

TRABAJO ESPECIAL DE GRADO

ESTUDIO DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE UNA PLATAFORMA DE GESTIÓN REMOTA DE CPE (EQUIPO LOCAL DEL CLIENTE) BASADO EN EL PROTOCOLO TR-069

Presentado ante la Ilustre
Universidad Central de Venezuela
por el Br. TSU. Alarcón D, Euler.
para optar al Título de
Ingeniero Electricista

Caracas, 2014

TRABAJO ESPECIAL DE GRADO

ESTUDIO DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE UNA PLATAFORMA DE GESTIÓN REMOTA DE CPE (EQUIPO LOCAL DEL CLIENTE) BASADO EN EL PROTOCOLO TR-069

Prof. Guía: Ing. Carlos Moreno
Tutor Industrial: Miguel Zambrano

Presentado ante la Ilustre
Universidad Central de Venezuela
por el Br. TSU. Alarcón D, Euler.
para optar al Título de
Ingeniero Electricista

Caracas, 2014

CONSTANCIA DE APROBACIÓN

Caracas, 30 de mayo de 2014

Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por el Bachiller Euler Alarcón, titulado:

"ESTUDIO DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE UNA PLATAFORMA DE GESTION REMOTA DE CPE (EQUIPO LOCAL DEL CLIENTE) BASADO EN EL PROTOCOLO TR-069"

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista en la mención de Comunicaciones, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.


Prof. María Lejed
Jurado


Prof. Ricardo Santana
Jurado


Prof. Carlos Moreno
Prof. Guía

RECONOCIMIENTO Y AGRADECIMIENTO

Principalmente a la Universidad Central de Venezuela (UCV), por ser mi segundo hogar, es un orgullo haber alcanzado esta meta en “La casa que vence la sombra”.

Al Ing. Carlos Moreno por la canalización, colaboración y guía para llevar a cabo el presente trabajo especial de grado.

Al Ing. Miguel Zambrano por brindarme la oportunidad de realizar el trabajo especial de grado en una de las compañías de comunicaciones más importante del país. Igualmente al Ing. Mauricio Bromfman por todo su apoyo y ayuda en la realización de este proyecto conjuntamente con Friendly Technologies.

Y finalmente quiero expresar también mi más sincero agradecimiento a Maria Auxiliadora Rojas, por tu infinita paciencia, por tu valiosa compañía y tu inagotable apoyo.

DEDICATORIA

A toda mi familia en especial a cinco (5) personas; mis padres (Eulogio Alarcón y Mary Cely Díaz), a mis primos; la Ing. Yelitza Contreras y el Ing. Richard Lacruz y a mi tía Rosa de Alarcón, ya que estuvieron en todo momento para brindarme su apoyo y comprensión en la culminación de esta dura carrera.

Euler Alarcón Díaz

Alarcón D., Euler

ESTUDIO DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE UNA PLATAFORMA DE GESTIÓN REMOTA DE CPE (EQUIPO LOCAL DEL CLIENTE) BASADO EN EL PROTOCOLO TR-069.

Prof. Guía: PhD. Carlos Moreno. Tutor Industrial: Ing. Miguel Zambrano. Tesis. Caracas. U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Ingeniero Electricista. Opción: Comunicaciones. CANTV (Gerencia de Arquitectura de Redes y Sistemas – Laboratorio de Estandarización de Equipos de CANTV). Septiembre 2013 - Febrero 2014.

Palabras Claves: ADSL, ADSL2X, ABA, ACS, DMT, FTP, DHCP, SOAP, XML, FRIENDLY, CPE, DSLAM, BRAS.

Resumen. La Compañía Anónima Nacional de teléfonos de Venezuela (CANTV), con la finalidad de prestar un mejor servicio de acceso al Internet y de auto gestión para controlar, supervisar y diagnosticar la red de ABA, emprende un proyecto para evaluar e implementar una plataforma de gestión remota. Dicha plataforma busca trabajar a la par del servicio de acceso a internet de banda ancha (ABA), el cual estaba basado sobre la tecnología ADSL (Asymmetric Digital Subscriber Line / Línea de Abonado Digital Asimétrica) y se ejecuta en la infraestructura de la empresa sobre el medio de transmisión del par de cobre. La plataforma de gestión remota está diseñada por la empresa Friendly Technologies, la cual es un proveedor de soluciones optimizadas de gestión de dispositivos para operadores fijos o móviles. El enfoque del proyecto es conocer y verificar que protocolos de comunicación se manejan, además a través de dicha plataforma se realizarán una serie de pruebas para evaluar su adaptación y operatividad a la arquitectura ABA-CANTV (CPE-ACS-DSLAM-BRAS) y paralelamente indagar que la misma cumpla con los requerimientos que CANTV para su escalabilidad de gestión de equipos en un corto o mediano plazo.

ÍNDICE GENERAL

CONSTANCIA DE APROBACIÓN	iii
RECONOCIMIENTOS Y AGRADECIMIENTOS	iv
DEDICATORIA	v
RESUMEN	vi
LISTA DE FIGURAS	x
LISTA DE TABLAS	xii
ACRÓNIMOS	xiii
INTRODUCCIÓN	1
CAPÍTULO I	
1. PLANTEAMIENTO DEL PROBLEMA	
1.1 Planteamiento del Problema.....	4
1.2 Objetivos.....	6
1.2.1 Objetivo General.....	6
1.2.2 Objetivos Específicos.....	6
1.3 Alcance.....	6
1.4 Justificación.....	7
1.5 Limitaciones.....	8
CAPÍTULO II	
2. MARCO TEÓRICO	
2.1 Internet / Banda Ancha.....	9
2.2 Modelo OSI.....	10
2.2.1 Capa Física.....	11
2.2.2 Capa Enlace de Datos.....	11
2.2.3 Capa de Red.....	11
2.2.4 Capa de Transporte.....	11
2.2.5 Capa de Sesión.....	11
2.2.6 Capa de Presentación.....	12
2.2.7 Capa de Aplicación.....	12
2.3 Modelo TCP-IP.....	12
2.3.1 Capa de Acceso de Red.....	12
2.3.2 Capa de Internet.....	13
2.3.3 Capa de Transporte.....	13
2.3.4 Capa de Aplicación.....	13
2.4 Direccionamiento IP.....	14
2.5 Tecnología x.DSL.....	14
2.5.1 ADSL.....	15
2.5.2 ADSL2.....	15

2.5.3 ADSL2X.....	15
2.6 Transmisión DMT.....	16
2.7 Acceso Alámbrico a Internet.....	18
2.7.1 Atenuación.....	18
2.7.2 Ruido.....	19
2.7.3 Relación Señal a Ruido	19
2.8 Plataforma de Gestión de Red.....	20
2.9 Migración de Modems “Modo Puente” a “Modo Enrutador”.....	20
2.9.1 Modo Puente (Bridge).....	21
2.9.2 Modo Enrutador (Router).....	21
2.10 Componentes Funcionales del Protocolo TR-069.....	22
2.10.1 Auto-Configuración y Prestación de Servicios Dinámicos.....	22
2.10.2 Software / Firmware Gestión de Imágenes.....	23
2.10.3 Gestión del Módulo de Software.....	23
2.10.4 Estatus y Rendimiento.....	24
2.10.5 Diagnóstico.....	24
2.11 Posicionamiento de la Arquitectura Extremo a Extremo del TR-069.....	24
2.12 Objetivos de Seguridad del TR-069.....	24
2.13 Objetivos de la Arquitectura del TR-069.....	25
2.14 Supuestos del TR-069.....	27
2.15 Arquitectura del TR-069.....	27
2.15.1 Componentes del Protocolo.....	27
2.15.2 Mecanismo de Seguridad.....	28
2.15.3 Componentes de la Arquitectura del TR-069.....	29
2.15.3.1 Parámetros.....	29
2.15.3.2 Transferencias de Archivos.....	30
2.15.3.3 Inicio de Sesión del CPE.....	31
2.15.3.4 Sesiones Asíncrona Iniciadas por el ACS.....	32
2.16 Estructura de Normas TR-069.....	32
2.16.1 TR-098 para Dispositivos con Gateways a Internet.....	33
2.16.2 TR-104 para Gateways de VoIP.....	35
2.16.3 TR-106 para Dispositivos Digitales del Hogar.....	36
2.16.4 TR-110 para Configuraciones VoIP.....	38
2.16.5 TR-111 para Dispositivos LAN/NAT.....	39
2.16.6 TR-131 para interfaz NBI.....	44
2.16.7 TR-140 para Almacenamiento en Red.....	45
2.16.8 TR-142 para Dispositivos PON.....	46
2.16.9 TR-143 para Pruebas de Rendimiento de la Red.....	47
2.16.10 TR-156 para Acceso GPON.....	49
2.16.11 TR-157 para Módulo de Software de Gestión.....	50
2.16.12 TR-181 para Modelo de Datos de Dispositivos.....	51

CAPÍTULO III

3. RED ACTUAL DEL SERVICIO PARA ADSL/ADSL2X Y PLATAFORMA DE GESTIÓN REMOTA DE FRIENDLY TECHNOLOGIES

3.1 Arquitectura de Red de CANTV.....	55
3.2 Red de Acceso de Banda Ancha.....	56
3.2.1 Dispositivos que conforman la Red de acceso.....	56
3.2.1.1 CPE (Customer Premises Equipment).....	56
3.2.1.2 DSLAM.....	56
3.3 Red Metro-Ethernet.....	57
3.3.1 B-RAS (Broadband Remote Access Server).....	57
3.3.2 DHCP Server (Dynamic Host Configuration Protocol).....	58
3.4 Backbone IP.....	58
3.4.1 Borde.....	59
3.4.2 Core.....	59
3.4.3 Distribución.....	60
3.4.4 Agregación.....	60
3.5 Centro de Operaciones de Red (COR).....	60
3.6 Estatus de la Red de Internet Banda Ancha.....	63
3.7 Análisis de los indicadores de Falla de la Red.....	64
3.8 Proveedor Friendly Technologies de solución basada en TR-069.....	65
3.9 Aprovisionamiento Automatizado de Nuevos Usuarios y Servicios.....	69
3.10 Friendly TR-069 Suite Management Console.....	71
3.11 Friendly TR-069 Support Center.....	74

CAPÍTULO IV

4. MARCO METODOLÓGICO

4.1 Arquitectura para las Pruebas de la Plataforma FRIENDLY.....	77
4.2 Modelo de plantilla para las Pruebas de los CPEs.....	80
4.3 Descripción de los Dispositivos Evaluados (CPEs – Módems).....	82

CAPÍTULO V

5. RESULTADOS Y ANÁLISIS

5.1 Visualización de los CPEs en la Plataforma.....	83
5.2 Análisis de Resultados.....	88
5.3 Red IP de Banda Ancha con TR-069.....	89

CONCLUSIONES	90
---------------------------	----

RECOMENDACIONES	92
------------------------------	----

REFERENCIAS BIBLIOGRÁFICAS	94
---	----

BIBLIOGRAFÍA	96
---------------------------	----

ANEXOS	97
---------------------	----

LISTA DE FIGURAS

Figura 1. Comparación del modelo TCP-IP y modelo OSI.....	14
Figura 2. Ancho de banda ADSL2X.....	16
Figura 3. ADSL2/ADSL2X (distancia vs data).....	16
Figura 4. Modo Puente vs Modo Enrutador.....	22
Figura 5. Componentes del Protocolo TR-069.....	27
Figura 6. Estructura TR-104.....	35
Figura 7. Asociación de Flujo TR-111.....	43
Figura 8. Modelo TR-131.....	44
Figura 9. Estructura TR-140.....	46
Figura 10. OLT y ONT.....	47
Figura 11. Transparencia del TR-069.....	47
Figura 12. Componentes para prueba de Rendimiento.....	48
Figura 13. DownloadDiagnostics CPE usando HTTP Transport.....	48
Figura 14. Estructura TR-156.....	50
Figura 15. Modelo de datos TR-181.....	52
Figura 16. Modelo de datos a detalle (1) de TR-181.....	53
Figura 17. Modelo de datos a detalle (2) de TR-181.....	53
Figura 18. Modelo de datos a detalle (3) de TR-181.....	54
Figura 19. Red IP de Banda Ancha de CANTV.....	55
Figura 20. Arquitectura Metro-Ethenet en Caracas.....	58
Figura 21. Arquitectura CORE.....	59
Figura 22. Arquitectura Distribución.....	60
Figura 23. Contacto para el COR de CANTV.....	61
Figura 24. Representación Gráfica (%) de Red del 2013.....	64
Figura 25. Fallas comunes PC, CPE y Plataforma de Acceso.....	64
Figura 26. Niveles de Fallas de CPE.....	65
Figura 27. Página web de Friendly Technologies www.friendly-tech.com	66
Figura 28. Solución Friendly 3MM CPEs.....	67
Figura 29. Suite TR069 para Friendly.....	67
Figura 30. Arquitectura Friendly Technologies TR-069 Suite.....	68
Figura 31. Modelo de Gestión Friendly Technologies.....	69
Figura 32. Pantalla principal Management Console Friendly.....	71
Figura 33. Reportes de la Consola de Administración (Management Console).....	72
Figura 34. Reporte distribución de los CPEs.....	72
Figura 35. Reporte de firmware descargados.....	73
Figura 36. Pantalla principal para un CPE en Específico.....	73
Figura 37. Pantalla Principal del Centro de Soporte (Support Center) Friendly.....	74
Figura 38. Datos Configuración Support Center Friendly.....	75
Figura 39. Reporte de registro CPE.....	75
Figura 40. Actividad de la plataforma.....	76

Figura 41. Pantalla principal para monitoreo de un CPE en Específico.....	76
Figura 42. Arquitectura para la prueba de la plataforma FRIENDLY.....	77
Figura 43. Modems (CPE) gestionados.....	82
Figura 44. CPE BROADCOM 190.74.55.35.....	83
Figura 45. CPE BROADCOM 190.203.136.48.....	83
Figura 46. CPE BROADCOM 201.249.43.104.....	84
Figura 47. CPE BROADCOM 190.38.248.83.....	84
Figura 48. CPE BROADCOM 201.208.21.167.....	85
Figura 49. CPE STARBRIDGE 201.249.43.120.....	85
Figura 50. CPE HUAWEI 190.72.245.116.....	86
Figura 51. CPE HUAWEI 190.79.199.34.....	86
Figura 52. CPE ZyXEL 201.249.43.199.....	87
Figura 53. CPE ZTE 201.249.43.122.....	87
Figura 54. Red IP de Banda Ancha con TR-069.....	89
Figura 55. Ventajas de implementar TR-069.....	89

LISTA DE TABLAS

Tabla 1. Características de cada protocolo.....	28
Tabla 2. Estructuras de normas TR-069.....	33
Tabla 3. TR-098.....	34
Tabla 4. Parámetros TR-098.....	35
Tabla 5. VoIP Gateways.....	36
Tabla 6. Nombre de Objetos (ObjectsName) TR-106.....	38
Tabla 7. Definiciones de Parámetro de Objetos de Componentes.....	51
Tabla 8. Estatus de red durante el 2013 / Servicio Internet de Banda Ancha.....	53
Tabla 9. Costos referenciales para la implementación de la plataforma.....	125

ACRÓNIMOS

ABA	<i>Acceso a Banda Ancha</i>
ACS	<i>Auto-Configuration Server</i>
ADSL	<i>Asymmetric Digital Subscriber Line</i>
ANSI	<i>American National Standards Institute</i>
ASCII	<i>American Standard Code Information Interchange</i>
ATM	<i>Asynchronous Transfer Mode</i>
BGP	<i>Border Gateway Protocol</i>
BOSS	<i>Bussines Operations Supports Systems</i>
B-RAS	<i>Broadband Remote Access Server</i>
CANTV	<i>Compañía Anónima Nacional de Teléfonos de Venezuela</i>
CN	<i>Common Name</i>
COR	<i>Centro de Operaciones de Red</i>
CPE	<i>Customer Premises Equipment</i>
CWMP	<i>CPE WAN Management Protocol</i>
DHCP	<i>Dynamic Host Configuration Protocol</i>
DMT	<i>Discrete Multitone</i>
DNS	<i>Domain Name System</i>
DSLAM	<i>Digital Subscriber Line Access Multiplexer</i>
EFM	<i>Ethernet In The First Mile</i>
FFT	<i>Fast Fourier Transform</i>
FTP	<i>File Transfer Protocol</i>
FTTH	<i>Fiber To The Home</i>
GPON	<i>Giga-Passive Optical Network</i>
GUI	<i>Graphical User Interface</i>
HTTP	<i>Hypertext Transfer Protocol</i>
IFFT	<i>Inverse Fast Fourier Transform</i>
IGD	<i>Internet Gateway Device</i>
IP	<i>Internet Protocol</i>
IPv4	<i>Internet Protocol version 4</i>
IPv6	<i>Internet Protocol version 6</i>
ISDN	<i>Integrated Services Digital Network</i>
ISP	<i>Internet Service Provider</i>
LAN	<i>Local Area Network</i>
MAC	<i>Media Access Control</i>
MPLS	<i>Multi Protocol Label Switching</i>
NAT	<i>Network Address Translation</i>
NBI	<i>Northbound Interface</i>
OAC	<i>Oficina de Atención al Cliente</i>
OFF-THE-SHELF	<i>Manufacturado para ser comprado / Listo para ser utilizado</i>
OLT	<i>Optical Line Termination</i>
ONT	<i>Optical Network Terminal</i>

OSI	<i>Open System Interconnection</i>
OUI	<i>Organizationally Unique Identifier</i>
PIE	<i>Plan Internet Equipado</i>
PON	<i>Passive Optical Network</i>
PSTN	<i>Public Switched Telephone Network</i>
QAM	<i>Quadrature Amplitude Modulation</i>
QoS	<i>Quality of Service</i>
RDCD	<i>Red de Datos Dedicado</i>
RFC	<i>Request for Comments</i>
RRQ	<i>Registration Request</i>
RPC	<i>Remote Procedure Call</i>
RSVP	<i>Resource Reservation Protocol</i>
RTCP	<i>Real Time Control Protocol</i>
RTP	<i>Real Time Protocol</i>
SDH	<i>Synchronous Digital Hierarchy</i>
SIP	<i>Session Initiation Protocol</i>
SNMP	<i>Simple Mail Transfer Protocol</i>
SNR	<i>Signal To Noise Ratio</i>
SOAP	<i>Simple Object Access Protocol</i>
SSL	<i>Secure Sockets Layer</i>
STB	<i>Set To Box</i>
TELNET	<i>Telecommunication Network</i>
TCP	<i>Transmission Control Protocol</i>
TDM	<i>Time Division Multiplexing</i>
TLS	<i>Transport Layer Security</i>
TR069	<i>Technical Report 069</i>
UDP	<i>User Datagram Protocol</i>
UMTS	<i>Universal Mobile Telecommunications Systems</i>
UIT	<i>Unión Internacional de Telecomunicaciones</i>
URL	<i>Uniform Resource Locator</i>
VLAN	<i>Virtual Local Area Network</i>
VoIP	<i>Voice over Internet Protocol</i>
VPN	<i>Virtual Private Network</i>
XML	<i>Xtensible Markup Language</i>
WAN	<i>Wide Access Network</i>
WIFI	<i>Wireless Fidelity</i>
WiMAX	<i>Worldwide Interoperability for Microwave Access</i>

INTRODUCCIÓN

El presente trabajo especial de grado se desarrolló en la Compañía Anónima Nacional de Teléfonos de Venezuela (CANTV), ente adscrito al Ministerio del Poder Popular para la Ciencia, Tecnología e Innovación, la cual es la primera compañía de telecomunicaciones de Venezuela que tiene como objetivo principal fomentar la inclusión social y la disminución de la brecha al acceso de tecnologías digitales, facilitando así el alcance de todos a los servicios de telecomunicaciones.

Para CANTV es un objetivo fundamental garantizar que la población venezolana pueda contar con los servicios de telecomunicaciones y así mejorar su calidad de vida. La CANTV ha logrado impulsar el buen vivir de todas y todos llevando los servicios de Telefonía fija, alámbrica e inalámbrica, Telefonía móvil, Internet, Plan Internet Equipado (PIE) a las poblaciones más remotas del país.

CANTV cubre el territorio nacional con las tecnologías más efectivas y esto gracias a la red construida de fibra óptica interurbana que se encuentra alrededor de los 7800 km de longitud a través de 7 anillos, logrando la máxima confianza y seguridad en el servicio de las comunicaciones. Paralelamente, el servicio de transporte de datos y voz está basado en Frame Relay (el cual gestiona la conmutación de tramas, a partir de un uso dinámico del ancho de banda, con una velocidad de acceso desde los 64 Kbps hasta los 2048 Kbps con alta disponibilidad).

El servicio de acceso a internet de banda ancha (ABA), está basado sobre la tecnología ADSL (Asymmetric Digital Subscriber Line / Línea de Abonado Digital Asimétrica) el cual permite a CANTV aprovechar la infraestructura sobre la que realmente funciona el servicio telefónico (par de cobre). Desarrollando la idea del porque a esta tecnología se le llama asimétrica, es debido a que la capacidad de descarga es mucho mayor que la capacidad de subida, otro punto importante es que en toda línea ADSL se establecen tres (3) canales de comunicación:

1. El envío de datos.
2. El de recepción de datos.
3. Servicio telefónico analógico.

Para el caso del acceso a internet de banda ancha, a lo largo del territorio nacional habitualmente se dan diversas sugerencias, críticas, acotaciones y quejas debido a que el servicio no es el óptimo. Actualmente no existe una plataforma centralizada en la que pueda verificarse y corregirse las distintas fallas que se presentan. En vista de esto y resaltando la necesidad de la comunicación de todo el pueblo venezolano, el cual cada día se vuelve más exigente, la Compañía Anónima de Teléfonos de Venezuela busca mejorar de manera continua la calidad del servicio, lo cual permite incorporar muchos más usuarios, mejorar el nivel de satisfacción de los usuarios y una mejor operatividad de la red.

La plataforma de gestión remota promovida por la empresa Friendly Technologies se adapta inicialmente con las necesidades de la compañía, es por ello la importancia del presente proyecto en donde se realizara un estudio completo y detallado de los protocolos de comunicación que intervienen en dicha plataforma y se evaluarán las normas internacionales.

Con la intención de familiarizar al lector con los conceptos o definiciones en el presente proyecto, se expone la información concerniente a cada capítulo; el capítulo 1, está referido al planteamiento del problema, conjuntamente con los objetivos, el alcance, la justificación y las limitaciones.

En el capítulo 2, que comprende el marco teórico, se hace una recopilación teórica de las cualidades de la tecnología x.DSL asimétricas, y la importancia de una plataforma de gestión de red, estos dos conceptos son la base de la investigación. El capítulo 3, sigue con parte de la documentación teórica pero ahora vinculada al funcionamiento de CANTV relacionado al servicio de internet.

En el capítulo 4, se define la normativa asociada al protocolo TR-069 y sus especificaciones técnicas, aquí se explica en detalle como con dicho protocolo se realiza el diagnóstico y monitoreo de los diversos CPEs (Customer Premise Equipment / Equipo Local del Cliente). (Estructura del protocolo TR-069).

En el capítulo 5, se define la metodología empleada y conformación de la plataforma de gestión remota de Friendly Technologies bajo el protocolo TR-069 y se describe como se visualiza el diagnóstico y monitoreo de los CPEs en dicha plataforma.

Y finalmente se presentan las conclusiones, recomendaciones, bibliografía y anexos derivados de la realización del proyecto de tesis y análisis de los resultados obtenidos.

CAPÍTULO I

1. PLANTEAMIENTO DEL PROBLEMA

1.1 Planteamiento del Problema

La gestión de CANTV tras su nacionalización, se enfoca para seguir llevando la etiqueta como principal operadora de telefonía, internet y datos y esto gracias al pensamiento de que la empresa debe estar en constante revisión para innovarse, mejorando el servicio y seguidamente satisfacer al usuario final.

El servicio de ABA para CANTV es uno de los que ha representado mayor impacto de las telecomunicaciones al país y por ello representa un eje importante para la compañía, sin embargo, este impacto ha provocado la masificación de las telecomunicaciones lo que ha arrojado el uso continuo y un aumento significativo de usuarios en la red, que traen consigo un incremento considerable de tráfico de datos en la red.

Algunos factores negativos relevantes en la red se enumeran a continuación:

1. Alta demanda sobre el ancho de banda.
2. Reducción de la capacidad de procesamiento.
3. Fallas continuas.
4. En algunos casos no se tiene especificado el tipo de falla.
5. No existe un soporte eficaz.
6. No hay capacidad para la anticipación a una interrupción del servicio.
7. Se carece de un proceso para actualizar el software o firmware de un modem y mejorar su rendimiento.
8. No existe la gestión remota de los diversos CPE en la red de ABA.

Asumiendo todos estos factores, el servicio de ABA de CANTV carece relativamente de supervisión, monitoreo y control de manera remota.

Esto no permite atacar las fallas de manera efectiva y al instante, es más con el pasar de un tiempo provoca en el usuario un descontento ya que ve afectado su trabajo del día a día en la red, donde se generan dos situaciones especiales:

- i. Movilización del usuario a las oficinas de atención al cliente (OAC) y/o llamada al número de contacto 0-800-CANTV-00 en donde se genera un reporte, que registra el estatus del servicio y dependiendo del caso se intenta vía telefónica solventar la falla (interacción operador-usuario).
- ii. Rescisión del contrato, la cual ocurre como consecuencia directa de la anterior, que es cuando el usuario decide cancela el servicio y recurre a otra compañía de telecomunicaciones que satisfaga sus necesidades.

La puesta en práctica de una plataforma de gestión remota abarcaría una amplia gama de factores, corrigiendo así la operatividad de la red en forma continua.

1.2 Objetivos

1.2.1 Objetivo General

- Estudiar la factibilidad para la implementación de una plataforma de gestión remota de CPE (Equipo Local del Cliente) basado en el protocolo TR-069.

1.2.2 Objetivos Específicos

1. Realizar un levantamiento de información de los aspectos básicos relacionados con el servicio de internet de banda ancha.
2. Evaluar la red de datos actual, y basado en el servicio de internet estudiar la plataforma de gestión remota.
3. Describir el marco teórico del protocolo TR-069.
4. Identificar las especificaciones técnicas de la plataforma de gestión remota del CPE.
5. Estudiar la normativa internacional asociada al protocolo TR-069.
6. Analizar la integración de la plataforma de gestión remota con gestores paraguas y con otros sistemas.
7. Determinar las ventajas y estructuras de costos referenciales de implementación de dicha plataforma.
8. Establecer posibles soluciones para mejorar el servicio.

1.3 Alcance

El alcance del presente TRABAJO ESPECIAL DE GRADO está enfocado en la puesta en práctica de una plataforma de gestión remota bajo ambiente web suministrada por Friendly Technologies para supervisar, controlar y monitorear la conexión a internet con el servicio de acceso a banda ancha (ABA) de CANTV.

Al finalizar la tesis, lo que se desea es verificar la capacidad de que la plataforma ejecute las siguientes tareas:

- ✓ Elaborar una plantilla donde se verifique para cada módem, cuales tareas se ejecutara de manera correcta y cuáles no.
- ✓ Registrar el estatus de cualquier CPE (encendido o apagado).
- ✓ Verificación de los parámetros de línea de cada CPE.
- ✓ Generar reportes estadísticos o históricos mediante los cuales se pueda verificar su operatividad.
- ✓ Que se puedan realizar descargas de software o firmware a los diversos CPEs.
- ✓ Que se cumplan en su totalidad los requerimientos mínimos de toda plataforma de gestión remota y los que define CANTV.
- ✓ Toda esa información suministrada al sistema pueda ser procesada y almacenada a través de registros en una base de datos, para que luego un operador pueda utilizar esos reportes en pantalla de acuerdo a los criterios que este emplee para tal fin.

1.4 Justificación

Como se mencionó en la parte del planteamiento del problema, existe un repunte en el crecimiento de usuarios en la red lo que ha provocado la inquietud y a la vez el incentivo de mejoras para la actual demanda. CANTV al estar consciente de este panorama desarrolla proyectos pilotos como este, que le garantizan extender la utilización de redes legadas y proteger a los usuarios mediante alguna migración enfocada del servicio FRAME RELAY basado en el protocolo TR-069, esto provoca un estudio detallado de cada una de las etapas del proyecto de manera que se puede asegurar la calidad del servicio al usuario.

CANTV siempre tiene la necesidad de mantener su competitividad en el acceso a banda ancha, cada vez con más exigencia y en la red que tiene actualmente intervienen unos factores que degradan el servicio. Es por ello que se debe evaluar un nuevo modelo de auto gestión que siga garantizando su rentabilidad.

La propuesta de trabajar utilizando estándares internacionales para los procesos, lleva consigo una ventaja para la compañía CANTV como pionera entre los proveedores de servicios en Venezuela.

Desarrollar este estudio enfocado en una infraestructura de entrega de servicio basado en estándares y protocolos internacionales que tome en cuenta la pronta implementación y los requerimientos planteados por el protocolo TR-069 permitirán en un mediano o largo período la estandarización del servicio.

1.5 Limitaciones

El presente proyecto incluye un estudio de factibilidad donde se abarcan todas las operaciones y tareas más comunes en los CPEs y los procedimientos involucrados en la plataforma con el protocolo TR-069 de manera que se compruebe la mejora del servicio de internet. Con este panorama, se pretende una optimización e integración de soluciones que beneficien a la compañía CANTV en dicho servicio. Las limitaciones que se presentaron es que pudieron haberse incorporado más equipos y de más tipos de proveedores, no se tuvo acceso a los DSLAM (Digital Subscriber Line Access Multiplexer) que gestionan los CPEs y la otra limitación en los ensayos o pruebas del servicio fue con uno de los módems de la marca ZTE – modelo ZXHN-HL08L, de que a pesar que logro incorporarse a la plataforma fue el que presento mas fallas.

En este proyecto no se incluyen los aspectos vinculados a la comercialización, venta y asistencia al cliente. Estos parámetros serán evaluados en otra fase del nexo de Friendly Technologies con CANTV.

CAPITULO II

2. MARCO TEÓRICO

2.1 Internet --- Banda Ancha

El fenómeno del internet ocasiono una revolución en cuanto a la manera de comunicarse la sociedad en general. Este creciente auge en el acceso de la información y a los servicios de toda índole a través del internet contrasta con la invitación reiterada por parte de los diversos operadores de telecomunicación a que desarrollen innovaciones en pro de la competencia legal y efectiva.

Con esto se desea fijar el interés de brindar servicios en banda ancha para las compañías de telecomunicaciones a nivel mundial. El termino banda ancha hay que definirlo claramente y por ello acá se incluye donde inicialmente se introdujo dicho termino, lo cual fue en la asamblea plenaria de la CCITT (actualmente llamado UIT Unión Internacional de las Telecomunicaciones) celebrada en Brasilia en el año 1989, donde se definieron las nuevas redes públicas de servicios integrados. *“El aspecto más visible de cara al abonado, sería el acceso a cadencias iguales o superiores a 155 Mbps. La definición oficial de la UIT es especificando que un servicio es de banda ancha cuando requiere canales de transmisión con capacidad mayor que un acceso primario (2.048 Mbps)”*.

A partir de este concepto, surgió la palpable revolución tecnológica en el acceso al usuario, el mercado como tal paso a divulgar la expresión “banda ancha” para vincular a tecnologías que permiten velocidades de acceso de usuario en el orden de los Mbps.

A continuación se presentan las tecnologías de redes de acceso que han sido particularmente asociadas a banda ancha, incluyendo las que tradicionalmente se emplean para ofrecer servicios comerciales, como aquellas otras que, aun con un nivel de madurez insuficiente, pueden construir la base para futuras redes de acceso.

➤ Tecnologías con medio de transmisión sobre cables:

1. Bucle Digital de abonado x.DSL
2. Redes híbridas de fibra y cable HFC
3. Fibra Óptica Pasiva FTTH
4. Comunicaciones por vía eléctrica PLC
5. Ethernet en la primera milla EFM

➤ Tecnologías inalámbricas:

1. Bucle Inalámbrico LMDS
2. Redes de acceso por satélites
3. Redes Inalámbricas WAN: WiFi Mallado y WiMAX
4. Comunicaciones móviles de tercera generación UMTS

El presente trabajo especial de grado se enfoca sobre la tecnología x.DSL (específicamente ADSL2X), con la cual es que se ofrece el acceso a internet por parte CANTV. Más adelante en el apartado “2.5” se presenta la tecnología x.DSL asimétrica. A continuación se hace referencia a los dos modelos de telecomunicaciones (Modelo OSI y Modelo TCP-IP).

2.2 Modelo OSI

El modelo OSI (Open System Interconnection) es el modelo principal para las comunicaciones por red. Aunque existen otros, actualmente una gran parte de los proveedores de redes relacionan sus productos con el modelo OSI, especialmente cuando desean enseñar a los usuarios cómo utilizar sus productos.

Está representada por 7 capas donde cada una cumple una función específica pero cada una está vinculada con la que le sigue.

2.2.1 Capa Física

Está vinculada con las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas. Las características tales como niveles de voltaje, temporización de cambios de tensión eléctrica, velocidad de datos, distancias de transmisión máximas, conectores físicos.

2.2.2 Capa Enlace de Datos

Proporciona el tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo.

2.2.3 Capa de Red

Esta capa proporciona conectividad y selección de ruta entre dos sistemas que pueden estar ubicados en redes geográficamente distintas.

2.2.4 Capa de Transporte

La capa de transporte segmenta los datos originados en el sistema emisor y los reensambla en una corriente de datos dentro del sistema del sistema receptor. Mientras que las capas de aplicación, presentación y sesión están relacionadas con la ejecución de las aplicaciones, las cuatro capas inferiores se encargan del transporte de datos.

2.2.5 Capa de Sesión

Esta capa provee los servicios utilizados para la organización y sincronización del diálogo entre usuarios y el manejo e intercambio de datos.

2.2.6 Capa de Presentación

Está garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común.

2.2.7 Capa de Aplicación

Es la capa del modelo OSI más cercana al usuario; suministra servicios de red a las aplicaciones del usuario. Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI.

2.3 Modelo TCP-IP

El modelo TCP/IP fue desarrollado para la transmisión entre redes de computadoras y en realidad es un conjunto de protocolos, pero toma el nombre de los dos protocolos más importantes, estos son el TCP (*Transport Control Protocol*) (ubicado en la capa 4 de modelo OSI) y el IP (*Internet Protocol*) (ubicado en la capa 3). Aunque el modelo OSI es el conocido generalmente como el modelo de conexión entre redes de computadoras, es el modelo TCP/IP el que se utiliza como la base de Internet desde el punto de vista técnico, ya que este modelo simplifica al modelo OSI. El modelo OSI está compuesto por siete capas o niveles mientras que el modelo TCP/IP solo posee cuatro capas o niveles.

2.3.1 Capa de Acceso de Red

Está capa se encarga de diversos tópicos que requiere un paquete IP para realizar realmente un enlace físico y luego realizar otro enlace físico. Esta capa incluye los

detalles de tecnología LAN y WAN y todos los detalles de la capa física y de enlace de datos del modelo OSI.

2.3.2 Capa de Internet

La función de esta capa es enviar paquetes origen desde cualquier red en el internet y que estos paquetes lleguen a su destino independientemente de la ruta y de las redes que recorrieron para llegar hasta allí.

2.3.3 Capa de Transporte

Esta capa provee comunicación extremo a extremo desde un programa de aplicación a otro, asegura que los datos lleguen sin error a su destino y en la secuencia correcta a su aplicación correspondiente en el lado remoto. En esta capa se encuentran los protocolos TCP y UDP usados para dar servicio a una serie de aplicaciones de alto nivel como aplicaciones de descarga (audio y video).

2.3.4 Capa de Aplicación

En esta capa se encuentran las aplicaciones disponibles para los usuarios y se puede decir que engloba las capas de aplicación, presentación, sesión y transporte del modelo OSI.

Comprende el manejo de protocolos de alto nivel como TELNET, FTP, SNMP, HTTP y muchos otros que permiten acceder a otras computadoras de la misma red y garantiza que los datos relacionados con las aplicaciones estén correctamente empaquetados para ser enviados a la siguiente capa.

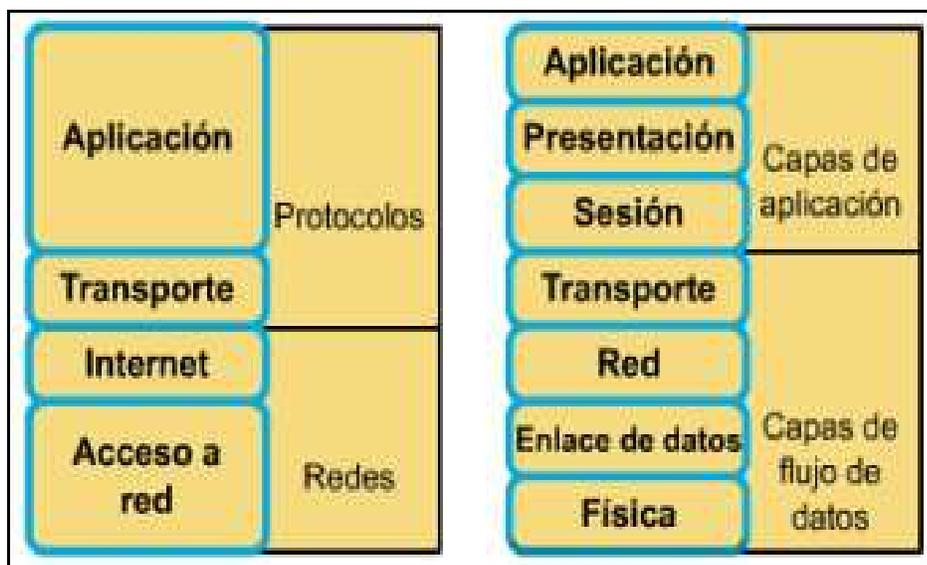


Figura 1: Comparación del Modelo TCP-IP y Modelo OSI.

Fuente: Cisco Network.

2.4 Direccionamiento IP

Una dirección de Internet (dirección IP), es un número específico que identifica de manera lógica y jerárquica a una interfaz de un dispositivo dentro de una red. Esta puede modificarse al reconectar el terminal a la red, y a esta forma de asignación de dirección IP se le denomina IP dinámica, mientras que aquellos dispositivos que por su naturaleza requieren utilizar la misma dirección IP cada vez que se conecten a la red hacen uso de una dirección IP fija.

2.5 Tecnología x.DSL

La tecnología x.DSL comprende una amplia utilización de códigos de líneas y técnicas de modulación que permiten transmitir datos de alta velocidad sobre el medio de transmisión más común y antiguo; el par de cobre.

Haciendo un poco de historia de cómo surgió dicha tecnología puede decirse que gracias a Joseph Lechleider quien laboraba para la compañía Bellcore y sus trabajos

para poder transmitir mayores volúmenes de información por internet alrededor de los años 80, logra demostrar la viabilidad de enviar señales de banda ancha y desarrolla la idea de la transmisión asimétrica, la cual partía de que enviaba más información en un sentido que en el otro sobre el par de cobre. Los 3 tipos de tecnologías enfocadas en el presente trabajo son x.DSL asimétricas (ADSL, ADSL2 y ADSL2X) a las cuales se les dará un breve concepto.

➤ **2.5.1 ADSL**

(Asymmetric Digital Subscriber Line)

Cubre de manera efectiva las necesidades del usuario común (grandes velocidades de descargas y bajas velocidades de subida). Esta tecnología es empleada en distancias de hasta 5,5 Km y llega alrededor de velocidades de transmisión de 1,5 Mbps a 8 Mbps en descarga y de 16 Kbps a 1 Mbps en subida.

➤ **2.5.2. ADSL2**

(Asymmetric Digital Subscriber Line 2)

Conocida como la segunda generación de la ADSL, esta permite velocidades de transmisión mayor, logrando alcanzar velocidades de hasta 12 Mbps en descarga y 2 Mbps en subida. Esto se logró con la mejora de modulación/codificación haciendo uso de codificación trellis de 16 estados y modulación QAM con constelaciones de 1 bit.

➤ **2.5.3 ADSL2X**

(Asymmetric Digital Subscriber Line 2X)

Posee el mismo funcionamiento de ADSL2, el detalle radica en que permite la utilización de mayor espectro sobre el bucle de abonado, aumentado al doble su ancho de banda, de 1,1 MHz a 2,2 MHz. Ya que las frecuencias más altas se atenúan más rápidamente en el par telefónico, las velocidades de descargas disminuyen rápidamente a medida que se incrementa la distancia, pero permite velocidades de transmisión alrededor de 24 Mbps a 16 Mbps en lazos de abonados cortos, menores a

1 Km, y alrededor de 8 Mbps a 3 Km de distancia de la central local. Es por ello que CANTV emplea esta tecnología por su versatilidad y rendimiento. Maneja los detalles de distancia y transmisión de datos de manera efectiva y además permite que se le puedan prestar al usuario diferentes servicios dependiendo de la distancia a la cual se encuentre y la velocidad máxima de transferencia que se le pueda dar.

