

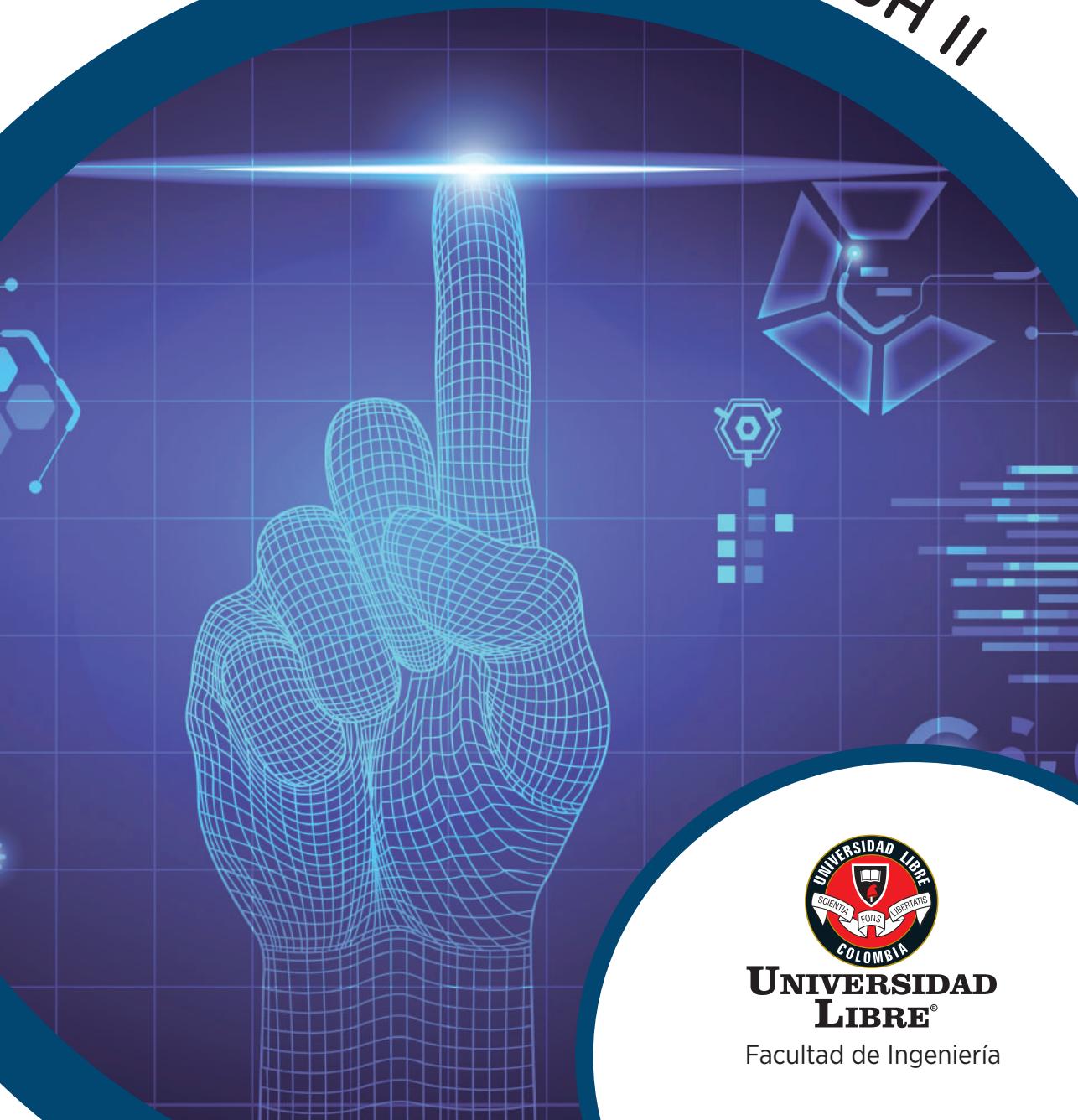
Fredys A. Simanca H.  
Fabián Blanco Garrido  
Eduardo Triana Moyano

# LAS REDES MESH II



Fredys A. Simanca H.  
Fabián Blanco Garrido  
Eduardo Triana Moyano

# LAS REDES MESH II



**UNIVERSIDAD  
LIBRE®**

Facultad de Ingeniería

Simanca H., Fredys A.  
Las Redes MESH II / Fredys A. Simanca H., Fabián Blanco Garrido, Eduardo Triana Moyano.  
-- Bogotá: Universidad Libre, 2018.

240 p.: il.; 17x24 cm.

Incluye referencias bibliográficas.

ISBN: 978-958-5466-41-8

1. Redes de computadores 2. Arquitectura de redes de computadores 3. Redes de computadores – Protocolos I. Blanco Garrido, Fabián II. Triana Moyano, Eduardo

004.6 SCDD 21

Catalogación en la Fuente – Universidad Libre. Biblioteca.

Fredysa.simancah@unilibre.edu.co  
Fabian.blancog@unilibre.edu.co  
Eduardo.trianam@unilibre.edu.co

© Fredys A. Simanca H., Fabián Blanco Garrido, Eduardo Triana Moyano, 2018  
© Facultad de Ingeniería, 2018  
© Universidad Libre Sede Principal, 2018

ISBN IMPRESO: 978-958-5466-41-8  
ISBN DIGITAL: 978-958-5466-42-5

Queda hecho el depósito que ordena la ley.  
Reservados todos los derechos. No se permite la reproducción total o parcial de esta obra, ni su incorporación a un sistema informático, ni su transmisión en cualquier forma o por cualquier medio (electrónico, mecánico, fotocopia, grabación u otros) sin la autorización previa y por escrito de los titulares del copyright.

Editorial: Universidad Libre

Coordinación de edición: Siby I. Garcés Polo  
Correo-e: sibygarcés@unilibre.edu.co  
Coordinación de Publicaciones y Comunicaciones: Luz Bibiana Piragauta Correa  
Correo-e: comunicaciones@unilibre.edu.co  
Calle 8 No. 5-80, Tel.: 3821000, Bogotá D.C.

Corrección de estilo: Sonia Sánchez  
Correo-e: sancsonia@gmail.com

Diagramación e impresión:  
Xpress Estudio Gráfico y Digital S.A.S. - Xpress Kimpres  
Tel. 602 0808  
Bogotá, D.C., septiembre 2018

Esta obra está cofinanciada por el Fondo de Publicaciones de la Universidad Libre  
Impreso en Colombia

Bogotá D.C., Colombia, 2018  
*Printed in Colombia*



## **UNIVERSIDAD**

**LIBRE®**

### **DIRECTIVAS**

JORGE ALARCÓN NIÑO

**PRESIDENTE**

JORGE GAVIRIA LIÉVANO

**VICEPRESIDENTE**

FERNANDO ENRIQUE DEJANÓN RODRÍGUEZ

**RECTOR NACIONAL**

FLORO HERMES GÓMEZ PINEDA

**SECRETARIO GENERAL**

RICARDO ZOPÓ MÉNDEZ

**CENSOR NACIONAL**

ALEJANDRO MUÑOZ ARIZA

**DIRECTOR NACIONAL DE PLANEACIÓN (E)**

ELIZABETH VILLARREAL CORRECHA

**DIRECTORA NACIONAL DE INVESTIGACIONES**

JULIO ROBERTO GALINDO HOYOS

**PRESIDENTE SECCIONAL**

JESÚS HERNANDO ÁLVAREZ MORA

**RECTOR SECCIONAL**

MARTHA RUBIANO GRANADA

**DECANA FACULTAD DE INGENIERÍA**

SIBY INÉS GARCÉS POLO

**DIRECTORA CENTRO DE INVESTIGACIÓN FACULTAD INGENIERÍA (CIFI)**

MAURICIO ALONSO MONCADA

**DIRECTOR PROGRAMA DE INGENIERÍA DE SISTEMAS**





# Contenido

INTRODUCCIÓN .....	13
--------------------	----

## (1) Esquematización teórica

Introducción .....	15
1.1 Sistema electrónico de comunicación de datos.....	16
1.2 Red de cómputo.....	17
1.3 Sistema distribuido .....	20
1.4 Espectro electromagnético.....	21
1.5 Infraestructura de conectividad.....	23
1.6 Modelo IEEE 802.X .....	27
1.7 Estándar IEEE 802.11 .....	30
1.8 Comparaciones de estándares IEEE 802 .....	37
1.9 Redes MESH.....	42
1.10 Marco legal .....	51
1.11 Marco tecnológico .....	56
1.12 Contexto social de las redes MESH.....	71
1.13 Plan Vive Digital.....	74
1.14 Redes inalámbricas .....	80
1.15 Ataques.....	84
1.16 Protocolos de seguridad.....	91
Conclusión .....	100



## ( 2 ) Distribución y acceso a los servicios inalámbricos MESH para los estratos menos favorecidos

Introducción.....	101
2.1 Diseño y construcción ingenieril.....	101
2.2 Soporte lógico de comunicaciones MESH.....	113
2.3 Soporte de Modulación Especializado MESH.....	119
2.4 Validación de infraestructura tecnológica .....	141
2.5 Soporte decisional para selección de infraestructura tecnológica .....	142
2.6 Fase de configuración tecnología .....	148
2.7 Fase de configuración de servicios.....	149
Conclusión .....	153

## ( 3 ) Modelo de Implementación de protocolo OPEN SSL para el manejo de la seguridad en infraestructura de redes MESH

Introducción .....	155
3.1 Esquematización ingenieril.....	155
3.2 Generación de certificado AC y clave.....	159
3.3 Generación de certificado servidor cliente.....	159
3.4 Uso de los certificados.....	167
Conclusión .....	170

## ( 4 ) Diseño de una arquitectura de streaming para Redes MESH en entornos de bajos recursos en Colombia

Introducción.....	171
4.1 Montaje del servicio Streaming sobre plataformas de software libre .....	171
4.1.1 Ancho de banda requerido .....	173
4.1.2 Video.....	175
4.1.3 Audio.....	176
4.1.4 Montaje del servicio y emisión .....	176
4.1.5 Emisión de contenido.....	180



Fredys A. Simanca H., Fabián Blanco Garrido, Eduardo Triana Moyano

4.1.6 Visualización del contenido .....	186
Conclusión .....	190

## **( 5 ) Diseño e implementación de una Red MESH como alternativa de solución para redes comunitarias o rurales**

Introducción.....	191
5.1 Instalación de un nodo MESH .....	191
5.2 Cálculo del presupuesto de enlace .....	195
5.3 Instalación el nodo .....	203
5.4 Configuración del nodo MESH.....	207
5.5 B.A.T.M.A.N. (Better Approach to Mobile Adhoc Networking)	223
5.6 Webmin.....	224
5.7 Contenidos de servidor web: Joomla .....	228
5.8 Estableciendo la Wikipedia en el servidor web con KIWIX .....	231
Conclusión .....	236
Referencias bibliográficas .....	237



## Índice de figuras

Figura 1.1.	Configuración Sistema electrónico de comunicación de datos .....	16
Figura 1.2	Infraestructura operacional de una solución.....	17
Figura 1.3	Estructura Modelos convencionales de interconexión	19
Figura 1.4	Estructura sistema distribuido.....	20
Figura 1.5	Normativa de proceso distribuido.....	21
Figura 1.6	Espectro electromagnético.....	22
Figura 1.7	Descriptor de interconectividad. ....	25
Figura 1.8	Estructura IPV4.....	26
Figura 1.9	Estructura IPV6.....	26
Figura 1.10	Esquema operacional IEEE 802.11.....	28
Figura 1.11	Proceso de ajuste de reloj.....	30
Figura 1.12	Estructura del proyecto IEEE 802. ....	31
Figura 1.13	Antiguo estándar 802.1.....	33
Figura 1.14	Conexión con protocolo IEEE 802.3 Ethernet.....	34
Figura 1.15	Dirección que toma Token, estándar IEEE 802.4. ....	35
Figura 1.16	IEEE 802.5 formato de Token Ring. ....	35
Figura 1.17	Disposición de los equipos bajo la norma 802.11b.....	37
Figura 1.18	Distribución de canales normas IEEE 802.11b e IEEE 802.11g.....	38
Figura 1.19	Estructura de capas de la norma IEEE 802.16. ....	40
Figura 1.20	Estructura Servicio de Streaming.....	44
Figura 1.21	Etiqueta límites. ....	46
Figura 1.22	Etiqueta de autenticación.....	48
Figura 1.23	Etiqueta Directorio. ....	49
Figura 1.24	Configuraciones del servidor.....	49
Figura 1.25	Configuración de puerto. ....	50
Figura 1.26	Esquema Funcional de una red MESH.....	57
Figura 1.27	Topología de Red Ad-Hoc. ....	58
Figura 1.28	Distribución de una red Multi-Hop.....	59
Figura 1.29	Arquitectura plana: Nodo (N). ....	60
Figura 1.30	Arquitectura jerárquica: Nodo (N), Clusterhead (C) y Gateway (G).....	61
Figura 1.31	Esquema de una red MESH en una ciudad.....	61



Figura 1.32	Ilustración red MESH primera generación.....	68
Figura 1.33	Ilustración red MESH segunda generación.....	69
Figura 1.34	Ilustración red MESH tercera generación.....	70
Figura 1.35	Colegio Rafael Uribe Uribe, Sede Secundaria.....	72
Figura 1.36	Universidad Libre, Sede Bosque Popular – Bloque L y A.....	73
Figura 1.37	Ecosistema digital.....	75
Figura 1.38	Barreras que impiden la Masificación de Internet en Colombia .....	78
Figura 1.39	Gráfico de metas de conexión en Colombia. ....	80
Figura 1.40	Clases de redes inalámbricas .....	81
Figura 1.41	Red WPAN, dispositivos conectados a la red.....	82
Figura 1.42	Red WLAN, comunicación entre diferentes dispositivos de áreas diferentes. ....	83
Figura 1.43	Red inalámbrica metropolitana.....	83
Figura 1.44	Tecnologías WWAN, evolución a través del tiempo .....	84
Figura 1.45	Ataques y amenazas en una red inalámbrica.....	85
Figura 1.46	Ataque sniffing sobre una red inalámbrica.....	86
Figura 1.47	Ataque mediante suplantación .....	88
Figura 1.48	Ataque mediante DoS.....	88
Figura 1.49	Ataque mediante modificación – daño .....	89
Figura 1.50	Delitos informáticos .....	89
Figura 1.51	Mecanismos para la seguridad en redes inalámbricas..	90
Figura 1.52	Diagrama de protocolo PPTP Microsoft .....	99
Figura 2.1	Modelos de conectividad.....	103
Figura 2.2	Catalogación de interceptores.....	104
Figura 2.3	Especificación lógica del interceptor.....	105
Figura 2.4	Base de primitivas de socket TCP/IP .....	106
Figura 2.5	Parametrización Gráfica R (t).....	109
Figura 2.6	Catalogación de la Multitransmisión en Redes MESH...	111
Figura 2.7	Formalización 2PC/3PC.....	112
Figura 2.8	Onda SSBFC.....	114
Figura 2.9	Proceso general de banda única.....	116
Figura 2.10	Modulación FM/PM. ....	118
Figura 2.11	Componentes sistema celular. ....	121
Figura 2.12	Propagación de ondas .....	125
Figura 2.13	Tipología de antenas convencionales soluciones MESH	132



Figura 2.14	Antena BTC (Lata de Tomate) .....	134
Figura 2.15	Antena Frisko.....	135
Figura 2.16	Antena Biquad. ....	136
Figura 2.17	Antena de Flickeng.....	137
Figura 2.18	Área de cubrimiento Ciudad Bolívar .....	138
Figura 2.19	Área de cubrimiento localidad de Usme .....	139
Figura 2.20	Unidad rectora para configuración nodos MESH-UNILIBRE.....	140
Figura 2.21	Valoración proceso de asignación para compra de recursos .....	144
Figura 2.22	Grafo de asignación. ....	147
Figura 2.23	Registro de Usuario MESH. ....	152
Figura 2.24	Estructura de cursos.....	152
Figura 2.25	Validación temática de curso. ....	153
Figura 3.1	Verificación del certificado SSL.....	168
Figura 3.2	Verificación del certificado SSL en Google Chrome .....	169
Figura 3.3	Verificación del certificado SSL en Internet Explorer ....	170
Figura 4.1	Estructura servicio.....	172
Figura 4.2	Instalación Icecast2 .....	177
Figura 4.3	Configuración contraseña iceast2 .....	177
Figura 4.4	Instalación codificador OGG.....	177
Figura 4.5	Instalación codificador FFmpeg .....	178
Figura 4.6	Archivo de configuración Icecast .....	178
Figura 4.7	Configuración auto inicio icecast2 .....	179
Figura 4.8	Ejemplo dirección de servidor streaming. ....	180
Figura 4.9	Servidor Icecast en ejecución. ....	180
Figura 4.10	Menú “Medio” en VLC.....	181
Figura 4.11	Ventana para añadir archivos a emitir. ....	181
Figura 4.12	Ventana configuración fuente de contenido.....	182
Figura 4.13	Selección de servicio de transmisión. ....	182
Figura 4.14	Configuración Icecast en VLC .....	183
Figura 4.15	Ejemplo configuración Icecast.....	183
Figura 4.16	Selección de formatos de transmisión. ....	184
Figura 4.17	Cadena de emisión. ....	185
Figura 4.18	Servidor emitiendo contenido. ....	185
Figura 4.19	Descarga vínculo contenido Streaming.....	186
Figura 4.20	Descarga archivo xspf. ....	186

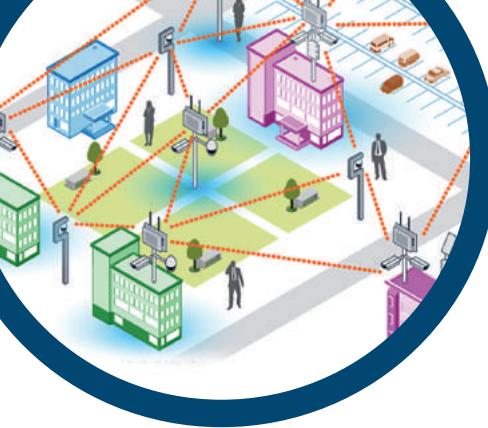


Figura 4.21	Archivo descargado.....	187
Figura 4.22	VLC ejecutándose.....	187
Figura 4.23	Página en dispositivo móvil.....	188
Figura 4.24	Reproducción de audio en dispositivo móvil.....	189
Figura 4.25	Reproducción de video en dispositivo móvil.....	189
Figura 5.1	Tensión de Paso y Tensión de Contacto respectivamente.....	198
Figura 5.2	Sistema de puesta a tierra para el nodo.....	200
Figura 5.3	Preparando la zona para el nodo.....	204
Figura 5.4	Preparando la zona para el router.....	205
Figura 5.5	Nodo Fátima-MESH .....	206
Figura 5.6	Nodo Fátima-MESH protegido.....	207
Figura 5.7	Servidor Debian, escritorio Mate.....	210
Figura 5.8	Entrando a OpenWRT .....	212
Figura 5.9	Interfaz Web OpenWRT LuCI.....	215
Figura 5.10	Instalando Batman-advanced en OpenWRT .....	220
Figura 5.11	Batman instalado en OpenWRT .....	221
Figura 5.12	Activando el servicio del Portal Cautivo NoDogSplash	222
Figura 5.13	Portal Cautivo NoDogSplash Funcionando.....	222
Figura 5.14	Webmin corriendo en servidor local.....	226
Figura 5.15	Interfaz de servidor web apache en Webmin.....	227
Figura 5.16	Creando el servidor virtual.....	228
Figura 5.17	Servidor virtual corriendo.....	229
Figura 5.18	Visualización de archivos de base de datos Joomla.....	230
Figura 5.19	Página web creada con Joomla en el servidor web.....	230
Figura 5.20	Kiwix corriendo en el servidor local.....	235
Figura 5.21	Wikipedia en servidor local UniMESH.....	235



## Índice de tablas

Tabla 1.1	Características y desventajas de estándares IEEE 802.11 b e IEEE 802.11 g.....	30
Tabla 1.1	Características y desventajas de estándares IEEE 802.11 b e IEEE 802.11 g ..	38
Tabla 1.2.	Frecuencias radioeléctricas. Resolución Número 2190 de 2003.....	54
Tabla 2.1	Registro de elementos de asignación.....	144
Tabla 2.2	Reducción de filas.....	145
Tabla 2.3	Resultados reducción por filas.....	145
Tabla 2.4	Reducción por Columna.....	145
Tabla 2.5	Conexión de ceros. ....	146
Tabla 2.6	Resultados reducción integral. ....	146
Tabla 2.7	Matriz de asignación de recursos. ....	147
Tabla 3.1	Versiones de Open SSL.....	156
Tabla 4.1	Consumo ancho de banda. mbps.....	174
Tabla 5.1	Ganancia de Antenas Inalámbricas. ....	192
Tabla 5.2	Ganancia de la antena nodo Fátima.....	202
Tabla 5.3.	Pérdidas de la antena nodo Fátima.....	202
Tabla 5.4	Presupuesto para el enlace de nodo - cliente.....	202
Tabla 5.5	Hardware del TL-WR941ND. ....	208
Tabla 5.6	Versión soportada de OpenWRT para el router TL-WR941ND.....	208



## Introducción

Redes MESH 2, es la continuación del primer libro que se dedicó a la caracterización del diseño e implementación de redes MESH por medio de conexión inalámbrica en comunidades rurales de Colombia con el propósito de disminuir la brecha tecnológica entre las comunidades y las TIC.

Luego del diseño, en este ejemplar, se avanza en la implementación de un nodo MESH con todas la implicaciones y requerimientos de infraestructura tecnológica y física, como fase experimental para lograr las pretensiones de una mayor cobertura en el mediano plazo.

Consecuentemente con el libro uno, la metodología se realizó bajo el concepto de ingeniería didáctica, y de investigación-acción-participativa con el ánimo de implementar una práctica de transformación social inclusiva.

Está conformado por cinco capítulos, en el primer capítulo se presentan los conceptos y principios teóricos de un sistema electrónico de comunicación de datos, y se exhibe un extenso recorrido por la esquematización de una red de computo, con énfasis en los modelos convencionales de interconexión; el sistema distribuido, con su respectiva normatividad; el espectro electromagnético y su representación gráfica piramidal invertida; la infraestructura necesaria para la conectividad; la línea del modelo IEEE 802.X que se formaliza en 1980 y se presentan sus diferentes versiones hasta la vigésima segunda. El capítulo se complementa con el marco legal, la topología, la arquitectura, la aplicación, las ventajas y desventajas, las generaciones y el contexto social de las redes MESH, y culmina con los linemanientos del Plan Vivel Digial, las redes inalámbricas, el análisis del flujo de trafico y los protocolos de seguridad que demanda la red.



El segundo capítulo trata de la distribución y acceso a los servicios inalámbricos MESH para los estratos menos favorecidos. Se parte de la construcción y diseño ingenieril con base en la plataforma lógica y de modulación que da soporte decisional para selección de infraestructura tecnológica que aborda la fase de configuración tecnológica y de servicios.

En el tercer capítulo, se presenta el modelo de implementación de protocolo open SSL para el manejo de la seguridad en infraestructura de redes MESH con su debida esquematización ingenieril.

El diseño de la arquitectura de seguridad de streaming para redes MESH para entornos de bajos recursos en Colombia, se presenta en el capítulo cuatro, la cual se basa en una plataforma de software libre, junto con los requisitos de banda ancha, video, audio para su montaje y emisión.

En el capítulo final se presenta el diseño e implementación de una red MESH, con toda la explicación conceptual, matemática y gráfica de la instalación y configuración de un nodo MESH, específicamente en el barrio Fátima de la ciudad de Bogotá, que incluye la adecuación del router, la instalación de la antena, considerando los factores de seguridad necesarios para la protección contra agentes externos.



# ( 1 )

## Esquematización Teórica

### • Introducción

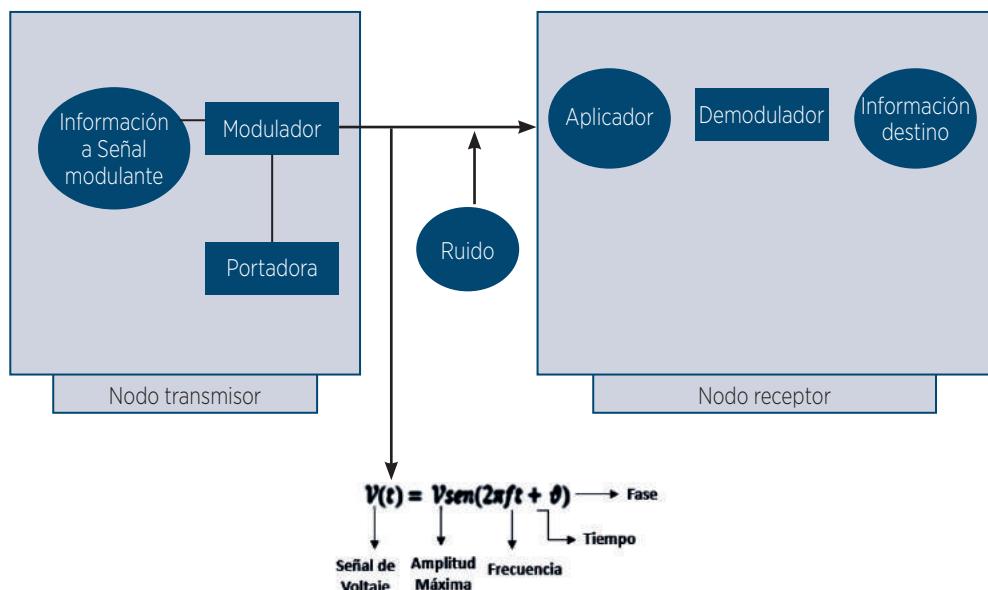
La conexión por medio de redes MESH a través de conexión inalámbrica, es uno de los avances mas importantes de las TIC en la última década. Las redes MESH estan reguladas a nivel internacional por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) y la Unión Internacional de Telecomunicaciones (UIT) y en Colombia por el Ministerio de las Tecnologías de la Información y Comunicaciones (MinTIC), el cual es el encargado de regular y/o administrar el espectro radioelectrónico. Este capítulo se especializa en presentar un amplia travesía teórica de redes MESH, en el que se especifica lo relacionado con la normatividad, el estudio, el diseño y aplicación de las redes, resaltando ventajas y desventajas. Para contar con un concepto extenso del modelo IEEE 802.X, se presenta desde su normalización en 1980, hasta la versión vigesima segunda de red inalambrica regional. Para completar el enfasis teórico, se relacionan las principales características de las tres generaciones de la redes MESH y se contempla la posibilidad de los ataques pasivos y activos que conlllevan a dimensionar los diferentes protocolos de seguridad con sus respectivas bondades y debilidades.

Se presentan los conceptos y principios que normalizan todo sistema electrónico de comunicación de datos; sus parámetros están dados por la configuración de una red telemática y lo determinan los principios que regulan las estructuras de interconectividad computacional, para hacer viable y pertinente la relación existente entre el nivel de aplicación, el nivel de

transporte, el nivel de red y el nivel de enlace de datos. Sus características se detallan a continuación.

## • 1.1 Sistema electrónico de comunicación de datos

Este sistema electrónico es una entidad funcional y operacional lógicamente dispuesta, para habilitar el intercambio transaccional de valores informáticos entre múltiples usuarios que emplean los recursos configurados para intercomunicarse (Tomasi, 2003). Su estructura se visualiza en la figura 1.1.



Fuente: (Tomasi, 2003).

En esta figura se observa que todo sistema electrónico de comunicación de *datos* facilita el diálogo entre un trasmisor y un receptor, bien sea mediante señales análogas o señales digitales, en cualquier caso, la información base o transmitida siempre podrá ser modificada por la presencia del agente distorsionador de la señal, conocido como ruido.



Los sistemas electrónicos de comunicación de datos, pueden ser agrupados en el entorno de las redes convencionales y de los sistemas distribuidos, cuyas características se muestran a continuación.

## • 1.2 Red de cómputo

La red de cómputo es la entidad configurada paramétricamente por interacción del *hardware* convencional, especializado o de soporte telemático, y un software o base logística que controla, supervisa y gestiona es intercambio de valores informáticos (Toueg, 2008). Toda red de cómputo permite identificar la infraestructura que se muestra en la figura 1.2.

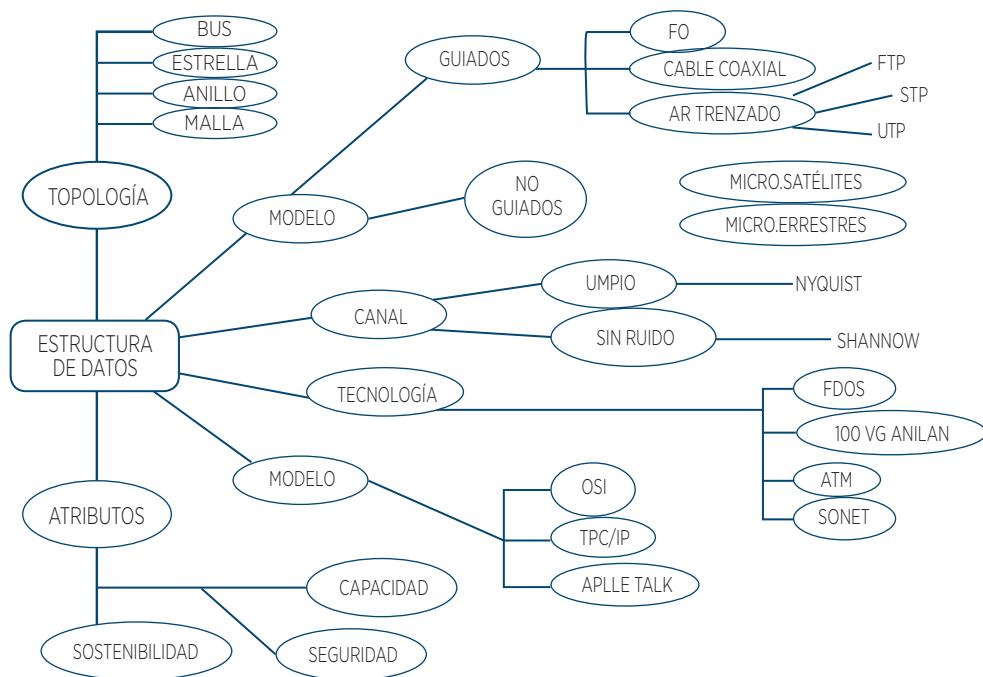


Figura 1.2 Infraestructura operacional de una solución

Fuente: (Toueg, 2008).



Los factores que conforman la infraestructura son:

**Topología:** distribución física de los componentes de la conectividad.

**Medio:** unidad física que habilita o permite el flujo de valores informáticos que se procesan por los usuarios de la red.

**Canal:** unidad dimensional que cuantifica los valores de información que se envían o se reciben durante el intercambio transaccional. En telemática se define el canal de Nyquist como la unidad no propensa al ruido y el canal de Shannon, el cual se caracteriza por operar bajo presencia de ruido.

Las velocidades que se catalogan para el envío o recepción de información son:

Canal de Nyquist:  $\mathcal{V} = 2w \log_2 n$

$\mathcal{V}$  = Velocidad Máxima

$w$  = Ancho de Banda

$n$  = Niveles de Codificación

Canal de Shannon:  $\mathcal{V} = w \log_2 (1 + s/n)$

$\mathcal{V} = 3.32w \log_{10} (1 + s/n)$

$\mathcal{V}$  = Velocidad Máxima

$w$  = Ancho de Banda

$s/n$  = Señal Potencia Ruido

**Tecnología:** soporte con el que se optimiza el intercambio transaccional sobre los componentes configurados en la red, según su característica y ambiente de trabajo. Comúnmente se mencionan las siguientes: FDDI, ATM, SONET, 100 BASE T, 100 VG ANYLAN.

**Modelo:** conjunto de normas y especificaciones que regulan y parametrizan, funcional y operacionalmente, los elementos requeridos para definir



un sistema de interconexión en sus diferentes ejes o escenarios (Tanembaum, 2008). Los modelos más utilizados para la configuración de soluciones de interconexión son: OSI/ISO, TSP/IP y APPLETALK.

Estos modelos estructuran su funcionalidad mediante los niveles o unidades de operación lógica, tal como se presenta en la figura 1.3.

La FDDI, interfaz de datos distribuido por fibra, fue diseñada para cumplir los requerimientos de redes individuales de alta velocidad, y conexiones de alta velocidad entre redes individuales.

MODELO OSI/ISO		MODELO APPLETALK	MODELO TCP/IP
7	Aplicación	Appleshared	Aplicación
6	Presentación	Protocolo de clasificación (AFP)	Transporte
5	Sesión	Protocolo de sesión: ASP, ADSP, ZIP, PAP	Internet
4	Transporte	Protocolo de transporte: ATPP; NBP, RTMP, AEP	Acceso a la red (NAL)
3	Red	Distribución de Datagramas DDP	
2	Enlace	Controladores LAN: LocalTalk, EtherTalk, TokenTalk	
1	Físico	Nivel físico	

**Nota:** Las palabras o acrónimos citados en el modelo APPLETALK se describen en el correspondiente glosario.

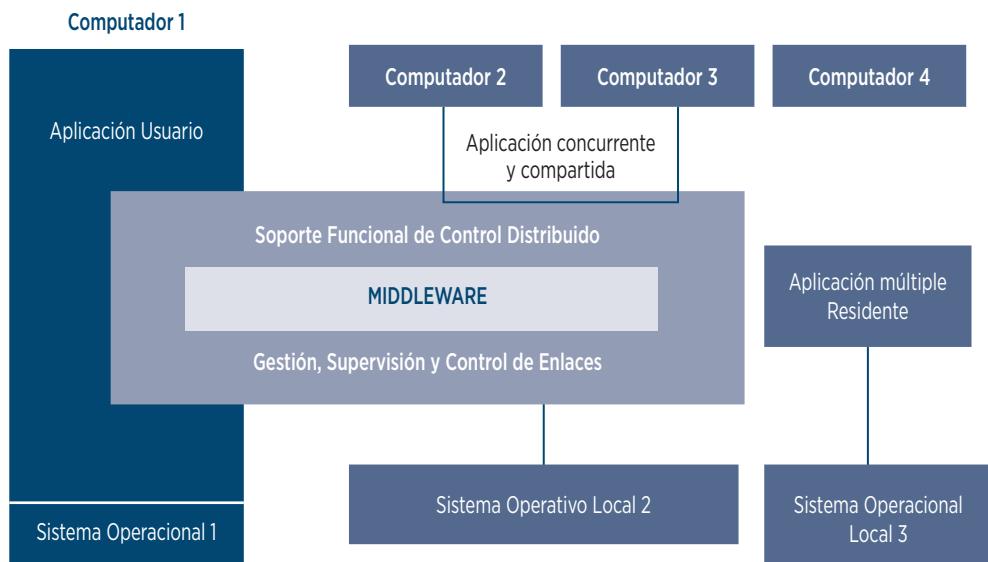
*Figura 1.3 Estructura Modelos convencionales de interconexión.*

*Fuente:* Elaborado por el grupo de investigación.

**Atributos:** entidades que cualifican y regulan el proceso de envío y recepción de valores informáticos en toda solución teleinformática, permitiendo catalogar y diferenciar los procesos de: interoperabilidad, gestionabilidad, seguridad y capacidad. Gracias a la primera, en toda red funcionan concurrentemente diferentes sistemas operativos, a saber: Windows, Linux, Unix, Solaris, o AIX; la gestionabilidad valora el diálogo electrónico entre los concentradores, los switch y los enrutadores; mientras que a nivel de seguridad se especifica lo pertinente a la autentificación, autorización, confidencialidad, integridad y no repudio (Stallings, 2008).

## • 1.3 Sistema distribuido

Un sistema distribuido se acepta en el universo de la telemática, como la conexión de computadores independientes, geográficamente dispersos y con sistemas operativos heterogéneos que permiten el intercambio transaccional, comportándose como un sistema coherente (Tanembaum, 2008). La estructura de un sistema distribuido presenta en la figura 1.4.



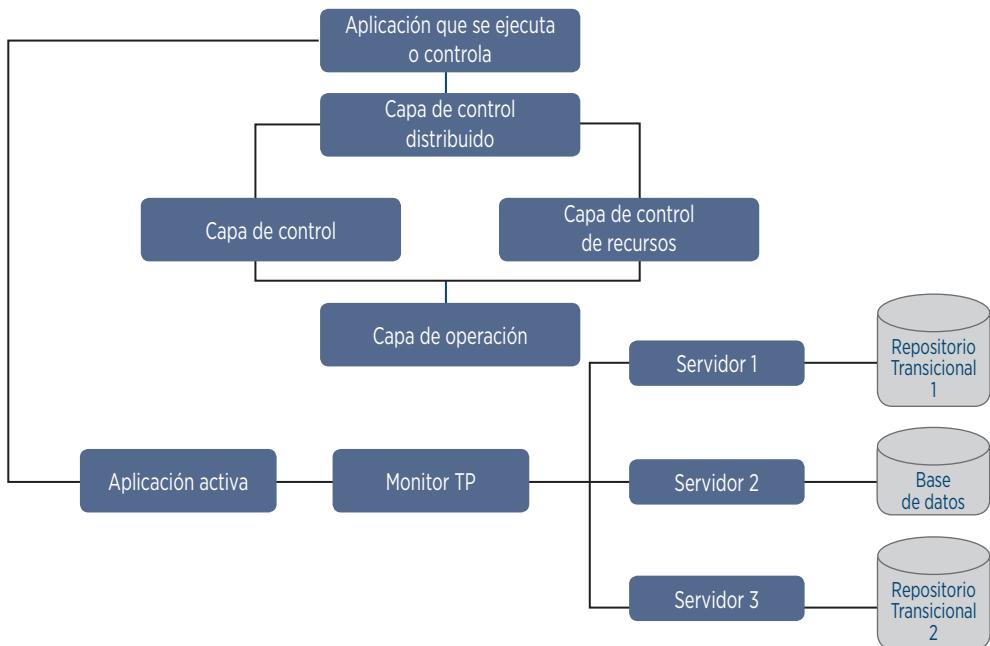
*Figura 1.4* Estructura sistema distribuido.

Fuente: Elaborado por el grupo de investigación.

Todo sistema distribuido, identifica el conjunto de facilidades de interacción usuario-máquina que expresan como factores diferenciadores:

- Facilidad de acceso.
- Ubicación del nodo o equipo.
- Potencialidad de migración.
- Facilidad de reubicación lógica.
- Proyección de réplica.
- Algoritmos y procesos de concurrencia.

Formalmente, los sistemas distribuidos se agrupan en sistemas tipo *Clúster*, los cuales permiten la implementación de la computación en paralelo, al distribuir o sementar tanto la información y las operaciones a realizar, como los sistemas en malla o *Grid*, que determinan la normativa operacional mediante la interacción de las capas de aplicación, las capas de control y las capas de distribución, por ayuda del llamado monitor de proceso transaccional, tal como se visualiza en la figura 1.5. Todo sistema distribuido facilita al usuario un conjunto de acciones y operaciones sobre las cuales se definen los calificadores de rendimientos, a saber: disponibilidad, confiabilidad, seguridad, mantenimiento y control de fallas.



*Figura 1.5* Normativa de proceso distribuido.

Fuente: Elaborado por el grupo de investigación.

## • 1.4 Espectro electromagnético

El espectro electromagnético es la distribución de frecuencias de la energía electromagnética transportada por una señal (Wayne, 2010). El espectro permite cualificar los segmentos operacionales subsónicos, auditivos,



ultrasónicos, regulares, satelitales, de fibra óptica y no convencional: rayos X, rayos Gamma, rayos cósmicos.

La operación con esta distribución de frecuencias constituye la base para calcular la longitud de onda:

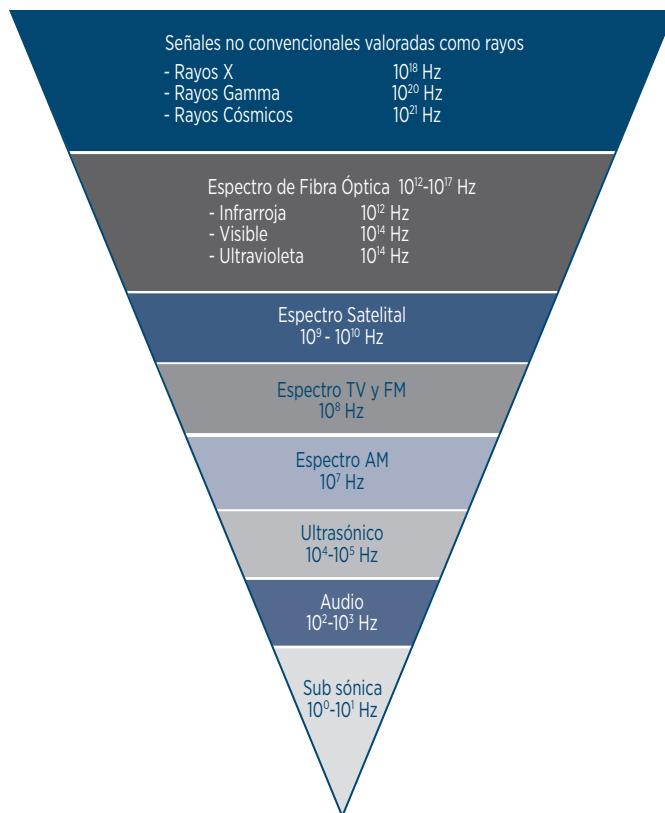
$$\lambda = \frac{v}{f} \quad (1)$$

$\lambda$  = Longitud de Onda

$v$  = Velocidad de la Luz

$f$  = Frecuencia en Hz

En la figura 1.6 se observan los discriminantes del espectro electromagnético.



*Figura 1.6* Espectro electromagnético.

Fuente: Elaborado por el grupo de investigación.



## • 1.5 Infraestructura de conectividad

El entorno de las soluciones de interconexión teleinformáticas, se parametrizan o expresan funcionalmente, al valorar las entidades de enlace, pudiéndose entonces hablar de soluciones con conectividad normal es decir aquellas que requieren de cableado para atar o unir sus nodos operacionales y soluciones inalámbricas, cuyo nivel de interacción e intercambio transaccional se estructura de manera directa aprovechando el flujo en el espacio geométrico de interconexión, independientemente de la infraestructura de conectividad, debe recordarse que dicho intercambio se materializa en cuatro grandes ejes (Stallings, 2008):

- Datos analógicos y señales digitales.
- Datos digitales y señales analógicas.
- Datos digitales y señales digitales.
- Datos analógicos y señales analógicas.

Cuando la infraestructura de conectividad definida opera digitalmente entonces es necesario considerar, que digitalmente se posee inmunidad de ruido, procesamiento multicanal, regeneración de señal, detección y corrección automática de error y medición o dimensionamiento simple de la señal, en este caso, se habla entonces de los esquemas de modulación por pulsos diferenciándose:

- **PWM:** Modulación por ancho de pulso.
- **PPM:** Modulación por posición de pulso.
- **PAM:** Modulación por amplitud de pulso.
- **PCM:** Modulación por codificación de pulso.

La seguridad en la infraestructura de conectividad, se garantiza por la validación de la paridad tanto a nivel de carácter como a nivel de bloque o mensaje total, para lo cual se emplea la técnica convencional del chequeo de redundancia cíclica (CRC), que se define matemáticamente así:

$$CRC = X \circ R \left[ \frac{M(X)}{P(X)} \right] \quad (2)$$



$M(\mathcal{X}) = \text{Mensaje Fuente}$

$M(\mathcal{X})^* = \text{Mensaje Modificado}$

$P(\mathcal{X}) = \text{Polinomio Generador}$

El cálculo del CRC, se establece generalmente mediante el empleo de los siguientes polinomios (Stallings, 2008):

$$\text{CRC } 16 = x^{16} + x^{15} + x^2 + 1$$

$$\text{CRC } UIT = x^{16} + x^{12} + x^5 + 1$$

$$\text{CRC } 32 = x^{32} + x^{28} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + 1$$

El soporte inherente a toda solución de interconectividad se define por la interacción de los recursos siguientes:

- Repetidores (REPEATER).
- Concentradores (HUBS).
- Conmutadores (SWICHT).
- Pasarelas (GATES).
- Puntos de acceso (AP).

A este conjunto de dispositivos, se le suma los recursos básicos de toda arquitectura computacional con los cuales se materializa su operación. El descriptor de interconectividad se observa de manera directa con la ayuda de la figura 1.7.

Para estructurar formalmente el proceso de interconexión o de conectividad entre los nodos que conforman la solución telemática, es posible utilizar el patrón IPV4 o el patrón IPV6 (IPng), con IPV4 se pueden operar las siguientes clases de máquinas, o direcciones formales: Clase A, Clase B, Clase C, Clase D y Clase E, las tres primeras clases son las direcciones globales de interconexión y las dos últimas se consideran direcciones de experimentación (ver figura 1.8), en el escenario IPng, se pueden observar fácilmente las siguientes características:

- Espacio de direcciones ampliado al trabajar 128 Bits, que garantiza un factor direccional de 2, lo que da la posibilidad de tener un espacio de direcciones por metro cuadrado de  $6 \times 10^{23}$  nodos (Davis, 2005).

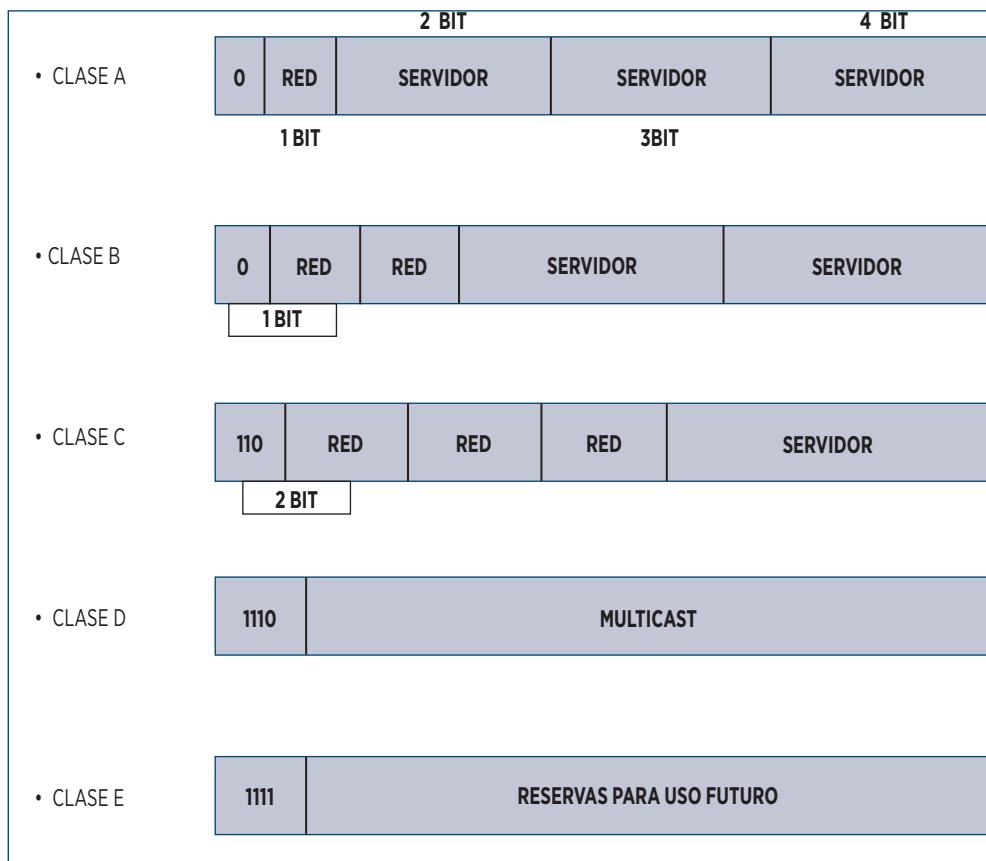


- Flexibilidad Anycast.
- Múltiple tipología de direcciones:  
Unicast (Unidistribución).  
Anycast (Monodistribución).  
Multicast (Multidistribución).
- Estructura compleja a nivel operacional (ver figura 1.7).

Configuración IP de Windows	
Número de host . . . . .	: YolyFernandez-PC
Sufijo DNS principal . . . . .	: 1
Tipo de nodo . . . . .	: híbrido
Enrutamiento IP habilitado . . . . .	: no
Proxy WINS habilitado . . . . .	: no
Adaptador de LAN inalámbrica Conexión de red inalámbrica:	
Sufijo DNS específico para la conexión . . . . .	:
Descripción . . . . .	: Ralink BT2.1in Wireless LAN Card
Dirección física . . . . .	: 74-35-43-10-10-10
DHCP habilitada . . . . .	: si
Configuración automática habilitada . . . . .	: si
Vinculo: dirección IPv6 local . . . . .	: fe80::40fe:7592:221:16d9%12(Preferido)
Dirección IPv4 . . . . .	: 192.168.0.3(Preferido)
Máscara de subred . . . . .	: 255.255.255.0
Concesión obtenida . . . . .	: domingo, 15 de diciembre de 2012 04:47:12 p.m.
La concesión expira . . . . .	: lunes, 16 de diciembre de 2013 04:47:11 p.m.
Porta de enlace predeterminada . . . . .	: 192.168.0.1
Servidores DHCP . . . . .	: 192.168.0.1
UIDB DHCPv6 . . . . .	: 225764575
UIDB de cliente DHCPv6 . . . . .	: 00-01-00-01-17-69-DC-30-F0-0F-41-4-0-14
Servidores DNS . . . . .	: 200.75.51.132 200.75.51.133
NetBIOS sobre TCP/IP . . . . .	: habilitado
Adaptador de Ethernet Conexión de área local:	
Estado de los medios . . . . .	: medios desconectados
Sufijo DNS específico para la conexión . . . . .	:
Descripción . . . . .	: Realtek PCIe GBE Family Controller
Dirección física . . . . .	: FE-0F-41-54-0A-14
DHCP habilitada . . . . .	: si
Configuración automática habilitada . . . . .	: si
Adaptador de Ethernet VMware Network Adapter VMnet8:	
Sufijo DNS específico para la conexión . . . . .	:
Descripción . . . . .	: VMware Virtual Ethernet Adapter for VMnet8
Dirección física . . . . .	: 00-50-56-C8-00-01
DHCP habilitada . . . . .	: no
Configuración automática habilitada . . . . .	: si
Vinculo: dirección IPv6 local . . . . .	: fe80::63:ec2fa:ceaxuz15(Preferido)
Dirección IPv4 . . . . .	: 192.168.91.1(Preferido)
Máscara de subred . . . . .	: 255.255.255.0
Puerta de enlace predeterminada . . . . .	: 192.168.91.1
UIDB DHCPv6 . . . . .	: 570445910
UIDB de cliente DHCPv6 . . . . .	: 00-01-00-01-17-69-DC-30-F0-0F-41-4-0-14
Servidores DNS . . . . .	: fe00::0:ffff::1:1x1 fe00::0:ffff::2:1 fe00::0:ffff::3:1
NetBIOS sobre TCP/IP . . . . .	: habilitado
Adaptador de túnel Isatap.(00149PS4-6C18-4067-000E-000300136190):	
Estado de los medios . . . . .	: medios desconectados
Sufijo DNS específico para la conexión . . . . .	:
Descripción . . . . .	: Adaptador ISATAP de Microsoft #4
Dirección física . . . . .	: 00-00-00-00-00-00-00-E0
DHCP habilitada . . . . .	: no
Configuración automática habilitada . . . . .	: si
Adaptador de túnel Isatap.(000C2641-10D4-4379-B573-20E393FEP720):	
Estado de los medios . . . . .	: medios desconectados
Sufijo DNS específico para la conexión . . . . .	:
Descripción . . . . .	: Adaptador ISATAP de Microsoft #3
Dirección física . . . . .	: 00-00-00-00-00-00-E0
DHCP habilitada . . . . .	: no
Configuración automática habilitada . . . . .	: si
Adaptador de túnel Isatap.(C9H540MF-C10F-4060-A387-18DFB3668906):	
Estado de los medios . . . . .	: medios desconectados
Sufijo DNS específico para la conexión . . . . .	:
Descripción . . . . .	: Adaptador ISATAP de Microsoft #3
Dirección física . . . . .	: 00-00-00-00-00-00-E0
DHCP habilitada . . . . .	: no
Configuración automática habilitada . . . . .	: si
Adaptador de túnel Teredo Tunneling Pseudo-Interface:	
Estado de los medios . . . . .	: medios desconectados
Sufijo DNS específico para la conexión . . . . .	:
Descripción . . . . .	: Teredo Tunneling Pseudo-Interface
Dirección física . . . . .	: 00-00-00-00-00-00-00-20
DHCP habilitada . . . . .	: no
Configuración automática habilitada . . . . .	: si

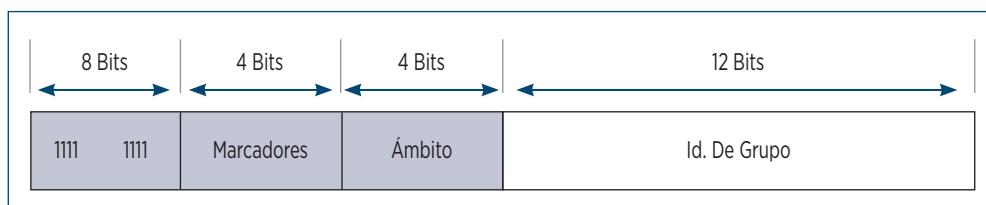
Figura 1.7 Descriptor de interconectividad.

Fuente: Elaborado por el grupo de investigación.



*Figura 1.8* Estructura IPV4

Fuente: Elaborado por el grupo de investigación.



*Figura 1.9* Estructura IPV6.

Fuente: Technet (s.f.).

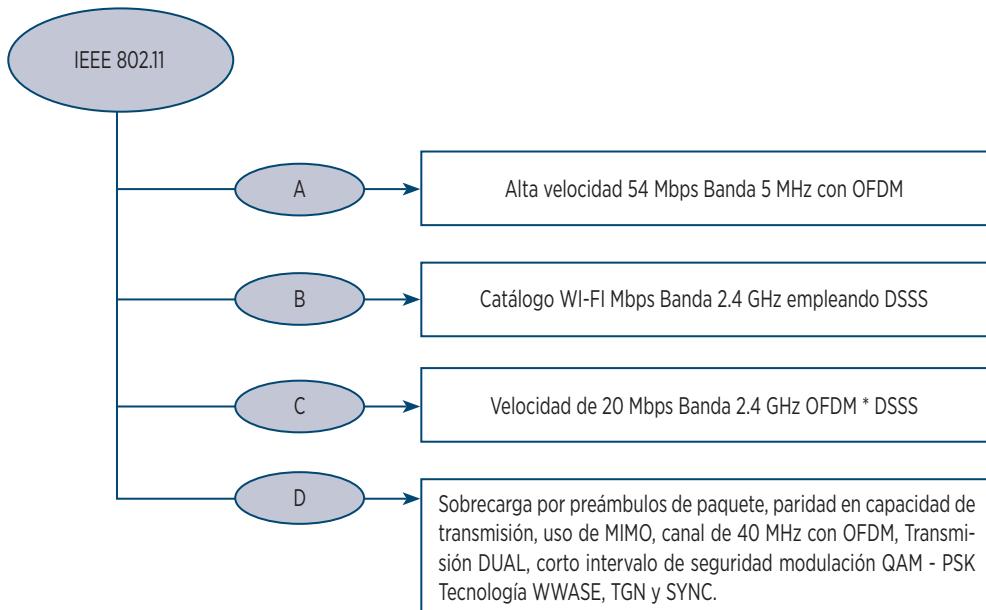


## • 1.6 Modelo IEEE 802.X

Este modelo fue promulgado por la IEEE en febrero de 1980, con el fin de estandarizar el nivel físico, el nivel de enlace y los demás descriptores (Tanembaum, 2008). El nivel de enlace fue subdividido en dos segmentos, el primero se ocupa del control de flujo, la comprobación de errores y la lógica de reenvío, mientras que el segundo controla y arbitra los conflictos de acceso simultáneo. Operacionalmente este modelo cataloga los referentes funcionales a continuación listados:

- IEEE 802.1: Normalización y especificación funcional de interface.
  - IEEE 802.1D: Control del protocolo de expansión de árbol.
  - IEEE 802.1Q: Redes virtuales de área local (VLAN).
  - IEEE 802.1aq: Control de trayectoria y puenteo (SPB: *Shortest Path Bridging*).
- IEEE 802.2: Control de enlace lógico.
- IEEE 802.3: CSMA/CD (ETHERNET).
- IEEE 802.4: Token Bus.
- IEEE 802.5: Token Ring.
- IEEE 802.6: Redes metropolitanas con fibra óptica (MAN/OF).
- IEEE 802.7: Control de banda ancha.
- IEEE 802.8: Funcionalidad con fibra óptica.
- IEEE 802.9: Servicios integrados para redes de área local.
- IEEE 802.10: Seguridad en interconexión IEEE 802.11: redes inalámbricas. (WI-FI).
- IEEE 802.12: Negociación de prioridad por demanda.
- IEEE 802.13: No utilizado.
- IEEE 802.14: Interconexión con módems cableados.
- IEEE 802.15: Redes de interconexión personal BLUETOOTH: WPAN.
- IEEE 802.16: redes inalámbricas de acceso metropolitano (WIMAX).
- IEEE 802.17: Control de conexiones con paquete de anillo.
- IEEE 802.18: Normativa de enlace por radio.
- IEEE 802.19: Patronato técnico de coexistencia.
- IEEE 802.20: Acceso inalámbrico móvil en banda ancha.
- IEEE 802.21: Control de medios independientes (*Media Independent Handover*).
- IEEE 802.22: Redes inalámbricas regionales (WRAN).

Se detalla lo relacionado con el esquema IEEE 802.11, el cual se realiza mediante la figura 1.10.



**Figura 1.10** Esquema operacional IEEE 802.11.

Fuente: Elaborado por el grupo de investigación.

