



Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

**DISEÑO PARA LA AUTOCONFIGURACIÓN DE DISPOSITIVOS
FINALES EN REDES xDSL BAJO PROTOCOLO TR-069**

Eduardo José Miralles Letrán

Asesorado por el Ing. Julio César Solares Peñate

Guatemala, marzo de 2015

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

**DISEÑO PARA LA AUTOCONFIGURACIÓN DE DISPOSITIVOS
FINALES EN REDES xDSL BAJO PROTOCOLO TR-069**

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA

POR

EDUARDO JOSÉ MIRALLES LETRÁN

ASESORADO POR EL ING. JULIO CÉSAR SOLARES PEÑATE

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, MARZO DE 2015

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA



NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Angel Roberto Sic García
VOCAL II	Ing. Pablo Christian de León Rodríguez
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Narda Lucía Pacay Barrientos
VOCAL V	Br. Walter Rafael Véliz Muñoz
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Romeo Nefalí López Orozco
EXAMINADOR	Ing. Julio César Solares Peñate
EXAMINADORA	Inga. María Magdalena Puente Romero
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

DISEÑO PARA LA AUTOCONFIGURACIÓN DE DISPOSITIVOS FINALES EN REDES xDSL BAJO PROTOCOLO TR-069

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 20 de mayo de 2013.

Eduardo José Miralles Letrán



FACULTAD DE INGENIERIA

Escuelas de Ingeniería Civil, Ingeniería
Mecánica Industrial, Ingeniería Química,
Ingeniería Mecánica Eléctrica, Técnica
y Regional de Post-grado de Ingeniería
Sanitaria.

Ciudad Universitaria, zona 12
Guatemala, Centroamérica

Guatemala, 6 de noviembre de 2014

Ing. Carlos Eduardo Guzmán Salazar
Coordinador del Área de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Ingeniero Guzmán:

Por este medio me permito dar aprobación al Trabajo de Graduación titulado: **"DISEÑO PARA LA AUTOCONFIGURACIÓN DE DISPOSITIVOS FINALES EN REDES xDSL BAJO PROTOCOLO TR-069"**, desarrollado por el estudiante **Eduardo José Miralles Letrán**, ya que considero que cumple con los requisitos establecidos.

Por lo tanto, el autor de este trabajo y yo como asesor, nos hacemos responsables del contenido y conclusiones del mismo.

Sin otro particular, aprovecho la oportunidad para saludarlo.

Atentamente,

ID Y ENSEÑAD A TODOS


Ing. Julio César Solares Peñate
Asesor

JULIO CESAR SOLARES P.
INGENIERO MECANICO ELECTRICISTA
COLEGIADO No. 2330



Ref. EIME 06 2015
Guatemala, 20 de NOVIEMBRE 2014.

Señor Director
Ing. Guillermo Antonio Puente Romero
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: DISEÑO PARA LA AUTOCONFIGURACIÓN DE DISPOSITIVOS FINALES EN REDES xDSL BAJO PROTOCOLO TR-069, del estudiante, Eduardo José Miralles Letrán, que cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,
ID Y ENSEÑAD A TODOS


Ing. **Carlos Eduardo Guzmán Salazar**
Coordinador Área Electrónica



SFO

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA



FACULTAD DE INGENIERIA

REF. EIME 06. 2015.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante; **EDUARDO JOSÉ MIRALLES LETRÁN** titulado: **DISEÑO PARA LA AUTOCONFIGURACIÓN DE DISPOSITIVOS FINALES EN REDES xDSL BAJO PROTOCOLO TR-069,** procede a la autorización del mismo.


Ing. Guillermo Antonio Puente Romero



GUATEMALA, 28 DE ENERO 2015.



El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica al trabajo de graduación titulado: **DISEÑO PARA LA AUTOCONFIGURACIÓN DE DISPOSITIVOS FINALES EN REDES XDSL BAJO PROTOCOLO TR-069**, presentado por el estudiante universitario: **Eduardo José Miralles Letrán** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, se autoriza la impresión del mismo.

IMPRÍMASE

Ing. Murphy Olympo Paíz Recinos
Decano

Guatemala, marzo de 2015



/cc

ACTO QUE DEDICO A:

Mi familia

Por constante apoyo y motivación para seguir adelante.

AGRADECIMIENTOS A:

Mi familia

Por su apoyo Incondicional.

Mis amigos

Por compartir sus conocimientos y amistad.

Mi asesor

Por su apoyo.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES	V
LISTA DE SÍMBOLOS	VII
GLOSARIO	IX
RESUMEN	XV
OBJETIVOS.....	XVII
INTRODUCCIÓN	XIX
1. FUNDAMENTOS DE REDES	1
1.1. Modelo OSI.....	1
1.2. Modelo TCP/IP	4
1.2.1. Capa de aplicación	4
1.2.2. Capa de transporte.....	5
1.2.2.1. TCP.....	5
1.2.2.2. UDP	6
1.2.3. Capa de internet	6
1.2.4. Capa enlace de datos.....	7
1.2.5. Capa física.....	7
1.3. Topologías de red.....	7
1.3.1. Topología de bus	8
1.3.2. Topología de anillo	8
1.3.3. Topología en estrella	9
1.3.4. Topología árbol.....	10
1.3.5. Topología de triángulo	10
1.3.6. Topología en malla	11
1.4. Dispositivos de red	11

1.4.1.	<i>Hub</i>	11
1.4.2.	<i>Switch</i>	12
1.4.3.	<i>Router</i>	12
1.4.4.	Balanceador de red.....	13
1.4.5.	<i>Firewall</i>	13
1.5.	Protocolos de enrutamiento.....	13
1.5.1.	Protocolos IGP	14
1.5.1.1.	Protocolos vector distancia.....	15
1.5.1.1.1.	RIP	15
1.5.1.1.2.	EIGRP	15
1.5.1.2.	Protocolos estado enlace	16
1.5.1.2.1.	IS-IS	16
1.5.1.2.2.	OSPF	16
1.5.2.	Protocolos EGP	17
1.5.2.1.	BGP.....	17
2.	REDES DE ACCESO ADAPTABLES A PROTOCOLO TR-069	19
2.1.	Red de acceso móvil	19
2.1.1.	Redes <i>wifi</i> (IEEE 802.11)	19
2.1.2.	Redes GSM.....	21
2.1.3.	Redes tercera generación	22
2.1.4.	Redes LTE	23
2.2.	Red de acceso fijo.....	25
2.2.1.	Red híbrido fibra y coaxial (HFC)	25
2.2.2.	Redes FTTx.....	27
3.	EVOLUCIÓN DE RED ACCESO XDSL	29
3.1.	Tecnología xDSL.....	29
3.1.1.	Envío y recepción de datos	31

3.1.2.	Tipos de modulación.....	32
3.1.2.1.	2B1Q.....	32
3.1.2.2.	CAP	33
3.1.2.3.	DMT	34
3.2.	Tipos de DSL.....	35
3.2.1.	HDSL.....	35
3.2.2.	SDSL	36
3.2.3.	IDSL.....	36
3.2.4.	VDSL y variantes	36
3.2.5.	ADSL	37
4.	FUNCIONALIDADES DEL PROTOCOLO TR-069.....	41
4.1.	Cliente TR-069.....	41
4.1.1.	Autoconfiguración y aprovisionamiento dinámico ...	41
4.1.2.	Administración de imágenes de software	42
4.1.3.	Monitoreo de estatus y rendimiento.....	42
4.1.4.	Diagnósticos	43
4.2.	Arquitectura	43
4.3.	Sistema en ACS	45
4.3.1.	Funcionamiento de TR-069	46
4.4.	Procedimiento de autoconfiguración.....	47
4.4.1.	Métodos RPC	48
5.	DISEÑO DE RED CON INTEGRACIÓN A PROTOCOLO TR-069	51
5.1.	Situación actual	51
5.2.	Requisitos físicos (características)	52
5.3.	Requisitos lógicos (características)	53
5.4.	Diseños para la integración a una red en producción.....	54

CONCLUSIONES.....61
RECOMENDACIONES.....63
BIBLIOGRAFÍA.....65

ÍNDICE DE ILUSTRACIONES

FIGURAS

1.	Capas modelo OSI.....	1
2.	Topología de bus.....	8
3.	Topología en anillo.....	9
4.	Topología en estrella.....	9
5.	Topología de árbol.....	10
6.	Topología triángulo.....	10
7.	Topología en malla.....	11
8.	Protocolos de enrutamiento.....	14
9.	Arquitectura GSM.....	21
10.	Arquitectura tercera generación.....	23
11.	Arquitectura LTE.....	24
12.	Arquitectura red HFC.....	26
13.	Tipos de redes FTTx.....	27
14.	Descripción visual conexión telefónica.....	29
15.	Modulación 2B1Q.....	33
16.	Comparativa gráfica de velocidades.....	39
17.	Arquitectura punto a punto.....	43
18.	Ejemplo interacción mensajes TR-069.....	46
19.	Alcance del protocolo.....	52
20.	Tipo de tráfico en solución TR-069.....	55
21.	Diseño I.....	56
22.	Diseño II.....	57
23.	Diseño III.....	58

TABLAS

I.	Modelo OSI – ejemplo de dispositivos y protocolos.....	3
II.	Modelo TCP/IP original y actual.....	4
III.	Velocidad por tecnología.....	38
IV.	Pila de protocolo TR-069	44
V.	Requerimientos mínimos	53
VI.	Consumo ancho de banda.....	54
VII.	Comparativa.....	59

LISTA DE SÍMBOLOS

Símbolo	Significado
<i>B</i>	Ancho de banda
Gbps	Gigabit por segundo
Kbps	Kilobit por segundo
Km	Kilómetro
Mbps	Megabit por segundo
M	Metro
Rt	<i>Router</i>
Sw	<i>Switch</i>
<i>V</i>	Tensión o voltaje

GLOSARIO

ACS	Acrónimo de Autoconfiguration Server (servidor de autoconfiguración). Es un servidor que posee la capacidad de brindar configuraciones automáticas a dispositivos compatibles.
Amplitud	Medida de la variación máxima del desplazamiento u otra magnitud física que varía periódica o cuasiperiódicamente en el tiempo.
ANSI	Acrónimo de American National Standards Institute, Instituto Nacional Estadounidense de Estándares. Es una organización sin fines de lucro que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos.
Bit	Unidad básica de información en el sistema binario.
Byte	Una unidad de información utilizada como un múltiplo del bit, equivale a 8 bits.
Cifrado de datos	Proceso por el que una información legible se transforma mediante un algoritmo en información ilegible llamado criptograma.

Clúster	Conjuntos o conglomerados de computadoras contruidos mediante la utilización de equipos comunes y que se comportan como si fuesen una única computadora.
Compresión de datos	Proceso por el cual se reduce el tamaño físico de bloques de información.
Corriente	Flujo de carga por unidad de tiempo que recorre un material, razón entre voltaje y resistencia.
Datagrama	Fragmento de un paquete que es enviado con la suficiente información para que la red pueda encaminarlo hacia el equipo terminal receptor de datos.
Decibelio	Unidad relativa empleada en acústica, electricidad, telecomunicaciones y otras especialidades, para expresar la relación entre dos magnitudes: la magnitud que se estudia y una de referencia.
Dirección IP	Etiqueta numérica que identifica de manera lógica y jerárquica a un interfaz de un dispositivo dentro de una red que utilice el protocolo de internet.
Dirección MAC	Es un identificador de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red.

DNS	Sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a internet o a una red privada.
DOS	Conjunto de programas que permiten ejecutar ciertas funciones a través de comandos en línea de texto.
DSL	Acrónimo inglés, Digital Subscriber Line (línea digital del suscriptor). Es un tipo de tecnología que se utiliza para brindar acceso a internet.
ESSID	Nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red.
<i>Ethernet</i>	Estándar de redes de área local para computadores, con acceso al medio por contienda. Define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI.
Fase	Indica la situación instantánea en el ciclo, de una magnitud que varía cíclicamente.
<i>Firmware</i>	Bloque de instrucciones de máquina para propósitos específicos; es el encargado de controlarla para ejecutar correctamente las instrucciones externas.

Formateo de datos	Proceso por el cual se da un formato específico a los datos.
<i>Full-duplex</i>	Capacidad de mantener una comunicación bidireccional, enviando y recibiendo mensajes de forma simultánea, en un sistema de comunicación.
Hardware	Conjunto de todas las partes tangibles de un sistema informático.
Internet	Conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen, funcionen como una red lógica única de alcance mundial.
Modulación	Conjunto de técnicas que se usan para transportar información sobre una onda portadora; permiten un mejor aprovechamiento del canal de comunicación.
OAM	Acrónimo del inglés Operation And Management (Operación y Mantenimiento). Término que hace referencia al tráfico que se utiliza para administrar soluciones.
Pila de protocolos	Colección ordenada de protocolos organizados en capas que se ponen unas encima de otras y en donde cada protocolo implementa una abstracción

encuadrada en la abstracción que proporciona la capa sobre la que está encuadrada.