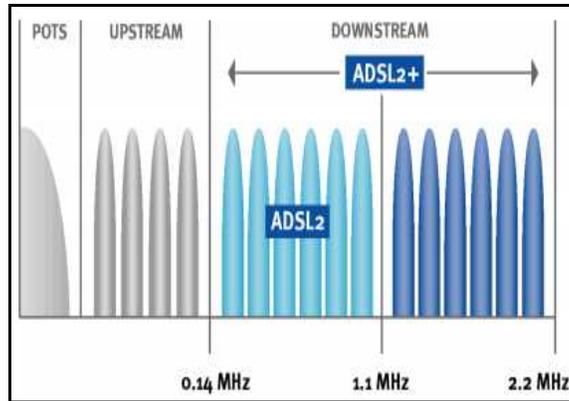


Figura 2: Ancho de Bandas ADSL+2(ADSL2X)

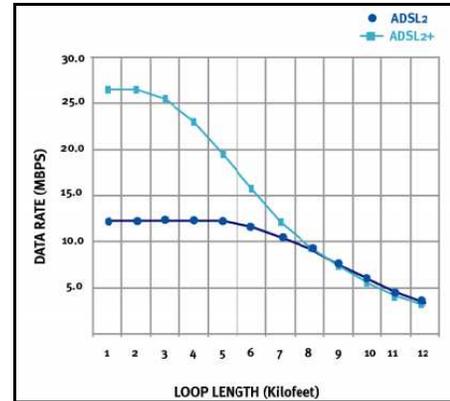


Figura 3: ADSL2/ADSL+2
(Distancia vs Data)

2.6 Transmisión DMT

Los estándares VSDL y ADSL utilizan QAM (*Quadrature Amplitude Modulation*) o DMT (*Discrete Miltitone*) como esquemas de modulación/codificación, pero cuando la UIT aprobó definitivamente el estándar, incorporó el esquema DMT en el cuerpo principal de la recomendación, y hoy en día la mayoría de los fabricantes de equipos utilizan DMT para la realización y desarrollo de sus tarjetas de línea y CPE. Sin embargo al no estar estandarizado como tal, existen algunos fabricantes que desarrollan sus equipos basándose en QAM, lo cual también está contemplado dentro de la recomendación emitida por la UIT, y origina que la compatibilidad entre equipos se vea comprometida, ya que no es posible la utilización de un CPE basado en DMT con una tarjeta de línea basada en QAM y viceversa.

La modulación por multi-tonos discretos es una técnica que divide el ancho de banda disponible de 1.104MHz en 256 sub-canales o tonos que van desde 0Hz hasta 1.104MHz. Cada tono ocupa 4.31kHz del ancho de banda total y utiliza una técnica de modulación en cuadratura llamada QAM (*Quadrature Amplitude Modulation*).

Cada tono puede transportar hasta un máximo de 15 bits de información, dependiendo de la relación señal a ruido presente en cada tono y es necesario aplicar la técnica de modulación QAM para codificarlos.

El primer tono se utiliza para los servicios de telefonía, los tonos del 2 al 6 se usan para evitar interferencia entre la telefonía y ADSL, los tonos del 7 al 32 ubicados entre 25.7KHz y 138KHz son utilizados para transferencia de datos en dirección de subida, mientras que los tonos del 33 al 256 ubicados entre 138KHz y 1.104KHz son utilizados para la transferencia de datos en dirección de bajada.

Estas frecuencias están estandarizadas por la ANSI (*American National Standards Institute*).

Con DMT se puede superar este problema utilizando las bandas del espectro que presenten menor atenuación e interferencia.

Posteriormente se prueba la línea para comprobar las bandas de frecuencia que están disponibles, y cuántos bits se pueden transmitir por unidad de ancho de banda.

Los bits son codificados en el transmisor, en el caso de VDSL las portadoras están igualmente espaciadas y son ortogonales entre sí. Para modular y demodular los símbolos se utilizan IFFT (Inverse Fast Fourier Transform – Transformada Inversa Rápida de Fourier) y FFT (Fast Fourier Transform – Transformada Rápida de Fourier) respectivamente, es necesario garantizar la ortogonalidad entre los tonos por lo que se hace necesario un cierto nivel de procesamiento en el transmisor y en el receptor, este proceso es realizado durante la inicialización del enlace.

2.7 Acceso Alámbrico a Internet

Un servicio como el de acceso a internet, en el cual el número de usuarios se incrementa de manera considerable y por ende, la estructura del proveedor debe estar preparada para soportar este incremento a través de procesos que mantengan un rendimiento adecuado a la red. Estos procesos deben enfocarse en controles que, a pesar de que existan muchos usuarios, mantengan estable la velocidad de cada uno de ellos para que de esta manera todos naveguen sin problema alguno y no se saturen los enlaces, evitándose así el perjuicio a los propios usuarios.

Según esto, el principal factor de falla que atraviesa la tecnología ADSL es la saturación de sus enlaces debido al incremento de usuarios y a la capacidad limitada de dichos enlaces.

La red ADSL también se ve afectada debido a la distancia de la central y el domicilio de usuario, ya que tanto los principales parámetros de línea que son el ruido como la atenuación son directamente proporcionales a la distancia que la señal debe recorrer por el canal, es decir, mientras mayor es la distancia, mayor es la sensibilidad de la señal al ruido y a la atenuación. Tanto el ruido como la atenuación son dos (2) parámetros muy importantes en el proceso de acceso a la red e influyen en el rendimiento de la conexión. Para que el usuario pueda navegar con normalidad y sin problema de lentitud o cortes de conexión, se debe minimizar la influencia de estos parámetros y lograr que no perjudiquen el servicio.

2.7.1 Atenuación

Es un parámetro del canal que aparece con la pérdida de la señal (disminuye la amplitud y la intensidad) cuando esta se propaga por el par de cobre, que es el caso de estudio en el presente proyecto. Es el cociente de la potencia recibida (P_1) en la

central, entre la potencia emitida (P_2) que es la presente en el CPE del cliente. Este parámetro generalmente viene expresado en decibelio (dB).

$$\alpha = 10 \times \log \frac{P_1}{P_2}$$

Ecuación 1: Atenuación en dB.

2.7.2 Ruido

Es cualquier señal no deseada que se acopla con la señal útil que se desea mantener en una transmisión. Es el resultado de diferentes tipos de perturbación que tiende a enmascarar la información y que provoca que el receptor lea erróneamente la señal que le envía el emisor. Las causas son principalmente componentes electrónicos, ruido térmico de las resistencias o interfaces de señales externas. Es imposible erradicar el ruido ya que los componentes electrónicos en la transmisión son imperfectos, pero se puede limitar el nivel de ruido, de manera que la calidad de la comunicación sea aceptable.

2.7.3 Relación Señal a Ruido (SNR)

Es el margen existente entre el nivel de referencia y el ruido de fondo (señal no útil) de un determinado sistema. Es medida en decibelios y sirve como parámetro para medir la calidad de la señal debido a que cuanto más alto es el valor de la SNR, la calidad de la señal es mejor. Esto es porque una SNR alta indica que la señal es más fuerte que el ruido (o que el ruido es más débil comparado con la señal); de cualquier forma, lo mejor y más importante es tener un valor de SNR alto, ya que, además de tener una mejor calidad de señal, se puede transmitir a través de una distancia mayor. Según esto, la SNR define la capacidad de transmisión del ADSL. En cualquier caso, una cierta SNR mínima es necesaria para la comunicación, en el caso de CANTV

partiendo de las normas de calidad, el nivel de relación SNR debe permanecer siempre por encima de por lo menos 6 dB.

2.8 Plataforma de Gestión de Red

Históricamente, la gestión de red se ejecuta mediante un conjunto de programas aislados, cada uno encargado de gestionar un número específico de componentes (dispositivos o datos de gestión) de red.

Se trata en sí, de una aplicación de software, especialmente diseñada para funcionar sobre computadores en el control y monitoreo de un sistema, proporcionando comunicación con una gran cantidad de dispositivos Paralelamente, envía la información generada de un proceso a varios dispositivos, es decir permite el control de calidad de tareas, supervisión y mantenimiento y por ende sirve para atacar posibles fallas ya no de manera correctiva sino preventiva.

Tomando en cuenta de manera general la optimización de costos, espacio físico, control, supervisión y monitoreo se plantea constantemente la necesidad de una gestión integrada desde un solo sistema, que debería presentar las interconexiones en un mapa de la red.

El objetivo de la plataforma es proporcionar una funcionalidad genérica para gestionar distintos dispositivos (marcas, modelos, generaciones, etc) de red.

2.9 Migración de Modems “Modo Puente” a “Modo Enrutador”

Todo modem utilizado para el servicio de internet de banda ancha de CANTV, puede estar configurado en el “Modo Puente” o en el “Modo Enrutador”; el detalle es que para trabajar con el protocolo TR-069, se requiere que la plataforma localice cada modem de manera continua y esto lo logra con el direccionamiento IP, a

continuación se presentan las diferencias entre ambos modos de operación y la justificación del porque hacer la migración en los módems a “Modo Enrutador”.

2.9.1 Modo Puente (*Bridge*)

Los módems en este modo de operación son dispositivos de interconexión que conectan y pasan paquetes entre dos segmentos de red que utilicen el mismo protocolo de comunicaciones. Los módems bridges solo cumplen la función de pasar paquetes o de no pasar según su dirección MAC (*Media Access Control*) de destino. Es por ello, que ellos pasan información entre redes que operan bajo diferentes protocolos de capa 2.

Ya que en este modo de operación se lleva a cabo en la capa de enlace de datos (capa 2), no se requiere revisar la información de capa superiores. Estos filtran el tráfico basándose particularmente en la dirección MAC.

Para filtrar o entregar selectivamente el tráfico de una red particular, estos elaboran tablas con todas direcciones MAC de la red, y de otras redes y hacen un mapeo con ellas. Si pasan datos a través de los medios de la red, un puente compara la dirección MAC destino que llevan los datos con las direcciones MAC que contienen sus tablas.

2.9.2 Modo Enrutador (*Router*)

Estos dispositivos de interconexión de redes operan en la capa nivel de red (capa 3). Su función principal es encaminar paquetes entre distintas redes. Los módems en modo router, son los equipos que conforman la red a nivel general, interconectando a nivel lógico las diferentes redes físicas, y gracias a ellos los datagramas IP pueden fluir desde cualquier parte de la red hasta cualquier otro lugar.

Al recibir un paquete, en modo de operación enrutador “*router*” se lee la cabecera del paquete IP y determina, mediante la dirección IP destino, si está dirigido a una red a la que el “*router*” tiene acceso de forma local. En este caso, envía el paquete a la dirección MAC correspondiente.



Figura 4: Modo Puente vs Modo Enrutador.

La finalidad de migrar todos los módems a modo “*router*” es que para el momento de incorporarlos a la plataforma, en esta se pueda realizar el diagnostico, monitoreo, revisión y actualización de manera precisa y eficiente.

2.10 Componentes Funcionales del Protocolo TR-069 (Technical Report 069)

El protocolo TR-069 está diseñado para soportar una variedad de funcionalidades para gestionar una colección de CPEs, incluyendo las siguientes capacidades principales:

- Auto-configuración y aprovisionamiento de servicios dinámicos
- Gestión de la imagen del software / firmware
- Software de gestión de módulos
- Supervisión de estado y el rendimiento
- Diagnóstico

2.10.1 Auto-Configuración y Prestación de Servicios Dinámicos

El protocolo TR-069 permite con un ACS (*Auto-Configuration Server*) la provisión de un CPE o la recolección de datos CPEs basados en una variedad de criterios.

El mecanismo de aprovisionamiento permite al CPE en el momento de la conexión inicial a la red de acceso de banda ancha, la capacidad de re-disposición o re-configurar en cualquier momento posterior.

Los mecanismos de identificación incluidos en el protocolo permiten al CPE el aprovisionamiento del CPE ya sea en los requisitos de cada CPE específico, o de criterios colectivos tales como el CPE proveedor, modelo, versión de software, o cualquier otro criterio. El protocolo también proporciona herramientas opcionales para gestionar los componentes específicos de CPE aplicaciones o servicios opcionales para los que se requiere un nivel adicional de seguridad de control, tales como los que implican pagos del servicio.

2.10.2 Software / Firmware Gestión de imágenes

El protocolo TR-069 proporciona herramientas para gestionar la descarga de software / firmware archivos de imagen al CPE. El mismo proporciona mecanismos para la versión identificación, archivo descarga iniciación (ACS descargas iniciadas y opcional CPE descargas iniciadas), y la notificación de los servidores ACS del éxito o fracaso de un archivo descargar.

2.10.3 Gestión del Módulo de Software

El protocolo TR-069 permite con un servidor ACS administrar el software modular y entornos de ejecución en un CPE. Capacidades previstas incluyen la habilidad de instalar, actualizar y desinstalar los módulos de software así como la notificación a los servidores ACS de éxito o fracaso de cada acción.

El protocolo también proporciona apoyo para iniciar y detener aplicaciones en el CPE, activar y desactivar entornos de ejecución, e inventariar el software módulos disponibles en el dispositivo.

2.10.4 Estatus y Rendimiento

El protocolo TR-069 proporciona soporte para un CPE de poner a disposición información que el servidor ACS puede utilizar para supervisar el estado del CPE y las estadísticas de rendimiento.

También se define un conjunto de mecanismos que permiten que el CPE de notificar activamente los ACS de cambios en su estado.

2.10.5 Diagnóstico

El protocolo TR-069 proporciona soporte para un CPE, de poner a disposición información que el servidor ACS puede utilizar para diagnosticar y resolver problemas de conectividad o servicio, así como la capacidad de ejecutar pruebas de diagnóstico definidos.

2.11 Posicionamiento de la Arquitectura END-TO-END del TR-069

El ACS es un servidor que reside en la red y gestiona los dispositivos en las instalaciones del abonado. El Protocolo de gestión CPE WAN se puede utilizar para gestionar tanto DSL y otros tipos de CPE, incluyendo routers independientes y clientes de la LAN dispositivos.

Es agnóstico al medio de acceso específico utilizado por el proveedor de servicios, a pesar de que no depende de IP-capa de conectividad de haber sido establecida por el dispositivo.

2.12 Objetivos de Seguridad del TR-069

El protocolo TR-069 está diseñado para proporcionar un alto grado de seguridad. El modelo de seguridad también está diseñado para ser escalable. Su objetivo es permitir

la seguridad básica para dar cabida a las implementaciones de CPE menos robusto, permitiendo al mismo tiempo una mayor seguridad para las que pueden apoyar los mecanismos de seguridad más avanzadas. En términos generales, el los objetivos de seguridad de protocolo de gestión de la CPE WAN son los siguientes:

- ✓ Evitar la manipulación de las funciones de gestión de un CPE o ACS, o las transacciones que tienen lugar entre un CPE y ACS.
- ✓ Proporcionar confidencialidad de las transacciones que tienen lugar entre un CPE y ACS.
- ✓ Permitir la autenticación adecuada para cada tipo de transacción.
- ✓ Evite el robo de servicio.

2.13 Objetivos de la Arquitectura del TR-069

El protocolo está diseñado para proporcionar flexibilidad en el modelo de conectividad. El protocolo está diseñado para proporcionar lo siguiente:

- ✓ Permitir tanto al CPE como al ACS iniciar establecimiento de la conexión, evitando la necesidad de una conexión persistente que debe respetarse entre cada CPE y un ACS.
- ✓ Las interacciones funcionales entre el ACS y el CPE deberían ser independientes de final que inició el establecimiento de la conexión. En particular, incluso cuando conectividad iniciada por el ACS no es compatible, todas las transacciones iniciadas por el ACS deben llevarse a cabo mediante una conexión iniciada por el CPE.
- ✓ Permitir uno o más servidores ACS para servir a una población de CPEs, que puede estar asociada con uno o más proveedores de servicios.

El protocolo tiene por objeto apoyar el descubrimiento y la asociación de ACS y CPE:

- ✓ Proporcionar mecanismos para el CPE, para descubrir los ACS adecuados para un determinado servicio proveedor.
- ✓ Proporcionar mecanismos para permitir a un ACS identificar con seguridad un CPE y asociarlo con un usuario/cliente. Procesos de asociación deben apoyar modelos que incorporen la interacción del usuario, así como aquellos que son totalmente automáticos. El protocolo está diseñado para permitir un acceso del ACS para controlar y supervisar varios parámetros asociados con un CPE.

Los mecanismos establecidos para acceder a estos parámetros están diseñados con las siguientes premisas:

- ✓ CPE diferentes pueden tener diferencias en los niveles de capacidad, la implementación de diferentes subconjuntos de funciones. Además, un ACS puede manejar una variedad de diferentes dispositivos tipos entrega de una gama de diferentes servicios. Como resultado, un ACS debe ser capaz de descubrir las capacidades de un CPE particular.
- ✓ Un ACS debe ser capaz de controlar y supervisar la configuración actual de un CPE.
- ✓ Otras entidades de control, además del ACS pueden ser capaces de controlar algunos parámetros de configuración del CPE (por ejemplo, a través de la LAN de configuración automática). Como resultado, el protocolo debe permitir al ACS para dar cuenta de los cambios externos a la configuración del CPE.
- ✓ El protocolo debe permitir que los parámetros específicos del proveedor que se definen y se accede a ellos.

El protocolo está diseñado para minimizar la complejidad de la implementación, mientras que proporciona flexibilidad frente a la funcionalidad. El protocolo incorpora un número de componentes opcionales que entran en juego sólo si la funcionalidad específica es requerida. El protocolo también incorpora las normas vigentes en su caso, lo que permite influencia de las implementaciones de (*off-the-shelf*).

El protocolo también está diseñado para ser extensible. Incluye mecanismos para apoyar futuras ampliaciones de la norma, así como los mecanismos explícitos para extensiones específicas del proveedor.

2.14 Supuestos del TR-069

Algunas suposiciones hechas en la definición del protocolo de gestión de CPE WAN se enumeran a continuación:

- ✓ Todo CPE sin importar el tipo (enrutador u otro) debe obtener una dirección IP con el fin de comunicarse con un ACS.
- ✓ Un CPE puede interactuar con un único ACS a la vez. En cualquier momento, un CPE es consciente de exactamente el ACS con la que se puede conectar.

2.15 Arquitectura del TR-069

2.15.1 Componentes del Protocolo

El protocolo TR-069 comprende varios componentes y hace uso de varios protocolos estándar. Dicha pila está definida por la gestión del CPE WAN como se muestra en la Figura 5. Una breve descripción de cada capa se presenta en la Tabla 1. Tenga en cuenta que el CPE y el ACS deben cumplir con los requisitos de los protocolos estándar subyacentes a menos que se especifique lo contrario. [1] [2]

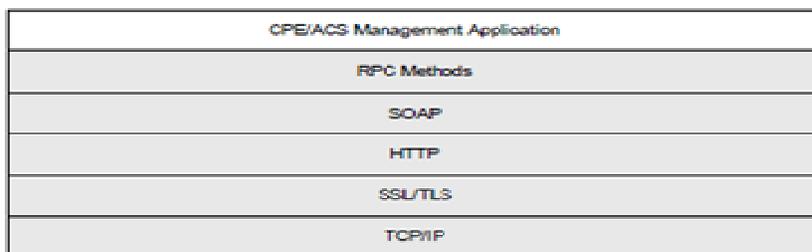


Figura 5: Componentes del protocolo TR-069

Fuente: Manual TR-069

Layer	Description
CPE/ACS Application	The application uses the CPE WAN Management Protocol on the CPE and ACS, respectively. The application is locally defined and not specified as part of the CPE WAN Management Protocol.
RPC Methods	The specific RPC methods that are defined by the CPE WAN Management Protocol. These methods are specified in Annex A.
SOAP	A standard XML-based syntax used here to encode remote procedure calls. Specifically SOAP 1.1, as specified in [9].
HTTP	HTTP 1.1, as specified in [6].
TLS	The standard Internet transport layer security protocol. Specifically, TLS 1.2 (Transport Layer Security) as defined in [11] (or a later version). Note that previous versions of this specification referenced SSL 3.0 and TLS 1.0.
TCP/IP	Standard TCP/IP.

Tabla 1: Características de cada Protocolo

Fuente: Manual del TR-069.

2.15.2 Mecanismos de Seguridad

El protocolo TR-069 está diseñado para permitir un alto grado de seguridad en las interacciones que lo utilizan.

El Protocolo de gestión CPE WAN está diseñado para evitar manipulación de las transacciones que tienen lugar entre un CPE y ACS, proporcionar confidencialidad de estas operaciones, y permitir los distintos niveles de autenticación.

Los siguientes mecanismos de seguridad se incorporan en este protocolo:

- ✓ El protocolo soporta el uso de TLS (*Transport Layer Security*) [3] para el transporte de las comunicaciones entre el CPE y ACS. Esta transacción proporciona confidencialidad, integridad de datos, y permite certificación basada de autenticación entre el CPE y ACS.
- ✓ La capa HTTP (*Hypertext Transfer Protocol*) proporciona un medio alternativo de autenticación de CPE y ACS base de códigos secretos compartidos. Hay que considerar que el protocolo no especifica cómo los secretos compartidos son aprendidos por el CPE y ACS.

2.15.3 Componentes de la Arquitectura del TR-069

2.15.3.1 Parámetros

La Especificación Método RPC (*Remote Procedure Call*), (véase el Anexo A del manual) define un mecanismo genérico por el cual un ACS puede leer o escribir parámetros para configurar un CPE y el monitor de estado de CPE y estadísticas. Parámetros para diversas clases de CPE se definen en documentos separados. Al momento de escribir las siguientes normas definen los modelos de datos TR-069.

- ✓ TR-098: Internet Gateway Device Modelo de Datos para TR-069. [4]
- ✓ TR-104: Parámetros de Aprovisionamiento de CPE VoIP. [5]
- ✓ TR-135: Modelo de datos para un STB habilitado con TR-069. [6]
- ✓ TR-140: TR-069 Modelo de datos para dispositivos habilitados con servicios de almacenamiento. [7]
- ✓ TR-143: Activación de Pruebas de rendimiento de la red y de supervisión y estadísticas. [8]
- ✓ TR-157: Objetos componentes para CWMP. [9]
- ✓ TR-181: Modelo de datos de dispositivos para TR-069. [10] [11]

Cada parámetro se compone de un par nombre-valor. El nombre identifica el parámetro particular, y tiene una estructura jerárquica similar a los archivos de un directorio, con cada nivel separados por un "." (punto).

Los parámetros pueden ser definidos como de sólo lectura o de lectura y escritura. Los parámetros de sólo lectura pueden ser utilizados para permitir al ACS determinar las características específicas del CPE, observar el estado actual del CPE, o reunir estadísticas.

Los parámetros configurables permiten al ACS personalizar diversos aspectos del funcionamiento de la CPE. Todos los parámetros configurables también deben ser legibles aunque los que contienen información confidencial del usuario, por ejemplo, contraseñas, pueden regresar valores vacíos cuando se leen (esto se especifica en la

definición del modelo de datos correspondiente). El valor de algunos parámetros configurables pueden ser independientemente modificables a través de medios distintos de la interfaz definida en esta especificación (por ejemplo, algunos parámetros pueden ser también modificados mediante un protocolo de auto-configuración de la LAN).

Debido a que otros protocolos (así como la acción del abonado) pueden modificar de forma independiente la configuración del dispositivo, el servidor ACS no puede asumir que es el único dispositivo de modificación entidad configuración. Además, es posible que un mecanismo del lado de LAN pudiera alterar la configuración del dispositivo de tal manera que se presente un conflicto con la configuración suministrada al ACS inicialmente.

Se debe tener cuidado en la aplicación tanto de la WAN y la configuración automática del lado de los mecanismos de la LAN, así como las interfaces de abonado, es por ello, necesario limitar las instancias en esta parte.

El protocolo soporta un mecanismo de descubrimiento que permite al servidor ACS determinar cuáles parámetros dan soporte al CPE.

El protocolo también incluye un mecanismo de extensibilidad que permite el uso específico de los parámetros del proveedor, además de los definidos en esta especificación.

2.15.3.2 Transferencia de Archivos

El método específico “RPC” (hágase referencia al Anexo A del manual) el cual define los mecanismos para facilitar las transferencias de archivos para un abanico de propósitos, tales como la descarga de las actualizaciones de firmware o archivos de configuración específicos (vendorSpecific), (opcionalmente) la instalación o la actualización de los módulos de software, y (opcionalmente) la configuración de cargar o de archivos desde el dispositivo de registro.

Las transferencias de archivos se pueden realizar por medio de Unicast o Multicast (para descargas) con protocolos de transporte. El Unicast incluyen los siguientes protocolos HTTP / HTTPS, FTP, SFTP y TFTP. Los soportes para HTTP [12] / HTTPS son obligatorios, y los protocolos que no sean los señalados aquí pueden ser soportados.

Cuando una transferencia de archivo se inicia por el ACS a través de cualquiera de las llamadas a métodos que pueden causar una transferencia de Archivos, el CPE se proporciona con la ubicación del archivo (o posiblemente los archivos en el caso de un módulo de software se instalan o actualizan) para ser transferidos. El CPE a continuación, realiza la o las transferencia(s), y notifica al ACS del éxito o fracaso.

Las descargas pueden estar opcionalmente iniciadas por un CPE. En este caso, el CPE solicita primero una descarga de un determinado tipo de archivo del ACS. El servidor ACS puede entonces responder al iniciar la descarga siguiendo los mismos pasos que una descarga iniciada por ACS.

Las transferencias de archivos también pueden estar opcionalmente iniciadas por un evento externo, por ejemplo, un Multicast con anuncio de disponibilidad de firmware o actualizaciones de los módulos de software iniciadas por el usuario.

En este caso, el CPE realiza la transferencia autónoma, y notifica al ACS del éxito o fracaso.

2.15.3.3 Inicio de sesión del CPE

El método RPC (hágase referencia al Anexo A) el cual define un mecanismo que permite a un CPE informar a un ACS correspondiente de diversas condiciones, y así asegurar que el CPE y el ACS tengan comunicación con cierta frecuencia mínima. Acá se manejan los mecanismos para establecer la comunicación después de la instalación inicial del CPE para el arranque “BOOTSTRAP” [22] los primeros parámetros personalizados en el CPE. También incluye un mecanismo para establecer una comunicación periódica con el ACS de forma permanente, o cuando se producen

eventos que deben ser reportados al ACS (como cuando la dirección IP de banda ancha ha sufrido modificaciones en el CPE).

En cada caso, se establece la comunicación cuando el CPE se identifica de forma única a través del fabricante y el número de serie (y opcional el identificador único de clase de producto “Manufacturer OUI” [17]) para que el ACS reconozca que el CPE se está comunicando con él y pueda responder de forma adecuada.

2.15.3.4 Sesiones Asíncrona Iniciadas por el ACS

Un aspecto importante del servicio de configuración automática es la capacidad del servidor ACS para informar al CPE de un cambio en la configuración de forma asíncrona. Esto permite que la configuración automática, trabaje como un mecanismo para los servicios que requieren reconfiguración en tiempo casi real de la CPE. Por ejemplo, esto puede ser usado para proporcionar a un usuario final con el acceso inmediato a un servicio o característica que hayan suscrito, sin esperar al próximo contacto periódico.

El mecanismo básico definido en el Protocolo CPE WAN para permitir una sesión asíncrona del servidor ACS inicia cuando la comunicación se asume con el direccionamiento IP directa del CPE de la ACS.

2.16 Estructura de Normas TR-069

Bajo el protocolo TR-069 se ejecutan unas series de normas para el correcto funcionamiento entre los dispositivos CPEs y el ACS que se manejen, estas normas están desarrolladas en documentos individuales ya que cada uno cumple una tarea distinta.

A continuación, se presenta una tabla que denota la norma (numeración) y la tarea que desempeña.

TR-XXX	ASOCIACIÓN	
TR-098	for Internet Gateways Devices	Dispositivos con puerta de enlace a Internet
TR-104	for VOIP gateways	Puertas de enlaces VOIP
TR-106	for digital home devices	Dispositivos digitales del hogar
TR-110	for VOIP configurations	Configuración VOIP
TR-111	for LAN/NAT devices	Dispositivos LAN/WAN
TR-131	for NBI "Northbound Interface"	NBI Interfaz en dirección norte
TR-135	for STB/Video	Set to box / Video
TR-140	for Network Storage	Almacenamiento de red
TR-142	for PON Devices	Dispositivos PON
TR-143	Enabling Network Throughput Performance Test and Statistical Monitoring	Habilitación de la red para prueba de rendimiento y seguimiento estadístico
TR-156	for GPON access	Dispositivos GPON
TR-157	SW Module Management	Modulo Software de Gestión
TR-181	Device Data Model	Datos Modelo del dispositivo

Tabla 2: Estructura de normas TR-069

En esta parte del informe se hará una breve descripción de lo que abarca cada norma, resaltando sus características y cualidades más resaltantes.

2.16.1 TR-098 for Internet Gateways Devices

Para los nombres de parámetros (*Parameter Names*) se usa una forma jerárquica similar a un árbol de directorios. El nombre de un parámetro en particular es representado por la concatenación de cada nodo sucesivo en la jerarquía separados por un "." (punto), comenzando en el tronco de la jerarquía y que lleva a las hojas. Al especificar una ruta parcial, lo que se indica es un nodo intermedio en la jerarquía, "." (punto) se utiliza siempre como el último carácter.

Todas las direcciones IP y las máscaras de subred se representan como cadenas en IPv4 utilizando la notación decimal punteada.

Todas las direcciones MAC se representan como cadenas de 12 dígitos hexadecimales (dígitos 0-9, letras A-F o a-f) y se muestran como seis pares de dígitos separados por dos puntos.

Un proveedor puede ampliar la lista de parámetros estandarizados con parámetros y objetos específicos del fabricante, (*vendorSpecific parameters*) y los objetos pueden ser definidos en una jerarquía de nombres separado o dentro de la jerarquía de nomenclatura estándar.

El nombre de un parámetro específico del proveedor o el objeto debe tener la forma:

X_ <vendor> _VendorSpecificName

En esta definición <vendor> es un identificador exclusivo del fabricante, que puede ser un OUI o un nombre con dominio. Un OUI [17] es un identificador único asociado a un fabricante u organización que tiene formato con cadena de dígitos en hexadecimal con todas las letras en mayúsculas e incluyendo los ceros iniciales. Un nombre de dominio debe estar en mayúsculas con cada punto (".") sustituido por un guión normal. En la siguiente tabla 3, se muestra una parte de esta norma donde se muestran los principales objetos definidos para el Internet Gateway Device:

Name ¹	Type	Write ²	Description	Default ³
InternetGatewayDevice	object	-	The top-level object for an Internet Gateway Device.	-
DeviceSummary	string(1024)	-	As defined in [3].	-
LANDeviceNumberOfEntries	unsignedint	-	Number of instances of LANDevice.	-
WANDeviceNumberOfEntries	unsignedint	-	Number of instances of WANDevice.	-
InternetGatewayDevice.DeviceInfo	object	-	This object contains general device information.	-
Manufacturer	string(64)	-	The manufacturer of the CPE (human readable string).	-
ManufacturerOUI	string(6)	-	Organizationally unique identifier of the device manufacturer. Represented as a six hexadecimal-digit value using all upper-case letters and including any leading zeros. The value MUST be a valid OUI as defined in [5].	-
ModelName	string(64)	-	Model name of the CPE (human readable string).	-
Description	string(256)	-	A full description of the CPE device (human readable string).	-
ProductClass	string(64)	-	Identifier of the class of product for which the serial number applies. That is, for a given manufacturer, this parameter is used to identify the product or class of product over which the SerialNumber parameter is unique.	-
SerialNumber	string(64)	-	Serial number of the CPE.	-
HardwareVersion	string(64)	-	A string identifying the particular CPE model and version.	-
SoftwareVersion	string(64)	-	A string identifying the software version currently installed in the CPE. To allow version comparisons, this element SHOULD be in the form of dot-delimited integers, where each successive integer represents a more minor category of variation. For example, 3.0.21 where the components mean: Major.Minor.Build.	-
ModemFirmwareVersion	string(64)	-	A string identifying the version of the modem firmware currently installed in the CPE. This is applicable only when the modem firmware is separable from the overall CPE software.	-
EnabledOptions	string(1024)	-	Comma-separated list of the OptionName of each Option that is currently enabled in the CPE. The OptionName of each is identical to the OptionName element of the OptionStruct described in [2]. Only those options are listed whose State indicates the option is enabled.	-
AdditionalHardwareVersion	string(64)	-	A comma separated list of any additional versions. Represents any additional hardware version.	-

Tabla 3: TR-098

Los requisitos de notificación y informes vienen dados como la muestra la siguiente la tabla 4:

Parameter
InternetGatewayDevice.DeviceSummary
InternetGatewayDevice.DeviceInfo.SpecVersion
InternetGatewayDevice.DeviceInfo.HardwareVersion
InternetGatewayDevice.DeviceInfo.SoftwareVersion
InternetGatewayDevice.DeviceInfo.ProvisioningCode
InternetGatewayDevice.ManagementServer.ConnectionRequestURL
InternetGatewayDevice.ManagementServer.ParameterKey
InternetGatewayDevice.WANDevice.{j}.WANConnectionDevice.{j}.WAN{""}Connection.{k}.ExternalIPAddress ⁸

Tabla 4: Parámetros TR-098

La definición de los perfiles está más detallada en el documento:

<http://www.broadband-forum.org/technical/download/TR-098.pdf> [4]

2.16.2 TR-104 for VoIP Gateways

Esta especificación define el modelo de datos para el aprovisionamiento de un (VoIP) dispositivo de voz sobre IP CPE por un servidor ACS Auto-Configuration Server mediante el mecanismo definido en el TR-069.

La figura 6, muestra la estructura del objeto completo para el servicio *VoiceService*.

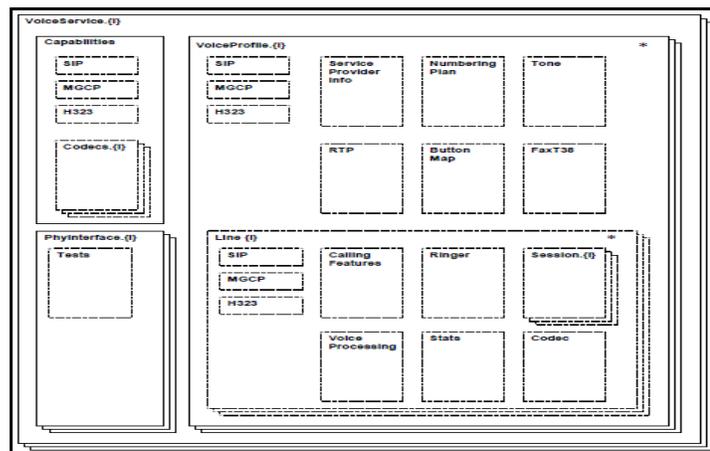


Figura 6: Estructura TR-104

En la siguiente tabla 5 se muestra una parte de esta norma donde se muestran los principales objetos definidos para una pasarela VoIP:

Name ¹	Type	Write ²	Description	Default ³
.VoiceService.{}	object	-	The top-level object for VoIP CPE.	-
VoiceProfileNumberOfEntries	unsignedInt	-	Number of instances of VoiceProfile.	-
.VoiceService.{}.Capabilities	object	-	The overall capabilities of the VoIP CPE.	-
MaxProfileCount	unsignedInt	-	Maximum total number of distinct voice profiles supported.	-
MaxLineCount	unsignedInt	-	Maximum total number of lines supported across all profiles. This parameter is applicable only for a VoIP endpoint.	-
MaxSessionsPerLine	unsignedInt	-	Maximum number of voice sessions supported for any given line across all profiles. A value greater than one indicates support for CPE provided conference calling. This parameter is applicable only for a VoIP endpoint.	-
MaxSessionCount	unsignedInt	-	Maximum total number of voice sessions supported across all lines and profiles. (This might differ from MaxLineCount if each line can support more than one session for CPE provided conference calling. This value MAY be less than the product of MaxLineCount and MaxSessionsPerLine.)	-
SignalingProtocols	string(256)	-	Comma-separated list of signaling protocols supported. Each item is an enumeration of: "SIP" "MGCP" "MGCP-NCS" "H.248" "H.323" Each entry MAY be appended with a version indicator in the form "X.Y". For example: "SIP/2.0" The list MAY include vendor-specific protocols, which MUST be in the format defined in [3]. For example: "X_EXAMPLE-COM_MyProf"	-
Regions	string(256)	-	Comma-separated list of geographic regions supported by the CPE. Each item in the list MUST be an alpha-2 (two-character alphabetic) country code as specified by ISO 3166.	-

Tabla 5: VoIP Gateways

La definición de los perfiles está más detallada en el documento:

<http://www.broadband-forum.org/technical/download/TR-104.pdf> [5]

2.16.3 TR-106 para Dispositivos Digitales del Hogar

TR-106 especifica una estructura de objetos de línea de base y un conjunto de parámetros de TR-069-accesibles a estar disponible en cualquier dispositivo habilitado con TR-069.

La capacidad de gestionar una red casera de forma remota tiene una serie de beneficios como la reducción de los costes asociados con la activación y el apoyo de

servicios de banda ancha, la mejora de tiempo de salida al mercado de nuevos productos y servicios, y la mejora de la experiencia del usuario.

Para un dispositivo en particular, se espera que la línea de base definida en TR-106 sería aumentada con objetos adicionales y parámetros específicos para el tipo de dispositivo. El modelo de datos utilizado en cualquier dispositivo TR-069 es capaz de seguir las directrices que se describen en esta norma. Estas directrices incluyen los siguientes aspectos:

- ✓ Necesidades estructurales para la jerarquía de datos.
- ✓ Los requisitos para el control de versiones de los modelos de datos.
- ✓ Requisitos para la definición de los perfiles.
- ✓ Un conjunto de objetos de datos comunes.
- ✓ Un perfil de línea de base para cualquier dispositivo que soporte estos objetos de datos comunes.

El TR-106 también define un esquema XML (*Xtensible Markup Language*) [13] que permite a un dispositivo, describir sus modelos de datos TR-069 compatibles.

Esta descripción es específica y detallada, lo que permite al ACS saber exactamente lo que soporta el dispositivo, incluyendo los objetos y los parámetros específicos del proveedor. El uso de este esquema mejora la interoperabilidad y facilita considerablemente la integración de los nuevos dispositivos con el ACS.

En la tabla a continuación (tabla 6) se presenta un resumen de los objetos de datos comunes que se definen en esta norma:

Object Name	Allowed Location in Hierarchy	Description
Capabilities	Root and Service Objects	Device capabilities.
DeviceInfo	Root and Service Objects	General information about the device, including its identity and version information.
ManagementServer	Root	Parameters associated with the communication between the CPE and an ACS.
GatewayInfo	Root	Information to identify an Internet Gateway Device through which the CPE is connected.
Time	Root and Service Objects	Parameters associated with an NTP or SNTP time client on the CPE.
Config	Root and Service Objects	Contains general configuration state.
UserInterface	Root and Service Objects	Parameters related to the user interface of the CPE.
LAN	Root and Service Objects	Parameters related to IP-based LAN connectivity of the CPE.

Tabla 6: Object Name – TR-106

La definición de los perfiles está más detallada en el documento:

http://www.broadband-forum.org/technical/download/TR-106_Amendment-3.pdf

[14]

2.16.4 TR-110 para Configuraciones VoIP

Esta norma resalta la importancia de la tecnología VoIP sobre ADSL, la adopción cada vez mayor de servicios de DSL para internet de alta velocidad, tiene dado lugar a un mercado por el que muchos usuarios finales tienen ahora suficiente ancho de banda para apoyar Voz sobre IP (VoIP).

Este norma ilustra y describe los modelos de referencia para configuraciones de VoIP y la operación continua de voz.

MODELOS DE REFERENCIA PARA CONFIGURACIONES VOIP

- ✓ Adaptador de Telefonía analógica. Standalone ATA (Analog Telephone Adapter)
- ✓ Teléfonos VoIP, Native IP Phone
- ✓ Software VoIP sobre PC, Typical PC Softphone
- ✓ Pasarela remota con funcionalidad ATA (Remote Gateway), RG with Embedded ATA Functionality

La definición y arquitectura para modelo de referencia está más detallada en el documento:

<http://www.broadband-forum.org/technical/download/TR-110.pdf> [15]

2.16.5 TR-111 para Dispositivos LAN/NAT

Esta norma específica dos mecanismos que amplían el protocolo de administración WAN CPE que se define como el TR-069 para mejorar la capacidad de gestionar de forma remota los dispositivos que están conectados a través de una LAN a través de un Gateway de Internet.

Estos mecanismos son:

1) Dispositivo (Pasarela Asociada)

Permite que un ACS gestione cualquier dispositivo, para identificar la puerta de entrada (gateway) asociada a través del cual, dicho dispositivo está conectado.

Esta capacidad podría ser necesaria, cuando el ACS establece QoS (*Quality of Service*) para un servicio en particular que puede necesitar a disposición ambos componentes, tanto el dispositivo, así como la puerta de enlace a través del cual está conectado dicho dispositivo. El ACS tendría que determinar la identidad de esa puerta de enlace particular.

Los procedimientos de asociación “Device Gateway” se resumen de la siguiente manera:

✓ Un dispositivo después de esta especificación pasará su identidad de dispositivos por la puerta de enlace a través de un proveedor específico como DHCP (Dynamic Host Configuration Protocol) [16]. Cuando la puerta de enlace recibe esta información, se rellena una tabla que contiene la información de identidad para cada

dispositivo en la LAN. Esta información se pondrá a disposición del ACS a través de una extensión al modelo de datos de la puerta de enlace.

✓ En las respuestas de DHCP, la puerta de enlace proporciona el dispositivo con su puerta de enlace de identidad, que el dispositivo pone a disposición del ACS a través del objeto de datos denominado “GatewayInfo”. El dispositivo notifica al ACS de los cambios en el contenido de este objeto. Así, un dispositivo que se conecta a una previamente puerta de enlace desconocida dará lugar al ACS para notificar la puerta de enlace de identidad.

