

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS



**Aplicación de redes mesh en el área de videovigilancia y
ampliación de zonas Wi-Fi en el municipio de San José las
Flores, Chalatenango.**

PRESENTADO POR:

FERNANDO JOSÉ AGURTO ARMERO

MARIO DAVID HERNÁNDEZ RIVAS

HEBER JONATHAN LÓPEZ GUARDADO

PARA OPTAR AL TÍTULO DE:

INGENIERO DE SISTEMAS INFORMÁTICOS

CIUDAD UNIVERSITARIA, MAYO 2016

UNIVERSIDAD DE EL SALVADOR

RECTOR INTERINO :

LIC. JOSÉ LUIS ARGUETA ANTILLÓN

SECRETARIA GENERAL :

DRA. ANA LETICIA ZAVALA DE AMAYA

FACULTAD DE INGENIERÍA Y ARQUITECTURA

DECANO :

ING. FRANCISCO ANTONIO ALARCÓN SANDOVAL

SECRETARIO :

ING. JULIO ALBERTO PORTILLO

ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

DIRECTOR :

ING. JOSÉ MARÍA SÁNCHEZ CORNEJO

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS
Trabajo de Graduación previo a la opción al Grado de:
INGENIERO DE SISTEMAS INFORMÁTICOS

Título

:

**Aplicación de redes mesh en el área de videovigilancia y
ampliación de zonas Wi-Fi en el municipio de San José las
Flores, Chalatenango.**

Presentado por

:

**FERNANDO JOSÉ AGURTO ARMERO
MARIO DAVID HERNÁNDEZ RIVAS
HEBER JONATHAN LÓPEZ GUARDADO**

Trabajo de Graduación Aprobado por:

Docente Asesor

:

ING. JULIO DAMIÁN MORALES AYALA

San Salvador, Mayo 2016

Trabajo de Graduación Aprobado por:

Docente Asesor :

ING. JULIO DAMIÁN MORALES AYALA

Tabla de Contenidos

I.	Introducción	1
1	Definición del problema	3
1.1	Formulación del problema	3
1.2	Tema	3
1.3	Alcances	3
1.4	Limitantes	4
2	Antecedentes	5
2.1	Antecedentes del municipio.....	5
2.1.1	Geografía.....	5
2.1.2	Cantones y caseríos del municipio.....	6
2.1.3	Población.....	6
2.1.4	Economía	6
2.2	Tecnológicos	7
2.2.1	Videovigilancia.....	7
2.2.2	Redes Mesh.....	9
3	Marco teórico	14
3.1	Redes informáticas.....	14
3.1.1	Clasificación de las redes informáticas.....	17
3.2	Física de ondas	24
3.2.1	¿Qué es una onda?	24
3.2.2	Ondas electromagnéticas	26
3.2.3	Comportamiento de las ondas electromagnéticas	31

3.2.4	Antenas	37
3.3	Estándar IEEE 802.11 (Wi-Fi).....	41
3.3.1	802.11n.....	43
3.3.2	802.11ac	44
3.3.3	Modos <i>Wi-Fi</i>	45
3.4	Red <i>Mesh</i>	47
3.4.1	Funcionamiento.....	48
3.4.2	Protocolos de enrutamiento para redes Mesh	49
3.5	Prototipo.....	57
3.5.1	Prototipo tecnológico	58
3.5.2	Prototipo de red.....	58
3.6	Videovigilancia.....	59
3.6.1	Sistemas CCTV.....	59
3.6.2	<i>Sistemas de videovigilancia basados en IP</i>	62
3.6.3	<i>Sistemas de videovigilancia Híbridos</i>	62
3.7	Videovigilancia IP	64
3.7.1	Cámara IP.....	65
3.7.2	Medio de comunicación.....	75
3.7.3	Software de la estación de monitoreo	75
4	Objetivos.....	77
4.1	Objetivo General.....	77
4.2	Objetivos específicos	77
5	Metodología de la investigación	78

