estado de una posible aplicación PVR. Se soporta el almacenamiento PVR mediante una referencia a storageService, definido en [BBF TR-140].

7.4 Perfil DTT

El perfil de televisión digital terrenal contiene los parámetros de configuración para la radiodifusión de video digital, así como parámetros de mantenimiento de sólo lectura y parámetros PM.

7.5 Perfil básico IPTV

El perfil TVIP contiene los parámetros de memoria tampón de QoS de lectura-escritura y una serie de parámetros de solo lectura que informan de las capacidades del descodificador y de su estado con respecto a las características de TVIP.

7.6 Perfil RTCP

El perfil de protocolo de control en tiempo real contiene el control de configuración simple (activar, configuración de intervalo) y un informe de estado.

7.7 Perfil RTP AVPF

El perfil de retroalimentación en tiempo real RTP configura la característica de retroalimentación RTP en tiempo real e informa sobre su estado vigente.

7.8 Perfil IPTV home network

El perfil de red doméstica TVIP informa del estado y las capacidades de las interfaces de red doméstica del descodificador, como se traducen desde el tren del lado WAN.

7.9 Perfil IGMP

El perfil IGMP ofrece un medio de configurar los parámetros IGMP, como el etiquetado VLAN, la robustez y el intervalo de información, así como el estado de sólo lectura y las estadísticas de PM.

7.10 Perfil básico perfmon

El perfil básico PM soporta la configuración de parámetros PM de alto nivel, por ejemplo, activación global, tiempo y tiempos de referencia de intervalo, etc. Remite estadísticas del descodificador en su conjunto, así como estadísticas de alto nivel de los principales componentes en varios niveles, por ejemplo, RTP, MPEG y descodificador de vídeo.

7.11 Perfil EC perfmon

El perfil PM de corrección de errores comunica estadísticas relacionadas con la capacidad de corrección de errores RTP.

7.12 Perfil Video perfmon

El perfil PM de vídeo comunica estadísticas asociadas con la calidad de la reproducción de vídeo.

7.13 Perfil Audio perfmon

El perfil PM de audio comunica estadísticas asociadas con la calidad de la reproducción de audio.

7.14 Perfil Audience stats

El perfil de estadísticas de audiencia recopila las estadísticas de cuenta y tiempo de canal.

7.15 Perfil Analog output

El perfil de salida analógica informa de las capacidades del descodificador para soportar dispositivos externos, como las pantallas de vídeo.

7.16 Perfil Digital output

El perfil de salida digital informa de si se utiliza la protección del contenido digital en gran anchura de banda (HDCP, *high-bandwidth digital content protection*) en una salida de vídeo concreta.

7.17 Perfil CA

El perfil de acceso condicional informa de la existencia del acceso condicional, que se modela mediante un lector de tarjeta inteligente.

7.18 Perfil DRM

El perfil de gestión de derechos digitales presenta parámetros de sólo lectura sobre el estado vigente de los trenes de medios en curso.

Apéndice I – Teoría de las operaciones

En este apéndice se describen un gran número de casos prácticos y se explica de qué manera se emplea el modelo de información del descodificador.

6.2.6 TR-140: *TR-069 data model for storage service enabled devices* (Modelo de datos TR-069 para dispositivos con servicio de almacén)

[BBF TR-140] permite que un ACS gestione un servicio de almacén básico. A continuación se enumeran algunas de las capacidades que puede ofrecer un ACS que utiliza CWMP:

- Configuración básica y configuración durante la activación del servicio (que se explican en [BBF TR-140] y [BBF TR-181 Issue 2]).
- Configuración de credenciales de usuario y acceso privilegiado a ficheros (que se explican en [BBF TR-140] (acceso a carpetas)).
- Extracción del estado del dispositivo (que se explica en [BBF TR-140] (parámetros) y [BBF TR-181 Issue 2]).
- Configuración inalámbrica (por ejemplo, seguridad WEP) para un dispositivo de almacén con acceso Wi-Fi.
- Diagnóstico de red y resolución de problemas, por ejemplo, conectividad de red al dispositivo de pasarela Internet y a Internet (que se explica en TR-181 Issue 2 (parámetros de conexión)).