✓ Para asegurar la validez de esta información, que se realiza a través de un intercambio de DHCP inherente, el ACS debe validar la identidad de la puerta de enlace proporcionada por el dispositivo, con la confrontación de la identidad de dispositivo proporcionado por la pasarela.

REQUERIMIENTOS PARA PASARELA O PUERTA DE ENLACE

Una puerta de enlace (Gateway) conforme a esta especificación deberá inspeccionar todas las peticiones DHCP recibidas en una interfaz LAN y determinar si el dispositivo solicitante ha incluido la identidad de dispositivo en la solicitud. Una solicitud de DHCP tiene que incluir la identidad del dispositivo si contiene una información de opción “DHCP VI Vendor-Specific (número de opción 125)”, que incluye la información de identidad del dispositivo. Las peticiones DHCP para los que se aplica este requisito son las siguientes: DHCPDISCOVER, DHCPREQUEST, y DHCPINFORM.

REQUERIMIENTOS PARA EL DISPOSITIVO

Una solicitud de DHCP tiene que incluir la identidad del dispositivo si contiene una información de opción “DHCP VI Vendor-Specific (número de opción 125)”, que incluye la información de identidad del dispositivo.

Las peticiones DHCP para los que se aplica este requisito son las siguientes: DHCPDISCOVER, DHCPREQUEST, y DHCPINFORM.

Si el mensaje DHCPACK incluye la identidad de la pasarela (Gateway Identity Carried) en el “VI Vendor-Specific Opción Información DHCP (opción número 125)”, el dispositivo debe registrar el valor recibido en el objeto de datos “*GatewayInfo*” con todos estos valores de registro:

- ✓ Device.GatewayInfo.ManufacturerOUI [17]
- ✓ Device.GatewayInfo.SerialNumber
- ✓ Device.GatewayInfo.ProductClass

Las respuestas de DHCP para los que se aplica este requisito son las siguientes: DHCPPOFFER y DHCPACK.

Si alguno de los elementos de la identidad de la pasarela (*Gateway Identity*) no están presentes en el VI Vendor-Specific Opción Información DHCP, el dispositivo debe grabar una cadena vacía para cada artículo (reemplazando el valor anterior, si los hay).

Para todos los parámetros del “*Device.GatewayInfo object*”, el dispositivo por defecto una notificación con atributos como notificación activa. El dispositivo debe aplicar esta por defecto siempre que la dirección URL del ACS quede activa o sea modificada posteriormente.

Siempre que este activa la notificación está habilitada para estos parámetros, el dispositivo debe notificar de forma activa al ACS, si el valor de cualquiera de estos parámetros cambia. Si la concesión DHCP es liberada o expira sin ser renovado, todas las entradas para “*GatewayInfo object*”, debe ser descartadas (ajustada a la cadena vacía).

REQUERIMIENTOS PARA ACS

Cada vez que un dispositivo está asociado a una puerta de enlace, el dispositivo le notificará al ACS, proporcionando la nueva información de puerta de enlace de identidad.

Cuando esto ocurre, el ACS debe hacer lo siguiente:

- ✓ Si el ACS ha asociado previamente el dispositivo con una puerta de enlace, el ACS debe examinar la puerta de enlace de identidad del dispositivo (desde el “GatewayInfo object”) y compararlo con la puerta de enlace identidad de la asociación anterior. Si la asociación no se ha modificado, la ACS no necesita tomar ninguna nueva medida.
- ✓ Si la puerta de enlace de identidad desde el dispositivo es diferente de la identidad de la puerta de enlace previamente asociado con el dispositivo, o si no hubo asociación anterior puerta de enlace para el dispositivo, entonces, el ACS debe primero validar la información proporcionada por el dispositivo, y si se valida, se actualiza la asociación Device-Gateway para indicar la nueva puerta de enlace de identidad.

ASOCIACIÓN DE FLUJO (*DEVICE-GATEWAY*)

La figura 7, muestra el flujo asociado con los procedimientos de asociación del dispositivo de puerta de enlace, en el que el dispositivo utiliza un mensaje de “DHCP Discover” para iniciar la asociación como parte de la asignación de direcciones DHCP.

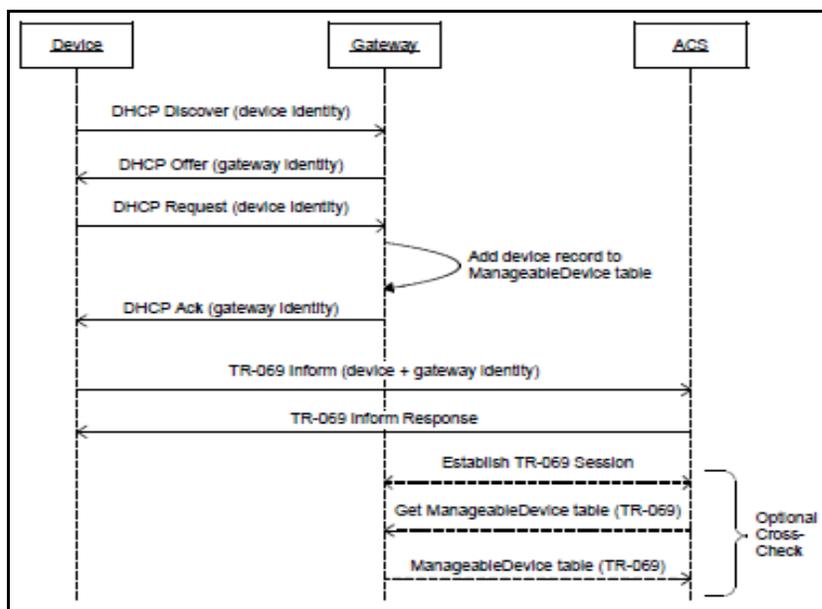


Figura 7: Asociación de flujo TR-111

2) De solicitud de conexión a través de puerta de enlace NAT

Permite que un ACS inicie una sesión TR-069 con un dispositivo que opera detrás de una puerta de enlace NAT.

Para dar cabida a la capacidad de un ACS para emitir una solicitud de conexión TR-069 a un CPE asignado, con una dirección privada a través de una puerta de enlace NAT, es indispensable lo siguiente:

- ✓ El CPE debe ser capaz de descubrir que su conexión con el ACS es a través de una puerta de enlace NAT que tiene asignada una dirección IP privada a la CPE.
- ✓ El CPE debe ser capaz de mantener un vínculo abierto de NAT, mediante el cual el ACS puede enviar paquetes no solicitados.
- ✓ El CPE debe ser capaz de determinar la dirección IP pública.

La definición y arquitectura para modelo de referencia está más detallada en el documento:

<http://www.broadband-forum.org/technical/download/TR-111.pdf> [18]

2.16.6 TR-131 para interfaz NBI (Northbound Interface Requirements)

Esta norma define los requisitos para una interfaz NBI para un ACS que permite sistemas de apoyo al negocio operacional y para acceder a la funcionalidad del ACS. Estos requisitos son derivados de un conjunto de casos de gestión de dispositivos y el uso de la gestión del servicio. La siguiente figura ilustra la relación entre un ACS y diversos sistemas:

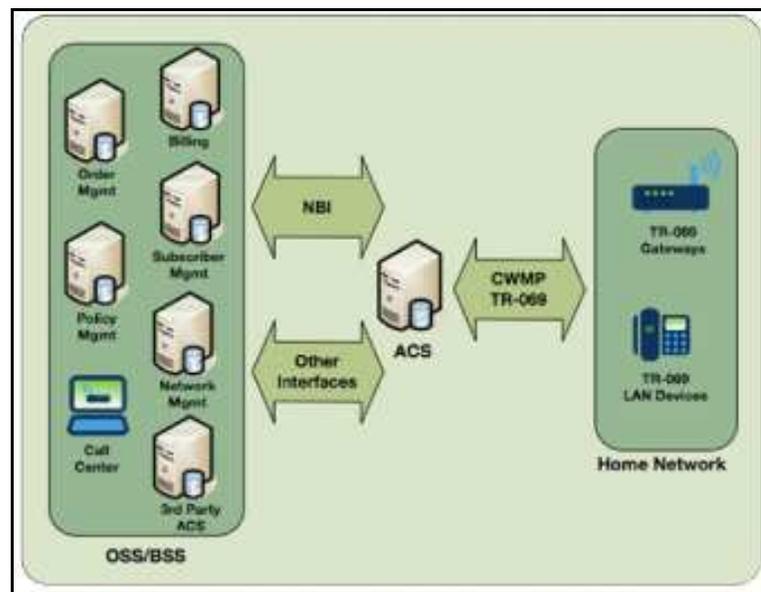


Figura 8: Modelo TR-131

El propósito principal de toda NBI es proporcionar una interfaz para comunicarse con la dirección operacional y sistemas de apoyo a las empresas en el ACS, para el aprovisionamiento y la gestión de todos los dispositivos. También proporciona una infraestructura de mensajería para permitir la comunicación de diversos eventos de operaciones y negocios de sistemas de apoyo. Los dispositivos administrados por el ACS podrían incluir las implementaciones del “InternetGatewayDevice (IGD)”.

Los requisitos de NBI no están destinados a cubrir todas las interfaces entre las operativas y de sistemas de apoyo de negocio y del ACS. Por ejemplo, la definición

de la configuración estática de los sistemas de ACS o ACS GUI (Graphical User Interface) esta fuera del alcance de esta norma.

La definición y arquitectura para modelo de referencia está más detallada en el documento:

<http://www.broadband-forum.org/technical/download/TR-131.pdf> [19]

2.16.7 TR-140 para Almacenamiento en Red

La presente norma, da servicio para el almacenamiento de datos de dispositivos, ésta permite el control remoto de la gestión de los dispositivos de almacenamiento a través del servicio CWMP. Cubre el modelo de datos para describir el servicio de almacenamiento de un dispositivo, así como las normas relativas a notificaciones de cambio de valor de parámetro. Casos de uso general también se describen incluyendo perfiles estándar de modelo de datos que normalmente se ven mientras que la gestión remota un dispositivo sea de esta naturaleza.

Los objetivos de esta memoria descriptiva son como sigue:

- ✓ Habilitar la resolución de problemas y la configuración remota de los dispositivos de almacenamiento de servicio de un ACS.
- ✓ Admitir dispositivos de servicio de almacenamiento que están incrustados ya sea como parte de un dispositivo de puerta de enlace de Internet, o un dispositivo independiente.

La figura 9, representa la estructura del objeto StorageService. Esta imagen ofrece una visión general de alto nivel de los diferentes objetos que existen en este modelo de datos y la forma en que se asocian.

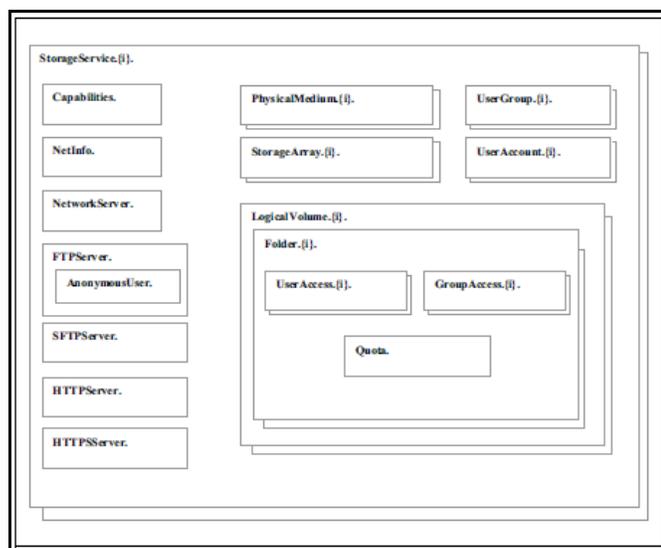


Figura 9: Estructura TR-140

La definición y arquitectura para modelo de referencia está más detallada en el documento:

<http://www.broadband-forum.org/technical/download/TR-140.pdf> [7]

2.16.8 TR-142 para Dispositivos PON

El objetivo de esta norma es proporcionar un marco para la configuración remota y gestión de los servicios de acceso PON (Passive Optical Network) sobre óptica pasiva.

Es importante resaltar que los protocolos (PLOAM, OMCI, G-OMCI, 802.3ah) sólo se utilizan en entre el OLT y el ONT, como se muestra en la figura 10. En cambio, la figura 11 muestra que TR-069 es transparente para la OLT y está directamente conectado al ACS, pero este a su vez está conectado con el ONT y los otros puntos con la red doméstica.

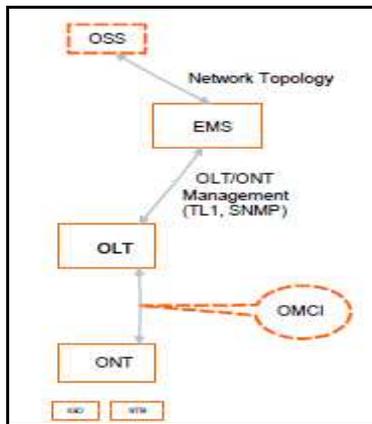


Figura 10: OLT y ONT

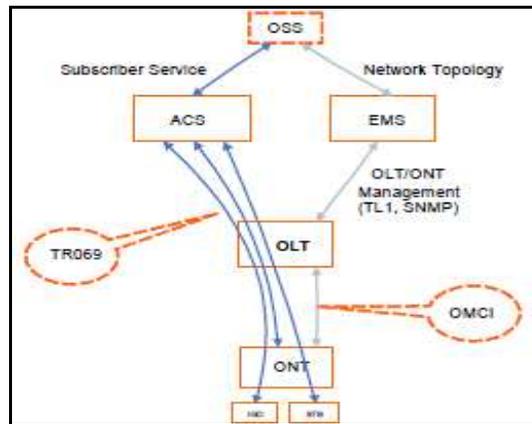


Figura 11: Transparencia de TR-069

La definición y arquitectura para modelo de referencia está más detallada en el documento:

<http://www.broadband-forum.org/technical/download/TR-142.pdf> [20]

2.16.9 TR-143 para Pruebas de Rendimiento de la Red y de Supervisión y Estadísticas

Esta norma define un conjunto de pruebas de vigilancia activa que pueden ser aprovechadas por los proveedores de servicios de red para monitorear y / o diagnosticar el estado de su banda ancha y rutas de red que sirven a poblaciones de los abonados que utilizan CPE compatibles. Con la opción TR-069 de Monitoreo Activo admite los diagnósticos iniciados por la red (*Network Initiated Diagnostic*) o por (*CPE Initiated Diagnostics*) para el seguimiento y la caracterización de los caminos de servicio, ya sea en forma continua o bajo demanda. Estas herramientas genéricas proporcionan una plataforma para la validación de objetivos QoS y acuerdos de nivel de servicio.

Las pruebas de diagnóstico no están diseñadas para funcionar en paralelo y sus resultados se basan en el tráfico normal que ocurre en el enlace y la utilización de cualquier ancho de banda restante. Múltiples pruebas puede consumir el exceso de

ancho de banda y los resultados son sesgados. El tráfico de monitoreo activo puede ser generado a partir de un CPE o un punto final de la red del servidor de prueba. La figura 12, es un marco conceptual diagrama para ilustrar esto.

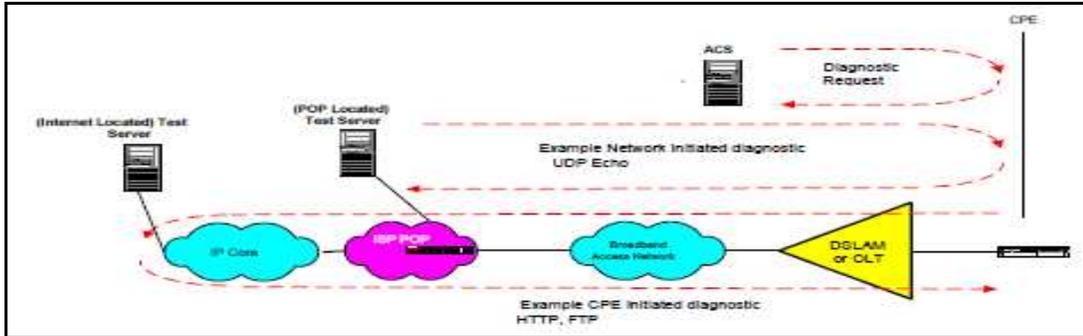


Figura 12: Componentes para la prueba de rendimiento

Diagnósticos “CPE iniciado”

El ACS inicia la petición DownloadDiagnostics al CPE, estableciendo parámetros de prueba y el inicio de la prueba. El CPE inicia el diagnóstico (FTP o transacción del cliente HTTP), y almacena los resultados de las pruebas. Una prueba de servidor de red responde al diagnóstico (FTP o HTTP) a través de un servidor HTTP / FTP.

En la Figura 13, es un diagrama de ejemplo de un “DownloadDiagnostics” utilizando una dirección URL HTTP.

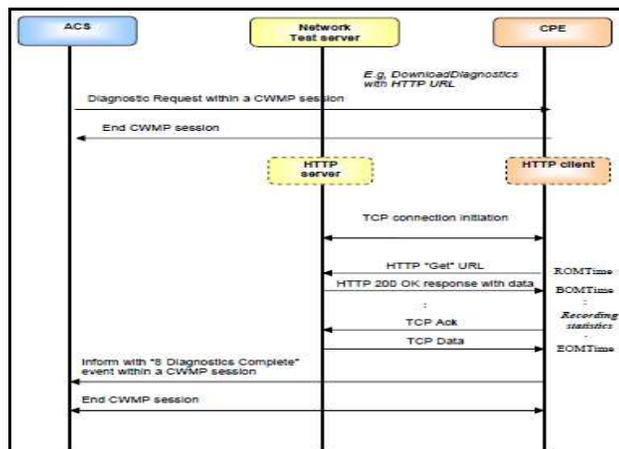


Figura 13: DownloadDiagnostics CPE usando HTTP Transport.

La definición y arquitectura para modelo de referencia está más detallada en el documento:

<http://www.broadband-forum.org/technical/download/TR-143.pdf> [8]

2.16.10 TR-156 para Acceso GPON

Esta norma tiene por objeto proporcionar la base arquitectónica y requisitos técnicos, además de los especificados en TR-101, que se necesitan para implementar correctamente los nodos de acceso GPON (Gigabit- Capable PON), ya sea de forma independiente o junto con otros tipos TR-101 de nodo de acceso.

La norma esboza una red de agregación Ethernet basada en el contexto de TR-101, pero mientras que en TR-101 se detalla una arquitectura para soportar nodos de acceso DSL, esta norma desarrolla la arquitectura de nodos de acceso que incluyen la terminación de línea óptica GPON (OLT) y la terminación de red óptica (ONU / ONT).

Se basa en los modelos arquitectónicos / topológicos de la red de agregación basados en Ethernet y escenarios de despliegues DSL definidos en TR-101, incluyendo en la red de banda ancha la puerta de enlace (BNG), el agregador Ethernet (Ethernet Aggregation), el nodo de acceso (AN), y la pasarela residencial (RG). Además, se sigue apoyando los requerimientos de negocios de TR-058 y TR-102.

Al hacerlo, se describe cómo agregar nodos de acceso GPON así como nodos de acceso híbrido con combinaciones de GPON y DSL en la arquitectura TR-101.

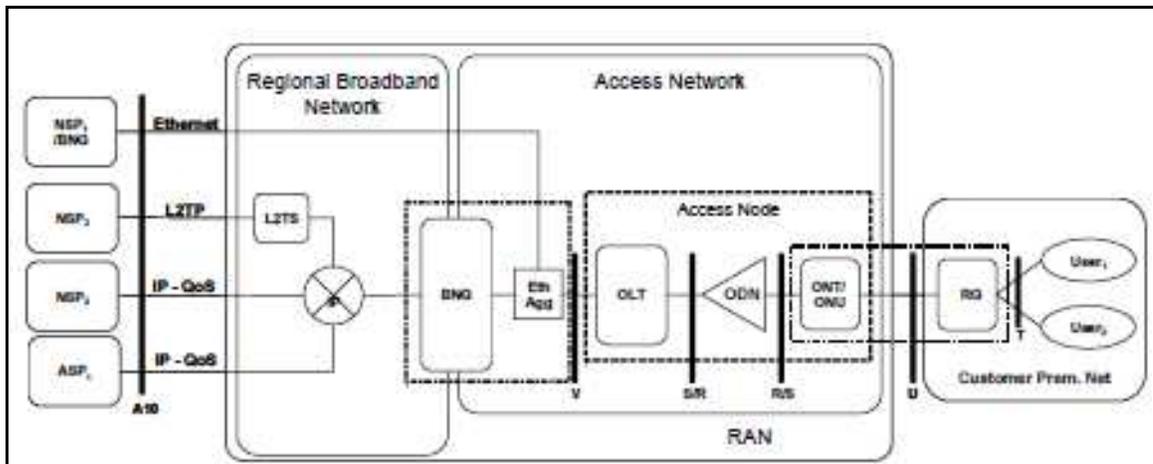


Figura 14: Estructura TR-156

La definición y arquitectura para modelo de referencia está más detallada en el documento:

<http://www.broadband-forum.org/technical/download/TR-156.pdf> [21]

2.16.11 TR-157 para Objetos Componentes para CWMP

El propósito de esta norma es proporcionar objetos de equipo para el TR-069.

Un objeto componente se define como un objeto y sus parámetros contenidos destinados a utilizar en cualquier modelo aplicable CWMP para raíz de datos (tanto de dispositivos y InternetGatewayDevice). Los objetos puede residir en el nivel superior o en un nivel sub-objeto apropiado.

Ejemplo de incluir un object en nivel top:

- ✓ *Device.NSlookupDiagnostics.*
- ✓ *InternetGatewayDevice.NSlookupDiagnostics.*

Ejemplo de incluir un object con uno ya definido:

- ✓ *Device.DeviceInfo.MemoryStatus.*
- ✓ *InternetGatewayDevice.DeviceInfo.MemoryStatus*

Name	Type	Write	Description	Object Default
UserNumberOfEntries	unsignedInt	-	Number of entries in the User table.	-
SmartCardReaderNumberOfEntries	unsignedInt	-	Number of entries in the SmartCardReader table.	-
.DeviceInfo.	object	-	This object contains general device information.	-
.DeviceInfo.MemoryStatus.	object	-	Status of the device's volatile physical memory.	-
Total	unsignedInt	-	The total physical RAM, in <i>kilobytes</i> , installed on the device.	-
Free	unsignedInt	-	The free physical RAM, in <i>kilobytes</i> , currently available on the device.	-
.DeviceInfo.ProcessStatus.	object	-	Status of the processes on the device.	-
CPUUsage	unsignedInt [:100]	-	The total amount of the CPU, in <i>percent</i> , rounded up to the nearest whole <i>percent</i> . In the case that multiple CPU are present, this value represents the average of all CPU.	-
ProcessNumberOfEntries	unsignedInt	-	Number of entries in the Process table. Since a Process can come and go very quickly, the CPE SHOULD place a locally specified limit on the frequency at which it will notify the ACS of value changes, as described in TR-069a2[1] Section 3.2.1.	-
.DeviceInfo.ProcessStatus.Process.{i}.	object	-	List of all processes running on the device. At most one entry in this table can exist with a given value for <i>PID</i> .	-
PID	unsignedInt	-	The Process Identifier.	-
Command	string(256)	-	The name of the command that has caused the process to exist.	-
Size	unsignedInt	-	The size in <i>kilobytes</i> of the memory occupied by the process.	-

Tabla 7: Definiciones de Parámetros de Objetos de Componentes

La definición y arquitectura para modelo de referencia está más detallada en el documento:

<http://www.broadband-forum.org/technical/download/TR-157.pdf> [9]

2.16.12 TR-181 para Modelo de Datos de Dispositivos

El presente modelo se compone de un conjunto de objetos de datos que cubre detalles como la información básica del dispositivo, la configuración de hora del día, interfaz de red y configuración de la pila de protocolo, la expedición y la reducción de la administración, las estadísticas de rendimiento, y pruebas de diagnóstico. También define un perfil de referencia que especifica un nivel mínimo de modelo de datos apoyo. La Figura 15 ilustra la estructura del modelo de datos. Figura 16, Figura 17, y la Figura 18 ilustrar la estructura del modelo de datos con mayor detalle.

- Los objetos de interfaz se identifican mediante un motivo de fondo "discontinua".
- Los objetos que hacen referencia a objetos de interfaz se indican con una trama de fondo "de puntos".

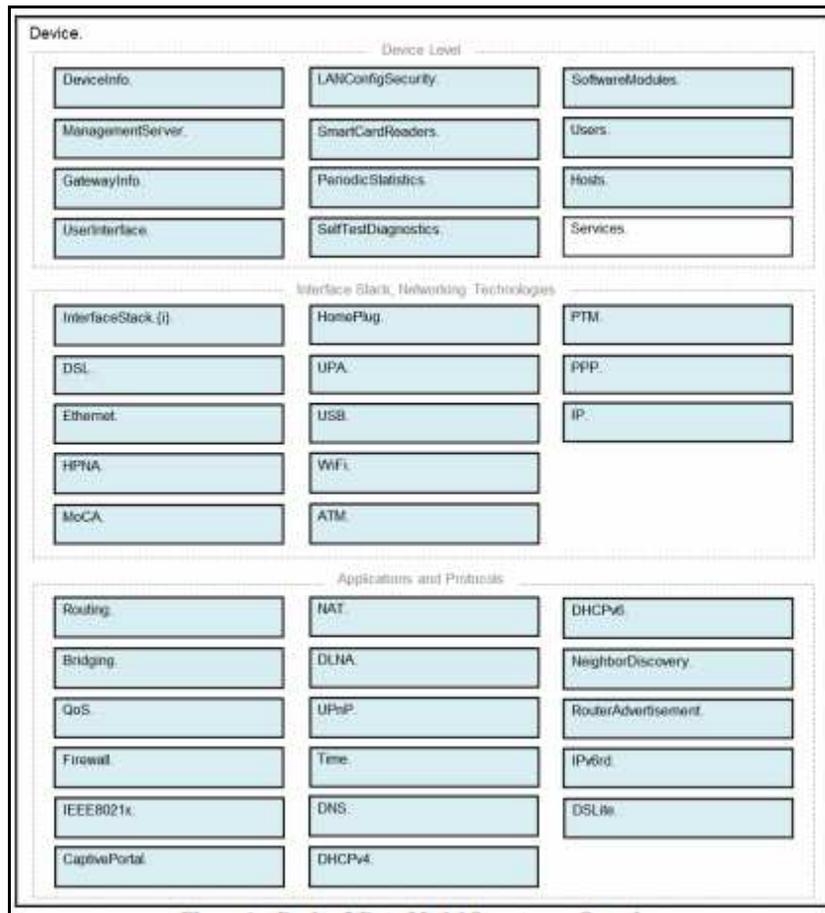


Figura 15: Modelo de datos TR-181

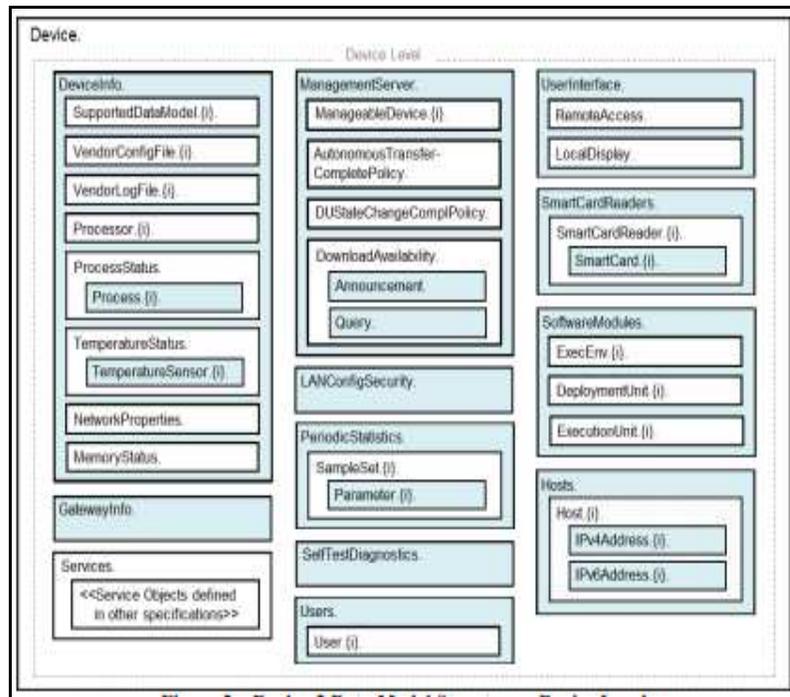


Figura 16: Modelo de datos (1) TR-181

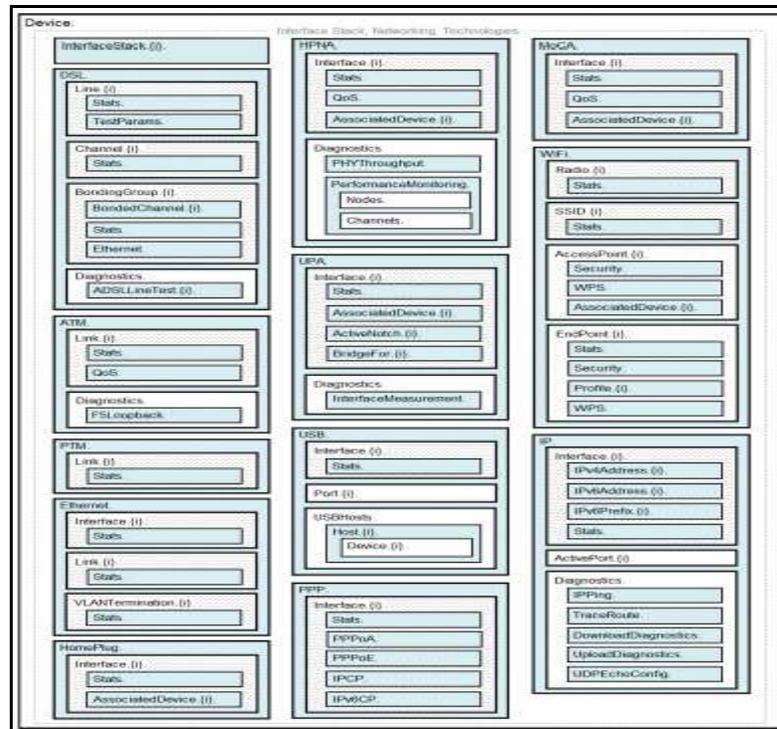


Figura 17: Modelo de datos (2) TR-181

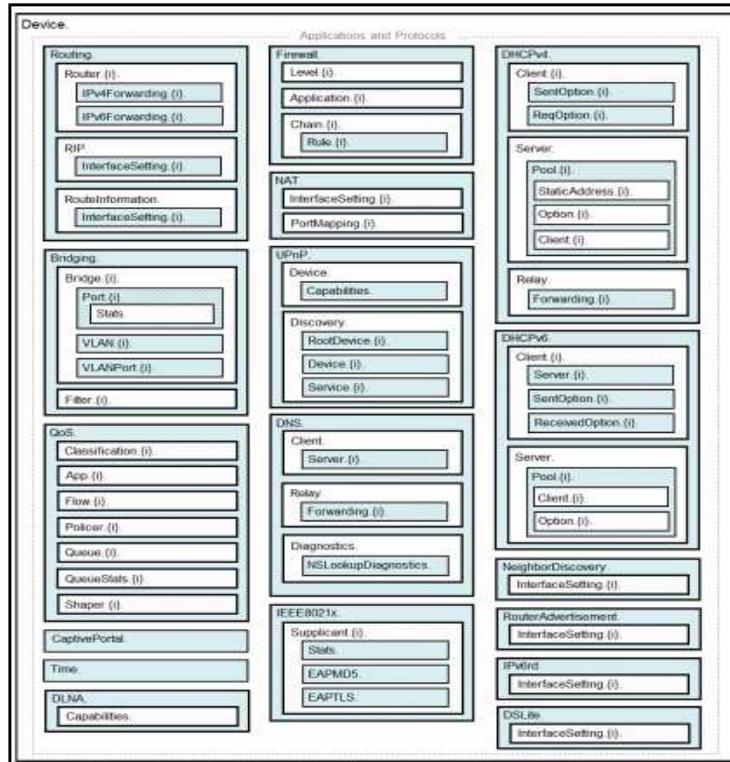


Figura 18: Modelo de datos (3) TR-181

CAPITULO III

3. RED ACTUAL PARA EL SERVICIO ADSL/ADSL2X Y PLATAFORMA DE GESTIÓN REMOTA DE FRIENDLY TECHNOLOGIES

3.1 Arquitectura de red de CANTV

De acuerdo a la Gerencia de Arquitectura de Redes y Sistemas, la cual esta adjunta a la Gerencia de Planificación (2014), de CANTV, la integración existente en las redes fijas incorporan todos los servicios de datos y voz a lo largo de toda Venezuela, entre los cuales se incluyen a la telefonía pública, internet y video.

Entre dichas redes están:

1. Red Pública de Voz (PSTN).
2. Red ATM-FR.
3. Red MetroEthernet.
4. Backbone IP
5. Red de Datos Dedicada (RD CD).
6. Redes de Transporte Urbana e Interurbanas.

La red IP de banda ancha es la que está relacionada directamente al servicio de internet, y tiene tres niveles de desempeño: la Red de Acceso a Banda Ancha, la Red Metro-Ethernet y el Backbone IP en base a diversos proveedores.

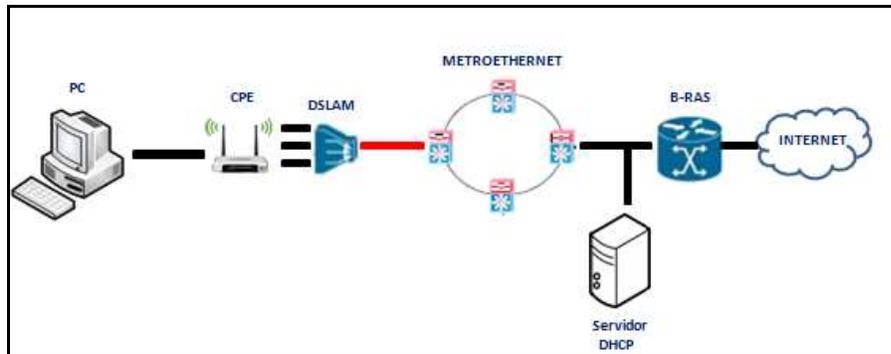


Figura 19: Red IP de Banda Ancha de CANTV.

3.2 Red de Acceso de Banda Ancha

Acá es donde radica el punto de partida del desarrollo para este trabajo especial de grado, ya que dicha red de acceso se encuentra fundamentada en la tecnología ADSL y trabaja sobre dos tipos de multiplexores de línea de acceso de abonado digital, mejor conocidos o denominados DSLAM (Digital Subscriber Line Access Multiplexer), los tipos son ATM y IP. Estos DSLAM sirven como nodos de acceso que concentran y agregan conexiones de los usuarios sobre la tecnología ADSL.

3.2.1 Dispositivos que Conforman la Red de Acceso de Banda Ancha

3.2.1.1 CPE (Equipo en los Predios del Usuario – Customer Premises Equipment)

De manera general, es un dispositivo de telecomunicaciones usado tanto en interiores como exteriores para originar, encaminar o terminar una comunicación. El dispositivo puede manejar un abanico de servicios tales como voz, video y datos. Para este caso del proyecto, el CPE está representado por el módem.

3.2.1.2 DSLAM (Digital Subscriber Line Access Multiplexer)

Las conexiones para la tecnología xDSL de un gran número de suscriptores son recibidas por estos equipos, los cuales son armarios que poseen las tarjetas de línea y las tarjetas de divisores o filtros para las diferentes tecnologías xDSL. Es en el DSLAM donde los paquetes xDSL y la señal de voz analógica (PSTN) se dividen, permitiendo la transmisión de diferentes servicios sobre el mismo par de cobre.

Los DSLAM de CANTV se encuentran a lo largo del territorio nacional, con información de su Gerencia de Arquitectura de Redes y Sistemas (2014), se

estableció que hay aproximadamente más de cuatrocientos veinte (420) DSLAM dispuestos en 300 localidades.

3.3 Red Metro-Ethernet

Este nivel de la red ofrece los servicios metropolitanos usando la conexión Ethernet, entre los más comunes tenemos los siguientes:

- Conexión a Internet.
- Transporte Metropolitano.

La red Ethernet de CANTV es una red diseñada por conmutadores (switches) capa 2 y capa 3 que poseen interfaces GE, que acoplan los diversos dispositivos que dan el óptimo servicio al usuario, con el backbone IP. Dicha red realiza las tareas de red de transporte, y en la cual trabajan una serie de protocolos tales como OSPF, MPLS, IGMP y IP.

Igualmente los dispositivos agregadores (B-RAS) implementados en la red de CANTV, proveen acceso a internet basado en DHCP. Dichos agregadores se comunican con los enrutadores de distribución por conexiones LAN y reciben el tráfico proveniente de los DSLAM a través de la red ATM, para el caso de los DSLAM ATM, y a través de la red metroethernet para el caso de los DSLAM IP.

3.3.1 B-RAS (Broadband Remote Access Server)

El servidor de acceso remote distribuye o converge tráfico del usuario, proporciona servicios de manejo, control de servicio, seguridad de la red, autenticación, contabilidad y acreditación. El B-RAS es la pasarela (*Gateway*) de control de servicio en la red metro-ethernet. Dicho servidor está configurado por CANTV para poder reajustar los perfiles del usuario dependiendo de su plan de datos.

3.3.2 DHCP Server (Dynamic Host Configuration Protocol)

El servidor DHCP [16] recibe las peticiones de dirección IP provenientes del BRAS, y se le asigna al usuario una IP válida de uno de las miles de direcciones que dicho servidor tenga cargado, a este grupo de direcciones se le denomina direcciones de retorno (loopback address). Antes de poder acceder a navegar en la internet, es imprescindible que la red de gestión de CANTV certifique al usuario que solicitó una dirección IP.

Inmediatamente, luego el B-RAS almacena en su memoria la dirección IP asignada por el servidor DHCP y la dirección MAC del dispositivo (CPE) que solicitó la dirección IP.

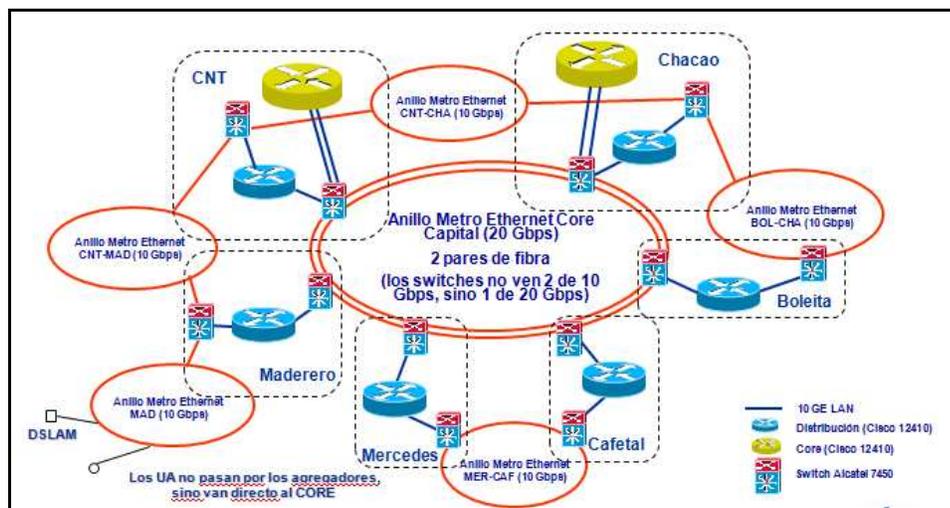


Figura 20: Arquitectura Metro-Ethernet en Caracas.

3.4 Backbone IP

Este nivel consta de cuatro (4) partes:

- Borde
- Core

- Distribución
- Agregación

Todas las capas están soportadas por enrutadores (routers) que pueden manejar velocidades aproximadamente en el rango de los 2,5 Gbps a los 40 Gbps por tarjeta.

3.4.1 Borde

Este nivel está constituido por los 3 puntos de acceso internacional para conexión hacia la internet. Estos puntos están localizados en Chacao con 2 enlaces STM-16 POS (Packet Over SDH) Camuri con 2 enlaces STM-16 POS y Punto Fijo con 2 enlaces STM-16 POS.

3.4.2 Core

Está formado por 4 enrutadores (router) Cisco redundantes, que se interconectan con enlaces STM-64 POS a través de DWDM; cada router tiene 2 enlaces, cada uno hacia un nodo del CORE diferente, conformando una red parcialmente mallada. Esto permite aumentar la disponibilidad de la red.

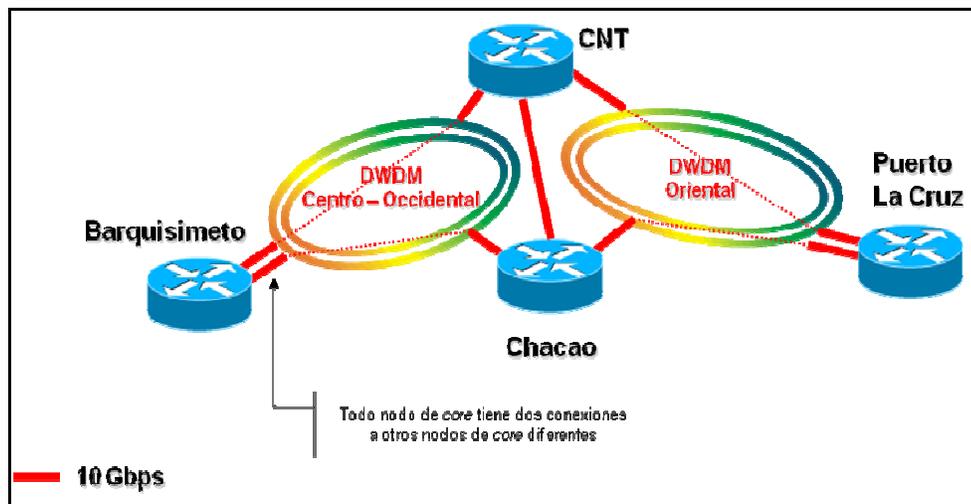


Figura 21: Arquitectura CORE.