5.1	Diseño del instrumento de recolección de datos.....	78
5.1.1	Calculo del universo	79
5.1.2	Métodos cuantitativos	80
5.1.3	Métodos cualitativos	84
5.1.4	Documentos institucionales	84
5.2	Diseño del instrumento tecnológico.....	85
5.2.1	Elección de componentes.....	87
5.2.2	Diseño	92
5.2.3	Obtención de resultados	93
5.3	Factores de influencia	93
5.4	Presentación de resultados	94
6	Análisis	96
6.1	Análisis de datos	96
6.1.1	Investigación social.....	96
6.2	Decisiones sobre prototipo.....	108
6.2.1	Elección del Hardware	108
6.2.2	Elección del sistema operativo.....	126
6.2.3	Elección de protocolos	128
7	Desarrollo.....	133
7.1	Diseño del prototipo.....	133
7.1.1	Diseño del prototipo.....	133
7.1.2	Esquema del prototipo	133
7.1.3	Red <i>mesh</i> del prototipo	134

7.1.4	Red interna de la Alcaldía.....	136
7.2	Comunicación de la red Mesh.....	137
7.2.1	Nodos “B” y “C” como puente	138
7.2.2	Rutas en la red Mesh.....	139
7.3	Diseño de servicios	140
7.3.1	Diseño del servicio de expansión de zonas Wi-Fi	140
7.4	Diseño del caso de estudio.....	141
7.5	Configuraciones	143
7.5.1	Instalar sistema operativo (Raspbian Wheezy).....	143
7.5.2	Primer inicio al sistema.....	153
7.6	Desarrollo del prototipo	154
7.6.1	Configuración de IPs estáticas a la interfaz eth0	154
7.6.2	Red <i>Mesh</i> y OLSR (Interfaz Wlan0)	157
7.6.3	Acceso a internet a la red Mesh y AP	162
7.6.4	Streaming de video en la Raspberry	174
7.7	Obtención de resultados	180
7.7.1	Distancia	181
7.7.2	Interferencia en la radiofrecuencia.....	182
7.7.3	Saltos entre nodos	182
7.7.4	Número de clientes por AP	182
7.7.5	Tasa de transferencia en el Streaming de video.....	183
8	Factibilidades	184
8.1	Técnica.....	184

8.2	Económica.....	188
8.2.1	Prototipo.....	188
8.2.2	Centro de monitoreo	189
8.2.3	Alcaldía.....	190
8.2.4	Costo de oportunidad	190
8.3	Operativa.....	193
9	Conclusiones.....	195
10	Recomendaciones	196
11	Lista de referencias	198
12	Anexos	202
12.1	Anexo 1.....	202
	Instalar sistema operativo (Raspbian Wheezy).....	202
12.2	Anexo 2.....	210

Lista de tablas

Tabla 2-1 Cantones y caseríos de San José Las Flores	6
Tabla 3-1 Versiones del protocolo 802.11	42
Tabla 3-2 Tabla de resoluciones más conocidas y utilizadas	71
Tabla 5-1 Población del municipio San José Las Flores	79
Tabla 6-1 Resultados de la entrevista	107
Tabla 6-2 Comparativa entre Raspberry, Arduino y Odroid C1	110
Tabla 6-3 Características de Hardware de los dispositivos Raspberry, Arduino y Odroid	111
Tabla 6-4 Comparativa entre D-Link DIR320, Open-Mesh OM2P y Mesh Potato	115
Tabla 6-5 Características de hardware de D-Link DIR320, Open-Mesh OM2P y Mesh Potato	116
Tabla 6-6 Comparativa de memorias SD según amazon.com	124
Tabla 6-7 Listado de componentes de Hardware del nodo y su consumo eléctrico	125
Tabla 7-1 Posibles saltos de los nodos en la red Mesh	139
Tabla 7-2 Puntos de interés para el prototipo.	141
Tabla 7-3 Dirección de la red alámbrica.....	155
Tabla 7-4 Dirección Ip de la red MESH	157
Tabla 7-5 Tasa de transferencia de datos por distancia entre nodos	181
Tabla 7-6 Consumo de red acorde a la resolución de la cámara.....	183
Tabla 8-1 Tasas de transferencia utilizadas en el prototipo	186
Tabla 8-2 Costo de nodo externo	188
Tabla 8-3 Costo de nodo frontera	189
Tabla 8-4 Operadores involucrados en el sistema	193