Protocolo	Conjunto de estándares que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red.
Red virtual	Tecnología de red que permite una extensión segura de la red local sobre una red pública.
Software	Conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas en un sistema informático.
TCP	Protocolo de comunicación orientado a conexión fiable del nivel de transporte.
UDP	Protocolo mínimo de nivel de transporte orientado a mensajes.
Voltaje	Protocolo mínimo de nivel de transporte orientado a mensajes.
WDS	Acrónimo inglés Wireless Distribution System (sistema de distribución inalámbrico). Permite la interconexión inalámbrica de puntos de acceso en una red IEEE 802.11, ampliada mediante múltiples puntos de acceso.

WLAN

Del acrónimo Wireless Local Area Network, red de área local inalámbrica.

WPA2

Sistema que permite proteger las redes inalámbricas; está basado en el estándar 802.11i.licación que permite instalar programas nativos de Windows en Linux.

RESUMEN

En el presente trabajo de graduación se muestra el diseño para integrar el protocolo TR-069, con la finalidad de autoconfigurar dispositivos finales en redes bajo tecnología DSL en redes de proveedores de servicio.

El trabajo se puede dividir en tres partes, de acuerdo con los temas expuestos en cada una. La primera parte corresponde al desarrollo de los conceptos básicos de redes y reseña histórica de tecnologías que utilizan los proveedores de servicio, para luego mostrar los tipos de redes de acceso, con dos vertientes: fija y móvil. Por medio de ellas se puede utilizar el protocolo TR-069 y por último profundizar en una de las tecnologías de acceso más utilizadas, xDSL, mostrando su evolución comparativa entre las distintas versiones y cómo pueden adoptar el protocolo TR-069.

En la segunda parte se describen las especificaciones, los procesos que ocurren dentro del protocolo TR-069 y cómo este puede establecer una comunicación máquina-máquina sin la intervención de un operario, y llevar a cabo las funciones de autoconfiguración y monitoreo de dispositivos finales CPE.

La tercera parte corresponde a la elaboración de diseños que pueden utilizarse para integrar el protocolo TR-069 dentro de una red de proveedor de servicios, dependiendo de las necesidades de este. Finalmente se presenta el diseño con las mejores características de robustez y alta disponibilidad.

OBJETIVOS

General

Elaborar un diseño para la autoconfiguración de dispositivos finales en redes xDSL bajo protocolo TR-069, para la red de un proveedor de servicios.

Específicos

1. Presentar los conceptos básicos de redes que conforman y hacen posible la comunicación en las redes de proveedores de servicio.
2. Mostrar los tipos de redes de acceso en las cuales se puede aplicar el protocolo de TR-069.
3. Profundizar en el concepto de redes DSL y mostrar la evolución de la tecnología para adoptar el protocolo TR-069.
4. Definir funciones, características y procesos que ocurren dentro del protocolo TR-069.
5. Realizar un diseño robusto y de alta disponibilidad para la integración del protocolo TR-069 en la red.

INTRODUCCIÓN

En la actualidad, la evolución de la tecnología ha provocado que el acceso a internet sea una herramienta útil, y para que los usuarios puedan acceder lo hacen por medio de un dispositivo final que puede ser un teléfono inteligente, o un CPE a través de una red de acceso móvil o fija, respectivamente.

El trabajo de graduación que se presenta a continuación, responde a la necesidad de proveer un diseño robusto capaz de integrar una plataforma que pueda autoconfigurar dispositivos finales en redes xDSL, utilizando el protocolo TR-069.

El diseño corresponde a un plan de cómo se deben interconectar los dispositivos, a través de un servidor llamado ACS que es el que posee todas las reglas y políticas definidas en el protocolo TR-069 y los dispositivos finales llamados CPEs.

Se hace referencia a CPEs como los dispositivos que están en las instalaciones del cliente, enfocados hacia las redes xDSL, ya que son redes fijas de acceso cuya tecnología es la de mayor penetración en Latinoamérica, por su bajo costo, al poder reutilizar el par trenzado de cobre para brindar el servicio.

Para lograr la comunicación estos establecen sesiones de manera automática; estas sesiones son para poder transmitir la información de un punto a otro de forma confidencial y segura, donde se puede obtener datos del CPE para poder llevar a cabo la autoconfiguración de dicho dispositivo sin la

intervención de un operario, así como obtener datos de monitoreo para agilizar el tiempo de respuesta a fallas y generar la sensación de un mejor servicio a un cliente.

1. FUNDAMENTOS DE REDES

1.1. Modelo OSI

Es un modelo de referencia para la delimitación de las funciones en los dispositivos, desarrollado en la década de los años ochenta, por la Organización Internacional de Estándares (ISO). Este modelo está conformado por siete capas en que deben fluir los datos para ir de un dispositivo a otro.

El modelo OSI está integrado por las capas siguientes:

Figura 1. Capas modelo OSI



Fuente: elaboración propia, con programa Microsoft Visio 2010.

Las capas del modelo OSI se describen a continuación:

- **Aplicación:** provee una interfaz entre el software y cualquier aplicación que necesite comunicación fuera del *host* en donde la aplicación resida. También define los procesos para autenticación de usuarios.
- **Presentación:** el propósito principal de esta capa es definir y negociar el formato de los datos, es decir, si las transacciones serán en código ASCII, EBCDIC, binario, BCD, JPEG, entre otros. La encriptación para la seguridad de los datos también es definida por esta capa.
- **Sesión:** es la capa que define cómo iniciar, controlar y finalizar una conversación. Esto incluye el control y administración de múltiples mensajes bidireccionales, de modo que la aplicación pueda ser notificada sobre el estatus de los mensajes.
- **Transporte:** define varias funciones, la más importante de ellas es la recuperación de errores y control de flujo.
- **Red:** la capa de red define tres funciones principales, direccionamiento lógico, enrutamiento y determinación del camino.
 - **Enrutamiento:** define cómo los dispositivos envían paquetes a su destino final.
 - **Direccionamiento lógico:** define cómo cada dispositivo puede tener una dirección que podría ser utilizada en el proceso de enrutamiento.

- Determinación del camino: proceso lógico que ejecuta el dispositivo con base al destino y protocolo de enrutamiento que este ejecutando.
- Enlace de datos: define las reglas que determinan cuándo un dispositivo puede enviar datos sobre un medio en particular; también definen el formato del encabezado y tráiler que permita a los dispositivos conectados el envío y recepción de datos satisfactoriamente.
- Físico: esta capa se refiere típicamente a estándares de otras organizaciones, como IEEE, ITU, ANSI, entre otros. Dichos estándares manejan las características físicas del medio de transmisión, incluyendo conectores, pines, el uso de pines, corriente eléctrica, codificación, modulación de la luz, y reglas sobre cómo activar y desactivar el uso del medio físico.

Tabla I. **Modelo OSI, ejemplo de dispositivos y protocolos**

Capa	Protocolo y especificaciones	Dispositivos
Aplicación, presentación, sesión	Telnet, HTTP, FTP, SMTP, POP3, VoIP, SNMP	<i>Firewall, IDS, hosts</i>
Transporte	TCP, UDP	<i>Hosts, firewalls</i>
Red	IP	<i>Router</i>
Enlace de datos	Ethernet (IEEE 802.3), HDLC, PPP	LAN switch, AP inalámbrico, cable modem, DSL modem.
Física	RJ-45, EIA/TIA-232, V.35, Ethernet	Cables, connectors

Fuente: CCENT/CCNA ICND1 640-802. Consulta diciembre de 2013.

1.2. Modelo TCP/IP

El modelo TCP/IP define y referencia una gran colección de protocolos que permite a los computadores comunicarse.

Para definir un protocolo, TCP/IP utiliza documentos llamados RFC (*Request For Comments*) por sus siglas en inglés.

Para ser comprendido y delimitado de mejor manera, el modelo está dividido en capas; originalmente había sido definido en cuatro capas y luego se actualizó a cinco, como se muestra a continuación:

Tabla II. **Modelo TCP/IP original y actual**

Original	Actual
Aplicación	Aplicación
Transporte	Transporte
Internet	Internet
Acceso a la red	Enlace de datos
	Físico

Fuente: elaboración propia.

Como se mencionó anteriormente, OSI es un modelo de referencia, pero el más utilizado en la actualidad es el TCP/IP.

1.2.1. Capa de aplicación

Los protocolos de la capa de aplicación de TCP/IP proveen servicios al software aplicativo que se ejecuta en el computador; esta capa no define a la aplicación en sí misma, pero define servicios que necesita dicha aplicación. En

otras palabras, provee el primer puente entre la aplicación y la red. Una de las aplicaciones más conocidas actualmente es el navegador web. Lo que ha provocado que muchos desarrolladores de software en sus programas elaboren interfaces para ejecutarse en navegadores y poder comunicarse en la web.

1.2.2. Capa de transporte

En la capa de transporte, a lo largo del tiempo han surgido varios protocolos, pero los más significativos y que se utilizan al día de hoy son: TCP (*Transmission Control Protocol*) y UDP (*User Datagram Protocol*).

En este caso la capa de transporte resulta de suma importancia, ya que esta es la que provee la jerarquía en sí de las capas, y utiliza los recursos de la capa subyacente para proporcionar un servicio confiable a la adyacente superior.

Además, para su funcionamiento esta capa asocia identificadores llamados puertos, que son dígitos 0 al 65536, utilizados para correlacionar con las aplicaciones de la capa superior.

1.2.2.1. TCP

Fue diseñado para proporcionar un flujo confiable de bytes de extremo a extremo en un medio no confiable, debido a que los datos pueden circular en redes, de las cuales se desconoce cómo se encuentran conformadas, es decir, no se conocen las topologías de las redes a las que se interconecta, anchos de banda, retardos que afecten el desempeño, entre otros factores.

Por ello al momento de utilizar TCP se establecen sesiones, y se posee un mecanismo de tres vías para establecerlas. Se envían notificaciones y/o acuses de recibo para mantener la sesión activa y en el momento que ya no es necesaria la sesión se procede a ejecutar el proceso para la finalización de la misma.

1.2.2.2. UDP

Fue diseñado para aplicaciones en las que se debe enviar información del punto A al punto B de modo no confiable, es decir, que es tolerable la pérdida de datos, ya que puede ser que en capas superiores posea mecanismos para la recuperación de la información. Este genera ventaja en tiempo, pues no lo utiliza, estableciendo sesiones como TCP, por lo que resulta adecuado para aplicaciones en tiempo real.

1.2.3. Capa de internet

Capa que se encarga de llevar los datos desde un punto de origen a su punto de destino, pasando por una o varias redes que según su alcance pueden ser denominadas LAN, MAN, WAN. Esto es posible ya que utiliza el protocolo IP. Además de que debe ser capaz de comunicarse con la capa de enlace de datos y capa de transporte.

El protocolo IP, es un protocolo conformado por direcciones que identifican *hosts* u otros dispositivos en la red, paquetes IP que contienen los datos que se están transmitiendo, así como su punto de origen y destino, y otros parámetros. Para ir de un punto a otro los paquetes necesitan de un elemento enrutador, estos elementos a su vez pueden llevar a cabo el enrutamiento de forma estática o dinámica.

1.2.4. Capa enlace de datos

En la capa enlace de datos se pueden destacar tres funciones básicas: proporcionar una frontera bien definida hacia la capa de red, manejar los errores de transmisión y regular el flujo de datos para que receptores lentos no sean saturados por emisores rápidos.

Con base en las tres características anteriores, se puede asegurar que esta capa se comporta como un alambre que va desde el punto A hacia el punto B, ya que los bits que se colocan en A llegan a B. Claro que para lograr esto se necesita de algoritmos que chequeen los datos en búsqueda de errores y contar con sistema de *buffers* para evitar saturar receptores lentos, de modo que se pueda asemejar la función de un cable.

1.2.5. Capa física

Es la capa más baja del modelo más no la menos importante, ya que esta es la que se encarga de transmitir los datos (bits) en el medio; en esta se definen los niveles eléctricos (voltaje, corriente, potencia), estándares de interconexión (especificaciones mecánicas de conectores, forma, y distribución pines), modulación de la señal, amplificación y/o regeneración de señal.

1.3. Topologías de red

Se refieren a la distribución física-lógica en la que pueden estar conectados los distintos dispositivos de una red.