3.4.3 Distribución

El nivel de jerarquía de distribución está formado igualmente por enrutadores (routers) Cisco con tarjetas procesadoras de nueva generación redundantes. Estos enrutadores (routers) de distribución interconectan los anillos Metro Ethernet de acceso y tienen configurados los servicios de IP/MPLS, QoS 11, enrutamiento, balanceo de carga (traffic, shaping), filtros, etc.

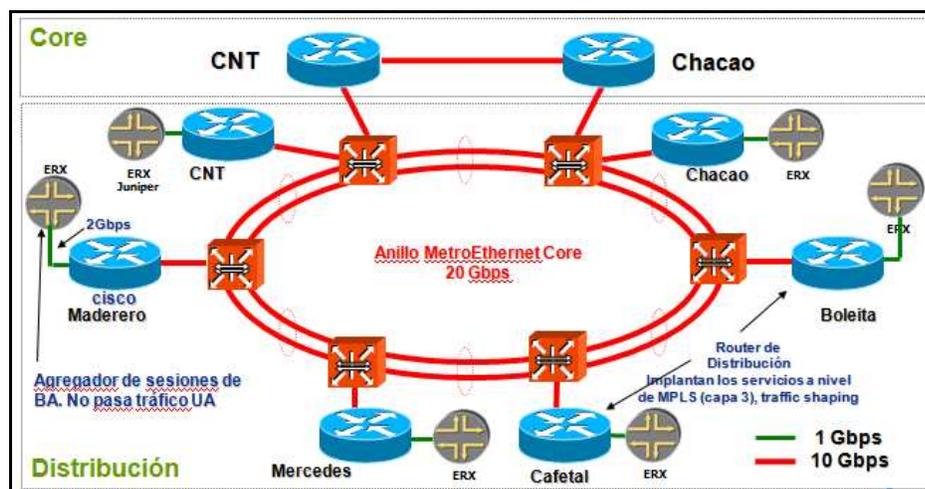


Figura 22: Arquitectura de Distribución.

3.4.4 Agregación

Esta capa está conformada por 32 nodos distribuidos ubicados en las mismas localidades donde se encuentran los enrutadores (routers) de distribución, los cuales tienen la función de coleccionar el tráfico IP e inyectarlo a la estructura de red IP.

3.5 Centro de Operaciones de la Red de CANTV

El (COR) Centro de Operaciones de Red tiene como eje principal garantizar, mediante la prevención, detección, diagnóstico y corrección de incidentes, con sistemas de alta tecnología, esquemas metodológicos especializados y personal

altamente capacitado, la continuidad operativa de los servicios y dispositivos de red que componen las diversas plataformas tecnológicas de CANTV, las 24 horas del día, durante todo el año.

Para el servicio de internet de banda ancha CANTV actualmente tiene la siguiente manera de que el usuario le plantee sus necesidades.

A continuación se presenta el número de contacto con las distintas opciones que se da en el servicio de internet, el mismo se entrega en la oficina de atención al cliente en las sedes de la compañía, con la intención de que el usuario no tenga que trasladarse hasta dicha oficina, sino que desde su propia residencia por teléfono ponga al tanto al operador del servicio que posee en un instante determinado.

Aún mas fácil...!!!	151 SERVICIO DE REPORTE AVERÍAS 0800-CANAIMA – 08002262462 0800-2100045 RET ABA POSTPAGO
0800CANTV00 0800-2268800	
<input type="checkbox"/> Consulta de Saldo 1-1 <input type="checkbox"/> Consulta de Saldo de Servicio de internet 1-2 <input type="checkbox"/> Información de Lugares de Pago 1-3 <input type="checkbox"/> Status de solicitud Línea Telefónica 2-1-1 <input type="checkbox"/> Status de Solicitud de Internet 2-1-2 <input type="checkbox"/> Compra de Productos y Servicios 2-2 <input type="checkbox"/> Reporte de Averías Línea Telefónica 3-1 <input type="checkbox"/> Reporte de Averías Teléfonos Públicos 3-2 <input type="checkbox"/> 0500-LAS GUIAS – (0500-5274842)	<input type="checkbox"/> Reporte Averías Internet o ABA 3-3-1 <input type="checkbox"/> Atención al Cliente Líneas Telefónicas 4-1-1 <input type="checkbox"/> Sugerencias de Líneas Telefónicas 4-1-2 <input type="checkbox"/> Reclamos de Líneas Prepago 4-2 <input type="checkbox"/> Atención al Cliente Internet y ABA 4-3 <input type="checkbox"/> Club CANTV 5

Figura 23: Contacto para el COR de CANTV.

En esta etapa del proyecto se va a abordar uno de los objetivos específicos, el cual está vinculado al estado de la red de datos actual y en base de ello, indicar la importancia de una plataforma de gestión remota en el servicio de internet de banda ancha, para que el servicio opere eficientemente al ser gestionado de manera correctiva y preventiva.

A partir de la información suministrada por el COR de CANTV, se denotarán los indicativos más resaltantes en el servicio de internet de indagar cuales fallas son las

más comunes y que similitudes existen entre los dispositivos que conforman la red del servicio de datos.

3.6 Estatus de la Red de Internet Banda Ancha

Cuenta de TICKET Rótulos de fila	is de columna												Total general
	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	
PC	12945	14896	13578	18115	18912	19115	20351	22222	20258	20672	14243	15809	211116
NO CAPTURA IP	5543	6152	5532	6015	6809	7055	7852	8545	7545	7663	5030	4944	78685
NO NAVEGA	2837	3151	3582	4044	4849	4718	5205	5702	5072	5008	3184	3971	51323
RECIBE IP / NO NAVEGA	3367	4219	3282	3613	4250	4486	4452	4474	4471	4361	3189	3425	47589
SISTEMA OPERATIVO	381	379	355	822	1504	1478	2037	2300	2173	2548	2049	2452	18478
PERCIBE NAVEGACION LENTA	689	857	658	3192	1248	1182	627	1055	868	1002	693	944	13015
NO CONECTA	84	79	107	99	181	121	122	78	81	57	81	55	1145
NO ACCEDE A URL ESPECIFICO	27	21	36	304	32	30	27	35	27	18	14	13	584
DESCONEXION	10	20	15	12	20	17	20	23	3	1	1	2	144
NO APTO	4	4		4	8	18	5	4	14	8	2	1	72
APLICACION NO FUNCIONA	3	10	8	9	11	9	4	3	4	6		2	69
NAVEGA LENTO			2										2
FALLA DE CONEXION FTP		2											2
ERROR EN PAGINA				1		1							2
FALLA DE CARGA/DESCARGA FTP		2											2
FALLA DE CARGA/DESCARGA									1				1
FALLA DE ACCESO A BASE DE DATOS									1				1
CONFIGURACION									1				1
FALLA DE ELIMINACION DE ARCHIVOS VIA FTP				1									1
CPE	11254	10242	10617	11232	13208	12059	13504	14750	14221	14508	10395	10873	146863
NO ENCIENDE	4917	3881	4004	4658	5874	4656	5408	5885	6257	6527	4785	4733	61585
NO SINCRONIZA	2834	2652	2773	2661	3075	2931	3357	3885	3592	3491	2412	2575	36238
RECIBE IP / NO NAVEGA	2236	2319	2394	2313	2627	2869	2983	2925	2730	2955	2113	2335	30799
NO CAPTURA IP	1152	1203	1179	1243	1278	1291	1391	1671	1224	1224	870	1044	14770
FALLA DE MODEM	99	157	217	318	305	258	318	357	380	285	199	161	3054
DESCONFIGURADO	16	30	50	39	49	53	25	27	38	26	15	25	393
NO SINCRONIZA / INTERMITENCIA							1	22					23
NO CONECTA											1		1
REGISTRO ABA	2172	2380	1948	2324	2310	1496	1378	1084	900	1153	869	806	18820
SOPORTE EN AUTOREGISTRO	2002	2190	1790	2111	2120	1366	1240	983	809	1014	783	756	17164
SOLICITA STATUS/ # DE ORDEN	101	133	122	173	168	116	125	91	79	122	70	42	1342
SOLICITA INSTALACION ASISTIDA	67	50	35	40	21	12	13	9	9	16	14	8	294
SOLICITA STATUS DE PRE-ORDEN	2	7	1		1	2		1	3	1	2		20
PLATAFORMA	21	32	972	1304	4473	1831	1449	173	1086	573	1229	198	13341
ABA	4	21	934	1259	4429	1683	1421	143	1073	559	315	189	12030
ACCESO WEB	10	11	27	3	9	121	12	25	1	5	889		1113
REMEDY	7		7	36	28	14	4	3	8	1	5	7	120
BOSS WEB			2	6	6	13	12	2	4	5			50
CORREO			2		1					3	20	2	28
PLATAFORMA DE ACCESO	92	116	110	115	179	150	217	172	152	162	125	109	1699
NO CAPTURA IP	29	27	43	36	43	50	116	52	39	39	34	37	545
RECIBE IP / NO NAVEGA	15	21	24	23	39	37	57	30	28	34	27	27	362
PERCIBE NAVEGACION LENTA	14	39	21	26	33	41	15	36	28	40	21	20	334
REQUIERE SOPORTE	19	5	5	6	40	11	14	26	33	28	23	10	220
NO ACCEDE A URL ESPECIFICO	7	11	3	14	9	5	7	12	6	9	6	7	96
FALLA REINCIDENTE	5	9	7	2	4	3	4	12	12	12	11	6	87
ERROR EN EL IVR	1		5	6	9		1		5		1	1	29
NO NAVEGA	1	3	1	1	1	3	3	1			2	1	17
CONEXION			1		1								3
NO CAPTURA IP / INTERMITENCIA				1					1	1			3
APLICACION NO FUNCIONA	1	1											2
NO CONECTA									1				1
CORREO ELECTRONICO	45	101	55	54	64	67	77	91	460	310	90	50	1464
NO ENVIA	31	82	41	38	44	44	49	62	419	291	66	31	1198
NO RECIBE	14	19	14	16	20	23	28	29	41	19	24	19	266
LINEA TELEFONICA	2	1	1	4	3	5	184	6	8	3	6	3	226
FALLA FRANCA	1			1		4	181	5	2		2	2	198
NO NAVEGA	1	1	1	2	1	1	3		4	2	2	1	19
AVERIA VOZ				1	2			1	2	1	2		9
BOSS	18	16	15	24	12	12	13	17	22	26	13	14	202
PROCESO DE REGISTRO	18	16	15	23	12	12	12	17	21	26	13	14	199
NO NAVEGA				1			1						2
NO CONECTA									1				1
TARJETA UNICA								2	1	1		1	5
NO PUEDE REALIZAR LA RECARGA DE SALDO								1	1	1		1	4
NO NAVEGA								1					1
DOMINIO		1										1	2
PAGINA CARGA SOLO EN CANTV.NET		1											1
ERROR EN PAGINA											1		1
ABA INALAMBRICO								1					1
FALLA DE MODEM								1					1
SOPORTE APROVISIONAMIENTO				1									1
CLIENTE NO REGISTRADO				1									1
Total general	26550	27784	27297	33172	39161	34735	37176	38516	37108	37407	26972	27862	393740

Tabla 8: Estatus de la red durante el 2013 / Servicio Internet Banda Ancha

3.7 Analisis de los Indicadores de Falla de la Red

Analizando los resultados del monitoreo de la red para el servicio de acceso de banda ancha, se interpreta que la mayoría de las fallas se dan en la PC y en el CPE, sumando sus porcentajes éstas se encuentran por encima del 90 %. Es por ello, que CANTV inicia la evaluación de una plataforma de gestión remota que permita resolver estos detalles, la idea principal es lograr tener un control preventivo más que correctivo del servicio de acceso de internet al usuario.

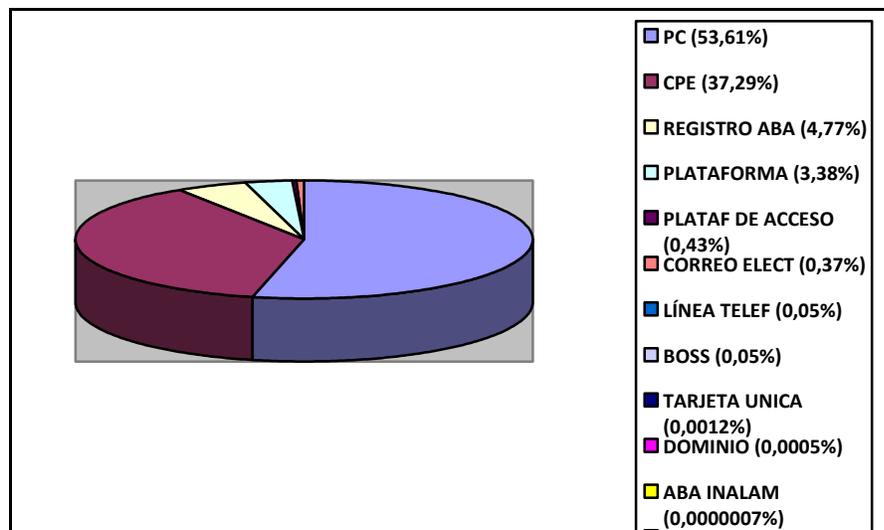


Figura 24: Representación gráfica (%) de la red 2013.

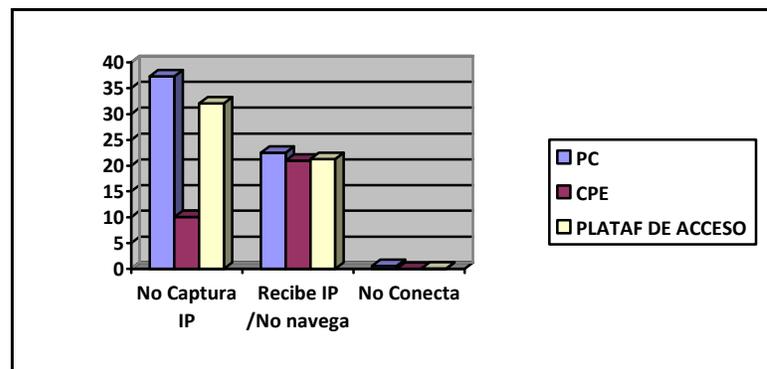


Figura 25: Fallas comunes en la PC, CPE y Plataforma de Acceso

Se detalla que para los CPEs, el mayor inconveniente se da cuando este no enciende, no sincroniza y no navega, estos factores puede atenderse de manera inmediata con una plataforma de gestión remota, resolviéndolos con un simple reinicio del CPE, borrado y retorno al estatus de fabrica, actualización del firmware, actualizando datos en el tiempo de asignación de direcciones IP por el servidor DHCP (DHCP lease time) o verificando sus parámetros de línea.

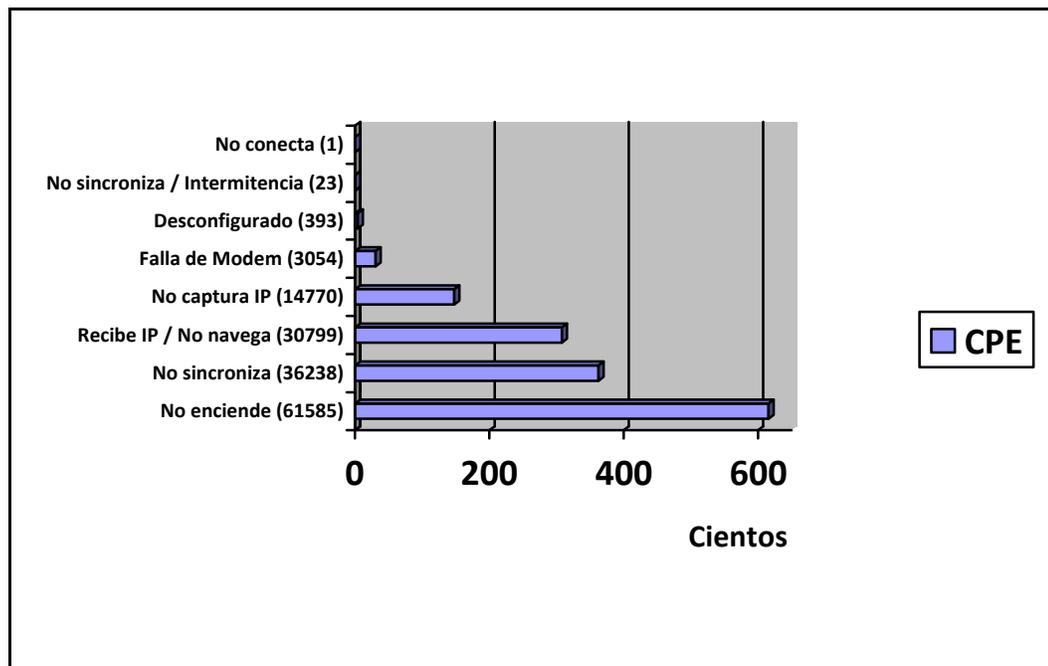


Figura 26: Niveles de Fallas en el CPE

3.8 Proveedor Friendly Technologies de Solución de Administración basada en TR-069

Friendly Technologies es un proveedor de soluciones optimizadas de gestión de dispositivos y de experiencia del usuario, para operadores fijos y móviles. Las soluciones que ejecuta Friendly Technologies facilitan y simplifican el servicio de banda ancha durante todo el ciclo de vida, permitiendo a los operadores aumentar la satisfacción del cliente, mientras reduce significativamente los costos operacionales.



Figura 27: Página web de Friendly Technologies: www.friendly-tech.com

Friendly Technologies ha desarrollado una plataforma de gestión remota donde supervisa, controla y monitorea una gran cantidad de equipos destinados a trabajar en la internet, dicha plataforma como se mostrara a continuación posee una serie de herramientas e imágenes que hacen que cada CPE se gestione desde la plataforma.

El sistema soporta la tecnología denominada TRIPLE-PLAY con equipos y CPEs detrás de la NAT. El sistema completo es capaz:

- ✓ Diagnosticar y configurar CPEs.
- ✓ Actualización de versiones de firmware.
- ✓ Rescates de archivos desde los distintos CPEs.
- ✓ Activación/Desactivación de servicios.
- ✓ Diagnóstico del rendimiento de DSL.
- ✓ Verificación del estatus de conectividad de los CPEs.
- ✓ Apagado y reinicio a los CPEs.
- ✓ Muestreo de la actividad de los CPEs.

Esta implementación del TR-069 surge de la necesidad de que actualmente en cualquier residencia se posee un enrutador inalámbrico y una red local, ya que casi todos los dispositivos están interconectados.

El servicio de internet de banda ancha es un desafío para el infinito número de proveedores, ya que deben constantemente suministrar una serie de servicios con la finalidad de aumentar los ingresos y reducir los costos con soporte tecnológico.

Todos los proveedores de servicios compiten para mejorar la experiencia y mantener la lealtad de los usuarios.

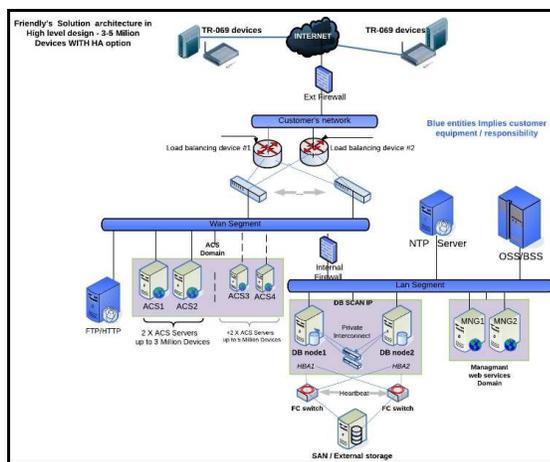


Figura 28: Solución Friendly 3MM CPEs



Figura 29: Suite TR para Friendly

De manera general con la plataforma de gestión remota de Friendly Technologies se da una solución completa, multifuncional y robusta que automatiza el despliegue y el soporte de servicios de datos, voz y videos.

La plataforma de ACS de Friendly Technologies que se basa en el protocolo TR-069, tiene soporte para innumerables dispositivos, incluyendo los módems de la generación de xDSL, pasarela residencial, STB (Set To Box), WiFi, WIMAX y LTE.

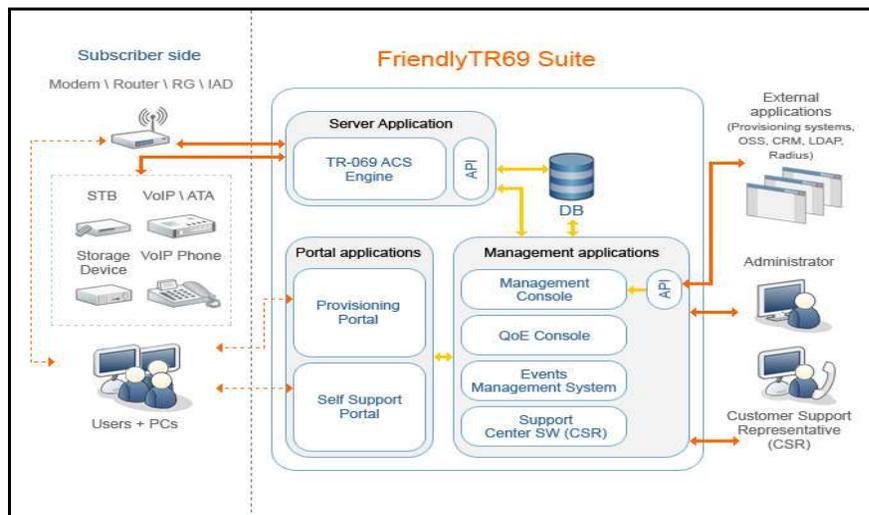


Figura 30: Arquitectura Friendly Technologies TR-069 Suite

La plataforma de gestión remota friendly que posee un diseño abierto y modular, incluye varias formas de despliegues, desde el nivel básico de un solo servidor hasta un despliegue distribuido de alta disponibilidad.

La solución del Centro de soporte Friendly Technologies es una innovación para el flujo de trabajo del asistente ya que permite la localización exacta de las fallas que se presentan, lo que disminuye eficientemente los costos de soporte y facilita el despliegue de costo-efectivo de los servicios de datos, VoIP e IPTV. El mismo integra el servicio, el dispositivo y la información del usuario en una sola pantalla. Maneja dos formatos que pueden resolver de manera rápida y eficientemente casi todo tipo de fallas, estos son el diagnóstico al toque (*Single Quick*) y la reparación rápida (*Quick Fix*).

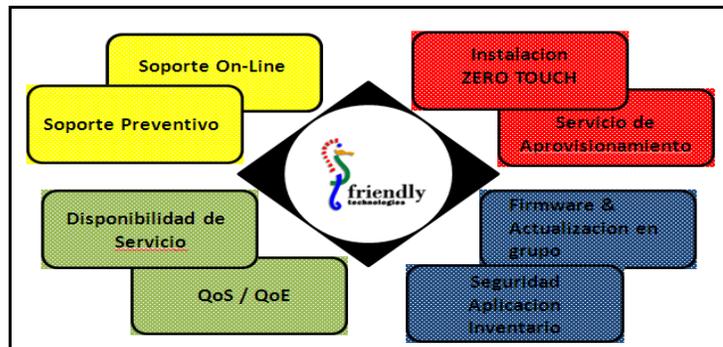


Figura 31: Modelo de Gestión Friendly Technologies

3.9 Aprovisionamiento Automatizado de Nuevos Usuarios y Nuevos Servicios

El portal de Friendly Technologies automatiza como se mencionó anteriormente, el aprovisionamiento de usuarios de datos, voz y video, lo que reduce drásticamente el coste por abonado, evitando la necesidad de complicados procesos de inscripción de bloques en eventos y el portal de aprovisionamiento ofrece una única interfaz unificada para el aprovisionamiento de todos los tipos de dispositivos y sirve como interfaz para todos los sistemas de procesamientos de datos centralizados (*back-office*) que intervienen en el proceso de aprovisionamiento.

El portal permite a los usuarios no técnicos que puedan instalar sin problemas y hacer que sus dispositivos configurados automáticamente se activen automáticamente los servicios adicionales, sin tener que llamar a la asistencia o solicitar un técnico in situ. Una solución de enchufar y ejecutar (*plug-and-play*), solo requiere que el usuario conecte el dispositivo a la línea de banda ancha y espere mientras todo está configurado y funcionando. El sistema permite una fácil integración con el sistema de procesamiento de datos (*back-office*), y soporta una amplia variedad de aprovisionamiento y reprovisionamiento escenarios.

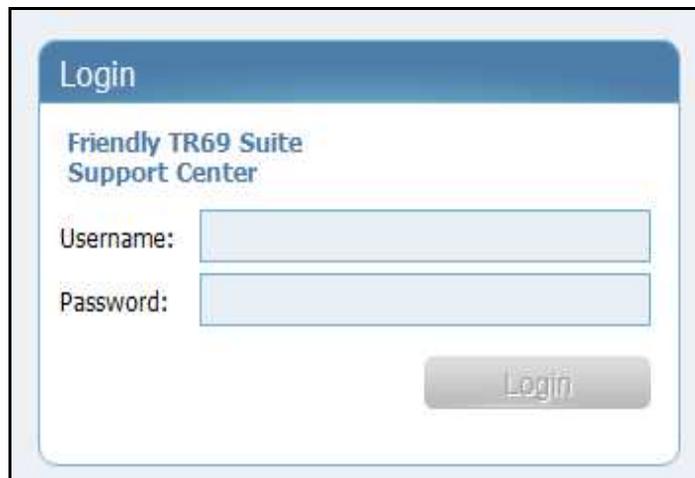
Friendly presentan dos portales: la Consola de Administración (*Management Console*) y el Centro de Soporte (*Support Center*), La Consola de Administración (*Management Console*) tiene un nivel de prioridad mayor respecto al otro. Esto con la

intención de que profesionales con mayor conocimiento y mayor responsabilidad puedan realizar un conjunto de tareas más específicas. Este portal lleva la etiqueta de un trabajo más gerencial.

El Centro de Soporte (Support Center) está asociado a un centro de llamadas (call center) donde pueda ser manejado por un personal que lleve a cabo tareas más específicas para corregir fallas instantáneas o elaborar una serie de instrucciones para levantar el servicio en un corto o mediano plazo.



<http://201.249.43.253/CpeAdmin/Login.aspx>



<http://201.249.43.253/CSR/Login.aspx>

3.10 Consola de Administración Friendly (TR-069 Suite Management Console)

La solución del Management Console consiste en un portal que abarca de manera general el trabajo del protocolo TR-069 para los distintos CPEs. A continuación se presentan las bondades que brinda la plataforma Friendly.

Luego de ingresar con el nombre y su clave, la pantalla principal se presenta como en la siguiente figura:

	Manufacturer	Model name	MAC Address	IP Address	Firmware	Created	Updated
<input type="checkbox"/>	trendchip	DSL-Gateway	6cfd5b-20f3-9c	201.249.43.102	*2.12.15.00UB-CM93.11.2.175	06/07/2013 12:49:09 p.m.	22/10/2013 11:04:56 a.m.
<input type="checkbox"/>	Broadcom	963281TAN		190.74.59.61	4.10L-01	07/07/2013 06:41:07 a.m.	04/02/2014 02:14:17 p.m.
<input type="checkbox"/>	Broadcom	963281TAN			4.10L-01	16/08/2013 06:52:37 p.m.	04/02/2014 02:14:53 p.m.
<input type="checkbox"/>	ZyXEL	AMG1202-T106	EC431F6-6E89-C4	186.89.16.50	V2.00(AAQP-0)02_F0	17/08/2013 09:23:23 a.m.	04/02/2014 02:14:28 p.m.
<input type="checkbox"/>	ZyXEL	P-660R-U-T1	b0b2dc-0e46-1d	201.249.43.126	A01.01(AB.1)03	19/08/2013 11:30:39 a.m.	18/11/2013 07:20:21 a.m.
<input type="checkbox"/>	Broadcom	96338mg	02-10-18-03-28-13	201.249.43.118	4.06L-01	19/08/2013 11:58:37 a.m.	29/10/2013 10:54:56 a.m.
<input type="checkbox"/>	REALTEK SEMICONDUCTOR CORP.	IGD	00-E9-00-00-00-09	201.249.43.106	CANTV-AR21RU-V2-20130813-MER	19/08/2013 02:10:57 p.m.	19/08/2013 03:49:32 p.m.
<input type="checkbox"/>	REALTEK SEMICONDUCTOR CORP.	NT3BB-1PWH-124	64-51-7E19-5E18	190.73.192.5	V2.1.1	21/08/2013 03:43:53 p.m.	21/08/2013 04:55:21 p.m.
<input type="checkbox"/>	Huawei Technologies Co., Ltd.	EchoFe H9521	84-AB-6A-29-64-C6	201.249.43.100	V100R001C3008011	22/08/2013 06:22:06 p.m.	02/12/2013 01:56:04 p.m.
<input type="checkbox"/>	Broadcom	IGD	02-10-18-03-15-E0	201.249.43.104	RTK V2.1.1	23/08/2013 08:05:02 a.m.	04/02/2014 02:12:43 p.m.
<input type="checkbox"/>	Broadcom	96332R			4.04L-01	03/08/2013 03:29:37 p.m.	15/10/2013 08:46:10 a.m.
<input type="checkbox"/>	ZTE	B600V4C			ker V40332820	19/09/2013 02:41:28 p.m.	04/02/2014 12:53:43 p.m.
<input type="checkbox"/>	Broadcom	IGD	02-10-18-03-17-91	190.38.248.83	RTK V2.1.1	22/10/2013 11:11:05 a.m.	20/01/2014 10:25:68 p.m.
<input type="checkbox"/>	trendchip	DSL-Gateway	6cfd5b-20f3-9c	200.11.174.237	*2.12.15.00UB-CM93.11.2.175	15/11/2013 05:30:02 p.m.	22/11/2013 10:04:15 a.m.
<input type="checkbox"/>	ZyXEL	AMG1202-T106	EC3F66-6B98-04	201.249.43.119	V2.00(AAQP-0)02_F0	21/11/2013 09:55:05 a.m.	27/01/2014 09:01:54 a.m.

Figura 32: Pantalla principal de la Consola de Administración (Management Console Friendly).

En la parte superior de la imagen anterior, se encuentran 8 pestañas (cada una con una función diferente) a continuación se hará una breve reseña de ellas.

La pestaña de configuración (Settings); muestra toda la identificación de la plataforma, la dirección ip y puerto asociado al servidor ACS, igualmente la configuración de la base de datos. Entre otros detalles muestra todos los usuarios de gestión con su correo electrónico, permisos, fecha de expiración y el estatus en el se encuentra cada usuario.

Es importante la revisión de esta pestaña ya que en ella se encuentra información muy valiosa con la plataforma, con sus respectivos nombre de usuario (login) y contraseña (password).

En la pestaña de reportes (Reports), se presentan un conjunto de reportes tanto para chequear la operatividad de los CPEs, como para ver el porcentaje de los diversos proveedores que estan presentes en la plataforma.

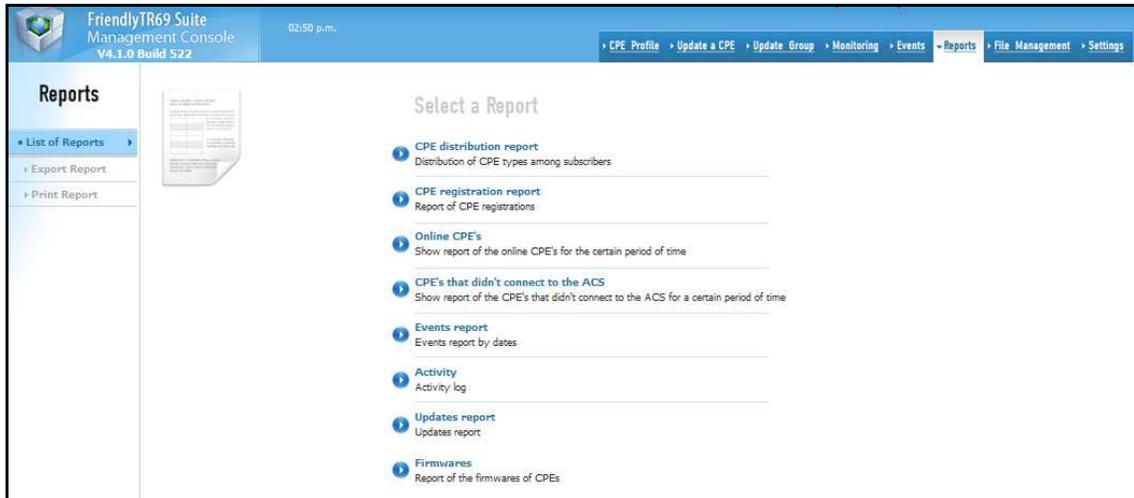


Figura 33: Reportes / Consola de Administraci3n (Management Console)

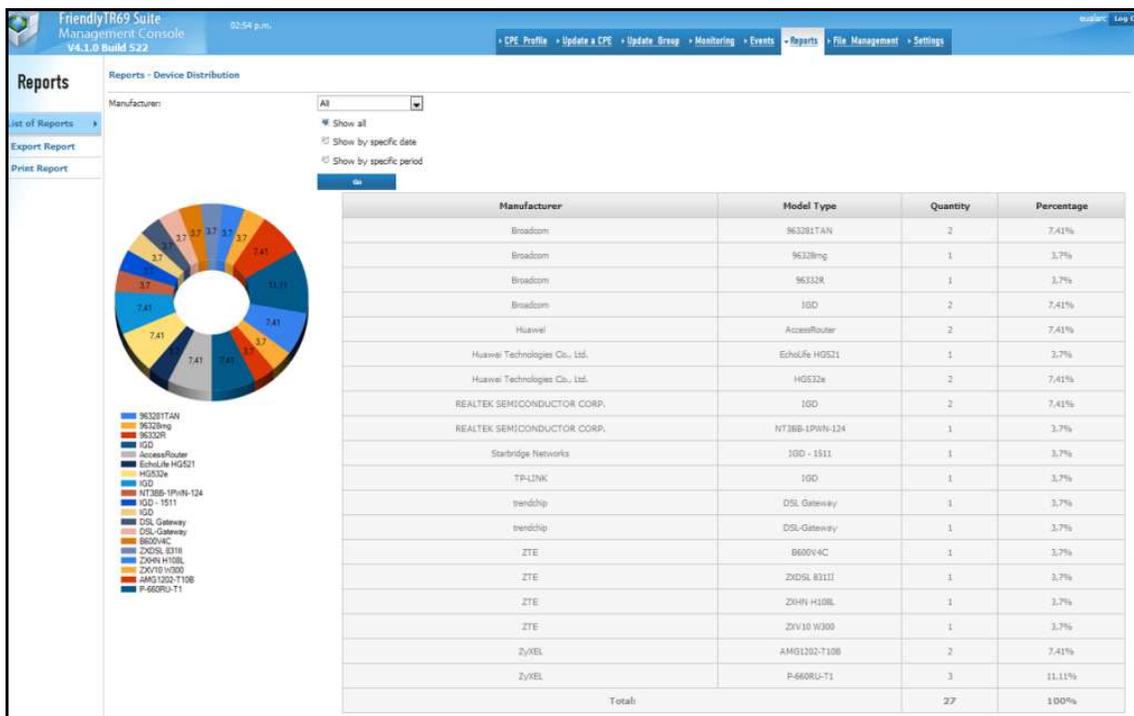


Figura 34: Reporte de distribuci3n de los CPEs

Reports - Firmwares Report

Manufacturer: All
Model: All

Manufacturer	Model	Firmware
Broadcom	9632B1TAN	4.10L.01
Broadcom	9632B1TAN	4.10L.01
Broadcom	9632Bmp	4.06L.01
Broadcom	9632ZR	4.04L.01
Broadcom	1GD	RTK V2.1.1
Broadcom	1GD	RTK V2.1.1
Huawei	AccessRouter	2.5.0.100
Huawei	AccessRouter	2.3.1.900
Huawei Technologies Co., Ltd.	EchoLife HG521	V100R001C1000011
Huawei Technologies Co., Ltd.	HG522e	V100R001C01B020
Huawei Technologies Co., Ltd.	HG522e	V100R001C01B020
REALTEK SEMICONDUCTOR CORP.	1GD	CANTV-AR21RU-V2-20130812-MER
REALTEK SEMICONDUCTOR CORP.	1GD	2.0.0
REALTEK SEMICONDUCTOR CORP.	NT388-1PWR-124	V1.1.1
Starbridge Networks	1GD - 1S11	1S11_CanTV_4_4_0-130116_1508

1 2 >> 1 Total amount: 27

Figura 35: Reporte de firmware descargados

Todos los reportes que pueden generarse tiene la capacidad de descargarlos en un archivo en excel y tenerlos como informe de todo lo que ha pasado en un día determinado.

Al pulsar click en un CPE en específico, la ventana que se muestra es la siguiente: acá se tiene una serie de información que puede modificarse para hacer un perfil más sencillo a la hora de encontrarlo rápidamente.

Update a CPE

Device Info: Manufacturer: Broadcom, Model name: 9632B1TAN, Firmware Version: 4.10L.01

Account Info: Full name: Proebas Lab, Location: Laboratorio

Network Status: Online

Registration Date: 07/07/2013 06:41:07 a.m.

Last Connection: 06/02/2014 11:46:31 a.m.

Quick Fix: Select case: Select case

Figura 36: Pantalla Principal para un CPE en específico.

A la izquierda de la información del dispositivo se encuentran los diferentes despliegues para las instrucciones a modificar o chequear.

3.11 Friendly TR069 Support Center

La solución del Centro de Soporte (Support Center) consiste en un portal que abarca de manera específica el trabajo del protocolo TR-069 para los distintos CPEs. A continuación se presentan las bondades que brinda la plataforma friendly.

Luego de ingresar con el nombre y su clave, la pantalla principal se presenta como en la siguiente figura:

The screenshot shows the 'Friendly TR069 Support Center' interface. At the top, there are navigation tabs: 'Update a CPE', 'User Management', 'Reports', and 'Settings'. Below these, there are search and filter options for 'View', 'Manufacturer', and 'Model name'. The main content is a table with the following columns: Manufacturer, Model name, MAC Address, IP Address, Firmware, and Created. The table contains 17 rows of device data.

Manufacturer	Model name	MAC Address	IP Address	Firmware	Created
trendchip	DSL-Gateway	6cfd69:20f3:9c	201.249.43.102	*2.12.15.0(UE9.C39)3.11.2.175	06/07/2013 12:49:09 p.m.
Broadcom	963281TAN		190.74.59.61	4.10L.01	07/07/2013 06:41:07 a.m.
Broadcom	963281TAN			4.10L.01	16/08/2013 06:52:37 p.m.
ZyXEL	AMG1202-T108	EC43:F64E49:C4	186.89.16.50	V2.00(AAQP.0)62_F0	17/08/2013 09:23:23 a.m.
ZyXEL	P-660RU-T1	b0b2dce4:6a1d	201.249.43.126	A01.01(A8.1)03	19/08/2013 11:30:39 a.m.
Broadcom	96328mg	02:10:18:63:28:13	201.249.43.118	4.06L.01	19/08/2013 11:58:27 a.m.
REALTEK SEMICONDUCTOR CORP.	IGD	00:E9:00:00:00:09	201.249.43.106	CANTV-AR21RU-V2-20130812-MER	19/08/2013 02:10:57 p.m.
REALTEK SEMICONDUCTOR CORP.	NT38B-1PWN-124	64:51:7E:16:5E:18	190.73.192.5	V2.1.1	21/08/2013 03:43:53 p.m.
Huawei Technologies Co., Ltd.	EthoLife HG521	84:A8:E4:25:64:C6	201.249.43.100	V100R001C1008011	22/08/2013 06:22:08 p.m.
Broadcom	IGD	02:10:18:01:15:E0	201.249.43.104	RTK V2.1.1	23/08/2013 08:01:02 a.m.
Broadcom	96332R			4.04L.01	03/08/2013 03:29:37 p.m.
ZTE	B600V4C			ker V40332820	19/09/2013 02:41:28 p.m.
Broadcom	IGD	02:10:18:01:17:91	190.38.248.83	RTK V2.1.1	22/10/2013 11:11:05 a.m.
trendchip	DSL Gateway	6cfd69:20f3:9c	200.11.174.237	*2.12.15.0(UE9.C39)3.11.2.175	15/11/2013 05:30:02 p.m.
ZyXEL	AMG1202-T108	EC3F:66:EB:9B:04	201.249.43.119	V2.00(AAQP.0)62_F0	21/11/2013 09:55:05 a.m.

Figura 37: Pantalla Principal Support Center Friendly

En la parte superior de la tabla, se encuentran 4 pestañas (cada una con una función diferente) a continuación se hará una breve reseña de ellas.

La pestaña de configuración (Settings); muestra toda la identificación de la plataforma, la dirección IP y puerto asociado al servidor ACS, igualmente la configuración de la base de datos. Entre otros detalles muestra todos los usuarios de gestión con su correo electrónico, permisos, fecha de expiración y el estatus en el que se encuentra cada usuario.