Lista de figuras

Ilustración 3-1 Red LAN	18
Ilustración 3-2 Red WAN	19
Ilustración 3-3 Red cableada.....	21
Ilustración 3-4 Red no cableada.....	23
Ilustración 3-5 Comunicación inalámbrica.....	24
Ilustración 3-6 Longitud de onda.....	25
Ilustración 3-7 Antena dipolo	27
Ilustración 3-8 Frecuencia de ondas	28
Ilustración 3-9 Canales de la banda 2.4 GHz.....	30
Ilustración 3-10 Ejemplo de absorción	33
Ilustración 3-11 Reflexión de ondas	34
Ilustración 3-12 Difracción de ondas	35
Ilustración 3-13 Interferencia de ondas.....	36
Ilustración 3-14 Alcance de las antenas direccionales.....	38
Ilustración 3-15 Alcance de las antenas omnidireccionales	39
Ilustración 3-16 Ondas de una antena omnidireccional.....	40
Ilustración 3-17 Ubicación del protocolo Wi-Fi.....	41
Ilustración 3-18 Topología Mesh.....	48
Ilustración 3-19 Muestra de posibilidad de comunicación ampliada con OLSR.....	52
Ilustración 3-20 Estructura de un mensaje HELLO de OLSR.....	55
Ilustración 3-21 Estructura de un mensaje TC de OLSR.....	56

Ilustración 3-22 DVR Swann modelo DVR4-2600.....	61
Ilustración 3-23 Arquitectura de la videovigilancia IP	64
Ilustración 3-24 Cámara IP	65
Ilustración 3-25 Funcionamiento de una Cámara IP.....	67
Ilustración 3-26 Esquema partes externas de una Cámara IP	67
Ilustración 3-27Ejemplo de un pixel, en una imagen ampliada digitalmente.....	69
Ilustración 3-28 Comparación entre distintas resoluciones	72
Ilustración 6-1 Placa Raspberry Pi 2B	111
Ilustración 6-2 Placa Arduino UNO	112
Ilustración 6-3 Odroid C1	112
Ilustración 6-4 Router Dlink DIR 320	116
Ilustración 6-5 Dispositivo Mesh Potato.....	116
Ilustración 6-6 Dispositivo Open Mesh OM2P	117
Ilustración 7-1 Diseño del prototipo	133
Ilustración 7-2 Cámara IP del prototipo.....	135
Ilustración 7-3 Cámara IP del prototipo.....	135
Ilustración 7-4 Comunicación entre nodos de la red Mesh.....	137
Ilustración 7-5 Rutas entre los nodos del prototipo	138
Ilustración 7-6 Distribución física del prototipo.....	143
Ilustración 7-7 Interfaz de configuración de Raspberry	147
Ilustración 7-8 Confirmación de expansión de disco.....	147
Ilustración 7-9 Interfaz de cambio de contraseña	148
Ilustración 7-10 Línea de comandos, cambio de contraseña	148