En esta figura se señalan las características de cada uno de los niveles que lo integran, catalogando operacionalmente sus características de referencia, a saber:

Operación e implementación de la modulación OFDM, que permite enviar los valores informáticos utilizando la QAM o la PSK como técnicas de modulación y trabajando un número de señales portadoras entre 48 y 52, garantizando el empleo de factores de carga útil parametrizados a nivel de 1/2, 3/4 y 5/6.

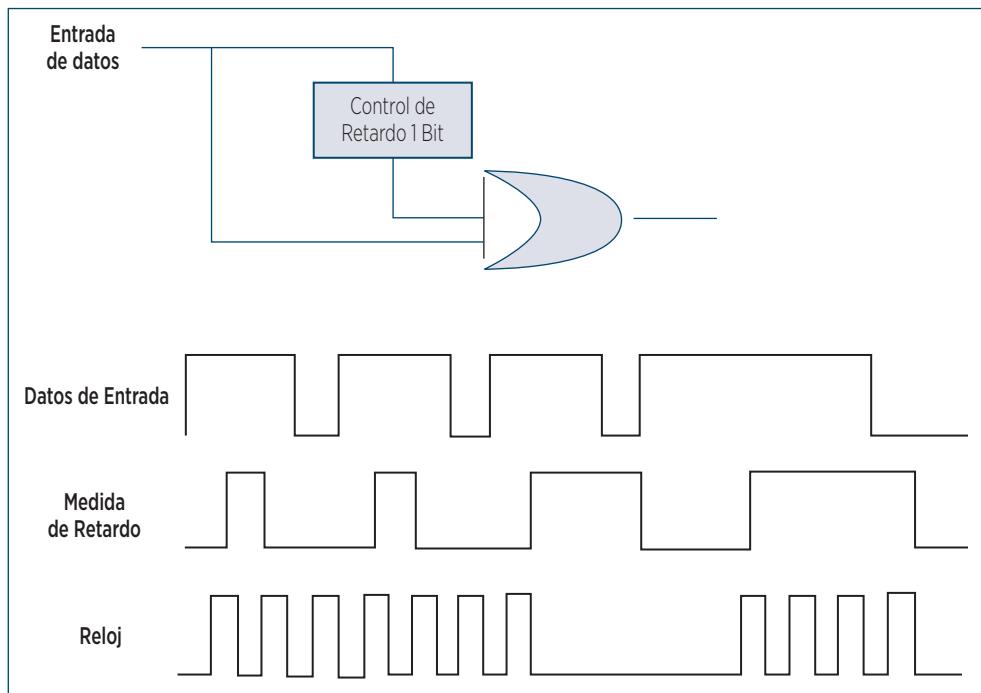
Categorización de la tecnología MIMO (*Múltiple Input Múltiple Output*), con la que se pueden transmitir hasta cuatro flujos de datos en paralelo sobre un mismo canal, utilizando las reflexiones de las ondas y sus características de distribución espacial, que permiten el envío de varias señales



simultaneas sobre un mismo medio, operando con velocidades superiores a 130 Mbps.

- Control de servicios especializados y supervisión directa sobre la capa física y capa de enlace para operar diferentes técnicas de transmisión, tales como:
  - Infrarrojo.
  - Salto de frecuencias de espectro expandido (FHSS).
  - Espectro Expandido con secuencia directa (DSSS).
  - Multiplexación por división ortogonal de frecuencia (OFDM).
  - Alta velocidad sobre espectro expandido (HRDSSS).
- Control de celdas mediante los puntos de acceso de la estación básica (BSS-AP).
- Utilización de canales físicos y canales virtuales por implementación del protocolo CSMA-CA (*Carrier Sense Multiple Access with Collision Avoidance*).
- Direccionalamiento especializado para detección de canal virtual, mediante la implementación del protocolo MACAW (*Multiple Access with Collision Avoidance for Wireless*).
- Difusión desde la estación base de tramas de sondeo que permiten mantener activo el diálogo formal, catalogando o implementando su funcionalidad en diferentes intervalos tales como:
  - IFS: *Short Inter Frame Spacing* (determina la no participación de la estación base en el proceso de control transaccional).
  - PIFS: *PCF Inter Frame Spacing* (la estación base puede enviar una trama de sondeo).
  - DIFS: *DCF Inter Frame Spacing* (cualquier estación intenta adquirir el control del canal y enviar una nueva trama).
  - EIFS: *Extended Inter Frame Spacing* (la estación que recibe una trama errónea reporta esta causa).
- Operación de los servicios de distribución (asociación, disoacción, re-asociación, enrutamiento e integración) y de los servicios de estación (autenticación, desautenticación y entrega de datos).

Con las características anteriormente citadas, debe entenderse que con la normatividad IEEE 802.11n se asegura la minimización en el proceso de ajuste de retraso del reloj, hecho que optimiza totalmente el nivel de operación en el entorno de las redes MESH, que constituye el núcleo de este proyecto, tal como se observa en la figura 1.11.

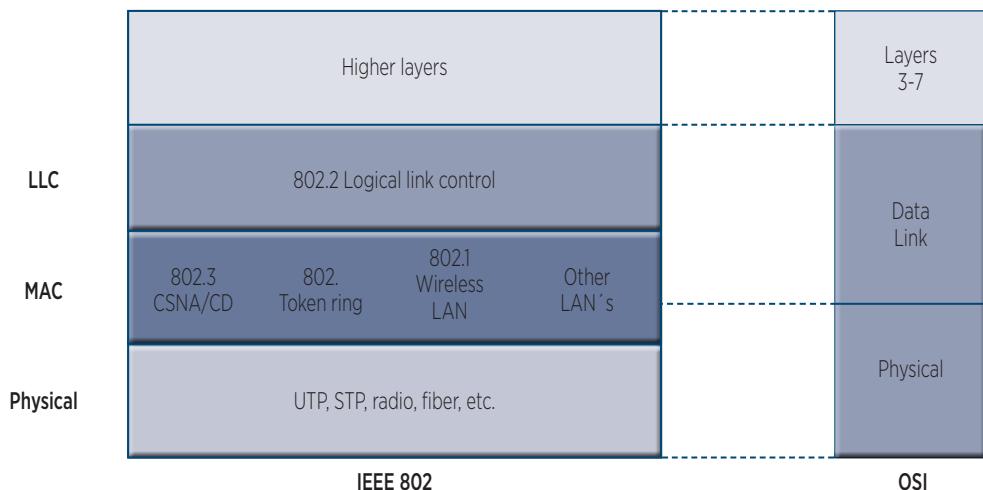


*Figura 1.11 Proceso de ajuste de reloj.*

*Fuente:* Elaborado por el grupo de investigación.

## • 1.7 Estándar IEEE 802.11

El protocolo IEEE 802.11 es un estándar de comunicaciones de la IEEE y se define como de los más bajos de arquitectura OSI (capa física y enlaces de datos), en el cual se especifican las normas de funcionamiento en una red WLAN. Esto se observa en la Figura 1.12, donde la capa física se divide en dos subcapas que se examinarán más adelante.



*Figura 1.12 Estructura del proyecto IEEE 802.*

Fuente: Bibling (s.f.a).

**LLC (Logical Link Control):** se encarga del envío de datos por medio físico, también es responsable del control de errores, el control de flujo y es el encargado de dar un direccionamiento a la subcapa MAC.

**PMD (Physical Medium Dependence):** es la que crea la interfaz y controla la comunicación hacia la capa MAC, a través del SAP: *Service Access Point*.

Estos estándares se utilizan en algunas redes MESH, ya que depende del fabricante quien tiene sus propios mecanismos para generar redes en malla. Además, este estándar define cuántos nodos van a participar en la arquitectura, la nueva funcionalidad de la capa MAC que permite tener un mayor control del acceso al canal. Este estándar ha encontrado una gran acogida desde que se aprobó la normal 802.11b en el año 1999. A continuación, se describen los diferentes componentes de la normal IEEE 802.11

### 1.7.1 Estándar 802.X

Los estándares 802.1X se crearon para contrarrestar la inseguridad y este específicamente, se desarrolló en el año de 1997 como un mecanismo diseñado para proporcionar un acceso controlado entre diferentes dispositivos



como: dispositivos inalámbricos clientes, puntos de acceso y servidores. Estos emplean unas llaves dinámicas y no estáticas que son usadas para que la autenticación se pueda conectar mediante protocolo de autenticación de reconocimiento. Para tener una conexión es necesario tener un servidor que proporcione los servicios necesarios para la autenticación de usuarios entrantes (RADIUS<sup>1</sup>, servicio de autenticación de usuarios remotos entrantes). Dentro de sus características se encuentra que:

- El comité de 802 de la IEEE se concentró en la interfaz física, de manera que relaciona los niveles físicos y de enlace de datos, tomando el modelo de referencia OSI de la ISO.
- Los productos que siguen la normal 802 incluyen otra característica que es la interfaz red *bridges*, estos son usados para crear redes LAN's de par trenzado y cable coaxial.
- Tiene dos subniveles, los cuales son MAC y LLC.
- Las subcapas son compatibles con las subcapas.

Las especificaciones para estándares 802 son:

- Tarjetas de red (NIC<sup>2</sup>).
- Componentes de las redes inalámbricas.
- Componentes que utilizan cables par trenzado y coaxial.
- Especificaciones de tarjetas de red que accedan y transfieran datos.

Por su parte, se encuentran las categorías del estándar IEEE 802.X:

### Protocolo IEEE.802.1 (Protocolos superiores LAN)

Es una norma de control que permite ver la correspondencia entre las partes de un documento y cuál es la relación con la gestión de redes. Permite la autenticación de los dispositivos para que se conecten a los puertos de la red, estableciendo así una conexión punto a punto y previendo

<sup>1</sup> Es un servidor de directivas de red (NPS), se puede usar como un servidor de autenticaciones remotas para telefonía de usuarios. Pueden ser servidores de acceso telefónico, puntos de acceso inalámbrico o proxy RADIUS” (Technet, 2015).

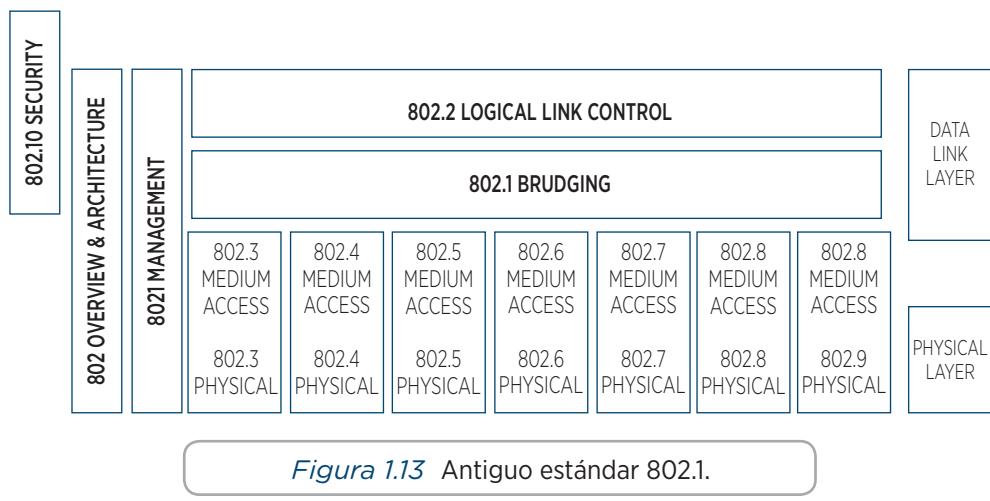
<sup>2</sup> Es un registro de nombres de dominio e información asociada a los registros de dominios superiores y sistema de dominios de internet (DNS). lo que permite tener un control administrativo de un nombre de dominio” .



un acceso al puerto si falla la autenticación. Este se utiliza, sobretodo, en algunos puntos de acceso inalámbrico cerrado y se basa en protocolos para la autenticación.

### Protocolo IEEE 802.2 (Control de enlace lógico)

Este estándar hace parte de la familia de estándares para la red LAN y MAN. La relación entre otros estándares y otras familias se observa en la Figura 1.13.



Fuente: Tanebaum (2003).

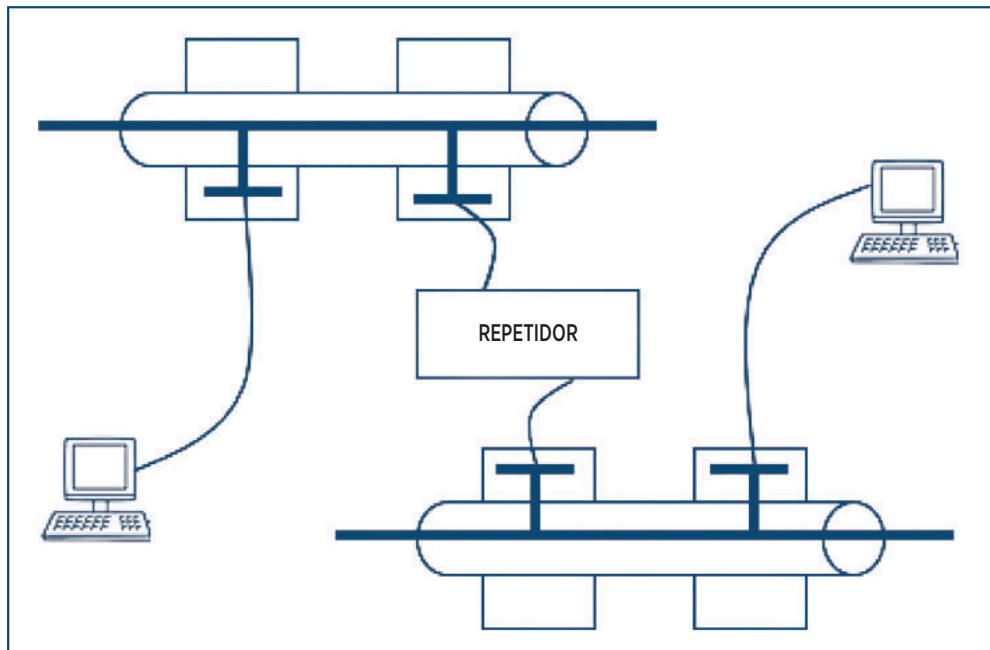
Este estándar define los métodos para el control de tareas de interacción entre tarjetas de red y el procesador (la capa de nivel 2 y 3 del modelo OSI) llamado LLC, asegura que la trasmisión de datos sea fiable a través de un enlace de comunicaciones LLC.

### Protocolo IEEE 802.3 (Ethernet)

Este protocolo se diseñó para que no se pudiera transmitir más de una información a la vez, con el fin de que no haya pérdida de información, lo cual se controla a través de un sistema CSMA/CD<sup>3</sup> (*Carrier Sense Multiple Access with Collision Detection*), Detección de portadora con acceso múltiple

<sup>3</sup> Protocolo de acceso al medio compartido, incorpora dos mejoras que aumentan el rendimiento. Su uso está extendido a redes Ethernet (Eecs.yorku, 2015).

y detección de colisiones). El principio del funcionamiento consiste en que una estación debe trasmisir y detectar la presencia de una señal portadora y, si existe, éste comienza la trasmisión. En la Figura 1.14. se representa la conexión del protocolo.

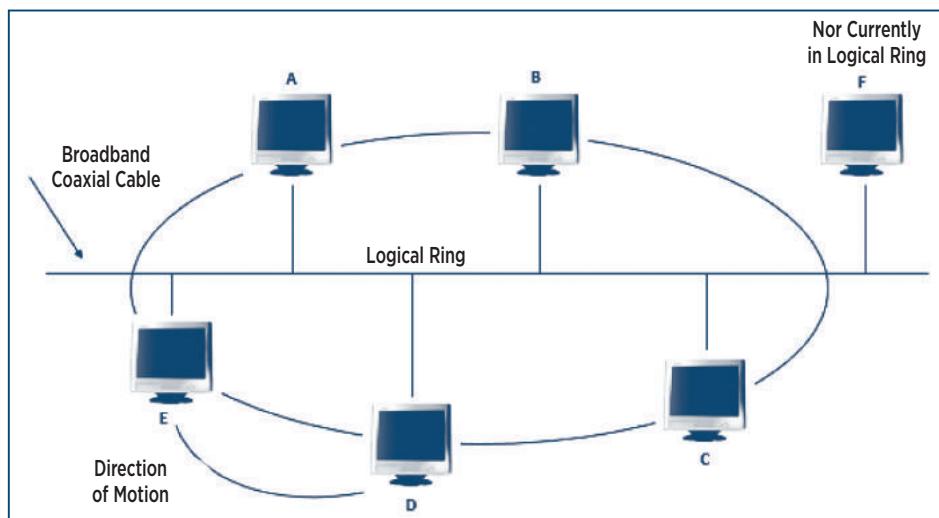


*Figura 1.14 Conexión con protocolo IEEE 802.3 Ethernet.*

*Fuente:* Colmenares (2008).

### Protocolo IEEE 802.4 (Token Bus)

El estándar para Token Bus de paso para redes LAN, brinda un único protocolo de acceso a medios para un uso con capas físicas múltiples. La representación es en forma de anillo lógico y de trasmisión por turno, el cual está implementado en forma de bus previendo cualquier ruptura del anillo que podría hacer que la red quede completamente desactivada. En la Figura 1.15 se contempla cómo funciona la dirección del Token.

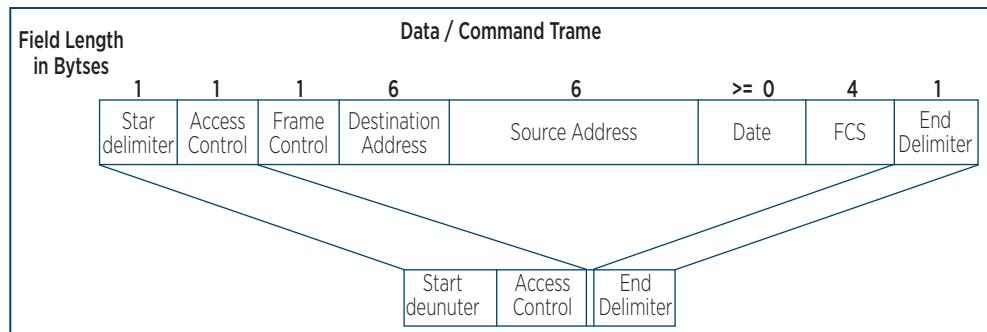


*Figura 1.15* Dirección que toma Token, estándar IEEE 802.4.

Fuente: Kharagpur (s.f.).

### Protocolo IEEE 802.5 (Token Ring)

Se define como una red con topología de anillo, el cual usa un token para la transmisión de información de un punto a otro. En las estaciones de trabajo se envía un mensaje dentro de un token y lo direcciona específicamente a un destino, la estación a la cual le llega este mensaje lo copia y lo envía a otro token, de regreso a la estación del cual fue enviado, esta borra el mensaje y pasa el token a la siguiente estación. En la Figura 1.16. se interpreta el estándar.



*Figura 1.16* IEEE 802.5 formato de Token Ring.

Fuente: Open Net (s.f.).



## Protocolo IEEE 802.6 (Red MAN)

Este estándar se realizó básicamente para las redes metropolitanas, ya que combina las ventajas de redes LAN y WAN, proporcionando los servicios de canalizar voz y video, digitalizándolos. Este protocolo fue abandonado ya que no es muy efectivo conectar varias estaciones de trabajo. Se ha reemplazado por otros protocolos de Ethernet (MPLS *Multi Protocol Label Switching*<sup>4</sup>).

## IEEE 802.7 (Asesoría técnica sobre banda ancha)

Este es un estándar para redes LAN que usan cable coaxial o par trenzado y fue desarrollado para las compañías que prestaban servicios de internet de banda ancha.

## IEEE 802.8 (Asesoría sobre fibra óptica)

Este es un estándar LAN de fibra óptica al igual que los anteriores estándares; el cual también es usado para el paso de token. En la actualidad este estándar se disolvió.

## IEEE 802.11a

Este estándar tiene la misma base del IEEE 802.11, el cual se caracteriza por la banda que opera de 5Ghz (ya que presenta menos interferencia con dispositivos electrónicos) y tiene una transmisión de velocidad hasta de 54Mbps. Esto hace que se trate un estándar práctico para redes inalámbricas que tengan velocidades reales aproximadas de 20Mbps.

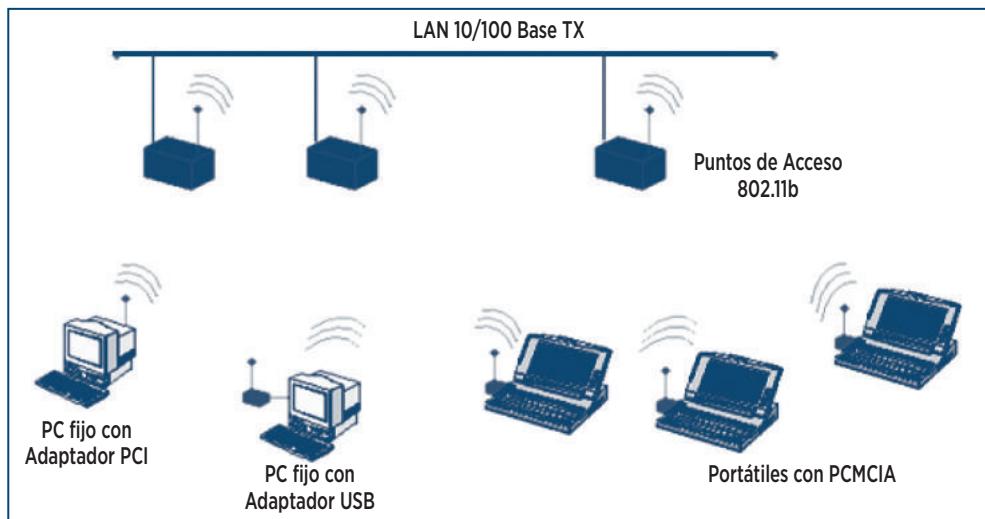
Tiene 12 canales no solapados, divididos en 4 para conexiones punto a punto y 8 para redes inalámbricas. Aunque tiene una desventaja, ya que restringe el uso de los equipos 802.11a a únicamente puntos en línea de vista, lo cual hace que sea necesaria la instalación de más número de accesos.

---

<sup>4</sup> Un mecanismo de trasporte creado por la IETF, este opera entre capas de datos y capas de red del modelo OSI, Tapasco García Martha, MPLS, (Pereira, 2008).

## IEEE 802.11b

A diferencia del estar IEEE 802.11<sup>a</sup>, este tiene una velocidad máxima de 11 Mbps y una operación de 2.4Ghz, así como la misma interferencia que se podía ver en la IEEE 802.11. La ventaja de este estándar es que no se necesita tener una licencia. En la Figura 1.17 se manifiesta la disposición de los equipos con esta norma.



*Figura 1.17* Disposición de los equipos bajo la norma 802.11b.

Fuente: Universidad Tecnológica de Pereira (2008).

## IEEE 802.11g

Este estándar ofrece una velocidad máxima de 54 Mbps para la trasferencia de datos y utiliza una banda ISM (*Industrial Scientific and Medical*). Opera con un espectro de 2.4Ghz sin tener licencia, tiene compatibilidad con el estándar 802.11b, aunque la presencia de estos nodos hace que se reduzca significativamente la velocidad de transmisión.

## • 1.8 Comparaciones de estándares IEEE 802

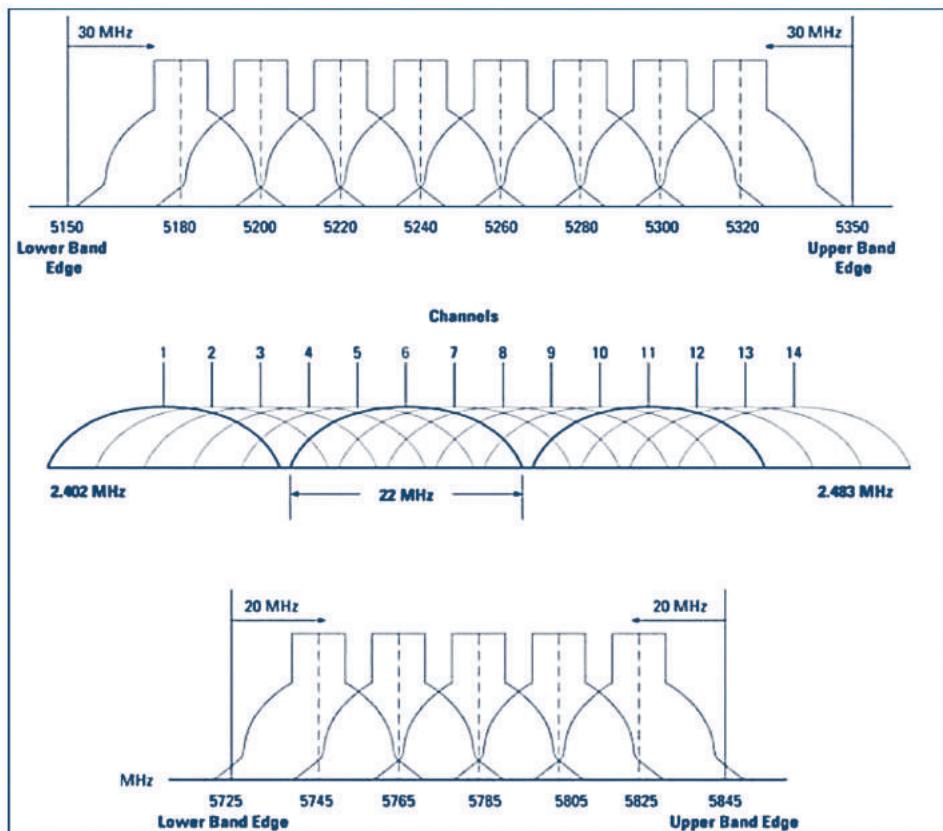
La comparación se realiza entre los estándares IEEE 802.11b y IEEE 802.11g, la cual se puede observar en la Tabla 1.2.

**Tabla 1.1** Características y desventajas de estándares IEEE 802.11 b e IEEE 802.11 g.

Operación de banda de los 2.4 GHz
Señal de transmisión aproximada de 30 MHz
Mismo problema de asignación de canales donde se cubre una alta densidad de usuarios.
Interferencia en RF de aparatos que usan banda 2.4GHz

Fuente: Genarro (2003).

En la Figura 1.18 se puede apreciar la distribución de las normas 802.11b y 802.11 g, donde se observa que la señal tiene un alcance real entre 20 y 30 MHz. La señal se distribuye en cada uno.



**Figura 1.18** Distribución de canales normas IEEE 802.11b e IEEE 802.11g.

Fuente: Univers-spb. (s.f.).



## Comparación 802.11 g y 802.11a

La diferencia que tienen estas dos bandas es que la 802.11g opera con una banda de 5GHz con 12 canales y se pueden tener los canales en una misma área sin que haya alguna interferencia entre cada uno. Esto hace que se facilite la asignación de los canales y que se incremente el rendimiento de la red.

A diferencia del estándar 802.11g, el 802.11a tiene una banda 54Mpps que emplea frecuencias más bajas que las normas mencionadas (802.11b y 802.11g).

## IEEE 802.15 (WPAN)

Este estándar se definió para redes de cortas distancias, como las redes Bluetooth ZigBee, de manera que permite que dispositivos inalámbricos como smartphones, portátiles, computadores personales, etc., puedan comunicarse entre sí. Ya que el Bluetooth no es compatible con redes inalámbricas de estándar 802.11x, se desarrolló este estándar para que hubiera una interoperabilidad en las redes.

## IEEE 802.16 (Acceso inalámbrico de banda ancha WiMAX, acceso inalámbrico desde casa)

Este estándar se desarrolló básicamente para banda ancha fija de redes inalámbricas de acceso metropolitano, en el año de 1999. Se comercializó con el nombre de Wimax (*World Wide Interoperability*), el cual promueve la interoperabilidad entre productos basados en estándares IEEE 802.16. En la Figura 1.19 se explica la estructura de las capas del estándar.

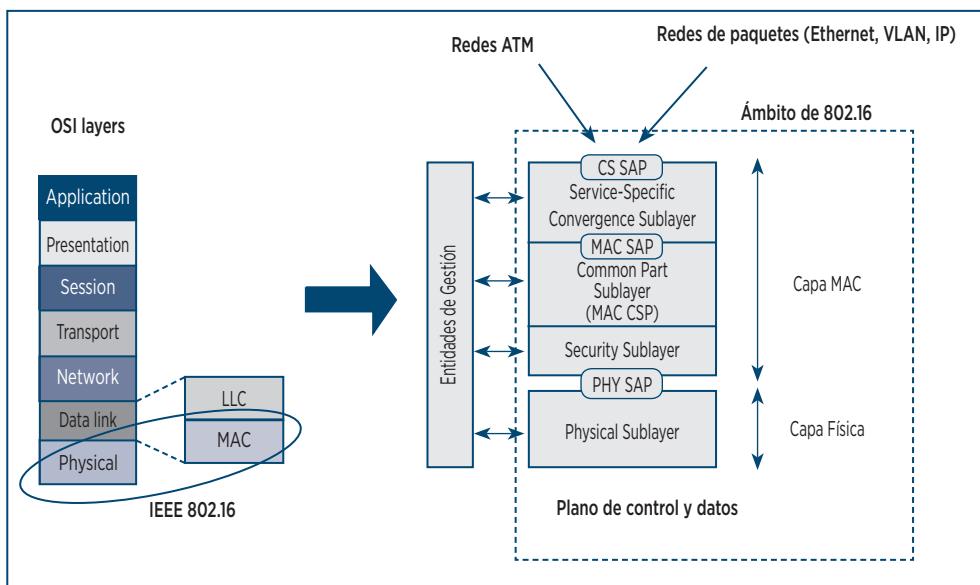


Figura 1.19 Estructura de capas de la norma IEEE 802.16.

Fuente: CCM (2016).

### IEEE 802.17 (Paquetes de anillos resistentes)

Este estándar fue diseñado para un óptimo trasporte de datos en las redes anillo de fibra óptica, proporcionando una transmisión basada en paquetes, con lo cual se incrementa la eficiencia del Ethernet y servicios IP.

### IEEE 802.18 (Grupo asesoría técnica, normativas de radio)

Este estándar se está empezando a desarrollar por RR-TAG (*Radio Regulatory Advisory Group*, en español Grupo asesor técnico de regulación de Radio)<sup>5</sup>, el cual también tiene a cargo otros estándares.

<sup>5</sup> Este grupo asesor apoya el trabajo de la IEEE 802 LMSC, la IEEE 802 Grupo inalámbrico de trabajo IEEE 802.11 (WLAN), WLAN), IEEE 802.15 (WPAN), IEEE 802.16 (WMAN), IEEE 802.20 (Movilidad inalámbrica), IEEE 802.21 (Traspaso / Interoperabilidad entre redes), y IEEE 802.22 (WRAN)-mediante el control y la participación en la radio de asuntos regulatorios en todo el mundo, como defensora de IEEE 802 activamente.



## IEEE 802.19 (Grupo técnico asesor para coexistencia inalámbrica)

Este estándar se encarga de la coexistencia entre las diferentes redes inalámbricas que no tienen una licencia, ya que muchos estándares de la IEEE 802 usan espectro sin una licencia, razón por la cual se vio la necesidad de empezar la coexistencia entre ellos. Los dispositivos sin licencia alguna pueden funcionar en la misma banda sin licencia dentro del mismo rango, pero esto puede ocasionar una interferencia entre las dos redes.

## IEEE 802.20 (Acceso inalámbrico de banda ancha móvil)

Este estándar es una especificación para las redes con acceso a internet móvil, publicado en el año 2008. Se especificó de acuerdo a una arquitectura por capas, ya que otros estándares de la IEEE 802 también trabajan con arquitectura por capas, como la capa física, control de acceso al medio y el enlace lógico.

## IEEE 802.21 (Interoperabilidad independiente del medio)

Este estándar fue publicado en el año 2008, define componentes independientes del método de acceso el cual permite optimizar el handover<sup>6</sup>, ya sea entre redes de estándar IEEE 802, redes del mismo tipo o redes móviles.

## IEEE 802.22 (Red inalámbrica regional)

Este estándar se creó para redes WRAN (*Wireless Regional Área Network*) el cual utiliza espacios en blanco en su espectro de frecuencia, en el momento de la transmisión de los canales de TV. Este desarrollo se enfocó hacia las técnicas de radio cognitiva, permitiendo que el espectro geográfico no utilizado que se asigna a un servicio de difusión de televisión, pueda ser de uso compartido. El objetivo es poder utilizar el espectro de frecuencia para ofrecer acceso de banda ancha a zonas que no estén al alcance de este servicio, como ambientes rurales, zonas de baja densidad de población, etc.

---

<sup>6</sup> Handover se refiere al sistema que se utiliza en las comunicaciones móviles celulares, este tiene como objetivo trasferir el servicio de un punto a otro cuando la calidad del enlace no es suficiente entre cada estación, con lo cual se garantiza la realización de un servicio cuando un móvil cambia de sitio.



## • 1.9 Redes MESH

El concepto de mayor aceptación en el escenario tecnológico y computacional dice que la tecnología MESH es la más interesante en el campo de las tecnologías emergentes que cobijan las redes inalámbricas, dado que el conjunto de nodos sobre los que operan la malla de conexión proporciona una amplia cobertura, balanceando la carga de tráfico y garantizando total tolerancia ante la presencia de fallos. Para el grupo realizador, una red MESH es la entidad telemática configurada de manera sencilla a nivel nodal, que permite interactuar a costo mínimo con los procesos de intercambio de valores transaccionales dentro de amplias coberturas, puesto que la medida de consumo eléctrico no supera los 2.5 W y por ende, la tarificación es más económica que cualquier red inalámbrica convencional.

Esta solución telemática se caracteriza por que para habilitar su funcionamiento, no se requiere contar con algún programa de control en los diferentes computadores, pues la administración y control se puede realizar a través del empleo de la red internacional o Internet.

La solución MESH que se proyecta en este libro, se caracteriza por facilitar la configuración automática y en forma dinámica de los diferentes nodos, es decir, la auto-formación y auto-restructuración son sus principales factores diferenciadores. Se listan a continuación los componentes o atributos que evidenciarán la solución a liberar y a experimentar operacionalmente en el área de prueba seleccionada, por el programa de Ingeniería de Sistemas (Holland, 2012):

**Uso comunitario:** la comunidad o estrato social señalado se apropiá de la red para compartir sus servicios, por ende, su propiedad se comparte.

**Formación automática:** la red inalámbrica MESH, se define y configura de manera directa tan pronto los nodos que la integran se configuran y activan.

**Redirecciónamiento dinámico:** Si falla algún nodo, la red corrige el error seleccionando de manera automática la ruta óptima disponible.



**Activación instantánea:** cuando un nodo falla y se retira del enlace telemático, tan pronto se restaura la red se apropia nuevamente de él.

**Normativa operacional de implementación:** las soluciones MESH son normatizadas y reguladas por los estándares WI-FI de la IEEE 802.11 a/b/g, su operación está basada en el convencional nodo *adhoc*, es decir cada nodo de la WMN\_Libre, garantiza el poseer el mismo número y nombre, definidos paramétricamente por ESSID<sup>7</sup> y BSSID<sup>8</sup>.

**Empleo homogéneo de canal:** en la solución WMN\_Libre proyectada todos los nodos trabajarán con la misma frecuencia o canal, facilitando entonces la vista de, por lo menos, dos nodos simultáneos y el control eficiente de la distribución de tráfico, al mantener las tablas de enrutamiento en forma dinámica.

**Conectividad supervisada:** la solución, determinará y garantizará la selección de las unidades de conexión, es decir, evitará que dispositivos inalámbricos desconocidos, o no direccionados, básicamente se conecten.

**Implementación por control funcional:** todo nodo de la red tendrá una dirección IP única y poseerá parámetros estructurales de conectividad para facilitar su enlace inalámbrico o su enlace convencional.

**Ajuste normativo legal:** la solución a construir será regulada por las normativas específicas existentes para el empleo de la banda de 2.4 GHz y 5.8 GHz

**Valoración funcional:** la infraestructura de interconectividad proyectada para el proyecto, se considera los efectos generadores de entropía para la conectividad tales como: los árboles, los materiales de construcción, las fuentes de interferencia WI-FI y también han considerado como elemento preponderante de protección, las unidades que demanda la acción dañina de los rayos eléctricos sobre los equipos WI-FI.

---

<sup>7</sup> ESSID Significa Extended Service Set ID y es el nombre identificable de la red.

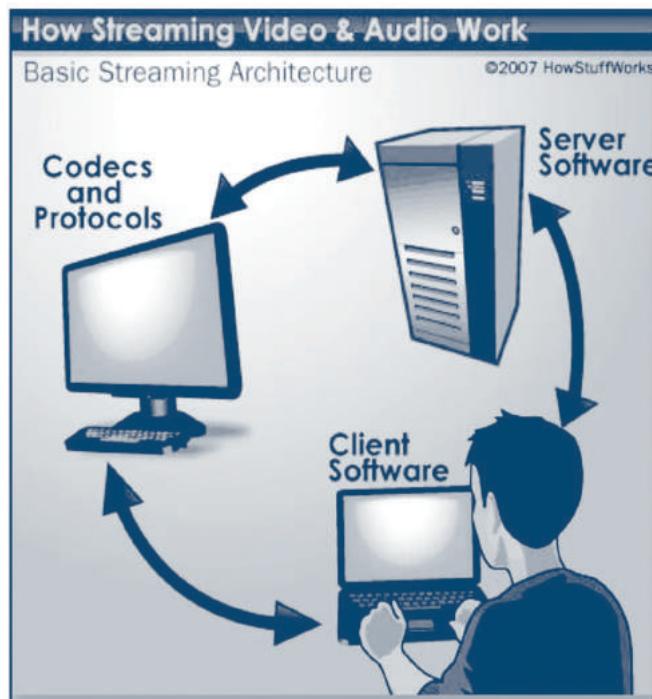
<sup>8</sup> BSSID: Significa Basic Service Set Identifier y se trata de la dirección MAC (física) del Access Point al que nos conectamos.

**Nodos:** es un componente que forma parte de una red. En otras palabras, tanto si se trata de Internet como de Intranet (utilizada en ámbitos cerrados, con acceso limitado a los usuarios autorizados), cada servidor u ordenador constituye un nodo y se encuentra conectado a otro u otros nodos.

**Streaming:** se utiliza para optimizar la descarga y reproducción de archivos de audio y video, los cuales suelen tener un cierto peso.

El Streaming funciona con la posibilidad de distribución de transmisiones de audio y vídeo en directo:

**Conexión con el servidor:** El reproductor cliente conecta con el servidor remoto y éste comienza a enviarle el archivo (véase figura 1.20).



*Figura 1.20 Estructura Servicio de Streaming.*

*Fuente: Howstuffworks(s.f.).*

**Buffer:** el cliente comienza a recibir el fichero y construye un buffer o almacén donde empieza a guardarlo.



**Inicio de la reproducción:** cuando el buffer se ha llenado con una pequeña fracción inicial del archivo original, el reproductor cliente comienza a mostrarlo, mientras continúa en segundo plano con el resto de la descarga.

**Codificadores, decodificadores y protocolos:** para la transmisión de contenido es necesario que esta sea convertida o codificada, es decir traducida a un lenguaje en la que el servidor la entienda para hacer efectiva su emisión. Para esto es necesario el uso de *Codecs* y protocolos, los cuales se encargan de codificar y decodificar el contenido durante el proceso de transmisión.

**Caídas de la velocidad de conexión:** si la conexión experimenta ligeros descensos de velocidad durante la reproducción, el cliente podría seguir mostrando el contenido, consumiendo la información almacenada en el buffer. Si llega a consumir todo el buffer, éste se detendría hasta que se volviera a llenar.

Existen dos tipos de Streaming según la tecnología que se use en el servidor:

**Descarga progresiva:** se ejecuta en servidores web que contengan *Internet Information Server* (IIS), Apache, entre otros. Cuando el cliente solicita el archivo de video o de audio, el servidor es el encargado de liberar este archivo, utilizando el protocolo HTTP. Es importante tener en cuenta que si el archivo se ha hecho para Streaming, simultáneamente al ser leído por el reproductor del solicitante se iniciará la reproducción, en el momento que se llene el buffer.

**Transmisión por secuencias:** se ejecuta en servidores multimedia que tengan instalado un software especializado, que se encargue de gestionar el Streaming de audio y video.

Las ventajas de un servidor multimedia frente a un servidor web son:

- Mayor rapidez en la visualización de este tipo de contenidos.
- La comunicación entre servidor/cliente se puede realizar por protocolos alternativos al HTTP. Tiene el inconveniente del bloqueo impuesto por Firewalls, pero tiene la ventaja de una mayor rapidez.



- Mejor gestión del procesador y ancho de banda de la máquina del servidor ante peticiones simultáneas de varios clientes del mismo archivo de audio o vídeo.
- Control predefinido sobre la descarga que pueden realizar los clientes.
- Autenticado, filtrado por IP, sin almacenarlo en la caché del cliente, etc.
- Mayor garantía de una reproducción ininterrumpida, gracias al establecimiento de una conexión de control inteligente entre servidor y cliente.

Icecast es un servidor de streaming de medios que actualmente soporta Ogg (Vorbis y Theora), Opus, WebM y audio MP3 (Xiph.org, 2014-2016). Se puede utilizar para crear una estación de radio por Internet o una máquina de discos corriendo en privado, entre otras muchas cosas en medio. Es muy versátil en cuanto a que los nuevos formatos se pueden añadir con relativa facilidad y es compatible con los estándares abiertos para la comunicación y la interacción. Se distribuye bajo la licencia GPL de GNU, versión 2.

El archivo de configuración del Icecast es donde se pueden configurar todas las características propias del servicio. El desarrollador recomienda que no se efectúe ningún cambio en este archivo xml, a menos de que se tenga conocimiento del mismo Fuente especificada no válida. El archivo está dividido de la siguiente manera:

**Límites:** esta sección contiene ajustes de nivel de servidor que, en general, no necesitan ser cambiadas. Sólo se debe modificar esta sección si se tiene pleno conocimiento de lo que se está haciendo (véase figura 1.21).

```
<limits>
    <clients>100</clients>
    <sources>2</sources>
    <queue-size>102400</queue-size>
    <client-timeout>30</client-timeout>
    <header-timeout>15</header-timeout>
    <source-timeout>10</source-timeout>
    <burst-on-connect>1</burst-on-connect>
    <burst-size>65536</burst-size>
</limits>
```

*Figura 1.21 Etiqueta límites.*

Fuente: Icecast (2011).



**Clients:** número total de clientes simultáneos admitidos por el servidor. Los oyentes son considerados clientes, pero también lo son los accesos del contenido estático (es decir, el contenido del servidor de archivos) y también alguna petición para recopilar estadísticas. Éstas son conexiones simultáneas máximas para todo el servidor (no por el punto de montaje).

**Sources:** número máximo de fuentes conectadas admitidas por el servidor. Esto incluye relés activos y clientes de origen.

**QueueSize:** Este es el tamaño máximo (en bytes) de la cola de Streaming. Un oyente puede retrasarse temporalmente debido a la congestión de la red y en este caso, una cola interna se mantiene para los oyentes. Si la cola se hace más grande que este valor de configuración, entonces es truncado y cualquier detector encontrado será retirado del Streaming. Este será el escenario del Streaming que es 512k menos para que se anule por defecto. Se puede anular esta configuración en un montaje individual, que puede ser útil si se tiene una mezcla de alto ancho de banda, y de vídeo y audio de bitrate bajo.

**Clients-timeout:** esta función está deshabilitada.

**Header-timeout:** el tiempo máximo (en segundos) de espera de una solicitud para entrar, una vez que el cliente ha hecho una conexión con el servidor. En general no debería ser ajustado este valor.

**Source-timeout:** si una fuente conectada no envía datos dentro de este período de tiempo de espera (en segundos), entonces la conexión de origen se elimina del servidor.

**Burst-on-connect:** este ajuste es en realidad, un alias para tamaño de ráfaga de datos. Cuando está habilitado el tamaño de ráfaga es de 64 Kbytes y deshabilitado, es de 0 kbytes. Esta opción está en desuso; utilizar el tamaño de ráfaga en su lugar.

**Burst-size:** el tamaño de ráfaga es la cantidad de datos (en bytes) para enviar a un cliente en el tiempo de conexión. Burs-on-size, es para llenar rápidamente el pre-buffer utilizado por los reproductores multimedia. El valor por defecto es de 64 Kbytes, que es un tamaño típico utilizado por



la mayoría de los clientes, por lo que el cambio no suele ser necesario. Este ajuste se aplica a todos los puntos de montaje, a menos que se reemplace en la configuración de montaje. Se debe asegurar que este valor sea menor que la QueueSize, si es necesario aumenta el tamaño de las colas para ser más grande que el tamaño de ráfaga deseado. El no hacerlo podría resultar en intentos de conexión de cliente abortados, debido a que la transmisión inicial que conduce a la conexión ya excede el límite de la cola.

**Autenticación:** esta sección contiene todos los nombres de usuario y las contraseñas utilizadas para fines de administración o para conectar fuentes y relés (véase figura 1.22).

```
<authentication>
    <source-password>hackme</source-password>
    <relay-user>relay</relay-user>
    <relay-password>hackme</relay-password>
    <admin-user>admin</admin-user>
    <admin-password>hackme</admin-password>
</authentication>
```

Figura 1.22 Etiqueta de autenticación.

Fuente: Icecast (2011).

**Source-password:** es la contraseña sin cifrar utilizada por fuentes para conectarse a Icecast. El nombre de usuario por defecto para todas las conexiones de origen es “source”, pero esta opción permite especificar una contraseña por defecto. Nombre de usuario y contraseña se pueden cambiar en el montaje individual.

**Relay-user:** se utiliza en el servidor maestro como parte de la autenticación cuando un dispositivo esclavo solicita la lista de flujos de relé. El nombre de usuario por defecto es *relay*.

**Relay-password:** se utiliza en el servidor maestro como parte de la autenticación, cuando un dispositivo esclavo solicita la lista de flujos de relay.



**Admin-user / admin-password:** el nombre de usuario / contraseña que se utiliza para todas las funciones de administración. Esto incluye la recuperación de las estadísticas, el acceso a las pantallas de administración basadas en la web, etc. Una lista de estas funciones se puede encontrar en la sección “Administrator” del manual.

**Stream Directory Settings:** esta sección contiene todos los ajustes para la inclusión de un streaming en cualquiera de los servidores de directorio Icecast YP. Múltiples ocurrencias de esta sección se pueden especificar con el fin de ser incluido en varios servidores de directorio (véase figura 1.23).

```
<directory>
    <yp-url-timeout>15</yp-url-timeout>
    <yp-url>http://dir.xiph.org/cgi-bin/yp-cgi</yp-url>
</directory>
```

Figura 1.23 Etiqueta Directorio.

Fuente: Icecast (2011).

**Yp-url-timeout:** este valor es el tiempo máximo que Icecast esperará una respuesta de un servidor de directorio en particular. El valor recomendado debería ser suficiente para la mayoría de los servidores de directorio.

**Yp-url:** es la URL que Icecast utiliza para comunicarse con el servidor de directorio. El valor de esta opción es proporcionado por el propietario del servidor de directorios.

**Misc Server Settings:** esta sección contiene la información referente a Icecast y sus configuraciones predefinidas de ubicación, administración, versión, etc. (véase figura 1.24.).

```
<hostname>localhost</hostname>
<location>earth</location>
<admin>icemaster@localhost</admin>
<fileserve>1</fileserve>
<server-id>icecast 2.3</server-id>
```

Figura 1.24 Configuraciones del servidor.

Fuente: Icecast (2011).



**Hostname:** este es el nombre DNS o la dirección IP que se usará para las búsquedas de directorio streaming o posiblemente la generación de la lista de reproducción, si no se proporciona un encabezado de *host*. Mientras *local host* se muestra como un ejemplo, este nombre cambiará para la configuración personalizada del servidor, por una IP local.

**Location:** esta etiqueta establece la cadena de ubicación para esta instancia Icecast. Por ejemplo, se muestra en la interfaz web.

**Admin:** este debe contener la información de contacto para ponerse en contacto con el administrador del servidor. Por lo general, esta será una dirección de correo electrónico, pero como esto puede ser una cadena arbitraria, también podría ser un número de teléfono. Ello se muestra, por ejemplo, en la interfaz web.

**Fileserve:** este indicador se enciende en el servidor de archivos icecast2 en donde los archivos estáticos se pueden publicar. Todos los archivos se publican en relación con la ruta especificada en la ruta <paths> <Webroot> en los ajustes de configuración. Por defecto, la opción está habilitada de manera que las solicitudes de las imágenes en la página de estado son recuperables.

**Server-id:** esta configuración opcional permite al administrador del servidor anular la identificación del servidor predeterminado. Este valor es por defecto “Icecast”, seguido por un número de versión y, aunque no es de gran importancia, el ajuste cambia esto.

**Listen Socket:** esta es la sección donde se encuentra la etiqueta de configuración de puerto de acceso (véase figura 1.25).

```
<listen-socket>
  <port>8000</port>
</listen-socket>
```

Figura 1.25 Configuración de puerto.

Fuente: Icecast (2011).



**Port:** Es el puerto por el cual se podrá acceder al streaming y por el cual se podrá solicitar el servicio a través del explorador web. También será la salida a través de emisor de contenido.

**FFMpeg:** es el marco multimedia líder, capaz de decodificar, codificar, transcodificar, multiplexar, desmultiplexar, hacer streaming, filtrar y reproducir casi cualquier cosa que los humanos y las máquinas han creado.

**Codificador Oggfwd FFMpeg:** es un simple cliente de código para reenviar un archivo ogg a un servidor de streaming Icecast2. Se reenvía ogg de audio o vídeo leídos de la entrada estándar.

**VLC Media Player:** VLC es un reproductor multimedia libre y de código abierto multiplataforma y un “framework” que reproduce la mayoría de archivos multimedia, así como DVD, Audio CD, VCD y diversos protocolos de transmisión.

## • 1.10 Marco legal

IEEE 802.11s es el estándar en desarrollo para redes Wi-Fi malladas, también conocido como redes MESH. La malla es una topología de red en la que cada nodo está conectado a uno o más nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos. Según la normativa 802.11 actual, una infraestructura Wi-Fi compleja se interconecta usando LANs fijas de tipo Ethernet. El estándar 802.11s pretende responder a la fuerte demanda de infraestructuras WLAN móviles con un protocolo para la autoconfiguración de rutas entre puntos de acceso mediante topologías multisalto. Dicha topología constituirá un WDS (*Wireless Distribution System*) que deberá soportar tráfico unicast, multicast y broadcast. Para ello se realizarán modificaciones en las capas física y MAC de 802.11 y se sustituirá la especificación BSS (*Basic Service Set*) actual, por una más compleja conocida como ESS (*Extended Service Set*).

### 1.10.1 Regulación en Colombia

Existen varios organismos internacionales que definen estándares para el área de las telecomunicaciones, entre ellas se encuentran el Instituto



de Ingenieros Eléctricos y Electrónicos (IEEE) y la Unión Internacional de Telecomunicaciones (UIT).

En Colombia, el ente regulatorio de este tema es el Ministerio de las Tecnologías de la Información y Comunicaciones (MINTIC), el cual es el encargado de regular y/o administrar el espectro radioelectrónico; concibe la ley TIC, la cual determina el uso del espectro y donde se ubica la banda no licenciada ISM.

Para el caso de las ISM (*Industrial, Scientific And Medical Band*), comúnmente conocidas como “frecuencias no reglamentadas”, se tienen radiofrecuencias de 2.4 GHz y 5 GHZ asignadas por la UIT, estas frecuencias no requieren licencias por parte de los entes reguladores de Colombia, sin embargo, es importante tener en cuenta el: “Proyecto de Ley No. 021 de 2007: por el cual se fijan políticas y se establecen criterios para la administración y adquisición de programas de computación por parte del estado” (Acta No. 17 del cinco (05) de diciembre de dos mil siete (2007)).

En referencia el Artículo No. 4:

Artículo 4. Política de uso de Software. El Gobierno Nacional desarrollará una política para la promoción y uso de las TIC en las entidades públicas, conforme a los siguientes criterios:

La definición de procedimientos y el empleo de estándares que permitan la interoperabilidad entre los distintos sistemas de las entidades públicas y privadas.

La democratización de la información, mediante el acceso de las personas a bases de datos que requieran para ejercer sus derechos, participar en la vida política y en la vida económica, administrativa y cultural de la Nación, salvo en aquellos casos en que se comprometa la seguridad nacional o la divulgación de la información que sea objeto de reserva, protección o restricción legal.

El apoyo a proyectos de Investigación y Desarrollo para las entidades de carácter científico y tecnológico, que fomenten la apropiación tecnológica, la inclusión digital y la integración de las comunidades.



La capacitación en uso de TIC y el fomento de una cultura de uso en los servidores públicos.

La aplicación de incentivos, preferencias y apoyo al sector de la informática, en especial al sector público, empresarial y educativo.

La promoción de proyectos educativos que promuevan el uso de TIC, en las entidades de educación pública.

Otra de las regulaciones en Colombia a tener en cuenta es la Resolución Número 2190 de 2003<sup>9</sup>, por la cual se adoptan medidas en materia del ordenamiento técnico del espectro radioeléctrico, para utilizar radios portátiles de baja potencia y corto alcance de operación itinerante y se dictan otras disposiciones (MinTic, 2003)

**Artículo 30.** Atribución de frecuencias radioeléctricas que data de las frecuencias radioeléctricas relacionadas a continuación, podrán ser utilizadas libremente por el público en general (véase tabla 1.2), en aplicaciones de radios de baja potencia y corto alcance de operación itinerante, con las características técnicas descritas en los siguientes casos:

---

<sup>9</sup> Resolución número 2190 DE 2003, ordenamiento técnico del Espectro 30 de Julio de 2003. Recuperado el agosto de 2016, [mintic.gov.co/portal/604/articles-6604\\_documento.pdf](http://mintic.gov.co/portal/604/articles-6604_documento.pdf).



Tabla 1.2. Frecuencias radioeléctricas. Resolución Número 2190 de 2003.

Frecuencias radioeléctricas (MHz)	Límite de potencia (m W)	Ancho de banda de canal (KHz)	Aplicación
462,5625	500	12,5	Radios portátiles de baja potencia y corto alcance de operación itinerante, que deberán operar con potencia igual o inferior a 0,5 varios.
462,5875	500	12,5	
462,6125	500	12,5	
462,6375	500	12,5	
462,6875	500	12,5	
462,7125	500	12,5	
467,5625	500	12,5	
467,5875	500	12,5	
467,6125	500	12,5	
467,6375	500	12,5	
467,6625	500	12,5	
467,6875	500	12,5	
467,7125	500	12,5	
151,6125	2000	12,5	Radios portátiles de baja potencia y corto alcance de operación itinerante, que deberán operar con potencia igual o inferior a 0,2 varios.
153,0125	2000	12,5	
467,7625	2000	12,5	
467,8125	2000	12,5	
467,8375	2000	12,5	
467,9125	2000	12,5	

Fuente. Mintic (2003).

**Artículo 4º.** Características técnicas de operación: los radios portátiles de baja potencia y corto alcance de operación itinerante deberán operar en las frecuencias atribuidas, dentro de las características técnicas de potencia y ancho de banda establecidas en el artículo 3º de la presente Resolución.



## La resolución 689 DE 2004<sup>10</sup>

Atribuyó unas bandas de frecuencias radioeléctricas para su libre utilización dentro del territorio nacional, mediante sistemas de acceso inalámbrico y redes inalámbricas de área local, que utilicen tecnologías de espectro ensanchado y modulación digital, de banda ancha y baja potencia, en las condiciones establecidas por dicha resolución (ANE, 2004).

**Artículo 5º: Bandas de frecuencias.** Se atribuyen dentro del territorio nacional, a título secundario, para operación sobre una base de no-interferencia y no protección de interferencia, los siguientes datos de frecuencias radioeléctricas, para su libre utilización por sistemas de acceso inalámbrico y redes inalámbricas de área local, que empleen tecnologías de espectro ensanchado y modulación digital, de banda ancha y baja potencia, en las condiciones establecidas por esta resolución.

- Banda de 902 a 928 MHz.
- Banda de 2 400 a 2 483,5 MHz.
- Banda de 5 150 a 5 250 MHz.
- Banda de 5 250 a 5 350 MHz.
- Banda de 5 470 a 5 725 MHz.
- Banda de 5 725 a 5 850 MHz.

**Artículo 6º: Condiciones operativas en las bandas de 902 MHz,** 2400 a 2 483.5 MHz Y DE 5 725 A 850 MHz. Son condiciones operativas para los sistemas de espectro ensanchado por salto de frecuencia y de modulación digital, en las bandas de 902 a 928 MHz, de 2400 a 2 483.5 MHz y de 5 725 A 850 MHz.

Adicionalmente al Marco Legal, se debe tener en cuenta la legislación colombiana que se adopte a la parte tecnológica.

<sup>10</sup> RESOLUCION 689 DE 2004, Por la cual se atribuyen unas bandas de frecuencias para su libre utilización dentro del territorio nacional, mediante sistemas de acceso inalámbrico y redes inalámbricas de área local, que utilicen tecnologías de espectro ensanchado y modulación digital, de banda ancha y baja potencia, y se dictan otras disposiciones. 21 de abril de 2004. Recuperado el agosto de 2016, [http://www.ane.gov.co/cnabf/modulos/pdfs/Resolucion\\_689\\_2004.pdf](http://www.ane.gov.co/cnabf/modulos/pdfs/Resolucion_689_2004.pdf).



## • 1.11 Marco tecnológico

**Antenas:** una antena es un dispositivo metálico capaz de radiar y recibir ondas electromagnéticas del espacio. En los circuitos transmisores y receptores de radio se producen corrientes y tensiones eléctricas de altas frecuencias y asociadas a ellas, se encuentran las ondas electromagnéticas.

**Dispositivos móviles:** es un aparato de tamaño pequeño, con algunas capacidades de procesamiento, conexión permanente o intermitente a una red y memoria limitada, que permite acortar distancias. Existen tres tipos de dispositivos a saber Fuente especificada no válida.