Es importante la revisión de esta pestaña ya que en ella se encuentra información muy valiosa con la plataforma, con sus respectivos login y password.

The screenshot shows the 'ACS and DB' configuration page. The interface includes a navigation menu on the left with options like 'Email server', 'Alerts', 'File Server', and 'Sessions'. The main content area is divided into several sections:

- ACS address:** IP address: 201.249.43.254, Port: 8080.
- Database type:** Database type: MySQL (selected), Oracle.
- ACS database settings:** IP address: 201.249.43.254, Database name: ftacs, Username: ftacs, Password: ftacs.
- Login database settings:** IP address: 201.249.43.254, Database name: csr, Username: ftacs, Password: ftacs.

Figura 38: Datos Configuración Centro de Soporte (Support Center) Friendly

En la pestaña de reportes (Reports), se presentan 2 opciones tanto para chequear el registro de los CPEs, como para ver las actividades que han tenido los CPEs en un lapso de tiempo determinado que lo especifica el operador.

The screenshot shows the 'Reports - Registration Report' page. It includes a filter section with 'Manufacturer' and 'Model' dropdowns set to 'All', and 'From date' (1/1/2007) and 'To date' (2/8/2014) input fields. A 'Go' button is present below the filters. The main content is a table with the following data:

Serial	Manufacturer	Model	Registration date	Last connection date	Phone
6CFDB920F39C	trendchip	DSL-Gateway	06/07/2013 12:49:09 p.m.	22/10/2013 11:04:56 a.m.	
000e4e2503a	Broadcom	963281TAN	07/07/2013 06:41:07 a.m.	08/02/2014 10:20:06 p.m.	
000e4e2503c	Broadcom	963281TAN	16/08/2013 06:52:37 p.m.	08/02/2014 10:20:07 p.m.	04168000404
S132E17200018	ZyXEL	AMG1202-T10B	17/08/2013 09:23:23 a.m.	08/02/2014 10:13:22 p.m.	04168000404
B0B2DCE46A1D	ZyXEL	P-660RU-T1	19/08/2013 11:30:39 a.m.	18/11/2013 07:20:21 a.m.	
021018632811	Broadcom	96328mg	19/08/2013 11:58:27 a.m.	29/10/2013 10:54:56 a.m.	
001AEF000009	REALTEK SEMICONDUCTOR CORP.	IGD	19/08/2013 02:10:57 p.m.	19/08/2013 03:49:32 p.m.	5555555
64517E165E18	REALTEK SEMICONDUCTOR CORP.	NT3BB-1PWN-124	21/08/2013 03:43:53 p.m.	21/08/2013 04:55:21 p.m.	
2153030567517000299	Huawei Technologies Co., Ltd.	EchoLife HG521	22/08/2013 06:22:08 p.m.	02/12/2013 01:56:04 p.m.	2125002952
0210180115DF	Broadcom	IGD	23/08/2013 08:01:02 a.m.	08/02/2014 10:14:45 p.m.	2126721953
000e4e25000c	Broadcom	96328R	03/08/2013 03:29:37 p.m.	15/10/2013 08:46:35 a.m.	
1160010026ED522565	ZTE	B600V4C	19/09/2013 02:41:28 p.m.	06/02/2014 04:02:34 p.m.	
021018011790	Broadcom	IGD	22/10/2013 11:11:05 a.m.	20/01/2014 10:25:58 p.m.	
6CFDB920F39C	trendchip	DSL Gateway	15/11/2013 05:30:02 p.m.	22/11/2013 10:04:15 a.m.	
S132E17200014	ZyXEL	AMG1202-T10B	21/11/2013 09:55:05 a.m.	27/01/2014 09:01:54 a.m.	8888

At the bottom of the table, there is a pagination control: '<< 1 2 >> Total amount: 27'.

Figura 39: Reporte de Registro de CPEs

V4.1.0 Build 633 | Update a CPE | User Management | Reports | Settings

Reports - Activity

Activity log type: Update a CPE

User: All users | From date: 1/8/2014 | To date: 2/8/2014

Activity type: All

Device serial: []

Go

Username	Activity type	Manufacturer	Model	Serial number	Telephone	Date
evalarc	Add diagnostic	REALTEK SEMICONDUCTOR CORP.	IGD	00000000002		08/01/2014 08:43:02 a.m.
evalarc	Add diagnostic	REALTEK SEMICONDUCTOR CORP.	IGD	00000000002		08/01/2014 08:43:22 a.m.
evalarc	Add diagnostic	REALTEK SEMICONDUCTOR CORP.	IGD	00000000002		08/01/2014 08:43:42 a.m.
evalarc	Add diagnostic	REALTEK SEMICONDUCTOR CORP.	IGD	00000000002		08/01/2014 08:48:33 a.m.
evalarc	Add diagnostic	REALTEK SEMICONDUCTOR CORP.	IGD	00000000002		08/01/2014 08:48:51 a.m.
evalarc	Add diagnostic	REALTEK SEMICONDUCTOR CORP.	IGD	00000000002		08/01/2014 08:49:11 a.m.
evalarc	Add diagnostic	REALTEK SEMICONDUCTOR CORP.	IGD	00000000002		08/01/2014 08:51:03 a.m.
evalarc	Add diagnostic	REALTEK SEMICONDUCTOR CORP.	IGD	00000000002		08/01/2014 08:51:24 a.m.
evalarc	Add diagnostic	REALTEK SEMICONDUCTOR CORP.	IGD	00000000002		08/01/2014 08:57:40 a.m.
evalarc	Add diagnostic	REALTEK SEMICONDUCTOR CORP.	IGD	00000000002		08/01/2014 08:58:01 a.m.
evalarc	Add diagnostic	REALTEK SEMICONDUCTOR CORP.	IGD	00000000002		08/01/2014 08:58:20 a.m.
evalarc	Change parameters	REALTEK SEMICONDUCTOR CORP.	IGD	00000000002		08/01/2014 09:00:05 a.m.
evalarc	Add diagnostic	REALTEK SEMICONDUCTOR CORP.	IGD	00000000002		08/01/2014 09:04:32 a.m.
evalarc	Add diagnostic	REALTEK SEMICONDUCTOR CORP.	IGD	00000000002		08/01/2014 09:04:50 a.m.
evalarc	Add diagnostic	REALTEK SEMICONDUCTOR CORP.	IGD	00000000002		08/01/2014 09:06:31 a.m.

<< 1 2 3 ... 41 42 43 >> 1 | Go | Total amount: 641

Figura 40: Actividades de la plataforma

Friendly TR69 Suite Support Center | V4.1.0 Build 633 | Update a CPE | User Management | Reports | Settings | Connected with User: evalarc | 08/02/2014 10:26:57 a.m.

Main | Device Settings | Custom RPC | Provision Manager | Diagnostics and monitoring | File download and upload | Activity and Logs

Search List

Subscriber info
Full name: Probas Lab
Location: Laboratorio
Edit

Device Information
Manufacturer: Digidom
Manufacturer OUI: 0004f4
Model name: 9623817AN
Serial number: 0004f4e2503a
Hardware version: rmp_hardware1.0
Firmware version: 4.10L01
Uptime (seconds): 2946
IP address: 192.168.1.1

Device tracks
Vendor ID: Completed: 476
Rejected: 0
Paged: 2

Network Map
No data found

Device Status
Status: Online
WiFi: UP
Connectivity failure (last 24h): 0
Reboot amount (last 24h): 0
Downstream: Mbps 7.048
Upstream: Mbps 0.124
Registered: 01/01/2014 08:41:19 a.m.
Last connect: 08/02/2014 10:26:23 p.m.

WAN
URL for Ping: Google (Ping OK) [Link] [Link]
Priority: Priority (Ping OK) [Link] [Link]
DNS: DNS (Ping OK) [Link] [Link]
VCL/VP: 0 / 53
DNS Servers: 200.44.32.12 | 200.11.248.12

WiFi/Wireless Status
Network: [] enable
Network name: [] autoselect
Channel: 9
Unsecured []
OUI/WEP []
Advanced(WPA) []
Comprehensive(WPA2) []
Mixed(WPA and WPA2 mixed mode) []
Security key: [] auto2011

DHCP parameters
Router IP Address: 192.168.1.1
Router Subnet Mask: 255.255.255.0
DHCP Min Address: 192.168.1.2
DHCP Max Address: 192.168.1.254
DHCP Lease Time (seconds): 280000

DSL parameters
Name: []
Current Rate (Mbps): Downstream 2.048 | Upstream 0.124
Max Rate (Mbps): 13.592 | 0.369
Noise Margin (NM): 8 | 2.1
Attenuation (dB): 51.5 | 22.3
Power (dBm): 14.3 | 12.2
Traffic (MB): []

Diagnostics
Ping diagnostics: [] google.com

Tools
Restart device
Restore device to factory settings
Delete device
Start device trace
View device trace
Ping to device
Trace to device
Access device remotely
Non-miscellaneous CPU

Figura 41: Pantalla Principal para Monitoreo de un CPE en específico

CAPÍTULO IV

4. MARCO METODOLÓGICO

4.1 Arquitectura para las Pruebas de la Plataforma Friendly

En este capítulo se explica en detalle los procedimientos para la evaluación de la plataforma de gestión remota de red Friendly Technologies, CANTV puso a disposición una serie de dispositivos (Servidores/DSLAM/BRAS/Modems). Con la red de CANTV se activan, en el se usaron diversos módems, por ello se trabajo con 10 modems de tecnología ADSL2X y configurados en modo enrutador (router).

Cinco (5) módems de la marca BROADCOM, dos (2) módems de la marca HUAWEI, un (1) modem de la marca STARBRIDGE NETWORKS, un modem de la marca ZyXEL y finalmente un (1) modem de la marca ZTE.

De igual manera se trabajó con cuatro (4) servidores, siendo todos de la misma marca y modelo (HP/DL360g8), tanto el servidor ACS y el servidor DB tienen Linux Cent OS (64 bits) como sistema operativo. Otro servidor para aplicaciones de gestión (Management Application Server) con sistema operativo MS Windows 2008 Ent OS (64 bits) y el servidor DHCP con Windows Server 2008 R2.

La figura a continuación presenta la arquitectura de prueba para la plataforma Friendly.

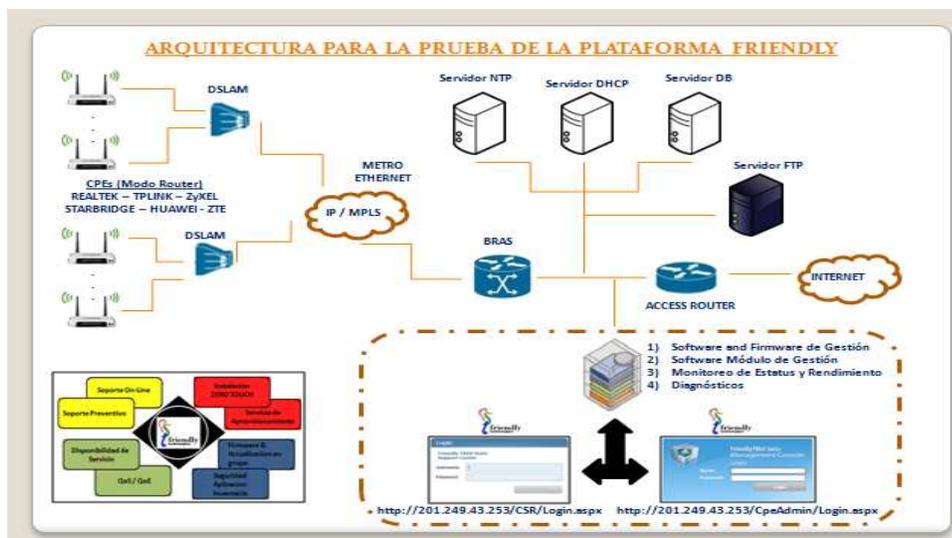


Figura 42: Arquitectura para la Prueba de la Plataforma FRIENDLY

Para añadir cada CPE a la plataforma fue necesario, acceder a cada uno de ellos, en sus configuraciones y en la opción de gestión (Management Settings) de URL se colocó la siguiente dirección <http://201.249.43.254:8080/ftacs-basic/ACS> , seguidamente con la clave y/o password definida por FRIENDLY y CANTV.

Inmediatamente la plataforma al censar el CPE, aparece en la pantalla principal tanto de la Consola de Administración (Management Console) como en la pantalla del Centro de Soporte (Support Center). Al realizar click en un CPE específico, se accede a la pantalla de monitoreo de dicho CPE.

Generalmente en esta pantalla de monitoreo aparecen entre 8 o 9 ventanas, cada una de ella con una función específica, estas ventanas son dinámicas es decir aparecen de acuerdo a los diferentes TR-XXX de la suite TR-069 que pueda soportar.

Cada ventana presenta información detallada del CPE, en donde realizaron las pruebas y se verificaron por tres vías, una de ella es en un recuadro que se encuentra en la parte inferior izquierda de la pantalla donde se especifican las tareas llevadas por el CPE, en este aparecen 4 estatus (Pendiente/Completada/Negada y Fallada).

Se decidió evaluar 45 tareas en cada router para ello se diseño una plantilla de pruebas, donde se presenta toda esa información de manera mas senciclla y detallada. Se diseño para 16 puntos clave de evaluación: (MAPA DE RED, ESTATUS DEL DISP, WAN, WIFI, PARÁMETROS DHCP, PUERTOS, PARÁMETROS DSL, DIAGNOSTICOS/HERRAMIENTAS/CONFIGURAR RESPALDO/REVISIÓN RÁPIDA/CONFIG DISPOSITIVO/RPC CUSTOM/DIAGNOSTICO Y MONITOREO/DESCARGA Y SUBIDA DE ARCHIVOS Y ACTIVIDADES Y REGISTROS).

Al final de este punto, se presenta el diseño de la plantilla, con los datos básicos de cada modem con sus respectivas tareas a evaluar. Y la sección de los anexos del presente informe se encuentra todas las plantillas completamente llenas con las evaluaciones para cada modem.

Parte también de la metodología para evaluar la plataforma de Friendly Technologies, se realizo la verificación de los 182 requerimientos que toda plataforma de gestión remota debe tener aprobada. Acá también se diseño una plantilla para la evaluación de la misma, pero que fueron administradas bajo 16 categorías, entre las cuales se tienen: (CRITERIOS DE LOS PROVEEDORES, REQUERIMIENTOS GENERALES DEL SISTEMA, ARQUITECTURA Y ESCALABILIDAD, GESTIÓN ADICIONAL, SOPORTE DE TR-XXX DEL CPE DATA MODEL, GESTIÓN DE PERIFERICOS Y POLITICAS DE EJECUCIÓN,

OPERACIONALES, UNIDAD DE ABONADO, REQUISITOS DE CONFIGURACIÓN AUTOMÁTICA, DIAGNÓSTICO Y MONITOREO, FIRMWARE Y SOFTWARE, SEGURIDAD, WEB/PORTAL, RSC, MÓDULOS DE INFORMES Y PRUEBAS DE AUTOMATIZACIÓN).

4.2 Modelo de Plantilla para Evaluación de Tareas

A continuación se muestra el modelo de plantilla que se diseñó para las pruebas en los diversos CPEs.

CANTV -- Centro Nacional de telecomunicación de CANTV Gerencia de Planificación y Arquitectura de TI Laboratorio de Estandarización. Edif. Equipos II /Piso 6 (BROADCOM -- 963281TAN -- 190.74.55.35 -- 4.10L.01)		 		
		ESTATUS	EXPLICACIÓN EN DETALLE	VINCULO
MAPA DE RED --- NETWORK MAP		SI / NO		
	Ubicar en la ventana "Network Map" el conjunto de dispositivos que se encuentran conectados con el dispositivo (modem) en estudio			
1.1	La prueba consiste en desconectar o quitar alguno(s) de los dispositivos y verificar que desaparezca del mapa, puede utilizarse el boton "refresh" de manera de actualizar el mapa			
ESTATUS DEL DISPOSITIVO --- DEVICE STATUS				
	Ubicar en la ventana "Device Status" las características principales del modem			
2.1	Status: ONLINE / OFFLINE			
2.2	Wifi: UP / DOWN			
2.3	Falla de conectividad : (Representa el número de fallas que ha tenido en las últimas 24 horas)			
2.4	Número de reinicios del dispositivo : (Representa el número de reinicio que ha tenido en la últimas 24 horas)			
2.5	Verificar que los valores que aparecen en <u>downstream</u> y <u>Upstream</u> coincidan con los valores de la ventana de los parámetros de línea DSL (DSL Parameters)			
WAN				
	Ubicar la ventana "WAN" y hacer ping de prueba a las siguientes URL:			
3.1	Google Validar el ping testing			
	Friendly Validar el ping testing			
	DNS Validar el ping testing			
WIRELESS STATUS				
	Ubicar la ventana "Wireless Status"			
4.1	Desactivar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.			
4.2	Activar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.			
4.3	Modificar el nombre de la red "Network Name" y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.			
4.4	Modificar la contraseña "Security Key" y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.			
PARAMETROS DHCP --- DHCP PARAMETERS				
	Ubicar la ventana "DHCP Parameters"			
5.1	Hacer cambios sobre la operación DHCP Lease Time (seconds), 86400seg (1dia), 129600seg (DdayMedio) Validar posteriormente que la creación de la tarea, se realizo.			
PUERTOS --- PORTS				
	Ubicar la ventana "PORTS"			
6.1	Verificar el número de camaras IP activas y identificación de los puertos asociadas a las mismas.			
PARAMETROS DSL --- DSL PARAMETERS				
	Ubicar la ventana "DSL Parameters", apareceran los siguientes parametros:			
7.1	Current Rate			
	Max Rate			
	Noise Margin			
	Attenuation			
	Power			
	Traffic			
DIAGNOSTICOS (PING DIAGNOSTICS AND SPEED TEST)				
	Ubicar el recuadro "Diagnostics", en la casilla desplegable "Ping Diagnostics" apareceran varias opciones entre las cuales estan:			
8.1	google.com			
	80.80.80.80			
	friendly.com			
	Enter URL/IP 200.44.32.12			
	Escoja una de las opciones y ejecute el boton que se encuentra debajo PLAY y verifique que se llevo a cabo la tarea			
8.2	En el mismo recuadro "Diagnostics" se ubicará la ejecución "SPEED TEST" (esta solo podrá ejecutarse en aquellos modems que soporten TR-143). Utilice el botón que se encuentra debajo PLAY y al instante debe evaluarse la velocidad download y upload en Mbps. Validar esos resultados			

HERRAMIENTAS --- TOOLS			
9.1	Reinicio del dispositivo (Restart Device) Ubicar la acción "Restart Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a traves de la pestana "Activity and Logs" que en el dispositivo se realizo satisfactoriamente la operación		
9.2	Borrado del dispositivo y configuración de fabrica (Restore device to factory seeting) Ubicar la acción "Restore device to factory seeting" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a traves de la pestana "Activity and Logs" que en el dispositivo se realizo satisfactoriamente la operación		
9.3	Ping al dispositivo (Ping to device) Ubicar la acción "Ping to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a traves de la pestana "Activity and Logs" que en el dispositivo se realizo satisfactoriamente la operación		
9.4	Borrado del dispositivo (Delete device) Ubicar la acción "Delete Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a traves de la pestana "Activity and Logs" que en el dispositivo se realizo satisfactoriamente la operación		
9.5	(Start device trace) Ubicar la acción "Star device Trace" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a traves de la pestana "Activity and Logs" que en el dispositivo se realizo satisfactoriamente la operación		
9.6	(Trace to device) Ubicar la acción "Trace to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a traves de la pestana "Activity and Logs" que en el dispositivo se realizo satisfactoriamente la operación		
9.7	Acceso remoto al dispositivo (Access device remotely) Ubicar la acción "Access device remotely" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a traves de la pestana "Activity and Logs" que en el dispositivo se realizo satisfactoriamente la operación		
9.8	Reprovision CPE Ubicar la acción "Reprovision CPE" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a traves de la pestana "Activity and Logs" que en el dispositivo se realizo satisfactoriamente la operación		
CONFIGURATION BACKUP/RESTORE			
10.1	Ubicar la ventana "PORTS" Realizar un backup, especificando un nombre xxxxx, validar a traves de las tareas completadas que se ejecuto la instrucción de manera correcta.		
REVISIÓN RÁPIDA --- QUICK FIX			
11.1	Ubicar la ventana "QUICK FIX" Realizar el chequeo "FIX CONNECTIVITY" en donde se genere otra ventana con 4 datos relacionados a conectividad.		
11.2	Realizar el chequeo "FIX WIRELESS" en donde se genere otra ventana con 4 datos al wireless.		
CONFIGURACIÓN DEL DISPOSITIVO --- DEVICE SETTINGS			
12.1	Ubicar "Simplified View" Verificar el valor fijado y por defecto que tiene el parametro "inform interval"		
12.2	Verificar que la ruta coincida con la que se fijo en el modem para se evaluado en la plataforma Ubicar "Tab View"		
12.3	Realizar un (send update) modificando el valor "periodic inform interval), validar posteriormente que el dispositivo realizo satisfactoriamente la operación. (MANAGEMENT)		
12.4	Comparar las características con la ventana device information que se encuentra a la izquierda. (INFORMATION)		
12.5	Visualizar la direcciones IP o nombres de los diversos NTPServer (TIME)		
12.6	Visualizar las casillas referentes a PVC, ATMEncaps y ATMQoS (DSL)		
12.7	Visualizar las casillas referentes a Name, Default Gateway y DNSServer (WAN)		
12.8	Corroborar que el DHCP Lease Time corresponda con el establecido en la sección 5.1 (LAN)		
12.9	Visualización SSID, MaxRate, Channel, Standard (WIRELESS)		
RPC CUSTOM			
13.1	Ubicar "RPC Custom" GetParametersNames GetParametersValues GetParametersAttributes GetRPCMethods Reboot SetParametersAttributes SetParametersValues		
DIAGNOSTICOS Y MONITOREO --- DIAGNOSTICOS AND MONITORING			
14.1	En Diagnostics, ubicar la opción diagnostics type IPPingDiagnostics		
14.2	LoopbackDiagnostics		
14.3	DSLdiagnostics		
14.4	En Monitoring, hacer click en add parameters y se mostrara el abanico de parametros a monitorear WANDevice --> WANDevice.1 --> WANDSLInterfaceConfig (HACER CHECK EN EL PARAMETRO QUE SE DESEE)		
DESCARGA Y SUBIDA DE ARCHIVOS --- FILE DOWNLOAD AND UPLOAD			
15.1	Ubicar File Download Se selecciona el tipo de archivo que se desea (Firmware Image o Vendor Configuration File), luego se busca por lista o manualmente luego se ejecuta la Instrucción en "Send Update"		
15.2	Ubicar File Upload Se selecciona el tipo de archivo que se desea (Vendor Configuration File o Vendor Log File), luego se busca por lista o manualmente luego se ejecuta la Instrucción en "Send Update"		
ACTIVIDADES Y REGISTROS --- ACTIVITY AND LOGS			
16.1	Ubicar Activity Fijar por fecha y definir las actividades de todas las tareas o alguna en particular		
16.2	Ubicar Logs Fijar por fecha y definir los eventos de manera global o alguno en particular		

4.3 Descripción de los Dispositivos Evaluados

Los módems que se utilizaron son de tipo ADSL+2:

- Cinco (5) Módems BROADCOM (●).
- Dos (2) Módems HUAWEI (●).
- Un (1) Modem STARBRIDGE NETWORK (●)
- Un (1) Modem ZTE (●).
- Un (1) Modem ZyXEL (●).

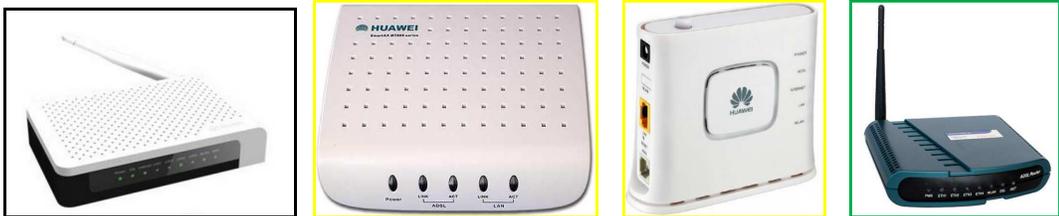


Figura 43: Módems (CPE) gestionados.

CAPÍTULO V

5. RESULTADOS Y ANÁLISIS

5.1 Visualización de los CPEs en la Plataforma

A continuación se presenta la pantalla principal para el CPE BROADCOM 190.74.55.35 en el Centro de Soporte (Support Center) de Friendly Technologies.

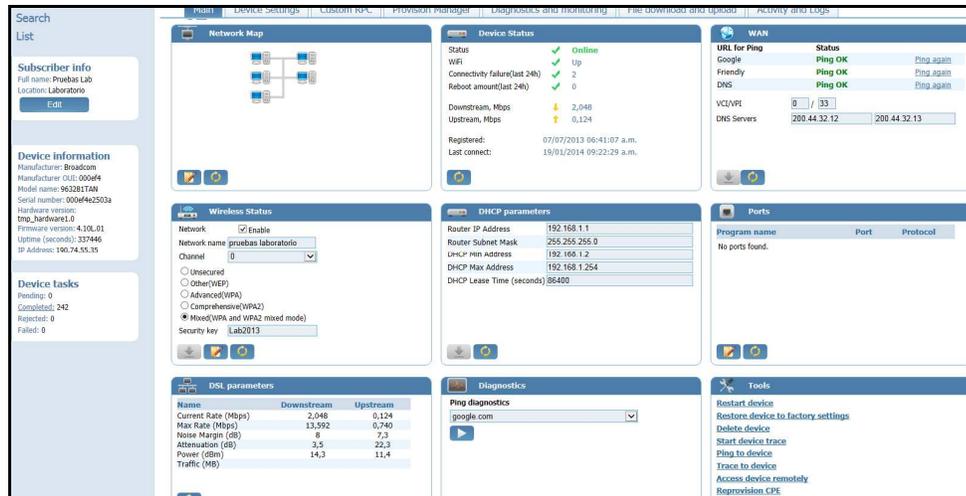


Figura 44: CPE BROADCOM 190.74.55.35

A continuación se presenta la pantalla principal para el CPE BROADCOM 190.203.136.48 en el Centro de Soporte (Support Center) Friendly Technologies.



Figura 45: CPE BROADCOM 190.203.136.48

A continuación se presenta la pantalla principal para el CPE BROADCOM 201.249.43.104 en el Centro de Soporte (Support Center) Friendly Technologies.

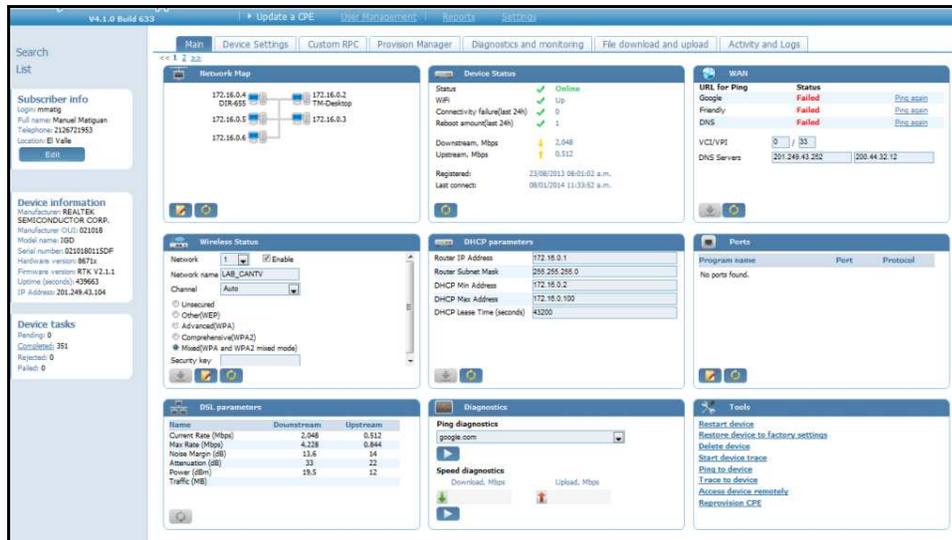


Figura 46: CPE BROADCOM 201.249.43.104

A continuación se presenta la pantalla principal para el CPE BROADCOM 190.38.248.83 en el Support Center (Friendly Technologies).

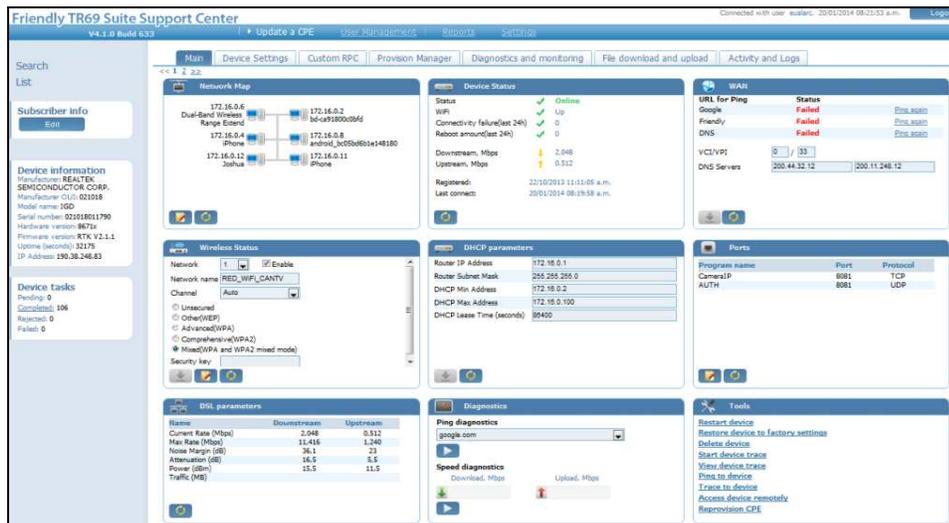


Figura 47: CPE BROADCOM 190.38.248.83

A continuación se presenta la pantalla principal para el CPE BROADCOM 201.208.21.167 en el Support Center (Friendly Technologies).

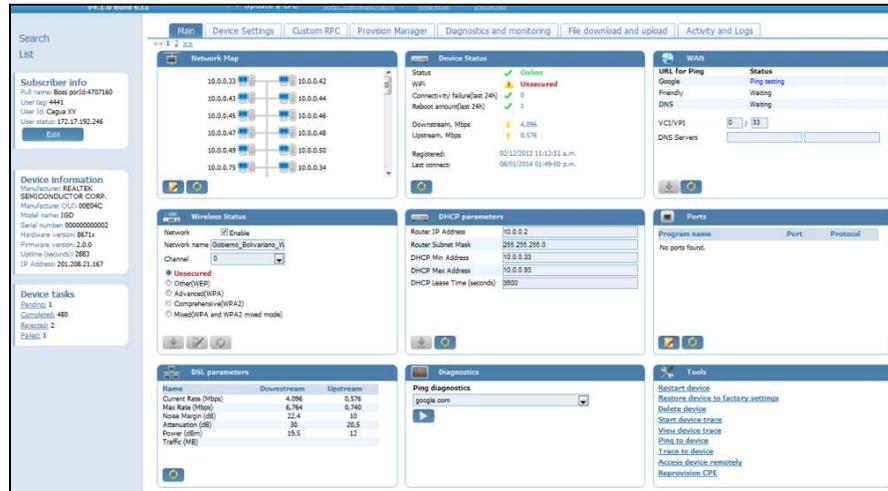


Figura 48: CPE BROADCOM 201.208.21.167

A continuación se presenta la pantalla principal para el CPE STARBRIDGE NETWORK 201.249.43.120 en el Support Center (Friendly Technologies).



Figura 49: CPE STARBRIDGE NETWORK 201.249.43.120

A continuación se presenta la pantalla principal para el CPE HUAWEI 190.72.245.116 en el Support Center (Friendly Technologies).

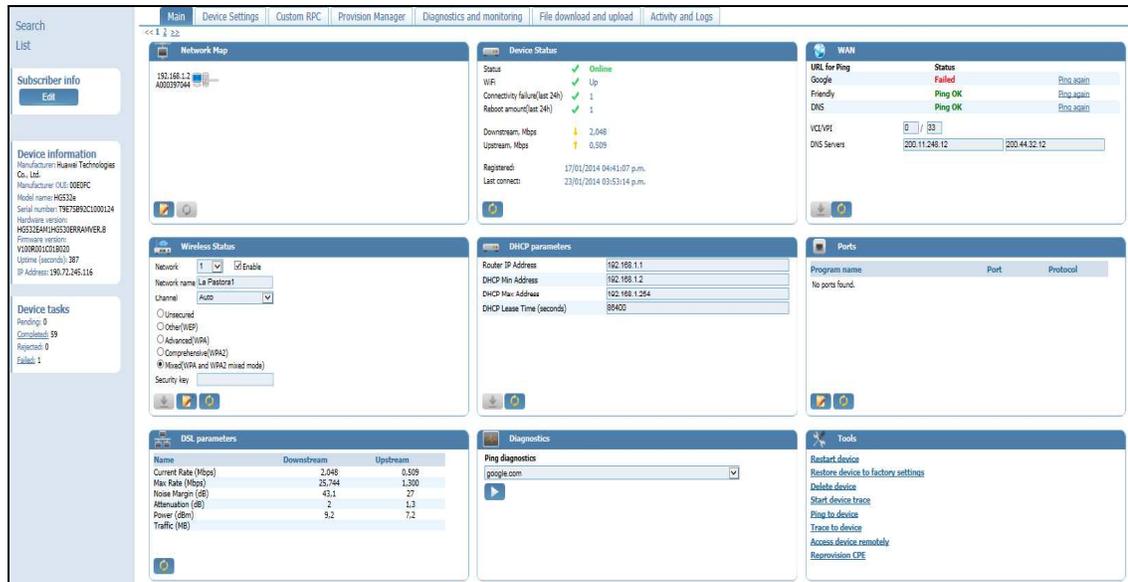


Figura 50: CPE HUAWEI 190.72.245.116

A continuación se presenta la pantalla principal para el CPE HUAWEI 190.79.199.34 en el Support Center (Friendly Technologies).

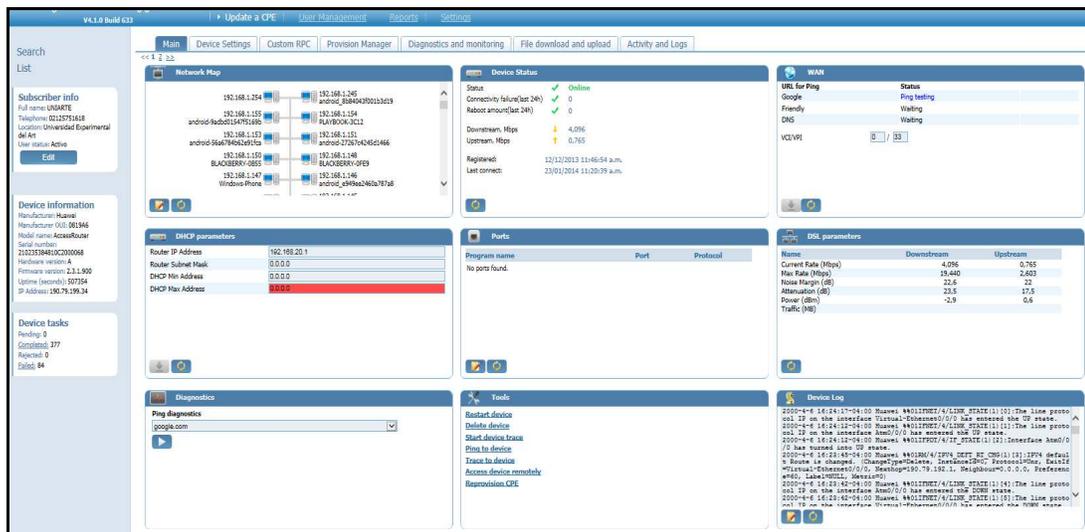


Figura 51: CPE HUAWEI 190.79.199.34

A continuación se presenta la pantalla principal para el CPE ZyXEL 201.249.43.119 en el Support Center (Friendly Technologies).

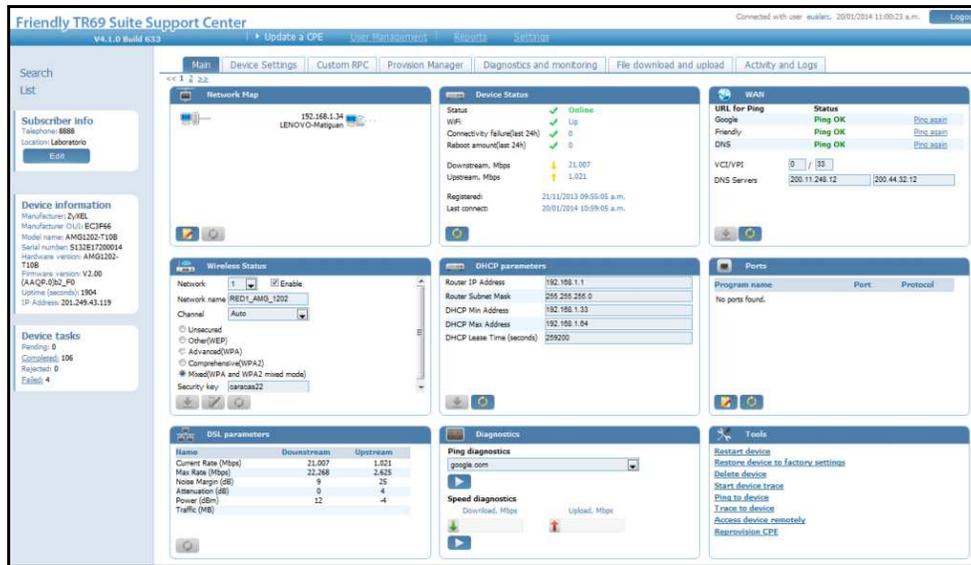


Figura 52: CPE ZyXEL 201.249.43.119

A continuación se presenta la pantalla principal para el CPE ZTE 201.249.43.122 en el Support Center (Friendly Technologies).

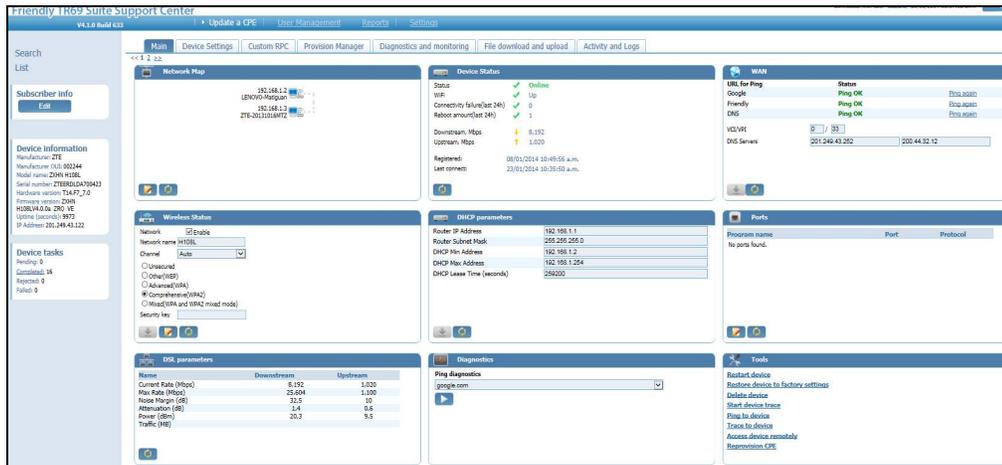


Figura 53: CPE ZTE 201.249.43.122

5.2 Análisis de Resultados

Luego de haber realizado todas las pruebas pertinentes en los módems, y verificar que en un porcentaje muy alto, estas se cumplieron satisfactoriamente, se puede afirmar que la plataforma de gestión remota FRIENDLY TECHNOLOGIES se encuentra en total cumplimiento con la tecnología actual, que involucra los protocolos de comunicación TR-069, TR-111, TR-104, TR-106 entre otros.

Se comprobó que la plataforma, es capaz de gestionar dispositivos en este caso simulados como si fueran pertenecientes a la red que posee un usuario específico, con los módems ADSL+2, permitiendo identificar, diagnosticar y resolver fallas de manera rápida.

Un punto resaltante en este capítulo es que la actualización de los CPEs se llevan a cabo con pocos clicks, es decir la configuración de actualizaciones tanto en la Consola de Administración (Management Console) como en el Centro de Soporte (Support Center), reducen considerablemente el proceso de actualizar los CPEs. La estructura de situar, escoger y identificar las opciones de actualizaciones en la plataforma, en pocos pasos, permite enviar información a los dispositivos añadidos a la plataforma, dicho proceso representa una transparencia para un supuesto usuario final, que seguramente reduciría llamadas al COR de CANTV relacionadas con la infraestructura, instalación y resolución de fallas.

Las diversas pruebas realizadas garantizan en una primera fase, la operatividad para diversos proveedores, el mantenimiento es remoto, el diagnóstico es inteligente para el operador de la plataforma, las ventanas de la plataforma son fáciles para ubicar una opción determinada, la gestión de configuración es sencilla y el registro de bitácora para cada CPE está perfectamente estructurado, almacena una gran cantidad de información vinculada al rendimiento, diagnóstico y monitoreo.

Finalmente, con las diversas pruebas de los módems en ambos sitios web, otro parámetro resaltante que ofrece la plataforma es la presentación de reportes y estadísticas, ya que este muestra reportes de un CPE particular o de un grupo de CPEs. El reporte supervisa, recoge los datos del CPE y además genera un estado del servicio del sistema del usuario.