Ilustración 7-11 Confirmación del cambio de contraseña	148
Ilustración 7-12 Ventana de confirmación.....	149
Ilustración 7-13 Mensaje de error	149
Ilustración 7-14 Interfaz de configuración de Raspberry	150
Ilustración 7-15 Interfaz de configuración de Raspberry	150
Ilustración 7-16 Ventana de habilitación de la cámara.....	151
Ilustración 7-17 Interfaz de configuración de Raspberry	151
Ilustración 7-18 Interfaz de configuración de Raspberry	152
Ilustración 7-19 Interfaz de habilitación	152
Ilustración 7-20 Ventana de confirmación.....	152
Ilustración 7-21 Interfaz de configuración de Raspberry	153
Ilustración 7-22 Aviso de reinicio del sistema.....	153
Ilustración 7-23 Distribución de Ips dentro de la red	155
Ilustración 7-24 Distribución de Ips dentro de la red MESH	158
Ilustración 7-25 Archivo "ifplud" de Raspbian	159
Ilustración 7-26 Archivo de configuración de OLSRD	161
Ilustración 7-27 Diseño de la red MESH.....	162
Ilustración 7-28 Archivo de configuración de OLSRD	163
Ilustración 7-29 Ejemplo de configuración de NAT desde boot	166
Ilustración 7-30 Archivo de configuración de isc-dhcp-server.....	168
Ilustración 7-31 Archivo de configuración por default de isc-dhcp-server	170
Ilustración 7-32 Configuración estática de una interfaz inalámbrica	171
Ilustración 7-33 Archivo de configuración de HOSTAPD.....	172

Ilustración 7-34 Interfaz de ZoneMinder	175
Ilustración 7-35 Ventana emergente para agregar un monitor.....	176
Ilustración 7-36 Configuración de un monitor remoto	177
Ilustración 7-37 Configuración para guardar streaming de video.	178
Ilustración 7-38 Configuración de un monitor remoto	179
Ilustración 7-39 Configuración básica de ZoneMinder	180

I. Introducción

Montar una red es un proceso tedioso y largo que muchas veces es delegado a terceros, más aún si se trata de redes de medios cableados, sin mencionar los costos que esta conlleva; La expansión de la red es otro proceso que acarrea gastos, tiempo y mano de obra. Imagine por un momento un producto que le permita realizar todas estas acciones fácilmente, que no tenga que lidiar con cables, materiales de alto costo, y que le brinde las mismas prestaciones, de lo que estaríamos hablando es de redes inalámbricas, las cuales no son nuevas, pero, tener un sistema de videovigilancia en una red inalámbrica que sea escalable en el tiempo y de bajos costos sí que lo es, por si esto fuera poco, imagine que la misma red le permite poner a disposición de la comunidad su enlace de internet, brindando un servicio gratuito a su comunidad el cual se ha vuelto casi indispensable.

A lo largo de este trabajo de graduación se realizó dicho producto, utilizando herramientas gratuitas y software libre, creando así un producto novedoso cumpliendo todo lo antes mencionado y con la posibilidad de incrementar sus prestaciones, el resultado fue totalmente satisfactorio. Queda plasmado en este documento su realización y resultados obtenidos, para que si así lo desea el lector pueda replicar o tomar como base este trabajo para implementar o mejorar este producto, que es una de la finalidades del mismo, que sirva como insumo para buscar y crear nuevas soluciones a los problemas, poniendo a disposición de todos, no importando si poseen grandes recursos económicos,

tecnologías que les permitan poseer un sistema de videovigilancia y expandir su cobertura de red Wi-Fi.

1 Definición del problema

1.1 Formulación del problema

¿Es factible la aplicación de las redes *Mesh*, como alternativa viable, en sistemas de videovigilancia y ampliación de zonas *Wi-Fi* para reducir costos, manteniendo un desempeño aceptable en cuanto a calidad de imagen y transmisión de datos?

1.2 Tema

Aplicación de redes *Mesh* en el área de videovigilancia y ampliación de zonas *Wi-Fi* en el municipio de San José las Flores, Chalatenango.

1.3 Alcances

- Diseño y desarrollo de un prototipo de red basado en la topología *Mesh*, que permita sostener un sistema de video vigilancia en tiempo real sin almacenamiento y que permita la ampliación de zonas *Wi-Fi*.
- Plan de implementación de sistema de videovigilancia y zonas *Wi-Fi* basado en topología *Mesh* para el municipio de San José las Flores.
- Factibilidad técnica, económica y operativa del uso de la topología *Mesh* como alternativa a las topologías alámbricas (fibra óptica y cobre).