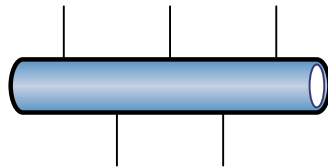
Cabe destacar que estas topologías de red pueden estar distribuidas en distintos rangos de cobertura, áreas pequeñas como un edificio, áreas

medianas como un campus universitario, centro de datos o bien en área grandes que cubran un país.

1.3.1. Topología de bus

En esta topología todos los elementos se conectan a un enlace dorsal común, es una topología simple y básica. Por otro lado, cabe señalar que si el elemento dorsal se daña, toda la red queda incomunicada; además el ancho de banda es compartido por todos los elementos que se encuentren enviando información al mismo tiempo.

Figura 2. Topología de bus



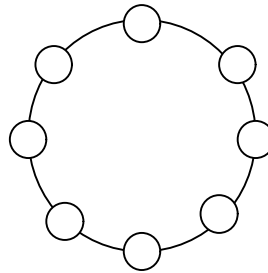
Fuente: elaboración propia, con programa Microsoft Visio 2010.

1.3.2. Topología de anillo

La topología de anillo, como lo dice su nombre, posee la forma de un anillo, ya que sus elementos se conectan de forma consecutiva. Como ventaja se puede mencionar que elementos que se conectan al anillo poseen dos caminos, que luego por factores de las capas del modelo OSI se decide qué camino utilizar.

Otro factor a considerar es que los elementos del anillo deben poseer la misma capacidad física y lógica, ya que habrá datos que circulen de un extremo a otro.

Figura 3. **Topología en anillo**

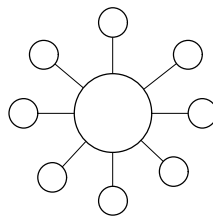


Fuente: elaboración propia, con programa Microsoft Visio 2010.

1.3.3. **Topología en estrella**

En esta topología existe un elemento central en donde se interconectan los elementos. En modo estrella existe la desventaja que solamente hay un punto central, por lo que este punto debe poseer una alta capacidad de procesamiento de datos, ya que es el concentrador de todas la comunicaciones.

Figura 4. **Topología en estrella**

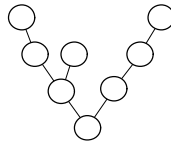


Fuente: elaboración propia, con programa Microsoft Visio 2010.

1.3.4. Topología árbol

Esta topología es muy utilizada ya que posee un punto central o raíz en donde inician las comunicaciones y luego se esparce en ramas, generando niveles en la red; en este caso es susceptible a que algún enlace de la rama falle y quede incomunicado o bien falle el elemento central (raíz).

Figura 5. **Topología de árbol**

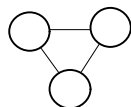


Fuente: elaboración propia, con programa Microsoft Visio 2010.

1.3.5. Topología de triángulo

Esta es una topología robusta, ya que cada elemento se conecta a dos elementos centrales o de alta capacidad, por lo que posee dos caminos para el tráfico de entrada/salida.

Figura 6. **Topología triángulo**

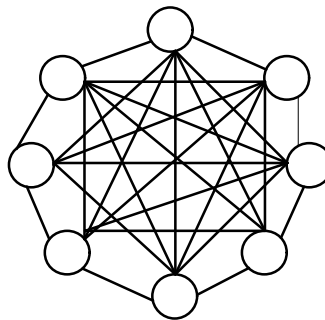


Fuente: elaboración propia, con programa Microsoft Visio 2010.

1.3.6. Topología en malla

Esta topología es la más completa ya que todos los elementos están conectados entre sí, de modo que si falla algún enlace es indiferente para los otros elementos. La desventaja de esta topología es su alto costo de implementación.

Figura 7. Topología en malla



Fuente: elaboración propia, con programa Microsoft Visio 2010.

1.4. Dispositivos de red

Son los elementos que conforman la red de extremo a extremo. Para ello se utilizan distintos dispositivos con fines puntuales. Por lo que a continuación se ampliarán.

1.4.1. Hub

Es considerado el dispositivo de red más básico, ya que únicamente repite las señales recibidas en uno de sus puertos, en todos los demás.

Su funcionamiento está limitado ya que solamente puede transmitir uno a la vez y si en caso dos elementos o más conectados al *hub* transmiten al mismo tiempo, se provoca una colisión de datos y se debe retransmitir la información.

Las capacidades de transmisión y el número de puertos varían de acuerdo con el modelo y fabricante del dispositivo. En la actualidad estos elementos ya no son utilizados, pero se mencionan como referencia, ya que fueron los primeros dispositivos para interconexión de periféricos.

1.4.2. *Switch*

Este dispositivo de red es la evolución de un *hub*; a diferencia del *hub*, los *switches* poseen mecanismos para transmitir simultáneamente de varios o todos los puertos, sin que exista colisión de datos. Se caracterizan porque trabajan en la zona de la capa dos del modelo OSI, por lo que poseen alta capacidad de conmutación de tramas. Por distintas aplicaciones han surgido *switches* que poseen capacidades propias de la capa tres del modelo OSI.

1.4.3. *Router*

Los enrutadores son los dispositivos que trabajan según la capa tres del modelo OSI; estos se encargan de buscar, encontrar y llevar a su destino los paquetes de datos que llegan a él.

Para buscar y encontrar utilizan las direcciones IP asociadas al paquete y para llevar a su destino pueden utilizar rutas estáticas o aprendidas por protocolos de enrutamiento.

1.4.4. Balanceador de red

Es un dispositivo que trabaja en las capas tres a siete del modelo OSI, ya que intenta no sobresaturar algún enlace y envía la información por distintos caminos, de modo que pueda mantener en un estado óptimo los enlaces y equipos conectados a él, sin que sufran saturación.

1.4.5. Firewall

Los *firewall* son elementos de seguridad que intentan detener posibles intrusiones o ataques a los que se pueda ver sometida una red. Estos usualmente están divididos en al menos tres zonas: la zona interior, es la red local, la zona desmilitarizada, es la zona en donde se pueden encontrar servidores a los que elementos externos deban hacer consultas, y la zona externa es la zona que todos los elementos ajenos a la red pueden observar.

1.5. Protocolos de enrutamiento

En el mundo de las redes, gran parte del transporte se ejecuta a nivel de la capa tres del modelo OSI, por lo que es conveniente aclarar los distintos medios que se pueden utilizar para el transporte de la información en este medio.

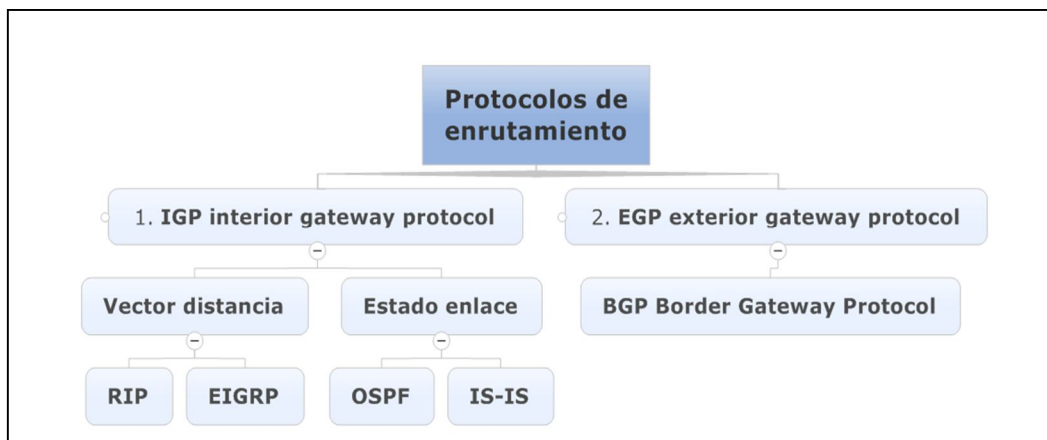
Los protocolos de enrutamiento se encargan de decidir el camino de una dirección IP origen a una IP destino, con base en el protocolo que se encuentre ejecutando el dispositivo enrutador.

Una de las características básicas de los protocolos de enrutamiento son la métrica y distancia administrativa. Distancia administrativa es una

característica que utilizan los enrutadores para decidir qué protocolo utilizar en caso se ejecute más de uno a la vez en dicho dispositivo. Mientras la métrica, es un valor característico de cada protocolo, el cual es calculado dinámicamente según la topología de la red.

Los protocolos de enrutamiento pueden dividirse en dos grandes grupos IGP (*Interior Gateway Protocol*) y EGP (*Exterior Gateway Protocol*) por sus siglas en inglés.

Figura 8. **Protocolos de enrutamiento**



Fuente: elaboración propia, con programa Microsoft Visio 2010.

1.5.1. **Protocolos IGP**

Los protocolos de IGP se utilizan dentro de un sistema o entidad. Puede identificarse como sistema la red de un centro de llamadas, centro de datos, campus universitario, empresas, la red de un proveedor de servicios, etcétera.

Dentro de los protocolos de IGP, estos se subdividen en dos grandes grupos: los protocolos vector distancia y los de estado enlace.

1.5.1.1. Protocolos vector distancia

Los protocolos vector distancia se caracterizan porque utilizan como factor principal los saltos a los que se encuentra el destino.

1.5.1.1.1. RIP

Routing Information Protocol (RIP) fue el primer protocolo de enrutamiento dinámico que se generó, la primer versión ya obsoleta, data de 1988. La versión que aún se utiliza en la actualidad es la dos, que data de 1993.

Este protocolo se caracteriza porque utiliza como factor principal en su métrica el conteo de saltos, es decir, cada vez que un paquete IP pasa por un *router* incrementa en uno. La desventaja es que el máximo valor de métrica que acepta es de quince (15), ya que fue diseñado en un época en la que no se concebía un crecimiento tan acelerado en el área de redes.

Su uso actual es de pequeñas empresas, campus universitarios pequeños y laboratorios de desarrollo.

1.5.1.1.2. EIGRP

Enhanced Interior Gateway Protocol (EIGRP) fue por mucho tiempo propietario de la empresa Cisco Systems, pero en el 2013 se convirtió en un estándar abierto.

Este protocolo utiliza distintos parámetros para el cálculo de métrica como el ancho de banda, retrasos de tiempo en la red, carga y número de saltos. Al tener estos valores, el enrutador puede tomar decisiones más acertadas de qué camino seleccionar para los paquetes IP. Al igual que RIP, EIGRP está concebido para ambientes de pequeñas, medianas y grandes empresas, más no está en la capacidad para ser utilizado por proveedores de servicio.

1.5.1.2. Protocolos estado enlace

Los protocolos estado enlace se caracterizan porque utilizan estatus del enlace (es decir si se encuentra en funcionamiento o no), y la carga del enlace para determinar su métrica.

1.5.1.2.1. IS-IS

Este protocolo fue definido por la Organización Mundial de Estándares ISO. Basa su métrica en el estatus de los enlaces y en el algoritmo de Dijkstra para hacer los cálculos de cómo y dónde enviar el tráfico de forma más rápida. Una característica distintiva de este protocolo es que no utiliza direcciones IPv4 o IPv6, sino direcciones ISO, que resultan más complejas de manejar, por lo que es un protocolo no muy utilizado en la industria. Este protocolo puede ser utilizado por pequeñas o grandes empresas como proveedores de servicios.

1.5.1.2.2. OSPF

Open Shortest Path First (OSPF) es un protocolo abierto que puede ser utilizado por cualquier fabricante de equipamiento. Es el protocolo estado de enlace más utilizado en el mundo.

Para el cálculo de su métrica utiliza el estatus de sus enlaces, así como el algoritmo de Dijkstra. Además, este posee ventajas como crear jerarquías dentro de una red con base en áreas, es decir, se crea un área cero o central y de esta se despliega una serie más de áreas para crear una jerarquía.

1.5.2. Protocolos EGP

Los protocolos EGP se diseñaron para comunicar sistemas autónomos entre sí y el único existente es BGP.

1.5.2.1. BGP

El protocolo *Border Gateway Protocol*, se utiliza para comunicar distintos sistemas autónomos. Una característica de este es que por lo general utiliza direccionamiento público, ya que es con el cual se transfiere la información interna de un sistema hacia el globo de las comunicaciones internet.

A diferencia de los otros protocolos la métrica es más compleja, ya que utiliza más parámetros para colocar una ruta en la tabla de enrutamiento, debido a que se puede utilizar para generar estrategias en la comunicación entre sistemas autónomos, según requerimientos del administrador de red.

2. REDES DE ACCESO ADAPTABLES A PROTOCOLO TR-069

2.1. Red de acceso móvil

Las redes de acceso móvil son ampliamente utilizadas y conforme ha evolucionado la tecnología, una de las tendencias es un acceso rápido y seguro de manera inalámbrica.