**Dispositivo móvil de datos limitados:** se caracterizan por tener pantallas pequeñas de tipo texto y ofrecen servicios de datos limitados a SMS y acceso WAP.

**Dispositivo móvil de datos básicos:** su pantalla es de tamaño mediano; ofrece acceso a emails, lista de direcciones, SMS y un navegador web básico.

**Dispositivo móvil de datos mejorados:** son dispositivos con pantallas de medianas a grandes; ofrece las mismas características de los dispositivos móviles básicos más aplicaciones nativas como aquellas de Microsoft Office Mobile y aplicaciones corporativas (figura 1.26).

### 1.11.1 Topología de una red MESH

La topología que tiene una red MESH es en malla, ya que cada nodo que hay en la red está conectado a cada uno de los demás nodos para proporcionar diferentes rutas y recibir y enviar información de un nodo a otro por diferentes caminos. Si la red tiene todos sus nodos conectados, no va haber ninguna interrupción en las comunicaciones, por ello, una de las mayores ventajas de estas redes son sus entornos dinámicos. Ya que las redes MESH trabajan el enrutamiento dinámico, se necesita conocer las diferentes topologías relacionadas, las cuales se mencionan a continuación:

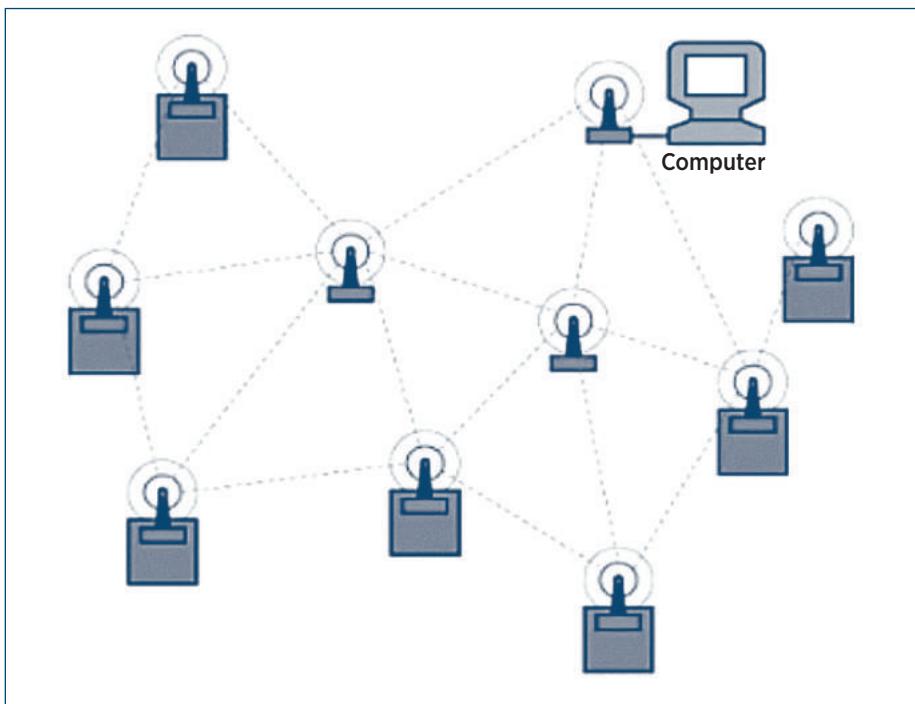


Figura 1.26 Esquema Funcional de una red MESH.

Fuente: Astudillo y Arancibia (2012).

### Redes Ad Hoc

Son redes de WLAN cuyos nodos se encuentran sin control o donde no existe un punto de acceso (*Access Point*), dando lugar a que cada nodo suscriptor se comunique con otro de forma directa y sin ninguna coordinación, generando así, la comunicación entre un nodo suscriptor y un nodo central que puede realizarse a través de otros terminales. Este Grupo de Servicio Independiente (*Independent Basic Service Set*) sólo permite la comunicación entre los distintos nodos subscriptores. En la Figura 1.27, se muestra la comunicación entre los dispositivos en una red *Ad Hoc* (Fredys A. Simanca H., 2018).

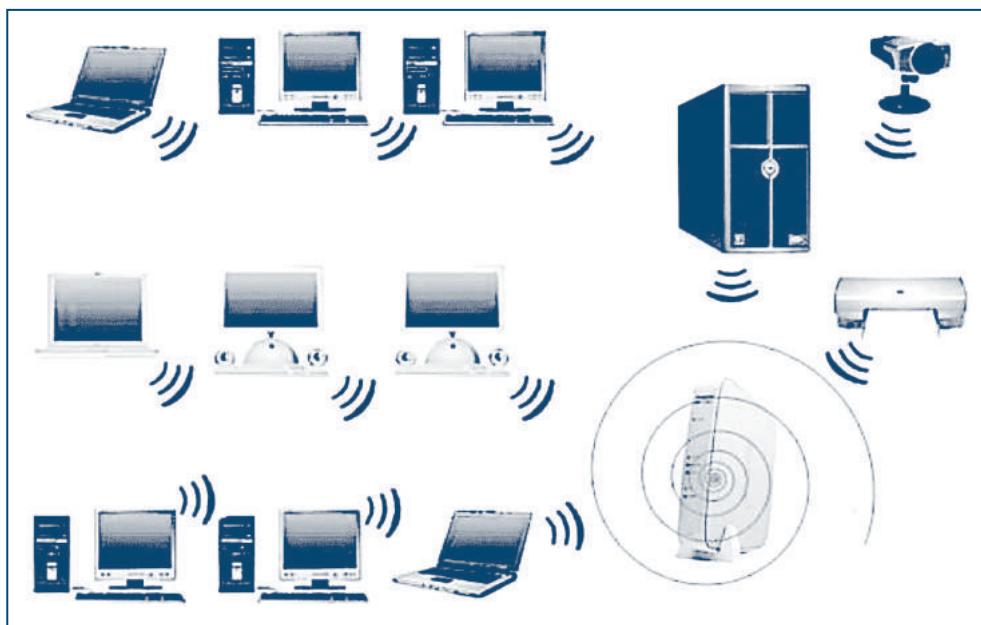
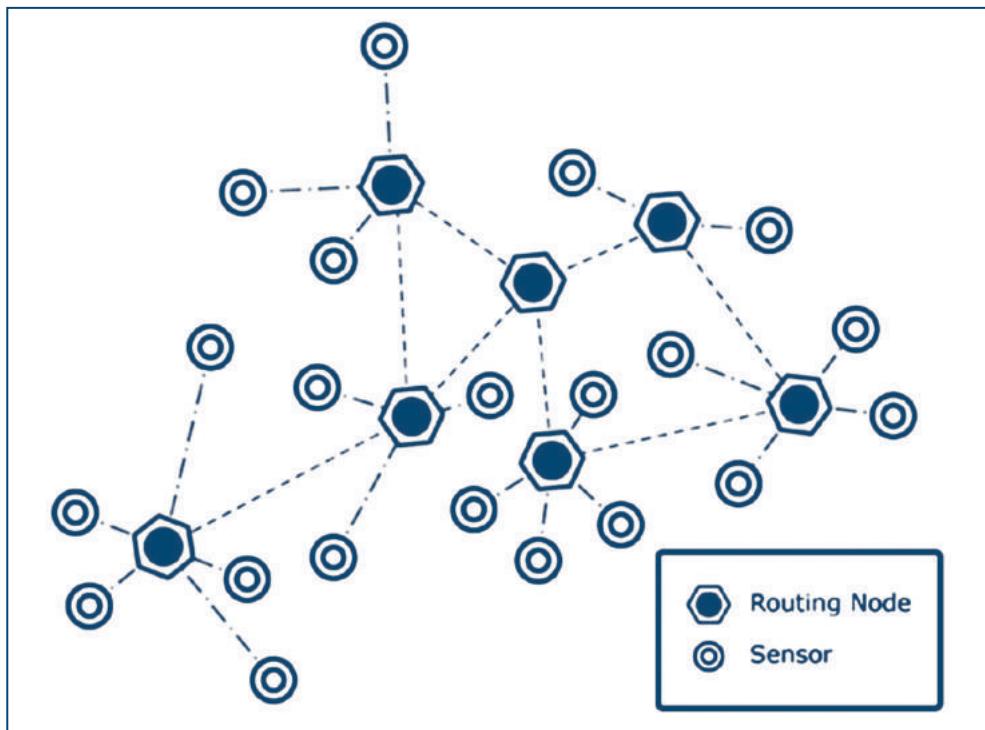


Figura 1.27 Topología de Red Ad-Hoc.

Fuente: Astudillo y Arancibia (2012).

## Redes Multi-Hop

Son redes que representan un paso importante en las comunicaciones inalámbricas. Lo que las caracteriza son diversas aplicaciones como: las redes comunitarias, sistemas de seguridad, redes en malla y redes de sensores; y en cuanto a la infraestructura de bajo costo: su flexibilidad y robustez, confiabilidad y movilidad, mecanismos de administración, entre otros. Estas redes se componen de nodos (mecanismos inalámbricos), los cuales funcionan por interconexión a través de los enlaces (canales inalámbricos). El rango de transmisión en cada uno de los nodos es limitado y la participación que tiene cada uno de ellos permite el establecimiento de una comunicación entre nodos que estén apartados, con lo cual cada nodo brinda los recursos que pueda ofrecer y participar en el proceso de unión de la información. Las características que tiene cada nodo le brindan la capacidad de actuar como un *host* y al mismo tiempo como un dispositivo de unión. En la Figura 1.28 se describe como son las redes Multi-Hop y sus partes.



*Figura 1.28 Distribución de una red Multi-Hop.*

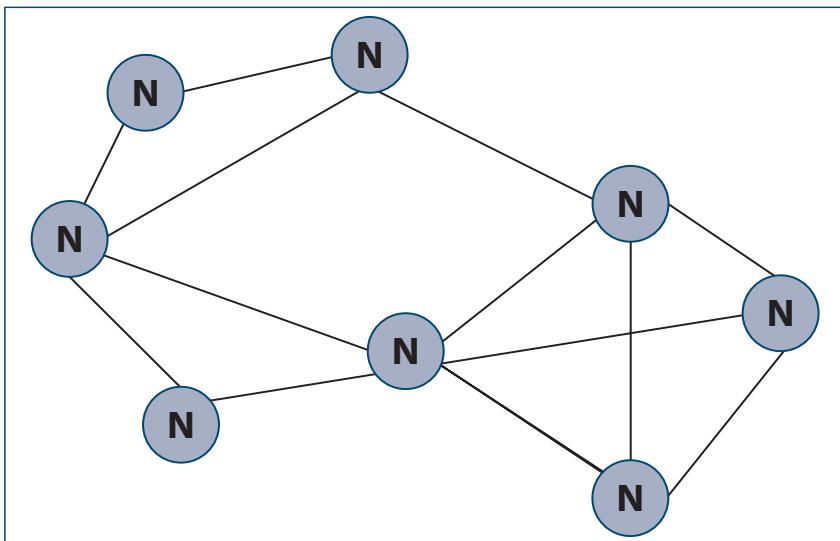
*Fuente:* Hop-by-hop\_TCP (s.f.).

### Manet (Red AD HOC Móvil)

Son redes *Ad Hoc* Móviles cuyos nodos pueden cambiar de posición, haciendo que la topología y el servicio de los dispositivos vaya transformándose continuamente, es decir, englobando con el objetivo de sustentar fuertemente el enrutamiento de la información entre los nodos móviles, pero poseyendo alguna que otra restricción, debido a su generación espontánea. Su arquitectura se comprende en:

#### Arquitectura plana y arquitectura jerárquica

La primera, arquitectura plana (Figura 1.29), se encarga de efectuar una vinculación independiente entre los nodos y se emplea el Multi-Hop para que la información llegue a los demás nodos.



*Figura 1.29 Arquitectura plana: Nodo (N).*

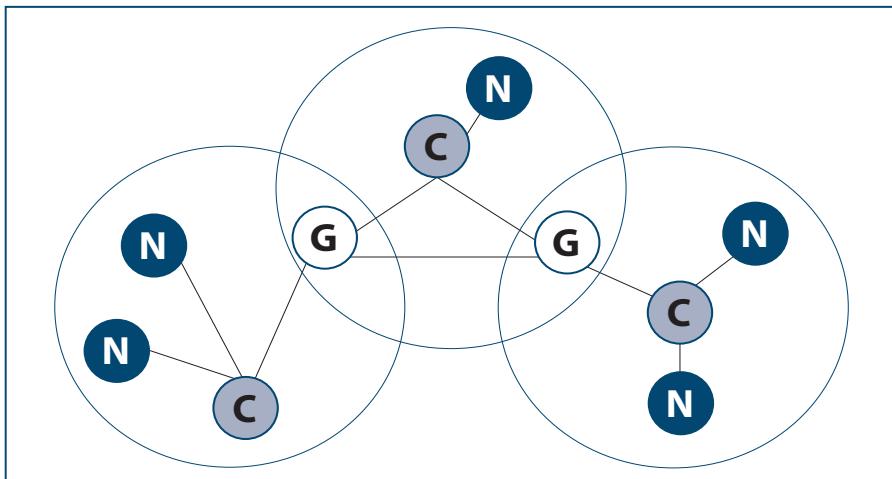
*Fuente:* Landero (2005).

La segunda, arquitectura jerárquica (Figura 1.30), se organiza en Clústers<sup>11</sup>, grupos que se unen con otros Clústers gracias a un nodo de cabecera o de borde que se propaga entre sí con otros nodos, posibilitando su jerarquización, otorgando distintos trabajos a los nodos y autorizando la comunicación entre toda la red.

### 1.11.2 Arquitectura de una red MESH

Para tener una arquitectura en las redes MESH se necesita una infraestructura modular, que permita realizar un diseño en escala para tener la precisión como se requiera dependiendo de la aplicación. Los nodos se utilizan para dispositivos de comunicación entre los mismos, como la de dispositivos de los clientes. Esta tecnología que se emplea en las redes MESH se considera con mayor capacidad de trasmitir con una menor latencia (retardos temporales que hay en una red). La ventaja es que los usuarios pueden disponer de cualquier tipo de aplicación en tiempo real.

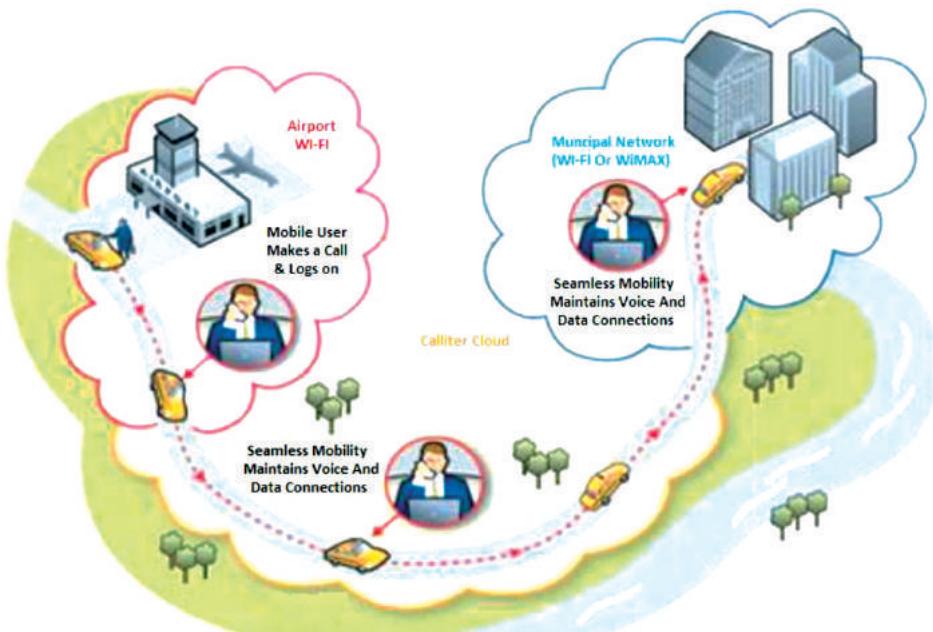
<sup>11</sup> Según el Diccionario de términos informáticos de Madrid (España), un Clúster en la tecnología de las computadoras, es la unidad de almacenamiento en el disco rígido. Un archivo está compuesto por varios Clústers que pueden estar almacenados en diversos lugares del disco.



**Figura 1.30** Arquitectura jerárquica: Nodo (N), Clusterhead (C) y Gateway (G).

Fuente: Landero (2005).

En la Figura 1.31, se evidencia una red MESH en una zona donde tiene diferentes elementos como edificios, aeropuertos, carros, etc.



**Figura 1.31** Esquema de una red MESH en una ciudad.

Fuente: Tecno Empresarial (2009-2010).



## MESH híbrido

La arquitectura híbrida combina la infraestructura con los clientes MESH. Los clientes MESH pueden acceder a través de la red mediante *routers* u otros clientes MESH, con lo cual esta infraestructura va aumentando la cobertura de la red. Una de sus características es que se interconectan con otros tipos de redes ya existentes, entre ellas: WI-FI, WiMax, redes móviles, redes de radio, etc. Las arquitecturas de los routers tienen una movilidad reducida, además de esto se encargan de realizar las tareas de configuración y encadenamiento, facilitando las tareas de los nodos y otros clientes, reduciendo la carga de trabajo, con lo cual se mantiene la tecnología Multi-Hop presente, ya que no es necesario que todos los nodos se vean entre sí en la red de routers, sino que tengan visión de los que están cercanos a ellos.

## Protocolos de enrutamientos

En apartados anteriores se han estudiado topologías y protocolos de las redes inalámbricas, dado que se trata de una topología dinámica y auto configurable, las direcciones de los dispositivos cambian dinámicamente, por lo cual es necesario tener varios protocolos para la transmisión de datos con bajos costos de transmisión (es decir, encontrar rutas con menos saltos para transmitir la información).

Los protocolos manejan ciertos enlaces y sus estados; dependiendo de la forma en que se quieran manejar, es posible distinguir diferentes protocolos como los que se ven a continuación:

### i) Reactivos

Estos protocolos utilizan algunos mecanismos de enrutamiento, sólo cuando un nodo solicite enviar información. Los protocolos reactivos suelen asumir la latencia alta para el primer paquete, aunque en ocasiones la topología cambie una ruta individual dura cierto tiempo, con lo cual las rutas tienen cierta indecencia. El número de rutas útiles son las que están en la parte más baja, no hace falta buscar todas las posibles rutas.

### ii) Ad-hoc On Demand Distance Vector (AODV)

Este protocolo de enrutamiento de vector distancia es reactivo para redes móviles Ad-hoc, por lo que la tabla donde se encuentran los enrute-



tamientos se actualiza cuando se envía una demanda, de manera que la información recuperada permanecerá el tiempo que se requiera para que se pueda realizar la comunicación. Cuando un nodo hace una petición de información, envía mensajes de **route request** (RREQ), después tiene que esperar a que los nodos que estén contiguos contesten con un **route reply** (RREP) para formar la ruta adecuada, una vez esta se crea, si algún nodo falla se envía un error (RERR) al nodo que está haciendo la petición para que vuelva hacer una búsqueda eficiente.

### iii) Proactivos

Estos protocolos son los que mantienen en cada uno de los nodos, información acerca de la topología de red, la cual es almacenada en tablas de enrutamientos que se actualizan de forma periódica o por eventos que puedan ocurrir. Estos protocolos se basan en protocolos de vector distancia y de estado de fase enlace.

### iv) Multiple MAC Registration Protocol (MMRP)

Proporciona mecanismos que permiten a estaciones y MAC BRIDGES poder registrarse dinámicamente y después borrarse. El funcionamiento de este protocolo se basa en los servicios que son prestados por MRP. La información que se registra se difunde a través de MMRP con información sobre miembros de grupo (presencia de participantes en MMRP), intercambio de información concreta de miembros del grupo, con el fin de actualizar las entradas de un registro en el BD.

### v) Optimized Link State Routing (OLSR)

El protocolo OLSR permite trabajar de forma distribuida para poder establecer conexiones entre nodos mediante un mecanismo de enrutamiento estándar, para una red inalámbrica *ad hoc*. El protocolo OLSR fue diseñado principalmente por INRIA y tiempo después, fue estandarizado por el IETF.

### vi) Open Shortest Path First (OSPF)

Este es un protocolo de encaminamiento, el cual usa algoritmo *Smooth Wall Dijkstra* para buscar cual es la ruta más corta y menos costosa entre



cada uno de los nodos. Este protocolo se usa en partes internas de una red, verificando el estado de cada uno de los enlaces y trasmitiendo la información recopilada en todos los enrutadores de una misma jerarquía.

## vii) Híbridos

Son algoritmos que toman como rasgos un vector distancia y del estado de enlace.

Uno de esos protocolos es el **HWMP**, definido por la IEEE 802.11s, el cual se basa en AODV y procesos de enrutamiento establecidos en árboles. Este protocolo permite una optimización de manera eficiente, mediante elementos proactivos y reactivos, buscando una ruta amplia. HWMP utiliza mensajes basados en AODV, adaptados para el direccionamiento MAC de la segunda capa, con el fin de descubrir rutas reactivamente. Si cualquier punto está conectado dentro del entorno de la red por cable, no se requiere de HWMP, ya que selecciona caminos unidos por complicación de los puntos pares por los que está compuesta el mapa en la malla.

### 1.11.3 Características de las redes MESH

Las redes MESH cada vez se vuelven más significativas para la sociedad y van creciendo de manera gradual en un punto donde ya no es inadvertida por la sociedad tecnológica. El primer despliegue que se realizó de una comunidad MESH en gran escala ha demostrado que estas redes tienen grandes ventajas.

Como se vio anteriormente, los nodos de las redes funcionan de dos formas: como cliente y como comunicación entre nodos, esto significa un potencial de ahorro en el número de radios que se necesitan, con lo cual estas redes son de bajo costo en comparación con otras.

La topología de las redes MESH promete una estabilidad en condiciones variables, ya sea debido a fallas de algún nodo o por el tipo de terreno en donde se encuentra la red, haciéndolas confiables con respecto a fallas. La estabilidad en cuanto a los nodos, exceptuando los que se mantienen conectados con enlace directo a la red, es que pueden ser construidos con baja energía porque pueden ser desplegados con unidades autónomas ya sea con energía eólica, solar, hidráulica, entre otras.



La integración del *hardware* de las redes MESH con sus nodos es simple, ya que los estos son pequeños, no hacen ruido y son fácilmente encapsulados en pequeñas cajas a prueba de agua.

#### 1.11.4 Aplicación de las redes MESH

La procedencia de las redes MESH es militar, ya que se requería tener conexión con el pelotón relativamente lejano, en el cual se encontraba dentro de la zona donde se podía emitir y recibir mensajes. En la actualidad, el uso de estas redes abarca todo tipo de grupos que se entregan a su investigación y a lo que las acota, por ejemplo, empresas privadas centradas en la comercialización de redes MESH, instituciones sociales, laboratorios o grupos de inspección.

**Redes MESH comunitarias.** Integradas por empresas, instituciones y usuarios, los cuales se encargan de construir la red con la finalidad de tener una comunicación alternativa y/o red de emergencia que no precise de canales, dando la posibilidad de conexión sin importar la posición y asegurándose de que funcione para transmitir voz y datos y atender las necesidades que surjan.

**Redes MESH comerciales.** Empresas ocupadas en la evolución de redes inalámbricas, brindando resultados de intercambio en interconexiones de redes de más profesionales que las redes comunitarias, empleándose como una red *self-healing* que va destinada a clientes particulares o profesionales.

**Redes MESH de laboratorio.** Redes de ensayo que proporcionan realizaciones de proyectos de investigación.

**Clientes MESH.** Los clientes proporcionan conexiones punto a punto entre dispositivos, con las funciones básicas de la red como la configuración o encaminamiento. Con lo cual no es necesario tener routers MESH. Estos clientes son similares a los que conforman una red *ad hoc*, la diferencia es que los clientes MESH disponen de una tecnología mejor a la habitual, puesto que el *hardware* y *software* son capaces de soportar las funciones que se necesiten para tener una conexión en la red.



## 1.11.5 Ventajas y desventajas de las redes MESH

### Ventajas de las redes MESH

El beneficio de este diseño de red es que aún si ninguno de los nodos es alcanzable desde el punto de acceso central, igual pueden comunicarse entre sí.

#### Áreas municipales

#### Áreas rurales

Las redes inalámbricas MESH son la solución natural para la implantación de nuevas tecnologías en entornos municipales. Su utilización puede destinarse a servicios como:

- Seguridad ciudadana.
- Supervisión y control del tráfico.
- Servicios al ciudadano en materia de sociedad de la información: acceso a Internet en centros escolares y bibliotecas, así como información y orientación turística, redes intranet, entre otras.
- Redes corporativas para uso en las estaciones móviles (policía municipal, administración).

#### Áreas rurales

Permiten introducir servicios de banda ancha en entornos rurales, para implantar servicios sociales esenciales y promocionar la sociedad de la información. La instalación en estas zonas de las redes inalámbricas no requiere ninguna infraestructura previa de telecomunicaciones.

- Su implantación resulta rentable.
- Cada nodo presta cobertura a grandes extensiones.
- Enlaces directivos de “Backhaul” entre nodos.

**Auto-formación:** la red inalámbrica se forma automáticamente, una vez que los nodos de la malla se han configurado y activado.



**La tolerancia a fallos:** si existen rutas redundantes en la red, el flujo de información no se interrumpe en el resto de la misma cuando un nodo falla. La red de forma dinámica, redirige la información a través de la ruta disponible.

**La auto-sanación:** una vez restaurado, un nodo vuelve a unirse a la red de malla sin problemas.

**Propiedad de la comunidad:** la propiedad de la red se comparte, por lo tanto, la carga del soporte de la red no se apoya en una sola persona.

**Bajo costo:** la infraestructura se puede construir a partir de nodos de bajo costo. Costo incremental de la red con la adición de un nodo adicional. El costo marginal de expansión es bajo para ese nodo, sin embargo, el alcance y el valor de la red es mayor.

**Facilidad de implementación:** la formación de miembros en la comunidad permite que ellos construyan sus propios nodos y configuren e implementen la red en la comunidad.

**Posibilidad de utilización de repetidores:** que resuelvan problemas de orografía e interconecten largas distancias.

## Desventajas de las redes MESH

**Latencia:** retraso debido al número de saltos que puede llegar a dar un paquete hasta su destino. Problemas no permitidos en servicios de tiempo real, como la telefonía IP.

**Compartiendo el medio:** puede haber interferencias entre usuarios debido al limitado número de frecuencias de las redes WLAN. Se podrían provocar problemas de direcciones duplicadas y conflictos de red (Solución IPv6).

**Seguridad:** las redes *ad-hoc* necesitan hablar con sus clientes antes de autenticarlos, son vulnerables a ataques DoS y los datos pueden ser interceptados. Algunas empresas han desarrollado protocolos que utilizan técnicas de cifrado diferentes a las de WiFi y que no pueden ser interceptados con una tarjeta de red inalámbrica 802.11 común.

**Rendimiento:** la disminución del rendimiento (*Throughput*) se provoca por el número de saltos de acuerdo a  $\frac{1}{k*n}$  (“n” es el número de saltos). MESH se ha implementado en equipos 802.11 con dos radios, uno en la banda de 2,4 GHz y otro, en la banda de 5 GHz. De esta manera, el rendimiento no disminuye con el número de saltos (recibir y transmitir simultáneamente en bandas distintas).

### 1.11.6 Generaciones de las redes MESH

#### Primera generación

En esta generación el sistema mallado tiene un sólo radio para hacer la interconexión entre nodos y dar servicio; los datos se retransmiten de un nodo a otro de una manera *store-and-forward*, es decir, un nodo primero recibe los datos y luego, éste los retransmite (ver figura 1.32).

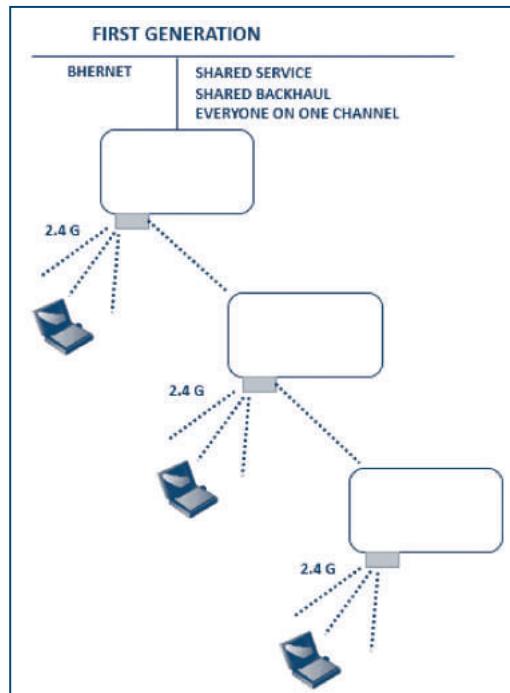


Figura 1.32 Ilustración red MESH primera generación.

Fuente: Pérez y Granados (2010).

## Segunda generación

En esta generación se decidió combinar dos radios, uno para dar servicio con el estándar 802.11b/g y el otro, para interconectar los nodos con el estándar 802.11a.

Con este sistema se logró eliminar la interferencia en los nodos, ya que se trabaja con diversas bandas de frecuencia (entre 2.4GHz y 5.8GHz) para dar servicio a los usuarios e interconectar nodos. El problema surge cuando aumenta la demanda de servicio por parte del usuario, se presentan contenciones y congestiones significativas en la parte de la radio que se usa para interconectar los nodos, lo cual hace que este sistema tenga una ligera desventaja (ver figura 1.33).

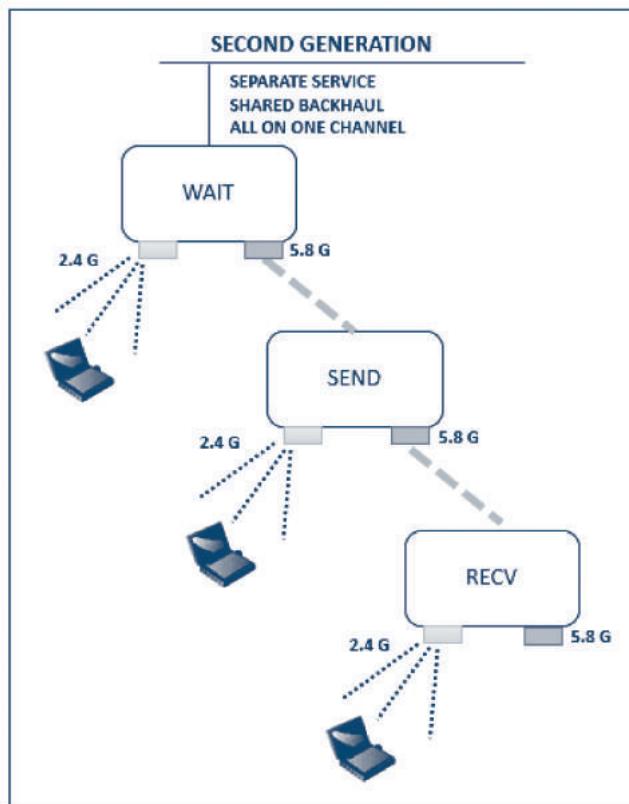


Figura 1.33 Ilustración red MESH segunda generación.

Fuente: Pérez y Granados (2010).

## Tercera generación

Los equipos de esta generación llevan una gran ventaja en comparación con las generaciones anteriores, ya que son considerados equipos inteligentes por utilizar una tecnología moderna. Cada nodo puede enviar y recibir datos de sus vecinos (ver figura 1.34); además, los canales disponibles se pueden reutilizar, haciendo que el espectro disponible sea más amplio y que el funcionamiento de la red aumente 50 o más veces.

Las empresas fabricantes de los equipos de esta generación se basan en productos multi-radios que soportan múltiples configuraciones de red. Un radio de los equipos de tercera generación se usa para crear un enlace hacia su nodo *upstream* (nodo más cerca al *gateway*) y otro radio se utiliza para un enlace *downstream* al nodo vecino siguiente. A diferencia de la generación anterior, estos radios pueden hacer uso de diversos canales.

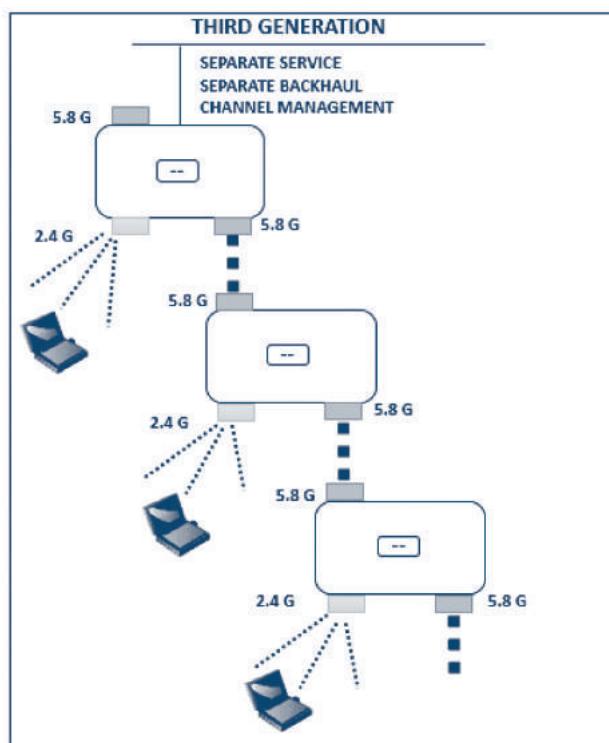


Figura 1.34 Ilustración red MESH tercera generación.

Fuente: Pérez y Granados(2010).



## • 1.12 Contexto social de las redes MESH

### 1.12.1 ¿Cómo puede ser útil un nodo MESH?

Aunque no deja de ser un proyecto experimental, hoy en día es posible implementar tecnologías MESH para proporcionar servicios útiles a más de una persona. Para que pueda aprovecharse un nodo en beneficio de un cualquier grupo interesado, en este proyecto se resalta la capacidad de proporcionar ciertos elementos en común que permitan el desarrollo cultural e integral de las personas, por medio de conocimientos que pueden ser aprovechados vía inalámbrica. Conocimientos como los encontrados en Wikipedia, un servidor web que contiene documentación y en lo posible, un servidor de archivos de video con contenido variado; este material puede ser estudiado y analizado libremente gracias a las licencias libres de uso que permiten su manipulación e intercambio, para que todas las personas puedan beneficiarse y aprender “libremente”.

### 1.12.2 Escenarios apropiados para un nodo MESH

Se tienen pensados tres escenarios inicialmente como modelos de aplicación:

**Colegio.** En un colegio con bajos recursos, puede adquirirse la infraestructura necesaria para poner un mínimo de un nodo para dictar un cronograma de actividades que aprovechen sus recursos, siendo el mismo análisis de los recursos del nodo y el nodo en sí, propiedades útiles de estudio.

Mientras que niños de grados menores, pensado en cursos desde tercero de primaria hasta octavo de secundaria, podrían simplemente utilizar Wikipedia, documentos del servidor del nodo a modo de consulta rápida, entre otras cosas, alumnos de grados superiores pueden aprender recursos valiosos de capacitación como podría ser la implementación de servicios en red, diseño de una página web, programación web en diversos lenguajes de programación web como JavaScript, HTML, CSS entre otros, y aprender la capacidad de otros sistemas operativos aparte de Windows, como Linux, y las diversas filosofías que rodean su administración, que dicho sea de paso, es aprender la utilidad de usar alternativas de manejo de sistemas.



**Figura 1.35** Colegio Rafael Uribe Uribe, Sede Secundaria.

*Fuente:* Elaborado por el grupo de investigación.

Un trabajo muy interesante es el proyecto Edubuntu, una línea de aprendizaje basada en el proyecto Ubuntu, que provee conocimientos en pro de la educación de niños siendo una plataforma de manejo simple, pero muy eficaz para el desarrollo de nuevas sinergias de conocimiento.

Podría darse un ejemplo, albergando los archivos de instalación, sin que tenga que reemplazarse el sistema inicial (recordando que un nodo puede manejarse y consultarse desde Windows o Linux o cualquier sistema, pero se sugiere Linux, al menos para el único servidor de trabajo para el nodo) usando un entorno rápido de virtualización como VirtualBox o VMware (como experiencia personal, el *software* de Oracle VirtualBox es mucho más eficaz y más cómodo para prácticas) con Edubuntu o cualquier *software* para aprender.

Es fundamental entender que todos estos documentos pueden ser implementados dependiendo de la capacidad del administrador, y que básicamente es un material introductorio para no representar una asignatura pesada de aprender, sino simplemente una lúdica agradable para disfrutar.



Fredys A. Simanca H., Fabián Blanco Garrido, Eduardo Triana Moyano

**Universidad.** Continuando rápidamente con la línea de aprendizaje sobre el entorno de redes MESH, podría implementarse un cronograma de estudios mucho más elaborado, siendo importante resaltar las siguientes pautas no necesariamente en el siguiente orden:

- Política de redes MESH.
- Infraestructura.
- Instalación.
- Introducción de redes.
- Introducción a servidores
- Virtualización
- Administración de recursos.
- Resolución de problemas.
- Programación, diseño y desarrollo web.
- Seguridad de recursos.
- Linux y BSD.
- Monitoreo y Auditoría.



*Figura 1.36* Universidad Libre, Sede Bosque Popular – Bloque L y A.

Fuente: Elaborado por el grupo de investigación.



## • 1.13 Plan Vive Digital

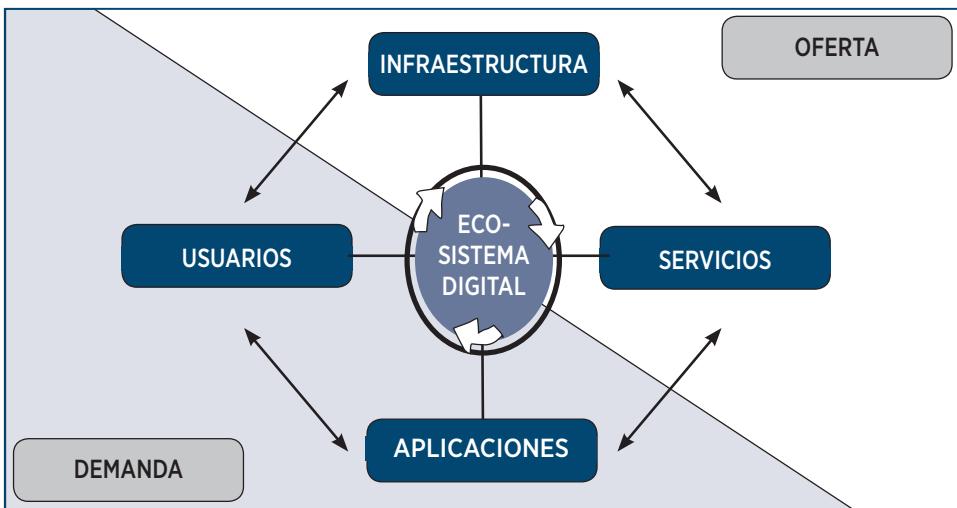
El actual gobierno, apoyado en las políticas y directrices formuladas por el ministerio de las tecnologías de la información y telecomunicaciones, ha considerado pertinente la estructuración del modelo desarrollado por el Banco Mundial para catalogar los ecosistemas digitales<sup>12</sup>, con el fin de validar la infraestructura de telecomunicaciones, el desarrollo de aplicaciones y la utilización por parte de los interesados o usuarios finales, pensando también la proyección de unidades de negocios que caracteriza a la industria de las tecnologías de información y de los BPO&O (*Business Process Outsourcing and Offshoring*); sin olvidar lo pertinente a las estrategias de Ciberseguridad, Ciberdefensa, Telesalud y Educación Virtual (Vitek y Bryce, 2003).

Estructuralmente el ecosistema digital del cual se apropiá Colombia para formular el correspondiente Plan Vive Digital, identifican las entidades que se presentan en la Figura 1.37, a saber: infraestructura (soporte físico), servicios (unidades de uso y operación), aplicaciones (plataforma de soporte interactivo) y los usuarios (quienes emplean los servicios y se benefician con las aplicaciones). El ecosistema digital, como entidad económica balancea la relación oferta-demanda, es decir, interpreta la asociación entre la infraestructura y los servicios, con los usuarios y las aplicaciones.

El Plan Vive Digital, contempla e integra la infraestructura básica que soportarán múltiples tecnologías y lograrán la densificación de la conectividad por fibra óptica al pasar de 200 a 400 municipios totalmente conectados; adicionalmente, con la cobertura y aplicación del Plan Vive Digital, Colombia evidenciará los siguientes beneficios:

- Cubrimiento total con la telefonía móvil con tecnologías 3G y 4G.
- Asignación integral del espectro IMT (*International Mobile Telecommunications*), para operar bandas desde 1.9 GHz a 2.5 GHz y entre 1.7 y 2.1 GHz.
- Habilitación de conexión internacional CDN (*Content Distribution Networks*) y data center.

<sup>12</sup> El plan vive digital estimula los cuatro componentes del ecosistema digital mediante la expansión de la infraestructura, la creación de nuevos servicios a precios más bajos, la promoción del desarrollo de aplicaciones y contenidos digitales y el impulso a la apropiación tecnológica por parte de estos.



*Figura 1.37* Ecosistema digital.

Fuente: MinTic (2010-2014).

- Dimensionamiento y aplicación de la infraestructura para cubrimiento rural, operando los estándares de compartición de datos (*Duct Sharing*) y cableado interior (*In-House Wiring*).
- Despliegue de redes de última milla para facilitar la instalación de nuevas antenas para eliminar problemas de despliegue.
- Garantiza el amplio uso de la televisión y la radio digital, proyectándose la red de telecomunicaciones para la prevención y atención de desastre.
- Fomenta la fabricación y ensamble a nivel nacional, de componentes de la red y de soporte computacional.
- Implementación del Gobierno en línea para construir un estado más eficiente frente a las demandas del desarrollo económico, permitiendo el salto de Colombia en la escala mundial desde el puesto 56 hasta los primeros lugares.
- Impulsa y estructura estrategias para el desarrollo de las MiPyMEs para la utilización de las aplicaciones móviles, pretendiendo utilizar las ventajas de la comunicación terrestre (TDT), asegurándose la promoción de contenidos digitales y el teletrabajo.

El Plan Vive Digital, representa para Colombia la estrategia de desarrollo tecnológico más importante en todos los escenarios de la sociedad, la producción y el pensamiento, los logros proyectados facilitarán la integración



de la operación en todos los ejes de impacto y desarrollo, basados en el contacto directo con las soluciones teleinformáticas requeridas para el usuario del siglo XXI.

El gobierno con la presencia directa de MinTIC, se estructura en los vértices de un triángulo que definen:

**Proyección académica e integración al entorno virtual.** Tendencia a los servicios integrados ofrecidos por la llamada *Cloud Computing*, que favorecerá en todos los aspectos el fortalecimiento de la economía y el incremento de PIB.

Estructuración y consideración del gobierno en línea, integrando la totalidad de ministerios, los quehaceres de la rama judicial y la normativa de control de los entes reguladores tales como la Procuraduría, la Contraloría, la Fiscalía y las Altas Cortes de Justicia.

Con este plan el gobierno del Doctor Juan Manuel Santos proyecta a Colombia hacia la total transformación, hacia la verdadera reingeniería de procesos y hacia la estandarización y refinamiento de los procesos realizados por la sociedad sin importar su ubicación. Por fin la fibra óptica y la banda ancha garantizan a cada habitante colombiano disfrutar del mejoramiento del nivel y calidad de vida; este plan conlleva además la revolución en el aula, pues el aprendizaje por escenarios virtuales es garantía de la innovación y de la serendipia<sup>13</sup>.

Analíticamente en el ámbito de la economía y desarrollo global, el plan Vive Digital incluye formalmente las tres plataformas de desarrollo que requiere cada país para, sin pretender reducir los costos, incrementar sus utilidades (a la luz del pensamiento del gran filósofo Heidegger). Con este plan, la administración gubernamental actual espera dilucidar los conocidos factores de acción existencial, a saber:

- **Befind Lichkeit:** se estudiará y comprenderá la relación con el medio tecnológico, al encontrar la respuesta a las preguntas: ¿En dónde estamos?

<sup>13</sup> Serendipia es un descubrimiento distinto de los que se buscaba, no previsto pero identificado, reconocido y aceptado a pesar de ser inesperado, surgido accidentalmente. Coincidencia, accidente, suerte, destino. Proceso que permite encontrar un producto o solución cuando se está buscando otro.



¿Para dónde vamos? ¿A dónde queremos llegar? ¿A dónde realmente podemos llegar?

- **Verstehen:** Colombia interpretará y valorará la necesidad de la conversión de tecnología en el ámbito del ciberespacio, considerando siempre que su ingeniería valore su desarrollo en soluciones competitivas y de alto posicionamiento; por fin los logros de la ingeniería colombiana, se incluirán como generadores directos del PIB.
- **Rede:** Colombia escalará peldaños en la escala de desarrollo tecnológico, al integrar la potencialidad de la banda ancha en todo su espacio geográfico, es decir que adquirirá la conciencia que demanda el desarrollo puntual del ciberespacio y de la teleinformática, desde San Andrés hasta Leticia, y desde la Gorgona hasta el Orinoco, nuestro país disfrutará de los servicios y beneficios de la economía de la información.

### 1.13.1 Principios básicos del Plan Vive Digital

Para asegurar que las intervenciones estatales sean adecuadas e integrales y logren optimizar el uso de los recursos, el Plan Vive Digital sigue cinco principios básicos:

“El mercado hasta donde sea posible, el Estado hasta donde sea necesario”. Promover el desarrollo del sector privado para expandir infraestructura y ofrecer servicios.

Incentivar de forma integral la oferta y la demanda de servicios digitales para alcanzar una masa crítica.

Reducir barreras normativas e impositivas para facilitar el despliegue de infraestructura y oferta de servicios de telecomunicaciones.

Priorizar los recursos del Estado en inversiones de capital.

El Gobierno va a dar ejemplo.

Algunas de las barreras que impiden la masificación del uso de Internet en Colombia (ver figura 1.38), se detectaron a partir del análisis realizado. Si bien en el Plan Vive Digital se plantean diversas iniciativas para superarlas, dichas barreras se presentan a continuación.

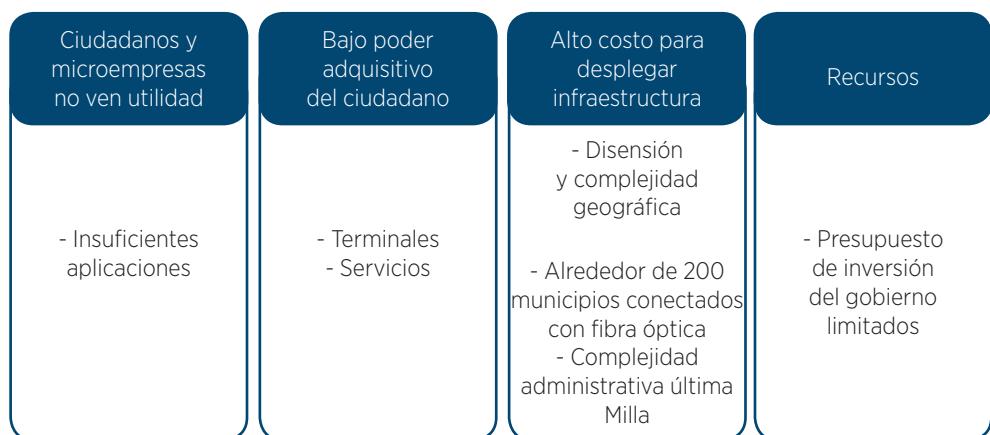


Ciudadanos y microempresas que no ven la utilidad. Como muestran las encuestas, una de las grandes razones para no tener Internet, tanto para los ciudadanos como para las microempresas, es que no encuentran la necesidad o utilidad del servicio; lo cual se debe, en parte, a la falta de contenidos y aplicaciones locales útiles para el ciudadano o microempresa nacional, así como a la falta de apropiación de la tecnología.

Bajo poder adquisitivo del ciudadano. El costo de los terminales y el servicio de Internet sigue siendo relativamente alto para los ingresos de la mayoría de ciudadanos, por lo que muchos de ellos no tienen posibilidad económica de acceder a estos.

Altos costos para desplegar infraestructura. Actualmente, en el país sólo alrededor de 200 de los 1.102 municipios están conectados a través de la red de fibra óptica. Las características geográficas y de dispersión han limitado el despliegue de las redes de telecomunicaciones. También, existen dificultades administrativas tanto en los territorios como en la última milla para el despliegue de infraestructura.

Recursos. La realidad colombiana hace que los recursos con los que cuenta el estado para invertir en infraestructura sean limitados, por lo que es importante encontrar la mejor manera de invertirlos.



**Figura 1.38** Barreras que impiden la Masificación de Internet en Colombia.

Fuente: MinTic (2010-2014).



## 1.13.2 Inversión, tiempo, metas y objetivos para la ejecución del Plan Vive Digital

La cifra que se estimó en octubre de 2010 para la implementación de las iniciativas fue de 5.5 billones de pesos, de los cuales 3.2 billones resultan de las iniciativas del Ministerio de Tecnologías de la Información y las Comunicaciones y 2.3 billones hacen parte de las iniciativas de los demás ministerios.

### Tiempo de duración

El Plan Vive Digital será la política de gobierno en materia TIC durante cuatro años (2014-2018).

### Metas del Plan Vive Digital

Las metas específicas para la masificación de Internet en 2014 fueron:

- Pasar de 27% a 50% de hogares y del 7% al 50% de MiPyMEs conectadas a Internet.
- Multiplicar por cuatro las conexiones a Internet pasando de 2.2 a 8.8 millones.

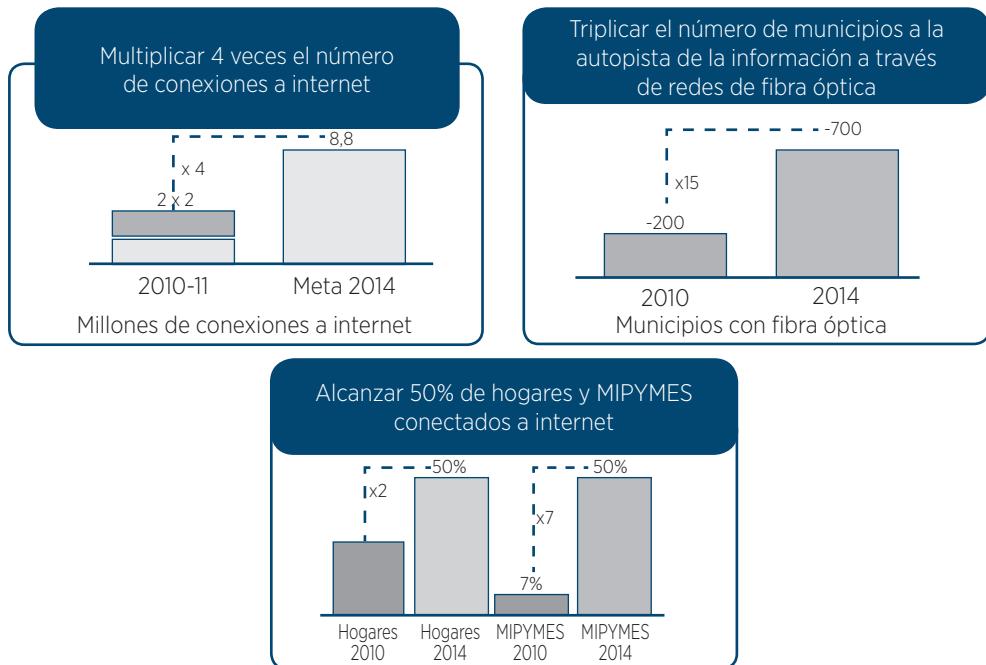
Triplicar el número de municipios conectados a la autopista de la información, a través de redes de fibra óptica de aproximadamente 200 a 700 municipios.

¿Qué busca el Plan Vive Digital en cuanto a servicios?

- Reducir el IVA para Internet.
- Masificar los terminales para Internet.
- Crear un esquema de subsidios para Internet para estratos 1 y 2.
- Crear un marco legal y regulatorio para la convergencia.
- Reducir el impacto de las TIC en el medio ambiente.

El objetivo principal del Plan Vive Digital es impulsar la masificación del uso de Internet para dar un salto hacia la prosperidad democrática.

Para lograr esta masificación, el equipo del plan Vive Digital ha fijado algunas metas concretas para el año 2014 (ver figura 1.39):



*Figura 1.39* Gráfico de metas de conexión en Colombia.

Fuente: MinTic (2010-2014).

- Triplicar el número de municipios conectados a la autopista de la información. Queremos expandir esta infraestructura para llegar al menos a 700 municipios del país.
- Conectar a Internet al 50% de las MIPYMES y al 50% de los hogares. Queremos en el 2014 llegar al 50% tanto de hogares como de MiPyMEs.
- Multiplicar por 4 el número de conexiones a Internet. Queremos llegar en el 2014 a 8.8 millones MinTic (2010-2014).

## 1.14 Redes inalámbricas

Una red inalámbrica es la unidad de interconexión para intercambio transaccional que habilita el flujo de la información, sin contar con un me-

dio de geometría sólida (Guerrero, 2017), su estructura de catalogación se visualiza en la Figura 1.40.

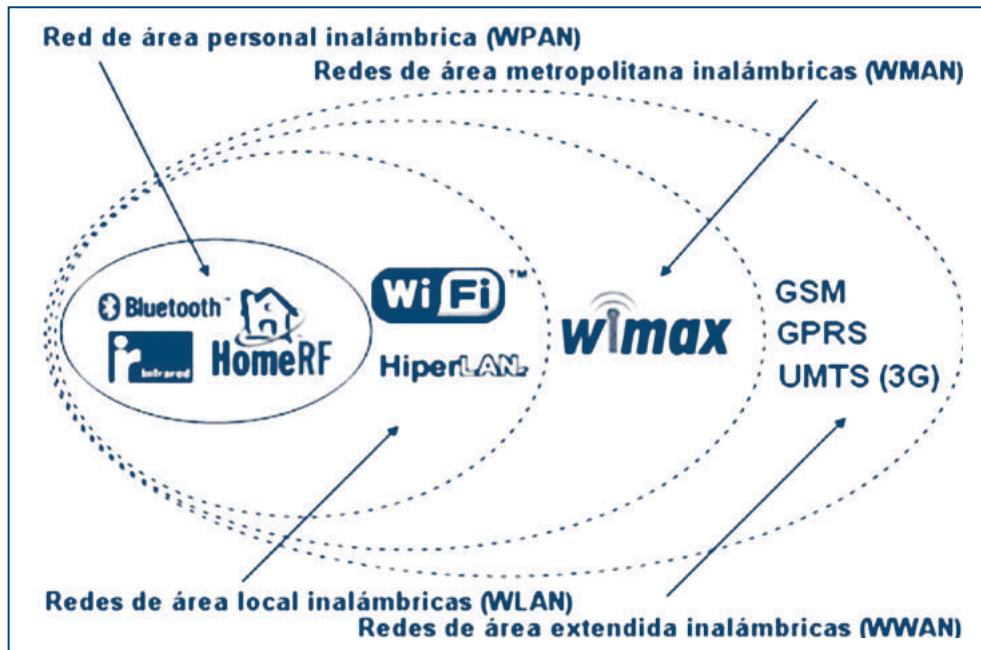


Figura 1.40 Clases de redes inalámbricas.

Fuente: Guerrero (2017).

Las redes inalámbricas son sistemas de comunicaciones entre dos o más dispositivos independientes se comuniquen entre sí, sin la necesidad de cables. En la Figura 1.40 se reconoce las diferentes clases de redes inalámbricas dependiendo de la cobertura. Para conocer un poco más, aquí se mencionarán cuáles son las ventajas y desventajas de cada una de las redes.

**WPAN (Red de área personal inalámbrica).** Son redes inalámbricas que permiten comunicar diferentes dispositivos a una corta distancia entre 10 y 20 metros, la cantidad de dispositivos máximo es de 255. Y como se distingue en la Figura 1.41, este tiene como propósito la conectividad de dispositivos ubicados principalmente en oficinas, impresoras y scanner. El estándar que se requiere para esta red es IEEE 802.15.4, el cual define la capa física y el control de acceso.



*Figura 1.41 Red WPAN, dispositivos conectados a la red.*

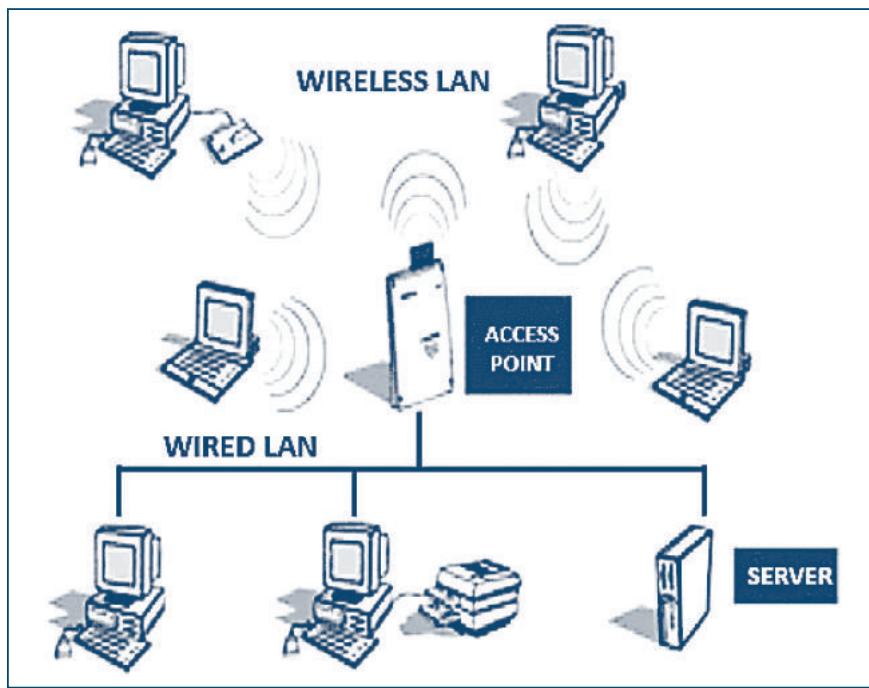
Fuente: The Office Network (2014).