1.4 Limitantes

- Adquisición de interfaces de red compatibles con el protocolo 802.11n, cuyo chipset sea compatible con los modos Ad-Hoc y Master. Estas interfaces no son adquiribles fácilmente en el mercado local.

2 Antecedentes

2.1 Antecedentes del municipio

San José las Flores, sus orígenes se remontan al año de 1785, fecha en la cual en el paraje de *Silaiquin* se fundó la aldea de San José Las Flores, en 1832 esta aldea da el primer paso y se convierte en pueblo, dicho pueblo perteneció a San Salvador hasta el año 1835 a partir de este año pasa a la jurisdicción del departamento de Cuscatlán. Finalmente, el 14 de febrero de 1855 el pueblo se convierte en municipio de Chalatenango, según la Ley de Régimen Publico el pueblo se llama oficialmente “Las Flores” y no “San José Las Flores”. **(Arnoldo, Pablo 2010)**

2.1.1 Geografía

La cabecera del municipio es el pueblo de Las Flores, situado a 425 m SNM. Entre las coordenadas geográficas centrales: 14° 02'08" LN. y los 88° 50'19" LWG **(FISDL, 2006)**. Sus poblaciones vecinas son: Nueva Trinidad, Las Vueltas, Chalatenango, San Isidro Labrador, y San Antonio La Cruz. Las fiestas patronales son del 19 al 22 de marzo en honor a San José.

2.1.2 Cantones y caseríos del municipio

Tabla 2-1 Cantones y caseríos de San José Las Flores

<i>Cantón</i>	<i>Caserío</i>
Hacienda	Los Guardados y Agua Caliente
Hacienda Vieja	Los Alas
Lagunita	Los Urbina, Palo verde y Gualpeto
Las Limas	Las Limas
Llano Verde	Tierra Colorada
Aldea Vieja	El Tamarindo y El Llano

Datos obtenidos de <http://lasflores.sumpul.com/>

2.1.3 Población

Es un municipio que cuenta con una población de 1,583 habitantes según el Censo de Población y Vivienda 2007. **(DYGESTIC, 2007)**

2.1.4 Economía

La economía del municipio radica en su mayoría en 3 rubros que son: la ganadería, la agricultura y las remesas familiares que los pobladores reciben del extranjero.

Según el almanaque “Estado del desarrollo humano en los municipios de El Salvador 2009” creado por el FISDL **(FISDL, 2009)**, el índice de desarrollo humano del

municipio es de 0.66 y el PIB per cápita es de 2,939.1 como lo constatan estos datos observamos que es un municipio que tiene población de escasos recursos.

Además, está catalogado por el gobierno de El Salvador como un municipio de pobreza extrema alta según el estudio “Mapa Nacional de Extrema Pobreza” desarrollado por el FISDL (Fondo de Inversión Social para el Desarrollo Local) en el año 2005 (FISDL, 2005). Este estudio nos da como resultado que el índice Tasa de Extrema Pobreza (Hogares) es de 41.8.

2.2 Tecnológicos

2.2.1 Videovigilancia

“La vigilancia es el arte de observar las actividades de personas o grupos desde una posición de autoridad. En ese sentido la videovigilancia es la implementación de vigilancia a partir de medios tecnológicos que permiten el monitoreo visual de zonas o elementos de interés.” (Wikipedia vigilancia, 2015)

En muchas ciudades del mundo la implementación de sistemas de videovigilancia es algo muy común desde relativamente largo tiempo. Originalmente se esperaba de la videovigilancia un efecto directo en la disminución de crímenes, pero esto se demostró que se conseguía principalmente para crímenes vandálicos, pero el efecto era bajo en crímenes violentos a pesar de que si se mostraba un efecto de disminución, como lo evidencio el estudio *Measuring the Effects of Video Surveillance on Crime* en Los Ángeles de la USC en 2008. Sin embargo, actualmente con el avance de la tecnología, se ha visto que el efecto de la videovigilancia se puede potenciar tomando un carácter

preventivo, apoyándose en nuevas funciones como reconocimiento facial de las personas y estudios de comportamiento que puedan ayudar a detectar tendencias o relaciones criminales de sujetos. Es tan importante el efecto de los sistemas de videovigilancia que es considerada una poderosa herramienta para el combate de terrorismo y criminalidad en países del primer mundo como Estados Unidos tal como plantea *Constitution Project* en **GUIDELINES FOR PUBLIC VIDEO SURVEILLANCE (2007)**.