2.1.1. Redes *wifi* (IEEE 802.11)

Una de las tecnologías más desplegadas en la actualidad es el acceso a través del protocolo IEEE 802.11. Este modo de acceso ha tenido una alta aceptación ya que posee un rango de cobertura aceptable, una alta transferencia de velocidad de datos y bajo costo.

Wifi (wireless fidelity) es una comunicación inalámbrica que utiliza el protocolo de la IEEE 802.11, este opera en la capa física y el enlace de datos.

- Capa física: define la modulación de las ondas de radio y la técnica de codificación.
 - Espectro ensanchado por frecuencia directa (DSSS)
 - Espectro ensanchado por salto de frecuencia (FHSS)

- Capa enlace de datos: esta capa define la interconexión entre la capa física y el bus del equipo.
 - Control de enlace lógico (LLC)

- Control de acceso al medio (MAC)

A lo largo del tiempo han existido distintas versiones del protocolo que han aportado mejoras. Las principales características según la versión son:

- IEEE 802.11a: esta versión admite un ancho de banda con una velocidad máxima de 54 Mbps teóricos. Provee doce canales en la banda de frecuencia de 5 GHz.
- IEEE 802.11b: con esta versión se obtuvo gran éxito en el mercado. Ofrece una velocidad máxima de 11 Mbps teóricos y tiene un alcance de hasta 300 metros en espacio abierto, esto se logra utilizando la frecuencia de 2,4 GHz.
- IEEE 802.11g: esta es la evolución de la versión 802.11b, opera en el mismo rango de frecuencia pero logra ofrecer 54 Mbps teóricos en el rango de frecuencia de 2,4 GHz, gracias a técnicas de modulación y codificación.
- IEEE 802.11i: esta versión se realizó para proveer seguridad en la red, utilizando un sistema de encriptamiento estándar de cifrado avanzado (AES) y puede cifrar las comunicaciones que utilizan 802.11a, 802.11b y 802.11g.
- IEEE 802.11n: es la versión más actual que puede ofrecer tasa de transmisión de hasta 300 Mbps. Además opera en dos bandas de frecuencia 2,4 GHz y 5 GHz.

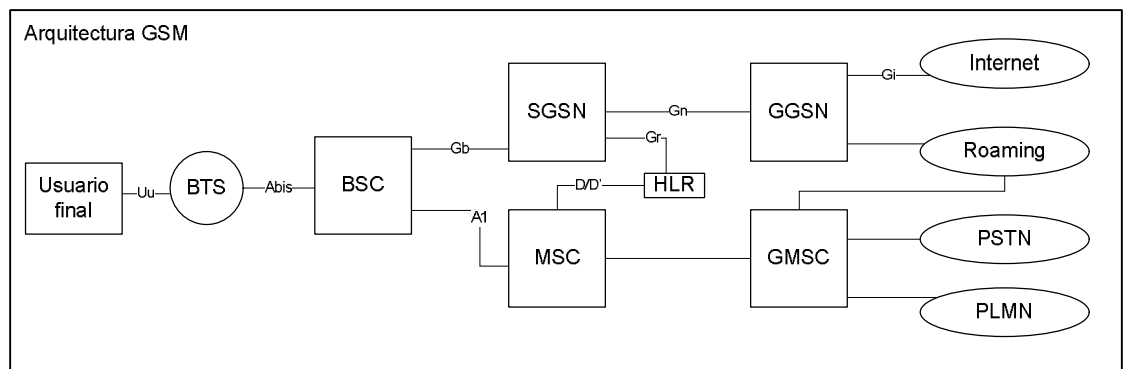
2.1.2. Redes GSM

Las redes GSM (*Global System for Mobile Communications*) constituyen la segunda generación de redes móviles. Fue con ellas que se logró la mayor penetración de servicios a nivel mundial. A través de este estándar y sus evoluciones pudieron agregarse servicios como mensajería de texto y datos.

El estándar se desplegó bajo distintas bandas de frecuencia a 850, 900, 1800 y 1900 MHz, a cada banda le es asignado un ancho de banda para los canales de subida y bajada de tráfico.

Su arquitectura a un alto nivel está compuesta como se muestra en la figura siguiente.

Figura 9. **Arquitectura GSM**



Fuente: elaboración propia, con programa Microsoft Visio 2010.

- Usuario final: consiste en dispositivo móvil capaz de interpretar las señales de radio bajo la modulación del estándar GSM.

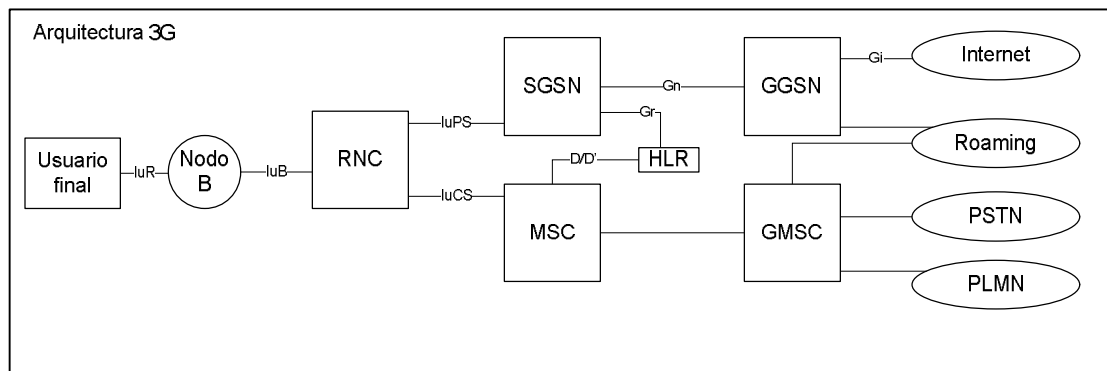
- **BTS (Base Transceiver Station):** este contiene los transmisores y receptores que se acoplan hacia la antena para comunicarse con el usuario final, así como establecer la señalización hacia la BSC.
- **BSC (Base Station Controller):** controla los recursos de radio para las BTS que se encuentren conectadas a este.
- **MSC (Mobile Switching Center):** se encarga de controlar las BSC conectadas o asociadas a este y realiza la conmutación de llamadas.
- **GMSC (Gateway Mobile Switching Center):** se encarga de interconectar hacia redes de voz externas como redes fijas u otras redes móviles internas o externas a la localidad geográfica de la red del operador.
- **SGSN (Serving GPRS Support Node):** se encarga de la autenticación y registro de usuarios en la red para servicios de movilidad como *roaming*, generar datos de facturación.
- **GGSN (Gateway GPRS Support Node):** encargado de conectar hacia las redes de paquetes, donde se destacan dos grandes servicios: proveer internet al usuario final y servicio de *roaming*.

2.1.3. Redes tercera generación

La evolución de la red GSM fue al estándar UMTS. su arquitectura básicamente se conforma al igual que en las redes GSM, su mayor diferencia radica en la mejora para la utilización del espectro radioeléctrico para brindar mayores tasas de transferencia de datos al usuario final.

Dentro de esta generación se desplegó la utilización de teléfonos inteligentes que pueden realizar diversas tareas, para los cuales se requiere una alta disponibilidad en las redes de acceso.

Figura 10. **Arquitectura tercera generación**



Fuente: elaboración propia, con programa Microsoft Visio 2010.

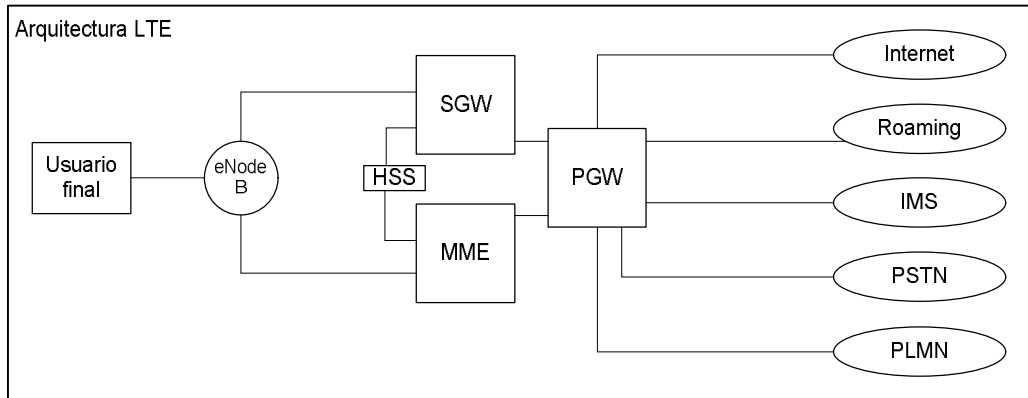
La evolución radica en la red de acceso, ya que los elementos del núcleo de la red MSC, GMSC, SGSN y GGSN continúan siendo los mismos y realizando las mismas funciones.

RNC (*Radio Network Controller*) es el homólogo a la BSC y nodo B, es el homólogo a la BTS, se modula la señal bajo otras técnicas para lograr la eficiencia en el espectro radioeléctrico.

2.1.4. **Redes LTE**

Es la última evolución de redes móviles que se ha liberado comercialmente. En esta sí se observan cambios en el acceso y núcleo de la red.

Figura 11. **Arquitectura LTE**



Fuente: elaboración propia, con programa Microsoft Visio 2010.

- Usuario final: dispositivo capaz de recibir y transmitir información bajo la modulación utilizada por LTE.
- eNodeB (*evolved Node B*): es el punto de acceso de la red, maneja las capas uno y dos. No requiere un nodo de control (2G/BSC o 3G/RNC). Se encarga de la modulación y demodulación, así como de la codificación y decodificación.
- SGW: es el punto de terminación de la interfaz de paquetes de datos hacia la red de acceso.
- PGW: es el punto de terminación de la interfaz de paquetes de datos hacia las distintas redes externas a las que esté interconectado el nodo.
- MME (*Mobility Management Entity*): este nodo se encarga de manejar la señalización y brindar los recursos necesarios entre eNodeB, SGW y PGW.

- HSS: este nodo posee una base de datos de los usuarios de la red y controla la autenticación de los usuarios.

2.2. Red de acceso fijo

Las redes de acceso fijo son aquellas en que la última milla que se conecta hacia el usuario final es por un medio físico cable u óptico.

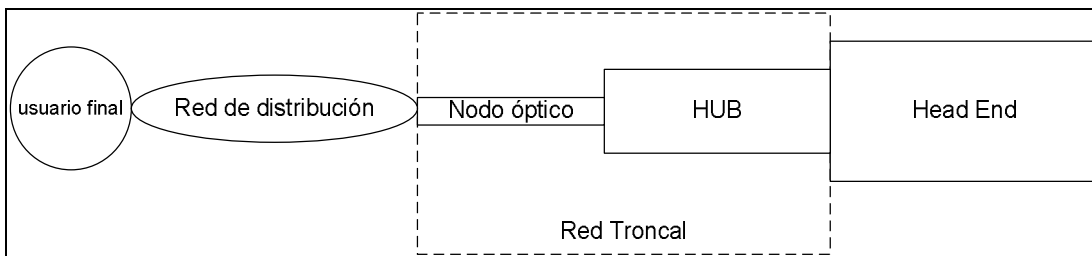
2.2.1. Red híbrido fibra y coaxial (HFC)

En el caso de las redes HFC se combinan tecnologías para transportar información por medios óptico y eléctrico. Su función original fue la de transportar señales de vídeo, el cual fue adoptando cambios para transportar no solamente señales de vídeo, sino también de voz y datos.

La proliferación de este tipo de redes fue a través de los operadores de cable, donde su mayor auge fue en EE.UU. y Canadá; con base en los avances de la tecnología, la posibilidad de habilitar mas portadoras dentro del cable coaxial y la necesidad de poseer servicios convergentes, hizo posible brindar tres servicios por un medio de transporte.

Los componentes básicos para una red HFC son como los que se muestran en la figura a continuación:

Figura 12. **Arquitectura red HFC**



Fuente: elaboración propia, con programa Microsoft Visio 2010.