NOTA – No todas estas capacidades se manejan con este modelo de datos. Algunas capacidades forman parte del protocolo CWMP nativo y otras se manejan con otros modelos de datos.

4 Definiciones de parámetros

En la cláusula 4 se definen la sintaxis y la semántica específicas de los parámetros de un dispositivo de almacén. Los parámetros se agrupan en lotes que, a su vez, se reúnen en perfiles para las diversas aplicaciones de la cláusula 6.

5 Notificaciones

6 Definiciones de perfil

6.1 Notación

6.2 Perfil básico

El perfil básico ofrece información de sólo lectura sobre el servicio de almacén, incluidas sus capacidades de almacén y acceso, dispositivos físicos, sistemas de ficheros y carpetas de alto nivel. Los parámetros escribibles se limitan a la configuración de la identidad de red externa del servicio de almacén.

6.3 Perfil User access

El perfil de acceso de usuario permite la configuración de la red y los usuarios locales, junto con sus derechos de acceso y credenciales de ingreso.

6.4 Perfil Group access

El perfil de acceso de grupo amplía el perfil de acceso de usuario a los grupos de usuarios, y permite la definición de los privilegios de acceso en el grupo.

6.5 Perfil FTP server

El perfil de servidor FTP configura un posible servidor FTP asociado al servicio de almacén, incluida su voluntad de dar servicio a usuarios anónimos.

6.6 Perfil SFTP server

El perfil de servidor SFTP amplía el perfil de servidor FTP para configurar también un posible servidor SFTP asociado con el servicio de almacén.

6.7 Perfil HTTP server

El perfil de servidor HTTP configura un posible servidor HTTP asociado con el servicio de almacén, incluida su política de seguridad.

6.8 Perfil HTTPS server

El perfil de servidor HTTPS amplía el perfil de servidor HTTP para incluir parámetros HTTPS adicionales.

6.9 Perfil Volume config

El perfil de configuración de volumen amplía el perfil básico para gestionar la configuración de volumen lógico y de carpetas de alto nivel.

6.10 Perfil RAID

El perfil RAID configura las matrices de almacenamiento e informa sobre el estado actual y la capacidad de la matriz.

6.11 Perfil Folder quota

El perfil de cuota de carpetas permite configurar la política de capacidad de carpetas, incluido el umbral de alerta de sobrecarga.

6.12 Perfil Volume threshold

El perfil de umbral de volumen configura las políticas de capacidad en el nivel del volumen lógico.

6.13 Perfil Network server

El perfil de servidor de red configura los protocolos de acceso a la red que se pueden utilizar para acceder a distancia al servicio de almacén.

7 Casos prácticos

El principal objetivo del servicio de almacén gestionado con TR-069 es restar la gestión del almacén de la responsabilidad del abonado. Al mismo tiempo, es posible acceder desde fuera a parte o todo lo almacenado para su utilización por parte de un abonado nómada o un servidor externo, como el ACS (actualización del software) o un almacén de grabador de vídeo personal (PVR) (véase [BBF TR-135]).

Anexo A – Teoría de las operaciones

En el Anexo A se detalla el funcionamiento del dispositivo de almacén, incluida la gestión de dispositivos extraíbles, la seguridad de acceso y casos prácticos detallados.

Anexo B – Descripciones de tipo RAID

El Anexo B es una guía didáctica sobre las distintas maneras de combinar los discos bajo la denominación RAID.

6.2.7 TR-196: *Femto access point service data model* (modelo de datos de servicio de punto de acceso femto)

En [BBF TR-196] se especifica el modelo de datos del punto de acceso femto (FAP, *femto access point*) para la gestión a distancia con CWMP. El objetivo de [BBF TR-196] es permitir a un operador ofrecer un servicio de acceso femto gestionado a los abonados. Así, la mayoría de aspectos del servicio están controlados por el ACS.

El alcance de este modelo de datos FAP es el nodo doméstico B UMTS FDD (3G HNB). Sin embargo, la estructura y organización del modelo de datos puede ampliarse para abarcar otro(s) tipo(s) de dispositivos FAP que utilizan otras tecnologías de interfaz radioeléctrica.