**WLAN (Red de área local inalámbrica).** Es aquella que tiene dos o más terminales; son redes privadas que cubren un área equivalente a la red de una empresa. Un ejemplo de su empleo se puede observar en la Figura 1.42, donde se puede notar que se usa principalmente para conexiones de computadoras personales y estaciones de trabajo. Además, tiene un alcance de 100 metros aproximadamente. Esta red trabaja con estándares IEEE 802.11 y sus variantes 802.11a, b, g.

**WMAN (Red de área metropolitana inalámbrica).** Estas redes fueron diseñadas para la interconexión de sistemas de una ciudad a otra, dentro de un país (Figura 1.43). Esta red tiene una velocidad de transmisión de 1.5 Mbps a 2.4 Gbps y un área geográfica de 100 a 1000 km; ya que la red debe ser muy extensa tiene un alto costo de transmisión, con lo cual, usualmente se implementa entre redes públicas para disminuir costos, aunque esto presenta problemas de seguridad en la información que se trasmite en la red.

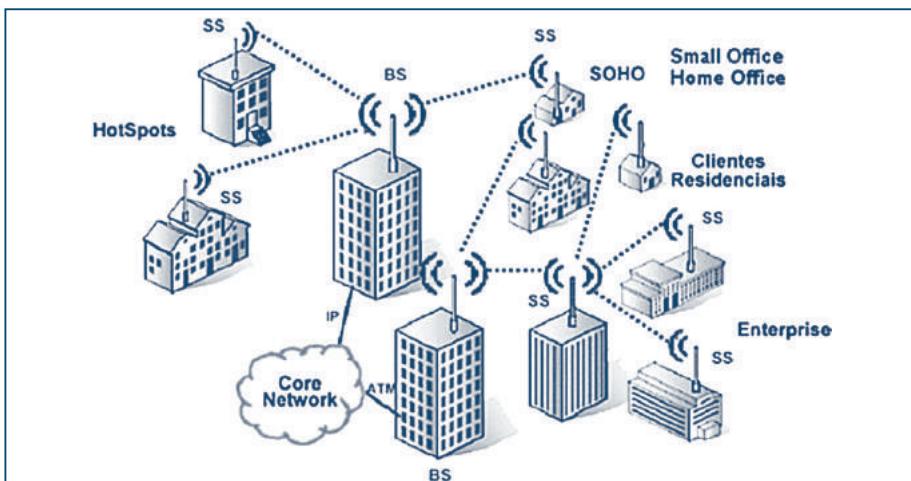


Fredys A. Simanca H., Fabián Blanco Garrido, Eduardo Triana Moyano



*Figura 1.42* Red WLAN, comunicación entre diferentes dispositivos de áreas diferentes.

Fuente: 34t (2016).



*Figura 1.43* Red inalámbrica metropolitana.

Fuente: Teleco (2016).



**WWAN (Red de área extensa inalámbrica).** Las redes inalámbricas tienen largo alcance mayor a las redes mencionadas anteriormente, por esta razón su infraestructura se utiliza para la telefonía móvil, con el fin de proporcionar un *roaming*<sup>14</sup> de conexión inalámbrica. La mayor ventaja de esta red es que el usuario puede estar conectado a esta, incluso si se está moviendo. En la siguiente Figura 1.44, se ve cómo han evolucionado las redes a través del tiempo, proporcionando una mayor transmisión de datos.

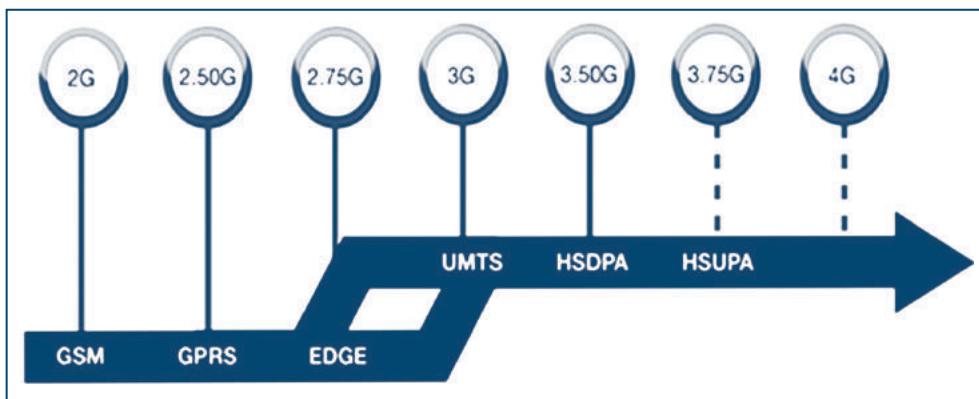


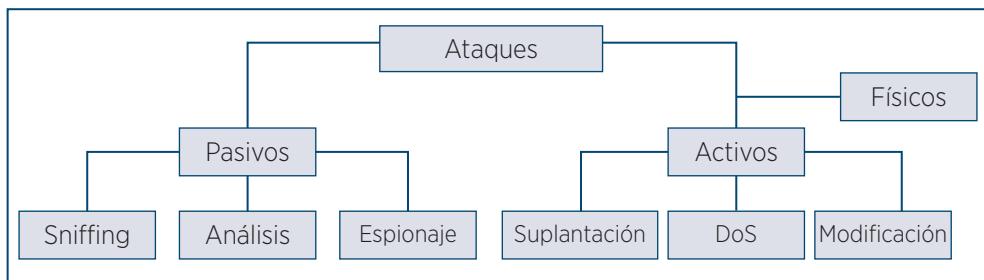
Figura 1.44 Tecnologías WWAN, evolución a través del tiempo.

Fuente: 1.bp.blogspot (2011).

## • 1.15 Ataques

Uno de los aspectos a tener en cuenta en las redes inalámbrica son los ataques informáticos, ya que pueden tener pérdida de información al estar conectados. A continuación, se hablará de los distintos ataques que pueden suceder como: monitorización, espionaje, intercepción de datos, intrusos en la red, interferencia radial, denegación de servicios, etc. En la Figura 1.45. Se advierten los diversos ataques que se pueden categorizar de tres formas: pasivos, activos y físicos.

<sup>14</sup> El *roaming* internacional para móviles es un servicio que permite a los usuarios continuar usando sus teléfonos móviles u otros dispositivos móviles mientras visitan otro país, para realizar y recibir llamadas de voz, enviar mensajes de texto, navegar por internet y enviar y recibir correos electrónicos.



*Figura 1.45 Ataques y amenazas en una red inalámbrica.*

Fuente: Uzcátegui (2012).

### Ataques pasivos

El principal objetivo de estos ataques es obtener información de un dispositivo que se haya conectado a la red y después de esto, atacar. Un ejemplo común real, es el hecho ocurrido en el 2010 por *Anonymous*, sobre el robo de documentos diplomáticos y confidenciales en Estados Unidos. Estos ataques se conocieron en la época como *Operation Avenge Assange*.

Se han registrado diferentes clases de ataques pasivos, entre los que se encuentran:

- **Sniffing.** Comprende técnicas para reunir información a través de las redes inalámbricas; se hace mediante un *sniffer*.

Un *sniffer* es un programa para monitorear y analizar el tráfico en una red de computadoras. Este puede ser visto de manera positiva, dado que cumple la función de monitoreo para capturar las tramas enviadas en una red y de esa forma puede analizar si existe información que viaja en la red en texto plano; esto es información sin cifrado.

Sin embargo, desde un punto de vista negativo, un *sniffer* puede convertirse en un instrumento peligroso si es manejado por personas con propósito de robo de información.

En las técnicas más utilizadas se encuentran *eavesdropping*, el cual hace un uso de una tarjeta o adaptador para redes inalámbricas que trabajan sobre el mismo rango y uso de la misma transmisión que emplean las redes

inalámbricas, permitiendo así que se pueda capturar el tráfico de transmisión sobre la red, como se puede notar en la Figura 1.46.

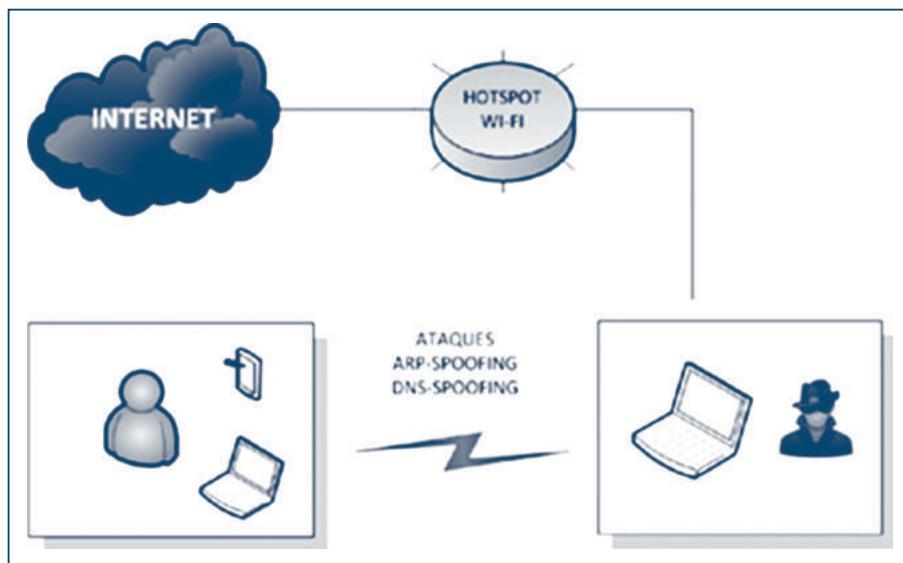


Figura 1.46 Ataque sniffing sobre una red inalámbrica.

Fuente: Arroyo (2011).

El *sniffer* pone a trabajar a la tarjeta de red del ordenador (donde está instalado) en un modo denominado “promiscuo”, el cual desactiva el filtro de verificación de direcciones y hace que la tarjeta “escuche” todos los paquetes y por lo tanto, todos los paquetes enviados a la red llegan a esta placa, no sólo los destinados a ella sino todos aquellos que se transmiten por la red (Goncalves, 1997, p.25).

*AirSnort* o *WEPCrack* son algunas de las herramientas utilizadas por los *sniffers* con capacidad de desencriptar claves de seguridad de las transmisiones inalámbricas y así, adquirir información legible para el atacante, el cual sólo lee y obtiene el mensaje sin atacarlo de vuelta.

#### ○ Análisis de flujo de tráfico

Consisten en monitorizar las transmisiones inalámbricas para lograr conocimiento minucioso sobre el diseño de red, como conocer el tipo de



usuario que hace uso de la red, información que puede ser accesible, averiguar la capacidad del equipo del cliente, entre otros.

Para que este ataque se pueda llevar a cabo, debe haber información reunida en el flujo de los mensajes difundidos entre los equipos, permitiendo que el atacante pueda revisar todos los mensajes, documentos y datos que han sido enviados, dando lugar a la realización de conexiones y analizando todo el contenido de estos, sin afectarlos y sin hacerles cambio alguno.

## Espionaje

También denominado *surveillance*, es el ataque más sencillo porque sólo consiste en observar el entorno donde se encuentra instalada la red inalámbrica para así, almacenar información. No necesita de *hardware* ni *software*, únicamente se genera el ataque teniendo acceso a la instalación.

## Ataques Activos

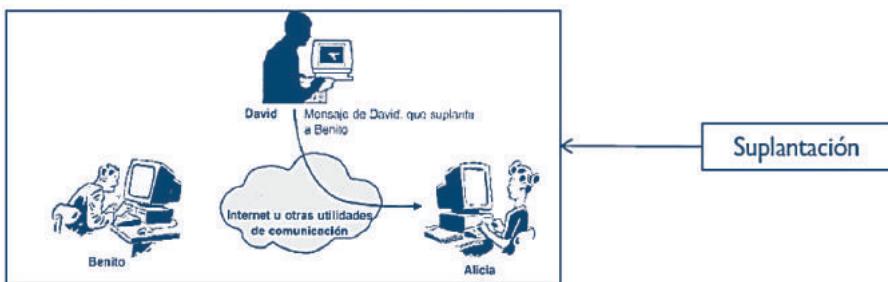
Este tipo de ataques van desde una alteración en el flujo de datos a la creación de falsos flujos en la transmisión de datos, con dos objetivos fundamentales que son:

- Pretender ser alguien que en realidad no se es.
- Colapsar los servicios que puede prestar la red.

Un ejemplo de este tipo de ataque, el cual se ha convertido en un hecho histórico, es el apagón del canal internacional francés TV5 Monde, ocurrido el viernes 10 de abril del 2015 por los hackers que utilizaron *phishing*, dejando completamente apagados los sistemas informáticos y abarcando desde cuentas de correo electrónico del equipo de producción hasta los servidores que se utilizan para transmitir la señal de televisión (Villacañas, 2015).

### O Suplantación

También llamado *spoofing*, consiste en ingeniar tramas TCP/IP utilizando una dirección IP falseada para llevar a cabo la usurpación de identidad de un usuario y/o servidor, con el propósito de adquirir información. Una forma esquematizada de esto se puede observar la Figura 1.47.



*Figura 1.47 Ataque mediante suplantación.*

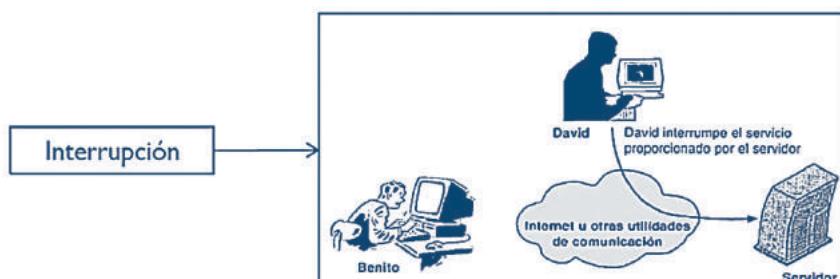
Fuente: Prieto (2012).

En este tipo de ataque es imprescindible que:

- Exista el atacante, el atacado y el sistema suplantado relacionado con el atacado.
- Por un lado, se establezca una comunicación falseada con el objetivo y por otro, se evite que el equipo suplantado interfiera en el ataque (Zona Virus, 2015).

## DoS

Traducido del inglés como: ataque de denegación de servicios o interrupción de servicios, consiste en denegar a los usuarios legítimos el uso de un servicio o recurso (ver figura 1.48). Es decir, que deja inutilizado el host en la red y hace que las conexiones que hasta el momento hubiera abiertas se ralenticen, de manera que se quedarán “colgadas” o serán desconectadas. Asimismo, también puede producir fallos en aplicaciones, sistemas, protocolos de red, servidores de web y de negocio.

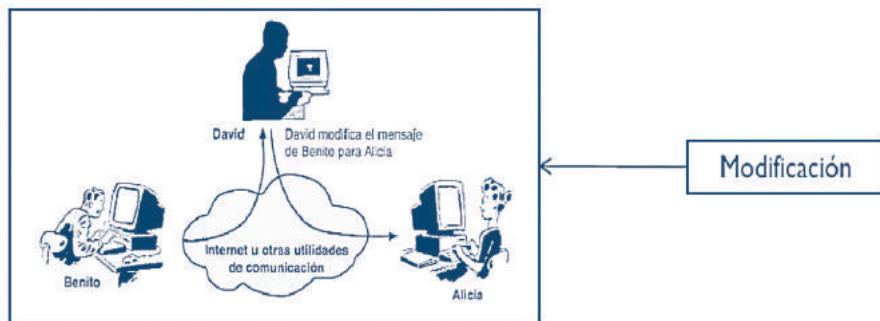


*Figura 1.48 Ataque mediante DoS.*

Fuente: Prieto (2012).

## ○ Modificación

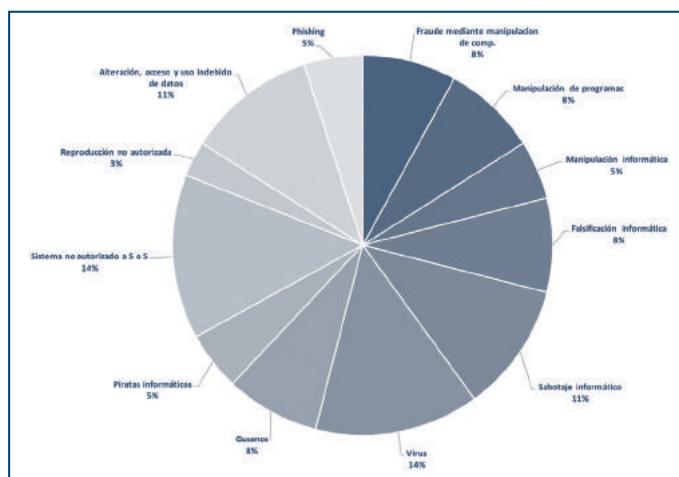
Como se muestra en la Figura 1.49, consiste en la alteración o anulación desautorizada de la información y/o *software* que se localiza, de alguna forma ya validada en computadoras y bases de **datos**. Por ejemplo, es muy común este tipo de ataque en **bancos** y casas de bolsa ya que inventan falsas cuentas para desviar fondos de cuentas ajenas.



*Figura 1.49* Ataque mediante modificación – daño.

Fuente: Wordpress (2012).

Para tener una idea sobre los delitos informáticos de la actualidad, se indican algunos de ellos en la Figura 1.50.



*Figura 1.50* Delitos informáticos.

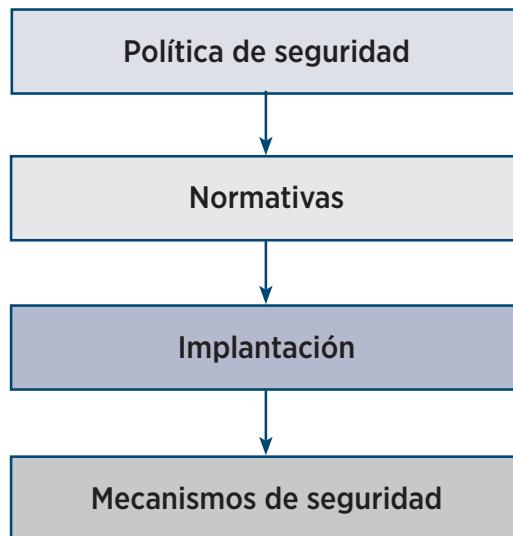
Fuente: Elaboración del grupo de investigación con información de Bustamante (2015).

## ○ Ataques físicos

El deterioro que padecen los elementos físicos (puntos de acceso, cables, antenas, adaptadores inalámbricos y *software*) propios de las redes inalámbricas para su buen funcionamiento, ocasiona restricción de la superficie de cobertura, disminución del ancho de banda o aumento en la inseguridad en la capacidad de los usuarios para acceder a los datos y a los servicios de información.

## ○ Estándares en la seguridad actual

En las redes inalámbricas existe gran variedad de terminologías y mecanismos de seguridad para las mismas, desde la instalación hasta la conectividad. A continuación (Figura 1.51) se presentan los mecanismos de seguridad para la instalación de redes inalámbricas:



*Figura 1.51* Mecanismos para la seguridad en redes inalámbricas.

Fuente: edgaracredes (2013).

En primer lugar, debe hacer un análisis de las amenazas que puedan ocurrir en el sistema de información, dando una estimación sobre lo que se pueda perder en esas amenazas para luego hacer un estudio de las posibilidades que ocurran. A partir de esto se hará un análisis para diseñar la



política de seguridad que se va establecer, reglas y responsabilidades para poder evitar la amenaza y minimizar los riesgos.

## • 1.16 Protocolos de seguridad

### 1.16.1 WEP (Wired Equivalent Privacy o Privacidad equivalente al cable)

Fue creado por inexpertos de la seguridad informática y es el precursor del protocolo de encriptación implantado en el estándar IEEE 802.11 alrededor de 1999.

Se fundamenta en el algoritmo de encriptación RC4, con una clave entre 40 a 104 bits, incorporada con un Vector de Inicialización (IV) de 24 bits para encriptar el mensaje de texto M y su checksum – el ICV (*Integrity Check Value*).

El mensaje encriptado C se determina utilizando la siguiente fórmula:

$$C = [M \parallel ICV(M)] + [RC4(K \parallel IV)] \quad (3)$$

Donde  $\parallel$  es un operador de concatenación y  $+$  es un operador XOR. Claramente, el vector de inicialización es la clave de la seguridad WEP.

Por supuesto, el IV debe ser aplicado a cada paquete para que los siguientes estén encriptados con claves diferentes<sup>15</sup>.

<sup>15</sup> Rodríguez Carlos y Calabuig Carlos. Auditoria WEP para las clases de REDES. Tomado de <https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCAQFjAAahUKEwi-veqlycDHAhXMJB4KHXPwCs&url=http%3A%2F%2Fwww.uv.es%2F~montanan%2Fredes%2Ftrabajos%2FSeguridadWEP.pps&ei=xnPaVb7CKszJePPgr9gO&usg=AFQjCNHxAvTqEbkapqFW5j13Czq3E5PlhA>, consultado el día 31 de mayo del 2015.



Fecha	Descripción
Septiembre 1995	Vulnerabilidad RC4 potencial (Wagner)
Octubre 2000	Primera publicación sobre las debilidades de WEP: Insegura para cualquier tamaño de clave; análisis de la encapsulación WEP (Walker)
Mayo 2001	Ataque contra WEP/WEP2 de Arbaugh
Juio 2001	Ataque CRC bit flipping - Intercepting Mobile Communicationsd: The Insecurity of 802.11 (Borisov, Goldberg, Wagner).
Agosto 2001	Ataques FMS - Debilidades en el algoritmo de programación de RC4 (Fluhrer, Mantin, Shamir)
Agosto 2001	Publicación de Air Snort
Febrero 2002	Ataques FMS optimizados por h1kari
Agosto 2004	Ataques KoreK (IVs únicos) - publicación de chopchop y chopper
Julio/Agosto 2004	Publicación de Aircrack (Devine) y WepLab (Sánchez, poniendo en práctica los ataques KoreK

Fuente: Lehembre (s.f.).

Ventajas	Desventajas
Clave secreta compartida por todos los comunicadores, que se emplea para cifrar datos enviados.  Da protección a las redes inalámbricas en los estándares IEEE 802.11, con el fin de garantizar compatibilidad entre distintos fabricantes.  WEP proporciona un nivel de seguridad aceptable sólo para usuarios domésticos y aplicaciones no críticas	En la actualidad, todas las estaciones y puntos de acceso comparten una misma clave, lo que reduce el nivel de seguridad que puede ofrecer este sistema.  El IV es transmitido en texto simple, y el estándar 802.11 no obliga a la incrementación del IV, dejando fácil su acceso.  Los bytes iniciales del flujo de clave dependen de tan sólo unos pocos bits de la clave de encriptación. No ofrece servicio de autenticación. Existen varias herramientas que rompen su clave.

## 1.16.2 Acceso protegido WI-FI (WI-FI Protected Access WPA)

Fue creado por la WI-FI Alliance en 2003. Tiene su origen en los problemas detectados en el anterior sistema de seguridad (WEP) y fue creado como solución temporal mientras que en IEEE se trabajaba sobre el estándar IEEE 802.11i (WPA2). Este protocolo requiere un cambio de *hardware*.



WPA reparte mejor el movimiento de claves, utilizando el vector de inicialización, dando lugar a la encriptación de tráfico de datos e incluye las siguientes tecnologías:

IEEE 802.1X. Estándar del IEEE de 2001 para proporcionar un control de acceso en redes basadas en puertos.

Protocolo de Autentificación Extensible (EAP). Realiza el reconocimiento, autorización y contabilidad.

TKIP (*Temporal Key Integrity Protocol*). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave dinámica para cada trama, lo que mejora notablemente el cifrado de datos, incluyendo el vector de inicialización.

MIC (*Message Integrity Code*) o Michael. Código que verifica la integridad de los datos de las tramas.

También tiene dos sistemas de control de acceso:

- WPA – PSK (*Pre-Shared Key*).
- Sistema de control de acceso más simple.
- Consiste en un sistema de clave compartida, formada entre 8 y 63 caracteres. Es un sistema fácil de utilizar y configurar y el más recomendable para entornos familiares o pequeñas empresas.

### 1.16.3 WPA Enterprise Sistema más complejo

La adoptan aquellas empresas que hacen uso de las redes inalámbricas. Funciona mediante el uso de usuario y contraseña o sistemas de certificados.

Ventajas sobre WEP:

- Una clave de encriptación diferente en cada paquete. El mecanismo TKIP (Protocolo de Integridad de Clave Temporal) comparte una clave inicial entre equipos. Cada equipo cambia entonces su clave de encriptación para cada paquete. Es extremadamente difícil para los *hackers* poder leer los mensajes, incluso si han interceptado los datos.



Ventajas	Desventajas
<p>Proporciona gran seguridad inalámbrica.</p> <p>Añade autenticación a la encriptación WEP básica.</p> <p>Ofrece apoyo técnico a WEP antiguo para equipos que no están actualizados.</p> <p>Se integra con los servidores RADIUS para permitir administración, auditoría y registro.</p> <p>Parte de la configuración recomendada es un Servidor de Autoridad de Certificación, para asegurar a las computadoras con WPA que las computadoras con quienes comparten las claves son quienes dicen ser</p>	<p>El firmware antiguo no se actualizará para servir de soporte.</p> <p>Incompatible con anteriores sistemas operativos tales como Windows 95.</p> <p>Mayor costo de rendimiento que el WEP.</p> <p>Vulnerabilidad a los ataques de DoS (Denegación de Servicio).</p> <p>Como WPA es añadido al tamaño del paquete, la transmisión tarda más.</p> <p>La encriptación y desencriptación son más lentas para equipos que usan software WPA en vez de hardware WPA.</p> <p>Se puede identificar por medio del uso de la fuerza bruta, es decir, ir comprobando distintas claves hasta dar con la correcta, de ahí que sea fundamental utilizar claves complejas alfanuméricas</p>

- La Autenticación del Certificado (CA) se puede usar para bloquear el acceso de un *hacker* que se hace pasar por un usuario.

#### 1.16.4 WPA2 (Protocolo 802.11i)

Es el acrónimo de WI-FI Protected Access versión 2 y consiste en la versión certificada y mejorada que cumple el estándar 802.11i. Se difundió en septiembre 2004 por la Wi-Fi Alliance. Este protocolo fue creado para solucionar los problemas de vulnerabilidad detectados en la primera versión (WPA) e incorporar todas las características del estándar IEEE 802.11i que WAP no hacía.

Presenta un destacado cambio respecto a WPA: reemplaza el algoritmo RC4 por el algoritmo AES, uno de los más seguros actualmente.



Ventajas	Desventajas
WLAN más seguras. Reemplazo del algoritmo RC4 por el algoritmo AES. Puede utilizarse en el hogar y/o en las grandes empresas. Incorpora los métodos de autenticación y el cifrado WPA. Su cifrado se realiza por paquetes, por consiguiente, emplea una clave para cada paquete.	Tiene el inconveniente de que no todos los routers permiten este tipo de cifrado, además de no ser compatible con el sistema WAP. No es compatible con las tarjetas de red más antiguas. Se le puede hacer "fuerza bruta" que consisten en ingresar, a través de un software, un diccionario completo de posibles keywords, esperando acertar a la correcta

### 1.16.5 Secure Shell (SSH)

El protocolo SSH fue impulsado en 1995 por el finlandés Tatu Ylönen. Más tarde se patentó la marca SSH y se estableció la empresa *SSH Communications Security* con propósito comercial, la cual permitía el uso del protocolo gratuitamente para uso doméstico y educativo. Esto ocasionó que los creadores del sistema operativo OpenBSD empezaran a desarrollar en 1999 una versión libre de este protocolo, que recibió el nombre de OpenSSH.

Posibilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor que permite a los usuarios conectarse a un *host* de forma remota. A diferencia de otros protocolos de comunicación remota, tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

Posee confidencialidad SSH, la cual se obtiene mediante el cifrado para comunicar datos y/o información. Y añade el servicio de confidencialidad a la identidad del usuario. Por otra parte, autentifica la identidad del ordenador servidor como el usuario que se quiere conectar, lo cual se suele hacer a la vez con el intercambio de claves. Finalmente, realiza la autenticación del mensaje; con respecto al SSH2, la autenticidad de los datos se garantiza cuando a cada paquete se le añade un código MAC calculado con una clave secreta.

Su eficiencia se evidencia en que:



- Haciendo referencia al SSH, comprende los datos intercambiados para reducir la longitud de los paquetes.
- Mientras que en SSH2 permite negociar el algoritmo que se utilizará en cada sentido de la comunicación, este algoritmo es compatible con el que utilizan programas como gzip (RFC 1950-1952).
- Permite extensibilidad.
- El SSH2 negocia algoritmos de cifrado, de autentificación de usuario, de MAC, de compresión y de intercambio de claves.

Ventajas	Desventajas
Reducción de ataques a su seguridad, cuando es usado para inicios de sesión de Shell remota y para copiar archivos.	Dificultad para admitir acceso anónimo al repositorio.
El cliente SSH y el servidor usan firmas digitales para verificar su identidad.	Obligatoriedad de tener configurado el acceso SSH al servidor, pese a que sea con permisos de solo lectura.
La comunicación entre los sistemas cliente y servidor es encriptada.	La emisión de comunicación entre cliente y el servidor se realiza completamente en texto plano (sin cifrar), por lo que con cualquier sniffer puede capturar contraseñas.
Paquete cifrado por medio de una llave conocida sólo por el sistema local y el remoto, con lo que quedan inutilizados los intentos de falsificación de identidad.	Modificación no sustentada de contraseñas, ni certificados de claves públicas.

### 1.16.6 Secure Sockets Layer (SSL)

Se trata del protocolo de seguridad de la capa de transporte, se diseñó para permitir a las aplicaciones trasmítir información de ida y regreso de manera segura, utilizando protocolos criptográficos. Este estándar se desarrolló por Netscape, sus colaboradores más cercanos fueron Mastercard, Bank of America, MCI y Silicon Graphics. El método protocolo SSL se basa en cifrado de claves públicas, el cual el cifrado entre dos equipos (cliente, servidor) se establece en un canal de comunicación seguro después de tener una autentificación.

Este sistema es independiente del protocolo que se utiliza, asegura las transacciones que se realicen a través de la web de protocolo HTTP y también otras conexiones con protocolos IMPA, FTP y POP. El protocolo SSL funciona con una capa adicional, la cual permite garantizar la seguridad de datos y se ubica entre la capa de aplicación y la de transporte.



- Proporciona métodos criptográficos que proporcionan integridad y confidencialidad entre redes de comunicación TPC/IP.
- Protege las conexiones entre cliente y servidores web mediante protocolo HTTP.
- Numeración de registros con un número de secuencia y el número generado en los códigos de autenticación de mensajes (MAC).
- Con un protocolo apoyado en firmas digitales, el cliente puede confirmar la identidad al servidor.
- Protege la comunicación end-to-end.
- El diseño del protocolo se realizó para que cualquier aplicación que lo implementara utilizase TPC a través de los llamados de sockets, solamente cambiando estas llamas para la utilización del protocolo SSL.
- La definición de sesiones y compresión de datos permite mejorar la eficiencia de la comunicación.
- El protocolo es extensible, ya que deja abierta la posibilidad de que se añadan nuevos algoritmos, si son más eficientes y seguros, al momento del intercambio de claves, autenticación y cifrado, para utilizar algoritmos criptográficos.

Ventajas	Desventajas
<p>SSL encripta los datos que son enviados y recibidos por el cliente al servidor, por lo cual, es seguro.</p> <p>Proporciona una comunicación, confidencial (cifrado criptográfico), integridad (mediante la capa HMAC), autenticidad de servidor (cliente-servidor) y protocolos de seguridad en el comercio electrónico.</p> <p>Se puede evitar que los sitios web donde se utiliza este protocolo, tengan una infraestructura de claves tanto pública como certificada por el SSL de un proveedor fiable.</p> <p>Aporta seguridad durante la transmisión de datos. Es transparente para el usuario. No se requiere de muchas modificaciones en los programas que se utiliza.</p> <p>Aumenta la confianza de los clientes gracias a los certificados que tiene SSL para empresas, brindando confianza si hay la pérdida de datos.</p> <p>Eliminación de malware de la web, escaneando los sitios buscando programas que puedan dañar el sistema o que puedan robar información</p>	<p>El uso del certificado SSL es costoso.</p> <p>Para la utilización del protocolo se requieren más recursos del servidor, cuando la información enviada es cifrada</p>



## 1.16.7 Protocolo Seguro de Trasferencia de Hipertexto (HT-TPS)

Este protocolo de aplicación basado en HTTP se destinó para la trasferencia segura de datos de hipertexto y se utiliza sobre todo para entidades bancarias, tiendas de ventas en línea, y servicios que requieran envío de datos personas y/o contraseñas. Este sistema utiliza cifrados de nivel servidor remoto y del navegador utilizado por los clientes, este protocolo logra desarrollar e-commerce, permitiendo realizar transacciones de forma segura. Se trata de un modelo de negocio confiable para la economía.

Para crear un canal de transferencia cifrado, se debe aumentar la seguridad en el tráfico de información teniendo en cuenta los siguientes aspectos:

- Protocolo de comunicación estándar, el cual comunica servidores, proxys y clientes, permitiendo transferir documentos web, sin la importancia de cuál es el servidor o el cliente.
- Este protocolo se basa en el esquema de petición-respuesta.
- En el envío de mensajes de petición hacia un servidor, el servidor contesta con un mensaje de respuesta cuyo contenido es función de la petición que realizó el cliente.

Ventajas	Desventajas
Se pueden hacer repositorios de sólo lectura, teniendo trasferencias encriptadas.	La protección depende de la implementación del navegador web, el algoritmo de cifrado y el software del servidor.
El protocolo permite codificar el certificado digital en la sección que se inicie.	Cuando son contenidos estáticos de publicaciones disponibles son vulnerables.
Usa un control de acceso para clientes con el propósito de limitar el acceso	El sitio web puede ser indexado con el uso de una araña web, y URI del recurso cifrado, con lo cual el cifrado puede ser adivinado conociendo el tamaño de la petición/respuesta



### 1.16.8 Protocolo de Túnel punto a punto (Point to point Tunneling Protocol PPTP)

Este protocolo fue desarrollado por el colectivo (Microsoft, Robotics, Asced Communications, 3Com/Primart Access, ECI Telematics), el cual lo utilizó para redes privadas virtuales o VPN. Este protocolo encapsula paquetes PPP (*Point to Point Protocol*) de datagramas IP para transmitir bajo redes TCP/IP. Esta tecnología hace viable tener un acceso remoto del PPP, permitiendo trasferencia segura de datos bajo un equipo remoto a un servidor privado, al momento de crear una conexión de red virtual privada.

El protocolo PPTP agrega un nuevo nivel de seguridad y de comunicaciones multiprotocolo a través de internet. En la Figura 1.52 se estudia el diagrama de un protocolo.

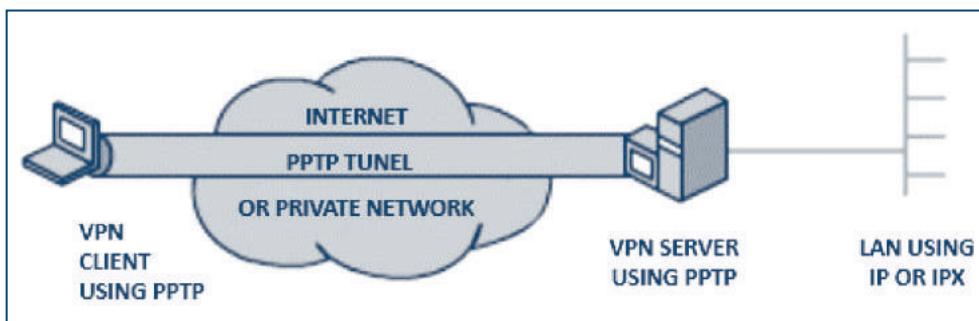


Figura 1.52 Diagrama de protocolo PPTP Microsoft.

Fuente: Microsoft.com

- Permite acceder a las redes de forma segura y remota a través de internet y una red privada virtual.
- Los datos se pueden encapsular en datagramas IP.
- Los datos son cifrados a través de IP.
- El protocolo PPTP está basado en PPP y GRE (*Generic Routing Encapsulation*)
- Conexión rápida, básica y con una seguridad alta. Esta puede ser utilizada en computadores de escritorio, portátiles, tablets, smartphones, etc. Realiza una encriptación de 128 bits.



Ventajas	Desventajas
Es fácil, sencilla y rápida la configuración y utilización.	La seguridad es más baja a comparación con L2TP.
Los datos son encriptados sin IPsec, por lo que no es necesario tener instalación de certificados de equipo con infraestructura de clave pública.	No proporciona una integridad de datos.
La plataforma que soporta es de Windows y soporta plataformas con servidores PPTP	Puede tener problemas de rendimiento cuando las redes son inestables. Dado que está montando en sistemas de Microsoft, tiene más fallas en la implementación del protocolo. La versión de 40 Bytes es muy débil y la clave de usuario es basada en la clave de la seguridad.

## • Conclusión

Las redes MESH están reguladas al nivel internacional y nacional. El ente que regula estas redes en Colombia es el MinTIC. La primera generación de redes MESH se caracteriza por contar con un solo radio para realizar la interconexión entre nodos y ofrecer el servicio, en la segunda, se combinan dos radios, uno para ofrecer el servicio, y otro para interconectar los nodos. La tercera generación supera las dos anteriores, al utilizar multiples configuraciones de red de recepción y envío de datos con diversos canales. El sentido social de las redes, se agrupa en el conjunto de beneficios de licencias libres para usuarios, en ámbitos académicos como colegios y universidades. El Plan Vive Dígital concebido como la ruta que integra infraestructura, servicio, aplicación y usuarios, pretende reducir la brecha digital en Colombia, al proyectar conectividad a por lo menos el 40% de los municipios del país a 2018.



( 2 )

## Distribución y acceso a los servicios inalámbricos MESH para los estratos menos favorecidos

### • Introducción

Partiendo del principio de una sociedad inclusiva, el uso eficiente de las TIC se convierte en un potenciador que favorece la población menos privilegiada al masificar tecnologías a bajo costo. Para lograr ese propósito, se presenta sistemáticamente la forma de construir y diseñar una red MESH, a partir de los modelos de conectividad. Así mismo, se tiene en cuenta la confiabilidad que surge de la formalización matemática. El soporte lógico de comunicaciones se basa en el alistamiento para la prestación del servicio en términos de transmisión de onda SSBFC y transmisión con modulación angular. En cuanto al soporte de modulación, se operan moduladores directos, indirectos, transmisores directos, estabilizadores puros y transmisores FM con fase cerrada.

### • 2.1 Diseño y construcción ingenieril

Se presentan en este capítulo las principales operaciones que enmarcan las redes MESH, se describe su andamiaje y estructura paramétrica de enlaces, señalando su infraestructura de conectividad y categorizando sus servicios como ejes de inclusión social, a la luz del plan de masificación de las tecnologías de la información y las comunicaciones que son la plataforma de desarrollo en el gobierno actual.



## 2.1.1 Modelos de conectividad

Los sistemas de interconexión teleinformática catalogan su funcionalidad, integrando mecanismos de operación y unidades modulares de interfaces de cuatro formas especiales, las cuales son:

- Modelo o arquitectura por capas.
- Arquitectura basada en objetos.
- Modelo centrado en datos.
- Arquitectura basada en eventos.

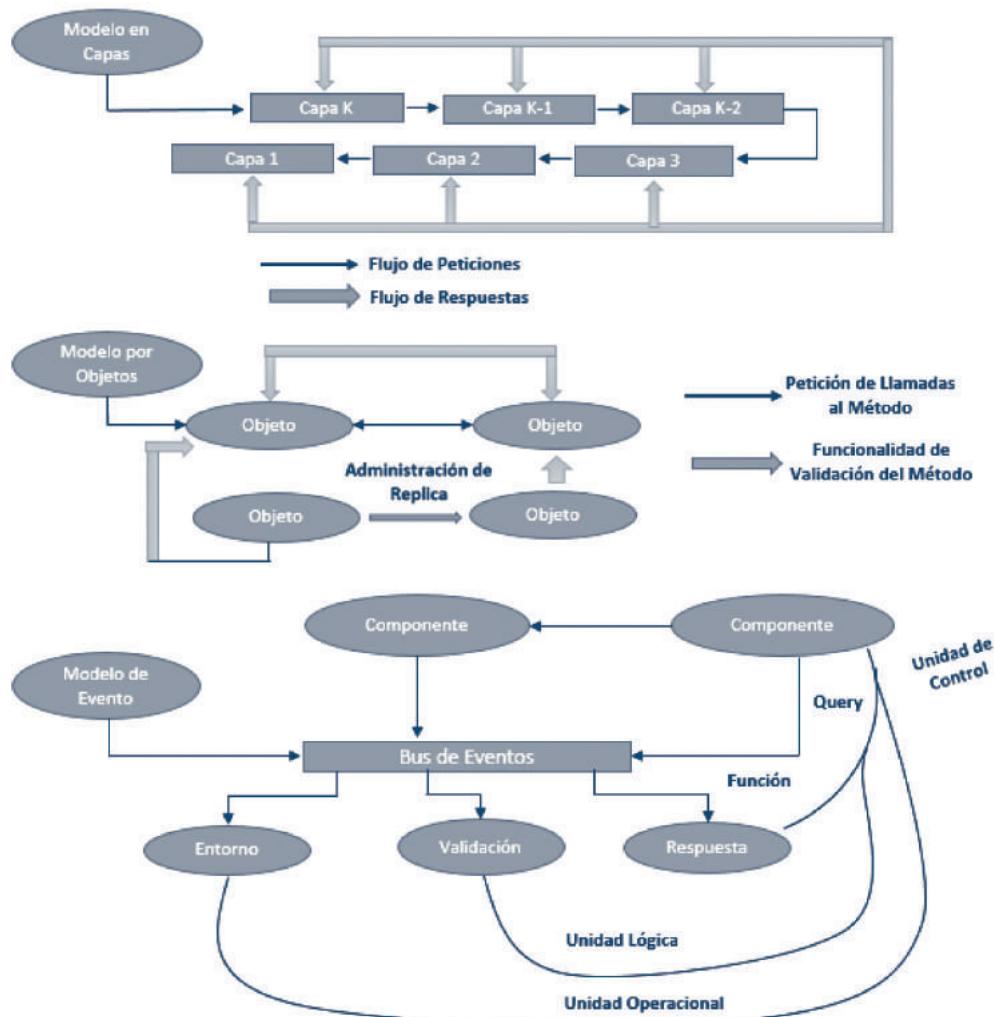
Estas arquitecturas, señalan los procesos de enlace y los nodos, tal como se demuestra en la Figura 2.1. La interpretación funcional de la interconexión jerarquizada por estas arquitecturas, define las características propias del nodo escenario multinivel (Umar, 2007), es decir, al cliente que orienta el proceso de interfaz del usuario y el servidor que operacionaliza los programas para el procesamiento y acceso a la información. De esta manera se puede validar cómo, en todo sistema orientado al intercambio transaccional, se integran tres grandes niveles, a saber:

- Interfaz de usuario.
- Procesamiento.
- Datos.

En los canales se integran estos componentes:

- Generación de consulta.
- Bases de datos.
- Catalogadores de información.
- Algoritmos de ordenamiento.
- Algoritmo de despliegue.
- Algoritmo de transmisión/recepción.
- Algoritmos de visualización y control.
- Algoritmo de implementación de interfaces.

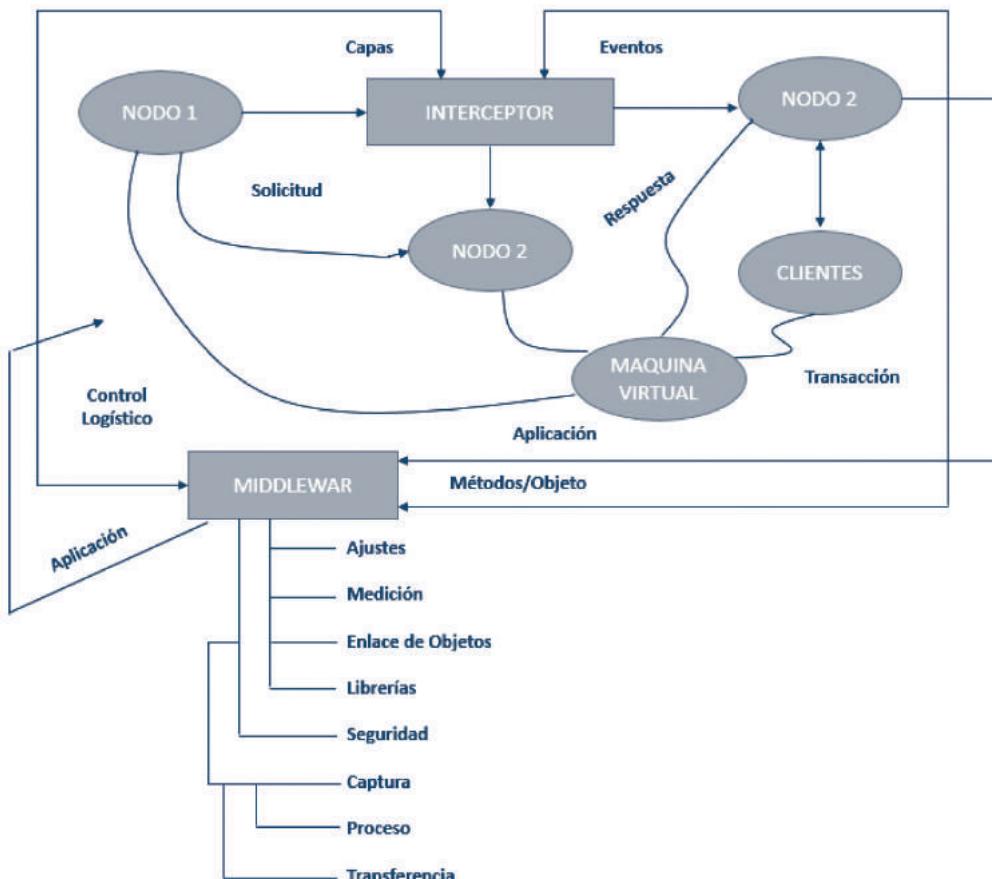
El concepto de interceptor permite evaluar una entidad lógica de *software* que interrumpe el flujo nominal, habilitando la ejecución de otra transacción o código al operar, llamados o interfaces o métodos catalogados, los



*Figura 2.1* Modelos de conectividad

Fuente: Elaboración del grupo de investigación

cuales, básicamente se resumen en el proceso de hilos y en la activación de máquinas de estado finito, cuyo engranaje funcional (Figura 2.2) y especificación lógica (Figura 2.3) se señalan a continuación.

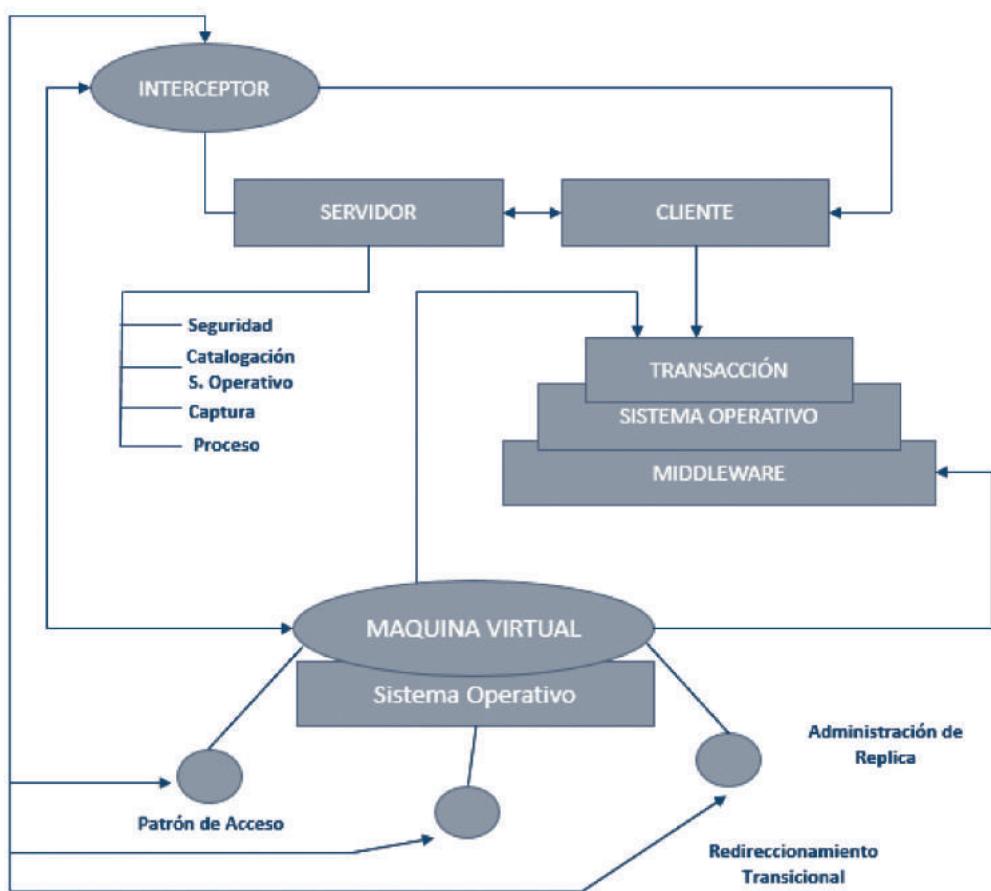


**Figura 2.2** Catalogación de interceptores.

Fuente: Elaborado por el grupo de investigación

Técnicamente, la conectividad queda determinada por la acción de las normativas validadoras del flujo, especificación y control, que se asocian genéricamente como protocolos, cuya manipulación permite catalogarlos en:

- Protocolo de nivel básico.
- Protocolo de transporte.
- Protocolo de alto nivel.
- Protocolo middleware.
- Protocolo de enlace remoto (RPC).



*Figura 2.3 Especificación lógica del interceptor.*

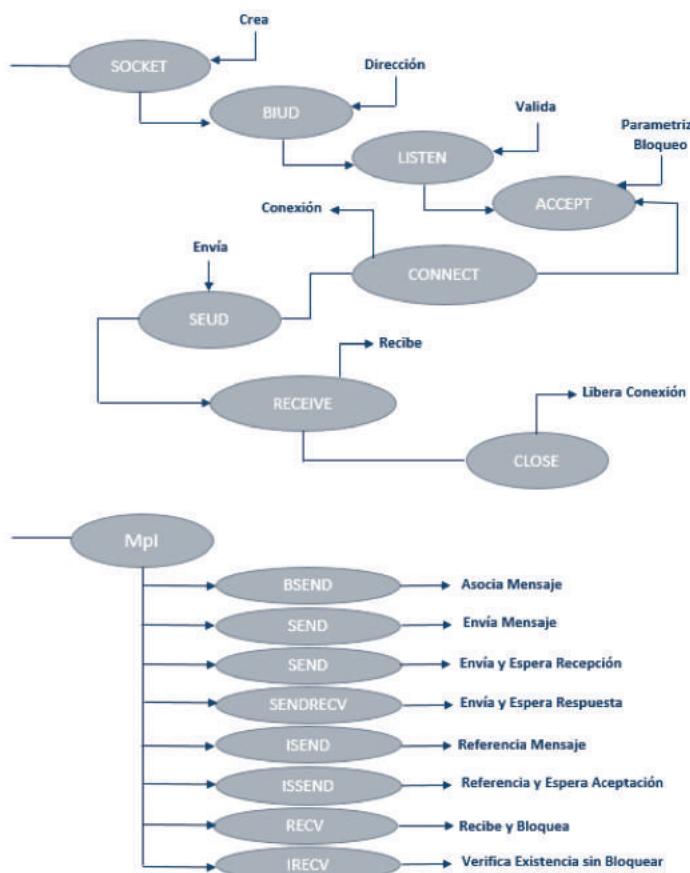
*Fuente:* Elaborado por el grupo de investigación.

Por su estructura lógica e importancia para el núcleo operacional del trabajo, se procede a registrar las fases del RPC:

- El procedimiento cliente enlaza al resguardo.
- El resguardo llama al sistema operativo local.
- Se cataloga sesión local con el sistema operativo remoto.
- El sistema operativo remoto encadena al resguardo del servicio.
- El resguardo fragmenta y parametriza la transacción.
- Se ejecuta solicitando y se envía por la línea.

- g) Se produce diálogo RPC-Local y se procede a catalogar el envío de la transacción.
- h) El sistema operativo del cliente ejecuta estas operaciones:
  - Validación integridad neutral.
  - Parametriza estructura: demonio.
  - Retorna señal de aceptación al RPC (remoto).
  - Despliega resultados.

Las operaciones anteriores, se refieren al interpretar el concepto formal de un *socket* y al validar la interface de paso de mensajes (MPI), cuyo contenido se visualiza en la Figura 2.4.



*Figura 2.4* Base de primitivas de socket TCP/IP.

Fuente: Elaborado por el grupo de investigación.



Todo sistema de conectividad valida con jerarquía, los requerimientos de calidad de servicio (QoS) al operacional el flujo transaccional (Narasimhan y Moser, 2004), garantizando el control y supervisión de los siguientes factores:

- Velocidad de transporte.
- Retraso máximo.
- Variancia por retraso.
- Tipo de reenvío.
- Sincronización.
- Diseminación de datos.
- Multitransmisión.
- Estiramiento.

El modelo de conectividad, define formalmente los ejes funcionales aquí citados:

- Procesos.
- Comunicación:
  - Validación cliente/objeto.
  - Enlace RPC.
  - Paso de paramétrica.
  - Operación de mensajes.
- Referenciarion de nombres.
- Sincronización.
- Consistencia y replicación.
- Tolerancia o fallas.
- Seguridad.

## 2.1.2 Confiabilidad en las redes MESH

Matemáticamente, la confiabilidad de un sistema en el tiempo  $t$ , está definido por:

$$R(t) = P(T > t) \quad (4)$$

$t$  = tiempo de control

$T$  = duración del sistema en óptimas condiciones



$R(t)$  = función de confiabilidad

$$R(t) \int_t^{\infty} F(s) ds \quad (5)$$

$$F(t) = \frac{1}{\sqrt{1\pi\theta}} e^{(\frac{1}{2}[\frac{t-\mu}{\theta}]^2)} \quad (6)$$

$$F(t) = \text{conducta de la falla} \quad (7)$$

Consideraciones que permiten establecer la confiabilidad de sistema en serie y paralelo (Meyer, 1999) según se expresa aquí:

- Sistema en serie

$$\begin{aligned} R(t) &= R_1(t) * R_2(t) * R_3(t) * \dots * R_n(t) \\ R(t) &= e^{-\alpha_1 t} * e^{-\alpha_2 t} * e^{-\alpha_3 t} * \dots * e^{-\alpha_n t} \\ R(t) &= e^{-(\alpha_1 + \alpha_2 + \alpha_3 + \dots + \alpha_n)t} \end{aligned} \quad (8)$$

$$T(f) = \frac{1}{R(t)} = \text{tiempo esperado de falla}$$

- Sistema en paralelo

$$\begin{aligned} R(t) &= 1 - [1 - R_1(t)][1 - R_2(t)][1 - R_n(t)] \\ R(t) &= 1 - [1 - R(t)]^N \end{aligned} \quad (9)$$

Que al operacionalizar para  $N=2$ , se tiene

$$\begin{aligned} R(t) &= R_1(t) + R_2(t) - R_1(t)R_2(t) \\ R(t) &= e^{-\alpha_1 t} + e^{-\alpha_2 t} - e^{-T(\alpha_1 + \alpha_2)} \end{aligned} \quad (10)$$



El tiempo de fallo, se expresa así

$$T(F) = \frac{1}{\alpha_1} + \frac{1}{\alpha_2} - \frac{1}{\alpha_1 + \alpha_2}$$

$$T(F) = \frac{\alpha_1 + \alpha_2}{\alpha_1 \alpha_2} - \frac{1}{\alpha_1 + \alpha_2} \quad (11)$$

$$T(F) = \frac{\alpha_1^2 + 2\alpha_1\alpha_2 + \alpha_2^2 - \alpha_1\alpha_2}{(\alpha_1\alpha_2)(\alpha_1 + \alpha_2)}$$

$$T(F) = \frac{\alpha_1^2 + \alpha_1\alpha_2 + \alpha_2^2}{\alpha_1^2\alpha_2 + \alpha_1\alpha_2^2} \quad (12)$$

Expresiones, cuyo comportamiento, se ajustan a la curva señalada por la Figura 2.5, curva que registra estos parámetros:

$R(t)$  = función de confiabilidad

$T$  = Intervalo de medida de tiempo

$E$  = Espacio de medida

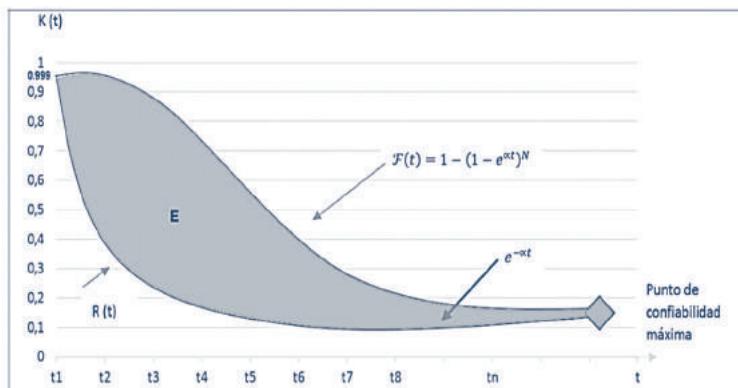


Figura 2.5 Parametrización Gráfica  $R(t)$ .

Fuente. Elaborado por el grupo de investigación.