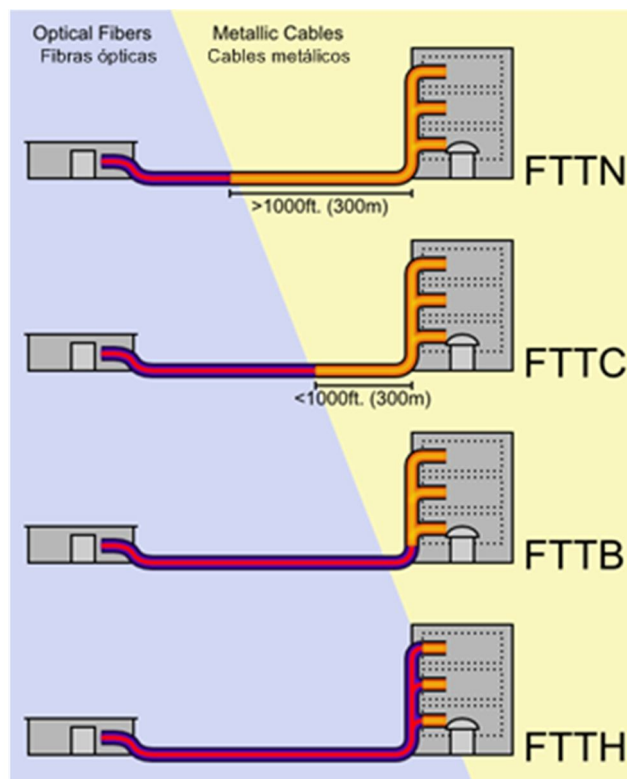
- **Cabecera (*head-end*):** es el centro de recepción, procesamiento, control y transmisión de todos los servicios que ofrece la red. Recopila todas las fuentes de información vía satélite, enlaces terrestres o producción propia, que luego ubica en los canales del espectro de cable. Además, se utiliza como el punto de conexión hacia redes de transporte fijas y/o móviles.
- **Red troncal:** red óptica con topología a dos niveles, con una cobertura geográfica amplia, que se encarga de transportar la señal desde la cabecera hasta los puntos de distribución.
- **Red de distribución:** está compuesta de nodos secundarios en los cuales se realiza la conversión óptico-eléctrica, y se distribuye a los abonados (usuarios) a través de una topología tipo bus. Tiene como objetivo multiplexar la información y adaptar el sistema de transporte a las características específicas del bucle de abonado.

2.2.2. Redes FTTx

Fibra a la x (FTTx) es un término genérico para cualquier banda ancha, utilizando la arquitectura de red de fibra óptica para reemplazar todo o parte del metal (usualmente cobre) habitual, bucle local utilizado para la última milla de las telecomunicaciones.

El acrónimo FTTx es conocido ampliamente como *Fibre-to-the-x*, donde x puede denotar destinos. Los más importantes son los que se muestran en la figura siguiente.

Figura 13. Tipos de redes FTTx



Fuente: <http://sx-de-tx.wikispaces.com/FTTx>. Consulta: agosto de 2014.

- **FFTN:** fibra hasta el nodo, es una arquitectura de telecomunicaciones basadas en cables de fibra óptica, para ejecutar un armario que sirve en un vecindario. El área de servicio para este despliegue se encuentra dentro de un radio de trescientos (300) a mil (1000) metros. Fibra hasta el nodo permite el suministro de servicios de banda ancha, como internet de alta velocidad, interconectar equipos de acceso como DSLAM, MSAN y nodo de HFC.
- **FFTC:** fibra hasta la curva o acera, es un método de servicios de banda ancha de alta velocidad para negocios y hogares, acortando la distancia que viaja la conexión de la línea de cobre. Para lograr esto se deben instalar los equipos de acceso en la calle. El área de servicio para este tipo de despliegue se encuentra bajo un radio máximo de trescientos (300) metros.
- **FTTB:** fibra hasta el edificio, es una solución para aquellas propiedades que contienen varios espacios de trabajo o existen múltiples viviendas. La fibra óptica termina antes de que realmente llegue a los suscriptores en el edificio. La distancia final se transmite utilizando otros medios de acceso no ópticos.
- **FFTH:** fibra hasta el hogar, posee un alcance directo hasta el espacio físico donde se encuentra el destinatario final, y se debe utilizar en el punto final un dispositivo que convierta la señal luminosa a una señal eléctrica o de RF, según el servicio que se pretenda brindar.

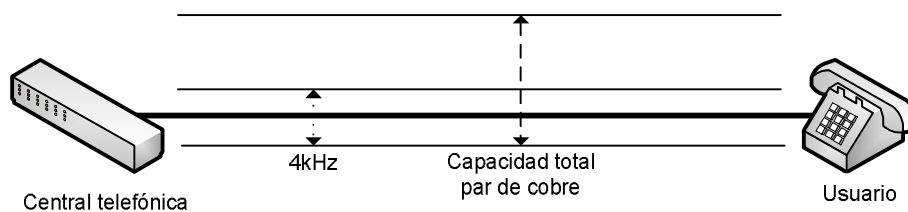
3. EVOLUCIÓN DE RED ACCESO XDSL

3.1. Tecnología xDSL

La tecnología DSL (*Digital Subscriber Line*) surgió con base en la evolución de la conexión que se realizaba entre el par de cobre que interconectaba el hogar o la oficina y la central de telefónica. Esta conexión originalmente fue diseñada para transportar la voz a través de señales análogas.

La transmisión de una señal analógica (voz) a través de los pares de cobre, se utiliza en promedio 4 kHz del ancho de banda de la capacidad teórica total del par de cobre. Por lo que la tecnología DSL supone la eliminación de la transformación de la señal digital a señal analógica, la información es transferida y recibida de forma digital, de manera que pueda ser utilizado todo el ancho de banda que brinda el par de cobre.

Figura 14. Descripción visual conexión telefónica



Fuente: elaboración propia, con programa Microsoft Visio.

Como se mencionó anteriormente, la tecnología DSL utiliza el par de cobre y para ello se emplean técnicas de modulación para alcanzar elevadas velocidades de transmisión.

Esta tecnología puede ofrecer servicios de banda ancha sobre conexiones que no superen un radio de 5 a 6 km del equipo modulador. Otros factores que influyen en la velocidad máxima son la calidad del par de cobre, distancia, calibre del cable, esquema de modulación utilizado y factores físicos como calidad de instalación.

La evidente ventaja que ofrecen estas técnicas es la posibilidad de hacer funcionar varios canales sobre un único par de cables, dos canales para transmisión de datos y uno para la transmisión de voz.

Los servicios de envío y recepción de datos se establecen por medio de un módem especial que reconoce la tecnología DSL. Cabe destacar que antes de llegar al módem los datos pasan por un separador o *splitter* como más se le reconoce, que divide las señales de voz y datos.

La teoría en la que se basa la operación de la tecnología DSL permite la separación de canales sin problemas y sin necesidad de utilizar ningún *splitter*. En la práctica la variabilidad del estatus de los pares de cobre o incluso el propio teléfono al codificar la señal puede ocasionar que a veces el canal de voz y el de datos puedan provocar pequeñas interferencias entre sí, por ello se utiliza el *splitter*, para que elimine todo el espectro de ondas que no son necesarias para la comunicación telefónica y viceversa, para la transmisión de datos.

Entre los principales beneficios y desventajas dentro de la tecnología DSL se pueden mencionar los siguientes:

- El principal beneficio de la tecnología DSL reside en el par trenzado de cobre, ya que este tipo de cableado es el que utiliza la red telefónica. Supone un ahorro considerable de implantación, ya que no es necesario volver a cablear el área donde se desee brindar el servicio.
- El tipo de conexión es permanente y no necesita un proceso de activación o desactivación física. En algunos proveedores de servicios sí puede llegar a incurrir un tiempo de activación o desactivación lógica.
- El principal inconveniente de esta tecnología reside al momento de realizar su implantación. La distancia entre el usuario y la unidad central o remota telefónica no deben de estar separados en más de cinco 5 km.

3.1.1. Envío y recepción de datos

Como se hizo mención anteriormente para el envío y recepción de datos son necesarios dos canales:

- Canal bajada (*downstream*): este canal va en sentido de la central o unidad remota telefónica hasta el usuario, con el que puede alcanzar velocidades desde 128 kbps hasta 100 Mbps, dependiendo del tipo de DSL utilizado. El canal puede ser uno solo o compuesto por múltiples subcanales para alcanzar la velocidad necesaria. Las transmisiones de envío se realizan en la banda de espectro más alta.

- Canal subida (*upstream*): en el caso de este canal, es el utilizado para enviar los datos con velocidades que pueden variar desde los 64 kbps hasta los 50 Mbps, de igual manera estas velocidades dependen de la tecnología de DSL utilizada. Y para esta es necesaria que el envío sea realizado a través de la banda de espectro menor a la de bajada.
- Canal de línea telefónica: este puede ser utilizado para el servicio tradicional de telefónico (POTS) o bien para red digital de servicios integrados (ISDN). Este canal es separado de los dos anteriores por medio del uso de filtro externos (*splitter*), y es alimentado por la central o unidad remota telefónica, para mantenerlo operando aún en el caso de una caída de tensión. Para la transmisión de este canal se realiza desde la banda base de 0 a 4 kHz.

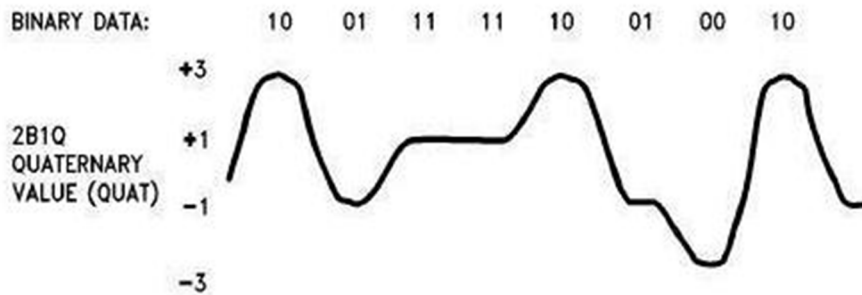
3.1.2. Tipos de modulación

Las señales que son transmitidas por el cable de cobre deben ser moduladas, para que puedan alcanzar altas distancias de transmisión. Para la tecnología xDSL existen distintos tipos de modulación, los cuales se describen a continuación.

3.1.2.1. 2B1Q

La modulación 2B1Q (dos binario uno cuaternario) es un tipo de codificación de línea, en la cual, pares de bits son codificados mediante 4 niveles de señal para la transmisión.

Figura 15. **Modulación 2B1Q**



Fuente: http://hw-server.com/constrc/atm_prog_lpt_shift/programmer.html. Consulta: septiembre de 2014.

3.1.2.2. **CAP**

CAP (Carrier-less Amplitude Modulation). Esta modulación está basada en QAM, donde necesita una señal de entrada que tenga la misma relación entre espectro y fase que la señal transmitida. En las líneas telefónicas no pueden garantizar este comportamiento.

CAP es una implementación de QAM para xDSL, de bajo costo, ya que es más simple y puede otorgar una velocidad de 1,544 Mbps.

CAP divide la señal modulada en segmentos que luego almacena en memoria. La diferencia radica en que la señal portadora se suprime, puesto que no aporta ninguna información, y a su vez para evitar inducir ruido. Aunque esto posee la repercusión del lado del receptor debido a que necesita más dispositivos electrónicos para reconstruirla, claro está que el costo de la electrónica ya no es muy elevado.

QAM establece constelaciones basándose en dos valores de la señal recibida (amplitud y diferencia de fase). CAP es una modulación tipo QAM en la que la constelación es de rotación libre, ya que no lleva portadora que nivele. Lo que hace posible que se pueda utilizar todo el ancho de banda del bucle local, a excepción del ancho de banda dedicado para voz, para enviar todos los bits y hacer caso omiso de subportadoras y subcanales, y de este modo lograr un comportamiento similar a QAM y más eficiente para implementaciones digitales.

3.1.2.3. DMT

DMT (*Discrete Multi-Tone modulation*) es un tipo de modulación de varias portadoras o multiportadoras, que elimina el problema de las altas frecuencias que aumentan considerablemente las pérdidas debido al ruido en las líneas de cobre, dividiendo el ancho de banda disponible en 256 subcanales, que son comprobados para determinar su capacidad portadora.

El proceso de modulación es como se describe a continuación:

- La modulación DMT emplea la transformada discreta de Fourier para crear y demodular cada una de las 256 portadoras individuales, dividiendo el ancho de banda disponible en unidades más pequeñas.
- La línea se comprueba para determinar qué banda de frecuencias es posible y cuántos bits pueden ser transmitidos por unidad de ancho de banda.
- Los bits se codifican en el transmisor mediante la transformada rápida de Fourier inversa y después pasan a un conversor analógico/digital.

- Al recibirse la señal, esta se procesa mediante una transformada rápida de Fourier para decodificar la trama de bits recibida.

CAP y DMT son los tipos de modulación más utilizados en la actualidad. CAP fue la primera solución y está ampliamente distribuida en despliegues actuales, aunque para poder alcanzar las nuevas velocidades se está haciendo más uso de la técnica DMT.