Para la equiparación técnica de la Recomendación con [BBF TR-196], esta cláusula (enmarcada) se estructura de conformidad con [BBF TR-196]. Los números de los títulos denotan los números de las cláusulas de [BBF TR-196].

4 Definición del modelo de datos

En la cláusula 4 se definen la sintaxis y la semántica específicas de los parámetros de un FAP. Los parámetros se agrupan en lotes que, a su vez, se reúnen en perfiles para las diversas aplicaciones de la cláusula 5.

5 Definiciones de perfil

En TR-196 se definen un gran número de perfiles para agrupar las características FAP. En el perfil básico se detalla la configuración que se espera en cualquier FAP. Otros perfiles describen las políticas de acceso local, la política de seguridad, los distintos protocolos inalámbricos que se pueden soportar, y las capacidades PM, de alarma y de diagnóstico.

La lista de perfiles incluye los siguientes:

2. Perfil básico
3. Perfil ACL
4. Perfil de acceso IP local
5. Perfil REM WCDMA FDD
6. Perfil REM GSM
7. Perfil GPS
8. Perfil SCTP de transporte
9. Perfil en tiempo real de transporte
10. Perfil de túnel IPSec
11. Perfil básico UMTS
12. Perfil de autoconfiguración UMTS
13. Perfil de NL de autoconfiguración UMTS utilizado en la célula de frecuencia
14. Perfil de NL de autoconfiguración UMTS utilizado entre células de frecuencia
15. Perfil de NL de autoconfiguración UMTS utilizado entre células RAT
16. Perfil básico de configuración de célula UMTS
17. Perfil avanzado de configuración de célula UMTS
18. Perfil de medición de frecuencia de configuración de célula UMTS
19. Perfil de medición interna UE de configuración de célula UMTS
20. Perfil de NL de configuración de célula UMTS en la célula de frecuencia
21. Perfil de NL de configuración de célula UMTS entre células de frecuencia
22. Perfil de NL de configuración de célula entre células RAT
23. Perfil de alarmas soportadas por la gestión de fallos
24. Perfil de alarmas activas en la gestión de fallos
25. Perfil de historia de eventos del perfil de gestión de fallos
26. Perfil de entrega rápida del perfil de gestión de fallos
27. Perfil de entrega en cola del perfil de gestión de fallos
28. Perfil de gestión de calidad de funcionamiento

Bibliografía

[b-UIT-T G.988] Recomendación UIT T G.988 (2010), *Especificaciones de la interfaz de gestión y control de unidades de red óptica*.

[b-UIT-T Y.101] Recomendación UIT T Y.101 (2000), *Terminología de la infraestructura mundial de la información – Términos y definiciones*.

[b-BBF01] Broadband Forum Technical Report Approval Process.
<http://www.broadband-forum.org/about/download/trapprovalprocess.pdf>

[b-BBF TR-098] Broadband Forum TR-098 Amendment 2 (2008), *Internet Gateway Device Data Model for TR-069*.
<http://www.broadband-forum.org/technical/download/TR-098_Amendment-2.pdf>

[b-BBF TR-181 Issue 1] Broadband Forum TR-181 Issue 1 (2010), *Device Data Model for TR-069*.
<http://www.broadband-forum.org/technical/download/TR-181_Issue-1.pdf>

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

Otros documentos relacionados

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

[b-BBF TR-68] Broadband Forum TR-68 (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] Broadband Forum TR-122 Amendment 1 (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] Broadband Forum TR-124 (2006), *Functional Requirements for Broadband Residential Gateway Devices*.
<http://www.broadband-forum.org/technical/download/TR-124.pdf>

[b-BBF TR-131] Broadband Forum TR-131 (2009), *ACS Northbound Interface Requirements*.
<http://www.broadband-forum.org/technical/download/TR-131.pdf>

[b-BBF TR-133] Broadband Forum TR-133 (2005), *DSLHome TR-064 Extensions for Service Differentiation*.
<http://www.broadband-forum.org/technical/download/TR-133.pdf>

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

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	**Sistemas y medios de transmisión, sistemas y redes digitales**
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos, comunicaciones de sistemas abiertos y seguridad
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2014