Al considerarse el interior de las redes MESH, la función de confiabilidad dimensiona tanto el principio de atomicidad como el principio de funcionalidad (Kopetz, 2008), que involucran el análisis de estos parámetros:

- Disponibilidad: probabilidad de que el sistema opere correctamente en un instante de tiempo dado
- Confiabilidad: propiedad que hace que la red MESH, funcione de manera continua sin fallar.
- Seguridad: parámetro que dimensiona en la red MESH la no ocurrencia de algún evento desastroso, cuando la red deja de funcionar por causa de algún evento, amenaza o ataque.
- Mantenimiento: factor de medida del nivel de facilidad para reparar la MESH, cuando se evidencia alguna falla.

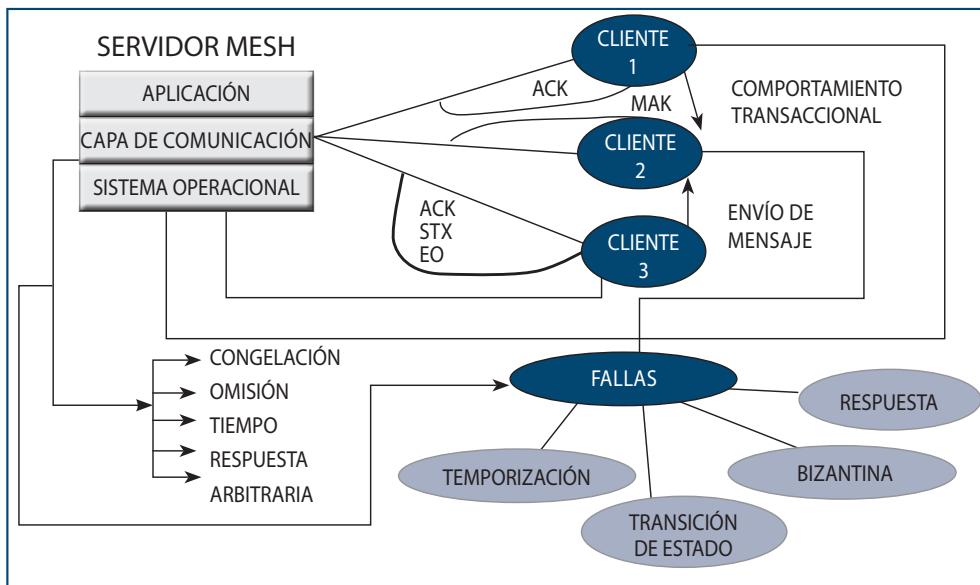
La red MESH puede, según características técnicas, mostrar los siguientes tipos de falla (Cristian y Fetzer, 1998):

- Congelación
- Omisión: recepción y envío.
- Tiempo
- Respuesta: valor y transacción de estado.
- Arbitraria: falla endógena por evento propio de la arquitectura.

La operación de la red MESH estructura el proceso de interacción remota (RPC), la manipulación de los casos o categorías de fallas, a saber:

- La estación cliente no enlaza al servidor al no poder localizarlo.
- El mensaje enviado por el cliente nunca llega al servidor.
- El servidor falla al capturar la petición transaccional enviada.
- La respuesta generada por el servidor no puede ser capturada en la estación cliente.
- La estación cliente se congela o falla después de reconocer al servidor y enviar una transacción o solución.

Eventos pertinentes la consideran propia del protocolo de Multitransmisión confiable escalable (SRM), para abordar el conocido problema de Multitransmisión atómica<sup>55</sup>, lo que se puede interpretar al ver la Figura 2.6.



*Figura 2.6 Catalogación de la Multitransmisión en Redes MESH.*

Fuente: Elaborado por el grupo de investigación.

Debe tenerse presente que, la operacionalidad MESH conlleva o implementa las siguientes versiones de multitransmisión (Hádzilacos y Toueg, 2008).

- Multitransmisión confiable.
- Multitransmisión FIFO.
- Multitransmisión casual.
- Multitransmisión atómica.
- Multitransmisión atómica FIFO.
- Multitransmisión atómica casual.

La operacionalidad en el entorno de la confiabilidad de toda red MESH, implica la consideración funcional de dos importantes protocolos, a saber:

- Protocolo de realización bifásico (2pc) 56Two Phase Commit Protocol.
- Protocolo de realización trifásico (3pc) 57Theer Phase Commit Protocol.

Su comportamiento estructural se observa en la Figura 2.7, la cual registra la especificación de las correspondientes máquinas de estado finito.

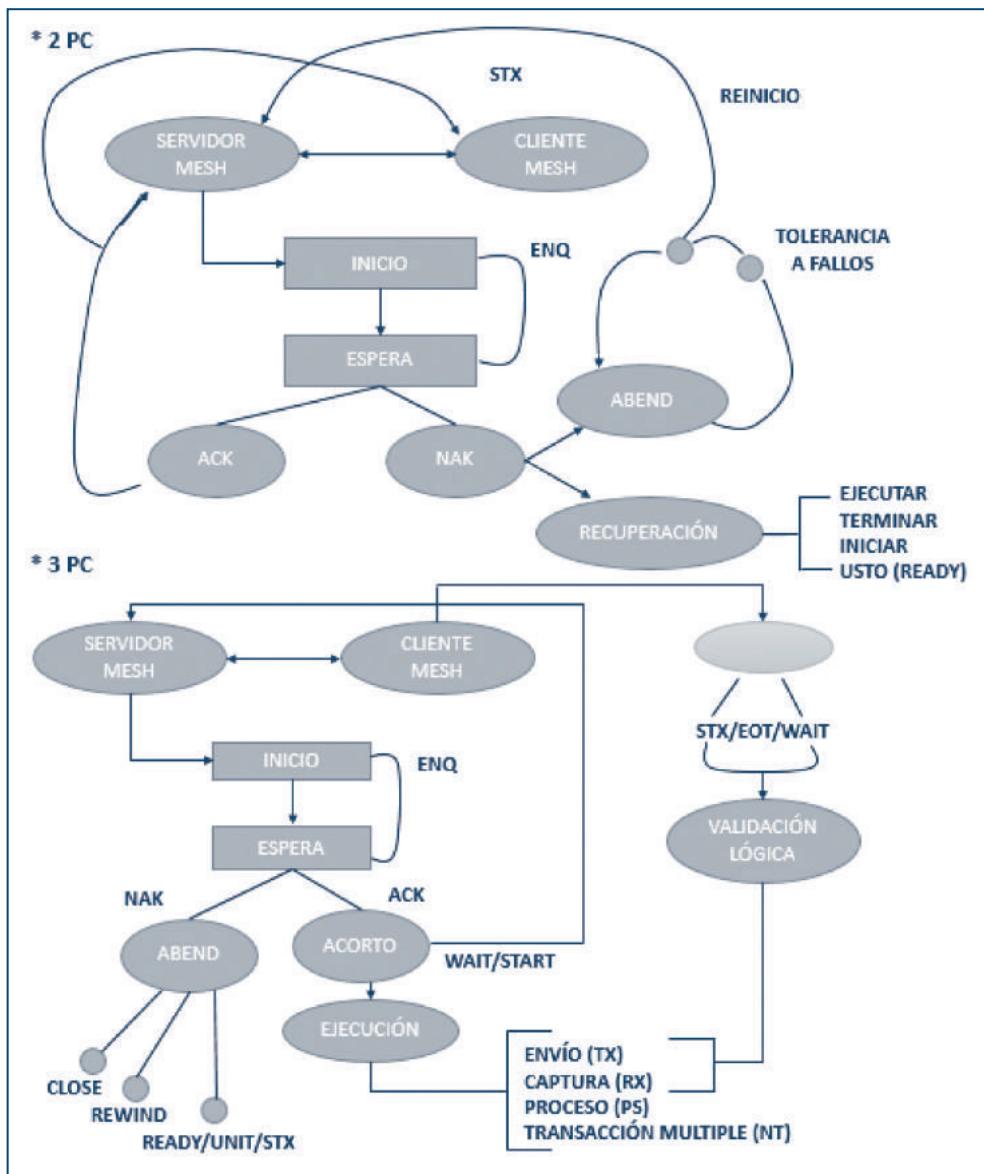


Figura 2.7 Formalización 2PC/3PC.

Fuente: Elaborado por el grupo de investigación.

El desarrollo tecnológico ha permitido que las redes MESH estén configuradas para operar en el entorno de la computación orientada a la recuperación (Taiani y Fabre, 2011), manteniendo así los problemas pertinentes



a la parametrización de la confiabilidad manifestada en la replicaciones como técnica de escalamiento y en la consistencia que evidencia el flujo de proceso y la infraestructura de alineamientos, cuya validación se presenta estructuralmente al estudiar los protocolos basados en PUSH y en PULL. Para entender estos ejes de operación se debe tener en cuenta:

- Estado del servidor en la MESH.
- Mensajes transferidos.
- Tiempo de respuesta en el cliente.

Se precisa establecer que, por estructura de configuración, toda red MESH evidencia propiedades inherentes al proceso de tolerancia o fallas, significando que esta proporciona servicios en presencia de fallas cualquiera que sea su característica, a saber:

- Falla transitoria: se presenta una vez y luego desaparece.
- Falla intermitente: se presenta, desaparece y luego repite su actividad.
- Falla permanente: detectado o valorado por el registro de anomalías que se registran por:
  - Error en programar activo.
  - Error en el estado de supervisión del sistema operativo.
  - Funcionamiento de tarjetas y circuitos.
  - Funcionamiento equivoco de unidad de I/O.
  - Direccionamiento errores de clientes.
  - Error en captura de transacciones (ACK-NAK-STX-EOT).

## • 2.2 Soporte lógico de comunicaciones MESH

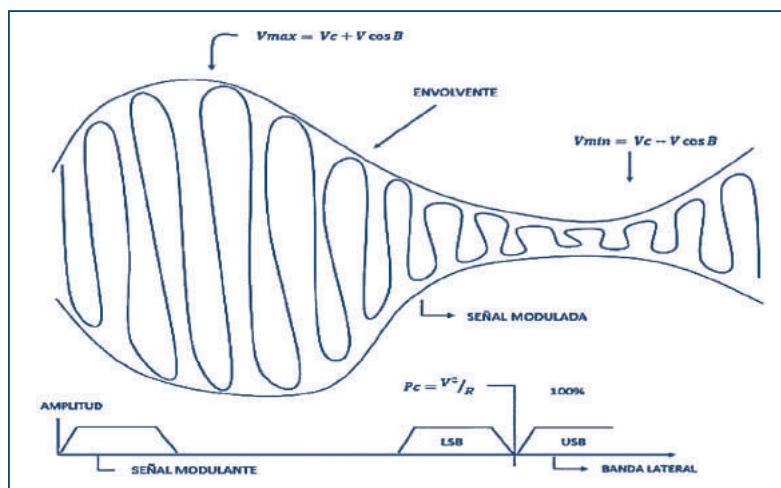
El sistema de comunicación electrónica base para el intercambio transaccional de valores informáticos, integra la funcionalidad proporcionada por los receptores y sistema de modulación de ángulo que operan ampliamente las señales FM/PM, como acción de corrección operacional a la registrada por modulación de amplitud (AM). Esta, a pesar de asociar a la portadora una señal modulante que varía en amplitud, no elimina la presencia de ruido que hace que la amplitud de la envolvente cambie y distorsione el flujo de señal.

En este tema se expondrá la fundamentación correspondiente a la banda lateral única, la transición formal con modulación angular, el soporte móvil y los elementos que definen el proceso de programación de ondas en las líneas de transmisión junto con la interpretación selectiva de las guías de onda.

Con este fundamento se prepara el escenario de desarrollo y presentación de los servicios que se implementan para beneficio de la comunidad en el entorno de las redes MESH, según objetivos propios del proyecto.

## 2.2.1 Transmisión SSBFC

Integra los procesos de enlace asociados con banda lateral única con portadora completa y opera con la mitad del ancho de banda que requiere la modulación por amplitud ( $A_n$ ) normal o convencional. Bajo este esquema se observa que en la banda lateral sólo el 20% de la potencia transmitida y la relación de repetición de la envolvente, es igual a la frecuencia de la señal modulante, haciendo que la profundidad de modulación sea proporcional a la amplitud de la señal modulante y permitiendo que la información trancaccional se integre en la envolvente de la señal modulada de la portadora, tal como se observa en la Figura 2.8.



*Figura 2.8 Onda SSBFC.*

Fuente: Wayne (2010).



La modulación con banda lateral puede trabajarse en cualquiera de estas formas:

- SSBSC58: AM de banda lateral única con portadora superior.
- SSBRC59: AM de banda lateral única con portadora reducida.
- ISB60: AM de banda lateral independiente.
- VSB61: AM de banda lateral vertical.

La transmisión con banda lateral, permite valorar las características listadas a continuación (Meyer, 1999).

- Conservación ancha de banda.
- Conservación de potencia.
- Desvanecimiento selectivo.
- Reducción de ruido.

Características obtenidas del comportamiento del modulador, por su estructura como modulador producto, que permiten que la portadora se multiplique por la señal del producto.

$$V_{AM}(t) = [\alpha + m \sin(2\pi f_m t)][E_c \sin 2\pi f_c t]$$

$\alpha + m \sin(2\pi f_m t) = \text{constructor} + \text{señal modular}$  (13)

$\sin(2\pi f_c t) = \text{portadora no modulada}$

Cuya operación matemática, permite obtener

$$V_{cm}(t) = -\frac{cmE_c}{2} \cos[2\pi(f_c + f_m)t] + \frac{cmE_c}{2} \cos[2\pi(f_c - f_m)t] \quad (14)$$

Facilitando interpretar sus componentes como:

$$-\frac{cmE_c}{2} \cos[2\pi(f_c + f_m)t] = \text{componentes de frecuencia lateral superior} \quad (15)$$

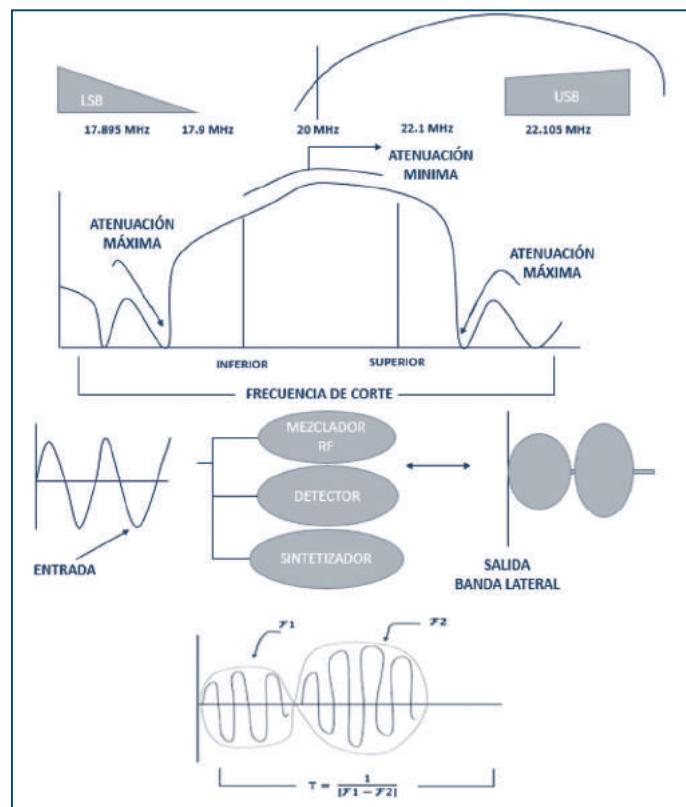
$$+\frac{cmE_c}{2} \cos[2\pi(f_c - f_m)t] = \text{componentes de frecuencia lateral inferior} \quad (16)$$

Complementariamente, se debe tener presente que el proceso de transmisión con banda lateral única se presenta con técnica de filtrado( y con desplazamiento de fase y que la recepción es producto del proceso del oscilador de frecuencia pulsante (BFO), tal como se señala en la Figura 2.9.

Cuando, por ejemplo, se considera como entrado la señal sin  $wmf$ , la que se desplaza 90 ( $\cos wf$ ), se plantea matemáticamente que la señal se comporta así:

$$\text{Salida del modulador } \frac{1}{2} \cos (wc-wm)t - \frac{1}{2} \cos(wc+wm)t \quad (17)$$

Comprobándose que la señal de la banda lateral inferior es la señal de diferencia dada por  $\cos (w_c - w_m)t$



*Figura 2.9* Proceso general de banda única.

Fuente. Elaborado por el grupo de investigación.



## 2.2.2. Transmisión Con Modulación Angular

Técnicamente, la modulación angular se presenta cuando el ángulo de fase ( $\theta$ ), de una onda de comportamiento sinusoidal varía con el tiempo:

$$cm(t) = V_c \cos[w_c t + \theta(t)] \quad (18)$$

$cm(t) = \text{onda modulada}$

$V_c$  = amplitud de portadora

$w_c t$  = frecuencia portadora

$\theta(t)$  = desviación de fase

Comportamiento que implica la consideración de dos tipos de modulación, a saber:

- FM: modulación en frecuencia directa.
- PM: modulación en fase directa.

Cuya diferenciación se obtiene el interpretar estos parámetros:

- Desviación de fase instantánea.
- Fase instantánea.
- Frecuencia instantánea.

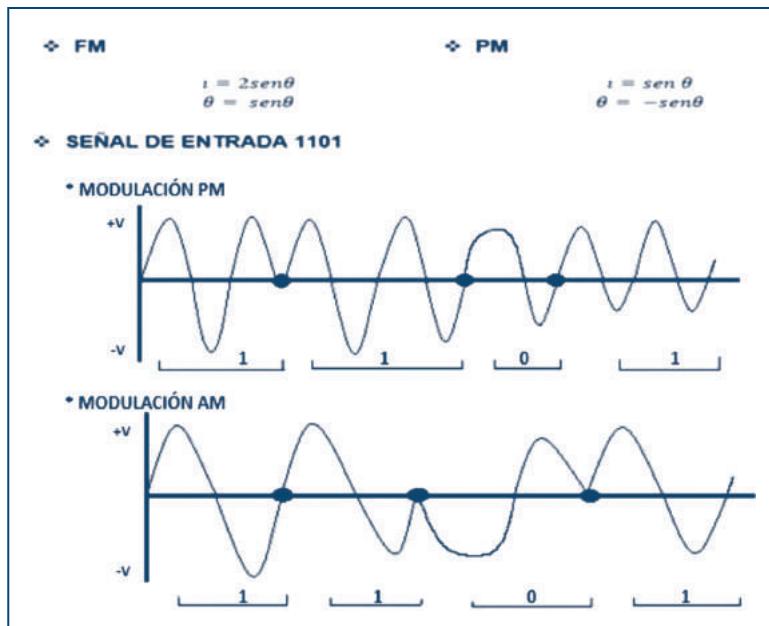
Y al considerar como condicionados res operacionales estos receptores, saber:

- Modulación en Frecuencia.

Caso 1	Señal modulante
	$V_m(t)$
	Onda de modulación angular
	$v_c \cos(w_c t + k_i \int v_m(t) dt)$

	Señal modulada $n(wm t)$
Caso 2	Onda de modulación angular $vc \cos \left[ wc t + \frac{ki Vm}{wm} \cos (wm t) t \right]$
Caso 3	Señal modulada $vm \cos (wm t)$
	Onda de modulación angular $vc \cos \left[ wc t + \frac{ki Vm}{wm} \operatorname{sen} (wm t) t \right]$

Con ayuda de la Figura 2.10, se establece lógicamente la diferencia entre la modulación FM y PM.



*Figura 2.10* Modulación FM/PM.

Fuente: Elaborado por el grupo de investigación.



## • 2.3 Soporte de Modulación Especializado MESH

El proceso de intercambio de valores informáticos sobre arquitecturas de proceso MESH, puede mejorarse al trabajar operacionalmente la FM directa como expresión de la modulación angular, en la cual se verifica cómo la frecuencia de la portadora varía, empleándose diferentes oscilaciones de voltajes (VCO), en las que se verifica:

$$f_c = \frac{1}{2\pi \sqrt{lc}} \text{ hertz}[frecuencia \, básica] \quad (19)$$

$$f_c = \frac{1}{2\pi \sqrt{2(c + \Delta c)}} [frecuencia \, señal \, modulador] \quad (20)$$

Que se parametrizan de esta *manera*:

*I = inductancia*

*c = capacitación*

*fc = frecuencia central*

*f = frecuencia modulante*

Haciendo entonces preciso adelantar que el proceso involucra la operación de:

- Moduladores directos FM.
- Moduladores indirectos FM.
- Transmisores directos FM.
- Estabilizadores puros AFC64.
- Transmisores FM con fase cerrada.

### 2.3.1 Conversores FM-PM

Razones fundamentales para denotar la importancia de la modulación de ángulo para asegurar la portabilidad en redes MESH, por la utilización apropiada de los conversores.

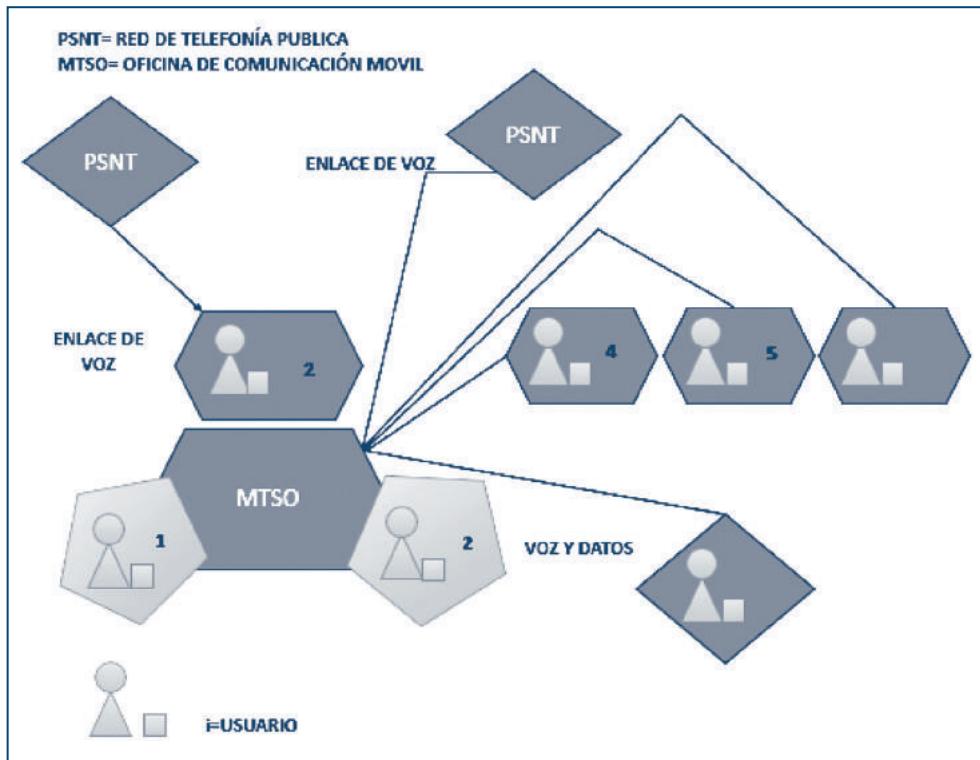


- Detectores de pendiente balanceados.
- Discriminadores de FS (*Foster-Seeley*).
- Detectores de relación.
- Demoduladores PLL (circuito de fase cerrado).
- Demoduladores FM en cuadratura.

Con la implementación de los conversores se asegura la operación integral de los sistemas de IF de FM con mezcladores de alto rendimiento, que permiten valorar la utilización apropiada de las comunicaciones de radio de FM de dos vías y la telefonía móvil o radio celular, las cuales catalogan los sistemas de administración de frecuencia para el servicio de telefonía móvil avanzado (AMPS)<sup>66</sup> y el sistema de acceso total (TACS) que evidencia plena diferenciación entre el espaciamiento del canal, distribución de espectro, espectro adicional y número de canales.

El esquema operacional de esta tipología de proceso para intercambio transaccional, se observa en la Figura 2.11. Las entradas funcionales de este esquema son:

- Centro de conmutación electrónica.
- Centro de conmutación.
- Proceso de información.
- Control de sitio de celular.
- Administración de canales de radio.
- Supervisión de llamadas.
- Control y diagnóstico.
- Transceptor de radio.
- Interconexión de sistema.
- Unidades de telefonías móviles.
- Protocolos de commutadores.
- AMPS68.
- Aurora POO.
- RC 2000.
- NMT69.
- NETZ70.
- C450.
- PTT71.



*Figura 2.11 Componentes sistema celular.*

Fuente: Elaborado por el grupo de investigación.

No debe olvidarse que, en todo sistema teleinformático se necesita considerar los siguientes factores como unidades de control directo, a saber:

- Factores de velocidad

$$V_F = \frac{V_p}{C} \quad (21)$$

$V_F$  = factor de velocidad

$V_p$  = velocidad de propagación

$C$  = velocidad de la luz = velocidad de propagación en espacio libre.



- Tiempo de desplazamiento

$$T = \sqrt{LC}$$

$$V_p = \frac{D}{T} \quad (22)$$

$$V_p = \frac{D}{\sqrt{LC}}$$

- Pérdidas de la línea
  - Por el conducto.
  - Por radiación.
  - Por calentamiento del dieléctrico.
  - Por acoplamiento.
- Coeficiente de reflexión

$$r = \frac{E_r}{E_i} \quad (23)$$

$$r = \frac{I_r}{I_i}$$

$r$  = coeficiente de reflexión

$E_i$  = voltaje incidente

$E_r$  = voltaje reflejada

$I_i$  = coeficiente incidente

$I_r$  = corriente reflejada

- Relación de onda estacionaria de voltaje

$$SWR = \frac{V_{máximo}}{V_{mínimo}} \quad (24)$$

$$V_{mínimo} = E_i - E_r$$

$$V_{máximo} = E_i + E_r \quad (25)$$



$$SWR = \frac{E_i + E_r}{E_i - E_r}$$

$$rE_i = E_r$$

$$SWR = \frac{E_i(1+r)}{E_i(1-r)} = \frac{1+r}{1-r}$$

$$SWR = (1+r) = 1+r$$

$$SWR - SWRr = 1 + r \quad (26)$$

$$SWR = 1 + r + SWRr$$

$$SWR = 1 + r + SWRr$$

$$SWR - 1 = r(1 + SWR)$$

$$r = \frac{SWR - 1}{SWR + 1}$$

La construcción operacional MESH demanda tener presente las propiedades óptimas que evidencian las ondas, las cuales se listan a continuación:

- Refracción

$$N = \frac{C}{V} \quad (27)$$

$N$  = índice de refracción

$C$  = velocidad de la luz

$V$  = velocidad de la luz en el medio

Que, al operar con la ley de suelo, se obtiene

$$\begin{aligned} N_1 \sin \theta_1 &= N_2 \sin \theta_2 \\ \frac{\sin \theta_1}{\sin \theta_2} &= \frac{N_2}{N_1} \\ \frac{\sin \theta_1}{\sin \theta_2} &= \sqrt{\frac{E_{r2}}{E_{r1}}} \end{aligned} \quad (28)$$



$E_{r1}$  = constante dieléctrica medio 1

$E_{r2}$  = constante dieléctrica medio 2

- Reflexión

$$r = \frac{E_r e^{j \theta r}}{E_i e^{j \theta i}}$$
$$r = \frac{E_r}{E_i} e^{j(\theta r - \theta i)} \quad (29)$$

$\theta r$  = fase reflejada

$\theta i$  = fase ncidente

$E_r$  = voltaje reflejado

$E_i$  = oltaje incidentado

$E_i$  = eficiente de reflexión

- Difracción: modulación de la energía en un frente de onda.
- Interferencia: combinación de dos ondas electromagnéticas.
- Propagación de ondas (ver figura 2.12).
  - Terrestre.
  - Espacial.

$$d = \sqrt{2H} = \text{radio horizontal} \quad (30)$$

$d$  = distancia a radio horizontal

$\sqrt{2H}$  = altura sobre el nivel de mar de la altura

$$d = d_t + d_r$$

$$d = \sqrt{2H_t} + \sqrt{2H_r}$$

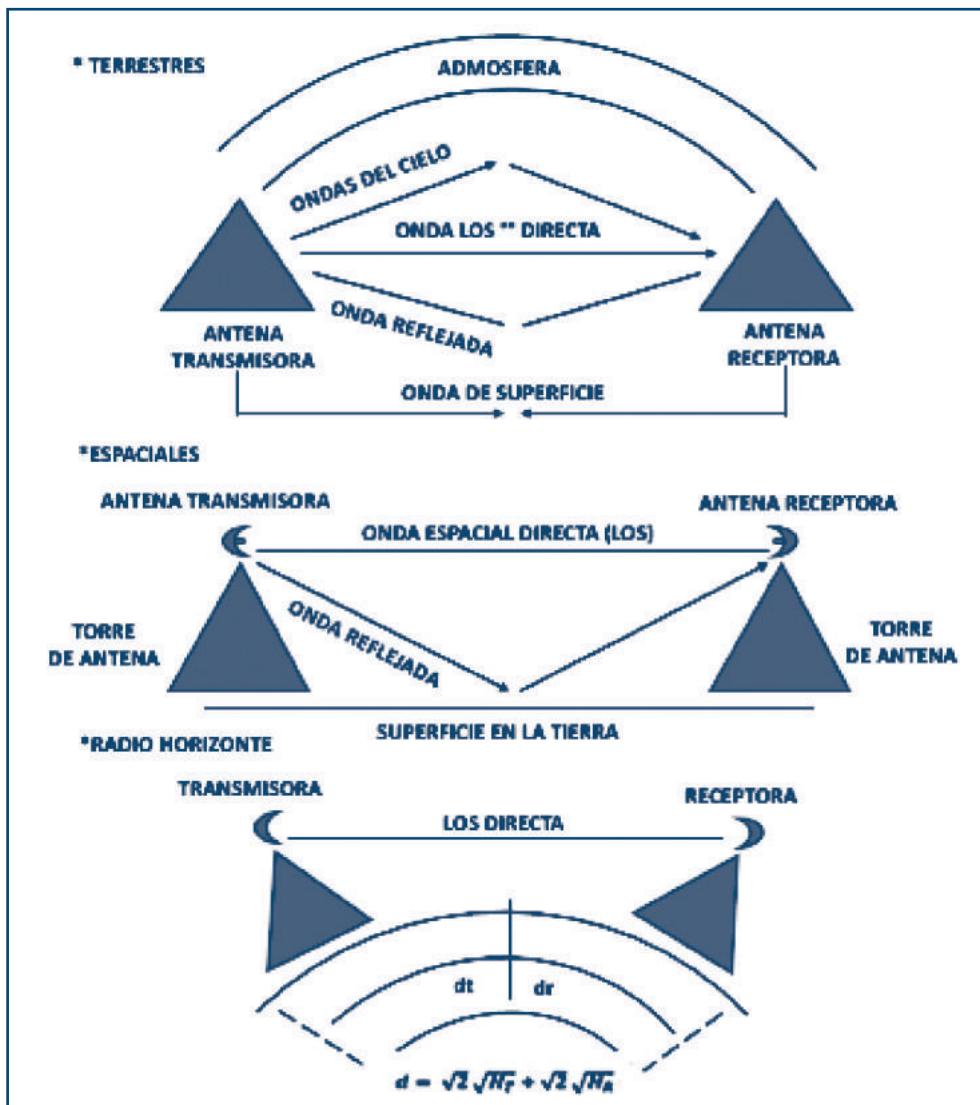
$d$  = distancia total

$d_t$  = radio horizontal antena transmisor

$d_r$  = radio horizontal altura receptora

$H_t$  = altura antena receptora

$$d = \sqrt{2}\sqrt{H_t} + \sqrt{2}\sqrt{H_r} \quad (31)$$



*Figura 2.12 Propagación de ondas.*

Fuente: Elaborado por el grupo de investigación.

- Ondas del cielo: ondas electromagnéticas que superan el nivel del horizonte.
  - Capa D: capa inferior ionosfera 30 y 60 millas.
  - Capa E: 60 y 85 millas.
  - Capa F: 85 y 155 millas.



- Altura virtual: sitio en el cual parece que una onda refractada ha sido reflejada.
- Frecuencia máxima utilizada.

$$MUF = \frac{\text{frecuencia crítica}}{\cos \theta} \quad (32)$$

$$MUF = \text{frecuencia crítica} * \cos \theta$$

### 2.3.1 Antenas

Comúnmente una antena es definida como un sistema de conductor metálico que recibe y radia ondas electromagnéticas. El estudio de la teoría de antenas permite comprender los parámetros operacionales que se listan a continuación:

- Patrón de radiación: diagrama pulsar que señala las intensidades de los campos o de densidades de potencia.
- Campo de radiación: entorno físico de expansión operacional de la señal, pudiéndose observar el campo de inducción o cercanías y el campo de radiación o lejanía.
- Resistencia de radiación: mide la resistencia de la antena.

$$R_r = \frac{P}{C^2} \quad (33)$$

$R_r$  = resistencia de la radiación

$P$  = potencia radiada

$C^2$  = coeficiente de la altura

Eficiencia de antena: relación entre potencia radiada y potencia total de entrada.

$$\begin{aligned} m &= \frac{C^2 R_r}{C^2 (R_R + R_C)} \\ m &= \frac{R_r}{R_r + R_C} \end{aligned} \quad (34)$$

$m$  = eficiencia de la altura



$c = \text{capacitación de antena}$   
 $R_r = \text{resistencia de radiación}$   
 $R_c = \text{eficiencia de antena efectiva}$

- Ganancia directiva

$$D = \frac{P}{P_r} \quad (35)$$

$P = \text{densidad de potencia en un punto de la antena (watts/metro}^2\text{)}$

$P_r = \text{densidad de referencia}$

- Potencia radiada isotrópica efectiva

$$EIRF = P_e A_t \quad (36)$$

$$EIRF = 10 \log \frac{P_r}{0.001} + 10 \log A_t$$

$A_t = \text{ganancia directiva}$

$P_r = \text{potencia radiada}$

- Ancho de haz: separación angular entre los dos puntos de medida potencia (0,-3 db).
- Ancho de banda: ángulo sobre frecuencia sobre el cual se define la operación de la antena.
- Impedancia de entrada: relación del voltaje de entrada con la corriente de entrada.

$$Z_e = \frac{V_i}{I_I} \quad (37)$$

$Z_e = \text{impedancia de antena}$

$V_i = \text{voltaje de entrada}$

$I_I = \text{corriente de entrada}$

Los procesos de intercambio transaccional se sustentan lógicamente con los siguientes tipos de antena, a saber:

- Doblete elemental



$$C(t) = I \sin(2\pi ft + \theta) \quad (38)$$

$$E = \frac{60\pi I L \sin \theta}{X_r} = \text{radiación}$$

$$P = \frac{30 \pi L^2 X_R^2 \sin^2 \theta}{X_R^2 R^2} = \text{densidad de potencia}$$

- Antena Monopolio.
- Dipolo de media onda.
- Dipolo plegado.
- Yagi-Uda.
- Logarítmica periódica.
- Antena de Loop.
- Antena de arreglo de fase.
- Antena helicoidal.
- Antena de ULTF (0.3-3.6 GHz).
- Antena de microonda (1-100 GHz).
- Antena reflectora parabólica.

### O Ancho de haz

$$\theta = \frac{70X}{D} \quad (39)$$

$\theta$  = ancho de haz

$X$  = longitud de la onda

$D$  = diámetro de la antena

- Ganancia de potencia de antena

$$A_p = m \left( \frac{\pi D}{X} \right)^2 \quad (40)$$

$A_p$  = ganancia de potencia

$D$  = diámetro de antena

$m$  = eficiencia de antena

$X$  = longitud de onda



- Mecanismos de alineamiento: proceso de irradiación de la energía electromagnética.
  - Central.
  - Corneta.
  - Cassegrain.

Con el fin de sustentar el núcleo, forma del sustento teórico de este proyecto, se describen a continuación las características operacionales que tendría que poseer la antena que debe sustentar la implementación del conjunto de servicios, el cual como entregable de este proyecto, validará el cumplimiento del objetivo formulado.

El desarrollo ingenieril de carácter integral de este proyecto, permitirá verificar el uso de antenas directivas que habilitan la cobertura de Back Haul<sup>16</sup> (comunicación entre nodos). No debe dejarse de lado que en una solución MESH, se pueden emplear las antenas inteligentes, adaptativas y auto configurables y hasta las reprogramables por *software*, sin olvidar que la gran mayoría de estas se pueden fabricar en casas o con materiales a costo mínimo. Para ello, se precisa tener como fundamento de desarrollo la tecnología MIMO<sup>17</sup>, que determina el empleo de múltiples antenas para transmisión y recepción validando la normatividad señalada por la IEEE 802.11n, en lo pertinente al uso simultáneo de las bandas 2.4-5.4 GHz.

Específicamente, al considerar las antenas Wifi 802.11n se permite sustentar como premisas de desarrollo básico, estos enunciados de carácter operacional:

---

<sup>16</sup> Conexión baja, media o alta velocidad que conecta a computadores u otros equipos de telecomunicaciones encargados de hacer circular la información, los *Backhaul* conectan redes de datos, redes de telefonía celular y constituyen una estructura fundamental de las redes de comunicación. <http://mundocontact.com/glossary/backhaul-red-de-retorno/>

<sup>17</sup> MIMO es un mecanismo que incrementa la eficiencia espectral de un sistema de transmisión inalámbrica, por medio de la utilización de domino especial, aprovechando fenómenos físicos como la propagación multirayecto para incrementar la velocidad de transmisión o reducir la tasa de errores. Dado que MIMO se basa en el domino especial, requiere el uso de múltiples antenas en el transmisor y en el receptor. <http://www.albentia.com/Docs/WP/Whitepaper%20MIMO.pdf>



- Mejora absoluta del *Throughput*<sup>18</sup> y la confiabilidad.
- Explotación total de los parámetros de expectativa de la OFDM<sup>19</sup> (multiplicación por división de frecuencias ortogonales).
- Duplicación de las velocidades, al ampliarse el canal de 20 GHz a 40 GHz.
- Garantiza conectividad MIMO (múltiple entrada-múltiple salida).
- Ofrece ganancias típicas en Dbi isotrópicos, que fluctuando entre 2 Dbi para antenas integradas simples, 5 Dbi con antenas omnidireccionales estándar, 25 Dbi para omnidireccionales externas, y hasta 25 o 30 Dbi para las parabólicas.
- Atención al espectro de reflexión al direccionar antenas con polarización circular.

La Universidad Libre al liberar este proyecto, debe considerar obligatoriamente la minimización de radiación de las antenas, según normativas de la OMS<sup>19</sup> y el Decreto 195 del 2005, que acepta y adopta lo dispuesto por la recomendación UIT-K52; y según lo dispuesto por la normativa de la Unión Europea 519/EC/1999, que regula los límites de exposición a campos electromagnéticos para las redes MESH, trabajando en las bandas de 2.4 a 2.42 GHz y de 5 a 5.46 GHz del espectro radioeléctrico (Ouidis Hertziauns). Para este fin, es necesario evaluar el documento que libera la Universidad Javeriana, para la Comisión de Regulación de Telecomunicaciones CRT 2002<sup>20</sup>, que referencia el proyecto “Estudio de los límites”.

Toda solución MESH, es producto de la catalogación efectiva del estándar IEEE 802.11 N, que detalla como características fundamentales las siguientes:

---

<sup>18</sup> *Throughput* en redes de comunicaciones, como *Ethernet*, se llama *Throughput* a la tasa promedio de éxito en la entrega de un mensaje sobre un canal de comunicación. Este dato puede ser entregado sobre un enlace físico o lógico, o a través de un cierto nodo de la red. Por regla general, el *Throughput* es medido en bit por segundo y, a veces, en paquetes de datos por segundo o paquete de datos por franja de tiempo. <http://diarioredesy servicios.wordpress.com/2012/01/11/conceptos-basicos-sobre-planificacion-de-redes/>

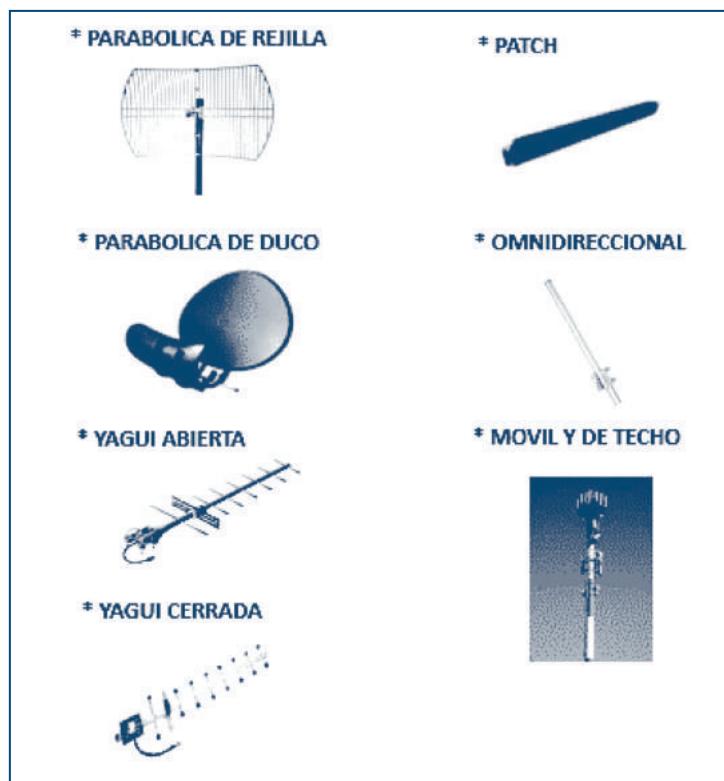
<sup>19</sup> La Organización Mundial de la Salud (OMS) está examinando los aspectos sanitarios de esta situación en el marco de su Proyecto Internacional sobre los Campos Electromagnéticos. Es necesario determinar claramente las posibles consecuencias sanitarias y, si se considera procedente, habrá que adoptar las medidas paliativas apropiadas. <http://influenciascamposelectromagneticos.blogspot.com/2008/04/los-campos-electromagnéticos-y-la-salud.html>

<sup>20</sup> Resolución 575 de 2002 por la cual se modifica la numeración de la resolución CR4T 087 de 1997 y se actualiza sus modificaciones en un sólo cuerpo resolutivo <http://www.crcm.gov.co/?idcategoria=59938>



- Alta utilización (por su popularidad).
- Velocidad entre 80 – 100 Mbps.
- Bajo costo.
- Frecuencia nominal 2.4 GHz – 5.4 GHz.
- Acceso público y rango operacional amplio.
- Secuencialización de codificación según estructura Barker78 para uso de canales DSSS79.
- Empleo de PSK y QPSK.
- Control de intercambio por acción de protocolos como:
  - AODV
  - BATMAN
  - BMX
  - BATMAN – ADV
  - OLSR
  - TORA
  - HSLS
  - BABEL
- Estructura funcional definida por coherencia funcional de:
  - BSS (Basic Services Set).
  - IBSS (Independent Basic Services Set).
  - DS (Distributed System).
  - ESS (Extended Service Set).

Para los efectos pertinentes, se describe como ejemplo formal el proceso de construcción de una antena para señalización inalámbrica, mostrando previamente con ayuda de la Figura 2.13, los tipos convencionales de mayor uso.



*Figura 2.13 Tipología de antenas convencionales soluciones MESH.*

Fuente: Jmtelcom (2010).

Para generalizar el procedimiento de elaboración se citan en primer lugar, los diferentes elementos que permiten su terminación y utilización, los cuales son (Carballar, 2012):

- Antena BTC (Bellingham Technical College)
  - Antena Direccional.
  - Diámetro 9 a 11 centímetros.
  - Longitud 3/4 de longitud de onda (Lg).
  - Conector 14 de longitud de onda.
  - Fórmula de contexto.

$$\left(\frac{1}{Lg}\right)^2 = \left(\frac{F}{300}\right)^2 - \left(\frac{1}{1 - 706 * D}\right)^2 \quad (41)$$



*Lg = longitud de onda*

*m = frecuencia*

*X = diámetro en milímetros*

- Longitud de cable

$$L = \frac{1}{4} \text{ onda de señal al aire} \quad (42)$$

$$L = \frac{1}{4} (300/F)$$

Por ejemplo, si se tienen diámetros de 9 y 11 centímetros los parámetros de uso son:

- Diámetro 9 centímetros.

Longitud de onda 201 Nm

$$-\frac{1}{4} \lambda = 50 \text{ Nm} \quad (43)$$

$$-\frac{3}{4} \lambda = 151 \text{ Nm}$$

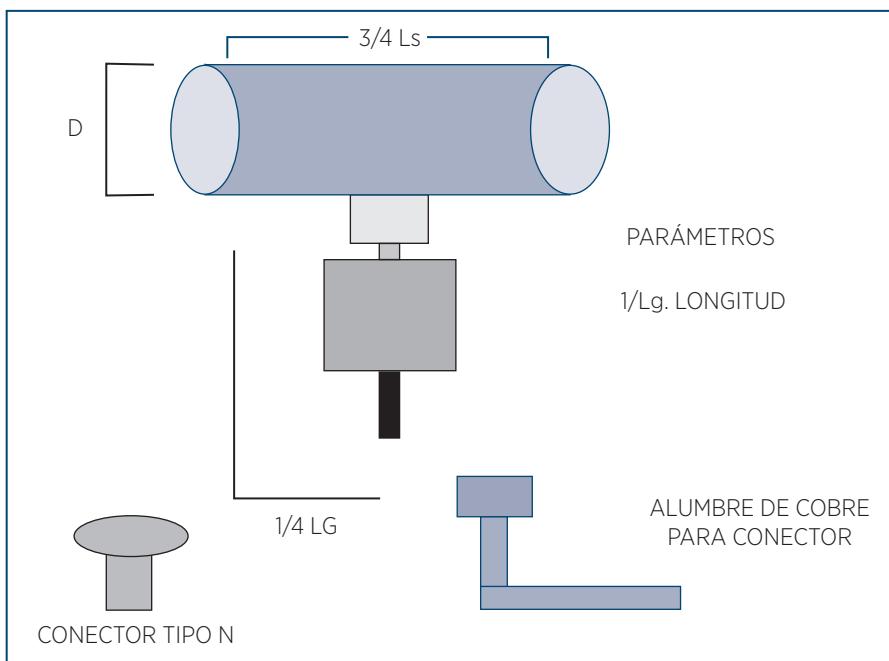
- Diámetro 11 centímetros

Longitud de onda 160 Nm

$$-\frac{1}{4} \lambda = 40 \text{ Nm} \quad (44)$$

$$-\frac{3}{4} \lambda = 120 \text{ Nm}$$

Su estructura se muestra en la Figura 2.14.



*Figura 2.14 Antena BTC (Lata de Tomate).*

*Fuente:* Elaborado por el grupo de investigación.

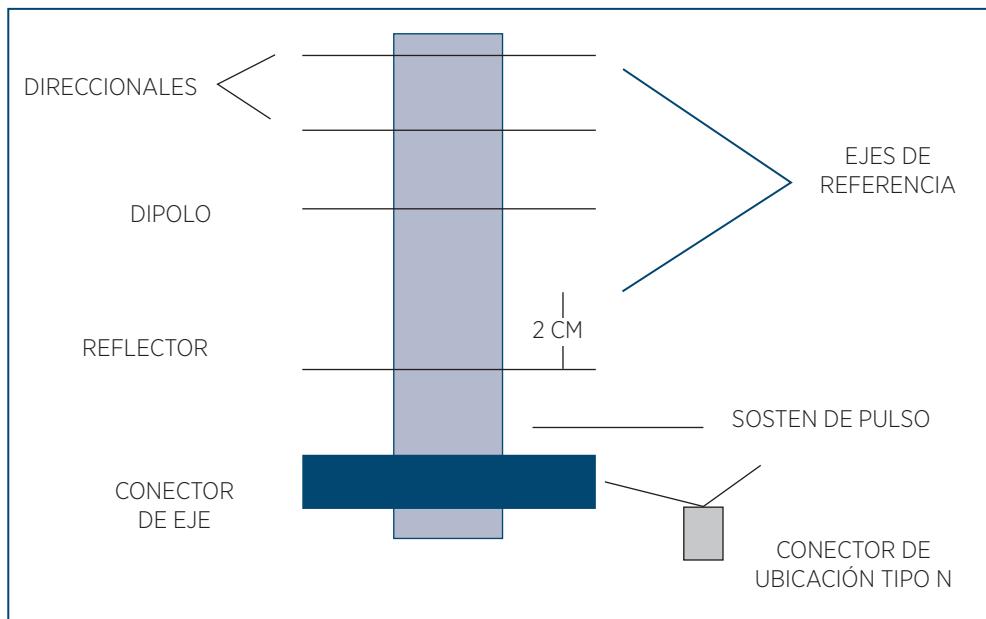
El proceso de construcción, integra las siguientes fases:

- Abrir por un lado la lata.
- Implementar el conector y unir con el cable de 30 cm de longitud, soldando la unión.
- Atornille o solde el conector, garantizando elegancia de visión.
- Practicar un orificio en el fondo para eliminar agua que se filtre, o si se puede ubicar una tapa plástica protectora, previa prueba de resistencia o microondas. Para esto se coloca la tapa en un horno de microondas y se observa su estado final.
- Prueba integral para comprobar su funcionalidad al estar bien construido, uniéndola al adaptador de red.

### 2.3.2 Antena de clip o Antena de Frisko

Semeja la operación de una antena Yagui con 9 Dbi de ganancia de sencillo, construcción tal como se observa en la Figura 2.15, se requiere:

- Tres varillas de longitud diferente con dipolo radiante.
- Soporte de madera o corcho con longitud de 10 cm.
- Cable coaxial de 50 Ohmios.
- Conector Tipo N.



*Figura 2.15 Antena Frisko.*

Fuente: Elaborado por el grupo de investigación.

Debe recordarse que las varillas direccionales tendrán 5.15 y 5.20 cm, el dipolo debe medir 11.40 cm y el reflector 5.8 cm; el dipolo se doblará con espesor de 4 mm para, desde allí, conectar de manera simétrica, manteniendo una separación entre el dipolo y el reflector de 2 cm.

### 2.3.3. Antena Biquad

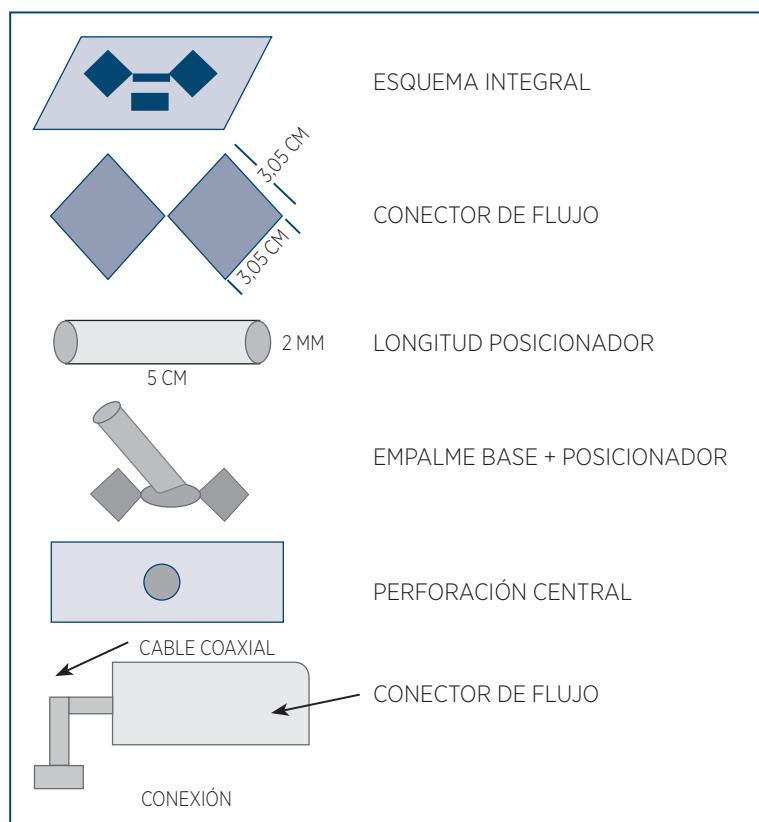
Antena propuesta por Trevor Marshall que garantiza 11 Dbi de ganancia, para ello se requiere:

- Base cuadrada de 12.3 cm con baquelita.
- Tubo de cobre de 5 cm de largo y 1.2 cm de diámetro (21 pulgada).
- Cable coaxial de 30 cm tipo CNT-400 o LNR-400.

- Hilo de cobre de 1.5 milímetros de diámetro y 25 cm de largo.
- Conector tipo N.

Para su montaje, se procede a realizar los siguientes pasos:

- Perforar el centro de la baquelita con orificio de 1/2pulgada.
- Rebanar el hilo de cobre y preparar para soldar.
- Colocar el tubo perpendicular a la base o baquelita y soldar.
- Tomar el hilo de cobre y darle forma de rombo alargado (ver figura 2.16), con longitud por lado es 3.0 centímetros (30.5 mm); sus extremos confluyen en el centro, la longitud del lado en  $\frac{1}{4}$  de la longitud de onda.
- Preparar extremos de cable coaxial para su empalme con el centro del hilo en rombo y fijar el extremo sobrante con el conector tipo N.



*Figura 2.16 Antena Biquad.*

Fuente. Elaborado por el grupo de investigación.

### 2.3.4 Antena de Flickenger o de tarro de papas

Con alcance de hasta 500 metros y 9 Dbi de ganancia, su esquema se visualiza en la Figura 2.17, los componentes de fabricación son:

Tarro de papas vacío con tapa plástica con largo de 23 cm y diámetro de 7 cm.

- Conector de antena hembra tipo N.
- Varilla de 3 mm de diámetro con rosca.
- Tuercas de enroscado.
- Cinco arandelas de 2.5 cm de diámetro y 1.5 milímetros de espesor.
- Tubo de aluminio de 6 milímetros de diámetro con largo de 16 centímetros.
- Cable grueso de cobre de 4 cm de largo y un solo hilo.

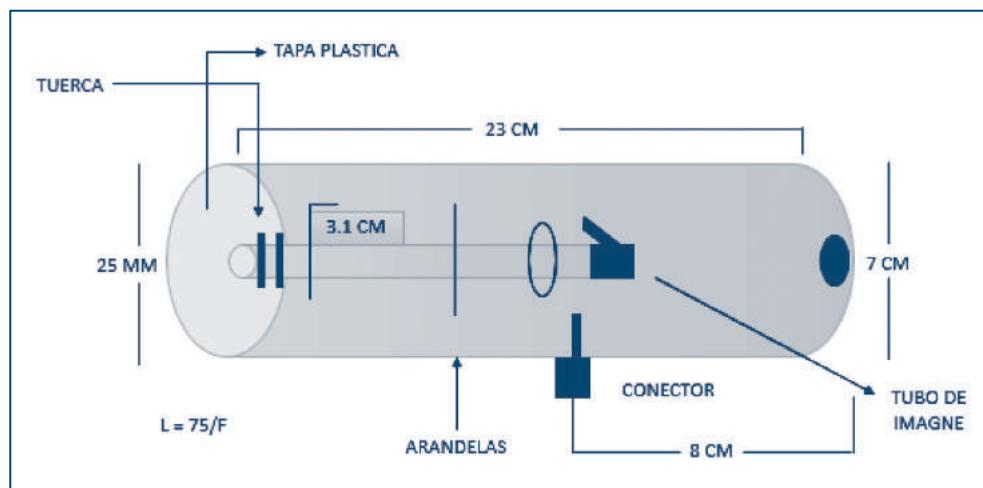


Figura 2.17 Antena de Flickeng.

Fuente: Elaborado por el grupo de investigación.

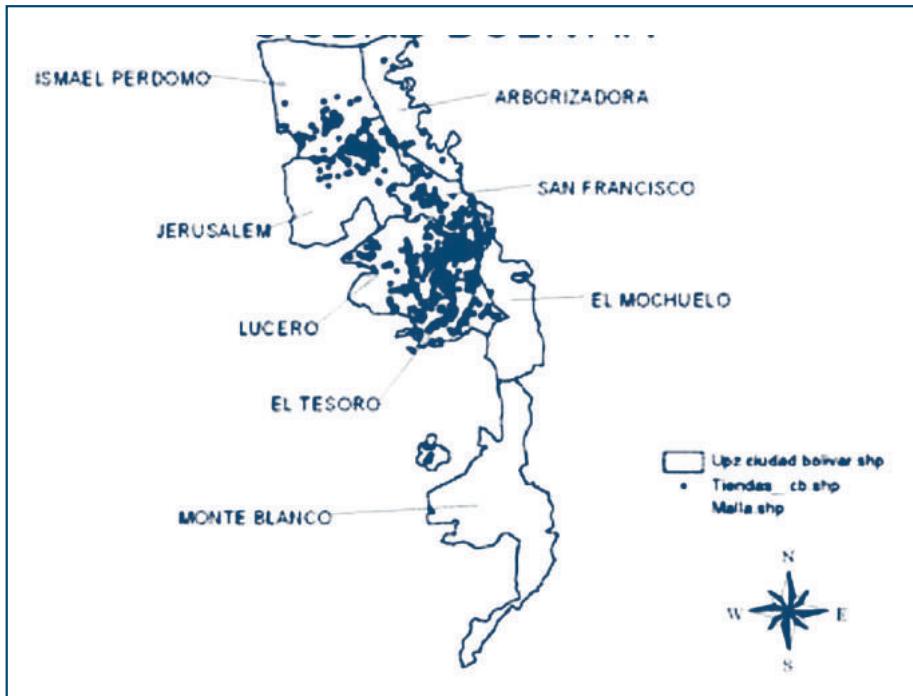
Para probar esta antena, sólo basta colocarla con el equipo de TV.