La plataforma genera un conjunto completo de reportes para optimizar la capacidad de operación del servicio.

5.2 Red IP de Banda Ancha con TR-069

Configuración para la plataforma de CANTV una vez finalmente implementado la plataforma de gestión remota basado en el protocolo TR-069.

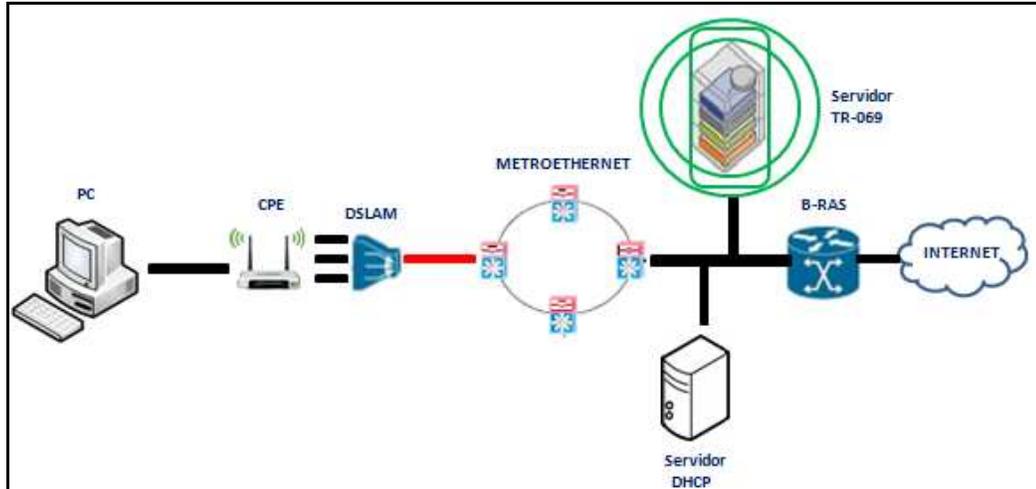


Figura 54: Red IP de Banda Ancha con TR-069

	Hoy	Mañana
Instalación de Dispositivos de Casa	<ul style="list-style-type: none"> • Visita a cada casa del suscriptor • Instalación en sitio • Requiere Personal Técnico / Costos Operativos 	<ul style="list-style-type: none"> • Visita a cada casa de suscriptor (opcional) • Plug and Play • Auto-instalación por parte del suscriptor
Activación de Servicio	<ul style="list-style-type: none"> • Visita a cada casa del suscriptor • Es necesario entrenar al instalador para realizar configuraciones complejas del servicio • Requiere mayor tiempo para activar los servicios 	<ul style="list-style-type: none"> • Auto-configuración • Plug and Play • Rápida activación del servicio
Diagnóstico y Troubleshooting	<ul style="list-style-type: none"> • Visita a cada casa del suscriptor • Mantenimiento en Sitio • Requiere de uso de Personal Técnico / Costos Operativos • Dificultad para encontrar la causa raíz • Requiere mas tiempo para recuperar el servicio 	<ul style="list-style-type: none"> • Diagnóstico Inteligente • Reporta la causa raíz de forma clara • Recuperación Remota
Mantenimiento de Rutina	<ul style="list-style-type: none"> • Mantenimiento en Sitio • Visita a cada casa del suscriptor • Requiere Personal Técnico / Costos Operativos 	<ul style="list-style-type: none"> • Mantenimiento Remoto (Firmware, Configuración, Reboot, Reset, etc.) • Operación por Lotes • Programación de Tareas

Figura 55: Ventajas de implementar TR-069

CONCLUSIONES

Friendly Technologies se presenta como una solución novedosa para el diagnóstico y monitoreo de CPEs, además el presente proyecto para Friendly no es el primero, esta empresa tiene reconocimiento a nivel mundial donde se ha evaluado de manera eficiente las prestaciones del servicio y la escalabilidad de dispositivos.

Luego de las pruebas en el Laboratorio de Estandarización de Equipos de CANTV, donde allí se encuentran los diversos servidores al igual que la variedad de módems, se observa que cumple satisfactoriamente con las expectativas de auto-gestión para los CPEs que inicialmente se habían fijado.

La plataforma dispone una infinidad de soluciones enfocadas a los requerimientos de la tecnología y para el operador como protagonista secundario, de la misma manera reduce notablemente los tiempos de ubicación de una falla y finalmente podría hacer que el usuario sea transparente al momento de resolver alguna falla específica en el servicio.

El diseño del Management Console y el Support Center de Friendly presentan una gran ventaja al operador de ubicar fácil y rápidamente los despliegues de instrucciones, esto representa eficiencia en todos los tópicos de la gestión.

Otro punto a destacar de la plataforma es en el formato de actividades o diagnósticos dependiendo del estatus de la instrucción realizada, esta es sombreada en 4 colores distintos, cada una de ella con etiqueta de la siguiente manera:

Azul claro – Activa – Active

Blanco – Completada – Completed

Rosado – Error – Error

Gris – No Posee Información – No Info

Identificación visual del cómo va la instrucción en un momento determinado.

La documentación existente permite realizar el enfoque para poder llevar a cabo una segunda fase para las pruebas de los módems y chequear las otras ventajas que ofrece

la plataforma con el ACS como protagonista principal, igualmente ya en un mediano plazo evaluar compatibilidad con la parte de OSS de CANTV. La temática de la plataforma de Friendly Technologies luego de la verificación de la primera fase invita a pensar que un número mayor de dispositivos pueden ser agregados y gestionados de manera eficiente, y a la vez poner en práctica las otras instrucciones y evaluaciones como podrían ser para el servicio de ABA de CANTV.

RECOMENDACIONES

En esta sección correspondiente a las recomendaciones al proyecto, en primer lugar es que en la segunda fase del mismo se tomen en cuenta un número mayor de dispositivos y con proveedores diversos. De manera que en el mediano plazo se evalué la escalabilidad de gestión con ese mayor número de equipos y a la vez el manejo de los datos, instrucciones, tareas, y archivos. Bajo esta premisa se iría pensado en gestionar tareas para grupos, por categoría o por fechas.

Paralelamente la factibilidad de esta plataforma de gestión remota está vinculada a trabajar para las diversas marcas existentes en el mercado y así permitir a CANTV un abanico de opciones en los acuerdos, reglamentos y permisos con los proveedores.

Un punto importante en la realización de este estudio, es la necesidad de CANTV de tener dentro de la ventana de los diagnósticos, la prueba de velocidad (o mejor conocida como speed test), esta prueba está directamente vinculada con la norma TR-143 la cual como se hizo mención en el segundo capítulo es la encargada de las pruebas de rendimiento y de seguimiento estadístico. A los diversos módems que se realizaron las pruebas de rigor en la plataforma solo 3 modems lo soportaban, es por ello lo imprescindible de que todos los proveedores incluyan en la configuración de fábrica de sus módems la norma TR-143. Para así garantizar de manera directa la ejecución de esta prueba.

En un segundo punto, sería poder colocar alarmas en los datos relacionados a los parámetros DSL de manera de si en un momento ese valor esta fuera del rango considerado como normal, considerar inmediatamente que parámetro se encuentra crítico y atacarlo como una falla puntual.

En un tercer punto de estudio, la prueba de diagnóstico relacionada a los ping con las páginas google, friendly o el 80.80.808.80 en una buena parte de todos los módems no fue satisfactoria pero al colocar su valor ip la prueba se hace 100 % efectiva, lo mejor para las siguientes evaluaciones es colocar para esas pruebas de ping, la dirección IP directamente.

Como apoyo a este punto, es necesario acotar que para el modem Broadcom (con ip 201.208.21.167) no se hizo correcto el IpDiagnostics en la ventana de la WAN, se escribió la dirección IP del servidor DNS pero abortó dicha instrucción como un error.

El cuarto punto está asociado al proyecto WIFI en el cual se agregaron una cantidad de dispositivos y solo aparece uno, todos ellos tienen el mismo serial y pertenecen al mismo fabricante, aparece uno distinto cada 600 segundos debido a que cambia su IP y la dirección MAC, el problema se abordó y está asociado a la configuración de los módems y eso se resuelve es con el proveedor.

(La plataforma de friendly no tiene que ver con este con esta situación, pero es indispensable acotarla acá en el informe para plantearse al proveedor).

REFERENCIAS BIBLIOGRÁFICAS

Las siguientes referencias están asociadas con los componentes necesarios del TR-069.

- [1] Simple Object Access Protocol (SOAP) 1.1,
<http://www.w3.org/TR/2000/NOTESOAAP-20000508>
- [2] RFC 2965, HTTP State Management Mechanism,
<http://www.ietf.org/rfc/rfc2965.txt>
- [3] RFC 5246, The Transport Layer Security (TLS) Protocol, Version 1.2,
<http://www.ietf.org/rfc/rfc5246.txt>
- [4] TR-098 Amendment 2, Internet Gateway Device Data Model for TR-069.
- [5] TR-104, Provisioning Parameters for VoIP CPE, Broadband Forum Technical Report.
- [6] TR-135, Data Model for a TR-069 Enabled STB, Broadband Forum Technical Report.
- [7] TR-140 Issue 1.1, TR-069 Data Model for Storage Service Enabled Devices.
- [8] TR-143 Corrigendum 2, Enabling Network Throughput Performance Tests and Statistical M.
- [9] TR-157 Amendment 3, Component Objects for CWMP, Broadband Forum Technical Report.
- [10] TR-181 Issue 1, Device Data Model for TR-069, Broadband Forum Technical Report.
- [11] TR-181 Issue 2, Device Data Model for TR-069, Broadband Forum Technical Report.
- [12] RFC 2616, Hypertext Transfer Protocol – HTTP/1.1,
<http://www.ietf.org/rfc/rfc2616.txt>
- [13] XML-Signature Syntax and Processing,
<http://www.w3.org/2000/09/xmldsig>
- [14] TR-106 Amendment 4, Data Model Template for TR-069-Enabled Devices.
- [15] TR-110, Amendment 3, for VoIP Configuration.
- [16] RFC 2131, Dynamic Host Configuration Protocol,
<http://www.ietf.org/rfc/rfc2131.txt>

- [17] Organizationally Unique Identifiers (OUIs)
<http://www.standards.ieee.org/faqs/OUI.html>
- [18] TR-111, Amendment 3, for LAN/NAT Devices
- [19] TR-131, Amendment 3, for NBI Northbound Interface Requeriment
- [20] TR-142, Amendment 3, for PON Devices
- [21] TR-156, Amendment 3, for GPON Access

BIBLIOGRAFÍA

- AG Communication Systems. *Asymmetric Digital Subscriber Line (ADSL)*. Tutorial. <http://www.iec.org>
- Auto-Configuration Server (ACS). *Sizing Consideration Fundamentals & Systems Hardware Requirements*. V 2.4.2. April, 2012.
- Auto-Configuraron Server (ACS). *CANTV 2013*. Agosto 2013.
- CANTV, Página web, www.cantv.com.ve
- CPE Diagnostics Made Easy. Guide Incognito Software.
- Goralki, Walter. 2000. *Tecnologías ADSL y XDSL*. McGrawHill/Interamericana de España. S.A.U.
- TR-069, Amendment 3. *CPE WAN Management Protocol*, Protocol versión: 1.2. Issue Date: November 2010.
- Manual. *Homologación Informe TW_DSL699S, sin USB*. CANTV. Junio 2013.
- Friendly Technologies. Gestión de dispositivos. Friendly Portafolio. 2013.
- Friendly Technologies. Zero Touch Provisioning of CPEs. Brochure. 2013.
- Friendly Technologies. Administración y Optimización de dispositivos. Folleto 2013.
- Friendly Technologies. Friendly Support Center. Datasheet. 2013.
- Friendly Support Center Login, <http://201.249.43.253/CSR/Login.aspx>
- Friendly Management Console Login, <http://201.249.43.253/CpeAdmin/Login.aspx>
- Documento: Arquitecturas de redes y plataformas de servicios de CANTV, Julio, 2006.
- Centro de Operaciones de la Red (COR) CANTV. Manuales y documentos, Caracas: 2013.

ANEXOS

PLANTILLAS DE PRUEBAS PARA CPEs "BROADCOM"

CANTV -- Centro Nacional de telecomunicación de CANTV Gerencia de Planificación y Arquitectura de TI Laboratorio de Estandarización. Edif. Equipos II /Piso 6 (BROADCOM -- 963281TAN -- 190.74.55.35 -- 4.10L.01)		 		
		ESTATUS	EXPLICACIÓN EN DETALLE	VINCULO
		SI / NO		
MAPA DE RED --- NETWORK MAP				
Ubicar en la ventana "Network Map" el conjunto de dispositivos que se encuentran conectados con el dispositivo (modem) en estudio				
1.1	La prueba consiste en desconectar o quitar alguno(s) de los dispositivos y verificar que desaparezca del mapa, puede utilizarse el botón "refresh" de manera de actualizar el mapa	✓	5 Equipos	
ESTATUS DEL DISPOSITIVO --- DEVICE STATUS				
Ubicar en la ventana "Device Status" las características principales del modem				
2.1	Status: ONLINE / OFFLINE	✓		
2.2	Wifi: UP / DOWN	✓		
2.3	Falla de conectividad : (Representa el número de fallas que ha tenido en las últimas 24 horas)	✓	2	
2.4	Número de reinicios del dispositivo : (Representa el número de reinicio que ha tenido en las últimas 24 horas)	✓	0	
2.5	Verificar que los valores que aparecen en <u>downstream</u> y <u>Upstream</u> coincidan con los valores de la ventana de los parámetros de línea DSL (DSL Parameters)	✓		
WAN				
Ubicar la ventana "WAN" y hacer ping de prueba a las siguientes URL:				
3.1	Google Validar el ping testing	✓		
	Friendly Validar el ping testing	✓		
	DNS Validar el ping testing	✓		
WIRELESS STATUS				
Ubicar la ventana "Wireless Status"				
4.1	Desactivar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
4.2	Activar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
4.3	Modificar el nombre de la red "Network Name" y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
4.4	Modificar la contraseña "Security Key" y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
PARAMETROS DHCP --- DHCP PARAMETERS				
Ubicar la ventana "DHCP Parameters"				
5.1	Hacer cambios sobre la operación DHCP Lease Time (seconds), 86400seg (1dia), 129600seg (DiyMedio) Validar posteriormente que la creación de la tarea, se realizo.	✓	86400 259200	
PUERTOS --- PORTS				
Ubicar la ventana "PORTS"				
6.1	Verificar el número de camaras IP activas y identificación de los puertos asociadas a las mismas.	✓	"0" Dispositivos	
PARAMETROS DSL --- DSL PARAMETERS				
Ubicar la ventana "DSL Parameters", apareceran los siguientes parametros:				
7.1	Current Rate	✓		
	Max Rate	✓		
	Noise Margin	✓		
	Attenuation	✓		
	Power	✓		
	Traffic	✓		
DIAGNOSTICOS (PING DIAGNOSTICS AND SPEED TEST)				
Ubicar el recuadro "Diagnostics", en la casilla desplegable "Ping Diagnostics" apareceran varias opciones entre las cuales estan:				
8.1	google.com	✓		
	80.80.80.80	✗		
	friendly.com	✓		
	Enter URL/IP 200.44.32.12	✓		
	Escoja una de las opciones y ejecute el botón que se encuentra debajo PLAY y verifique que se llevo a cabo la tarea			
8.2	En el mismo recuadro "Diagnostics" se ubicará la ejecución "SPEED TEST" (esta solo podra ejecutarse en aquellos modems que soporten TR-143). Utilice el botón que se encuentra debajo PLAY y al instante debe evaluarse la velocidad download y upload en Mbps. Validar esos resultados	✗	NO SOPORTA TR-143	

HERRAMIENTAS --- TOOLS				
9.1	Reinicio del dispositivo (Restart Device) Ubicar la acción "Restart Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.2	Borrado del dispositivo y configuración de fabrica (Restore device to factory setting) Ubicar la acción "Restore device to factory setting" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.3	Ping al dispositivo (Ping to device) Ubicar la acción "Ping to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.4	Borrado del dispositivo (Delete device) Ubicar la acción "Delete Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación			
9.5	(Start device trace) Ubicar la acción "Star device Trace" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.6	(Trace to device) Ubicar la acción "Trace to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✗		
9.7	Acceso remoto al dispositivo (Access device remotely) Ubicar la acción "Access device remotely" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.8	Reprovisión CPE Ubicar la acción "Reprovision CPE" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✗		
CONFIGURATION BACKUP/RESTORE				
10.1	Ubicar la ventana "CONFIG BACKUP/RESTORE" Realizar un backup, especificando un nombre xxxxx, validar a través de las tareas completadas que se ejecuto la instrucción de manera correcta.	✓	eupruebaslab01	
REVISIÓN RÁPIDA --- QUICK FIX				
	Ubicar la ventana "QUICK FIX"			
11.1	Realizar el chequeo "FIX CONNECTIVITY" en donde se genere otra ventana con 4 datos relacionados a conectividad.	✓		
11.2	Realizar el chequeo "FIX WIRELESS" en donde se genere otra ventana con 4 datos al wireless.	✓		
CONFIGURACIÓN DEL DISPOSITIVO --- DEVICE SETTINGS				
	Ubicar "Simplified View"			
12.1	Verificar el valor fijado y por defecto que tiene el parámetro "inform interval"	✓	600	
12.2	Verificar que la ruta coincide con la que se fija en el modem para ser evaluado en la plataforma	✓		
	Ubicar "Tab View"			
12.3	Realizar un (send update) modificando el valor "periodic inform interval", validar posteriormente que el dispositivo realizó satisfactoriamente la operación. (MANAGEMENT)	✓	500	
12.4	Comparar las características con la ventana device information que se encuentra a la izquierda. (INFORMATION)	✓		
12.5	Visualizar la direcciones IP o nombres de los diversos NTPServer (TIME)	✓		
12.6	Visualizar las casillas referentes a PVC, ATMEncaps y ATMQoS (DSL)	✓		
12.7	Visualizar las casillas referentes a Name, Default Gateway y DNSServer (WAN)	✓		
12.8	Corroborar que el DHCP Lease Time corresponda con el establecido en la sección 5.1 (LAN)	✓		
12.9	Visualización SSID, MaxRate, Channel, Standard (WIRELESS)	✓		
RPC CUSTOM				
	Ubicar "RPC Custom"			
13.1	GetParametersNames	✓		
	GetParametersValues	✓		
	GetParametersAttributes	✗		
	GetRPCMethods	✓		
	Reboot	✓		
	SetParametersAttributes	✓		
	SetParametersValues	✓		
DIAGNOSTICOS Y MONITOREO --- DIAGNOSTICOS AND MONITORING				
	En Diagnostics, ubicar la opción diagnostics type			
14.1	IPPingDiagnostics	✓		
14.2	LoopbackDiagnostics	✓		
14.3	DSL Dagnostics	✓		
	En Monitoring, hacer click en add parameters y se mostrara el abanico de parametros a monitorear			
14.4	WANDevice --> WANDevice.1 --> WANDSLInterfaceConfig (HACER CHECK EN EL PARAMETRO QUE SE DESEE)	✓		
DESCARGA Y SUBIDA DE ARCHIVOS --- FILE DOWNLOAD AND UPLOAD				
	Ubicar File Download			
15.1	Se selecciona el tipo de archivo que se desea (Firmware Image o Vendor Configuration File), luego se busca por lista o manualmente luego se ejecuta la instrucción en "Send Update"	✓		
	Ubicar File Upload			
15.2	Se selecciona el tipo de archivo que se desea (Vendor Configuration File o Vendor Log File), luego se busca por lista o manualmente luego se ejecuta la instrucción en "Send Update"	✓		
ACTIVIDADES Y REGISTROS --- ACTIVITY AND LOGS				
	Ubicar Activity			
16.1	Fijar por fecha y definir las actividades de todas las tareas o alguna en particular	✓		
	Ubicar Logs			
16.2	Fijar por fecha y definir los eventos de manera global o alguno en particular	✓		

CANTV -- Centro Nacional de telecomunicación de CANTV Gerencia de Planificación y Arquitectura de TI Laboratorio de Estandarización. Edif. Equipos II /Piso 6 (BROADCOM -- 963281TAN -- 190.203.136.48 -- 4.10L.01)		cantv		friendly technologies	
BROADCOM		ESTATUS	EXPLICACIÓN EN DETALLE	VINCULO	
MAPA DE RED --- NETWORK MAP		SI / NO			
Ubicar en la ventana "Network Map" el conjunto de dispositivos que se encuentran conectados con el dispositivo (modem) en estudio					
1.1	La prueba consiste en desconectar o quitar alguno(s) de los dispositivos y verificar que desaparezca del mapa, puede utilizarse el botón "refresh" de manera de actualizar el mapa	✓	4 Equipos		
ESTATUS DEL DISPOSITIVO --- DEVICE STATUS					
Ubicar en la ventana "Device Status" las características principales del modem					
2.1	Status; ONLINE / OFFLINE	✓			
2.2	Wifi; UP / DOWN	✓			
2.3	Falla de conectividad : (Representa el número de fallas que ha tenido en las últimas 24 horas)	✓	0		
2.4	Número de reinicios del dispositivo : (Representa el número de reinicio que ha tenido en la últimas 24 horas)	✓	0		
2.5	Verificar que los valores que aparecen en <u>downstream</u> y <u>Upstream</u> coincidan con los valores de la ventana de los parámetros de línea DSL (DSL Parameters)	✓			
WAN					
Ubicar la ventana "WAN" y hacer ping de prueba a las siguientes URL:					
3.1	Google Validar el ping testing	✓			
	Friendly Validar el ping testing	✓			
	DNS Validar el ping testing	✓			
WIRELESS STATUS					
Ubicar la ventana "Wireless Status"					
4.1	Desactivar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓			
4.2	Activar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓			
4.3	Modificar el nombre de la red "Network Name" y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓			
4.4	Modificar la contraseña "Security Key" y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓			
PARAMETROS DHCP --- DHCP PARAMETERS					
Ubicar la ventana "DHCP Parameters"					
5.1	Hacer cambios sobre la operación DHCP Lease Time (seconds), 86400seg (1dia), 129600seg (DiyMedio) Validar posteriormente que la creación de la tarea, se realizo.	✓	86400 43200		
PUERTOS --- PORTS					
Ubicar la ventana "PORTS"					
6.1	Verificar el número de camaras IP activas y identificación de los puertos asociadas a las mismas.	✓	"2" Dispositivos		
PARAMETROS DSL --- DSL PARAMETERS					
Ubicar la ventana "DSL Parameters", apareceran los siguientes parametros:					
7.1	Current Rate	✓			
	Max Rate	✓			
	Noise Margin	✓			
	Attenuation	✓			
	Power	✓			
	Traffic	✓			
DIAGNOSTICOS (PING DIAGNOSTICS AND SPEED TEST)					
Ubicar el recuadro "Diagnostics", en la casilla desplegable "Ping Diagnostics" apareceran varias opciones entre las cuales estan:					
8.1	google.com	✘	TIMEOUT		
	80.80.80.80	✘			
	friendly.com	✓			
	Enter URL/IP 200.44.32.12	✓			
Escoja una de las opciones y ejecute el boton que se encuentra debajo PLAY y verifique que se llevo a cabo la tarea					
8.2	En el mismo recuadro "Diagnostics" se ubicará la ejecución "SPEED TEST" (esta solo podra ejecutarse en aquellos modems que soporten TR-143). Utilice el botón que se encuentra debajo PLAY y al instante debe evaluarse la velocidad download y upload en Mbps. Validar esos resultados	✘	NO SOPORTA TR-143		

HERRAMIENTAS --- TOOLS				
9.1	Reinicio del dispositivo (Restart Device) Ubicar la acción "Restart Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.2	Borrado del dispositivo y configuración de fabrica (Restore device to factory seeting) Ubicar la acción "Restore device to factory seeting" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.3	Ping al dispositivo (Ping to device) Ubicar la acción "Ping to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.4	Borrado del dispositivo (Delete device) Ubicar la acción "Delete Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación			
9.5	(Start device trace) Ubicar la acción "Star device Trace" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓	NO APARECE LA OPCIÓN "VIEW DEVICE TRACE"	
9.6	(Trace to device) Ubicar la acción "Trace to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación			
9.7	Acceso remoto al dispositivo (Access device remotely) Ubicar la acción "Access device remotely" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✗		
9.8	Reprovision CPE Ubicar la acción "Reprovision CPE" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✗		
CONFIGURATION BACKUP/RESTORE				
	Ubicar la ventana "CONFIG BACKUP/RESTORE"			
10.1	Realizar un backup, especificando un nombre xxxxx, validar a través de las tareas completadas que se ejecuto la instrucción de manera correcta.	✓	eummati01	
REVISIÓN RÁPIDA --- QUICK FIX				
	Ubicar la ventana "QUICK FIX"			
11.1	Realizar el chequeo "FIX CONNECTIVITY" en donde se genere otra ventana con 4 datos relacionados a conectividad.	✓		
11.2	Realizar el chequeo "FIX WIRELESS" en donde se genere otra ventana con 4 datos al wireless.	✓		
CONFIGURACIÓN DEL DISPOSITIVO --- DEVICE SETTINGS				
	Ubicar "Simplified View"			
12.1	Verificar el valor fijado y por defecto que tiene el parametro "inform interval"	✓	600	
12.2	Verificar que la ruta coincida con la que se fija en el modem para se evaluado en la plataforma	✓		
	Ubicar "Tab View"			
12.3	Realizar un (send update) modificando el valor "periodic inform interval", validar posteriormente que el dispositivo realizo satisfactoriamente la operación. (MANAGEMENT)	✓	720	
12.4	Comparar las características con la ventana device information que se encuentra a la izquierda. (INFORMATION)	✓		
12.5	Visualizar las direcciones IP o nombres de los diversos NTPServer (TIME)	✓		
12.6	Visualizar las casillas referentes a PVC, ATMEncaps y ATMQoS (DSL)	✓		
12.7	Visualizar las casillas referentes a Name, Default Gateway y DNSServer (WAN)	✓		
12.8	Corroborar que el DHCP Lease Time corresponda con el establecido en la sección 5.1 (LAN)	✓		
12.9	Visualización SSID, MaxRate, Channel, Standard (WIRELESS)	✓		
RPC CUSTOM				
	Ubicar "RPC Custom"			
13.1	GetParametersNames	✓		
	GetParametersValues	✓		
	GetParametersAttributes	✓		
	GetRPCMethods	✓		
	Reboot	✓		
	SetParametersAttributes	✓		
	SetParametersValues	✓		
DIAGNOSTICOS Y MONITOREO --- DIAGNOSTICOS AND MONITORING				
	En Diagnostics, ubicar la opción diagnostics type			
14.1	IPPingDiagnostics	✓		
14.2	LoopbackDiagnostics	✓		
14.3	DSLdiagnostics	✓		
	En Monitoring, hacer click en add parameters y se mostrara el abanico de parametros a monitorear			
14.4	WANDevice --> WANDevice.1 --> WANDSLInterfaceConfig (HACER CHECK EN EL PARAMETRO QUE SE DESEE)	✓		
DESCARGA Y SUBIDA DE ARCHIVOS --- FILE DOWNLOAD AND UPLOAD				
	Ubicar File Download			
15.1	Se selecciona el tipo de archivo que se desea (Firmware Image o Vendor Configuration File), luego se busca por lista o manualmente luego se ejecuta la instrucción en "Send Update"	✓		
	Ubicar File Upload			
15.2	Se selecciona el tipo de archivo que se desea (Vendor Configuration File o Vendor Log File), luego se busca por lista o manualmente luego se ejecuta la instrucción en "Send Update"	✓		
ACTIVIDADES Y REGISTROS --- ACTIVITY AND LOGS				
	Ubicar Activity			
16.1	Fijar por fecha y definir las actividades de todas las tareas o alguna en particular	✓		
	Ubicar Logs			
16.2	Fijar por fecha y definir los eventos de manera global o alguno en particular	✓		

CANTV -- Centro Nacional de telecomunicación de CANTV Gerencia de Planificación y Arquitectura de TI Laboratorio de Estandarización. Edif. Equipos II /Piso 6 (BROADCOM -- IGD -- 201.249.43.104 -- RTK V2.1.1)		 		
		ESTATUS	EXPLICACIÓN EN DETALLE	VINCULO
MAPA DE RED --- NETWORK MAP		SI / NO		
	Ubicar en la ventana "Network Map" el conjunto de dispositivos que se encuentran conectados con el dispositivo (modem) en estudio			
1.1	La prueba consiste en desconectar o quitar alguno(s) de los dispositivos y verificar que desaparezca del mapa, puede utilizarse el boton "refresh" de manera de actualizar el mapa	✓	5 Equipos	
ESTATUS DEL DISPOSITIVO --- DEVICE STATUS				
	Ubicar en la ventana "Device Status" las características principales del modem			
2.1	Status: ONLINE / OFFLINE	✓		
2.2	Wifi: UP / DOWN	✓		
2.3	Falla de conectividad : (Representa el número de fallas que ha tenido en las últimas 24 horas)	✓	0	
2.4	Número de reinicios del dispositivo : (Representa el número de reinicio que ha tenido en las últimas 24 horas)	✓	1	
2.5	Verificar que los valores que aparecen en downstream y Upstream coincidan con los valores de la ventana de los parámetros de línea DSL (DSL Parameters)	✓		
WAN				
	Ubicar la ventana "WAN" y hacer ping de prueba a las siguientes URL:			
3.1	Google Validar el ping testing	✗	FALLIDA	
	Friendly Validar el ping testing	✗	FALLIDA	
	DNS Validar el ping testing	✗	FALLIDA	
WIRELESS STATUS				
	Ubicar la ventana "Wireless Status"			
4.1	Desactivar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
4.2	Activar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
4.3	Modificar el nombre de la red "Network Name" y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
4.4	Modificar la contraseña "Security Key" y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
PARAMETROS DHCP --- DHCP PARAMETERS				
	Ubicar la ventana "DHCP Parameters"			
5.1	Hacer cambios sobre la operación DHCP Lease Time (seconds), 86400seg (1día), 129600seg (DiyMedio) Validar posteriormente que la creación de la tarea, se realizó.	✓	43200 86400	
PUERTOS --- PORTS				
	Ubicar la ventana "PORTS"			
6.1	Verificar el número de camaras IP activas y identificación de los puertos asociadas a las mismas.	✓	"0" Dispositivos	
PARAMETROS DSL --- DSL PARAMETERS				
	Ubicar la ventana "DSL Parameters", aparecieran los siguientes parametros:			
7.1	Current Rate	✓		
	Max Rate	✓		
	Noise Margin	✓		
	Attenuation	✓		
	Power	✓		
	Traffic	✓		
DIAGNOSTICOS (PING DIAGNOSTICS AND SPEED TEST)				
	Ubicar el recuadro "Diagnostics", en la casilla desplegable "Ping Diagnostics" aparecieran varias opciones entre las cuales estan:			
8.1	google.com	✗		
	80.80.80.80	✗		
	friendly.com	✗		
	Enter URL/IP 200.44.32.12	✓		
	Escoja una de las opciones y ejecute el boton que se encuentra debajo PLAY y verifique que se llevo a cabo la tarea			
8.2	En el mismo recuadro "Diagnostics" se ubicará la ejecución "SPEED TEST" (esta solo podra ejecutarse en aquellos modems que soporten TR-143). Utilice el botón que se encuentra debajo PLAY y al instante debe evaluarse la velocidad download y upload en Mbps. Validar esos resultados	✓	Soporta TR-143 (No realiza el speed test)	

HERRAMIENTAS --- TOOLS				
9.1	Reinicio del dispositivo (Restart Device) Ubicar la acción "Restart Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.2	Borrado del dispositivo y configuración de fabrica (Restore device to factory seeting) Ubicar la acción "Restore device to factory seeting" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación			
9.3	Ping al dispositivo (Ping to device) Ubicar la acción "Ping to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.4	Borrado del dispositivo (Delete device) Ubicar la acción "Delete Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación			
9.5	(Start device trace) Ubicar la acción "Star device Trace" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		NO APARECE LA OPCIÓN "VIEW TRACE DEVICE"
9.6	(Trace to device) Ubicar la acción "Trace to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✗		
9.7	Acceso remoto al dispositivo (Access device remotely) Ubicar la acción "Access device remotely" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.8	Reprovisión CPE Ubicar la acción "Reprovision CPE" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✗		
CONFIGURATION BACKUP/RESTORE				
Ubicar la ventana "CONFIG BACKUP/RESTORE"				
10.1	Realizar un backup, especificando un nombre xxxxx, validar a través de las tareas completadas que se ejecuto la instrucción de manera correcta.	✓	euelvalle01	
REVISIÓN RÁPIDA --- QUICK FIX				
Ubicar la ventana "QUICK FIX"				
11.1	Realizar el chequeo "FIX CONNECTIVITY" en donde se genere otra ventana con 4 datos relacionados a conectividad.	✓		
11.2	Realizar el chequeo "FIX WIRELESS" en donde se genere otra ventana con 4 datos al wireless.	✓		
CONFIGURACIÓN DEL DISPOSITIVO --- DEVICE SETTINGS				
Ubicar "Simplified View"				
12.1	Verificar el valor fijado y por defecto que tiene el parámetro "inform interval"	✓	600	
12.2	Verificar que la ruta coincida con la que se fija en el modem para se evaluado en la plataforma	✓		
Ubicar "Tab View"				
12.3	Realizar un (send update) modificando el valor "periodic inform interval", validar posteriormente que el dispositivo realizo satisfactoriamente la operación. (MANAGEMENT)	✓	500	
12.4	Comparar las características con la ventana device information que se encuentra a la izquierda. (INFORMATION)	✓		
12.5	Visualizar la direcciones IP o nombres de los diversos NTPServer (TIME)	✓		
12.6	Visualizar las casillas referentes a PVC, ATMEncaps y ATMQoS (DSL)	✓		
12.7	Visualizar las casillas referentes a Name, Default Gateway y DNSServer (WAN)	✓		
12.8	Corroborar que el DHCP Lease Time corresponda con el establecido en la sección 5.1 (LAN)	✓		
12.9	Visualización SSID, MaxRate, Channel, Standard (WIRELESS)	✓		
RPC CUSTOM				
Ubicar "RPC Custom"				
13.1	GetParametersNames	✓		
	GetParametersValues	✓		
	GetParametersAttributes	✓		
	GetRPCMethods	✓		
	Reboot	✓		
	SetParametersAttributes	✗		
	SetParametersValues	✓		
DIAGNOSTICOS Y MONITOREO --- DIAGNOSTICOS AND MONITORING				
En Diagnostics, ubicar la opción diagnostics type				
14.1	IPPingDiagnostics	✓		
14.2	LoopbackDiagnostics	✓		
14.3	DSLdDiagnostics	✓		
En Monitoring, hacer click en add parameters y se mostrara el abanico de parametros a monitorear				
14.4	WANDevice --> WANDevice.1 --> WANDSInterfaceConfig (HACER CHECK EN EL PARAMETRO QUE SE DESEE)	✓		
DESCARGA Y SUBIDA DE ARCHIVOS --- FILE DOWNLOAD AND UPLOAD				
Ubicar File Download				
15.1	Se selecciona el tipo de archivo que se desea (Firmware Image o Vendor Configuration File), luego se busca por lista o manualmente luego se ejecuta la instrucción en "Send Update"	✓		
Ubicar File Upload				
15.2	Se selecciona el tipo de archivo que se desea (Vendor Configuration File o Vendor Log File), luego se busca por lista o manualmente luego se ejecuta la instrucción en "Send Update"	✓		
ACTIVIDADES Y REGISTROS --- ACTIVITY AND LOGS				
Ubicar Activity				
16.1	Fijar por fecha y definir las actividades de todas las tareas o alguna en particular	✓		
Ubicar Logs				
16.2	Fijar por fecha y definir los eventos de manera global o alguno en particular	✓		

CANTV -- Centro Nacional de telecomunicación de CANTV Gerencia de Planificación y Arquitectura de TI Laboratorio de Estandarización. Edif. Equipos II /Piso 6 (BROADCOM -- IGD -- 190.38.248.83 -- RTK V2.1.1)		 		
		ESTATUS	EXPLICACIÓN EN DETALLE	VINCULO
MAPA DE RED --- NETWORK MAP		SI / NO		
Ubicar en la ventana "Network Map" el conjunto de dispositivos que se encuentran conectados con el dispositivo (modem) en estudio				
1.1	La prueba consiste en desconectar o quitar alguno(s) de los dispositivos y verificar que desaparezca del mapa, puede utilizarse el boton "refresh" de manera de actualizar el mapa	✓	6 Equipos	
ESTATUS DEL DISPOSITIVO --- DEVICE STATUS				
Ubicar en la ventana "Device Status" las características principales del modem				
2.1	Status: ONLINE / OFFLINE	✓		
2.2	Wifi: UP / DOWN	✓		
2.3	Falla de conectividad : (Representa el número de fallas que ha tenido en las últimas 24 horas)	✓	0	
2.4	Número de reinicios del dispositivo : (Representa el número de reinicio que ha tenido en las últimas 24 horas)	✓	0	
2.5	Verificar que los valores que aparecen en downstream y Upstream coincidan con los valores de la ventana de los parámetros de línea DSL (DSL Parameters)	✓		
WAN				
Ubicar la ventana "WAN" y hacer ping de prueba a las siguientes URL:				
3.1	Google Validar el ping testing	✗	FALLIDA	
	Friendly Validar el ping testing	✗	FALLIDA	
	DNS Validar el ping testing	✗	FALLIDA	
WIRELESS STATUS				
Ubicar la ventana "Wireless Status"				
4.1	Desactivar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completó y aparezca el estado del módulo como válido.	✓		
4.2	Activar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completó y aparezca el estado del módulo como válido.	✓		
4.3	Modificar el nombre de la red "Network Name" y validar posteriormente que la creación de la tarea, se completó y aparezca el estado del módulo como válido.	✓		
4.4	Modificar la contraseña "Security Key" y validar posteriormente que la creación de la tarea, se completó y aparezca el estado del módulo como válido.	✓		
PARAMETROS DHCP --- DHCP PARAMETERS				
Ubicar la ventana "DHCP Parameters"				
5.1	Hacer cambios sobre la operación DHCP Lease Time (seconds), 86400seg (1dia), 129600seg (DayMedio) Validar posteriormente que la creación de la tarea, se realizó.	✓	86400 259200	
PUERTOS --- PORTS				
Ubicar la ventana "PORTS"				
6.1	Verificar el número de camaras IP activas y identificación de los puertos asociadas a las mismas.	✓	"2" Dispositivos	
PARAMETROS DSL --- DSL PARAMETERS				
Ubicar la ventana "DSL Parameters", apareceran los siguientes parametros:				
7.1	Current Rate	✓		
	Max Rate	✓		
	Noise Margin	✓		
	Attenuation	✓		
	Traffic	✓		
DIAGNOSTICOS (PING DIAGNOSTICS AND SPEED TEST)				
Ubicar el recuadro "Diagnostics", en la casilla desplegable "Ping Diagnostics" apareceran varias opciones entre las cuales estan:				
8.1	google.com	✗		
	80.80.80.80	✗		
	friendly.com	✗		
	Enter URL/IP 200.44.32.12	✗		
Escoja una de las opciones y ejecute el boton que se encuentra debajo PLAY y verifique que se llevo a cabo la tarea				
8.2	En el mismo recuadro "Diagnostics" se ubicará la ejecución "SPEED TEST" (esta solo podra ejecutarse en aquellos modems que soporten TR-143). Utilice el botón que se encuentra debajo PLAY y al instante debe evaluarse la velocidad download y upload en Mbps. Validar esos resultados	✓	Soporta TR-143 (No realiza el speed test)	