3.2. Tipos de DSL

El ADSL surge como necesidad de ofrecer una mayor velocidad de conexión a internet, sin necesidad de modificar las infraestructuras actuales del par de cobre, empleadas tradicionalmente para las líneas telefónicas. Tecnología que fue desarrollada en 1989 en los laboratorios de Telecordia Technologies Inc. y desde entonces ha sufrido de distintas evoluciones.

A continuación se hará mención de las principales tecnologías xDSL con una breve descripción, para luego enfocar hacia la más extendida ADSL.

3.2.1. HDSL

HDSL (*High bit rate Digital Subscriber Line*): este tipo de tecnología DSL simétrica es capaz de llegar a los 2 Mbps sobre (3) tres pares de cobre en una distancia de 3,6 km, ya que realiza correcciones de la señal transmitida y por tanto no hay degradación.

Existe una pequeña variación de esta tecnología, llamada SHDSL, que permite ser utilizada sobre un solo par de cobre.

Esta es una de las más avanzadas tecnologías DSL que no utilizan repetidores y se suele utilizar en comercios donde se requiere que una gran cantidad de datos circulen a muy alta velocidad. El ratio de transmisión es de 1.168 Kbps por par de cobre, lo que hace que existan variaciones para un par de cobre, dos e incluso tres pares de cobre.

3.2.2. SDSL

SDSL (*Single-line Digital Subscriber Line*), es una versión reducida de HDSL que permite operar bajo una sola línea de cobre trenzado, ofreciendo el acceso tradicional y el intercambio de datos, aunque no a la misma velocidad que puede llegar a ofrecer ADSL bajo los mismos parámetros, ya que es más lento.

3.2.3. IDSL

IDSL (*Integrated services Digital Subscriber Line*) es una red de servicios integrados basada en DSL y puede soportar velocidades de hasta 144 Kbps, ligeramente más rápido que la velocidad que puede alcanzar ISDN de 128 Kbps.

3.2.4. VDSL y variantes

VDSL (*Very high speed Digital Subscriber Line*), como su nombre lo indica, esta tecnología se ha diseñado para lograr máxima velocidad a costa de sacrificar la distancia entre los nodos.

- VDSL: puede poseer velocidades simétricas o asimétricas según los perfiles que se definan. Su mayor ventaja reside en las velocidades que

pueden ser alcanzadas. Para esto emplea un ancho de banda para modular la señal de 12 MHz en donde define más de un canal para la transmisión de datos en sentido *downstream* de central o nodo hacia cliente o abonado, como en sentido *upstream*.

- VDSL2: esta es una evolución del anterior VDSL, su característica principal reside en que se puede alcanzar hasta 100 Mbps como tasa de transferencia en *downstream* (nodo a cliente), para ello emplea hasta 4.096 portadoras. Su desventaja es que por ser una alta velocidad, el medio de transmisión (cobre) provoca que la señal se atenúe conforme aumenta la distancia, logrando únicamente alcanzar 2.500 metros.

3.2.5. ADSL

Dentro de esta variante se puede encontrar ADSL, ADSL2 y ADSL2+.

- ADSL (*Assymetric DSL*) es la variante con mayor índice de penetración de mercado a nivel mundial. Esta tiene características como el poseer diferentes velocidades en cada sentido, ser capaz de sincronizar ambos extremos con diferentes velocidades. Así como, permitir la implementación de servicios como voz sobre IP, TV IP, o bien de llevar el servicio de voz en un canal diferente como POTS o ISDN, emplea hasta 1.1 MHz
- ADSL2: a diferencia de su predecesor, puede soportar un modo digital en donde no se transmite la voz vía POTS o ISDN, lo cual libera ancho de banda y permite ser utilizado como *upstream*. Implementó una mejora al disminuir la atenuación en largas distancias. Se puede obtener velocidades de *downstream* mínimo de 8 y máximo de 12, y velocidades

de *upstream* de 0,8 Mbps a 1 Mbps. La negociación inicial entre el CPE y DSLAM es más rápida, puede soportar *bonding*, es decir, utilizar varios pares para transmitir una misma señal.

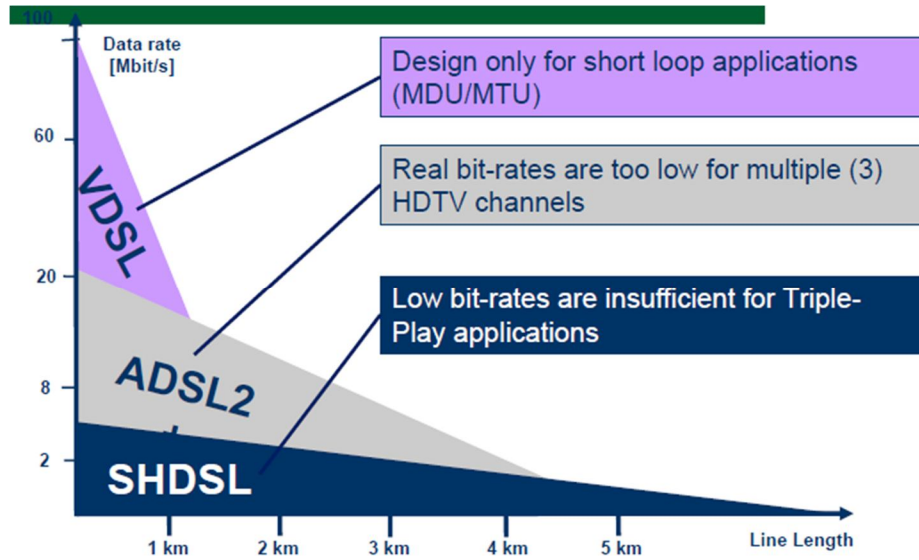
- ADSL2+: esta variante posee las características de ADSL2 con unas mejoras como ampliar el BW hasta 2,2 MHz y se pueden alcanzar velocidades de *downstream* estables de entre 16 y 20 Mbps. Estas velocidades pueden ser alcanzadas solo en distancias menores a 2,4 Km.

Tabla III. **Velocidad por tecnología**

Tecnología	Máx. velocidad bajada	Máx. velocidad subida	Distancia
HDSL	T1	E1	3,66 km
SHDSL	5.6 Mbps	5.6 Mbps	3,66 km
ADSL	6.1 Mbps	0,640 Mbps	5,5 km
ADSL2	12 Mbps	1 Mbps	2,5 km
ADSL2+	24,5 Mbps	1 Mbps	2,4 km
VDSL	55 Mbps	30 Mbps	1,4 km
VDSL2	100 Mbps	100 Mbps	2,5 km

Fuente: <https://www.tlm.unavarra.es>. Consulta: septiembre de 2014.

Figura 16. Comparativa gráfica de velocidades



Fuente: <http://www.broadbandforum.com>. Consulta: septiembre de 2014.

4. FUNCIONALIDADES DEL PROTOCOLO TR-069

El protocolo *Technical Reference – 69* (TR-069) es un documento definido por el *Broadband Forum*, la cual es una organización que lidera el desarrollo de estándares neutrales a los que puedan acoplarse distintos fabricantes y sostener una alta competitividad de soluciones en el mercado. El compendio TR-069, describe a *CPE WAN Management Protocol* (CWMP), este fue elaborado con la intención de definir el mecanismo para comunicar un servidor de autoconfiguración, ACS y un CPE.

4.1. Cliente TR-069

Con el protocolo TR-069 se pretende soportar una variedad de funcionalidades para administrar una colección de CPEs y como principales funcionalidades se pueden identificar las siguientes:

- Autoconfiguración y aprovisionamiento dinámico
- Administración de imágenes de software
- Monitoreo de estatus y rendimiento
- Diagnósticos

4.1.1. Autoconfiguración y aprovisionamiento dinámico

El CWMP permite el aprovisionamiento a través de un ACS a un CPE o un conjunto de CPEs con base en distintos criterios definidos dentro del ACS.

El mecanismo de aprovisionamiento permite al CPE el ser aprovisionado desde el momento en que se conecta a la red de acceso, así como realizar reaprovisionamiento o reconfiguración subsecuentes en el tiempo.

Para lograr esto, se debe identificar cuál CPE o grupo de CPEs son los que se desean manipular a través de distintos criterios como: marca, modelo, versión de *firmware* instalado entre otros.

4.1.2. Administración de imágenes de software

El CWMP provee herramientas para descargar e instalar imágenes software o firmware de CPE. El protocolo, como se mencionó anteriormente, posee mecanismos para identificar versiones, así como notificaciones hacia el ACS, para determinar si se aplicaron correctamente los cambios de software o firmware en el CPE.

El protocolo también define un formato de archivos autenticados digitalmente, que también pueden utilizarse para corroborar la autenticidad de archivos que se manipulan, y así asegurar la integridad de la información.

4.1.3. Monitoreo de estatus y rendimiento

El protocolo CWMP provee soporte a un CPE para hacer que se encuentre disponible información para el ACS, que sea útil para el monitoreo de estatus, rendimiento y obtención de estadísticas. Así también, permite definir mecanismos para que el CPE reporte o envíe notificaciones sobre cambios que ocurran en el mismo.

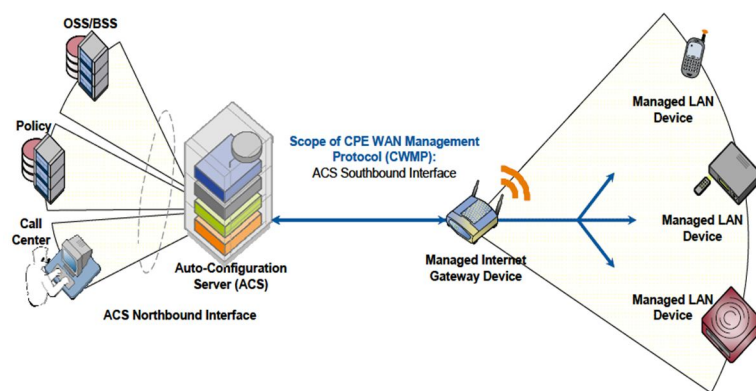
4.1.4. Diagnósticos

Parte del funcionamiento del CWMP es proveer soporte para procesar la información de estatus y monitoreo para realizar diagnósticos proactivos de los dispositivos CPE, y poder resolver fallas en conectividad o problemas con el servicio, así como ejecutar pruebas de diagnóstico predefinidas en el ACS.

4.2. Arquitectura

El ACS es un servidor que reside en la red y administra dispositivos que residen en las instalaciones del cliente. Por lo que el CWMP puede ser utilizado para administrar estos dispositivos (CPE) e inclusive otros. El protocolo no tiene limitantes con el medio de acceso utilizado por el administrador del ACS, usualmente un proveedor de servicios. Sin embargo, sí depende de la conectividad a nivel IP del dispositivo.

Figura 17. Arquitectura punto a punto



Fuente: <https://www.broadbandforum.com/>. Consulta: octubre de 2014.

Dentro de la arquitectura del protocolo, por ser una comunicación en ambas vías desde el administrador de red hasta un cliente, está diseñado con un alto nivel de seguridad y se pueden identificar distintos puntos de seguridad como:

- Prevenir la manipulación de datos por terceros.
- Proveer confidencialidad para las transacciones que se llevan a cabo.
- Brindar la autenticación apropiada para las transacciones que se llevan a cabo.
- Prevenir el robo de servicio.

El CWMP comprende varios componentes que son exclusivos de este protocolo, y utiliza varios protocolos estándar. La pila del protocolo se muestra en la tabla siguiente:

Tabla IV. **Pila de protocolo TR-069**

Pila de protocolo
Aplicación de administración CPE/ACS
Métodos RPC
SOAP
HTTP
SSL/TLS
TCP/IP

Fuente: elaboración propia.

Los componentes de la pila de protocolo TR-069 se describen a continuación:

- Aplicación de administración CPE/ACS: la aplicación utiliza el TR-069 en el CPE y ACS se define localmente y no está definida por el TR-069.
- Métodos RPC: son los métodos definidos por el CWMP, en los cuales se define las acciones que hará el ACS sobre el CPE o viceversa.
- SOAP: es una sintaxis estándar basada en XML para codificar los RPC, en específico la versión SOAP 1.1.
- HTTP: protocolo web que define la sintaxis y semántica para la comunicación de servicios web entre clientes y servidores.
- SSL/TLS: estándar de seguridad de TCP que utiliza *secure socket layer* 3.0 o *transport layer security* 1.0 para que la comunicación sea segura.
- TCP/IP: protocolo estándar de comunicación de red.