### 2.3.5 Marco descriptivo de servicios

El proyecto MESH-UNILIBRE, validará su calidad y efectividad al estructurar e implementar dos plataformas de carácter experimental, que según

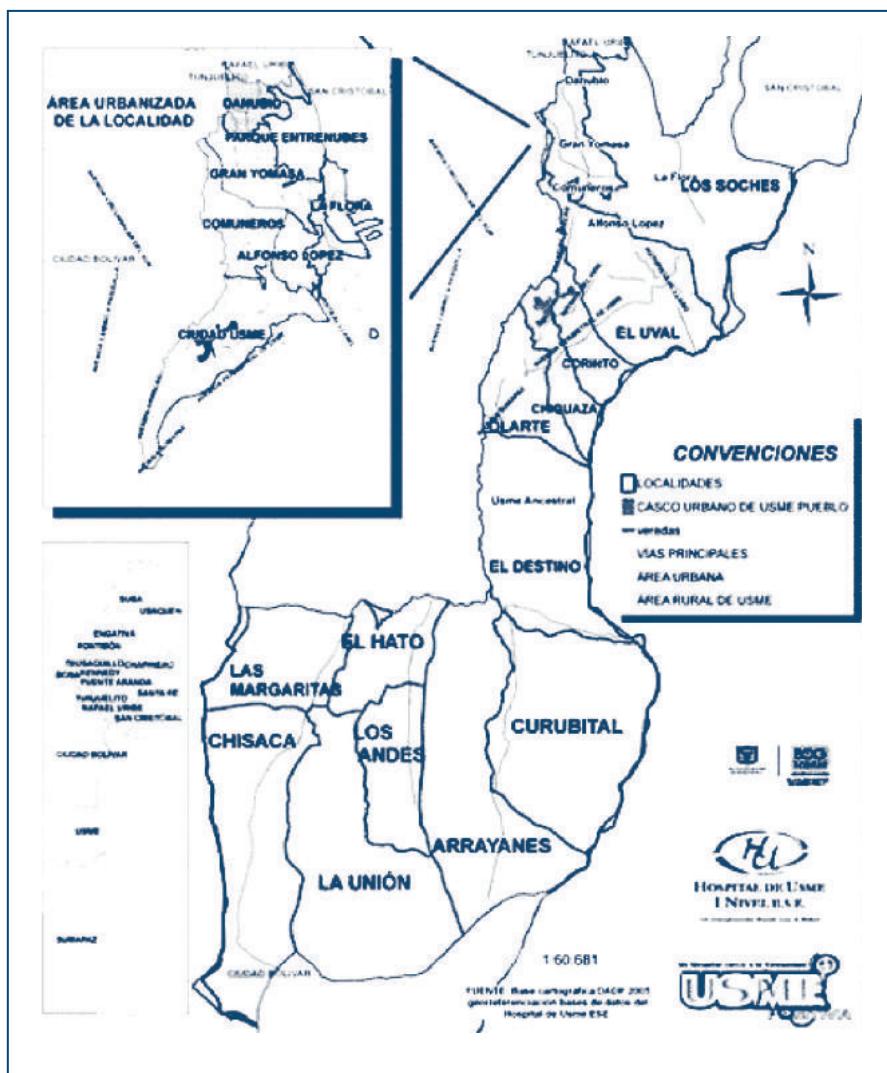
valoración de pertinencia social serán las localidades de Ciudad Bolívar (Sierra Morena) y Usme (El Uval), cuyo espacio geográfico se visualiza en las Figuras 2.18 y 2.19 respectivamente.

El esquema operacional que ofrecerá MESH-UNILIBRE, es de carácter escalable, con factor de multiplicidad de expansión según necesidades de las Juntas Administradoras Locales, las Juntas de Acción Comunal, las Alcaldías Locales y la Alcaldía Mayor de Bogotá, según se observa en la Figura 2.20.



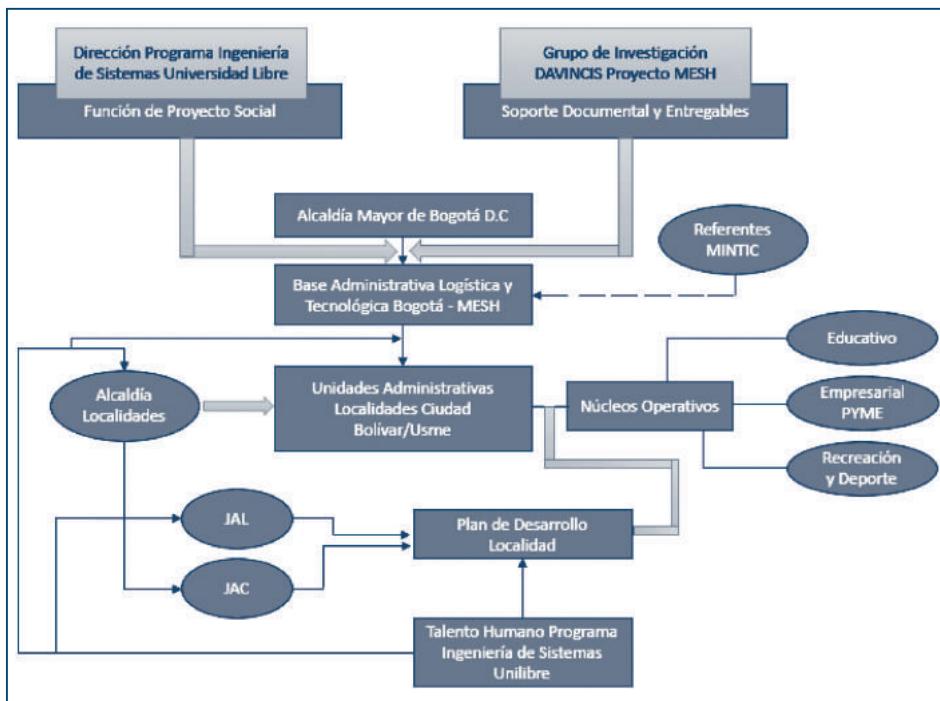
*Figura 2.18* Área de cubrimiento Ciudad Bolívar.

Fuente: Map data, google (2017).



*Figura 2.19 Área de cubrimiento localidad de Usme.*

Fuente: Map data, google (2017).



*Figura 2.20 Unidad rectora para configuración nodos MESH-UNILIBRE.*

Fuente: Elaborado por el grupo de investigación.

La implementación de los servicios que proyecta como entregables MESH-UNILIBRE, demanda el seguimiento y consideración formal y funcional de las fases siguientes que, para los efectos correspondientes de sustentación teórica, se exponen a continuación:

- Fase de contextualización
- Objetivo: exponer ante las autoridades administrativas, la estructura y conjunto de beneficios a recibir, con la implementación de los nodos proyectados por MESH-UNILIBRE.
- Soporte operacional
  - Cartas de solicitud de atención y agenda para exponer el proyecto.
    - Alcalde mayor.
    - Alcalde localidad.
    - Presidentes de acción comunal.
    - Ediles junta administrativa de acción comunal.



- Portafolio de presentación proyecto.
- Calendario de ejecución.
- Fecha de inicio: agosto 15 2014.
- Fecha de culminación: noviembre 30 2014.
- Entregable.

Autorización de configuración nodo piloto experimental para cada localidad.

El portafolio de presentación como documento para evaluación, deberá contener los siguientes factores:

- Marco descriptivo MESH-UNILIBRE.
- Listado de beneficios.
- Infraestructura tecnológica.
- Inversión requerida.
- Directorio de proveedores.
- Plan de capacitación.
- Estructura formato de establecimiento de acuerdo a suscribir.

## • 2.4 Validación de infraestructura tecnológica

### Objetivo

Dimensionar la confiabilidad operacional de la infraestructura tecnológica requerida, la cual se obtuvo como entregable del módulo del proyecto de investigación que lideró el Ingeniero Fabián Blanco G, quién orientó al egresado Manuel Camilo Cepeda Martínez, responsable del proyecto titulado: “Diseño e implementación de una red MESH como alternativa de solución para redes comunitarias y rurales”. Las pruebas de confiabilidad que deberían ser efectuadas son:

- Facilidad de adquisición soporte: tiempo, valoración de operación, inversión.
- Instalación de soporte logístico: tiempo, cuidados, respuesta a eventualidades, valoración de documentación y facilidad de acceso.



- Recepción y transmisión de valores informáticos con máxima confiabilidad
- Reducción y eliminación de interferencia que distorsiona el proceso de intercambio transaccional.

## Responsable

Líder del proyecto y talento humano que se asigne por parte de la dirección del programa de Ingeniería de Sistemas de la Universidad Libre.

## Soporte operacional

- Entregable proyecto citado.
- Documento referencial Bogotá MESH.

## Calendario de ejecución

- Fecha de inicio: agosto 01 de 2014.
- Fecha de culminación: agosto 15 de 2014.

## Entregable

Certificaciones de confiabilidad y efectividad integral de la infraestructura tecnológica seleccionada, expedida por la dirección del programa, como garantía de pertinencia y adecuación operacional de la solución, por vía validación de la oficina jurídica de la universidad.

## • 2.5 Soporte decisional para selección de infraestructura tecnológica

## Objetivo

Facilitar y permitir al grupo responsable que asigne cada localidad, para soportar el desarrollo e implementación del proyecto de instalación, configuración y prueba de MESH-UNILIBRE.



## Responsable

Líder del proyecto y grupo asesor de desarrollo y consultoría.

## Soporte operacional

- Portafolio de presentación de empresas proveedoras de tecnología que el líder del proyecto sugiera, para estudio del grupo asesor.
- Costos de producción a negociar.

## Algoritmo para asignación

Para asegurar que la Alcaldía Local, con la participación de la Junta de Acción Local y la Junta de Acción Comunitaria, obtendrá el mejor escenario de inversión, el líder del proyecto deberá discutir las ventajas del algoritmo húngaro o algoritmo de asignación, cuya estructura se visualiza en la Figura 2.21 y cuyas fases de operación, se ejemplifican a continuación.

Las fases operacionales del algoritmo humano que se ejemplificaron para el caso, admiten la simbología mostrada, a saber:

$$E_c = \text{Empresas ofertantes} \quad (45)$$

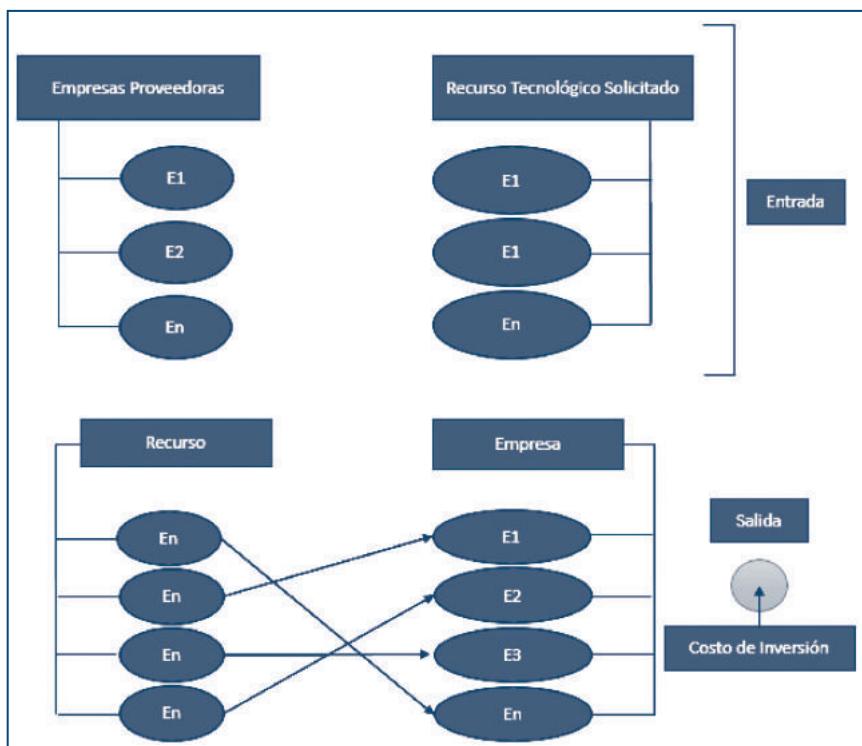
$$\begin{matrix} E_1 \\ E_2 \\ E_3 \\ E_4 \end{matrix}$$

$$R_c = \text{Recursos solicitados} \quad (46)$$

$$\begin{matrix} R_1 \\ R_2 \\ R_3 \\ R_4 \end{matrix}$$

$$C_L = \text{Costo de recursos según tabla de valores por empresa} \quad (47)$$

$$\begin{matrix} C_1 \\ C_2 \\ C_3 \\ C_4 \end{matrix}$$



Fuente: Elaborado por el grupo de investigación.

Para el desarrollo del ejemplo, se debe aclarar que los costos asignados son subjetivos en la información que se despliega en la Tabla 2.1, pero en la práctica serán reemplazados por los dispuestos por cada operante. Estos costos se presentan en millones de pesos.

*Tabla 2.1.* Registro de elementos de asignación.

Recurso	Empresa	E1	E2	E3	E4
R1		164	76	80	56
R2		80	48	56	42
R3		82	54	66	60
R4		44	76	82	72

Fuente: Elaborado por el grupo de investigación.



Las fases que considerar son:

### Fase de selección y reducción horizontal/vertical

Se obtiene el mayor valor por fila y se resta de los demás, como se muestra en la Tabla 2.2.

*Tabla 2.2.* Reducción de filas.

64	76	80	56
80	48	56	42
82	54	66	60
44	76	82	72

Fuente: Elaborado por el grupo de investigación.

Proceso con el que se obtienen los resultados mostrados en la Tabla 2.3. Procedimiento que señalar por columna el menor valor diferente de 0, restándolo de los demás elementos por columna, tal como lo muestra la Tabla 2.4.

*Tabla 2.3.* Resultados reducción por filas.

16	4	0	24
0	32	24	38
0	28	16	22
38	6	0	10

Fuente: Elaborado por el grupo de investigación.

*Tabla 2.4.* Reducción por Columna.

-28	0	0	14	
0	16	12	16	LT = 4 NF = 4 LT = NF
0	12	4	0	
-50	2	0	0	

Fuente: Elaborado por el grupo de investigación.



## Fase de conexión

Se unen los ceros adyacentes por filas y columnas, validando si el número de líneas trazadas es igual al número de filas de la matriz; si se da la igualdad, se procede a asignar, en caso contrario se continúa con la fase siguiente (ver tabla 2.5)

*Tabla 2.5.* Conexión de ceros.

16	0	0	14
0	28	24	28
0	24	16	(12)
28	2	0	0

LT = 3  
NF = 4  
LT ≠ NF  
↳ Filas de la matriz  
↳ Líneas Trazadas

Fuente: Elaborado por el grupo de investigación.

Como no se verifica que  $LT = NF$ , se pasa a esta fase.

## Fase de reducción integral

Se encuentra el menor valor no tachado, restándose de los elementos libres y sumándose a los que están en la intersección, luego se repite la fase de conexión de ceros adyacentes. En la Tabla 2.6, se marcó el 12 como valor menor no tachado.

*Tabla 2.6.* Resultados reducción integral.

28	0	0	14
0	16	12	16
0	12	4	0
50	2	0	0

LT = 4  
NF = 4  
LT = NF

Fuente: Elaborado por el grupo de investigación

Como se valida que  $LT = NF$ , se adelantará entonces el proceso de asignación.



## Fase de asignación

Se lee la matriz obtenida, desde la primera fila hasta la última, buscando el primer cero; al hallarse se marca con 1 y se reemplazan los demás elementos por \*. Debe tenerse presente que por cada columna sólo debe existir un 1, hecho que exige que en la tercera fila se tome como elemento de verificación de marcación el situado en la columna 4, tal como se observa en la Tabla 2.7.

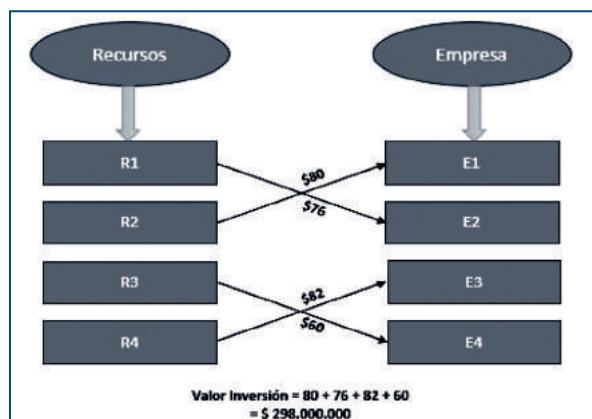
*Tabla 2.7. Matriz de asignación de recursos.*

	E1	E2	E3	E4
R1	*	1	*	*
R2	1	*	*	*
R3	*	*	*	1
R4	*	*	1	*

*Fuente:* Elaborado por el grupo de investigación.

## Fase de lectura y valoración

Se construye el grafo de asignación y se valora el costo de inversión, Cada empresa proveerá un solo recurso para asegurar transparencia en el proceso de adquisición, al momento de negociar con la Alcaldía Local correspondiente (ver figura 2.22).



*Figura 2.22. Grafo de asignación.*

*Fuente:* Elaborado por el grupo de investigación.



## Calendario de ejecución

Se define de común acuerdo con el grupo responsable, que designe cada localidad.

## Entregable

Carta de solicitud de adquisición elaborada por los responsables de la localidad, según la sugerencia de selección óptima que se detalló anteriormente. El proceso de negociación no requiere de la presencia directa del grupo de ingeniería de la Universidad Libre, hecho que por supuesto alude también al líder del proyecto.

## • 2.6 Fase de configuración tecnología

### Objetivo

Realizar el proyecto de instalación y configuración de la base tecnológica que se demanda, previa disposición del espacio físico que la localidad asigne. Espacio que con antelación permitió la realización de acometidas eléctricas, punto de conectividad lógica computacional y reguladores de seguridad física para prevención de incendios, inundaciones y sustracción de componentes.

### Responsables

Personal técnico delegado por la Junta de Acción Local y la Junta de Acción Comunitaria, previa autorización de la Alcaldía Local, y correspondientes certificaciones de normatividad de calidad que expida el líder el proyecto adscrito al programa de Ingeniería de Sistemas de la Universidad Libre.

### Soporte operacional

- Planos físicos de operación.
- Reporte de validación por parte de técnicos electricistas y certificaciones de conexión computacional.



- Certificado de funcionalidad para evitar problemas relacionados contra incendios e inundaciones o posibles saqueos.

## Calendario de ejecución

Treinta (30) días antes de elaborar el acta de liberación por parte del líder del proyecto a la Alcaldía Local, como garantía de apertura y difusión a servicios a ofrecer.

## Entregable

Portafolio elaborado por el líder del proyecto con destino al alcalde local, el cual contiene:

- Certificados de calidad de instalación.
- Certificados aspecto de conectividad electrónica y sanitaria.
- Certificados de seguridad de acceso físico.
- Esquema de mejorías y ajustes.

## • 2.7 Fase de configuración de servicios

### Objetivo

Instalación, configuración y normalización administrativas del conjunto de servicios que contempla el proyecto MESH-UNILIBRE, servicios que se dieron a conocer en su momento a las autoridades que asignó la Alcaldía Local, de manera conjunta con las Juntas de Acción Local y las Juntas de Acción Comunitaria.

### Responsable

Grupo designado por el programa que habrá de reportar el administrador de la plataforma que designe la Alcaldía Menor, según lo dispuesto por la Juntas de Acción Local y las Juntas de Acción Comunitaria correspondientes.



## Soporte operacional

El servidor dispuesto por cada localidad almacenará por sugerencia del proyecto los módulos siguientes:

- Formación educativa
- Formación en ofimática.
- Manejo de herramientas especiales.
- Uso de herramientas de gestión empresarial.

## Tablero de clasificados

- Ofertas de empleos y labores encontrados en la localidad o fuera de ella.

## Directorio de PyMEs y negocios

- Listado de pequeñas y medianas empresas o negocios familiares a nivel de páginas amarillas, para difundir su razón de negocio en el marco geográfico de la localidad.

## Tablero de información logística

- Directorio informativo para acceder a estos centros.
- CAI / Policía Nacional.
- Bomberos.
- Cami.
- Hospital.
- Droguerías.
- Centros educativos.
- Parque / centro de recreación.

## Cartilla de cultura física

- Guía que permitirá a los interesados realizar ejercicios para el mejoramiento físico y cuidado de la salud.



## Espacio de orientación profesional

- En periodos regulares, la comunidad recibirá información sobre temas tratados por profesiones de la justicia, salud, economía, educación y deporte, para facilitar la actualización que beneficia el mejoramiento del nivel de vida de los habitantes interesados.

## Tablero de imagen radial

- Enlace que facilita al interesado tener acceso a la plataforma radial existente cuyo uso libre determina su importancia.

## Entregable

Portafolio que registra la estructura de cada servicio, según expectativa operacional definida por el proyecto integral, desarrollado por la Universidad Libre. El formato del portafolio, será definido por acción conjunta del líder del proyecto y el talento designado por cada alcaldía.

Un ejemplo que para el caso del servicio de formación educativa se requiere el considerar obligatoriamente estas operaciones:

- Registro de usuario (ver figura 2.23).
- Catalogación de cursos.
- Estructura de cursos (ver figura 2.24).
- Validación de temas (ver figura 2.25).

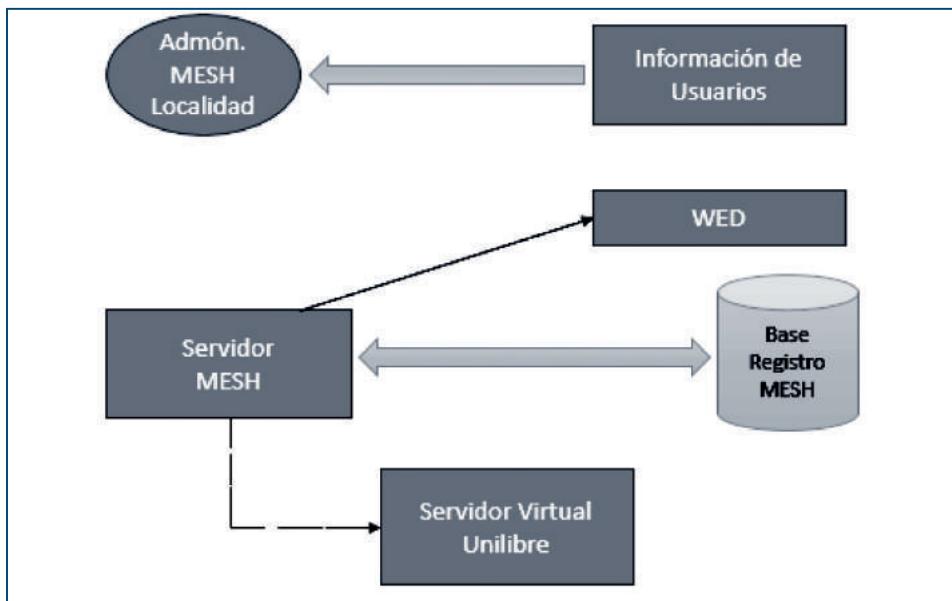


Figura 2.23 Registro de Usuario MESH.

Fuente: Elaborado por el grupo de investigación.

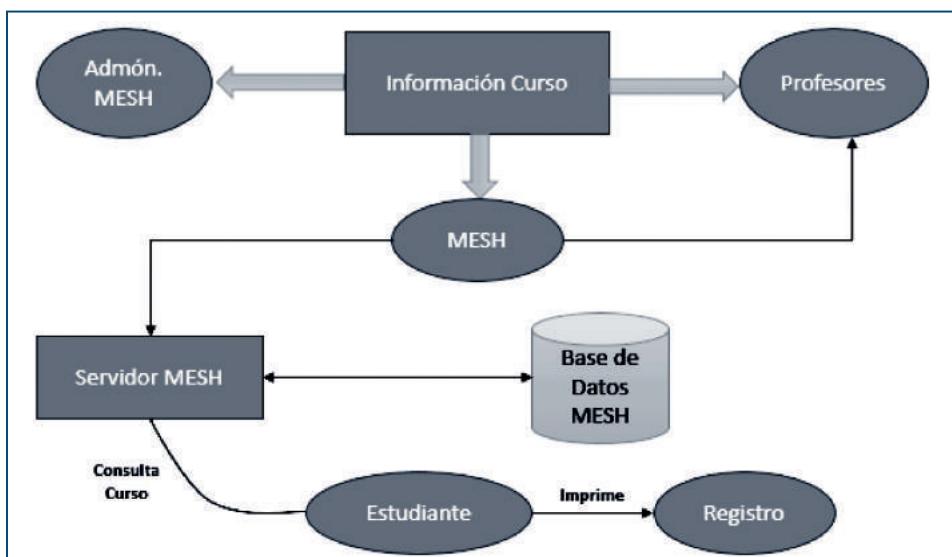
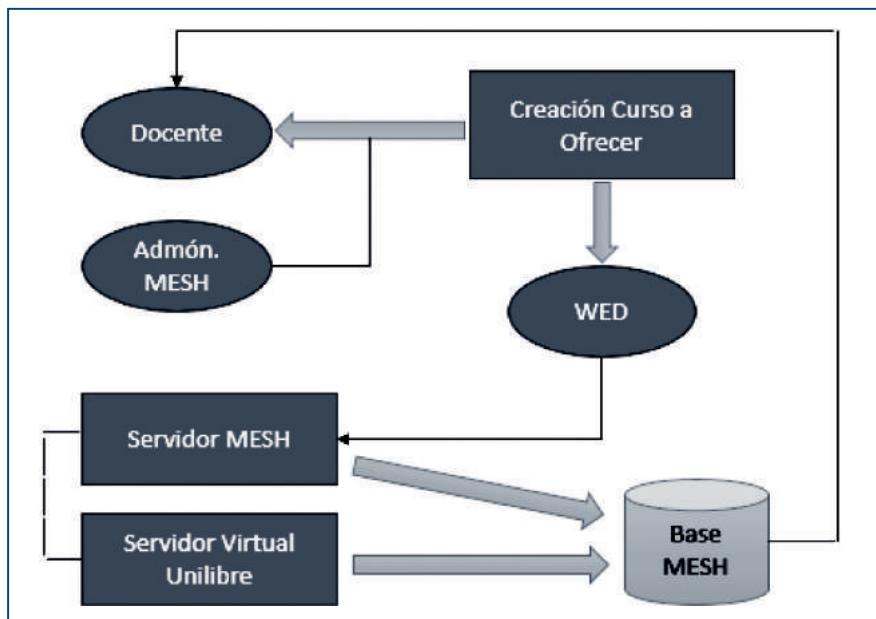


Figura 2.24 Estructura de cursos.

Fuente: Elaborado por el grupo de investigación.



*Figura 2.25* Validación temática de curso.

Fuente: Elaborado por el grupo de investigación.

## • Conclusión

Con el liderazgo de la facultad de ingeniería de la Universidad Libre de Colombia, por medio del grupo de investigación Davincis, el proyecto de redes MESH cuenta con una prueba piloto que se implementará en dos localidades de la ciudad de Bogotá, Cuidad Bolívar y Usme. En esta prueba participan, la Alcaldía Mayor de Bogotá, las alcaldías locales, las juntas de acción comunal, las juntas administradoras locales. En la fase inicial se realizará una contextualización con el fin de dar a conocer las bondades de las redes MESH y posteriormente el respectivo protocolo de presentación ante las instancias mencionadas. Para la implementación, se realizará la fase de configuración tecnológica y de configuración de servicios.





( 3 )

## **Modelo de implementación de protocolo open SSL para el manejo de la seguridad en infraestructura de redes MESH**

- **Introducción**

El protocolo open SSL conocido como el método más confiable de seguridad en internet, con licencia libre, se basa en la administración de bibliotecas criptográficas con una capa de sockets seguros. Para instalar el protocolo, se presenta la configuración de los archivos necesarios para la generación del certificado AC y clave, y, su respectiva implementación en el servidor. Este protocolo también puede usarse para conexiones remotas, por medio, tanto de un Shell interactivo como no interactivo. El uso de los certificados se valida en el marco de seguridad de tráfico de datos para servidor y usuarios.

- **3.1 Esquematización ingenieril**

### **3.1.1 Protocolo OPEN SSL**

Open SSL es un proyecto elaborado en 1998, con el objetivo primordial de establecer comunicaciones seguras en Internet. Consiste en paquetes de administración y bibliotecas de criptografías que se basan en un software libre llamado SSLeay, el cual radica el paquete de instrumentos de



administración y bibliotecas que estén relacionadas con criptografía, con una capa de sockets seguros, relacionando paquetes como Open SSH y navegadores. Este protocolo está basado en una licencia libre y se utiliza para fines comerciales y no comerciales.

### ¿Por qué usar Open SSL?

- Proporciona una conexión segura entre dos partes, es decir, su seguridad es criptográfica.
- También permuta exitosamente parámetros de cifrado desconociendo el código usado por el otro.
- Otorga nuevos métodos de cifrado evitando la elaboración de protocolos.
- Incorpora alguna que otra facilidad que mejora el uso de la red.

### Versiones del protocolo Open SSL

Las distribuciones que se encuentran del protocolo OPENSSL para Linux, son distribuciones binarias para las siguientes versiones:

*Tabla 3.1. Versiones de Open SSL.*

Distribución	Versión Open SSL
SUSE Linux Enterprise Desktop 10 (i586)	Openssl-09.8a-18.4
Debian Etch	0.9.8b-2
Red Hat Enterprise Linyux versión de cliente 4.91 (Tikanga)	Openssl-0.9.8-5
Ubuntu 6.06 LTS	0.9.8A-7Build1
Mandriva Linux 2006.0 realease (oficial= por 586	Openssl-0.9. 7g-2.1-2006mdk
Red hat Desktop versión 4 (Nahant Actualización 3)	Openssl-0.9. 7º-43.8

*Fuente:* Elaborado por el grupo de investigación

### Problemas con el protocolo

El tiempo de reproducción de números aleatorios depende del sistema operativo en el que se tenga el protocolo. Los servicios /dev/urandom/dev/daemon aza o egd, si no se encuentran no es posible producir un código binario compatible que se actúe diferente en tiempo de ejecución.



## Secuencia de eventos de una conexión

Los eventos que suceden entre nodos *host*, necesitan de una ayuda para proteger la integridad de una comunicación. Para ello, se necesitan tres (3) etapas las cuales se mencionan a continuación:

**Capa de transporte:** asegura que el cliente sepa que se está comunicando con el servidor correcto, para luego cifrar la comunicación entre el servidor y el cliente mediante un código simétrico.

**Autentificación:** una vez se tiene la capa de transporte, el cliente se autentica frente al servidor, sin tener que preocuparse por la información de autentificación que pueda exponerse. Open SSL usa clave RSA.

**Canales:** una vez autenticado el cliente frente al servidor, con los canales se puede usar diferentes conexiones como una sesión interactiva Shell, aplicaciones X11 y túneles TPC/IP.

## Archivos de configuración de Open SSL

Para poder tener control en la configuración de Open SSL se requiere la configuración de los siguientes archivos:

- Para tener un número de serie que controle los certificados se emite el comando:  
Cd /ca  
Echo '01' > serial  
Touch index.txt
- Tener una autoridad certificadora. Se crea el fichero de configuración ca/conf  
gedit caconfig.cnf
- Se copia la estructura  
#.....  
[ca]  
default\_ca=CA\_default  
[CA\_default]  
dir = /home/ca



```
Serial = $dir/serial
Database = $dir/index.txt
new_certs_dir = $dir/certs
Certificate = $dir/certs/cacert.pem
Private Key = $dir/private/cakey.pem
Default days = 365
Default_md = md5
Preserve = no
Email in_dn = no
Nameopt = default_ca
Certopt = default_ca
Policy = policy_match
[policy_match]
CountryName = match
StateOrProvinceName = match
OrganizationName = match
OrganizationalUnitName = optional
CommonName = supplied
EmailAddress = optional
[Req]
default_bits = 1024 # Size of keys
default_keyfile = key.pem # name of generated keys
default_md = md5 # message digest algorithm
string_mask = nombstr # permitted characters
distinguished_name = req_distinguished_name
req_extensions = v3_req
[req_distinguished_name]
# Variable name Prompt string
#-----
0. OrganizationName = Organization Name (company)
OrganizationalUnitName = Organizational Unit Name (department,
division)
EmailAddress = Email Address
EmailAddress_max = 40
LocalityName = Locality Name (city, district)
StateOrProvinceName = State or Province Name (full name)
CountryName = Country Name (2 letter code)
```



```
CountryName_min = 2
CountryName_max = 2
CommonName = Common Name (hostname, IP, or your name)
CommonName_max = 64
# Default values for the above, for consistency and less typing.
# Variable name Value
#-----
0. organizationName_default = My Organization
localityName_default = NEW YORK stateOrProvinceName_default
= NEW YORK
countryName_default = US
emailAddress_default = email@mydomain.net
[v3_ca]
basicConstraints = CA: TRUE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer:always
[v3_req]
basicConstraints = CA: FALSE
subjectKeyIdentifier = hash
```

### • 3.2 Generación de certificado AC y clave

En este punto es necesario tener en cuenta que el nombre de AC debe ser igual en todos los certificados. Para generarlos se utiliza este código:

```
openssl req -new -x509 -extensions v3_ca -keyout private/cakey.pem
-out certs/cacert.pem -days 365 -config conf/caconfig.cnf
```

Este genera un certificado válido por un año, llamado cacert.pem en el directorio “certs” y una clave privada RSA cakey.pem, que se guarda en el directorio “private”.

### • 3.3 Generación de certificado servidor cliente

En este paso, se genera una clave privada tanto para el cliente como para la petición firma para CA. Aquí se colocará el nombre del servidor



“www.pruebaCertificadoOpenSSL.com”. Por lo que, después de dirigirse al directorio /home/ca, entonces se lanza el comando de petición del certificado a CA.

El siguiente comando generará la clave “private” y la petición del certificado “certs”:

```
openssl req -new -nodes -out certs/localhost.req.pem -keyout private/localhost.key.pem -config conf/caconfig.cnf
```

## Firma de certificado

En este punto se habilitará como CA, para motivos de seguridad y se hará el certificado que será definitivo, actualizando la base de datos de certificados.

```
openssl ca -in localhost.req.pem -notext -out certs/localhost.cert -config conf/caconfig.cnf
```

## Cambiar la extensión del certificado

Los certificados que se han generado tienen la extensión. pem; para que los navegadores tengan mayor compatibilidad se cambia a la extensión **.crt**, por lo que se conducirá a /home/ca y se ejecutará el comando:

```
rename's/\.pem/\.crt/' *
```

## Implementación real en el servidor

Para poder tener una implementación se tienen que llevar los certificados y las claves a los directorios correctos, ssl.key y ssl.crt; actualizar el fichero de configuración del servidor, el cual va ser “ssl.conf”. En caso de que se utilice Lampp, se deberá dirigir a /opt/lampp/etc/extra/httpd-ssl.conf.

Se requiere crear un servidor virtual, con lo cual se genera la IP local. Después NameVirtualHost \*:443 # para que se active cuando se acceda por el puerto seguro.



En este caso un ejemplo serio:

DocumentRoot /var/www/html

ServerName 127.0.0.1

ServerAdmin certificadoOpenSSL@your.domain

Para poder acceder a log de los errores, se ejecuta el siguiente comando:

ErrorLog /etc/httpd/logs/ssl\_error\_log

TransferLog /etc/httpd/logs/ssl\_access\_log

SSLEngine On

SSLCertificateFile /opt/lampp/etc/ssl.crt/miCertificadoDelServidor.crt

SSLCertificateKeyFile /opt/lampp/etc/ssl.key/miClaveDelServidor.key

Después de hacer esta configuración e implementación se debe reiniciar el servidor, con el cual se ejecuta el siguiente comando:

/opt/lampp/lampp restart

Después de hacer esto, se modifican los ficheros de configuración para comprobar si está bien el documento de configuración. Se debe buscar la línea “Listen 443”, si no se encuentra se debe añadir:

## Un Shell seguro

Una interface de comandos seguros se puede iniciar de muchas formas al usar el SSH. Dada la cantidad apropiada de banda ancha, con sesiones X11 se pueden dirigir canales SSH o también, con el reenvío de TPC/IP se puede asignar a canales específicos, conexión de puertos en varios sistemas que previamente eran inseguros.

## Reenvío por X11

Esta técnica para el uso de aplicaciones de reenvío de x11, proporciona un medio seguro para el uso de aplicaciones gráficas sobre la red. Para poder abrir sesiones X11 a través de conexiones SSH es fácil: se requiere ejecutar cualquier programa desde comandos de Shell seguros, el cliente y servidor SSH crean un nuevo canal dentro de la conexión SSH con lo cual



se torna en un canal seguro, y los datos del programa que se ejecutan se envían a través del canal de la máquina de forma transparente.

Para poder utilizar el reenvío por X11 y crear una sesión segura, se puede utilizar el siguiente comando utilizando el servidor SSH:

- **Up2date &** Después de haber proporcionado la contraseña de *root* para el servidor que se está utilizando, el agente de actualización para el *Red Hat* aparecerá permitiendo al usuario remoto actualizar el sistema remoto de forma segura.
- Con SSH se pueden asegurar los protocolos TCP/IP mediante el reenvío de puertos. Al momento de usarlo, el servidor convierte el conducto encriptado para el cliente SSH. El reenvío de puertos se hace mediante un mapeo de un puerto local en el cliente a un puerto remoto del servidor, permitiendo mapear cualquier puerto desde el servidor a cliente, así los números de puerto no coincidan.

Para poder crear el canal de reenvío se utiliza el siguiente comando, es necesario estar como root:

```
ssh -L local-port:remote-hostname:remote-port username@hostname
```

Para poder realizar la verificación del correo en el servidor usando POP3 a través de la conexión encriptada, se puede usar el siguiente comando:

```
ssh -L 1100: mail.example.com:110 mail.example.com
```

Una vez el canal de reenvío del puerto se encuentra entre el servidor de correo y la máquina cliente, se puede direccionar el cliente POP3 para ser usado en el puerto 1100 en el *host* local.

El reenvío de puerto se usa principalmente para obtener información segura a través de los *firewalls* de red. El *firewall* debe estar configurado para que permita el tráfico SSH a través del puerto estándar aunque este bloquee el acceso a través de otros puertos, sin embargo, todavía se puede hacer la conexión entre dos *hosts*, usando los puertos bloqueados al redireccionar la comunicación de una conexión SSH ya establecida.



## Open SSL para conexiones remotas

Para poder realizar conexiones seguras remotas, se utilizará OpenSSL para la conexión segura al servidor de Entrada y Salida virtual. Para poder tener la conexión se realizan los siguientes pasos:

- a) Se necesita tener configurado e instalado el OpenSSL.
- b) Conectarse al Servidor de E/S virtual. Dependiendo de la versión que se utilice, se puede conectar mediante una Shell interactiva o no interactiva. Si se tiene una versión anterior a la 1.3.0, se puede conectar utilizando una Shell interactiva, si se tiene una versión superior a la 1.3.0, se puede conectar con una versión interactiva o no interactiva. A continuación, se mostrarán los dos procesos:

### Conección con un Shell interactivo

- Se debe escribir el siguiente comando para conectar el sistema remoto:  
ssh nombre\_usuario@nombre\_sis\_prin\_vi
- Donde el nombre\_usuario es el usuario para el servidor de E/S virtual.
- Nombre\_sis\_prin\_vi es el nombre del Servidor virtual de E/S.

### Conección con un Shell no interactivo

- Se debe escribir el siguiente comando para conectar el sistema remoto:  
ssh  
nombre\_usuario@nombre\_sis\_prin\_vi  
Mandato.
- Donde el nombre\_usuario es el usuario para el servidor de E/S virtual.
  - nombre\_sis\_prin\_vi es el nombre del Servidor virtual de E/S.
  - mandato es el mandato que se desea ejecutar. Ejemplo ioscli Lsmap - all.



Autenticación SSH. Si se utiliza una versión 1.3.0 o posterior, la autenticación se realiza mediante claves o contraseñas. Si se utiliza una versión previa, se realiza la autenticación sólo usando contraseñas.

## Autenticación mediante contraseña

Se especifica el nombre de usuario y la contraseña que solicite un cliente SSH.

## Autenticación mediante claves

Para tener una autenticación con clave se realizarán los siguientes pasos:

- Crear un directorio denominado **\$HOME/.ssh** para generar claves públicas y privadas. Un ejemplo en donde se puede ver esto es:  
`ssh-keygen -t rsa`

Este mandado creará archivos con el siguiente directorio **&HOME/.ssh:**

Clave privada: `id_rsa`  
Clave pública: `id_rsa.pub`

- Se ejecuta el siguiente mandato para añadir la clave pública al archivo `authorized_keys2` del sServidor de E/S virtual:  
`Cat $HOME/.ssh/archivo_clave_publica | ssh Nombre_usuario @nombre_sist_principal_vios tee -a /home/nombre_usuario/.ssh/authorized_keys2`

Dónde

- Archivo\_clave\_publica es el archivo de clave pública que se generó en el paso anterior. Ejemplo `id_rsa.pub`
- Nombre\_usuario es el nombre de usuario para el servidor de E/S virtual
- Nombre\_sis\_principal\_vios es el nombre del Servidor de E/S virtual



En el servidor de E/S este no podría incluir las versiones recientes de OpenSSL con cada releases de Servidor E/S virtual. Se tendría que estar descargando y actualizando el OpenSSL.

## Instalar y configurar Open SSL

Para poder instalar y configurar Open SSL, se necesita tener el paquete de instalación para poder descargarlo y se debe dirigir a la carpeta donde se guardará (en este caso es la siguiente: **Dom:cd /home/openSSL/**).

Después se ejecuta el siguiente comando: **wget http://www.openssl.org/source/openssl-1.0.1e.tar.gz**

Al finalizar la descarga del archivo, se ejecuta el siguiente comando: **tar - xvzf openssl-1.0.1e.tar.gz**

Una vez se haya descomprimido el archivo, hay que ir a la carpeta **openssl-1.0.1e** y ejecutar el siguiente comando: **/config -fPIC shared -prefix=/usr -openssldir=/etc/ssl**

Después, se utiliza el comando “make” para ejecutar. A continuación, se crea un directorio con el nombre OpenSSL para poder instalar el OpenSSL con el siguiente comando: **mkdir /home/installacion/openssl**

Y se ejecuta el comando para la instalación:

**Make install INSTALL\_PREFIX=/home/installacion/openssl/**

Una vez haya finalizado la instalación, se visualizarán los archivos en la carpeta que se instaló el protocolo para poder configurar el mismo.

Para la configuración se requiere entrar a la carpeta **/etc/ssl/openssl.cnf** y cambiar lo que se requiera, fecha de caducidad de entrada, nombre de la organización, etc. Los parámetros que pueden ser cambiados son los que están entre [ CA\_default ] y especialmente los [req\_distinguished\_name].



## Generación de certificados

La generación de certificados digitales para sitios web se puede realizar de la siguiente forma:

- Crear un directorio de trabajo /etc/apache2/ssl-local  
# Cd /etc/apache2  
# mkdir ssl-local  
# Cd ssl.local  
# mkdir certificados privado
- Se generan los archivos de control para el ente certificador  
# Echo '01' > serial  
# Touch index.txt
- Se copia el archive openssl.cnf a /etc/apache2/ssl-local.  
Este se encuentra en los anexos con el nombre “openssl.cnf”.
- Se generan los datos del ente certificador  
# Cd ./apache2/ssl-local  
# openssl req -new -x509 -extensions v3\_ca -keyout privado/cakey.pem  
-out cacert.pem  
-Days 3650 -config ./openssl.cnf
- Creando un certificado para un dominio
- Se crea el directorio de trabajo  
# Cd /etc/apache2/ssl-local  
# mkdir certificados/midominio.com
- Se crea el CSR (Certificate Signing Request)  
# openssl req -new -nodes -out certificados/midominio.com/midominio.com.csr -config ./openssl.cnf
- Creando las llaves  
# Mv key.pem certificados/midominio.com/midominio.com.key



```
# openssl rsa -in certificados/midominio.com/midominio.com.key  
-out certificados/  
midominio.com/midominio.com.key-unenc
```

○ Creando certificado openSSL

```
# openssl ca -out certificados/midominio.com/midominio.com.CERT  
-config ./openssl.cnf  
-Days 3650 -infiles certificados/midominio.com/midominio.com.csr
```

### • 3.4 Uso de los certificados

La utilidad de los certificados es para volver seguros los datos de tráfico que son enviados y recibidos entre usuario y servidor. Los certificados pueden ser autofirmados (por la misma empresa que necesita un certificado) o firmados por una autoridad certificadora.

La diferencia (y desventaja) del certificado autofirmado es que como no está firmado por la autoridad certificadora, el navegador no lo reconoce en la lista de certificados confiables que tiene por defecto, por lo que demandará al usuario conectado a que acepte el certificado para asegurar la conexión segura, pero si éste se siente inseguro y no acepta, no se podrá conectar al servidor Web seguro<sup>103</sup>.

Al respecto, el certificado SSL es una acreditación electrónica que incluye el protocolo SSL, el cual protege los datos e información personal y verifica que una persona, dispositivo y/o empresa sea quien dice ser, por lo que genera confianza entre los usuarios.

El funcionamiento de certificado SSL es el siguiente:

- Primero, el servidor creará dos claves numéricas encriptadas, una privada y otra pública.
- La clave privada debe ser confidencial, pues ésta es la que descodifica el tráfico de datos encriptado. La clave pública es aquella que se encuentra en el directorio *Certificate Signing Request (CSR)* y



la cual abarca detalladamente su identidad, por lo que es la que codifica el tráfico de datos.

- Entonces cuando el usuario se conecta, el servidor Web le envía el certificado SSL al navegador con clave pública y así, con la clave privada que sólo posee el servidor Web, el navegador del usuario reconocerá a dicho servidor y lo aceptará sin ponerle objeciones.

Ahora bien, ¿Cómo saber si la página web que se está viendo está conectada a un servidor Web protegido por el certificado SSL?

Existen dos opciones que pueden verificar esto:

- Cuando la URL de la página web que se está visitando empieza por HTTPS (como se ve a primera vista, se le ha añadido una “S” al HTTP común y corriente, de manera que la “S” significa que es segura esa conexión). Esto se puede observar en la Figura 3.1.

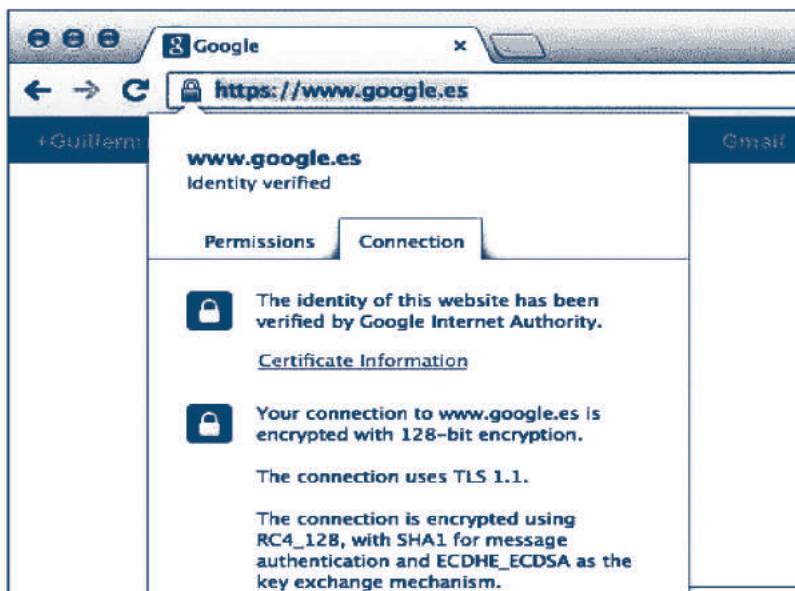


*Figura 3.1 Verificación del certificado SSL.*

Fuente: Velázquez (2009).

- En una de las partes de la ventana del navegador se visualiza un ícono con forma de candado cerrado (*Secured Seal*), y si se da clic sobre este se mostrará una pantalla con toda la información del certificado SSL y los datos de la Autoridad Certificadora (CA) que firmó este certificado.

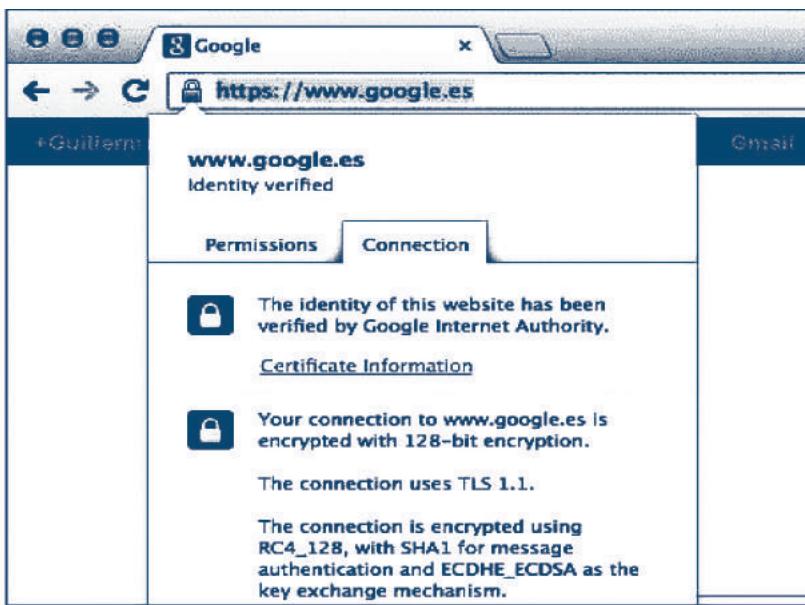
Si por ejemplo, se utiliza Google Chrome como navegador el candado cerrado aparecerá a la izquierda del HTTPS como se puede percibir en la Figura 3.2.



*Figura 3.2 Verificación del certificado SSL en Google Chrome.*

*Fuente:* Julian (2015).

Por el contrario, si el navegador es Internet Explorer el candado aparecerá a la derecha de la URL, como se contempla en la Figura 3.3.



*Figura 3.3 Verificación del certificado SSL en Internet Explorer.*

*Fuente:* Elaborado por el grupo de investigación.

## • Conclusión

Uno de los propósitos de la prestación de un servicio de conectividad, como el caso de redes MESH, es el de brindar comunicaciones seguras. Por esto, se contempla el protocolo open SSL con funciones criptográficas que establece canales seguros del tráfico de datos, usando clave y generando certificados, con el objetivo de asumir autenticidad de las personas, entidades y mensajes.



( 4 )

## Diseño de una arquitectura de streaming para Redes MESH en entornos de bajos recursos en Colombia

### • Introducción

La arquitectura de streaming para redes MESH en entornos de bajos recursos en Colombia requiere calcular el consumo de ancho de banda de acuerdo con las expectativas de audio y video para una adecuada emisión. Las respectivas conversiones y estimaciones se presentan teniendo como referencia el consumo por hora y las características de emisión. Para el montaje del servicio, se tiene en cuenta el paso a paso de las operaciones en el servidor para iniciar la emisión de contenido y su posterior visualización.

### • 4.1 Montaje del servicio Streaming sobre plataformas de software libre

Se debe definir el servicio o los servicios que se van a ofrecer (video, audio, radio, video conferencia, entre otros). Así mismo, es importante identificar la herramienta o *software* que se necesita, el *hardware* y la zona donde se prestará el servicio.



Se realizará énfasis en la transmisión y administración de contenido multimedia a través de puntos de acceso (dispositivos con conexión a redes Wireless).

El servicio estará compuesto por un nodo servidor que emitirá todo el contenido a los diferentes nodos receptores que puedan existir. Para este caso, el nodo emisor se encontrará en una máquina con sistema operativo Linux/Ubuntu en versión 14.04, el cual emitirá a través de un *Freeware Multimedia* llamado VLC Media Player.

Los nodos receptores pueden ser dispositivos móviles o dispositivos de escritorio, estos pueden tener cualquier sistema operativo, ya que para recibir el contenido sólo se necesita la misma herramienta de emisión (VLC Media Player) (ver figura 4.1).

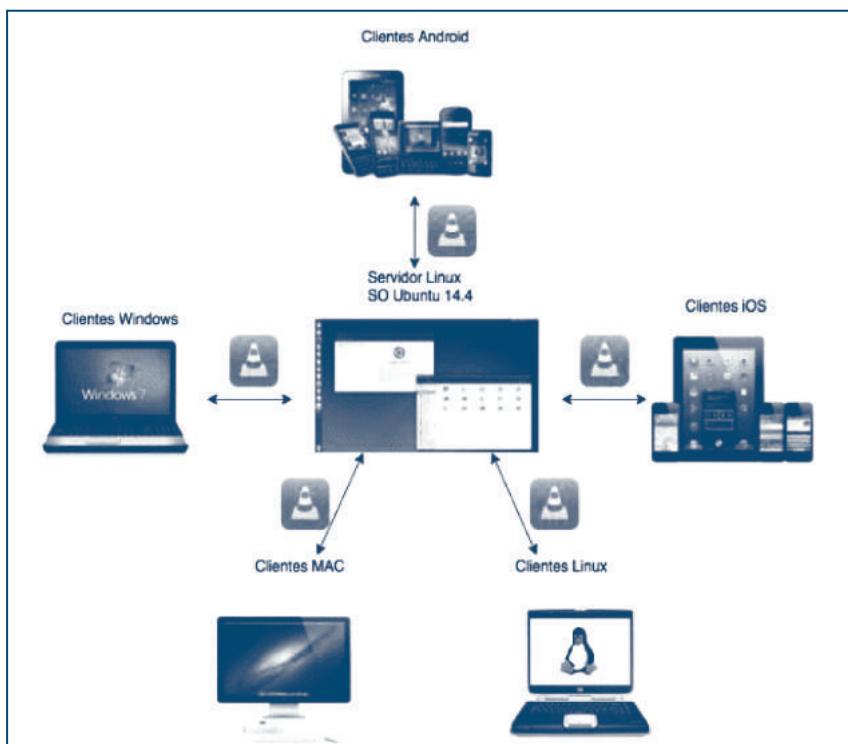


Figura 4.1 Estructura servicio.

Fuente: Aporte del Autor.



#### 4.1.1 Ancho de banda requerido

Para la realización de *streaming*, este se calcula en kilobits por segundo (kbps). Es importante distinguir que kilobits y kilobytes son diferentes. Para convertir kilobits por segundo a kilobytes por segundo, debe dividir el tamaño del *streaming* entre 8, ya que hay 1.024 kilobytes en un megabyte y 1024 megabytes en un gigabyte.

Para calcular el consumo de ancho de banda y gigabytes, se realizan las siguientes operaciones:

- **Dividir X8:** en primer lugar, se debe convertir (dividir) la tasa de flujo deseada (kilobits por segundo) entre el número 8 (kilobits a kilobyte factor de conversión) para obtener el número de kilobytes por segundo, y luego:
- **Multiplicar X60:** se debe multiplicar el resultado por 60 (segundos) para obtener los kilobytes por minuto.
- **Multiplicar X 60:** se debe multiplicar este resultado por 60 (minutos) para obtener kilobytes por hora.
- **Dividir X 1024:** a continuación, se deben tomar los kilobytes por hora y dividirlos entre 1024 (tasa de conversión de kilobytes a megabyte) para calcular megabytes por hora.

Una vez se hayan calculado los megabytes por hora (Mb / hora), se puede tomar esta información y calcular el consumo de ancho de banda.

A continuación, se presentan las fórmulas para calcular el ancho de banda necesaria para la transmisión de audio y de video.

##### Fórmula de audio:

Primero se calculan los megabytes por hora.

$$Y \frac{mb}{H} = \frac{\left( \left( \left( \frac{x \text{ kbps}}{8 \text{ factor de conversión}} \right) * 60 \text{ segs} \right) * 60 \text{ mins} \right)}{1024 \text{ kbs}} \quad (47)$$



Luego se calculan el número de horas que se podrá transmitir con determinado ancho de banda.

$$\text{Número de horas} = \frac{\text{Ancho de banda}}{(48)}$$

### Fórmula de video:

Primero se calculan los megabytes por hora, formula 48

Luego se calcula el ancho de banda necesario a partir de la siguiente formula.

*Ancho de banda*

$$= \frac{\left( \left( H \frac{mb}{H} * \text{horas consumidas} \right) * \text{No. horas por día} \right) * \text{No días}}{1024 kbs} \quad (49)$$

Una vez se conocen los anchos de banda se pueden realizar los cálculos necesarios para una emisión ideal, es por ello que se debe transmitir a un 50% o 66% de la velocidad de subida. Por ejemplo, para transmitir el vídeo a calidad móvil de 200Kbps, con una conexión de 512Kpbs debería ser más que suficiente. Con una mega de subida, se podrá transmitir correctamente una señal de vídeo de entre 400Kbps a 600Kbps. Los servicios más comunes y sus consumos en anchos de banda se presentan en la tabla 4.1.

*Tabla 4.1* Consumo ancho de banda mbps

	Bajada	Subida
VoIP	0,1	0,1
Navegación	0,5	0,1
Email	0,5	0,5
YouTube	0,7	0,1
Skype HD	1,5	1,5
Netflix	3,8	0,1

*Fuente:* Elaborado por el grupo de investigación.



En cuanto al esquema multibitrate, simplemente se tiene que hacer la suma de todas las calidades que desea transmitir. Por ejemplo:

- Normal + Móvil = 400 kbps + 200 Kbps = 600 Kbps
- HD + Normal + Móvil = 1300 kbps + 400 kbps + 200 Kbps = 1900 Kbps

Las resoluciones en pixeles y las velocidades constantes mínimas de subida para realizar la transmisión de video son:

- 640p\*360p= 750 kbps
- 640p\*480p= 1Mbs
- 640p\*720p=2,5 Mbps
- 640p\*1080p = 4,5 Mbps

Las conexiones a Internet también se miden en Kilobits por segundo (no Kilobytes, 1 byte=8bits). Así que el bitrate del video tiene la misma medida que el bitrate de la conexión a Internet. Si se tiene 1 mega de subida, es equivalente a decir se tiene 1024 Kbps de subida.

Luego, se debe tener en cuenta que la velocidad de conexión fluctúa, por las características de la red. Es por ello que nunca se debe intentar transmitir a un bitrate muy próximo al límite de velocidad de la conexión a Internet. Además, la velocidad de subida contratada de un servicio de Internet realmente nunca va a llegar a tener la velocidad por la que fue contratada.