HERRAMIENTAS --- TOOLS				
9.1	Reinicio del dispositivo (Restart Device) Ubicar la acción "Restart Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.2	Borrado del dispositivo y configuración de fabrica (Restore device to factory seeting) Ubicar la acción "Restore device to factory seeting" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación			
9.3	Ping al dispositivo (Ping to device) Ubicar la acción "Ping to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.4	Borrado del dispositivo (Delete device) Ubicar la acción "Delete Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación			
9.5	(Start device trace) Ubicar la acción "Star device Trace" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.6	(Trace to device) Ubicar la acción "Trace to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✗		
9.7	Acceso remoto al dispositivo (Access device remotely) Ubicar la acción "Access device remotely" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✗		
9.8	Reprovision CPE Ubicar la acción "Reprovision CPE" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✗		
CONFIGURATION BACKUP/RESTORE				
10.1	Ubicar la ventana "CONFIG BACKUP/RESTORE" Realizar un backup, especificando un nombre xxxxx, validar a traves de las tareas completadas que se ejecuto la instrucción de manera correcta.	✓	euIGD01	
REVISIÓN RÁPIDA --- QUICK FIX				
11.1	Ubicar la ventana "QUICK FIX" Realizar el chequeo "FIX CONNECTIVITY" en donde se genere otra ventana con 4 datos relacionados a conectividad.	✓		
11.2	Realizar el chequeo "FIX WIRELESS" en donde se genere otra ventana con 4 datos al wireless.	✓		
CONFIGURACIÓN DEL DISPOSITIVO --- DEVICE SETTINGS				
12.1	Ubicar "Simplified View" Verificar el valor fijado y por defecto que tiene el parametro "inform interval"	✓	600	
12.2	Verificar que la ruta coincida con la que se fijo en el modem para se evaluado en la plataforma	✓		
12.3	Ubicar "Tab View" Realizar un (send update) modificando el valor "periodic inform interval), validar posteriormente que el dispositivo realizo satisfactoriamente la operación. (MANAGEMENT)	✓	1200	
12.4	Comparar las características con la ventana device information que se encuentra a la izquierda. (INFORMATION)	✓		
12.5	Visualizar la direcciones IP o nombres de los diversos NTPServer (TIME)	✓		
12.6	Visualizar las casillas referentes a PVC, ATMEncaps y ATMQoS (DSL)	✓		
12.7	Visualizar las casillas referentes a Name, Default Gateway y DNSServer (WAN)	✓		
12.8	Corroborar que el DHCP Lease Time corresponda con el establecido en la sección 5.1 (LAN)	✓		
12.9	Visualización SSID, MaxRate, Channel, Standard (WIRELESS)	✓		
RPC CUSTOM				
13.1	Ubicar "RPC Custom" GetParametersNames GetParametersValues GetParametersAttributes GetRPCMethods Reboot SetParametersAttributes SetParametersValues	✓ ✓ ✓ ✗ ✓ ✗ ✓		
DIAGNOSTICOS Y MONITOREO --- DIAGNOSTICOS AND MONITORING				
14.1	En Diagnostics, ubicar la opción diagnostics type	✓		
14.2	IPpingDiagnostics	✓		
14.3	LoopbackDiagnostics	✓		
14.4	DSL Diagnostics En Monitoring, hacer click en add parameters y se mostrara el abanico de parametros a monitorear WANDevice --> WANDevice.1 --> WANDSLInterfaceConfig (HACER CHECK EN EL PARAMETRO QUE SE DESEE)	✓		
DESCARGA Y SUBIDA DE ARCHIVOS --- FILE DOWNLOAD AND UPLOAD				
15.1	Ubicar File Download Se selecciona el tipo de archivo que se desea (Firmware Image o Vendor Configuration File), luego se busca por lista o manualmente luego se ejecuta la instrucción en "Send Update"	✓		
15.2	Ubicar File Upload Se selecciona el tipo de archivo que se desea (Vendor Configuration File o Vendor Log File), luego se busca por lista o manualmente luego se ejecuta la instrucción en "Send Update"	✓		
ACTIVIDADES Y REGISTROS --- ACTIVITY AND LOGS				
16.1	Ubicar Activity Fijar por fecha y definir las actividades de todas las tareas o alguna en particular	✓		
16.2	Ubicar Logs Fijar por fecha y definir los eventos de manera global o alguno en particular	✓		

CANTV -- Centro Nacional de telecomunicación de CANTV Gerencia de Planificación y Arquitectura de TI Laboratorio de Estandarización. Edif. Equipos II /Piso 6 (BROADCOM -- IGD -- 201.208.21.167 -- 2.0.0)		 		
		ESTATUS	EXPLICACIÓN EN DETALLE	VINCULO
		SI / NO		
MAPA DE RED --- NETWORK MAP				
Ubicar en la ventana "Network Map" el conjunto de dispositivos que se encuentran conectados con el dispositivo (modem) en estudio				
1.1	La prueba consiste en desconectar o quitar alguno(s) de los dispositivos y verificar que desaparezca del mapa, puede utilizarse el botón "refresh" de manera de actualizar el mapa	✓	24 Equipos	
ESTATUS DEL DISPOSITIVO --- DEVICE STATUS				
Ubicar en la ventana "Device Status" las características principales del modem				
2.1	Status: ONLINE / OFFLINE	✓		
2.2	Wifi: UP / DOWN	✓	NO SEGURA	
2.3	Falla de conectividad : (Representa el número de fallas que ha tenido en las últimas 24 horas)	✓	0	
2.4	Número de reinicios del dispositivo : (Representa el número de reinicio que ha tenido en la últimas 24 horas)	✓	1	
2.5	Verificar que los valores que aparecen en <u>downstream</u> y <u>Upstream</u> coincidan con los valores de la ventana de los parámetros de línea DSL (DSL Parameters)	✓		
WAN				
Ubicar la ventana "WAN" y hacer ping de prueba a las siguientes URL:				
3.1	Google Validar el ping testing	✗	FALLIDA	
	Friendly Validar el ping testing	✗	FALLIDA	
	DNS Validar el ping testing	✗	FALLIDA	
WIRELESS STATUS				
Ubicar la ventana "Wireless Status"				
4.1	Desactivar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
4.2	Activar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
4.3	Modificar el nombre de la red "Network Name" y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
4.4	Modificar la contraseña "Security Key" y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
PARAMETROS DHCP --- DHCP PARAMETERS				
Ubicar la ventana "DHCP Parameters"				
5.1	Hacer cambios sobre la operación DHCP Lease Time (seconds), 86400seg (1dia), 129600seg (DiyMedio) Validar posteriormente que la creación de la tarea, se realizo.	✓	3600 86400	
PUERTOS --- PORTS				
Ubicar la ventana "PORTS"				
6.1	Verificar el número de camaras IP activas y identificación de los puertos asociadas a las mismas.	✓	"0" Dispositivos	
PARAMETROS DSL --- DSL PARAMETERS				
Ubicar la ventana "DSL Parameters", apareceran los siguientes parametros:				
7.1	Current Rate	✓		
	Max Rate	✓		
	Noise Margin	✓		
	Attenuation	✓		
	Power	✓		
	Traffic	✓		
DIAGNOSTICOS (PING DIAGNOSTICS AND SPEED TEST)				
Ubicar el recuadro "Diagnostics", en la casilla desplegable "Ping Diagnostics" apareceran varias opciones entre las cuales estan:				
8.1	google.com	✗		
	80.80.80.80	✗		
	friendly.com	✗		
	Enter URL/IP 200.44.32.12	✓		
	Escoja una de las opciones y ejecute el boton que se encuentra debajo PLAY y verifique que se llevo a cabo la tarea			
8.2	En el mismo recuadro "Diagnostics" se ubicará la ejecución "SPEED TEST" (esta solo podra ejecutarse en aquellos modems que soporten TR-143). Utilice el botón que se encuentra debajo PLAY y al instante debe evaluarse la velocidad download y upload en Mbps. Validar esos resultados	✗	NO SOPORTA TR-143	

HERRAMIENTAS --- TOOLS				
9.1	Reinicio del dispositivo (Restart Device) Ubicar la acción "Restart Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.2	Borrado del dispositivo y configuración de fabrica (Restore device to factory seeting) Ubicar la acción "Restore device to factory seeting" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación			
9.3	Ping al dispositivo (Ping to device) Ubicar la acción "Ping to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.4	Borrado del dispositivo (Delete device) Ubicar la acción "Delete Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación			
9.5	(Start device trace) Ubicar la acción "Star device Trace" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.6	(Trace to device) Ubicar la acción "Trace to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.7	Acceso remoto al dispositivo (Access device remotely) Ubicar la acción "Access device remotely" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación			
9.8	Reprovision CPE Ubicar la acción "Reprovision CPE" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación			
CONFIGURATION BACKUP/RESTORE				
Ubicar la ventana "PORTS"				
10.1	Realizar un backup, especificando un nombre xxxxx, validar a traves de las tareas completadas que se ejecuto la instrucción de manera correcta.	✓	eucagua01	
REVISIÓN RÁPIDA --- QUICK FIX				
Ubicar la ventana "QUICK FIX"				
11.1	Realizar el chequeo "FIX CONNECTIVITY" en donde se genere otra ventana con 4 datos relacionados a conectividad.	✓		
11.2	Realizar el chequeo "FIX WIRELESS" en donde se genere otra ventana con 4 datos al wireless.	✓		
CONFIGURACIÓN DEL DISPOSITIVO --- DEVICE SETTINGS				
Ubicar "Simplified View"				
12.1	Verificar el valor fijado y por defecto que tiene el parametro "inform interval"	✓	600	
12.2	Verificar que la ruta coincida con la que se fijo en el modem para se evaluado en la plataforma	✓		
Ubicar "Tab View"				
12.3	Realizar un (send update) modificando el valor "periodic inform interval", validar posteriormente que el dispositivo realizo satisfactoriamente la operación. (MANAGEMENT)	✓	610	
12.4	Comparar las características con la ventana device information que se encuentra a la izquierda. (INFORMATION)	✓		
12.5	Visualizar la direcciones IP o nombres de los diversos NTPServer (TIME)	✓		
12.6	Visualizar las casillas referentes a PVC, ATMEncaps y ATMQoS (DSL)	✓		
12.7	Visualizar las casillas referentes a Name, Default Gateway y DNSServer (WAN)	✓		
12.8	Corroborar que el DHCP Lease Time corresponda con el establecido en la sección 5.1 (LAN)	✓		
12.9	Visualización SSID, MaxRate, Channel, Standard (WIRELESS)	✓		
RPC CUSTOM				
Ubicar "RPC Custom"				
13.1	GetParametersNames	✓		
	GetParametersValues	✓		
	GetParametersAttributes	✓		
	GetRPCMethods	✓		
	Reboot	✓		
	SetParametersAttributes	✓		
SetParametersValues	✓			
DIAGNOSTICOS Y MONITOREO --- DIAGNOSTICOS AND MONITORING				
En Diagnostics, ubicar la opción diagnostics type				
14.1	IPPingDiagnostics	✓		
14.2	LoopbackDiagnostics	✓		
14.3	DSLdiagnostics	✓		
En Monitoring, hacer click en add parameters y se mostrara el abanico de parametros a monitorear				
14.4	WANDevice --> WANDevice.1 --> WANDSLInterfaceConfig (HACER CHECK EN EL PARAMETRO QUE SE DESEE)	✓		
DESCARGA Y SUBIDA DE ARCHIVOS --- FILE DOWNLOAD AND UPLOAD				
Ubicar File Download				
15.1	Se selecciona el tipo de archivo que se desea (Firmware Image o Vendor Configuration File), luego se busca por lista o manualmente luego se ejecuta la instrucción en "Send Update"	✓		
Ubicar File Upload				
15.2	Se selecciona el tipo de archivo que se desea (Vendor Configuration File o Vendor Log File), luego se busca por lista o manualmente luego se ejecuta la instrucción en "Send Update"	✓		
ACTIVIDADES Y REGISTROS --- ACTIVITY AND LOGS				
Ubicar Activity				
16.1	Fijar por fecha y definir las actividades de todas las tareas o alguna en particular	✓		
Ubicar Logs				
16.2	Fijar por fecha y definir los eventos de manera global o alguno en particular	✓		

PLANTILLA DE PRUEBA PARA CPES "STARBRIDGE"

CANTV -- Centro Nacional de telecomunicación de CANTV Gerencia de Planificación y Arquitectura de TI Laboratorio de Estandarización. Edif. Equipos II /Piso 6 (STARBRIDGE NETWORK -- IGD-1511 -- 201.249.43.120 -- 1511_Cantv_4_4_0-130116_1908)		 		
		ESTATUS	EXPLICACIÓN EN DETALLE	VINCULO
MAPA DE RED --- NETWORK MAP		SI / NO		
Ubicar en la ventana "Network Map" el conjunto de dispositivos que se encuentran conectados con el dispositivo (modem) en estudio				
1.1	La prueba consiste en desconectar o quitar alguno(s) de los dispositivos y verificar que desaparezca del mapa, puede utilizarse el botón "refresh" de manera de actualizar el mapa	✓	32 Equipos	
ESTATUS DEL DISPOSITIVO --- DEVICE STATUS				
Ubicar en la ventana "Device Status" las características principales del modem				
2.1	Status: ONLINE / OFFLINE	✓		
2.2	Wifi: UP / DOWN	✓		
2.3	Falla de conectividad : (Representa el número de fallas que ha tenido en las últimas 24 horas)	✓	0	
2.4	Número de reinicios del dispositivo : (Representa el número de reinicio que ha tenido en la últimas 24 horas)	✓	0	
2.5	Verificar que los valores que aparecen en <u>downstream</u> y <u>Upstream</u> coincidan con los valores de la ventana de los parámetros de línea DSL (DSL Parameters)	✓		
WAN				
Ubicar la ventana "WAN" y hacer ping de prueba a las siguientes URL:				
3.1	Google Validar el ping testing	✓		
	Friendly Validar el ping testing	✓		
	DNS Validar el ping testing	✓		
WIRELESS STATUS				
Ubicar la ventana "Wireless Status"				
4.1	Desactivar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
4.2	Activar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
4.3	Modificar el nombre de la red "Network Name" y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
4.4	Modificar la contraseña "Security Key" y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
PARAMETROS DHCP --- DHCP PARAMETERS				
Ubicar la ventana "DHCP Parameters"				
5.1	Hacer cambios sobre la operación DHCP Lease Time (seconds), 86400seg (1dia), 129600seg (DiyMedio) Validar posteriormente que la creación de la tarea, se realizo.	✓	3600 3601	
PUERTOS --- PORTS				
Ubicar la ventana "CONFIG BACKUP/RESTORE"				
6.1	Verificar el número de camaras IP activas y identificación de los puertos asociadas a las mismas.	✓	"18" Dispositivos	
PARAMETROS DSL --- DSL PARAMETERS				
Ubicar la ventana "DSL Parameters", apareceran los siguientes parametros:				
7.1	Current Rate	✓		
	Max Rate	✓		
	Noise Margin	✓		
	Attenuation	✓		
	Power	✓		
	Traffic	✓		
DIAGNOSTICOS (PING DIAGNOSTICS AND SPEED TEST)				
Ubicar el recuadro "Diagnostics", en la casilla desplegable "Ping Diagnostics" apareceran varias opciones entre las cuales estan:				
8.1	google.com	✓		
	80.80.80.80	✗		
	friendly.com	✓		
	Enter URL/IP 200.44.32.12	✓		
	Escoja una de las opciones y ejecute el boton que se encuentra debajo PLAY y verifique que se llevo a cabo la tarea			
8.2	En el mismo recuadro "Diagnostics" se ubicará la ejecución "SPEED TEST" (esta solo podra ejecutarse en aquellos modems que soporten TR-143). Utilice el botón que se encuentra debajo PLAY y al instante debe evaluarse la velocidad download y upload en Mbps. Validar esos resultados	✗	NO SOPORTA TR-143	

HERRAMIENTAS --- TOOLS				
9.1	Reinicio del dispositivo (Restart Device) Ubicar la acción "Restart Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.2	Borrado del dispositivo y configuración de fabrica (Restore device to factory setting) Ubicar la acción "Restore device to factory setting" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación			
9.3	Ping al dispositivo (Ping to device) Ubicar la acción "Ping to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.4	Borrado del dispositivo (Delete device) Ubicar la acción "Delete Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación			
9.5	(Start device trace) Ubicar la acción "Star device Trace" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.6	(Trace to device) Ubicar la acción "Trace to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✗		
9.7	Acceso remoto al dispositivo (Access device remotely) Ubicar la acción "Access device remotely" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✗		
9.8	Reprovisión CPE Ubicar la acción "Reprovision CPE" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✗		
CONFIGURATION BACKUP/RESTORE				
Ubicar la ventana "CONFIG BACKUP/RESTORE"				
10.1	Realizar un backup, especificando un nombre xxxxx, validar a través de las tareas completadas que se ejecuto la instrucción de manera correcta.	✓	eu55501	
REVISIÓN RÁPIDA --- QUICK FIX				
Ubicar la ventana "QUICK FIX"				
11.1	Realizar el chequeo "FIX CONNECTIVITY" en donde se genere otra ventana con 4 datos relacionados a conectividad.	✓		
11.2	Realizar el chequeo "FIX WIRELESS" en donde se genere otra ventana con 4 datos al wireless.	✓		
CONFIGURACIÓN DEL DISPOSITIVO --- DEVICE SETTINGS				
Ubicar "Simplified View"				
12.1	Verificar el valor fijado y por defecto que tiene el parametro "inform interval"	✓	600	
12.2	Verificar que la ruta coincide con la que se fijo en el modem para se evaluado en la plataforma	✓		
Ubicar "Tab View"				
12.3	Realizar un (send update) modificando el valor "periodic inform interval", validar posteriormente que el dispositivo realizo satisfactoriamente la operación. (MANAGEMENT)	✓	1200	
12.4	Comparar las características con la ventana device information que se encuentra a la izquierda. (INFORMATION)	✓		
12.5	Visualizar la direcciones IP o nombres de los diversos NTPServer (TIME)	✓		
12.6	Visualizar las casillas referentes a PVC, ATMEncaps y ATMQoS (DSL)	✓		
12.7	Visualizar las casillas referentes a Name, Default Gateway y DNSServer (WAN)	✓		
12.8	Corroborar que el DHCP Lease Time corresponda con el establecido en la sección 5.1 (LAN)	✓		
12.9	Visualización SSID, MaxRate, Channel, Standard (WIRELESS)	✓		
RPC CUSTOM				
Ubicar "RPC Custom"				
13.1	GetParametersNames	✓		
	GetParametersValues	✓		
	GetParametersAttributes	✓		
	GetRPCMethods	✓		
	Reboot	✓		
	SetParametersAttributes SetParametersValues	✓ ✓		
DIAGNOSTICOS Y MONITOREO --- DIAGNOSTICOS AND MONITORING				
En Diagnostics, ubicar la opción diagnostics type				
14.1	IPPingDiagnostics	✓		
14.2	LoopbackDiagnostics	✓		
14.3	DSLdiagnostics	✓		
En Monitoring, hacer click en add parameters y se mostrara el abanico de parametros a monitorear				
14.4	WANDevice --> WANDevice.1 --> WANDSLInterfaceConfig (HACER CHECK EN EL PARAMETRO QUE SE DESEE)	✓		
DESCARGA Y SUBIDA DE ARCHIVOS --- FILE DOWNLOAD AND UPLOAD				
Ubicar File Download				
15.1	Se selecciona el tipo de archivo que se desea (Firmware Image o Vendor Configuration File), luego se busca por lista o manualmente luego se ejecuta la instrucción en "Send Update"	✓		
Ubicar File Upload				
15.2	Se selecciona el tipo de archivo que se desea (Vendor Configuration File o Vendor Log File), luego se busca por lista o manualmente luego se ejecuta la instrucción en "Send Update"	✓		
ACTIVIDADES Y REGISTROS --- ACTIVITY AND LOGS				
Ubicar Activity				
16.1	Fijar por fecha y definir las actividades de todas las tareas o alguna en particular	✓		
Ubicar Logs				
16.2	Fijar por fecha y definir los eventos de manera global o alguno en particular	✓		

PLANTILLAS DE PRUEBAS PARA CPEs "HUAWEI"

CANTV -- Centro Nacional de telecomunicación de CANTV Gerencia de Planificación y Arquitectura de TI Laboratorio de Estandarización. Edif. Equipos II /Piso 6 (HUAWEI -- -- 190.72.245.116 -- v100R001C01B020)		 		
  		ESTATUS	EXPLICACIÓN EN DETALLE	VINCULO
MAPA DE RED --- NETWORK MAP		SI / NO		
Ubicar en la ventana "Network Map" el conjunto de dispositivos que se encuentran conectados con el dispositivo (modem) en estudio				
1.1	La prueba consiste en desconectar o quitar alguno(s) de los dispositivos y verificar que desaparezca del mapa, puede utilizarse el botón "refresh" de manera de actualizar el mapa	✓	1 Equipo	
ESTATUS DEL DISPOSITIVO --- DEVICE STATUS				
Ubicar en la ventana "Device Status" las características principales del modem				
2.1	Status: ONLINE / OFFLINE	✓		
2.2	Wifi: UP / DOWN	✓		
2.3	Falla de conectividad : (Representa el número de fallas que ha tenido en las últimas 24 horas)	✓	1	
2.4	Número de reinicios del dispositivo : (Representa el número de reinicio que ha tenido en las últimas 24 horas)	✓	1	
2.5	Verificar que los valores que aparecen en <u>downstream</u> y <u>Upstream</u> coincidan con los valores de la ventana de los parámetros de línea DSL (DSL Parameters)	✓		
WAN				
Ubicar la ventana "WAN" y hacer ping de prueba a las siguientes URL:				
3.1	Google Validar el ping testing	✗		
	Friendly Validar el ping testing	✓		
	DNS Validar el ping testing	✓		
WIRELESS STATUS				
Ubicar la ventana "Wireless Status"				
4.1	Desactivar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completó y aparezca el estado del módulo como válido.	✓		
4.2	Activar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completó y aparezca el estado del módulo como válido.	✓		
4.3	Modificar el nombre de la red "Network Name" y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
4.4	Modificar la contraseña "Security Key" y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
PARAMETROS DHCP --- DHCP PARAMETERS				
Ubicar la ventana "DHCP Parameters"				
5.1	Hacer cambios sobre la operación DHCP Lease Time (seconds), 86400seg (1dia), 129600seg (DiyMedio) Validar posteriormente que la creación de la tarea, se realizo.	✓	86400 259200	
PUERTOS --- PORTS				
Ubicar la ventana "PORTS"				
6.1	Verificar el número de camaras IP activas y identificación de los puertos asociadas a las mismas.	✓	"0" Dispositivos	
PARAMETROS DSL --- DSL PARAMETERS				
Ubicar la ventana "DSL Parameters", apareceran los siguientes parametros:				
7.1	Current Rate	✓		
	Max Rate	✓		
	Noise Margin	✓		
	Attenuation	✓		
	Power	✓		
	Traffic	✓		
DIAGNOSTICOS (PING DIAGNOSTICS AND SPEED TEST)				
Ubicar el recuadro "Diagnostics", en la casilla desplegable "Ping Diagnostics" apareceran varias opciones entre las cuales estan:				
8.1	google.com	✗		
	80.80.80.80	✗		
	friendly.com	✗		
	Enter URL/IP 200.44.32.12	✓		
	Escoja una de las opciones y ejecute el boton que se encuentra debajo PLAY y verifique que se llevo a cabo la tarea			
8.2	En el mismo recuadro "Diagnostics" se ubicará la ejecución "SPEED TEST" (esta solo podra ejecutarse en aquellos modems que soporten TR-143). Utilice el botón que se encuentra debajo PLAY y al instante debe evaluarse la velocidad download y upload en Mbps. Validar esos resultados	✗	NO SOPORTA TR-143	

HERRAMIENTAS --- TOOLS			
9.1	Reinicio del dispositivo (Restart Device) Ubicar la acción "Restart Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓	
9.2	Borrado del dispositivo y configuración de fabrica (Restore device to factory seeting) Ubicar la acción "Restore device to factory seeting" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación		
9.3	Ping al dispositivo (Ping to device) Ubicar la acción "Ping to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓	
9.4	Borrado del dispositivo (Delete device) Ubicar la acción "Delete Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación		
9.5	(Start device trace) Ubicar la acción "Star device Trace" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓	
9.6	(Trace to device) Ubicar la acción "Trace to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación		
9.7	Acceso remoto al dispositivo (Access device remotely) Ubicar la acción "Access device remotely" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación		
9.8	Reprovisión CPE Ubicar la acción "Reprovision CPE" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✗	
CONFIGURATION BACKUP/RESTORE			
Ubicar la ventana "CONFIG BACKUP/RESTORE"			
10.1	Realizar un backup, especificando un nombre xxxxx, validar a través de las tareas completadas que se ejecuto la instrucción de manera correcta.	✓	eu11huawei01
REVISIÓN RÁPIDA --- QUICK FIX			
Ubicar la ventana "QUICK FIX"			
11.1	Realizar el chequeo "FIX CONNECTIVITY" en donde se genere otra ventana con 4 datos relacionados a conectividad.	✓	
11.2	Realizar el chequeo "FIX WIRELESS" en donde se genere otra ventana con 4 datos al wireless.	✓	
CONFIGURACIÓN DEL DISPOSITIVO --- DEVICE SETTINGS			
Ubicar "Simplified View"			
12.1	Verificar el valor fijado y por defecto que tiene el parametro "inform interval"	✓	600
12.2	Verificar que la ruta coincida con la que se fijo en el modem para se evaluado en la plataforma	✓	
Ubicar "Tab View"			
12.3	Realizar un (send update) modificando el valor "periodic inform interval), validar posteriormente que el dispositivo realizo satisfactoriamente la operación. (MANAGEMENT)	✓	660
12.4	Comparar las características con la ventana device information que se encuentra a la izquierda. (INFORMATION)	✓	
12.5	Visualizar la direcciones IP o nombres de los diversos NTPServer (TIME)	✓	
12.6	Visualizar las casillas referentes a PVC, ATMEncaps y ATMQoS (DSL)	✓	
12.7	Visualizar las casillas referentes a Name, Default Gateway y DNSServer (WAN)	✓	
12.8	Corroborar que el DHCP Lease Time corresponda con el establecido en la sección 5.1 (LAN)	✓	
12.9	Visualización SSID, MaxRate, Channel, Standard (WIRELESS)	✓	
RPC CUSTOM			
Ubicar "RPC Custom"			
13.1	GetParametersNames	✓	
	GetParametersValues	✓	
	GetParametersAttributes	✓	
	GetRPCMethods	✓	
	Reboot	✓	
	SetParametersAttributes	✓	
	SetParametersValues	✓	
DIAGNOSTICOS Y MONITOREO --- DIAGNOSTICS AND MONITORING			
En Diagnostics, ubicar la opción diagnostics type			
14.1	IPPingDiagnostics	✓	
14.2	LoopbackDiagnostics	✓	
14.3	DSLIDiagnostics	✓	
En Monitoring, hacer click en add parameters y se mostrara el abanico de parametros a monitorear			
14.4	WANDevice --> WANDevice.1 --> WANDSLInterfaceConfig (HACER CHECK EN EL PARAMETRO QUE SE DESEE)	✓	
DESCARGA Y SUBIDA DE ARCHIVOS --- FILE DOWNLOAD AND UPLOAD			
Ubicar File Download			
15.1	Se selecciona el tipo de archivo que se desea (Firmware Image o Vendor Configuration File), luego se busca por lista o manualmente luego se ejecuta la instrucción en "Send Update"	✓	
Ubicar File Upload			
15.2	Se selecciona el tipo de archivo que se desea (Vendor Configuration File o Vendor Log File), luego se busca por lista o manualmente luego se ejecuta la instrucción en "Send Update"	✓	
ACTIVIDADES Y REGISTROS --- ACTIVITY AND LOGS			
Ubicar Activity			
16.1	Fijar por fecha y definir las actividades de todas las tareas o alguna en particular	✓	
Ubicar Logs			
16.2	Fijar por fecha y definir los eventos de manera global o alguno en particular	✓	

CANTV -- Centro Nacional de telecomunicación de CANTV Gerencia de Planificación y Arquitectura de TI Laboratorio de Estandarización. Edif. Equipos II /Piso 6 (HUAWEI --Access Router -- 190.79.199.34 -- 2.3.1.900)		 		
  		ESTATUS	EXPLICACIÓN EN DETALLE	VINCULO
MAPA DE RED --- NETWORK MAP		SI / NO		
	Ubicar en la ventana "Network Map" el conjunto de dispositivos que se encuentran conectados con el dispositivo (modem) en estudio			
1.1	La prueba consiste en desconectar o quitar alguno(s) de los dispositivos y verificar que desaparezca del mapa, puede utilizarse el botón "refresh" de manera de actualizar el mapa	✓	40 Equipos	
ESTATUS DEL DISPOSITIVO --- DEVICE STATUS				
	Ubicar en la ventana "Device Status" las características principales del modem			
2.1	Status: ONLINE / OFFLINE	✓		
2.2	Wifi: UP / DOWN	✗		
2.3	Falla de conectividad : (Representa el número de fallas que ha tenido en las últimas 24 horas)	✓		
2.4	Número de reinicios del dispositivo : (Representa el número de reinicio que ha tenido en las últimas 24 horas)	✓		
2.5	Verificar que los valores que aparecen en downstream y Upstream coincidan con los valores de la ventana de los parámetros de línea DSL (DSL Parameters)	✓		
WAN				
	Ubicar la ventana "WAN" y hacer ping de prueba a las siguientes URL:			
3.1	Google Validar el ping testing	✗	FALLIDA	
	Friendly Validar el ping testing	✗	FALLIDA	
	DNS Validar el ping testing	✗	FALLIDA	
WIRELESS STATUS				
	Ubicar la ventana "Wireless Status"			
4.1	Desactivar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	////		
4.2	Activar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	////		
4.3	Modificar el nombre de la red "Network Name" y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	////		
4.4	Modificar la contraseña "Security Key" y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	////		
PARAMETROS DHCP --- DHCP PARAMETERS				
	Ubicar la ventana "DHCP Parameters"			
5.1	Hacer cambios sobre la operación DHCP Lease Time (seconds), 86400seg (1dia), 129600seg (DiyMedio) Validar posteriormente que la creación de la tarea, se realizo.	////		
PUERTOS --- PORTS				
	Ubicar la ventana "PORTS"			
6.1	Verificar el número de camaras IP activas y identificación de los puertos asociadas a las mismas.	✓	"0" Dispositivos	
PARAMETROS DSL --- DSL PARAMETERS				
	Ubicar la ventana "DSL Parameters", apareceran los siguientes parametros:			
7.1	Current Rate	✓		
	Max Rate	✓		
	Noise Margin	✓		
	Attenuation	✓		
	Power	✓		
	Traffic	✓		
DIAGNOSTICOS (PING DIAGNOSTICS AND SPEED TEST)				
	Ubicar el recuadro "Diagnostics", en la casilla desplegable "Ping Diagnostics" apareceran varias opciones entre las cuales estan:			
8.1	google.com	✗	TIMEOUT	
	80.80.80.80	✗		
	friendly.com	✗		
	Enter URL/IP 200.44.32.12	✗	TIMEOUT	
	Escoja una de las opciones y ejecute el boton que se encuentra debajo PLAY y verifique que se llevo a cabo la tarea			
8.2	En el mismo recuadro "Diagnostics" se ubicará la ejecución "SPEED TEST" (esta solo podra ejecutarse en aquellos modems que soporten TR-143). Utilice el botón que se encuentra debajo PLAY y al instante debe evaluarse la velocidad download y upload en Mbps. Validar esos resultados	✗	NO SOPORTA TR_143	

HERRAMIENTAS --- TOOLS			
9.1	Reinicio del dispositivo (Restart Device) Ubicar la acción "Restart Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓	
9.2	Borrado del dispositivo y configuración de fabrica (Restore device to factory setting) Ubicar la acción "Restore device to factory setting" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación		
9.3	Ping al dispositivo (Ping to device) Ubicar la acción "Ping to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓	
9.4	Borrado del dispositivo (Delete device) Ubicar la acción "Delete Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación		
9.5	(Start device trace) Ubicar la acción "Star device Trace" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✗	
9.6	(Trace to device) Ubicar la acción "Trace to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓	
9.7	Acceso remoto al dispositivo (Access device remotely) Ubicar la acción "Access device remotely" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓	
9.8	Reprovisión CPE Ubicar la acción "Reprovisión CPE" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación		
CONFIGURATION BACKUP/RESTORE			
10.1	Ubicar la ventana "CONFIG BACKUP/RESTORE" Realizar un backup, especificando un nombre xxxxx, validar a través de las tareas completadas que se ejecuto la instrucción de manera correcta.	✓	euuniarte01
REVISIÓN RÁPIDA --- QUICK FIX			
	Ubicar la ventana "QUICK FIX"		
11.1	Realizar el chequeo "FIX CONNECTIVITY" en donde se genere otra ventana con 4 datos relacionados a conectividad.	✓	
11.2	Realizar el chequeo "FIX WIRELESS" en donde se genere otra ventana con 4 datos al wireless.	✓	
CONFIGURACIÓN DEL DISPOSITIVO --- DEVICE SETTINGS			
	Ubicar "Simplified View"		
12.1	Verificar el valor fijado y por defecto que tiene el parametro "inform interval"	✓	600
12.2	Verificar que la ruta coincida con la que se fijo en el modem para se evaluado en la plataforma	✓	
	Ubicar "Tab View"		
12.3	Realizar un (send update) modificando el valor "periodic inform interval", validar posteriormente que el dispositivo realizo satisfactoriamente la operación. (MANAGEMENT)	✓	1200
12.4	Comparar las características con la ventana device information que se encuentra a la izquierda. (INFORMATION)	✓	
12.5	Visualizar la direcciones IP o nombres de los diversos NTPServer (TIME)	✓	
12.6	Visualizar las casillas referentes a PVC, ATMEncaps y ATMQoS (DSL)	✓	
12.7	Visualizar las casillas referentes a Name, Default Gateway y DNSServer (WAN)	✓	
12.8	Corroborar que el DHCP Lease Time corresponda con el establecido en la sección 5.1 (LAN)	✓	
12.9	Visualización SSID, MaxRate, Channel, Standard (WIRELESS)	✓	
RPC CUSTOM			
	Ubicar "RPC Custom"		
13.1	GetParametersNames	✓	
	GetParametersValues	✓	
	GetParametersAttributes	✓	
	GetRPCMethods	✓	
	Reboot	✓	
	SetParametersAttributes	✓	
	SetParametersValues	✓	
DIAGNOSTICOS Y MONITOREO --- DIAGNOSTICOS AND MONITORING			
	En Diagnostics, ubicar la opción diagnostics type		
14.1	IPpingDiagnostics	✓	
14.2	LoopbackDiagnostics	✓	
14.3	DSLdiagnostics	✓	
	En Monitoring, hacer click en add parameters y se mostrara el abanico de parametros a monitorear		
14.4	WANDevice --> WANDevice.1 --> WANDSLInterfaceConfig (HACER CHECK EN EL PARAMETRO QUE SE DESEE)	✓	
DESCARGA Y SUBIDA DE ARCHIVOS --- FILE DOWNLOAD AND UPLOAD			
	Ubicar File Download		
15.1	Se selecciona el tipo de archivo que se desea (Firmware Image o Vendor Configuration File), luego se busca por lista o manualmente luego se ejecuta la instrucción en "Send Update"	✓	
	Ubicar File Upload		
15.2	Se selecciona el tipo de archivo que se desea (Vendor Configuration File o Vendor Log File), luego se busca por lista o manualmente luego se ejecuta la instrucción en "Send Update"	✓	
ACTIVIDADES Y REGISTROS --- ACTIVITY AND LOGS			
	Ubicar Activity		
16.1	Fijar por fecha y definir las actividades de todas las tareas o alguna en particular	✓	
	Ubicar Logs		
16.2	Fijar por fecha y definir los eventos de manera global o alguno en particular	✓	

PLANTILLA DE PRUEBAS PARA CPES "ZyXEL"

CANTV -- Centro Nacional de telecomunicación de CANTV Gerencia de Planificación y Arquitectura de TI Laboratorio de Estandarización. Edif. Equipos II /Piso 6 (ZyXEL -- -- 201.249.43.119 -- V2.00(AAQP.0) b2_F0)		 		
		ESTATUS	EXPLICACIÓN EN DETALLE	VINCULO
MAPA DE RED --- NETWORK MAP		SI / NO		
Ubicar en la ventana "Network Map" el conjunto de dispositivos que se encuentran conectados con el dispositivo (modem) en estudio				
1.1	La prueba consiste en desconectar o quitar alguno(s) de los dispositivos y verificar que desaparezca del mapa, puede utilizarse el botón "refresh" de manera de actualizar el mapa	✓	2 Equipos	
ESTATUS DEL DISPOSITIVO --- DEVICE STATUS				
Ubicar en la ventana "Device Status" las características principales del modem				
2.1	Status: ONLINE / OFFLINE	✓		
2.2	Wifi: UP / DOWN	✓		
2.3	Falla de conectividad : (Representa el número de fallas que ha tenido en las últimas 24 horas)	✓	0	
2.4	Número de reinicios del dispositivo : (Representa el número de reinicio que ha tenido en las últimas 24 horas)	✓	0	
2.5	Verificar que los valores que aparecen en <u>downstream</u> y <u>Upstream</u> coincidan con los valores de la ventana de los parámetros de línea DSL (DSL Parameters)	✓		
WAN				
Ubicar la ventana "WAN" y hacer ping de prueba a las siguientes URL:				
3.1	Google Validar el ping testing	✓		
	Friendly Validar el ping testing	✓		
	DNS Validar el ping testing	✓		
WIRELESS STATUS				
Ubicar la ventana "Wireless Status"				
4.1	Desactivar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
4.2	Activar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
4.3	Modificar el nombre de la red "Network Name" y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
4.4	Modificar la contraseña "Security Key" y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✓		
PARAMETROS DHCP --- DHCP PARAMETERS				
Ubicar la ventana "DHCP Parameters"				
5.1	Hacer cambios sobre la operación DHCP Lease Time (seconds), 86400seg (1dia), 129600seg (DayMedio) Validar posteriormente que la creación de la tarea, se realizó.	✓	259200 86400	
PUERTOS --- PORTS				
Ubicar la ventana "PORTS"				
6.1	Verificar el número de camaras IP activas y identificación de los puertos asociadas a las mismas.	✓	"0" Dispositivos	
PARAMETROS DSL --- DSL PARAMETERS				
Ubicar la ventana "DSL Parameters", apareceran los siguientes parametros:				
7.1	Current Rate	✓		
	Max Rate	✓		
	Noise Margin	✓		
	Attenuation	✓		
	Power	✓		
	Traffic	✓		
DIAGNOSTICOS (PING DIAGNOSTICS AND SPEED TEST)				
Ubicar el recuadro "Diagnostics", en la casilla desplegable "Ping Diagnostics" apareceran varias opciones entre las cuales estan:				
8.1	google.com	✓		
	80.80.80.80	✗		
	friendly.com	✓		
	Enter URL/IP 200.44.32.12	✓		
Escoja una de las opciones y ejecute el boton que se encuentra debajo PLAY y verifique que se llevo a cabo la tarea				
8.2	En el mismo recuadro "Diagnostics" se ubicará la ejecución "SPEED TEST" (esta solo podra ejecutarse en aquellos modems que soporten TR-143). Utilice el botón que se encuentra debajo PLAY y al instante debe evaluarse la velocidad download y upload en Mbps. Validar esos resultados	✓	Soporta TR-143 (No realiza el speed test)	

HERRAMIENTAS --- TOOLS				
9.1	Reinicio del dispositivo (Restart Device) Ubicar la acción "Restart Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.2	Borrado del dispositivo y configuración de fabrica (Restore device to factory seeting) Ubicar la acción "Restore device to factory seeting" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación			
9.3	Ping al dispositivo (Ping to device) Ubicar la acción "Ping to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.4	Borrado del dispositivo (Delete device) Ubicar la acción "Delete Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación			
9.5	(Start device trace) Ubicar la acción "Star device Trace" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✓		
9.6	(Trace to device) Ubicar la acción "Trace to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación			
9.7	Acceso remoto al dispositivo (Access device remotely) Ubicar la acción "Access device remotely" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	⚠		
9.8	Reprovisión CPE Ubicar la acción "Reprovision CPE" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	✖		
CONFIGURATION BACKUP/RESTORE				
Ubicar la ventana "CONFIG BACKUP/RESTORE"				
10.1	Realizar un backup, especificando un nombre xxxxx, validar a través de las tareas completadas que se ejecuto la instrucción de manera correcta.	✓	eu8801	
REVISIÓN RÁPIDA --- QUICK FIX				
Ubicar la ventana "QUICK FIX"				
11.1	Realizar el chequeo "FIX CONNECTIVITY" en donde se genere otra ventana con 4 datos relacionados a conectividad.	✓		
11.2	Realizar el chequeo "FIX WIRELESS" en donde se genere otra ventana con 4 datos al wireless.	✓		
CONFIGURACIÓN DEL DISPOSITIVO --- DEVICE SETTINGS				
Ubicar "Simplified View"				
12.1	Verificar el valor fijado y por defecto que tiene el parametro "inform interval"	✓	600	
12.2	Verificar que la ruta coincida con la que se fijo en el modem para se evaluado en la plataforma	✓		
Ubicar "Tab View"				
12.3	Realizar un (send update) modificando el valor "periodic inform interval), validar posteriormente que el dispositivo realizo satisfactoriamente la operación. (MANAGEMENT)	✓	540	
12.4	Comparar las características con la ventana device information que se encuentra a la izquierda. (INFORMATION)	✓		
12.5	Visualizar la direcciones IP o nombres de los diversos NTPServer (TIME)	✓		
12.6	Visualizar las casillas referentes a PVC, ATMEncaps y ATMQoS (DSL)	✓		
12.7	Visualizar las casillas referentes a Name, Default Gateway y DNSServer (WAN)	✓		
12.8	Corroborar que el DHCP Lease Time corresponda con el establecido en la sección 5.1 (LAN)	✓		
12.9	Visualización SSID, MaxRate, Channel, Standard (WIRELESS)	✓		
RPC CUSTOM				
Ubicar "RPC Custom"				
13.1	GetParametersNames	✓		
	GetParametersValues	✓		
	GetParametersAttributes	✖		
	GetRPCMethods	✓		
	Reboot	✓		
	SetParametersAttributes SetParametersValues	✓ ✓		
DIAGNOSTICOS Y MONITOREO --- DIAGNOSTICOS AND MONITORING				
En Diagnostics , ubicar la opción diagnostics type				
14.1	IPPingDiagnostics	✓		
14.2	LoopbackDiagnostics	✓		
14.3	DSLdDiagnostics	✓		
En Monitoring , hacer click en add parameters y se mostrara el abanico de parametros a monitorear				
14.4	WANDevice --> WANDevice.1 --> WANDSLInterfaceConfig (HACER CHECK EN EL PARAMETRO QUE SE DESEE)	✓		
DESCARGA Y SUBIDA DE ARCHIVOS --- FILE DOWNLOAD AND UPLOAD				
Ubicar File Download				
15.1	Se selecciona el tipo de archivo que se desea (Firmware Image o Vendor Configuration File), luego se busca por lista o manualmente luego se ejecuta la instrucción en "Send Update"	✓		
Ubicar File Upload				
15.2	Se selecciona el tipo de archivo que se desea (Vendor Configuration File o Vendor Log File), luego se busca por lista o manualmente luego se ejecuta la instrucción en "Send Update"	✓		
ACTIVIDADES Y REGISTROS --- ACTIVITY AND LOGS				
Ubicar Activity				
16.1	Fijar por fecha y definir las actividades de todas las tareas o alguna en particular	✓		
Ubicar Logs				
16.2	Fijar por fecha y definir los eventos de manera global o alguno en particular	✓		