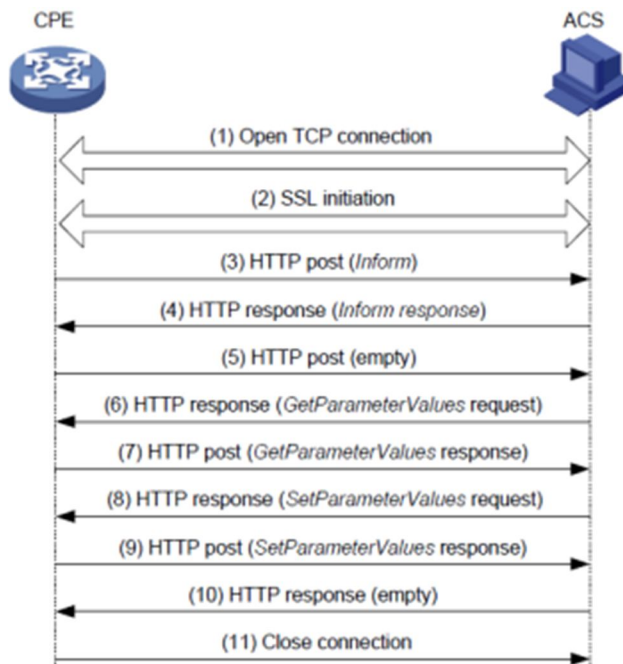
4.3. Sistema en ACS

El sistema que reside en el servidor ACS está compuesto por un sistema operativo, usualmente una versión Unix o Linux, donde luego se instala el software desarrollado para ejecutar el protocolo TR-069.

4.3.1. Funcionamiento de TR-069

El ejemplo siguiente es para ilustrar cómo funciona el estándar bajo el escenario descrito a continuación: existen dos ACSs, activo y pasivo en una determinada área. El ACS activo necesita reiniciarse para realizar un *upgrade* del sistema. De modo que para asegurar el monitoreo continuo de los CPEs, el ACS principal favorece que todos los CPEs en el área se conecten hacia el ACSs de respaldo. El proceso sería como el siguiente:

Figura 18. Ejemplo interacción mensajes TR-069



Fuente: <http://www.h3c.com>. Consulta: octubre de 2014.

4.4. Procedimiento de autoconfiguración

El objetivo principal del protocolo es lograr la autoconfiguración de dispositivos CPE. Para lograr esto se tuvo que haber conectado exitosamente el CPE hacia el servidor.

Todo lo anterior se logra luego de haber cumplido las premisas siguientes:

- El CPE está encendido, y puede encontrar a su servidor ACS con base en el URL preconfigurado e iniciar automáticamente la conexión hacia el ACS.
- El CPE está configurado para enviar mensajes de manera periódica para establecer conexión hacia el ACS.
- El CPE se encuentra configurado para enviar mensajes a una hora específica y establecerá conexión hacia el ACS.
- La sesión entre CPE-ACS estaba establecida y se interrumpió, por lo que el CPE intentará reconectarse.
- El ACS, una vez posea un CPE registrado y autenticado, puede iniciar la conexión hacia el CPE en cualquier momento.

Luego que se cumpla una de las premisas anteriores, el CPE se registra con el ACS y este puede automáticamente aplicar algunas configuraciones al CPE, para que se pueda habilitar la autoconfiguración.

Los parámetros de autoconfiguración soportados por el dispositivo incluyen, pero no se restringen únicamente a estos:

- Archivo de configuración (*ConfigFile*)
- Dirección de ACS (*URL*)
- Usuario de ACS (*username*)
- Contraseña de ACS (*password*)
- Mensajes de estatus periódicos (*PeriodicInformEnable*)
- Mensajes de estatus por intervalo (*PeriodicInformInterval*)
- Usuario de CPE (*ConnectionRequestUsername*)
- Contraseña de CPE (*ConnectionRequestPassword*)

4.4.1. Métodos RPC

Según las definiciones del TR-069, se utiliza una serie de métodos RPC (*Remote procedures call*) para la intercomunicación CPE y ACS. Los métodos RPC principales que se utilizan se describen a continuación:

- *Get*: este método es utilizado por un ACS para obtener un valor de uno o más parámetros del CPE.
- *Set*: método utilizado por un ACS para establecer un valor o valores dentro de la configuración del CPE.
- *Inform*: es un método utilizado por el CPE para enviar un mensaje a un ACS cada vez que este inicie una conexión hacia el ACS, o la configuración del CPE cambie, o bien para enviar información periódica del CPE.

- *Download*: este método es usado por un ACS para forzar que un CPE descargue un archivo de configuraciones, o de *firmware* o *software*.
- *Upload*: este método es usado por un ACS para indicar al CPE que envíe un archivo a una localidad especificada por el ACS.
- *Reboot*: el método es usado por un ACS para reiniciar un CPE, remotamente cuando el CPE reporta alguna falla o requiere un cambio de *firmware* o *software*.

5. DISEÑO DE RED CON INTEGRACIÓN A PROTOCOLO TR-069

Para elaborar el diseño de red se debe realizar un conjunto de actividades, cuyo objetivo debe ser revelar la situación actual o inicial para plantear los puntos de acción y presentar el diseño.

5.1. Situación actual

La situación actual debe ser un campo a evaluar en toda operación previa a realizar el diseño. En este caso, para el tema que se ha propuesto, la situación general que se posee es una infraestructura sin monitoreo ni control sobre los equipos CPEs que utilizan los clientes de los proveedores de servicio.

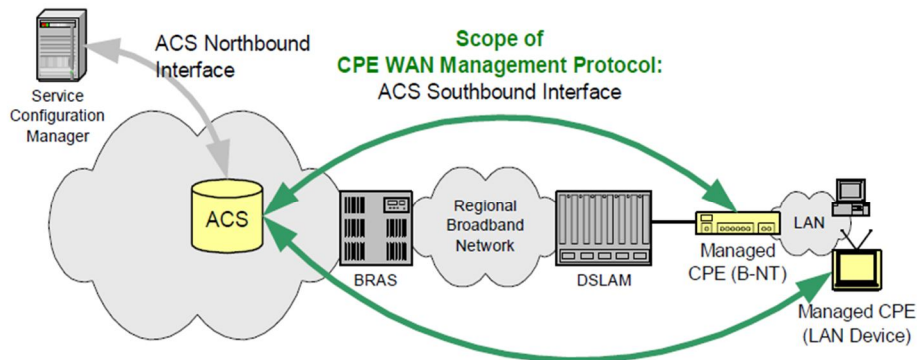
Los aspectos generales de un proveedor de servicios que brinda el servicio de acceso de banda ancha por medio de par trenzado de cobre, son usualmente los siguientes:

- Cliente: posee un CPE conectado al punto (b1) un *splitter* que se encarga de eliminar las portadoras de voz y del lado (b2) del *splitter* el teléfono, mientras del lado (a) el cable que proviene de la caja terminal.
- Proveedor:
 - Planta externa: la caja terminal se conecta a la red secundaria de cobre que llega hasta un armario o caja de distribución, donde se interconecta a la red primaria que proviene de una central telefónica o unidad remota.

- o Planta interna: la red de cobre que alcanza las cajas de distribución proviene de un *splitter* que se encarga de mezclar la señal de datos provenientes de un DSLAM y la voz proveniente de una central de conmutación.

Luego de describir el escenario anterior, se debe enfocar en el área de datos, puesto que es un área con mayor diversidad donde se pueden desarrollar las aplicaciones para poder llevar a cabo la aplicación del protocolo TR-069.

Figura 19. Alcance del protocolo



Fuente: www.broadbandforum.com. Consulta: octubre de 2014.

5.2. Requisitos físicos (características)

Dentro de los requisitos físicos está el identificar el hardware (servidor) o grupo de servidores que se instalarán. En este caso, los requerimientos pueden variar de instalación a instalación por las diferentes necesidades de cada proveedor. El factor principal que se debe tomar en consideración, es la cantidad de dispositivos (CPEs) que se gestionarán y/o monitorearán.

Los parámetros de diseño son: los CPEs que solamente poseen conexiones Ethernet cableadas; realizan en promedio de 2 a 4 sesiones de aprovisionamiento hacia el servidor, si son CPEs que proveen servicio wifi, la cantidad de sesiones aumenta de 4 a 8 por día. Con base en estos parámetros, el foro de *broadband* aconseja las siguientes capacidades en los servidores para la implementación del ACS.

Tabla V. **Requerimientos mínimos**

Ítem	Capacidad		
	100mil CPE	250mil CPE	500mil CPE
Arquitectura	64bits	64bits	64bits
Conectividad	2x1GigaEthernet	2x1GigaEthernet	2x1GigaEthernet
CPU	1x12Core	2x12Core	2x24Core
HDD	2X 250GB	2x 500GB	2X SAS 500GB
Fuente de Poder	Redundante	Redundante	Redundante
Sistema operativo	Unix/Linux	Unix/Linux	Unix/Linux

Fuente: www.broadbandforum.com. Consulta: octubre de 2014.

5.3. **Requisitos lógicos (características)**

Para los parámetros lógicos que se deben tomar en cuenta está el ancho de banda que utilizará la aplicación para comunicarse con los distintos CPEs que integren la red.

En específico, los requerimientos de ancho de banda dependen de lo siguiente:

- Cantidad de dispositivos a ser administrados
- Frecuencias de sesiones por día
- Cantidad de parámetros del CPE que serán monitoreados

Tabla VI. **Consumo ancho de banda**

	Tiempo de monitoreo	100.000 CPE	250.000 CPE	500.000 CPE
Sin sesión	Cada 30 minutos	4.7 1.8 Mbps	13.9 5.2 Mbps	23.1 8.7 Mbps
1 parámetro GPV		6.1 2.5 Mbps	18.1 17.4 Mbps	30.2 12.2 Mbps
2 parámetros GPV		6.3 2.6 Mbps	18.7 7.6 Mbps	31.1 12.7 Mbps
GPV adicional		+187 91 kbps	+561 274 kbps	+934 456 kbps
No. CPE/s		56	167	278
No. sesiones/s		112	334	556

Fuente: www.broadbandforum.com. Consulta: octubre de 2014.

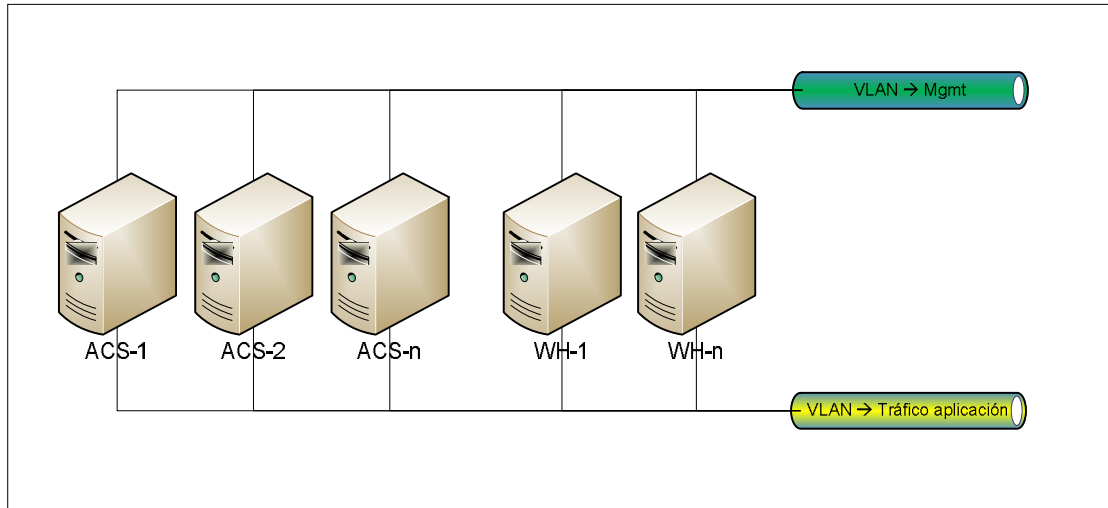
La tabla anterior se puede tomar como referencia para dimensionar el ancho de banda que ocupará dentro de la red al momento que esté en un ambiente de producción.

5.4. Diseños para la integración a una red en producción

A continuación se propone una serie de diseños para la integración de la plataforma, evaluando sus ventajas y desventajas.

Como primer paso se debe diferenciar al menos dos tipos de tráfico que cursarán por la solución: el primero, el tráfico de operación y mantenimiento, usualmente abreviado como OAM, servirá para que los usuarios del proveedor de servicio puedan acceder a la aplicación del software y ejecuten tareas de control y mantenimiento. El segundo tipo de tráfico debe ser el aplicativo, por donde se llevará a cabo la transmisión de la información del servidor hacia los CPEs, centro de atención al cliente, OSS, BSS.