#### 4.1.2 Video

Antes de iniciar a compartir video a través de *streaming* se debe definir:

- Con qué calidad de video se desea transmitir, es decir, que a mayor calidad de video, mayor será el bitrate que este posea y por ende, mayor tamaño del archivo.
- Qué dispositivos se utilizarán (móviles, escritorio o ambos).
- Con qué calidad se desea transmitir el contenido.

Al identificar los ítems anteriores, se pueden comenzar a establecer los requerimientos necesarios que permitan la transmisión de contenido, por ejemplo:



- Video con buena calidad: se puede realizar a partir de un bitrate de 200kbps.
- Usuarios con PC o portátiles: se necesita mejor calidad de video, haciendo necesario un bitrate de 400Kbps.
- Video con calidad alta: se necesita un bitrate de 800kbps.
- Video en Alta Definición HD: se necesita un bitrate que esté desde los 1300kbps.

#### 4.1.3 Audio

Para transmitir voz con las siguientes características se necesita de las siguientes velocidades:

- Calidad alta: necesita alrededor de unos 64 kbitps.
- Música de alta fidelidad: requiere 1.2 Mbitps.

Gracias a las ventajas del procesado digital, la información se puede comprimir eliminando toda la información redundante, de manera que un canal de vídeo comprimido típico, como los de televisión digital por satélite, puede ocupar alrededor de 1.2 Mbit/s, 20 veces menos que la velocidad de transmisión (anchura de banda) original.

#### 4.1.4 Montaje del servicio y emisión

Es importante tener presente que los equipos deben encontrarse en las mismas frecuencias de red. Se inicia instalando el sistema operativo Linux-Ubuntu, en la máquina que se eligió para que sirva como servidor y luego:

- Se abre la consola para ejecutar el siguiente comando, que instala icecast; permitiendo que la máquina funcione como server.  
**O** `sudo apt-get install icecast2`
- Luego de ejecutar el anterior comando, comenzará el proceso de instalación (ver figura 4.2).

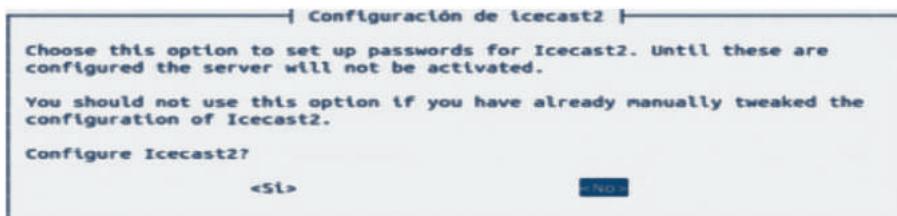


```
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Paquetes sugeridos:
  icecast2
Se instalarán los siguientes paquetes NUEVOS:
  icecast2
0 actualizados, 1 se instalarán, 0 para eliminar y 36 no actualizados.
Necesito descargar 221 kB de archivos.
Se utilizarán 702 kB de espacio de disco adicional después de esta operación.
0x [Conectando a pe.archive.ubuntu.com]
```

*Figura 4.2 Instalación Icecast2.*

Fuente: Elaborado por el grupo de investigación.

Después aparecerá una ventana preguntando si se desea configurar una contraseña para el acceso al Icecast2, se elegirá la opción “no”, ya que se efectuará la configuración manualmente (véase figura 4.3).



*Figura 4.3 Configuración contraseña iceast2.*

Fuente: Elaborado por el grupo de investigación.

- Al finalizar la instalación del Icecast2, se inicia la instalación de Oggfwd (véase figura 4.4) y FFmpeg, (véase figura 4.5) los cuales permiten difundir el contenido al servidor y la codificación del contenido, respectivamente. Para esto se deben ejecutar los siguientes comandos en la terminal:

a) sudo apt-get install oggfwd

```
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  oggfwd
0 actualizados, 1 se instalarán, 0 para eliminar y 36 no actualizados.
Necesito descargar 9.248 kB de archivos.
Se utilizarán 51.2 kB de espacio de disco adicional después de esta operación.
Des:1 http://pe.archive.ubuntu.com/ubuntu/ precise/universe oggfwd i386 0.2-6 [9
.248 kB]
Descargados 9.248 kB en 1seg. (5.274 B/s)
Seleccionando paquete oggfwd previamente no seleccionado
(Leyendo la base de datos ... 144633 ficheros o directorios instalados actualmen
te.)
Desempaquetando oggfwd (de .../archives/oggfwd_0.2-6_i386.deb) ...
Procesando disparadores para man-db ...
```

*Figura 4.4 Instalación codificador OGG.*

Fuente: Elaborado por el grupo de investigación.



b) sudo apt-get install ffmpeg2theora

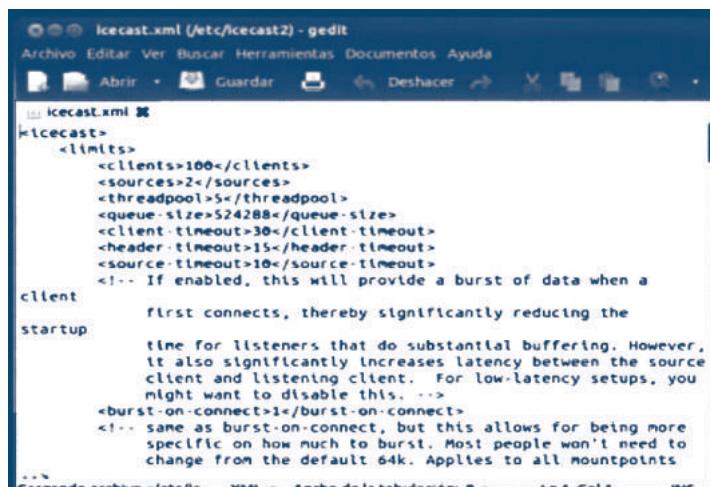
```
Leyendo lista de paquetes... Hecho
Estando árbol de dependencias
Leyendo la información de estado... Hecho
se instalarán los siguientes paquetes extras:
 libavcodec53 libavdevice53 libavformat53 libavutil51 libdc1394-22 libgsml
 libkate liboggkate libpostproc52 libschroedinger-1.0-0 libswscale2 libvai
 libvpx1
Se instalarán los siguientes paquetes NUEVOS:
 ffmpeg2theora libavcodec53 libavdevice53 libavformat53 libavutil51
 libdc1394-22 libgsml libkate liboggkate libpostproc52
 libschroedinger-1.0-0 libswscale2 libvai libvpx1
0 actualizados, 14 se instalarán, 0 para eliminar y 30 no actualizados.
Necesito descargar 8.139 kB de archivos.
Se utilizarán 21,1 MB de espacio de disco adicional después de esta operación.
[Desea continuar [S/n]? s
Desi: http://pe.archive.ubuntu.com/ubuntu/ precise-updates/main libavutil51 1386
4:0.8.5-0ubuntu0.12.04.1 [129 kB]
Desi: http://pe.archive.ubuntu.com/ubuntu/ precise/main libgsml 1386 1.0.13-3 [2
7.6 kB]
Desi: http://pe.archive.ubuntu.com/ubuntu/ precise/main libschroedinger-1.0-0 13
86.1.0-1 [293 kB]
Desi: http://pe.archive.ubuntu.com/ubuntu/ precise/main libvai 1386 1.0.15-4 [37
.6 kB]
8x [4 libvai 16.3 kB/37.6 kB 43%]
73.9 kB/s 1min. 43seg.
```

*Figura 4.5 Instalación codificador FFmpeg.*

Fuente: Elaborado por el grupo de investigación.

- Luego de completar las instalaciones, se debe acceder al archivo de configuración del Icecast2 (véase figura 4.6), a través de los siguientes comandos:
  - cd /etc/icecast2
  - sudo gedit icecast.xml

Al ejecutarse los anteriores comandos aparecerá la siguiente pantalla:



*Figura 4.6 Archivo de configuración Icecast.*

Fuente: Elaborado por el grupo de investigación.



Se recomienda no realizar modificaciones en este archivo de configuración, excepto en las etiquetas de contraseñas, para tener el acceso personalizado, y la etiqueta de <hostname>. En las etiquetas de contraseñas, por defecto, se encuentra “*hackme*”, se puede dejar tal cual o cambiarla por la contraseña que se deseé.

En la etiqueta de hostname viene por defecto “*localhost*”, esta etiqueta se debe cambiar por la dirección IP del equipo servidor. Luego se guardan los cambios en el archivo y se cierra.

Al realizar los cambios mencionados, se debe realizar el cambio en la configuración del Icecast2 para que el servicio se inicie automáticamente una vez se inicie la máquina (véase figura 4.7). Para eso se debe ejecutar la siguiente línea de comando:

- sudo gedit /etc/default/icecast2

Luego aparece la siguiente pantalla.

```
icecast2 x
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
Abrir Guardar Deshacer
icecast2
# Defaults for icecast2 initscript
# sourced by /etc/init.d/icecast2
# installed at /etc/default/icecast2 by the maintainer scripts

#
# This is a POSIX shell fragment
#

# Full path to the server configuration file
CONFIGFILE="/etc/icecast2/icecast.xml"

# Name or ID of the user and group the daemon should run under
USERID=icecast2
GROUPID=icecast

# Edit /etc/icecast2/icecast.xml and change at least the passwords.
# Change this to true when done to enable the init.d script
ENABLE=false

Cargando archivo... Texto plano Archivo de tabulación: R+ Int. Col1 INC
```

*Figura 4.7* Configuración auto inicio icecast2.

Fuente: Elaborado por el grupo de investigación.



En la línea de ENABLE, se cambia “false” por “true”. Se guardan los cambios y se cierra el archivo.

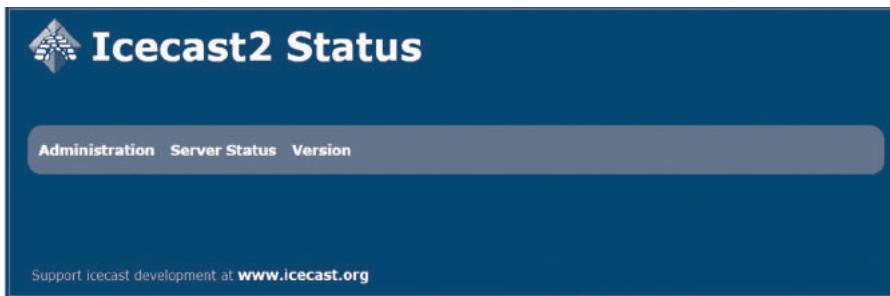
- Luego se iniciará el servicio del Icecast2 con la siguiente línea de comando:
  - sudo service icecast2 start
- Se comprueba el funcionamiento del servicio, ingresando por medio de cualquier explorador y digitando en la barra de búsqueda la IP del servidor con el puerto que esta predeterminado para el acceso (véase figura 4.8).



*Figura 4.8 Ejemplo dirección de servidor streaming.*

Fuente: Elaborado por el grupo de investigación.

Si el servicio está corriendo correctamente debería aparecer la página principal del servidor (véase figura 4.9).



*Figura 4.9 Servidor Icecast en ejecución.*

Fuente: Elaborado por el grupo de investigación.

#### 4.1.5 Emisión de contenido

Se emitirá contenido con la herramienta de software libre llamada VLC.

- Se inicia instalando el software a través de la ejecución de la siguiente línea de comando.
  - sudo get-apt install vlc



Al culminar la instalación, se podrá iniciar el *streaming* de contenido accediendo a la pestaña de “Medio” y a la opción de Emitir (véase figura 4.10).



Figura 4.10 Menú “Medio” en VLC.

Fuente: Elaborado por el grupo de investigación.

Una vez seleccionada esta opción, aparecerá una ventana en la cual se añadirán los archivos de audio o de video que se desean emitir (véase figura 4.11).

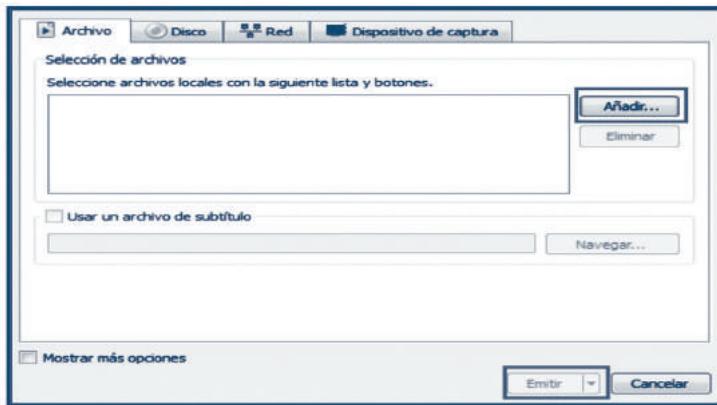


Figura 4.11 Ventana para añadir archivos a emitir.

Fuente: Elaborado por el grupo de investigación.

Dando clic en el botón “Añadir”, se podrán agregar los archivos. Una vez seleccionados los archivos, hacer clic en el botón emitir.



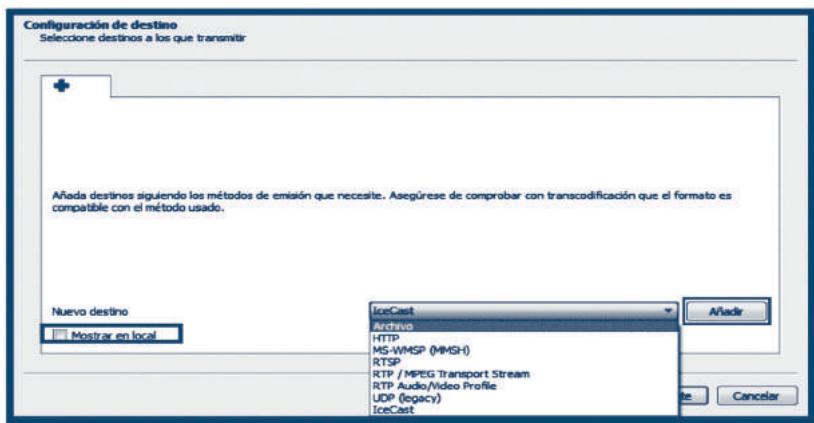
- Luego de que se hallan elegido los archivos, se comprobará la fuente de donde se usarán los archivos a transmitir (véase figura 4.12).



*Figura 4.12 Ventana configuración fuente de contenido.*

*Fuente:* Elaborado por el grupo de investigación.

Al hacer clic en “Siguiente” el proceso llevará a la pantalla de configuración del medio de transmisión de la lista desplegable, donde se debe elegir IceCast y dar clic en añadir. El checkbox “Mostrar en Local”, es una opción para reproducir localmente lo que se va a emitir, puede o no seleccionarse (véase figura 4.13).

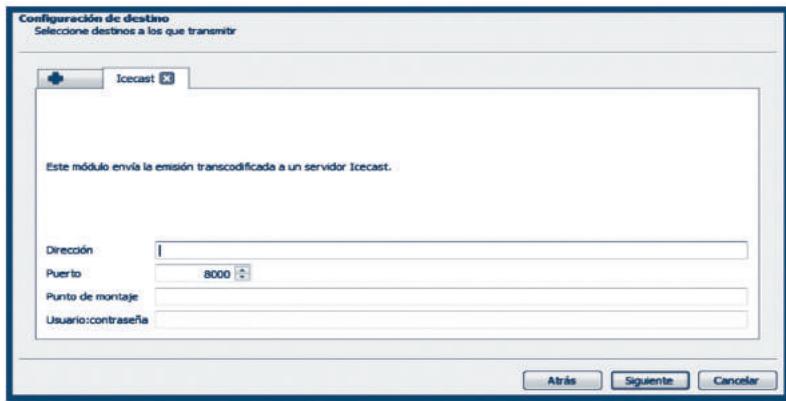


*Figura 4.13 Selección de servicio de transmisión.*

*Fuente:* Elaborado por el grupo de investigación.



Luego aparecerá la pantalla de configuración de Icecast (véase figura 4.14).



**Figura 4.14** Configuración Icecast en VLC.

Fuente: Elaborado por el grupo de investigación.

Se diligencia y/o escoge lo siguiente:

- Dirección: es la dirección IP del servidor. La misma que se configuró en el archivo del Icecast2 en la etiqueta <hostname>.
- Puerto: puerto configurado para el acceso al servicio. Por defecto, es el puerto 8000.
- Punto de montaje: nombre del archivo en el cual va a estar contenido la emisión y el cual descargarán el cliente del *streaming*. Este nombre puede ser el que desee el administrador.
- Usuario/contraseña: son el usuario y contraseña configurados para acceso al Icecast. Por defecto son “source” y “hackme”.

Para un ejemplo de la configuración de VLC con Icecast véase la figura 4.15.

Dirección	192.168.0.23
Puerto	8000
Punto de montaje	Canción
Usuario: contraseña	Source: hadome

**Figura 4.15** Ejemplo configuración Icecast.

Fuente: Elaborado por el grupo de investigación.

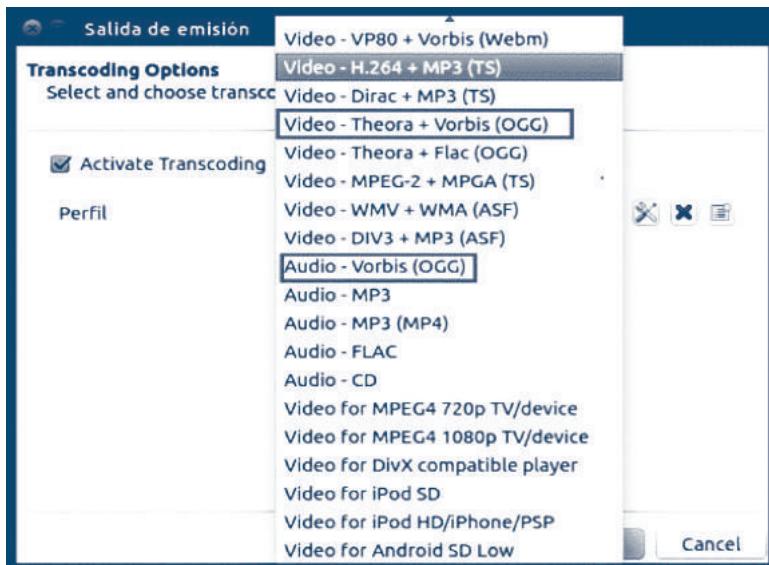


- Luego se da clic en “Siguiente”. Y se abre la pantalla de configuración para la transcodificación del contenido a emitir.

Dependiendo del material a trasmisir, se elegirá una opción diferente de la lista desplegable (véase figura 4.16) para:

- **Archivo de sólo audio:** se seleccionará la opción “Audio – Vorbis (OGG)”.
- **Archivo de video:** se seleccionará la opción “Video -Theora+Vorbis (OGG)”.

Ya que estos fueron los complementos instalados en el servidor.



*Figura 4.16 Selección de formatos de transmisión.*

Fuente: Elaborado por el grupo de investigación.

Seleccionada la opción correspondiente, se da clic en “Siguiente” y se desplegará la pantalla de configuración para las preferencias, en esta se observa la opción para habilitar la transmisión de emisiones elementales, permitiendo la transmisión de todos los componentes del archivo. También se visualiza la Cadena de salida para la emisión generada (véase figura 4.17).



Esta es la cadena de comandos que hace posible la emisión de contenido.

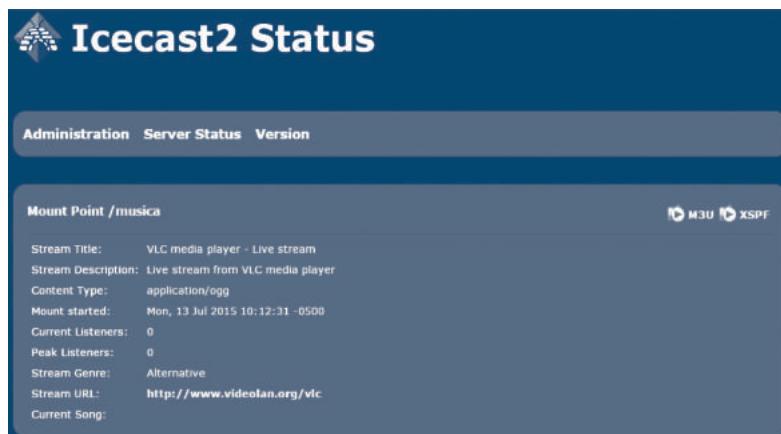


*Figura 4.17 Cadena de emisión.*

Fuente: Elaborado por el grupo de investigación.

- Se verifican las configuraciones realizadas, se hace clic en “Emitir” y el programa iniciará la emisión del contenido configurado.

Para verificarlo se puede ir a la dirección del servidor en cualquier explorador web y este mostrará la actividad del servidor (véase figura 4.18).



*Figura 4.18 Servidor emitiendo contenido.*

Fuente: Elaborado por el grupo de investigación.



#### 4.1.6 Visualización del contenido

- Usuario con equipo de mesa

El usuario o cliente que desee acceder a este servicio debe tener instalado el reproductor VLC en su equipo, sin importar el sistema operativo que tenga instalado (Mac, Windows, Linux).

Luego debe ir al sitio del servidor y descargar el archivo XSPF o el M3U, formatos que serán reproducidos por el VLC, y este recibirá todo lo que le transmita el servidor (véase figura 4.19).

The screenshot shows the 'Icecast2 Status' interface. At the top, there is a navigation bar with links for 'Administration', 'Server Status', and 'Version'. Below this, under the heading 'Mount Point /musica', there is a table with the following data:

Stream Title:	VLC media player - Live stream
Stream Description:	Live stream from VLC media player
Content Type:	application/ogg
Mount started:	Mon, 13 Jul 2015 10:12:31 -0500
Current Listeners:	0
Peak Listeners:	0
Stream Genre:	Alternative
Stream URL:	<a href="http://www.videolan.org/vlc">http://www.videolan.org/vlc</a>
Current Song:	

*Figura 4.19 Descarga vínculo contenido Streaming.*

Fuente: Elaborado por el grupo de investigación.

Después de hacer clic en el link, se iniciará la descarga del archivo con extensión .xspf o m3u, los cuales podrán ser abiertos con el programa VLC Media Player (véase figura 4.20 y figura 4.21).



*Figura 4.20 Descarga archivo xspf.*

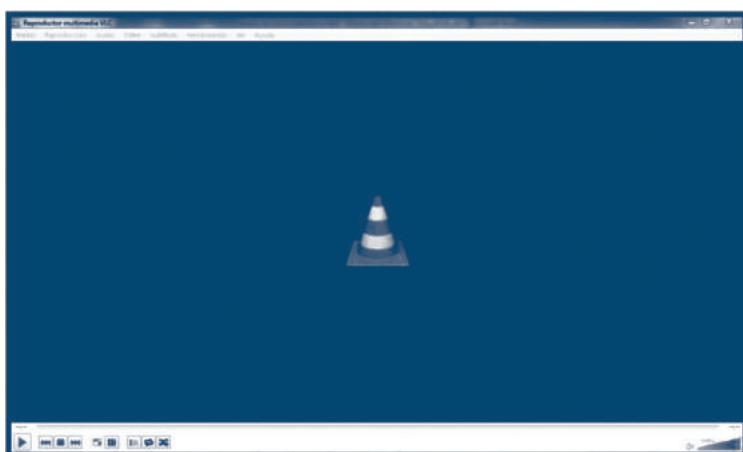
Fuente: Elaborado por el grupo de investigación.



*Figura 4.21 Archivo descargado.*

*Fuente:* Elaborado por el grupo de investigación.

Al ejecutar el archivo, este será abierto por el programa e iniciará la reproducción del contenido que este emitiendo el servidor (audio o video).



*Figura 4.22 VLC Ejecutándose.*

*Fuente:* Elaborado por el grupo de investigación.

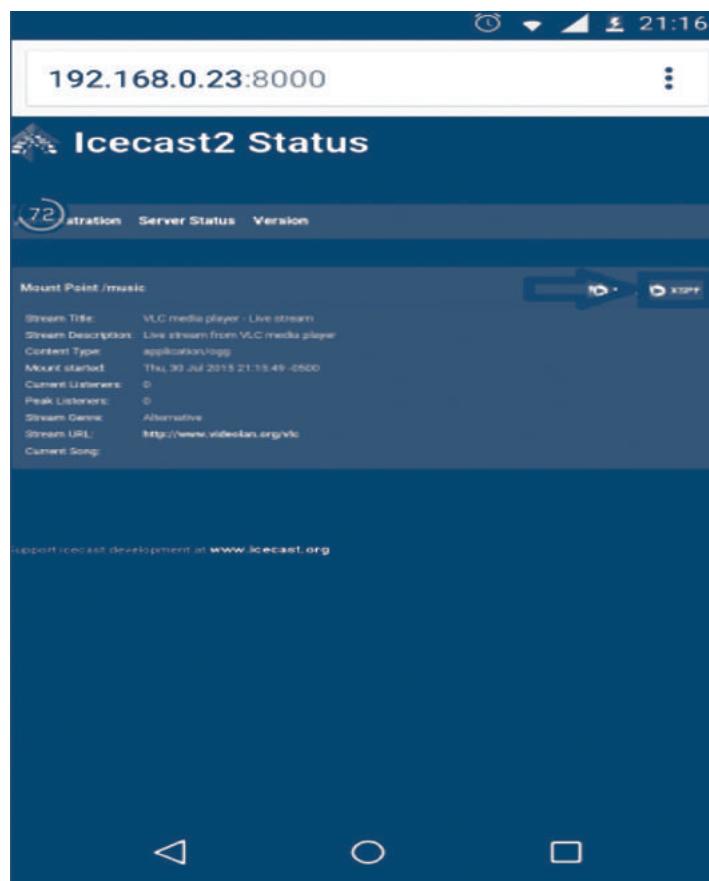
## Usuario con dispositivo móvil

El usuario debe tener instalada la aplicación VLC Media Player, que se encuentra disponible para dispositivos Android y iOS.

Luego se ingresa a la página del servidor a través de la dirección IP, por medio de algún explorador web, ya sea google Chrome, Zafari, Mozilla Firefox, etc., y en la barra de búsqueda se ingresa la dirección (véase figura 4.23). Se descarga cualquiera de los dos archivos, tal y como en el acceso por medio de un dispositivo de escritorio.



Fredys A. Simanca H., Fabián Blanco Garrido, Eduardo Triana Moyano



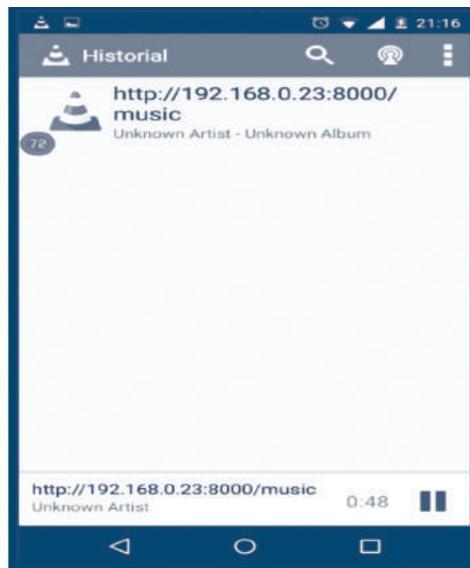
*Figura 4.23 Página en dispositivo móvil.*

*Fuente:* Elaborado por el grupo de investigación.

Después de abrir el archivo, este ejecutará la aplicación previamente instalada y reproducirá el contenido que esté enviando el servidor (audio o video) (véase figura 4.24 y figura 4.25).



Fredys A. Simanca H., Fabián Blanco Garrido, Eduardo Triana Moyano



*Figura 4.24 Reproducción de audio en dispositivo móvil.*

Fuente: Elaborado por el grupo de investigación.



*Figura 4.25 Reproducción de video en dispositivo móvil.*

Fuente: Elaborado por el grupo de investigación.



Fredys A. Simanca H., Fabián Blanco Garrido, Eduardo Triana Moyano

## • Conclusión

Las características de audio y video determinan el consumo de banda ancha requerido para el streaming de redes MESH. En el caso concreto de un video en alta definición HD, se demanda un bitrate de 1300kbps y para un audio en alta calidad se requiere de 64 kbitps, y música de alta fidelidad necesita 1.2 Mbitps.



( 5 )

## Diseño e implementación de una Red MESH como alternativa de solución para redes comunitarias o rurales

- **Introducción**

la explicación conceptual, matemática y gráfica de la instalación y configuración de un nodo MESH, específicamente en el barrio Fátima de la ciudad de Bogotá, que incluye la adecuación del router, la instalación de la antena, considerando los factores de seguridad necesarios para la protección contra agentes externos.

- **5.1 Instalación de un nodo MESH**

### 5.1.1 Planificando el enlace

Para este momento resulta obvio saber que para obtener un sistema básico de comunicación, es necesario contar con dos sujetos, un emisor y un receptor. Para el caso de una red MESH es igual, porque está compuesta por dos radios que pueden funcionar tanto como receptor y emisor, independientemente uno del otro, cada uno contando con una antena asociada. Requiere que la señal cumpla con una serie de requisitos mínimos para poder establecer una comunicación exitosa.



Para ello debe especificarse la viabilidad denominada **Presupuesto de Enlace**, este es un cálculo que determina si las señales pueden ser emitidas y recibidas por los radios en la zona que se específica.

Para determinar el Presupuesto de Enlace, es necesario determinar los siguientes factores, para esta investigación se realizará el cálculo teórico y luego de resolver las especificaciones técnicas se procederá a realizar el Presupuesto de Enlace del nodo instalado en Fátima de acuerdo a la infraestructura que lo compone.

- Potencia de Transmisión: como se mencionaba anteriormente, se calcula en milivatios o en dBm. Dependiendo del equipo, puede poseer un rango de 30 mW a 1000 mW. Normalmente la información proveída de la Potencia de Transmisión es indicada por el fabricante, en caso contrario, puede consultarse con ayuda de datos en línea.
- Ganancia de las antenas: una antena es un dispositivo estándar pasivo, esto quiere decir que la ganancia que posee es un valor constante, y que no es posible cambiar mediante alteración como overclock o técnicas similares. Independientemente de la potencia de transmisión su forma física indica su uso y ganancia, la cual puede generar para el nodo, por ello, es muy importante saber qué clase de proyecto ha de realizarse y conocer muy bien las variables implicadas para determinar qué tipo de antena es la que ofrece mejores beneficios.

En la siguiente tabla pueden encontrarse los valores regulares para las antenas más conocidas y utilizadas en los proyectos MESH.

*Tabla 5.1. Ganancia de Antenas Inalámbricas.*

Antena	dB <sub>i</sub>
Parabólica	19 – 32
Omni	5 – 17
Grillada	10 – 25
Sectorial	14 – 27
Yagi	3-20

*Fuente:* Elaborado por los autores.



Mínimo nivel de señal recibida (RSL – *Received Signal Level*): conocida como la sensibilidad del receptor, el RSL es un valor mínimo expresado en dBm negativo (-dBm, es el nivel más bajo de señal que un dispositivo inalámbrico puede recibir, dependiendo del dispositivo y sus características, generalmente el rango varía entre -75 a -95 dBm). El fabricante del dispositivo debe proveer esa información.

Pérdidas en los cables: el ambiente puede tener contaminación causante de ruido, interferencias y pérdidas de señal, entre otros fenómenos atmosféricos, además de pérdidas de energía que afectan la transmisión; parte de esa energía de la señal se pierde en cables y conectores que componen las estaciones de los nodos. Aunque es un margen de pérdida relativamente corto, con un rango de 2 a 3 dBm, en primera instancia es recomendable usar cables que sean lo más cortos posible y de la mejor calidad, al menos de tipo cat5.

Dejando a un lado estos elementos, se deben considerar fenómenos que afectan al nodo, denominados: **pérdida en espacio libre** como pueden ser la atenuación, dispersión y la contaminación ambiental que provocan distintos objetos. Además, a mayor distancia se requiere de mayores capacidades de transmisión, en parte, provocados porque a una mayor distancia la energía de la señal que se transmite se expande en función de la distancia desde el transmisor.

La pérdida en el espacio libre puede ser expresada en decibeles, utilizando 2,45 GHz como la frecuencia de la señal, la ecuación para la pérdida en el espacio libre es:

$$L_{(fs)} = 40 + 20 * \log(r)$$

Donde  $L_{(fs)}$  representa la pérdida en el espacio libre ( $fs$  = *Free Space Loss*) y ( $r$ ) es la distancia en metros entre el transmisor y el receptor. Junto a los demás fenómenos que son difíciles de plantear, ya que dependen mucho del ambiente y del diseño arquitectónico de la ciudad, pueden combinarse estos elementos: pérdida de espacio libre, atenuación, dispersión y otros, para resumir en la siguiente ecuación:

$$L (db) = 40 + 10 * n * \log (r) + L (\text{permitido})$$



Donde (n) viene a representar un exponente de variabilidad que indica el ambiente en oposición al nivel de transmisión, es decir, representa los obstáculos y contaminación que afectan de manera negativa la señal. Por ejemplo, con un nivel n = 1, considerando que es un ambiente regular con relativas temporadas de lluvia; con un n = 2, se podría añadir numerosos edificios y árboles que aumentan el nivel de atenuación en el fresnel; con un n=3 se considerarían otras antenas, aviones y demás centrales que operan a diferentes frecuencias; y con un nivel n = 4, se consideran detalles como el *smog*, la cantidad de personas que utilizan móviles, portátiles y demás elementos.

Para realizar una estimación apropiada del enlace y comprobar su viabilidad, se puede considerar solamente la pérdida en el espacio libre, sin embargo, es necesario indicar que el medio ambiente representa un factor muy importante que no debe ser ignorado para un cálculo preciso.

Deben conocerse muy bien las características en cada enlace, tanto para transmitir como recibir datos, la potencia TX debe ser sumada sólo en uno de los lados del enlace. Si se usan radios diferentes (o antenas diferentes) entonces deben aplicarse estos cálculos para el TX y para cada nodo, resumiendo:

$$\begin{aligned} & \text{TX Potencia del Radio 1} \\ & + \text{Ganancia de la Antena de Radio 1} \\ & - \text{Pérdida en los Cables de Radio 1} \\ & + \text{Ganancia de la Antena de Radio 2} \\ & - \text{Perdida en los Cables de Radio 2} \\ & \hline & = \text{Ganancia Total} \end{aligned}$$

Luego, puede obtenerse la señal así:

$$\begin{aligned} & \text{Ganancia Total} \\ & - \text{Pérdida en el trayecto} \\ & \hline & \text{Nivel de señal en un lado del enlace.} 582 \end{aligned}$$



Si el nivel de señal es mayor que el mínimo de señal recibido RSL, entonces el enlace es viable, recordando que el RSL siempre vendrá con datos negativos, así que posee un valor de señal de -40 dBm con un RSL de -58 dBm, así pues, el cálculo es exitoso, pues  $-40 > -58$ . También es importante que, si se tiene un enlace viable con un margen de diferencia entre la señal y el RSL de unos 10 o 20 dB, significará una buena calidad de transmisión, aún para entornos agresivos o con climas muy aleatorios.

Cuando se realiza un cálculo de estos, resulta sencillo aplicarlo a los demás, como se verá más adelante en un escenario simple del nodo central, con un portátil preparado para dicho escenario.

## • 5.2 Cálculo del presupuesto de enlace

Para comenzar, es muy importante saber los elementos de la Infraestructura del nodo

### Hardware

- *Board Foxconn 6627MA Series, BIOS Versión 662M02 661F1P41 050707, North Bridge: SiS 662, CPU DualCore Intel Pentium D 820, 2800 MHz (14 x 200), 2 GB de Memoria RAM DDR2-800 (400 MHz), Disco Duro 1 Tb Hitachi 5200 rpm.*
- Router inalámbrico N a 300Mbps TL-WR941ND.
- Interfaz: 4 puertos de red a 10/100 Mbps.
- 1 Puerto WAN de 10/100Mbps.
- Suministro de Energía Externa 9VDC / 0.6A.
- Estándares Inalámbricos IEEE 802.11n, IEEE 802.11g, IEEE802.11b.
- Antena: 3 antenas desmontables omnidireccionales de 3 dBi (RP-SMA)
- Dimensiones (Largo x Ancho x Alto): 7,9 x 5,5 x 1,2 pulgadas (200 x 140 x 28 mm).
- Cable UTP de 20 m cat5 gris. TÍA/EIA 5C8-B.
- Antena omnidireccional para exteriores TL-ANT2415D-2.4GHz 15dBi. Proporciona una ganancia de señal 15dBi y proporciona conector N Hembra.



- Aplicarse a las diversas condiciones meteorológicas.
- Compatible con todos los productos 802.11n/b/g (2.4 GHz).

## Software

- Sistema Operativo Debian: es un sistema cómodo para trabajar con opciones muy completas que permiten a cualquier administrador web o web master, desarrollar muchas gestiones de administración sin mayo complicación. Permite una rápida escalabilidad de servicios y aplicaciones y trae por defecto un entorno agradable y fácil de usar.
- Firmware: Openwrt, permite la creación de redes *Wireless* de despliegue rápido y sin necesidad de tener que realizar complicadas configuraciones. Openwrt permite que se extienda una red *Wireless* con la simplicidad de agregar equipos y funciona con la mínima intervención humana.
- Protección eléctrica.

Uno de los aspectos más importantes a tomar en cuenta en la preparación de un nodo MESH es la seguridad, y más precisamente, la seguridad eléctrica, ya que al tener una antena al aire libre, es necesario tomar medidas muy rigurosas y estrictas sobre este apartado para proporcionar un servicio óptimo y con un mínimo riesgo.

Dentro de las descargas eléctricas atmosféricas intervienen muchos factores, como son: el aire, las nubes y la tierra que pueden producir rayos muy peligrosos, tanto para los seres vivos como para las instalaciones.

El aire en estado seco se considera como elemento aislante, pero en la práctica se ioniza, convirtiéndose en conductor por la acción de radiaciones de material radioactivo terrestre, radiaciones de los elementos de la misma atmósfera o radiación cósmica, como es el caso del aire sobre masas terrestres marinas.

Por lo tanto, el aire tiene una conductividad que depende de la ionización, la cual es función de la cantidad de iones por  $\text{cm}^3$  ( $\text{ion}/\text{cm}^3$ ) y que varía sensiblemente entre diferentes puntos de la superficie terrestre.



Otro elemento son las nubes, estas son de diferente tipo (siendo ya por sí mismas, un obstáculo muy importante para la señal), pero las de mayor interés para el caso son las denominadas tipo cúmulos-nimbos (Cumulo-nimbus), llamadas nubes de tormenta, ya que contienen una masa de agua muy considerable.

La formación de las cargas eléctricas en el interior de estas nubes sigue un mecanismo complejo sobre el que existen varias teorías.

En general, se acepta que hay una masa de nubes con gotas, que descienden polarizadas con la carga positiva en la parte inferior, estas gotas capturan iones negativos y ceden los positivos.

Congeladas las gotas de agua, el centro se conserva líquido y los protones positivos quedan en el centro. Al partirse la gota se separan los iones positivos y los negativos, y aunque estos quedan en la parte inferior, se forman bolsas positivas en la parte baja de las nubes que generan la formación del rayo.

La tierra tiene una carga negativa y transfiere continuamente iones a la atmósfera; la transferencia depende de varios factores, tales como grado de acidez de los suelos, humedad, conductividad en las puntas, entre otros.

Los tres elementos descritos anteriormente, el aire, las nubes y la tierra constituyen el origen de la generación de las descargas atmosféricas o rayos.

Existen distintos tipos posibles de descarga: entre dos nubes, en el interior de una nube o entre una nube y la tierra.

El proceso de un rayo, para el caso nube-tierra, tiene varias fases sucesivas:

En la primera fase, se establece el llamado **leader** (Granados, 2007) en forma de dardo, donde el mecanismo inicial de encendido se establece entre una bolsa positiva y una prominencia del terreno. El dieléctrico (el aire) comienza a romperse y el leader avanza a saltos de 50 metros aproximadamente, cada uno a  $1/3$  de la velocidad de la luz. De esta forma, se va ionizando un camino irregular en diversas direcciones hasta unos 15 o 20 metros de la punta.

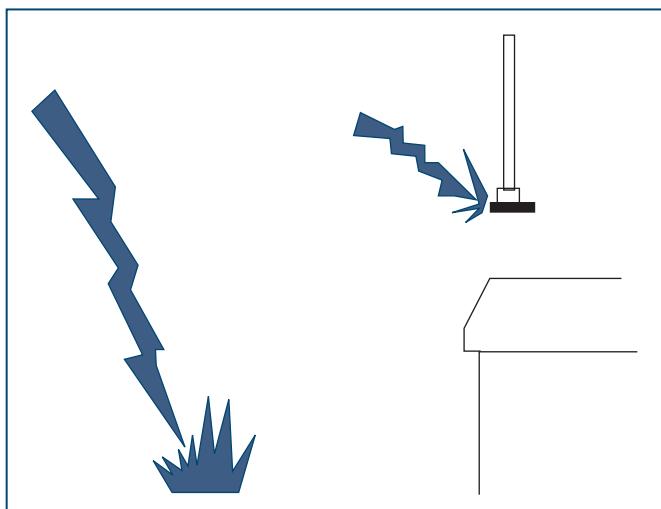


Posteriormente se dispara la corriente de retorno, mucho más brillante desde la prominencia hacia el camino ionizado y a una velocidad próxima a la de la luz. Así se efectúan repetidas descargas sucesivas.

Las tensiones que se ponen de manifiesto en las descargas atmosféricas se estiman del orden de 5 a 10 Kv por centímetro (km/cm), de modo que la descarga alcanza valores de millones de voltios.

Las intensidades son también muy elevadas y se admiten valores entre 10 y 200 millones de amperios y los tiempos del orden de 20 a 200 microsegundos; por lo tanto, se concluye que la energía de la descarga (Energía = Tensión x Corriente x Tiempo) es pequeña, pero la potencia (Potencia = Tensión x Corriente) es grande, por lo tanto, los efectos de la descarga son muy graves, si bien suceden en un tiempo extremadamente corto.

La energía del rayo se transfiere por el suelo o a través de una estructura (en este caso, el nodo), por donde ingrese, ocasionando graves riesgos a los seres vivos o a las propiedades.



*Figura 5.1 Tensión de Paso y Tensión de Contacto respectivamente.*

*Fuente:* Elaborado por el grupo de investigación.

La tensión de paso ( $V_p$ ) es la diferencia de tensión entre dos puntos de la superficie del terreno, separados por una distancia de un metro en la



dirección del gradiente de tensión máximo. Esta distancia es equivalente a un paso normal promedio.

La tensión de contacto ( $V_c$ ) se define como la tensión entre una estructura metálica puesta a tierra y un punto de la superficie del terreno a una distancia de un metro. Esta distancia horizontal es equivalente a la máxima que se pueda alcanzar al extender el brazo.

En cuanto a las medidas de prevención y control no existen medios para evitar los rayos, pero existen medidas para brindar seguridad a las personas y los equipos. Los sistemas de protección contra rayos se fundamentan en considerar la protección externa, interna y la seguridad de las personas.

El propósito de la protección externa es hacer posible la descarga y dispersión de las elevadas corrientes del rayo hacia la tierra, a través de un elemento conductor enterrado en el suelo, sin causar sobretensiones peligrosas tanto para las personas como para los equipos; se incluyen los pararrayos, los dispositivos de interceptación de rayos, las bajantes y el sistema de puesta a tierra, de acuerdo con los principios de la teoría electromagnética.

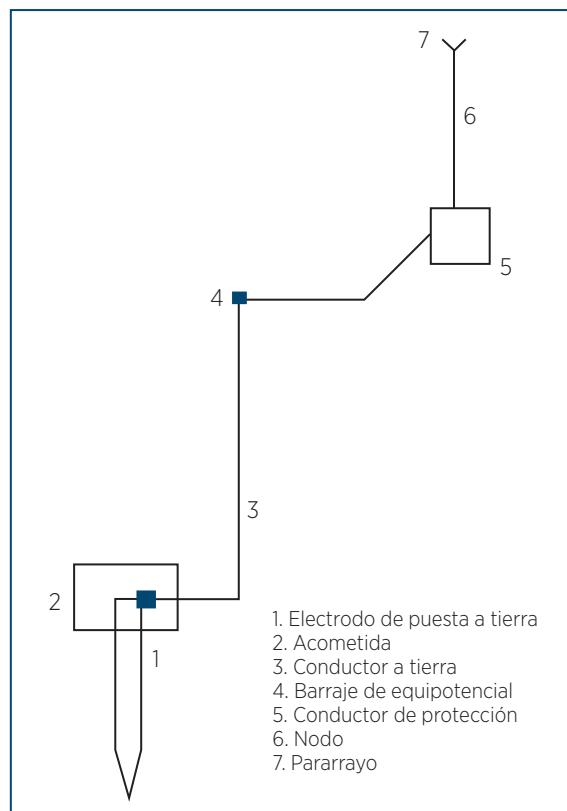
Para el nodo se ha implementado la política de seguridad por malla, incluyendo el uso de pararrayos de punta Franklin, y un sistema de puesta a tierra de alta calidad, que es una infraestructura equiparable a un entorno empresarial con elementos de gama alta.

El pararrayos es la forma más efectiva de protección contra los rayos. Fue inventado por Franklin en 1752 y consiste en una barra metálica, generalmente de hierro o cobre, que termina en punta, se sitúa en el punto más alto del edificio o estructura a proteger. Esta barra se conecta a tierra a través de un cable metálico.

Los elementos para interceptar los rayos tienen como función la protección en cercanías o directamente sobre la instalación a proteger, consisten en varillas sólidas o tubulares en forma de bayoneta, unidos mediante un anillo conductor en la cima de la estructura y conectado con las bajantes al sistema de puesta a tierra.

El sistema de puesta a tierra se obtiene mediante la unión de todos los aparatos eléctricos, estructuras metálicas, etc., a un electrodo de puesta a tierra de valor de resistencia óhmica baja. Los ductos, como el agua, gas y sistemas eléctricos, se deben conectar a un mismo potencial mediante un barraje equipotencial (BE), para así disminuir las consecuencias de un rayo.

Los conductores de puesta a tierra que unen los puntos de conexión deben ser lo más cortos y rectos posibles.



**Figura 5.2** Sistema de puesta a tierra para el nodo.

Fuente: Elaborado por el grupo de investigación.

Cuando se habla de protección interna y de seguridad, es una medida de prevención necesaria que, aunque logre canalizarse completamente por los conductores de bajantes y aterrizamientos, por efecto de la inducción o la



conducción, estas corrientes pueden ser muy peligrosas para las personas, estructuras o equipos instalados en el interior.

Se recomienda usar limitadores de sobretensión que protejan la instalación contra los daños, como UPS o SAI y usar polos a tierra para proteger los aparatos eléctricos para así, proteger a las personas de su uso y riesgo.

Además, como prevención hay que tener en cuenta las siguientes medidas en una tormenta eléctrica:

- Desconectar los equipos eléctricos o electrónicos evitando su uso.
- Buscar refugio en el interior de alguna edificación, carro y estructuras que ofrezcan seguridad contra descargas eléctricas.
- No salir al exterior, mientras haya una tormenta.
- Ubicarse en viviendas con un buen sistema de protección contra las descargas eléctricas.
- Nunca escampar en tiendas de campaña, vehículos descubiertos o no metálicos, edificaciones no protegidas.
- Alejarse de campos deportivos, piscinas, playas, lagos, líneas de transmisión, vallas metálicas, tenderos de ropa, entre otros.
- No se acueste en el suelo, mantenga los pies unidos, no escampe bajo un árbol, adopte la postura de cuclillas, no ponga las manos en el piso, colóquelas sobre las rodillas.

### 5.2.1 Presupuesto del enlace nodo Fátima

El siguiente cálculo toma un ejemplo simple de transmisión del nodo para equipo mini Lenovo, con características estándar en un equipo regular para WiFi. Independientemente del ancho de banda (2.4 o 5 GHz) los datos permanecen similares para la comunicación exitosa entre las estaciones de trabajo.

Teniendo en cuenta que las antenas 1 y 2 tienen una sensibilidad de -102 dBm y -90dBm:

Antena 1 - TL- ANT2415 TX:	30 dBm
Antena 1 - TL - ANT2415D Ganancia:	+ 15
Pérdida en los cables de Antena 1:	- 2 dBi



Antena 2 - Estándar de portátil TX:	+ 7 dBi
Pérdida en los cables de Antena 2:	0 dBi
Ganancia Total	= 50 dB

La pérdida en el trayecto de un enlace del radio de transmisión de la antena omnidireccional (100 m aproximadamente), considerando sólo la pérdida en el espacio libre.

Pérdida de transmisión:  $40 + 20 \log (100) = 80 \text{ dB}$

Restando la pérdida en el trayecto de la ganancia total:  $50 \text{ dB} - 80 \text{ dB} = -40 \text{ dB}$

El resultado es positivo para el estudio, pues es mayor que la sensibilidad del receptor del cliente (- 90 dBm), y el nivel de señal es más que suficiente para que el cliente sea capaz de oír al punto de acceso. El margen es bastante amplio ( $90 - 40 = 50 \text{ dB}$ ) por lo que la comunicación tendrá una buena estabilidad aún en malas condiciones climáticas.

A continuación, un pequeño resumen sobre el presupuesto de enlace.

*Tabla 5.2* Ganancia de la antena nodo Fátima.

Antena 1 (Nodo) (dBi)	Antena 2 (portátil) (dBi)	= Ganancia total de la antena dB
15	7	52

*Fuente:* Elaboración propia.

*Tabla 5.3.* Pérdidas de la antena nodo Fátima.

Radio 1 + Pérdida en los cables (dB)	Radio 2 + Pérdida en los cables (dB)	Pérdida en el espacio libre (dB)	= Pérdida Total
2	0	80	82

*Fuente:* Elaborado por el grupo de investigación

*Tabla 5.4* Presupuesto para el enlace de nodo – cliente.

Potencia TX de antena 1	*Ganancias de la antena	Pérdida total	= Señal	Mayor sensibilidad al cliente
30	15	80	-35	-90

*Fuente:* Elaborado por el grupo de investigación



## • 5.3 Instalación el nodo

Lo más importante para la instalación del nodo es tener los materiales necesarios, desde las herramientas más básicas, pero vitales como des-tornilladores hasta elementos de calidad como una sierra, cemento o una escalera. Es importante tener en cuenta que, dependiendo de la situación, el tipo de materiales que se trabajan pueden cambiar, dejando al usuario que decida los elementos necesarios, sin embargo, no está demás informar que, como cualquier tipo de infraestructura, debe usarse elementos que permitan la seguridad y el máximo beneficio.

Desde la simple adecuación del router, pasando por la instalación de la antena de exteriores y la preparación del sector para proteger tales elemen-tos, hasta la instalación de la puesta a tierra, requieren de un trabajo muy cuidadoso. No es la intención del proyecto de grado ejercer una obligatoria presión de indicaciones a seguir, pues dependiendo del tipo de: router, el punto de instalación, la antena, el sector, la zona de instalación y los ma-teriales con que se cuenten, ello influirá directamente en el rendimiento y la forma de instalación, por lo que las variables cambian completamente el resultado final; pero así mismo, lo importante es ofrecer una guía, y más allá del trabajo teórico, este tipo prácticas son en sí mismas, importantes para el aprendizaje de una forma práctica y personal.

### 5.3.1 Instalando la infraestructura del nodo: Router y Antena

- Materiales necesarios:
  - Destornilladores estrella y palas de diferentes tipos y tamaños.
  - Llaves inglesas y fijas de distintos tipos.
  - Alicates.
  - Cortafrios.
  - Hombresolo.
  - Agarraderas.
  - Ladrillos
  - Baldosas.
  - Extensiones.
  - Cortadoras o bisturí.

- Agua.
- Cemento y mezcla especial de materiales.
- Taladro.
- Sierra Eléctrica Black & Becker.
- Escalera.
- Carcasa de protección para router.

Preparando la zona: en este punto se instala una carcasa especial en una pequeña zona preparada para este tipo de antenas, protegiendo al router de cualquier tipo de climas y posibles amenazas que puedan afectar su funcionamiento.



*Figura 5.3* Preparando la zona para el nodo.

*Fuente:* Elaborado por el grupo de investigación.

Instalando la antena: para la antena es importante contar con unos materiales que sirvan como abrazaderas que puedan fijarse a un mástil que funcione como punto de apoyo para mantener fija la antena sin inclinarse

ni tener una inestabilidad, se necesita que la antena sea firme pues los vientos de la ciudad pueden ejercer una gran fuerza que pueda tumbar y dañar la antena.



**Figura 5.4** Preparando la zona para el router.

Fuente: Elaborado por el grupo de investigación.

Instalando el router: en esta ocasión, el espacio para el router fue preparado especialmente para que no sufriera ante la inclemencia de las tormentas del clima bogotano: lluvias, vientos, carga estática, polvo, mosquitos, entre otros factores fueron tenidos en cuenta en el momento de la instalación, por ello, se preparó una baldosa que lo soportara, aguantara y protegiera de todo este tipo de agentes dañinos para el *hardware*, ya que le pueden ocasionar serios problemas para el router.

Finalmente, se obtiene una preciosa instalación que finaliza la primera fase de infraestructura del Nodo Fátima-MESH.



*Figura 5.5 Nodo Fátima-MESH.*

*Fuente:* Elaborado por el grupo de investigación.

### 5.3.2 Instalando la infraestructura, la puesta a tierra

El proceso es simple y algo tedioso pero, muy importante, no sólo para el nodo sino para toda la propiedad en sí, ya que una puesta a tierra es algo fundamental para la protección de todos los elementos electrónicos que se usan, por lo que, más allá del presente proyecto, esta puesta a tierra fue muy importante para todos los habitantes de la propiedad.

- Materiales necesarios:
- Cable de cobre protegido.
- 2 puntas de cobre, 1 para punto a tierra en primer piso, otro como pararrayos en el nodo.
- Mástil para pararrayos de material plástico aislante.
- Abrazaderas para punta.



*Figura 5.6* Nodo Fátima-MESH protegido.

*Fuente:* Elaborado por el grupo de investigación.

## • 5.4 Configuración del nodo MESH

### 5.4.1 Características del Router TP-LINK TL-WR941ND

El router TP-LINK TL-WR941ND es sencillo. Obtenido por su eficiencia según el equilibrio precio-rendimiento; excelente para transmisión de exteriores e interiores, su estabilidad es dada por la capacidad de adaptar hasta tres antenas de capacidad variada según el tipo de conector y cableado adaptable para multipropósito. Dependiendo del modelo, se han fabricado seis modelos que utilizan un *hardware* variable, pero cuenta con una arquitectura de *hardware* similar, de acuerdo a esto, las versiones que se pueden usar en OpenWRT pueden ser diferentes según la versión del *hardware* del router. Las características del *hardware* del TL-WR941ND son:



*Tabla 5.5.* Hardware del TL-WR941ND.

Versión	CPU	Ram	Flash	Network	USB	Serial	JTag
v1	AR9132@400MHz	32MB	8MB	4x1	No.	Yes	N/A
v2	AR9132@400MHz	32MB	4MB	4x1	No.	Yes	N/A
v3	AR9132@400MHz	32MB	4MB	4x1	No.	Yes	N/A
v4	AR7240@400MHz	32MB	4MB	4x1	No.	Yes	N/A
v5.0	AR341@535MHz	32MB	4MB	4x1	No.	Yes	N/A
v5.1	AR7240@400MHz	32MB	4MB	4x1	No.	Yes	N/A
v6	AR344@560MHz	64MB	4MB	4x1	No.	Yes	N/A

Fuente: Elaborado por el grupo de investigación.

*Tabla 5.6* Versión soportada de OpenWRT para el router TL-WR941ND.

Versión Model	S/N	OpenWrt Versión Soportada	Notas específicas del Modelo
V1	•	Backfire 10.03	N/A
v2	•	Backfire 10.03	Similar a v1
v3 x	•	Backfire 10.03.1	Similar a v2
v3.8	•	Attitude Adjustment (12.09 final)	Igual que v3, pero cuenta con un chip flash diferente. Backfire puede corromperse
v4	•	Backfire 10.03	Similar a tl-wr741nd
v5.0	•	Attitude Adjustment (12.09 final)	Similar a tl-wr841nd
v5.1	•	Backfire 10.03	Similar a v4
v6	•	Trunk	Similar a tl-wdr3500

Fuente: Elaborado por el grupo de investigación.

La versión utilizada para el nodo Fátima-MESH es v3, por lo tanto, la versión seleccionada es la versión de OpenWRT Backfire 10.03.1.

#### 5.4.2 OpenWRT Backfire 10.03.1

Lanzada el 21 de diciembre de 2011, desarrollada directamente por el equipo de trabajo principal de OpenWRT, es una de las versiones más completas y con mejor soporte de paquetes externos adicionales, para el uso particular de cada instalación OpenWRT. Es una de aquellas versiones



consideradas “Old Stable” porque, si bien su ciclo ha terminado, su mantenimiento y soporte ha seguido vigente por su gran adaptabilidad a muchos dispositivos con capacidad de utilidad con OpenWRT.

Cuenta con un soporte de 486 de un máximo de 488 paquetes de adaptabilidad al sistema del Kernel principal, siendo el sistema OpenWRT el que goza de mayor aceptación y popularidad entre los desarrolladores, usuarios y fanáticos (*geeks*) de este sistema.

Se puede consultar el Anexo E para mayor información, respecto a las anotaciones técnicas del sistema Backfire 10.03.1, cuya fuente de datos es directamente la página principal de OpenWRT.

### 5.4.3 ¿Porque OpenWRT?

Por supuesto, cada sistema con el que viene cada dispositivo de red es óptimo en el correcto funcionamiento del mismo, sin embargo, con el respeto que merecen los fabricantes, al ser un *software* cerrado que no admite más elementos de los que se instalan inicialmente, sus limitaciones respecto a las necesidades de personas interesadas en explorar y conocer las capacidades de las máquinas son notables, por ello y para ello, fue desarrollado y han evolucionado este tipo de sistemas.