PLANTILLA DE PRUEBAS PARA CPE "ZTE"

CANTV -- Centro Nacional de telecomunicación de CANTV Gerencia de Planificación y Arquitectura de TI Laboratorio de Estandarización. Edif. Equipos II /Piso 6 (ZTE -- ZXHN H108L -- 201.249.43.122 -- ZHNX H108LV4.0.0a ZRQ_VE)		 		
		ESTATUS	EXPLICACIÓN EN DETALLE	VINCULO
MAPA DE RED --- NETWORK MAP		SI / NO		
Ubicar en la ventana "Network Map" el conjunto de dispositivos que se encuentran conectados con el dispositivo (modem) en estudio				
1.1	La prueba consiste en desconectar o quitar alguno(s) de los dispositivos y verificar que desaparezca del mapa, puede utilizarse el botón "refresh" de manera de actualizar el mapa	✓	2 Equipos	
ESTATUS DEL DISPOSITIVO --- DEVICE STATUS				
Ubicar en la ventana "Device Status" las características principales del modem				
2.1	Status: ONLINE / OFFLINE	✓		
2.2	Wifi: UP / DOWN	✓		
2.3	Falla de conectividad: (Representa el número de fallas que ha tenido en las últimas 24 horas)	✓		
2.4	Número de reinicios del dispositivo: (Representa el número de reinicio que ha tenido en la últimas 24 horas)	✓		
2.5	Verificar que los valores que aparecen en downstream y Upstream coincidan con los valores de la ventana de los parámetros de línea DSL (DSL Parameters)	✗		
WAN				
Ubicar la ventana "WAN" y hacer ping de prueba a las siguientes URL:				
3.1	Google Validar el ping testing	✓		
	Friendly Validar el ping testing	✓		
	DNS Validar el ping testing	✓		
WIRELESS STATUS				
Ubicar la ventana "Wireless Status"				
4.1	Desactivar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✗		
4.2	Activar la opción Enable en la casilla de verificación (donde aparece el check) y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✗		
4.3	Modificar el nombre de la red "Network Name" y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✗		
4.4	Modificar la contraseña "Security Key" y validar posteriormente que la creación de la tarea, se completo y aparezca el estado del módulo como válido.	✗		
PARAMETROS DHCP --- DHCP PARAMETERS				
Ubicar la ventana "DHCP Parameters"				
5.1	Hacer cambios sobre la operación DHCP Lease Time (seconds), 86400seg (1dia), 129600seg (DayMedio) Validar posteriormente que la creación de la tarea, se realice.	✗		
PUERTOS --- PORTS				
Ubicar la ventana "PORTS"				
6.1	Verificar el número de camaras IP activas y identificación de los puertos asociadas a las mismas.	✗		
PARAMETROS DSL --- DSL PARAMETERS				
Ubicar la ventana "DSL Parameters", apareceran los siguientes parametros:				
7.1	Current Rate	✓		
	Max Rate	✓		
	Noise Margin	✓		
	Attenuation	✓		
	Power	✓		
	Traffic	✓		
DIAGNOSTICOS (PING DIAGNOSTICS AND SPEED TEST)				
Ubicar el recuadro "Diagnostics", en la casilla desplegable "Ping Diagnostics" apareceran varias opciones entre las cuales estan:				
8.1	google.com	✗		
	80.80.80.80	✗		
	friendly.com	✗		
	Enter URL/IP 200.44.32.12	✗		
	Escoja una de las opciones y ejecute el boton que se encuentra debajo PLAY y verifique que se llevo a cabo la tarea			
8.2	En el mismo recuadro "Diagnostics" se ubicará la ejecución "SPEED TEST" (esta solo podra ejecutarse en aquellos modems que soporten TR-143). Utilice el botón que se encuentra debajo PLAY y al instante debe evaluarse la velocidad download y upload en Mbps. Validar esos resultados	✗		

HERRAMIENTAS --- TOOLS			
9.1	Reinicio del dispositivo (Restart Device) Ubicar la acción "Restart Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	+	
9.2	Borrado del dispositivo y configuración de fabrica (Restore device to factory setting) Ubicar la acción "Restore device to factory setting" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	+	
9.3	Ping al dispositivo (Ping to device) Ubicar la acción "Ping to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	+	
9.4	Borrado del dispositivo (Delete device) Ubicar la acción "Delete Device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación		
9.5	(Start device trace) Ubicar la acción "Star device Trace" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	+	
9.6	(Trace to device) Ubicar la acción "Trace to device" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	+	
9.7	Acceso remoto al dispositivo (Access device remotely) Ubicar la acción "Access device remotely" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	+	
9.8	Reprovision CPE Ubicar la acción "Reprovision CPE" en la ventana tools del Friendly TR069 Suite Support Center y ejecutarla Validar a través de la pestaña "Activity and Logs" que en el dispositivo se realizó satisfactoriamente la operación	+	
CONFIGURATION BACKUP/RESTORE			
10.1	Ubicar la ventana "CONFIG BACKUP/RESTORE" Realizar un backup, especificando un nombre xxxxx, validar a través de las tareas completadas que se ejecuto la instrucción de manera correcta.	+	
REVISIÓN RÁPIDA --- QUICK FIX			
Ubicar la ventana "QUICK FIX"			
11.1	Realizar el chequeo "FIX CONNECTIVITY" en donde se genere otra ventana con 4 datos relacionados a conectividad.	+	
11.2	Realizar el chequeo "FIX WIRELESS" en donde se genere otra ventana con 4 datos al wireless.	+	
CONFIGURACIÓN DEL DISPOSITIVO --- DEVICE SETTINGS			
Ubicar "Simplified View"			
12.1	Verificar el valor fijado y por defecto que tiene el parametro "inform interval"	✓	600
12.2	Verificar que la ruta coincida con la que se fijo en el modem para se evaluado en la plataforma	✓	
Ubicar "Tab View"			
12.3	Realizar un (send update) modificando el valor "periodic inform interval", validar posteriormente que el dispositivo realizo satisfactoriamente la operación. (MANAGEMENT)	+	
12.4	Comparar las características con la ventana device information que se encuentra a la izquierda. (INFORMATION)	✓	
12.5	Visualizar la direcciones IP o nombres de los diversos NTPServer (TIME)	✓	
12.6	Visualizar las casillas referentes a PVC, ATMEncaps y ATMQoS (DSL)	✓	
12.7	Visualizar las casillas referentes a Name, Default Gateway y DNSServer (WAN)	✓	
12.8	Corroborar que el DHCP Lease Time corresponda con el establecido en la sección 5.1 (LAN)	✓	
12.9	Visualización SSID, MaxRate, Channel, Standard (WIRELESS)	✓	
RPC CUSTOM			
Ubicar "RPC Custom"			
13.1	GetParametersNames	+	
	GetParametersValues	+	
	GetParametersAttributes	+	
	GetRPCMethods	+	
	Reboot	+	
	SetParametersAttributes SetParametersValues	+	
DIAGNOSTICOS Y MONITOREO --- DIAGNOSTICOS AND MONITORING			
En Diagnostics, ubicar la opción diagnostics type			
14.1	IPPingDiagnostics	+	
14.2	LoopbackDiagnostics	+	
14.3	DSLDiagnosics	+	
En Monitoring, hacer click en add parameters y se mostrara el abanico de parametros a monitorear			
14.4	WANDevice --> WANDevice.1 --> WANDSLInterfaceConfig (HACER CHECK EN EL PARAMETRO QUE SE DESEE)	+	
DESCARGA Y SUBIDA DE ARCHIVOS --- FILE DOWNLOAD AND UPLOAD			
Ubicar File Download			
15.1	Se selecciona el tipo de archivo que se desea (Firmware Image o Vendor Configuration File), luego se busca por lista o manualmente luego se ejecuta la instrucción en "Send Update"	+	
Ubicar File Upload			
15.2	Se selecciona el tipo de archivo que se desea (Vendor Configuration File o Vendor Log File), luego se busca por lista o manualmente luego se ejecuta la instrucción en "Send Update"	+	
ACTIVIDADES Y REGISTROS --- ACTIVITY AND LOGS			
Ubicar Activity			
16.1	Fijar por fecha y definir las actividades de todas las tareas o alguna en particular	+	
Ubicar Logs			
16.2	Fijar por fecha y definir los eventos de manera global o alguno en particular	+	

Verificación de los Requerimientos para una Plataforma de Gestión Remota

		Estado de Cumplimiento	Explicación en detalle	Comentarios
		SI / NO		
A	CRITERIOS DE LOS PROVEEDORES			
1	Reconocida trayectoria (nombre de la empresa y persona de contacto) con la administración del rango entre 500000 y 1000000 de diferentes CPEs	✔	✔	1
2	Experiencia probada en la implementación de un sistema ACS basado con xDSL (por lo menos 20 instalaciones)	✔	✔	1
3	Experiencia probada con el sistema ACS desplegado para apoyar tanto a los servicios de telecomunicaciones como servicios de ISP	✔	✔	1
4	Experiencia probada con el sistema ACS desplegado para apoyar un modelo mayor de telecomunicaciones (Operadores de red que proporcionan servicios // Infraestructura de acceso con otros proveedores de servicios // ISP)	✔	✔	1
B	REQUERIMIENTOS GENERALES DEL SISTEMA			
5	Soporte completo del estandar TR-069 y sus especificaciones de protocolos relacionados (Obligatorios y Opcionales)	✔		
6	El sistema es facil de usar, intuitivo y simple para implementar, sin necesitar el código de generación y/o secuencia de comandos	✔	✔	Pruebas
7	Reconocida trayectoria para el apoyo del estandar TR069 incluyendo todos los dispositivos : modem/router, ONTs, Femtocells, dispositivos VoIP IP-Phones, STB (Set ToBox)	✔	✔	1
8	El sistema debera tener la habilidad de adicionar automáticamente nuevos modelos de CPEs , sin necesitar el código de generación y/o secuencia de comandos	✔	✔	Pruebas
9	Habilidad para gestionar dispositivos LAN (via TR-111)	✔		
10	El sistema debe implementarse en un corto período con los servicios profesionales asociados mínimos	✔	✔	
11	API madura y bien definido para NBI INTERFAZ con los sistemas OSS BSS CRM	⚠	Fase Superior	2
12	Modulos de informacion avanzadas que permiten al operador generar SLA adnanced y reportes QoE / KIP	⚠	Fase Superior	2
13	EMBEDDED Aplicación basada en web de soporte al cliente utilizando SMART en la capa de abstraccion para facilitar el apoyo de llamadas tecnicas	⚠	Fase Superior	2
14	ADVANCED construido en aprovisionamiento Portal con capacidades GUI y API hacia interfaces de NBI	⚠	Fase Superior	2
C	ARQUITECTURA Y ESCALABILIDAD			
15	El sistema requiere gestionar _____ CPEs. Por favor colocar la información de referencia y contacto de sus gestiones entre 500000 y 1000000 CPEs	✔	>3000000	
16	Descripción al detalle de la arquitectura del sistema, incluyendo diagramas y componentes de hardware. Tipos de OS/DB y métodos de soporte	✔	✔	
17	El sistema debe basarse en una arquitectura multi-threaded	✔	✔	
18	El sistema debe tener la capacidad de despliegue de diversidad con la habilidad de desplegar módulos del sistema en varios servidores HW con la intención de reducir la carga del sistema	⚠	Fase Superior	2
19	El sistema debe tener un mecanismo para implementar políticas de seguridad. Que describa en detalle com funciona	✔	✔	3
20	Cuál es el número máximo compatibles de CPEs con el registro y la actualización constante de la base de datos con el árbol de datos completa de los CPEs	✔	✔	4
21	El sistema deberia soportar alta disponibilidad y full redundancia. Por favor que se exponga la arquitectura para dicho despliegue	✔		
22	El ACS debe diseñarse con redundancia (n + 1). Debe explicarse en detalle la aplicacion del mecanismo de redundancia	⚠	Fase Superior	2
23	El ACS deberá apoyar los mecanismo de tolerancia a fallos por ORACLE DB: * MODO DE FUNCIONAMIENTO / SUPPORT OD DATA ORACLE GUARD * MODO DE FUNCIONAMIENTO / TRABAJO DE ORACLE RAC	///// ///// ///// /////	///// ///// ///// /////	///// ///// ///// /////
24	La solución debe ser compatible con la base de datos ORACLE y MySQL	✔	MySQL	MySQL

(1) Presentación “Friendly & Overview”; (2) “No se evalúa en esta fase del proyecto”; (3) “Friendly TR-069 Security Aspects”

(4) “Relacionado a capítulo de pruebas”

D	GESTIÓN ADICIONAL / CAPACIDADES ESPECÍFICAS CONEXAS AL SISTEMA			
25	Soporte Automático, con la mínima interacción manual por parte del administrador para dar soporte a un nuevo DATA MODEL en el ACS (como son VoIP, IPTV, WiMAX, etc). No se necesita conocimiento extensivo del TR069	✓	✓	Pruebas
26	Crear aprovisionamiento de grupos en pantalla	✓	✓	Pruebas
27	El sistema deberá soportar múltiple tipos de conexión como xDSL/cable	✓	✓	Pruebas
28	Incluir mecanismo de balanceo de carga para tareas de grupo	⚠	Fase Superior	2
29	Habilitar para configurar los ajustes específicos de un dispositivo, por un CSR, API, ADMINISTRADOR o PORTAL WEB	✓	✓	Pruebas
30	Mostrar en pantalla inmediatamente los cambios realizados	✓	✓	Pruebas
31	Permitir la personalización de la interfaz del usuario en términos de datos de cada CPE a través de un control total sobre las pestañas o campos	✓	✓	Pruebas
32	Mostrar un mapa de los dispositivos de red	✓	✓	Pruebas
33	Fácil visualización de los puertos en uso	✓	✓	Pruebas
34	Proporcionar un EDITOR personalizado y facil de usar para la provision de escenario de CPE	✓	✓	Pruebas
35	Proporcionar una solución completa para la gestión automatizada de firmware	✓	✓	Pruebas
36	Que exista interacción con los depósitos de archivos de firmware. Aconsejar por favor una descripción del sistema de gestión de base de archivos	✓	✓	Pruebas
37	Capacidad para lograr REGRESIÓN de "buenos conocidos" de los últimos ajustes del dispositivo del usuario	✓	✓	Pruebas
38	Que describa como el sistema proporciona la política de gestión para determinar el comportamiento de la CPE en relación al descubrimiento, registro y en el ámbito de la política de actualización	✓	✓	Pruebas
39	El software debe permitir la asociación entre el usuario y el CPE, y gestionar múltiples CPEs de un solo usuario, incluyendo puertas de enlaces remotas y varios dispositivos de LAN	✓	✓	Pruebas
40	Gestión de múltiples CPEs por suscriptor	✓	✓	Pruebas
41	Disposición de un servidor STUN INTEGRADA	✓	✓	Pruebas
42	El sistema debe reconocer si el CPE es una GATEWAY o un dispositivo de LAN	✓	✓	Pruebas
43	El ACS debe proporcionar gestión para CPEs de diversos fabricantes que trabajen con el protocolo TR-069 y cumplir con los requisitos descritos con el protocolo TR-069 ENMIENDA	✓	✓	Pruebas
E	SOPORTE DEL TR-XXX DEL CPE DATA MODEL			
E.E	El sistema de control debe mantener y cumplir :			
44	TR-069 ENMIENDA 1/2/3. Las especificaciones completas	✓	✓	Informe (Cap2)
45	TR-098 (Enmienda Inc.) - Internet Gateway Device Data Model for TR-069. Amplia las capacidades iniciales de gestión de puerta de enlace para abarcar la calidad orientada a las políticas de servicio (QoS)	✓	✓	Informe (Cap2)
46	TR-104 – DSLHome™ / Parametros de aprovisionamiento para CPE VoIP	✓	✓	Informe (Cap2)
47	TR-106 Enmienda 1 / Data Model Template para TR-069 con dispositivos habilitados y plantillas para la administración remota a otros dispositivos del hogar digital	✓	✓	Informe (Cap2)
48	TR-110 Issue 1.01 – DSLHome™ Reference Models for VoIP Configurations in the DSL Home	✓	✓	Informe (Cap2)
49	TR-111 – Applying TR-069 to Remote Management of Home Networking Devices -- Permite facilidad para que el ACS pueda interactuar con los dispositivos basados en el hogar que viven detrás de un router NAT	✓	✓	Informe (Cap2)
50	TR-131 – NBI requirements	✓	✓	Informe (Cap2)
51	TR-135 – Data Model for a TR-069 Enabled STB	✓	✓	Informe (Cap2)
52	TR-140 Issue 1.1 – TR-069 Data Model for Storage Service Enabled Devices	✓	✓	Informe (Cap2)
53	TR-157 – SW Module Management	✓	✓	Informe (Cap2)
54	WT-123 – TR-069: Validation Testing Architecture (Validación de prueba de arquitectura)	✓	✓	Informe (Cap2)
55	TR-142 – Framework for TR-069 enabled PON devices	✓	✓	Informe (Cap2)
56	TR-143 – Network Service Provider Initiated Throughput Performance Test	✓	✓	Informe (Cap2)
57	TR-156 – Using GPON Access in the context of TR-101	✓	✓	Informe (Cap2)
58	TR-181 - Device Data Model	✓	✓	Informe (Cap2)

E.E.E	Otras referencias y/o protocolos: La solución debe ser compatible con las siguientes referencias y protocolos adicionales			
59	RFC 2246 – Transport Layer Security (TLS) Protocol Version 1.0	✓	✓	Informe (Cap1)
60	RFC 2616 – Hypertext Transfer Protocol -- HTTP/1.1	✓	✓	Informe (Cap1)
61	RFC 2617 – HTTP Authentication: Basic and Digest Access Authentication	✓	✓	Informe (Cap1)
62	RFC 2965 – HTTP State Management Mechanism	✓	✓	Informe (Cap1)
63	RFC 3986 – Uniform Resource Identifier (URI): Generic Syntax	✓	✓	Informe (Cap1)
64	Organizationally Unique Identifiers (OUIs)	✓	✓	Informe (Cap1)
65	Secure Sockets Layer (SSL) Protocol Version 3.0	✓	✓	Informe (Cap1)
66	Simple Object Access Protocol (SOAP) 1.1	✓	✓	Informe (Cap1)
67	TR-196: Femto Access Point Service Data Model	✓	✓	Informe (Cap1)
E	API / POLITICA DE EJECUCIÓN / GESTIÓN DE PERFILES / PERFILES DE DATOS			
E.F	La aplicación de gestión de nivel del administrador debe incluir las siguientes capacidades:			
68	La interfaz del usuario debe estar basada en la web	✓	✓	Pruebas
69	Las aplicaciones deberían ser intuitivas y fácil de usar	✓	✓	Pruebas
70	Permite la creación de un perfil de datos para un nuevo modelo de CPE	✓	✓	Pruebas
71	Manejar en pantalla tipo árbol de configuración (añadir, eliminar, editar el sub-árbol)	✓	✓	Pruebas
72	Permitir la actualización masiva a varios grupos de CPEs -- Operaciones a granel	✓	✓	Pruebas
73	Incluye mecanismo seguro y intuitivo para gestionar las versiones de firmware de forma manual y el uso de un depósito de archivo. POR FAVOR, DESCRIBIR LA SOLUCIÓN	✓	✓	Pruebas
74	Permite la supervisión de CPEs. Tanto para un sólo CPE como para un grupo de CPEs de acuerdo a la política definida	✓	✓	Pruebas
75	SUPPORTS EVENTS TRIGGERING -- Proporcionar las herramientas necesarias para un disparador basado en reglas definidas: Un "EVENTO" , basada en CPE , ajustes, grupo de usuarios	✓	✓	Pruebas
76	Administrar las alertas de fallas y activarlos con el sistema externo	⚠	Fase Superior	2
77	Administrar los usuarios del sistemas y permisos	✓	✓	Pruebas
78	Proporcionar reportes de inventarios	✓	✓	Pruebas
79	Reporte del historial de operaciones tanto del ACS como del usuario	✓	✓	Pruebas
80	Incluye una capacidad de presentación de informes -- y que sea flexible para hacer los informes solicitados	✓	✓	Pruebas
81	El sistema debe ser compatible con sistema de registro configurable	✓	✓	Pruebas
82	El sistema debe soportar alarmas exportadores y notificaciones de fallo al sistema de gestión de fallos externos y la notificación del administrador a través de SMS / EMAIL y OTROS	✓	✓	Pruebas
83	El sistema debe proporcionar capacidad de información completa con la posibilidad que permite al administrador cambiar los informes estandar y personalizados. DESCRIBA LA FUNCION DE INFORMACION DEL SISTEMA	✓	✓	Pruebas
84	Presencia API para la integración con el operador existente OSS/BSS	⚠	Fase Superior	2
85	El ACS o los ACSs deben asegurar la disponibilidad de la interfaz gráfica del usuario con funcionalidades adaptables (parte de la pantalla del funcional depende de la cuenta del usuario) que le permite crear una interfaz para los técnicos, así como de interfaz para el personal de apoyo a la gestión , configuración y diagnóstico como un unico dispositivo y el grupo de unidades del abonado	✓	✓	Pruebas

86	La presencia de un portal web para el suscriptor por medio del cual el abonado tenga la capacidad de controlar y cambiar el CPE, WiFi o STB , el establecimiento del servidor DHCP para la LAN, activar , desactivar o actualizar servicios.	✓	✓	Pruebas
87	Los ACSs deben proporcionar la capacidad de activar un nuevo servicio para un solo dispositivo o un grupo de dispositivo del usuario	✓	✓	Pruebas
88	Posibilidad de separación de los derechos de acceso para los usuarios del sistema:	✓	✓	Pruebas
	* INGENIERO	✓	✓	Pruebas
	* OPERADOR	✓	✓	Pruebas
	* ADMINISTRADOR DEL SISTEMA	✓	✓	Pruebas
	* SUPER-USUARIO	✓	✓	Pruebas
89	Actividades de todos los usuarios del sistema de registro	✓	✓	Pruebas
90	Sistema debe configurar automáticamente el dispositivo en función del tipo del dispositivo y perfil de abonado (que lo define el operador)	✓	✓	Pruebas
91	EL ACS deberá contener una base de datos de los dispositivos que son administrados por el sistema y que permita al operador visualizar una interfaz gráfica de todos los dispositivos de los suscriptores que son administrados por el sistema	✓	✓	Pruebas
92	El ACS tiene un mecanismo de integración con la base de datos externa de los abonados para la búsqueda CPE-DEVICE por atributos del suscriptor	✓	✓	Pruebas
93	El ACS debe apoyar mecanismos de búsqueda flexibles que permiten que al operador fácilmente encontrar un CPE en cuestión. La búsqueda debe llevarse a cabo de conformidad con un conjunto específico de parámetros tales como:			
	* DEVICE ID (OUI, TIPO DE PRODUCTO, NÚMERO DE SERIE)	✓	✓	Pruebas
	* La dirección MAC del CPE	✓	✓	Pruebas
	* CNT (Numero de cuenta personal)	✓	✓	Pruebas
94	Los ACS tiene que gestionar y monitorear el estatus de los CPEs de acuerdo con los escenarios especificador por el operador	✓	✓	Pruebas
95	Kit de herramientas para proporcionar información debiera ser implementado como una interfaz gráfica de usuario que brinde información detallada de los dispositivos que están disponibles en la base de datos de ACS:			
	* Número total de dispositivos	✓	✓	Pruebas
	* El número total de tipos del dispositivo	✓	✓	Pruebas
	* Número total de dispositivos que pertenecen a un tipo específico	✓	✓	Pruebas
96	La ACS tiene para gestionar y controlar el estado CPE de acuerdos a los parámetros especificados por el operador	✓	✓	Pruebas
97	El ACS se puede restaurar en cualquier momento en la configuración del estado de la unidad de abonado antes del fracaso de la CPE	✓	✓	Pruebas
98	El ACS debe almacenar configuraciones personalizadas en los últimos avances de CPE	✓	✓	Pruebas
99	El ACS debe permitir al operador controlar un dispositivo en tiempo real a través de un dispositivo de interfaz de control dedicado	✓	✓	Pruebas
100	El ACS debe ser capaz de restaurar de forma automática todos los ajustes y opciones del CPE luego del 'reset'	✓	✓	Pruebas
101	Será posible modificar (insert/insertar, eliminar/delete, modify/modificar) la información sobre el suscriptor en cualquier momento, ya sea a través de la interfaz gráfica de usuario o a través de la interfaz 'north/norte'	✓	✓	Pruebas
102	El ACS debe ser capaz de leer automáticamente todos los parámetros específicos del proveedor de TR-069 soportados por el dispositivo y permitir sus ajustes	✓	✓	Pruebas
103	En caso de ser posible llevar a cabo operaciones estándar en cualquier combinación a través de la interfaz gráfica del usuario:			
	* Para comprobar estado del dispositivo (online / offline)	✓	✓	Prueba
	* Reestablecer el dispositivo	✓	✓	Prueba
	* Reestablecer la configuración de fábrica	✓	✓	Prueba
	* Para actualizar el software (programas informáticos)	✓	✓	Prueba
	* Cargar un archivo de configuración para el dispositivo	✓	✓	Prueba
	* Subir un archivo de configuración desde el dispositivo	✓	✓	Prueba
	* Obtener los atributos de un parámetro para una propiedad específica	✓	✓	Prueba
	* Establecer los atributos de un ajuste particular del parámetro	✓	✓	Prueba
	* Establecer el nombre de un parámetro específico	✓	✓	Prueba
* Llame el método RPC para el dispositivo	✓	✓	Prueba	
	* Elimina el objeto TR-069	✓	✓	Prueba
104	En caso de ser posible automatizar secuencias típicas de acciones a través de escenarios especialmente desarrollados en cualquier combinación a través de la interfaz gráfica	✓	✓	Prueba
105	El ACS se soporta en la lógica condicional para tomar decisiones basadas en los datos obtenidos en tiempo real. Por ejemplo, ejecutar o producir una actualización de software	✓	✓	Prueba
106	Los escenarios para interacción con los diversos CPEs deben soportar la configuración de todo este número de dispositivos. Sistema de apoyo a la creación de escenarios específicos de diagnóstico y sin tratamiento adicional por parte del proveedor de ACS	✓	✓	Prueba

G REQUISITOS PARA LAS OPERACIONES DE DISPOSITIVOS EN GRUPO				
107	El ACS debe proporcionar al operador la disponibilidad de crear sus propios criterios de búsqueda especiales para agrupar los dispositivos del usuario	✓	✓	Pruebas
108	Todas las operaciones se llevan a cabo por una unidad de abonado y este debe ser realizado para un grupo de dispositivos. El sistema debe apoyar la implementación de acciones para un gran número de dispositivos agrupados según diferentes criterios de unidades de abonado disponibles bajo petición	✓	✓	Pruebas
109	El ACS debe tener un mecanismo límite para el número de operaciones simultáneas en grupos de dispositivos	✓	✓	Pruebas
110	El ACS debe permitir crear una serie de reglas para gestionar automáticamente los dispositivos del abonado	✓	✓	Pruebas
111	El ACS debe permitir crear plantillas y perfiles	✓	✓	Pruebas
H REQUISITOS PARA LA SUSTITUCIÓN DE UNIDAD DE ABONADO				
112	En caso de sustitución de la unidad de abonado en el mismo tipo de aparato, todos los servicios que están configurados en el dispositivo antes de la sustitución deben ser configurados en la unidad de abonado recién establecido	⚠	Fase Superior	2
L REQUISITOS PARA LA CONFIGURACIÓN AUTOMÁTICA DE LOS MECANISMOS DE CPE				
113	El ACS debe ser compatible con una variedad de mecanismos de configuración automática CPE: un preset (aprovisionamiento previo) y totalmente automático (zero-touch)	✓	✓	Pruebas
114	Todo el proceso debe ser totalmente automático con mínima o nula necesidad del cliente para insertar los datos manualmente. La solución debe cumplir los siguientes casos:			
	* Describir el proceso de aprovisionamiento sin interacción de diversos servicios	✓	✓	Pruebas
	* Describir el aprovisionamiento sin interacción para DSL	✓	✓	Pruebas
	* Usuario instala un nuevo CPE	✓	✓	Pruebas
	* Usuario instala un nuevo CPE, reemplazando uno ya existente	✓	✓	Pruebas
	* Usuario instala un modelo "desconocido" de CPE nuevo en el sistema	✓	✓	Pruebas
	* Durante el aprovisionamiento, > obtener una respuesta de éxito actual / fracaso de las tareas	✓	✓	Pruebas
M DIAGNÓSTICO Y MONITOREO				
115	Apoyo con tipos de diagnóstico tal como se define por el protocolo TR-069	✓	✓	Pruebas
116	El sistema debe detectar que los diagnósticos son apoyados por el CPE, y no tratar de realizar diagnósticos no admitidos	✓	✓	Pruebas
117	El sistema debe ser compatible para un CPE o para un grupo de ellos basado en las estadísticas de estado y rendimiento	✓	✓	Pruebas
118	Crear un evento sobre degradación de la QoS	⚠	Fase Superior	2
119	Comprobar que un CPE está "online"	✓	✓	Pruebas
120	El ACS debe ser capaz de obtener el estado de la unidad del abonado y la información acerca de sus rendimientos. Esta información puede ser un acontecimiento de la historia de un dispositivo que se almacena en la base de datos del sistema y en tiempo real	✓	✓	Pruebas
121	Debería ser posible aplicar pruebas de diagnóstico para el CPE por un sistema de ACS	✓	✓	Pruebas
122	Debería ser posible cambiar los parámetros y características de las pruebas realizadas en el CPE	✓	✓	Pruebas
123	Será posible leer los archivos de registro para cada CPE	✓	✓	Pruebas
124	Adquisición en tiempo real de la unidad de abonado (archivo de registro)	✓	✓	Pruebas
125	La reposición de un dispositivo de manera remota (hacerle 'reset')	✘	Fallida	
126	La reposición de un dispositivo de manera remota (regresando a la configuración de fábrica)	✘	Fallida	
127	Verificar los dispositivos de la red local del abonado (casa)	✓	✓	Pruebas
128	Utilizar el comando "PingIP" >> Iniciada por el equipo CPE, solicitar al operador ACS hacia la red local o de la interfaz del lado de la red para tener acceso a los resultados obtenidos	✓	✓	Pruebas
129	El ACS debe ser capaz de ajustarse remotamente con la interfaz gráfica, interfaz norte para cada unidad de abonado después de la localización de posibles errores:			
	* Volver a configurar el CPE en tiempo real	✓	✓	Pruebas
	* Actualiza el software en el lado CPE / Instalando una versión nueva o una anterior	✓	✓	Pruebas
	* CPE vuelve a la configuración de fábrica	✓	✓	Pruebas
	* Crear una copia de seguridad de la configuración del CPE, y almacenarlo en una base de datos de ACS o URL alternativo	✓	✓	Pruebas

K	FIRMWARE Y SOFTWARE DE GESTIÓN DE ARCHIVOS PARA CPE			
130	Debe ser posible realizar modificaciones en el software automáticamente sobre las políticas basadas en las reglas de un dispositivo o grupos de dispositivos	✓	✓	Pruebas
131	El archivo que contiene unidades de abonado debe ser almacenado en el servidor de configuración automática	✓	✓	Pruebas
132	Debería ser posible cambiar la versión de emergencia (el "rollback" a la última versión estable)	✓	✓	Pruebas
133	El ACS debe ser capaz de actualizar el software durante la primera activación de los CPEs	✓	✓	Pruebas
134	Debe ser posible establecer explícitamente el tiempo (periodo) de las actualizaciones de software	✓	✓	Pruebas
135	El ACS debe ser capaz de gestionar las actualizaciones de software de escenarios en los que los dispositivos de los usuarios respectivos están apagados. El ACS debe cumplir con exactitud este escenario, es decir CPE pone en cola y espera para encenderlo	✓	✓	Pruebas
136	Debería haber un mecanismo para confirmar la actualización de los suscriptores	✓	✓	
137	Si la actualización del software no se ha realizado correctamente, el sistema automáticamente avisará con un reporte al ACS. Después de un cierto tiempo deberá ejecutar el procedimiento nuevamente	✓	✓	Pruebas
138	Debería ser posible saber en cualquier momento determinar el estado de las actualizaciones de software de CPE, el estado del proceso para el cual es capaz de: completarla con éxito, se espera al final del proceso, o un final desafortunado para el CPE.	✓	✓	Pruebas
139	El ACS debe ser capaz de llevar a cabo todo el rastro del proceso de arranque del CPE, que están involucrado en el proceso de actualización	✓	✓	Pruebas
140	El ACS debe apoyar el uso de imágenes de software específico de un servidor para la gestión de dominios	✓	✓	Pruebas
L	SEGURIDAD			
LL	El sistema debe cumplir con los siguientes mecanismos de seguridad :			
141	Evitar la manipulación de las funciones de gestión de un CPE y un ACS, o las transacciones que se realizan entre ellos	⚠	Fase Superior	2
142	Proporcionar confidencialidad de las transacciones que realizan los diversos CPEs y el ACS	⚠	Fase Superior	2
143	Permitir una autenticación adecuada para cada tipo de transacción	⚠	Fase Superior	2
144	Evitar el robo del servicio	⚠	Fase Superior	2
145	El sistema debe tener un mecanismo de tratamiento de ataque para que pueda gestionar los ataques hostiles y/o descargas	⚠	Fase Superior	2
M	REQUISITOS PARA EL AUTO-SERVICIO WEB/PORTAL			
146	La aplicación del portal web debe ser intuitivo y fácil de usar. La interfaz del usuario debe ser con capacidad de auto-personalización (campos, botones, look & feel)	✓	✓	Pruebas
147	El portal debe apoyar la compra en línea de los servicios con aprovisionamiento automático	⚠	Fase Superior	2
148	El portal debe permitir al abonado acceder a su CPE desde cualquier lugar	✓	✓	Pruebas
149	El portal debe ser capaz de proporcionar la vista del mapa LAN / RED LOCAL	✓	✓	Pruebas
150	El portal debe proporcionar una indicación del estado de la CPE (ONLINE/OFFLINE)	✓	✓	Pruebas
151	El portal debe ser capaz de permitir que el abonado reinicie su CPE	✓	✓	Pruebas
152	El portal debe ser capaz de permitir que el abonado haga 'reset' a su CPE	✓	✓	Pruebas
153	El portal debe ser capaz de permitir que el abonado pueda realizar un 'quick fix' (detección automática de problemas)	✓	✓	Pruebas
154	El portal debe ser capaz de establecer los ajustes pertinentes de los CPEs (inalámbricos de seguridad, puertos abiertos, etc)	✓	✓	Pruebas
155	El portal debe ser capaz de permitir que el abonado pueda hacer retroceder a "LAST GOOD KNOW // ULTIMA CONFIGURACION VALIDA CONOCIDA" archivo de configuración de un cliente	✓	✓	Pruebas
156	El sistema basado de ACS debe ser capaz de crear y personalizar el portal web de "Auto-tuning CPE subscriber". A través de de la web, el usuario en el portal puede ver, comprobar y auto-control de encendido/apagado de los servicios de CPE	✓	✓	Pruebas

N	REPRESENTANTE DE ASISTENCIA AL CLIENTE (RSC) / APLICACION INGENIERO-SOPORTE			
N.N	La aplicacion RSC debe incluir al menos las siguientes características:			
157	La aplicación debe ser intuitiva y facil de usar. La interfaz del usuario debe ser con capacidad de auto-personalización (campos,botones,look & feel, etc) y equipo completo	✓	✓	Pruebas
158	Permisos basados en nombre del usuario y contraseña de la RSC	✓	✓	Pruebas
	Encontrar un dispositivo de acuerdo a varios criterios: (capacidad para gestionar y visualizar multiples dispositivos por suscriptor):			
159	* Numero de serie	✓	✓	Pruebas
	* La direccion MAC del CPE	✓	✓	Pruebas
	* Nombre del usuario	✓	✓	Pruebas
	* Numero de telefono	✓	✓	Pruebas
160	Ver estado del CPE (online/offline)	✓	✓	Pruebas
161	Reinicio del CPE / Reboot of CPE	✓	✓	Pruebas
162	Ajuste del CPE / Reset of CPE	✓	✓	Pruebas
163	QUICK FIX (deteccion automatica de errores y fijacion)	✓	✓	Pruebas
	Vista del mapa del usuario de red y los dispositivos conectados:			
164	* Tipo de conexion	✓	✓	Pruebas
	* La velocidad	✓	✓	Pruebas
	* Nombre del dispositivo	✓	✓	Pruebas
	* IP	✓	✓	Pruebas
165	Obtener información de monitoreo	✓	✓	Pruebas
166	Diagnóstico del TR-069 estandar	✓	✓	Pruebas
167	Escenarios de diagnósticos auto-customizados	✓	✓	Pruebas
168	Configurar los ajustes de CPEs	✓	✓	Pruebas
169	Revertir a "LAST GOOD KNOW // ULTIMA CONFIGURACION VALIDA CONOCIDA" , archivo de configuracion de un cliente	✓	✓	Pruebas
170	Subir un archivo / UPLOAD A FILE	✓	✓	Pruebas
171	Descarga de un firmware o archivo / DOWNLOAD FIRMWARE OR FILE	✓	✓	Pruebas
172	Los registros de actividades de los CPEs	✓	✓	Pruebas
173	Los registros de actividades de los CSR	✓	✓	Pruebas
Q	REQUISITOS PARA LOS MÓDULOS DE INFORMES			
Q.Q	El ACS debe garantizar y proporcionar contadores que muestren:			
174	El número de sesiones procesadas por TR-069	✓	✓	Pruebas
	El número de diferentes mensajes recibidos incluyendo:			
175	* Arranque	✓	✓	Pruebas
	* Solicitud de conexion	✓	✓	Pruebas
	* Periodo	✓	✓	Pruebas
	* Traslado	✓	✓	Pruebas
	* Cambio de valor	✓	✓	Pruebas
176	El número de operaciones de éxito (successful) y fracaso (unsuccessful) de gestionar dispositivos por suscriptor	✓	✓	Pruebas
177	El ACS debe tener un panel de control que permita a los administradores de sistemas llevar un registro de su trabajo en tiempo real, (el estado general del sistema, el estado de las solicitudes individuales que se ejecutan de medicion, diversos indicadores estadísticos y que sirvan para comparar los datos actuales con los criterios de los valores límites de los datos almacenados en el sistema.	✓	✓	Pruebas
178	La data debería ser presentada de manera fácil como los datos de interfaz de gráficos	✓	✓	Pruebas
179	Los grupos deberían estar basado en unos criterios específicos impuestos por el suscriptor	✓	✓	Pruebas
180	Que se presente un inventario de los dispositivos por consumo	/////	/////	/////
P	PRUEBAS DE AUTOMATIZACIÓN / IOT TEST AUTOMATION			
181	Detalle a detalle como el sistema puede probar los dispositivos de TR-069 (Compatibilidad automática)	✓	✓	Pruebas
182	Lista de informes disponibles del AUTOMATIC IOT TESTER	✓	✓	Pruebas

Dispositivos	Especificaciones Técnicas	Sistema Operativo	Cant	Precio Unitario USD	Precio Global USD
HARDWARE para 3,000,000 CPEs con TR-069					
Servidor ACS para TR-069	HP / DL360g8 HP DL360g8 : 2 x E5-2609 (2.4GHz) + 32GB RAM + 2 x 300GB HDD SAS, 4 x Gig Ethernet LAN, DVD RW, Red. Power Supply	Linux CentOS (64 bit)	2	4.000,00	8.000,00
Servidor DB	HP / DL360g8 HP DL360g8 : 2 x E5-2609 (2.4GHz) + 32GB RAM + 2 x 300GB HDD SAS, 4 x Gig Ethernet LAN, 2 x HBA, DVD RW, Red. Power Supply	Linux CentOS (64 bit)	2	4.000,00	8.000,00
Management Application Server	HP / DL360g8 HP DL360g8 : 2 x E5-2609 (2.4GHz) + 32GB RAM + 2 x 300GB HDD SAS, 4 x Gig Ethernet LAN, DVD RW, Red. Power Supply	MS Windows 2008 Ent. OS (64 bit)	2	4.000,00	8.000,00
Almacenamiento Externo SAN	HP / P2000 HP P2000 : 2 x Controller with 2xFC on each Controller, 6 x 600GB SAS HDD, expandable to 24 HDD (SFF) 2.5inch, Red. Power Supply	N/A	1	2.750,00	2.750,00
Switch SAN	HP / 8/8 SAN Switch HP /8/8 SAN Switch with 8 active port with SFP+ for 8Gb FC (8 modules)	N/A	2	3.499,00	6.998,00
Balancedador de Carga & FireWall	Citrix / MPX7500SE 1Gbps throughput with 8 port 10/100/1000BaseT with SSL offload function	N/A	2	15.000,00	30.000,00
Switch para el Segmento LAN & WAN	Extreme / X440 24 port 10/100/1000BaseT + 4 port 1000Base-X (Shared) + Stacking	N/A	4	4.000,00	16.000,00
TOTAL (Hardware)					79.748,00

Tabla 9: Tabla con costos referenciales para la implementación definitiva de la plataforma.