Figura 20. Tipo de tráfico en solución TR-069

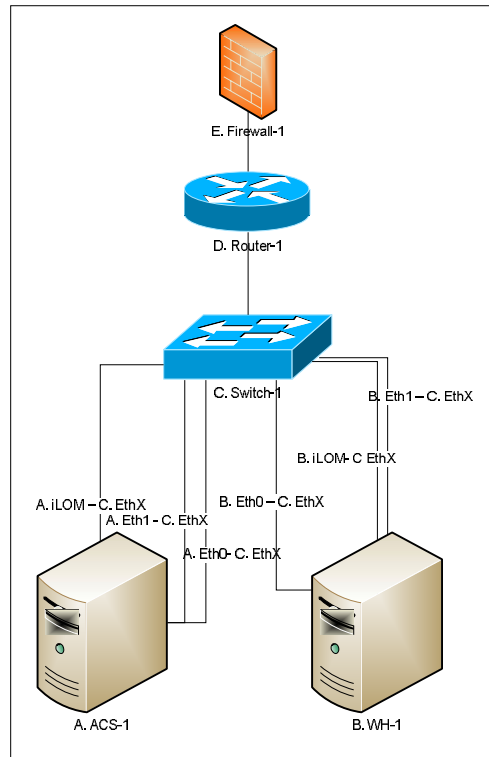


Fuente: elaboración propia, con programa Microsoft Visio 2010.

Como primer diseño básico en donde solamente se posee un servidor para autoconfiguración y un servidor como almacenamiento histórico de datos, se debe poseer al menos dos interfaces que brinden redundancia física a nivel de interfaz, así como una interfaz adicional de iLOM. Cabe destacar que se está considerando un elemento de capa 2 *switch* para que posea la alta conmutación de paquetes y luego al momento de requerir comunicación hacia los CPEs, debería llegar el tráfico hacia el elemento capa 3 *router*, que luego enviaría el tráfico hacia el elemento *firewall*, donde se poseerían las reglas de acceso para evitar vulnerabilidades de seguridad.

A continuación se muestra el diagrama de este primer diseño propuesto.

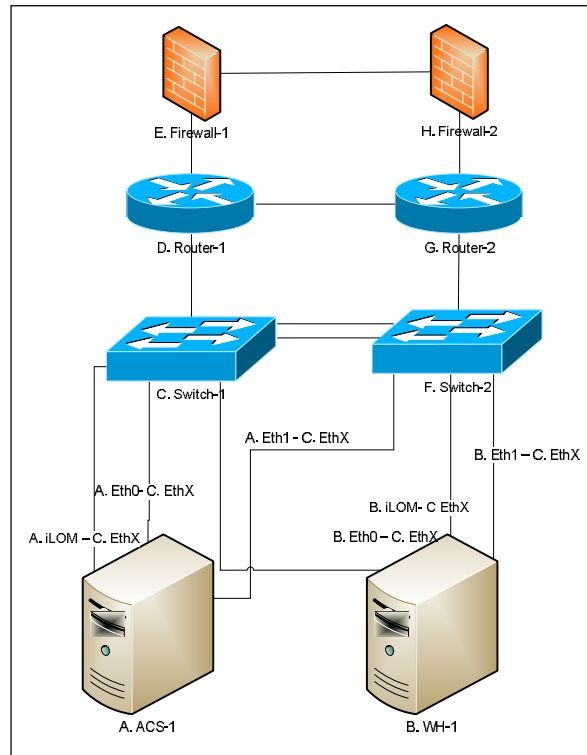
Figura 21. Diseño I



Fuente: elaboración propia, con programa Microsoft Visio 2010.

La variante que puede ocurrir es que se agregue una mayor cantidad de servidores, en cuyo caso se deberá agregar más elementos de red que soporten el tráfico de estos servidores. Por otro lado, la recomendación es colocar redundancia a nivel de elementos de capa 2 (switch), con el fin de establecer una capa de acceso, donde las conexiones *alpha* de un servidor se conecten hacia switch *alpha* y las conexiones *beta* hacia el switch *beta*, y las conexiones de los elementos de capa 2 se conectarían hacia elementos de capa 3 (*router*), como se muestra en el segundo diseño.

Figura 22. **Diseño II**



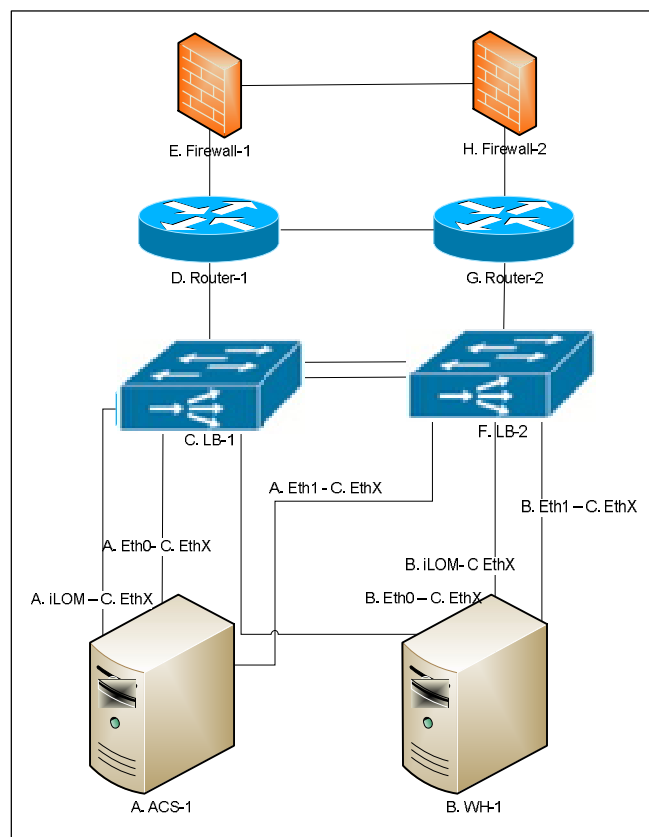
Fuente: elaboración propia, con programa Microsoft Visio 2010.

Los diseños mostrados anteriormente son los recomendables para instalaciones pequeñas y medianas, donde no se sobrepasará la cantidad de elementos CPE en 250.000.

Para despliegues mayores a los 250.000 dispositivos, ya no se debe poseer elementos físicos que no posean un elemento de respaldo. Además, en este caso se recomienda que quien conecte hacia los servidores físicos no sea un elemento capa 2 (switch), sino un elemento de red especializado en recibir conexiones como un balanceador de carga.

Como se mencionó anteriormente para despliegues mayores a los 250.000 dispositivos, es recomendable utilizar balanceadores de carga que son capaces de utilizar elementos de capas del modelo OSI, superiores para validar el estatus de las conexiones TCP o UDP y para controlar qué servidor está recibiendo una mayor carga. A nivel físico la topología no posee mayores variaciones, pues el elemento de capa 2 se sustituye por otro dispositivo, por lo que el diagrama topológico es el mismo.

Figura 23. **Diseño III**



Fuente: elaboración propia, con programa Microsoft Visio 2010.

De los diseños anteriores se pueden resumir las características físicas y lógicas en una tabla comparativa.

Tabla VII. **Comparativa**

Característica	Diseño I	Diseño II	Diseño III
Redundancia física servidor	<ul style="list-style-type: none"> • Se cumple al poseer doble link hacia dispositivo de red. 	<ul style="list-style-type: none"> • Se cumple al poseer doble link hacia dispositivo de red. 	<ul style="list-style-type: none"> • Se cumple al poseer doble link hacia dispositivo de red.
Redundancia lógica	<ul style="list-style-type: none"> • En este caso existen dos tipos: una brindada a nivel de red y otra a nivel de máquinas virtuales. 	<ul style="list-style-type: none"> • En este caso existen dos tipos: una brindada a nivel de red y otra a nivel de máquinas virtuales. 	<ul style="list-style-type: none"> • En este caso existen dos tipos una brindada a nivel de red y otra a nivel de máquinas virtuales.
Redundancia física elementos red	<ul style="list-style-type: none"> • Por ser el diseño más elemental, no cuenta con redundancia de elementos de red. 	<ul style="list-style-type: none"> • Se posee redundancia, factor altamente recomendable. 	<ul style="list-style-type: none"> • Se posee redundancia, factor altamente recomendable.
Balance de carga	<ul style="list-style-type: none"> • No se posee, ya que esta no es característica de <i>switches</i> o <i>routers</i>. 	<ul style="list-style-type: none"> • No posee ya que esta no es característica de <i>switches</i> o <i>routers</i>. 	<ul style="list-style-type: none"> • Sí cumple, ya que posee un elemento especializado para realizar dicha función.

Fuente: elaboración propia.

CONCLUSIONES

1. El desarrollo de los temas en el trabajo de graduación tiene en mayor porcentaje un enfoque cualitativo, para poder introducir al lector en los conceptos que integran y se utilizan en las redes de proveedores de servicio.
2. Se determinó que el protocolo TR-069 por operar en capas superiores del modelo OSI, se puede utilizar en distintas tecnologías de acceso como HFC e inalámbrico.
3. El estudio de la evolución en tecnologías DSL reveló que es más sencillo aplicar el protocolo TR-069 en versiones más recientes de DSL como ADSL2 y posteriores, debido a que los dispositivos elaborados para esta tecnología poseen compatibilidad nativa con el protocolo.
4. La investigación de las funciones del protocolo TR-069 reveló que los parámetros más importantes son la frecuencia con que se establecen las sesiones entre dispositivo y servidor.
5. La arquitectura que fue propuesta para el diseño es capaz de soportar la implementación del protocolo TR-069 de una manera robusta.

RECOMENDACIONES

1. Tomar en cuenta recopilar la información más actualizada de la red, en la que se pretende implementar el protocolo para elaborar el diseño más apropiado.
2. Considerar la cantidad de parámetros que se desean monitorear, porque estos tienen un impacto directo sobre el procesamiento del servidor y pueden limitar la cantidad de dispositivos que se van a monitorear y configurar.
3. Implementar la solución como una granja de servidores que se encuentren conectados detrás de un balanceador de carga.
4. Considerar la separación del tráfico de operación y mantenimiento del tráfico aplicativo, ya sea por medios lógicos o físicos.
5. Con base en el hardware y dispositivos de red que se utilicen para implementar la solución de TR-069 dentro de una red de proveedor de servicios, verificar cuáles son sus capacidades para considerarlo al momento de crecimiento en la red.

BIBLIOGRAFÍA

1. *Configuración TR-069*. [en línea]. <http://www.h3c.com/portal/Technical_Support_Documents/Technical_Documents/Security_Products/H3C_SecPath_U200-A_U200-M_U200-s/Configuration/User_Manual/01-Firewall_Web_Configuration_Manual-5PW100/201205/746107_1285_0.htm>. [Consulta: septiembre de 2014].
2. *Distancias administrativas*. [en línea]. <<http://switchingandrouting.wordpress.com/2011/07/10/administrative-distance-ad-values-in-cisco-juniper/>>. [Consulta: junio de 2014].
3. *Estándar GSM*. [en línea]. <<http://es.kioskea.net/contents/681-estandar-gsm-sistema-global-de-comunicaciones-moviles/>>. [Consulta: junio de 2014].
4. *FTTx*. >. [en línea]. <<http://wikitel.info/wiki/FTTx>> [Consulta: junio de 2014].
5. HESSELBACH, Xavier; BOSCH, Jordi. *Análisis de redes y sistemas de comunicaciones*. España: Universidad Politécnica de Cataluña, 2002. 186 p.
6. *IEEE 802.11*. [en línea]. <http://es.wikipedia.org/wiki/IEEE_802.11>. [Consulta: enero de 2013].

7. *Redes celulares.* [en línea]. http://switchingandrouting.wordpress.com/2011/07/10/administrative-distance-ad-values-in-cisco-juniper>. [Consulta: junio de 2014.]
8. *Redes FTTx.* [en línea]. <<http://sx-de-tx.wikispaces.com/FTTx/>>. [Consulta: agosto de 2014].
9. *Redes HFC.* [en línea]. <<http://es.kioskea.net/contents/681-estandar-gsm-sistema-global-de-comunicaciones-moviles/>>. [Consulta: junio de 2014].
10. TANENBAUM, Andrew. *Computer networks*. 4a ed. México: Pearson, 2003. 912 p.
11. *Tecnologías xDSL y ADSL.* [en línea]. <<http://es.kioskea.net/contents/681-estandar-gsm-sistema-global-de-comunicaciones-moviles/>>. [Consulta: 11 de agosto de 2014].
12. *TR-069.* [en línea]. <<http://www.broadband-forum.org/technical/download/TR069.pdf>>. [Consulta: septiembre de 2014].
13. *VDSL y VDSL2.* [en línea]. <http://albertllongueras.cat/albert_universitat/Telecos/Sistel/vdsl-vdsl2.pdf>. [Consulta: agosto de 2014].