OpenWRT ofrece muchas ventajas para cualquier interesado:

- Linux: para cualquier conocedor, es bien sabido que los sistemas Linux ofrecen una gran ventaja de administración de redes y sistemas, por lo que su implicación directa del kernel para este tipo de dispositivos es muy beneficiosa.
- Escalabilidad y expansión: como cualquier kernel Linux, viene integrado de forma que, si se necesita algo que no viene inicialmente en el sistema, puede instalarse posteriormente, ya sea desde los repositorios ofrecidos por la comunidad OpenWRT o directamente por compilación de paquetes.
- Una comunidad inmensa: qué mejor que ante cualquier duda, recurrir a toda una gran comunidad dispuesta a escuchar y ayudar, comunidades como OpenWRT, SeguridadWireless y Bogota-MESH siempre a la orden para ayudar a cualquier interesado.



- Una gran documentación: beneficio directo de la filosofía del bazar entre comunidades, es el de obtener una documentación para que los usuarios resuelvan sus dudas y puedan implementar sus propios servicios con el uso de OpenWRT.
- Es Linux: nuevamente, lo que empieza con Linux debe terminar con Linux, principal ventaja (cualquier “linuxero” entenderá lo que quiero decir), la intención de este proyecto no es difamar a Microsoft, Apple, Cisco o cualquier comunidad que promueva sus propios sistemas, sin embargo, este tipo de iniciativas son hechas de “linuxeros” para “linuxeros”, pues la capacidad de este sistema es prácticamente inagotable.

#### 5.4.4 Instalando OpenWRT

En esta parte del capítulo se ofrecerá la mejor explicación posible, acompañada de imágenes que servirán de guía para ofrecer una mayor claridad al respecto.

- Flasheando el router

A continuación, se puede ver el entorno debían:



*Figura 5.7* Servidor Debian, escritorio Mate.

Fuente: Elaborado por el grupo de investigación.



En el archivo se encuentra la compilación necesaria de OpenWRT, para este caso será la versión Backfire como se menciona anteriormente, compatible con el chipset atheros del router tp-link; el archivo se llama “openwrt-ar71xx-tl-wr941nd-v3-squashfs-factory.bin”.

Accediendo al *firmware* original del router por medio del navegador (también es posible hacerlo desde una terminal, pero se realiza a través del *software* Opera en su versión 12.10 para Linux). Simplemente se escribe en la ruta de exploración la dirección de la puerta de enlace “192.168.1.1”, por defecto, el nombre de la cuenta y el *pass* son “admin” <http://192.168.1.1/>

Username: admin

Password: admin

Teniendo acceso como administradores para el router, este irá inmediatamente a la opción “System Tools ➔ Firmware Upgrade”, donde inmediatamente se ubicará una ventana que ofrece la posibilidad de “Actualizar” el router.

Al ubicar el archivo rápidamente con “choose/examinar”, se selecciona y se da clic en la opción “Upgrade”.

Comienza la instalación de OpenWRT en el router, es muy importante **no apagarlo mientras se realiza la instalación**, y no interrumpirlo de ninguna manera, de lo contrario, se tiene un hermoso e innovador pisapapeles para la posteridad.

Importante tener en cuenta que el tiempo de instalación puede variar, para tener seguridad del proceso, es recomendable darle un espacio de cinco minutos para la instalación completa y exitosa de OpenWRT.

Ahora, puede que sea algo confuso, pero inmediatamente después de que el router complete su actualización, desplegará una información referente a su modelo, ello quiere decir que la instalación se realizó con éxito. OpenWRT realiza eso para demostrar su compatibilidad con el hardware, desafortunadamente no ofrece un sencillo mensaje de alerta en el que demuestra una instalación exitosa, es una curiosidad, pero es la realidad de las cosas.



OpenWRT también realiza una desconexión automática del router, por lo que es recomendable desconectar el cable de red, apagar y encender la máquina luego de que la instalación se haya completado, acto seguido, debe conectarse al router.

Luego de conectar la máquina, que en este caso lo hace rápidamente con la aplicación “wicd” se procederá a ejecutar los comandos “`ifconfig`” y se comprobará que el router provee una dirección IP al servidor elegido. También es importante comprobar rápidamente que reciba y proporcione información, un sencillo “`ping`” evaluará tal situación.

Linux ofrece un completo manejo al igual que el batch de Windows, con el comando “ping -c 3 192.168.1.1” con el que se está indicando que envíe tres paquetes icmp a la dirección del router para comprobar su estado.

Luego de comprobar que todo esté en su lugar, es hora de entrar en el router: la primera vez que entre a la máquina usará sabiamente una conexión telnet, que principalmente se usa para establecer un *pass* para la cuenta root, por seguridad, es prioridad ejecutar esta tarea.

Ejecutando “telnet 192.168.1.1” entrará a la máquina por el puerto telnet (puerto23).

*Figura 5.8* Entrando a OpenWRT.

*Fuente:* Elaborado por el grupo de investigación.



## 5.4.5 Seguridad SSH en OpenWRT

Aquí se realiza el procedimiento de seguridad que obligue a OpenWRT el solicitar una contraseña de acceso, para ello se usa el comando “passwd”, luego se ingresa la contraseña que debe solicitar cada vez que se inicia sesión como usuario root en OpenWRT.

```
root@OpenWrt:/# passwd
Changing password for root
New password: Adm1nUn1m3sh
Retype password: Adm1nUn1m3sh
Password for root changed by root
```

Para este escenario, se usará la clave “Adm1nUnim3sh”, algo simple pero eficaz, con un buen nivel de seguridad

## 5.4.6 Actualizando paquetes con OPKG

Ahora bien, teniendo pleno acceso a OpenWRT, pueden establecerse un par de comandos para indicarle a la máquina el control. Para ello es importante tener al router conectado en Internet, a través de un puerto WAN; también es posible realizar el correcto mantenimiento del *firmware* por paquetes binarios *offline*, pero ello haría demasiado complejo el uso de este *howto*, por lo que el capítulo de referencia a OpenWRT se convertiría en un espacio de compilación de paquetes y se perdería tiempo explicando la consistencia de cada paquete a usar en este nodo.

OpenWRT tiene una característica especial que es muy cómoda para este caso, el gestor de paquetes “opkg” es similar al uso que tiene el que usa Debian “dpkg”, su uso y facilidad de trabajo representa una potente ventaja para trabajar el manejo de repositorios y de paquetes, pues no se diferencia en absoluto de cualquier uso de PC.

Ejecutando “opkg update” se tendrá rápidamente una actualización de paquetes desde el repositorio oficial de OpenWRT, y con “opkg list-installed” aparecerá una lista completa de todas las librerías, paquetes y binarios que actualmente conforman el sistema OpenWRT.



```
opkg update  
opkg list-installed
```

Esto es importante porque, además de comprobar el estado del *software*, particularmente se busca un conjunto de paquetes muy importantes que conforman una aplicación potente, la cual permitirá administrar OpenWRT de una manera cómoda, con muchas ventajas y que además, permite una escalabilidad que deja ampliar la propia capacidad del *firmware*. La aplicación que se busca se llama LuCI.

#### 5.4.7 LuCI: Lua + UCI (Unified Configuration Interface)

Como una introducción al tema, se proporciona una pequeña introducción sobre lo que es LuCI, traducida directamente de la página oficial (<http://luci.subsignal.org/trac>).

LuCI es una excelente interfaz web que permite a los usuarios administrar OpenWRT de una manera eficiente y cómoda. Su mantenimiento es realizado por desarrolladores voluntarios sin ningún interés lucrativo y ha estado activo como parte de las ramas estable y en desarrollo (*trunk*) de OpenWRT.

LuCI fue fundado en marzo de 2008 como “FFLuCI”, como parte de un esfuerzo en conjunto para crear una versión del firmware de Freifunk para versiones OpenWRT WhiteRussian y Kamikaze, desde entonces, se ha implementado e incluido en versiones recientes.

La razón principal del proyecto LuCI fue la ausencia de una interfaz web libre, limpia, escalable y que pudiera ser mantenida fácilmente para dispositivos embebidos. Mientras que la mayoría de interfaces web usan unos scripts que hace muy pesado su uso, LuCI usa el lenguaje de programación Lua y divide la interfaz en partes lógicas como modelos y vistas, usando librerías y plantillas que usan orientación a objetos. Ello asegura un alto desempeño con un pequeño tamaño de instalación y una excelente velocidad de rendimiento, aunque lo más importante es su mejor capacidad de mantenimiento.



LuCI es un proyecto abierto e independiente, todo el que quiera contribuir al proyecto siempre será bienvenido.

### 5.4.8 Entrando a LuCI

La entrada a la interfaz web LuCI proporcionada por OpenWRT no se diferencia mucho de una entrada a cualquier otra interfaz web, simplemente basta con ingresar por medio de un navegador a la puerta de enlace y proporcionar el root que se usa en entrada SSH en el navegador.

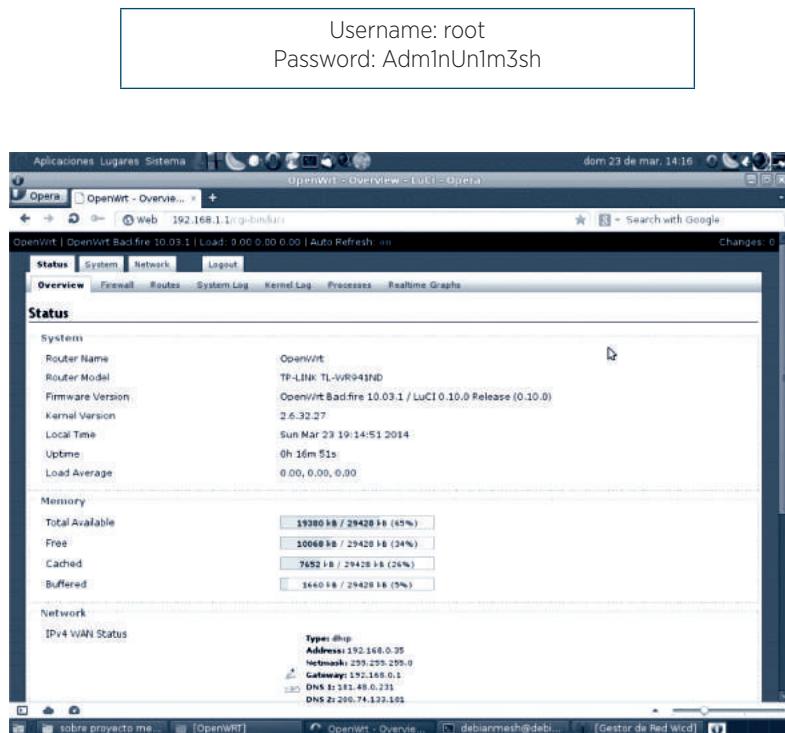


Figura 5.9 Interfaz Web OpenWRT LuCI.

Fuente: Elaborado por el grupo de investigación

Simple pero muy eficiente, como cualquier otro instrumento de exploración web, tiene sus herramientas listas para funcionar, OpenWRT (y LuCI), a diferencia de los demás *firmware*, posibilita instalar otras herramientas que permitirán sacarle el mejor provecho al nodo.



Puede comprobarse la capacidad de la máquina para instalación de paquetes, para este caso, en “System → Software” aparece un 92% de espacio para instalar aplicaciones.

#### 5.4.9 Configurando la interfaz de red inalámbrica

Por defecto, toda configuración de OpenWRT es aplicada a LuCI; una de ellas es que tenga desactivada la interfaz WiFi.

Para configurar la interfaz se puede ir a la etiqueta “Network → WiFi”, OpenWRT trae una configuración estándar con un ESSID “OpenWrt” que puede funcionar bajo las bandas b/g/n en modo máster, el cual permite el uso de un AP y/o Ad-Hoc, justo lo que necesita una red MESH. Sin embargo, es importante configurar correctamente sus parámetros para que inicie sin problemas, aunque esto no quiere decir que no pueda modificarse posteriormente, pero cada nuevo parámetro requiere que el router reinicie el servicio WiFi.

Al hacer clic en el botón “Edit” irá a las opciones que trae la configuración inalámbrica. En resumen, se establecen los siguientes parámetros:

Wireless Network: Master “OpenWrt” (radio0.network1)	
Device Configuration	
Wireless network: is disabled	<input checked="" type="checkbox"/> Enabled (hacer clic en la etiqueta)
Channel	11 (2.462 GHz)
Transmit Power	27 dBm (501 mW)
Interface Configuration	
ESSID	UniMESH
Mode	Access Point
Network	escribir “wlan” en unspecified or create

Dando clic en “Save And Apply” se tendrá una rápida configuración de la interfaz inalámbrica (WLAN) y el ESSID (UniMESH), aunque faltan algunas cosas, se puede comprobar su funcionamiento. En el ESSID se usa un protocolo de encriptamiento WPA2 para proteger la contraseña, esto es sólo a modo de prueba, ya que realmente en una red MESH no debe ir



ningún tipo de solicitud de contraseñas, sin embargo, en este caso se usará para comprobar la eficiencia de la red inalámbrica.

ESSID: UniMESH  
Clave: 20universidadlibre14

Luego de verificar todos los pasos correctamente, se implementará un espacio o zona en el cortafuego para que pueda aplicar restricciones de seguridad a la interfaz inalámbrica posteriormente.

Para ello, puede verificarse que en “Network à Interfaces” se ha creado una etiqueta “WLAN”, allí se encuentra la pestaña que se necesita para configurar el cortafuego aplicado a la interfaz, ingresando a “Network à Interfaces à WLAN à Firewall Settings e ingresando lo siguiente:

Interfaces-WLAN  
Create / Assign firewall - zone  
Unspecified -or- Create wlan

Acto seguido, hay que configurar los parámetros que usará la interfaz WiFi para proporcionar direcciones de red para equipos que se conecten a la interfaz y separar un segmento de red con su dirección y su máscara, su puerta, su amplitud o capacidad de proporcionar direcciones y demás parámetros.

Para ello, se emplea “Network à Interfaces à WLAN y se deja lo siguiente:

Interfaces – WLAN	
Common Configuration	
General Setup	
Protocol	Static
IPv4 Address	192.168.2.1
IPv4 Netmask	255.255.255.0
DHCP Server (debe habilitarse primero)	
General Setup	
Start	20
Limit	150
Lease Time	12h



Explicando rápidamente, se proporciona una dirección a la propia interfaz WLAN, que utiliza su propio servidor DHCP para entregar direcciones a quienes accedan a esa interfaz, asignando un total de 150 direcciones con un tiempo de autenticación de 12 horas, empezando por 192.168.2.20 hasta 192.168.2.170.

Volviendo a la pestaña de la interfaz Wifi, donde se añaden un par de cosas más para la interfaz WLAN, se comprueba que se han actualizado algunos datos, lo que demuestra que todo está funcionando correctamente.

Aquí están las modificaciones realizadas:

Mode:	802.11g+n
HT Mode:	20MHz
Country Code:	CO - Colombia

Se guarda la configuración (*Save and Apply*), se vuelve al menú principal “Network à WiFi”, se hace clic en “Enable” y sólo es cuestión de un par de minutos para tener una interfaz WiFi lista.

#### 5.4.10 Configurando LuCI en español

Para poner LuCI en español (este paquete no afecta a módulos extra, adicionales a LuCI) simplemente es suficiente con instalar el paquete “luci-i18n-spanish”.

```
Opkg update  
Opkg install luci-i18n-spanish
```

Puede comprobarse de inmediato que la interfaz ha sido actualizada con el paquete en español, simplemente accediendo por navegador a la puerta de enlace.

#### 5.4.11 Configurando el sistema de horario de LuCI

Lo siguiente se utiliza para estándares e indicaciones de sistema de reloj y fechas o dejar la zona horaria indicada. Sólo es cuestión de entrar a la pestaña “Sistema” y dejar la zona horaria para “América/Bogotá”.



### 5.4.12 Configurando el firewall de LuCI/OpenWRT

Para configurar correctamente un sistema de reglas de *firewall* en OpenWRT y en LuCI, se necesita habilitar los módulos correspondientes que hacen un uso adecuado de tal propiedad, para lo cual, se instalarán los siguientes paquetes:

```
iptables-mod-extra  
iptables-mod-contrack-extra  
iptables-mod-ipopt  
kmod-ipt-extra  
kmod-ipt-contrack-extra  
kmod-ipt-ipopt
```

Lo siguiente será dirigirse a “Red > Corta Fuego > Custom Rules/Reglas Personalizadas” y en el espacio correspondiente usar las reglas que se consideren apropiadas para proteger el sistema. Queda a libertad del administrador el uso de reglas personalizadas o usar las opciones que provee LuCI para establecer un control del tráfico de datos, aunque se recomienda principalmente el uso de reglas personalizadas por comando para lograr un máximo rendimiento. Puede consultar el Anexo G para consultar un script de reglas aplicadas para este apartado del firewall de OpenWRT LuCI.

### 5.4.13 Instalando el editor NANO en OpenWRT

Aunque indudablemente vi/vim es una gran herramienta para editar archivos en un kernel Linux, puede que el administrador opte por otro tipo de herramientas, como por ejemplo, nano. Esta es una útil herramienta que facilita la edición de archivos y mezcla las mejores características de vi o emacs, permitiendo un fácil uso de tales ventajas sin que ello implique una curva de aprendizaje muy alta. Fácil uso y gran rendimiento, así podría resumirse nano.

Instalar nano es muy sencillo

```
Opkg install nano
```



Rápidamente se contará con un editor de texto ligero y muy útil en nuestro OpenWRT.

#### 5.4.14 Instalando el protocolo Batman en OpenWRT

Antes de iniciar todo lo relacionado con el protocolo de conexión de una red MESH para establecer las comunicaciones inalámbricas entre nodos, hay que empezar desde lo más básico instalando el protocolo en sí mismo en el sistema OpenWRT. Para instalar Batman se debe hacer uso del siguiente comando:

```
Opkg install kmod-batman-adv
```

```
Archivo Editar Ver Buscar Terminal Ayuda
root@OpenWrt: # opkg update
Downloading http://downloads.openwrt.org/backfire/10.03.1/ar71xx/packages/Packag
es.gz.
Inflating http://downloads.openwrt.org/backfire/10.03.1/ar71xx/packages/Packages
.gz.
Updated list of available packages in /var/opkg-lists/packages.
root@OpenWrt: # opkg install kmod-batman-adv
Installing kmod-batman-adv (2.6.32.27+2011.2.0-1) to root...
Downloading http://downloads.openwrt.org/backfire/10.03.1/ar71xx/packages/kmod-b
atman-adv_2.6.32.27+2011.2.0-1_ar71xx.ipk.
Configuring kmod-batman-adv.
root@OpenWrt:~#
```

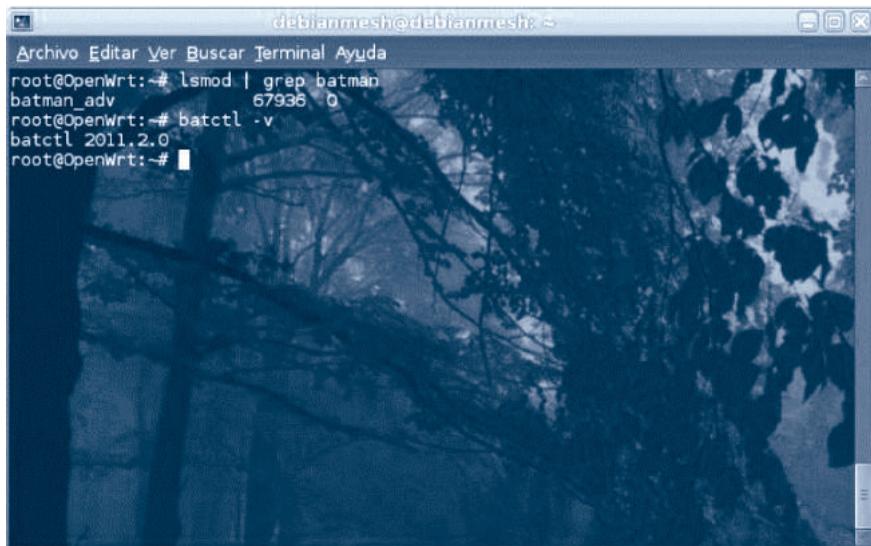
Figura 5.10 Instalando Batman-advanced en OpenWRT.

Fuente: Elaborado por el grupo de investigación.

Para comprobar que está instalado Batman en el kernel, se introduce el siguiente comando:

```
Lsmod | grep batman
```

```
Batctl -v
```



*Figura 5.11 Batman instalado en OpenWRT*

*Fuente:* Elaborado por el grupo de investigación.

#### 5.4.15 Instalando el Portal Cautivo NoDogSplash en OpenWRT

Instalar un portal cautivo es muy útil para controlar el tráfico de información y saber quiénes son los usuarios que forman parte y hacen uso de nuestra MESH. Permite administrar el nodo de una manera simple, sencilla y fácil, pero así mismo, muy eficientemente.

Introduzca en el sistema OpenWRT:

```
Opkg update  
Opkg install nodogsplash
```

Lo siguiente es activar el portal cautivo. OpenWRT deja por defecto deshabilitado el modulo, así que es necesario introducir los siguientes comandos:

```
Nodogsplash enable  
Nodogsplash start
```

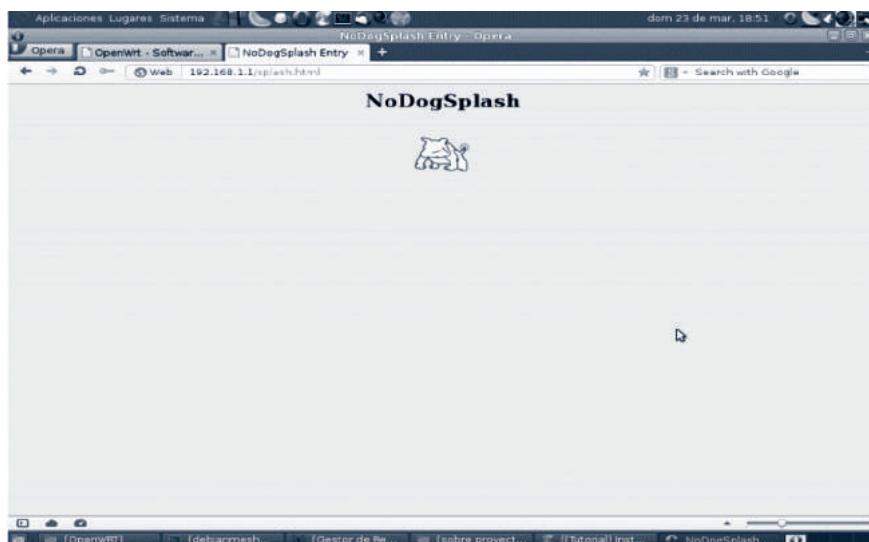


```
debianmesh@debianmesh: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@OpenWrt: # /etc/init.d/nodogsplash enable
root@OpenWrt: # /etc/init.d/nodogsplash start
Starting nodogsplash ...
Testing required modules
Testing module ipt_mac
ipt_mac is working
Testing module ipt_mark
ipt_mark is working
OK: nodogsplash started
root@OpenWrt: # Using intrapositioned negation ('--option ! this') is deprecated
in favor of extrapositioned ('! --option this').
```

**Figura 5.12** Activando el servicio del Portal Cautivo NoDogSplash.

Fuente: Elaborado por el grupo de investigación.

Puede comprobarse el portal introduciendo la siguiente dirección (la puerta de enlace puede variar):



**Figura 5.13** Portal Cautivo NoDogSplash Funcionando.

Fuente: Elaborado por el grupo de investigación.



### 5.4.16 Otros servicios para OpenWRT y LuCI

Aunque la cantidad de servicios disponibles para OpenWRT y LuCI son considerablemente variados y extensos, se ha resumido la siguiente lista que puede considerarse útil para un uso práctico del nodo:

- Estadísticas de tráfico de red en LuCI.
- Configurando QoS (*Quality of Service*) en LuCI.
- Volviendo a nuestro *firmware Original TP-LINK WR941ND*.

### • 5.5 B.A.T.M.A.N. (**Better Approach to Mobile Adhoc Networking**)

Batman es un protocolo de enrutamiento para enlaces multipunto, enlaces Ad-Hoc y redes MESH, el cual se encuentra desarrollado y soportado por la comunidad Freifunk, que fue creada para reemplazar OLSR.

En un sentido práctico, es una forma de enlazar diferentes puntos de acceso con parámetros en común en una red MESH (malla inalámbrica), ya que si se encuentran dentro de una cobertura de enlace y si tiene una línea de vista que permita la comunicación directa, pueden enlazarse automáticamente estableciendo ciertos parámetros en común. Si no es posible establecer un enlace directo, es necesario tener una conexión con la nube que permita enlazar los puntos de acceso.

Batman es un protocolo muy fácil de implementar, sólo es necesario cargar unos valores determinados, los cuales pueden ser cargados individualmente dentro de una terminal o con un *script* que incluya los valores a ser cargados dentro de los estándares de configuración que permitan utilizar el protocolo, es decir, usando archivos de configuración.

Independientemente de la forma utilizada, es necesario establecer una conexión SSH con el router, ya que fue creada de forma que sólo sean transmitidos estos valores al router o dispositivo de enrutamiento (para este escenario se habla del mismo nodo UniMESH Fatima) con encriptamiento por estándares de seguridad, pues se está hablando de un protocolo



inalámbrico, es decir que el aire al ser un medio de relativa facilidad de intrusión, necesitan de niveles avanzados de seguridad.

Ya se había explicado anteriormente como instalar Batman en el nodo Fatima, instalándolo rápidamente en el *firmware* embebido del router, OpenWRT. Lo siguiente es simplemente, entrar a una sesión con permisos de administrador (root) al dispositivo y editar los siguientes archivos.

```
/etc/config/wireless  
/etc/config/network  
/etc/config/batman-adv
```

Realmente, la única forma de comprobar en un sentido funcional el procedimiento es verificar en los nodos conectados que se tiene el SSID disponible para conectar.

Con este comando se puede comprobar que efectivamente, el SSID funciona para los nodos conectado en la red MESH UniMESH<sup>21</sup>:

```
Sudo iwlist wlan0 scan
```

## • 5.6 Webmin

Webmin es una herramienta de configuración de sistemas accesible vía web para OpenSolaris, GNU/Linux y otros sistemas Unix. Con él se pueden configurar aspectos internos de muchos sistemas operativos, como usuarios, cuotas de espacio, servicios, archivos de configuración, apagado del equipo, etcétera, así como modificar y controlar muchas aplicaciones libres, como el servidor web Apache, PHP, MySQL, DNS, Samba, DHCP, entre otros.

Webmin está escrito en Perl, versión 5, ejecutándose como su propio proceso y servidor web. Por defecto se comunica mediante TCP a través del puerto 10000, y puede ser configurado para usar SSL si OpenSSL está instalado con módulos de Perl adicionales requeridos.

<sup>21</sup> Puede consultar mayor información sobre Batman en su wiki oficial:<http://www.open-MESH.org/projects/open-MESH/wiki> <http://en.wikipedia.org/wiki/B.A.T.M.A.N>.



Está construido a partir de módulos, los cuales tienen una interfaz a los archivos de configuración y el servidor Webmin. Esto hace fácil la adición de nuevas funcionalidades sin mucho esfuerzo. Debido al diseño modular de Webmin, es posible que cualquier interesado pueda escribir extensiones para configuración de escritorio.

Webmin también permite controlar varias máquinas a través de una interfaz simple, o iniciar sesión en otros servidores webmin de la misma subred o red de área local.

Codificado por el australiano Jamie Cameron, Webmin está liberado bajo Licencia BSD. Existe también Usermin que es la versión reducida del Webmin.<sup>42</sup>

### 5.6.1 Instalando WEBMIN

```
apt-get install perl libnet-ssleay-perl openssl libauthen-pam-perl libpam-runtime  
libiopty-perl apt-show-versions python
```

También es posible realizar la instalación desde repositorios, pero es más recomendable instalar el paquete Debian y los módulos adicionales por separado.

Un ejemplo rápido de descarga y posterior instalación, como root es:

```
wget http://prdownloads.sourceforge.net/webadmin/webmin_1.680_all.deb dpkg  
-install webmin_1.680_all.deb
```

Para instalar desde repositorio es necesario editar el archivo /etc/apt/sources.list, añadiendo las siguientes líneas:

```
deb http://download.webmin.com/download/repository sarge contrib deb  
http://webmin.mirror.somersettechsolutions.co.uk/repository sarge contrib
```

Es necesario adicionar la llave GPG a los repositorios y actualizar con los siguientes comandos:



Fredys A. Simanca H., Fabián Blanco Garrido, Eduardo Triana Moyano

```
cd /root wget  
http://www.webmin.com/jcameron-key.asc  
apt-key add jcameron-key.asc
```

Para finalizar:

```
apt-get update  
apt-get install webmin
```

Con esto ya tendrá webmin instalados los comandos necesarios para iniciar, reiniciar y detener webmin:

```
/etc/webmin/start  
/etc/webmin/restart  
/etc/webmin/stop
```

Finalmente, para entrar a webmin desde cualquier navegador hay que entrar al servidor local desde el puerto 10000: <http://localhost:10000>.

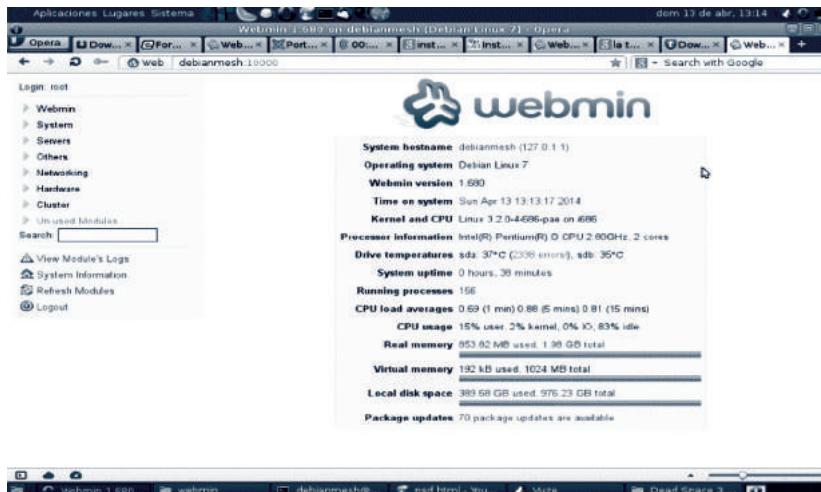


Figura 5.14 Webmin corriendo en servidor local.

Fuente: Elaborado por el grupo de investigación.



## 5.6.2 Configurando el Servidor Web Apache

En el módulo Servers > Apache WebServer, se encuentra todo lo necesario para realizar una configuración de un host virtual y poder tener un servidor web en marcha.

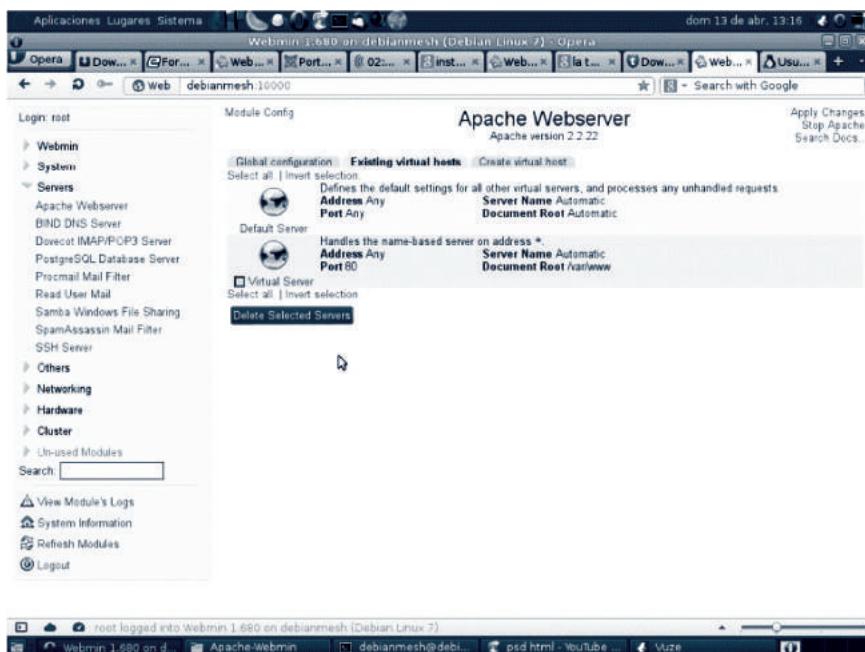


Figura 5.15 Interfaz de servidor web apache en Webmin.

Fuente: Elaborado por el grupo de investigación.

Establecer un servidor web en una carpeta determinada es bastante sencillo, solo es cuestión de establecer una ubicación con los permisos de acceso, lectura, escritura y ejecución para el administrador. Estableciendo un nombre para el servidor, se indica al servicio que concatene el nombre del dominio a una dirección web, que enlaza con el servidor virtual y que posee servidor web Apache.



The screenshot shows the Webmin control panel on a Debian Linux system. The main menu on the left includes sections for Webmin, System, Servers, Others, Networking, Hardware, Cluster, and Unmanaged Modules. The 'Servers' section is expanded, showing options like Apache Webserver, BIND DNS Server, Dovecot IMAP/POP3 Server, PostgreSQL Database Server, Pcremail Mail Filter, Read User Mail, Samba Windows File Sharing, SpamAssassin Mail Filter, and SSH Server. The Apache Webserver configuration page is displayed, with the 'Create a New Virtual Server' link being clicked. The 'Handle connections to address' section has 'Any address' selected. The 'Port' dropdown is set to 'Default' with '80' selected. The 'Document Root' field contains '/home/debianmesh/www'. The 'Server Name' field is set to 'Automatic' with 'www.uniMESH.org' entered. Under 'Add virtual server to file', 'Standard httpd.conf file' is selected. The 'Create Now' button is highlighted with a cursor.

*Figura 5.16 Creando el servidor virtual.*

Fuente: Elaborado por el grupo de investigación.

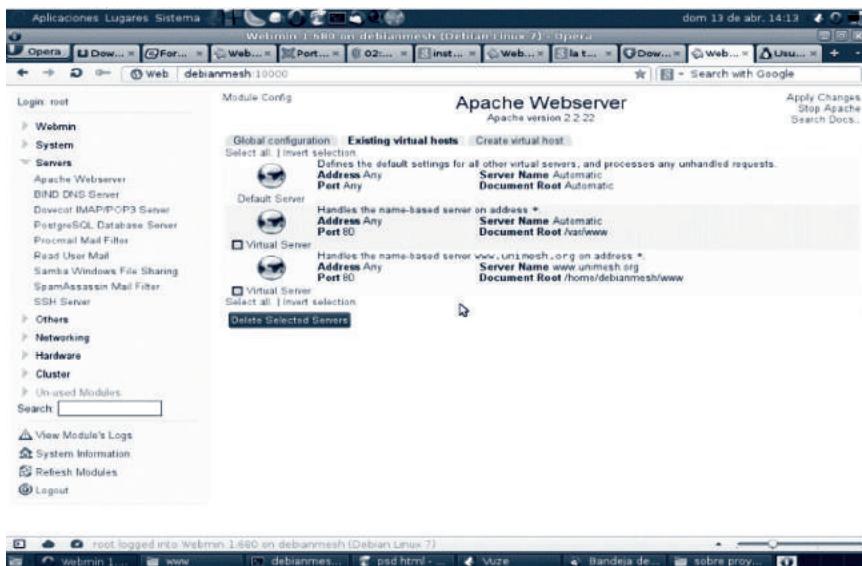
Campos requeridos:

Document Root /home/debianMESH/www (permitiendo el acceso al directorio) Server Name: www.uniMESH.org.

Se guardan todos los parámetros establecidos y en seguida se tiene a disposición un servidor virtual listo para trabajar.

## • 5.7 Contenidos de servidor web: Joomla

Respecto al servidor web, para este nodo se implementó el paquete de aplicaciones Joomla en su versión 3.2.3, el cual ha venido asentándose como uno de los mejores CMS del mercado (*Content Management System* o Sistema de Gestión de Contenidos). Es un excelente set, libre y gratuito, para implementar un servidor web funcional y contiene una gran comunidad tanto en español como en muchos otros idiomas, dispuesta a resolver dudas y problemas que se generen relacionados con Joomla.



*Figura 5.17 Servidor virtual corriendo.*

Fuente: Elaborado por el grupo de investigación.

Lo único necesario para implementar Joomla, es descargar el paquete de instalación (que viene en archivos .zip o .tar.gz o tar.bz) en una de las zonas delegadas por el servidor web (para Apache2 se trata de la carpeta /var/www/) y proporcionar los permisos apropiados (por ser una instalación local, se recomienda usar permisos tipo “chmod -R 755” que se debe aplicar tanto para carpetas como para subcarpetas, con todos los archivos que vienen en el paquete). Joomla ofrece una rápida interfaz de instalación muy fácil de implementar. Se recomienda usar mysql y phpmyadmin, para una rápida administración de la base de datos y levantar los servicios junto con el servidor web<sup>22</sup>.

Rápidamente puede comprobarse Joomla en el nodo.

<sup>22</sup> Más información en: <http://www.joomlaspanish.org/> y <http://www.joomla.org/>.



Figura 5.18 Visualización de archivos de base de datos Joomla.

Fuente: Elaborado por el grupo de investigación.

Figura 5.19 Página web creada con Joomla en el servidor web.

Fuente: Elaborado por el grupo de investigación.



## • 5.8 Estableciendo la Wikipedia en el servidor web con KIWIX

Kiwix es un lector de contenido web offline. Es un *software* especialmente creado para disponer de Wikipedia offline, sin embargo, es idóneo para cualquier contenido HTML. Kiwix es soportado por ZIM, un formato abierto de alta compresión con meta-datos adicional.

Kiwix es un software libre, lo que significa que puede ser copiado, modificado y distribuido libremente

Kiwix es muy fácil de usar. Ofrece una gama de características que hacen que el uso sea cómodo:

- Motor de búsqueda de texto completo.
- Marcadores y notas.
- Servidor HTTP.
- Exportación PDF/HTML.
- Interfaz de usuario en más de 100 idiomas.
- Fichas de navegación.
- Gestor integrado de contenido y descargas.

Kiwix es un *software* bastante pequeño y eficiente; puede ser utilizado perfectamente en ordenadores viejos o de bajos recursos. Funciona en una amplia gama de sistemas operativos, en Android y en los tres principales sistemas operativos disponibles para PC: Microsoft Windows, Apple Mac OSX y distribuciones de GNU/Linux<sup>23</sup>.

Se deben tener en cuenta los siguientes factores para implementar en el nodo UniMESH:

- El programa Kiwix.
- El archivo no-indexado de la Wikipedia con el contenido.
- Indexar el archivo correctamente, para ejecutar rápidamente los comandos de consulta.

<sup>23</sup> Más información en: [http://www.kiwix.org/wiki/Main\\_Page/es](http://www.kiwix.org/wiki/Main_Page/es)



- Compilar correctamente el programa Kiwix.
- Lanzar el servicio web de Kiwix para su uso en navegadores.
- Conectar el servicio con el portal web del nodo UniMESH.

Para resolver los siguientes parámetros es importante contar con los archivos específicos en un entorno apropiado.

Para ello, se necesitan los siguientes archivos:

- El programa Kiwix-Software Kiwix

En este caso, se necesita la versión para Linux, es muy recomendable utilizar la versión de 32 bits del software, [http://sourceforge.net/projects/kiwix/files/0.9\\_rc2/kiwix0.9-rc2-linux-i686.tar.bz2/download](http://sourceforge.net/projects/kiwix/files/0.9_rc2/kiwix0.9-rc2-linux-i686.tar.bz2/download)

- El archivo no-indexado de la Wikipedia con el contenido-Wikipedia

Es un paquete. zim que contiene todo el contenido necesario para las consultas, viene ofrecido en paquetes ligeros sin imágenes o un set muy completo con imágenes. Se actualiza anualmente y es mantenido por diferentes comunidades que ofrecen estos paquetes en más de 60 idiomas. Es recomendable utilizar el paquete con imágenes para ofrecer una mejor información de consulta.

[http://download.kiwix.org/zim/wikipedia/wikipedia\\_es\\_all\\_11\\_2013.zim](http://download.kiwix.org/zim/wikipedia/wikipedia_es_all_11_2013.zim).

### Indexar el archivo correctamente

Una vez ubicado el archivo, se crea una carpeta llamada “kiwix” por conveniencia se aconseja crearla en la ubicación “/home/—nombre de usuario—/Documentos”. Para poner un ejemplo, se creará de la siguiente forma:

```
cd /home/debianMESH/Documentos  
mkdir kiwix  
cd kiwix
```

Inmediatamente se ubican los archivos descargados en esa ubicación se debe guardar el archivo. zim de la Wikipedia en su propia carpeta (lo



que es más que recomendable para evitar confusiones), y denominarla simplemente “Wikipedia” dentro de la carpeta “kiwix”.

```
mkdir Wikipedia
```

Luego, debe extraerse el contenido del archivo de la aplicación kiwix, cualquier programa de extracción servirá, como el Engrampa para entornos Debian, el cual resultará muy útil para esta operación. Puede comprobarse la carpeta kiwix y sus archivos.

```
ls
```

Ahora, es muy importante establecer permisos para las carpetas, archivos que están dentro de la carpeta principal de kiwix.

```
cd ...  
sudo chmod -R 777 kiwix/
```

Lo siguiente es acceder a la carpeta que contiene el archivo de indexado

```
cd kiwix/bin
```

Y ejecutar el comando de indexado del archivo. zim de la siguiente manera:

```
./kiwix-index.../wikipedia/wikipedia_es_all_11_2013.zim./index/
```

Así, se ejecuta el archivo “kiwix-index” indicando dónde está el archivo indexado en la ubicación “.../Wikipedia/wikipedia\_es\_all\_11\_2013.zim” e indica que debe crear los índices en la carpeta principal y crear la carpeta que se indica “../index/”

Este comando puede durar muchas horas, entre unas 5 a 12 horas, dependiendo de la capacidad del equipo. Se debe tener bastante paciencia y no interrumpir el proceso, el mismo programa indicará cuando su finalización, además consume todos los recursos del PC, por lo que es buen momento para realizar alguna otra actividad.



- Compilar correctamente el programa Kiwix

Finalmente se ha instalado y configurado la enciclopedia Wikipedia, incluso puede ejecutarse *offline* mediante el comando Kiwix de la carpeta principal.

```
Cd /home/debianMESH/Documentos/kiwix. /  
kiwix
```

Todo esto resultará en una versión para escritorio de Kiwix y, por consiguiente, de la enciclopedia Wikipedia.

- Lanzar el servicio web de Kiwix para su uso en navegadores

Lanzar el servicio *online* es simple, pero algo complejo, pues es importante especificar correctamente los parámetros para que todo funcione correctamente.

En primer lugar, para tener el servicio web de Kiwix y la Wikipedia es importante contar con el servidor web (para el nodo UniMESH se trata de Apache), y lo segundo es tener todos los anteriores archivos de indexado en orden para facilitar la consulta.

Lo importante es estar en la carpeta de ejecutables dentro de Kiwix para ejecutar el archivo de servicio web de Kiwix.

```
cd /home/debianMESH/Documentos/kiwix/bin
```

Y ejecutar el siguiente comando:

```
./kiwix-serve /home/debianMESH/Documentos/kiwix/wikipedia/wikipedia_es_all_2013.zim  
-port=8010 -index=/home/debianMESH/Documentos/kiwix/index
```

Finalmente, se tendrá el servidor Kiwix corriendo Wikipedia en la web; para comprobarlo, abra un navegador y entre al servidor local por el puerto 8010, de la siguiente manera:

```
http://localhost:8010
```



## Conectar el servicio con el portal web del nodo UniMESH

Para enlazar la Wikipedia, simplemente se necesitará un link dentro del portal que se ha creado en Joomla, con una url hacia el link <http://localhost:8010>



Figura 5.20 Kiwix corriendo en el servidor local.

Fuente: Elaborado por el grupo de investigación.

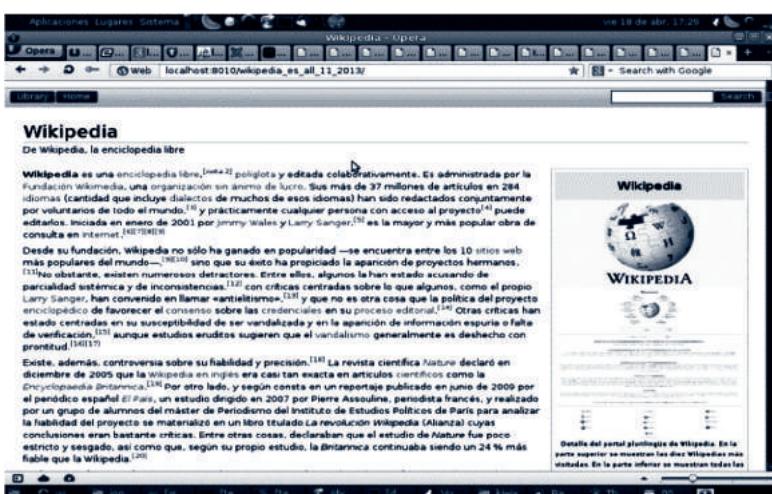


Figura 5.21 Wikipedia en servidor local UniMESH.

Fuente: Elaborado por el grupo de investigación.



Fredys A. Simanca H., Fabián Blanco Garrido, Eduardo Triana Moyano

## • Conclusión

La experiencia de diseñar e implementar una red MESH en el barrio Fátima, como proyecto visible y cuantificable es un avance importante tanto para el grupo de investigación como para la Universidad Libre. Como pioneros de una estrategia inclusiva y alcanzable para aquellos sectores de bajos recursos y difícil conectividad se logra articular la responsabilidad social al quehacer ingenieril.



## Referencias bibliográficas

- 1.bp.blogspot. (25 de mayo de 2011). *Comunicacion y Tecnología*. Recuperado de [http://1.bp.blogspot.com/\\_4ztRbe8nfk8/TN1VYM3Dkel/AAAAAAAEEQ/AN\\_QDrJful8/s640/evolucion+tec+celular.jpg](http://1.bp.blogspot.com/_4ztRbe8nfk8/TN1VYM3Dkel/AAAAAAAEEQ/AN_QDrJful8/s640/evolucion+tec+celular.jpg)
- 34t. (2016). *Aplicaciones del redes inalámbricas 802.11b en interiores*. Recuperado de <http://www.34t.com/box-docs.asp?doc=632>
- Arroyo, M. (Mayo de 2011). Un ataque a la infiltración. Recuperado de [http://hacking-etico.com/wpcontent/uploads/2012/05/diagrama\\_arp\\_dns\\_spoof.png](http://hacking-etico.com/wpcontent/uploads/2012/05/diagrama_arp_dns_spoof.png)
- Astudillo, C. y Arancibia, J. (2012). *Estudio preliminar para un sistema MESH*. Recuperado de [http://wiki.ead.pucv.cl/index.php/Red\\_MESH](http://wiki.ead.pucv.cl/index.php/Red_MESH)
- Bordando Identidad. (s.f.). *Ficha ambiental Ciudad Bolívar*. Recuperado de <http://bordando-identidad.blogspot.com/2009/03/ficha-ambiental-ciudad-bolivar.html>
- Bustamante, R. (12 de abril de 2015). *Seguridad en redes*. Universidad Autónoma del Estado de Hidalgo. Recuperado de <http://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad%20en%20redes.pdf>
- Carballar, W. (2012). *Redes Inalámbricas*. Editorial Prentice Hall.
- CCM. (Julio de 2016). *WiMAX-802.16-Interoperabilidad mundial para acceso por micro*. Recuperado de <http://es.ccm.net/contents/795-wimax-802-16-interoperabilidad-mundial-para-acceso-por-micro>
- Colmenares, J. (3 de febrero de 2008). *Estándares IEEE 802*. Recuperado de <http://estandaresieee802redes.blogspot.com.co/>
- Cristian, E. y Fetzer, C. (1998). *The Timed Asynchronous Distributed System Model*. IEEE Transactions.
- Davis, G. R. (2005). System Support For Pervasive Applications ACM Transactions. *Computer System*. Vol. 14.
- De la Rosa, J. (Agosto de 2011). *KVM Virtualizationin RHEL 6 Made Easy*.
- Edgaracredes. (Diciembre de 2013). *Mecanismos para la Seguridad*. Recuperado de <https://edgaracredes.wordpress.com/2013/02/16/mecanismo-de-seguridad-de-lainstalacion-de-una-red/>
- Eecs.yorku. (7 de enero de 2015). Recuperado de [http://www.eecs.yorku.ca/course\\_archive/2010-11/F/3213/CSE3213\\_13\\_RandomAccess\\_2\\_F2010.pdf](http://www.eecs.yorku.ca/course_archive/2010-11/F/3213/CSE3213_13_RandomAccess_2_F2010.pdf)
- Es la red. (2012). Obtenido de [http://www.eslared.org.ve/walc2012material/track4/Wireless/9\\_WLAN-Security.pdf](http://www.eslared.org.ve/walc2012material/track4/Wireless/9_WLAN-Security.pdf)
- Ese Usme. (s.f.). Obtenido de <http://www.eseusme.gov.co/phocadownload/AlasGestion/34MAPAS.pdf>



- Gen Beta. (s.f.). Obtenido de <http://www.genbeta.com/seguridad/que-es-un-certificado-ssl-y-porque-deberia-importarte>.
- Goncalves, M. (1997). *Firewalls Complete. Beta Book*. EE.UU: McGraw Hill. p. 25. En Segu-info. (7 de abril de 2015). Recuperado de [https://www.segu-info.com.ar/ataques/ataques\\_monitorizacion.htm](https://www.segu-info.com.ar/ataques/ataques_monitorizacion.htm)
- González, E. (2010). Gestor de Máquinas Virtuales. *Tesis de Maestría*.
- Guerrero, J. A. (5 de enero de 2017). *Redes inalámbricas Wireless LAN*. Recuperado de <http://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Redes%20inalambricas%20wireless%20LAN.pdf>
- Hadzilacos, V; Toueg, S. (2008). *Fault-Tolerant Broadcasts And Related Problems*. Addison Wesley.
- Holland, J. (2012). *Computer Network a Modern Approach*. Publication Press Nova University.
- Icecast. (2011). *Icecast-2.4.12*. Recuperado de <http://icecast.org/docs/icecast-2.4.0/config-file.html>
- Julian, G. (26 de marzo de 2015). *Qué es un Certificado SSL y por qué debería importarse*. Recuperado de <http://www.genbeta.com/seguridad/que-es-un-certificado-ssl-y-por-que-deberia-importarse>
- Kharagpur. (s.f.). *Nptel*. Recuperado de <http://nptel.ac.in/courses/117105076/pdf/5.4%20Lesson%202018%20.pdf>
- Kopetz, H. y Verissimo, P. (2008). *Real Time and Dependability Concepts In Distributed Systems*. Editorial Addison Wesley.
- Landero, M. (2005). *Protocolo de Ruteo Híbrido para Redes Móviles Ad Hoc*. Instituto Politécnico Nacional.
- Lehembre, G. (s.f.). *Seguridad Wi-Fi – WEP, WPA y WPA2*. Recuperado de [http://www.hsc.fr/ressources/articles/hakin9\\_wifi/hakin9\\_wifi\\_ES.pdf](http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf)
- Lerones, L. (Enero 2006). *Desarrollo de un analizador de red (Sniffer)*. En Openaccess. (7 de abril de 2015). Recuperado de <http://openaccess.uoc.edu/webapps/o2/bits-tream/10609/454/1/38443tfc.pdf>
- Meyer. B. (1999). *Object Oriented Software Construction*. Editorial Englewood Cliff Prentice Hall.
- Microsoft. (s.f.). *Microsoft TechNet*. Recuperado de <http://technet.microsoft.com/es-co/library/cc755248.aspx> consultado
- MinTic. (2010-2014). *El Plan Vive Digital*. Recuperado de <http://www.mintic.gov.co/portal/vivedigital/612/w3-propertyvalue-6106.html>
- Narasimhan, P. y Moser, I. (2004). *The Eternal System Of Distributed Systems*. Editorial Academic Publishers.
- Nazareno, G. (s.f.). *Virtualización de servidores. Conceptos básicos*. Recuperado de <http://www.gonzalonazareno.org/cloud/material/IntroVirtualizacion.pdf>
- Pérez, T. y Granados, G. (Noviembre de 2010). *Redes MESH*. Recuperado de [http://www.adminso.es/recursos/Proyectos/PFM/2010\\_11/PFM\\_MESH.pdf](http://www.adminso.es/recursos/Proyectos/PFM/2010_11/PFM_MESH.pdf)
- Prieto, G. (Noviembre, 2012). *Ataques y contramedidas en sistemas personales diapositiva 6*. Recuperado de <https://vicentesanchez90.files.wordpress.com/2012/12/ataques-y-contramedidas-ensistemas-personales.pptx>
- Schmidt, D. y Buschmann, F. (2004). *Patterns For Concurrent And Networked Systems*. Editorial John Wiley.



- Schneier, B. (s.f.). *Cryptanalysis of Microsoft's Point-to-Point TunnelingProtocol (PPTP)*. Recuperado de <https://www.schneier.com/paper-pptp.pdf>
- Simanca, F., Blanco, F., & Triana, E. (2018). *Las Redes MESH*. Bogotá: Universidad Libre.
- Stallings, W. (2008). *Sistemas Distribuidos*. Editorial Prentice Hall.
- Taiani, F. y Fabre, J. (2011). *A Multi-Level Meta-Object Protocol for Fault-Tolerance*. IEEE Computer Society Press.
- Tanembaum, A. (2008). *Computer Network*. Editorial Prentice Hall.
- Tecno Empresarial. (2009-2010). *Certificación en redes inalámbricas Redes MESH*. Recuperado de [http://tecnoeempresarial.com.mx/ri\\_certified.html](http://tecnoeempresarial.com.mx/ri_certified.html)
- Pymes y Autónomos. (s.f.). *Qué es la virtualización*. Recuperado de <http://www.tecnologiapyme.com/software/que-es-la-virtualizacion>
- Teleco. (2016). *Red inalámbrica metropolitana*. Recuperado de [http://www.teleco.com.br/imagens/tutoriais/tutorialmercwimax\\_figura4.gif](http://www.teleco.com.br/imagens/tutoriais/tutorialmercwimax_figura4.gif)
- The Office Network. (Agosto de 2014). *Red WPAN*. Recuperado de <http://www.theofficenetwork.co.uk/wp-content/uploads/2014/08/pan.jpg>
- Tomasi, W. (2003). *Sistemas de Comunicaciones*. Ed. Person.
- Toueg, H. V. (2008). *Fault-Tolerant Broadcasts And Related Problems*. Editorial Addison Wesley.
- Umar, A. (2007). *Object-Oriented Client/Server Internet Environment*. Editorial Prentice Hall.
- Universidad Tecnológica de Pereira. (2008). *El presente de las redes IP*. Recuperado de <http://repositorio.utp.edu.co/dspace/bitstream/11059/1311/1/0046T172.pdf>
- Univers-spb. (s.f.). *Distribucion de Canales Normas IEEE 802.11*. Recuperado de [http://www.univers-spb.ru/images/cisco/antennas/ccmigration\\_09186a-008008883b\\_09186a0080722f45-110.jpg](http://www.univers-spb.ru/images/cisco/antennas/ccmigration_09186a-008008883b_09186a0080722f45-110.jpg)
- Uzcátegui, L. (2012). *Seguridad en Redes Inalámbricas*. Recuperado de <http://www.eslared.org.ve/walc2012/material/track4/Wireless/9-WLAN-Security.pdf>
- Velázquez, E. (15 de enero de 2009). *¿Para qué sirven los certificados SSL?* Recuperado de <http://www.pymesautonomos.com/tecnologia/para-que-sirven-los-certificados-ssl>
- Villacañas, J. (10 abril de 2015). *Así apagaron los hackers la TV pública francesa*. En Cope (12 de abril de 2015). Recuperado de [www.cope.es/detalle/Asi-apagaron-los-hackers-la-TV-publica-francesa.html](http://www.cope.es/detalle/Asi-apagaron-los-hackers-la-TV-publica-francesa.html)
- Vitek, J. y Bryce, C. (2003). Coordinating Process with Secure Spaces. *Computer Programming Magazine Vol 46*.
- Wayne, T. (2010). *Sistemas de Comunicaciones Electrónicas*. Editorial Prentice Hall.
- Wordpress. (25 de noviembre de 2012). *Ataques y contramedidas en sistemas personales*. Recuperado de <https://vicentesanchez90.files.wordpress.com/2012/12/ataques-y-contramedidas-en-sistemas-personales.pptx>
- Xiph.org. (2014-2016). *Icecast Realease 2.4.3*. Recuperado de <http://icecast.org>
- Zona Virus. (12 de abril de 2015). *Qué es el spoofing*. Recuperado de <http://www.zonavirus.com/articulos/que-es-el-spoofing.asp>

## Las Redes MESH II

Se terminó de imprimir en septiembre de 2018.

Para su elaboración se utilizó papel bond blanco de 75 g en páginas interiores  
y papel esmaltado de 160 g para la carátula.

Las fuentes tipográficas empleadas son de la familia Gotham, en 12 puntos  
en texto corrido y 20 puntos en títulos.

La Red MESH es una red libre la cual intenta construir comunidad, buscando gente interesada en las redes y en las comunicaciones, sobre todo en las comunicaciones inalámbricas y en el desarrollo y/o uso de redes sean independiente de la infraestructura, en donde la base principal sean las redes de datos libre y comunitaria, para así dar una solución que permita aportar conectividad, contenidos, compartir recursos, entre otros usos.

Una Red Libre MESH son nodos distribuidos los cuales no son de propiedad de un particular, sino de toda una comunidad, simplemente es de todos, la cual tiene como principio ofrecer acceso libre y gratuito a las comunidades, entendiendo que cualquier persona puede tener acceso a la red en cualquier momento y puede llegar hasta cualquier parte de la red.

Con este libro sobre Redes Libre MESH se busca fomentar la instrucción técnica hacia las nuevas tecnologías mitigando las barreras existentes para el desarrollo de la sociedad de la información y creando nuevos canales de comunicación entre la comunidad y siendo una herramienta de apoyo.

*Los Autores*



**UNIVERSIDAD  
LIBRE**  
Facultad de Ingeniería