En el ámbito nacional, la videovigilancia también se encuentra en auge, ya que es un servicio que brindan las municipalidades como una muestra de esfuerzo por preservar la seguridad de sus habitantes.

Como se puede observar en municipios del territorio nacional.

Sistema de videovigilancia La Unión, La Unión.

Sistema de videovigilancia de 4 cámaras instaladas en el casco urbano del municipio. El proyecto tuvo un costo de 40 mil dólares y fue financiado por la Agencia de Cooperación Internacional del Japón (JICA), en coordinación con la alcaldía y Policía Nacional Civil. **(El diario de Hoy, 2015)**

Sistema de videovigilancia de San Salvador, San Salvador.

El alcalde de San Salvador, Nayib Bukele, anunció durante una entrevista televisiva que el proyecto de video vigilancia de la capital costará aproximadamente entre \$30 a \$40 millones. Así mismo declaro que una de sus principales apuestas es la de reducir los índices de violencia en el capital.

“Un proyecto de seguridad debe ser rápido”, dijo el alcalde, quien además agregó que los capitalinos “pueden estar seguros que va a tener un gobierno distinto”. El edil no detalló de dónde saldrán los fondos para financiar el proyecto. De acuerdo con el alcalde, el sistema de video vigilancia capitalino contará con un software que identificará el rostro de las personas que cometan un delito. Este permitirá acceder a una base de datos donde se conocerá la identidad del mismo. También, dice que permitirá rastrear las placas de vehículos robados o que hayan sido utilizados para delinquir. **(La Prensa Gráfica, 2015)**

2.2.2 Redes Mesh

El origen de las redes Mesh hay que buscarlo en las primeras redes ad-hoc. Una red ad-hoc inalámbrica es aquella en las que no hacen falta nodos especiales que enrutan y gestionan el tráfico, sino que cada nodo tiene la capacidad de reenviar paquetes dirigidos a otros nodos de la red.

Las primeras redes inalámbricas ad-hoc fueron desarrolladas por DARPA (Agencia de Investigación de Proyectos Avanzados de Defensa, EE.UU.) en los años 70 y operaban en radiofrecuencias UHF (*packet radio networks*). Las pioneras fueron ALOHAnet y PRNET.

El uso de redes Mesh se ha centrado especialmente en prestar servicios de internet o de comunicación en áreas metropolitanas como se puede observar en los siguientes proyectos:

- Lugro-Mesh, Rosario-Argentina (sitio web: <http://www.lugro-Mesh.org.ar>)
El grupo LUGRo-Mesh pertenece al Grupo de Usuarios de Software Libre de la ciudad de Rosario (LUGRo), Argentina. *“Uno de los proyectos en curso del grupo es la creación de la red Wi-Fi Comunitaria y Libre denominada Red LUGRo-Mesh, que sirve para brindar acceso a Internet en forma gratuita a los habitantes de Rosario y alrededores. La misma es redundante y desarrollada íntegramente en Software Libre.”*
- Freifunk (<http://freifunk.net>): es una comunidad de origen alemán que tiene sus inicios desde septiembre del 2003 (**Wikipedia, Freifunk 2015**) que busca democratizar el acceso a la red haciendo que los mismos usuarios presten sus propios recursos para el beneficio de toda la comunidad, haciendo que con los recursos de todos se pueda hacer una red Mesh que beneficie a la comunidad en general con *Wi-Fi* que permita acceso a internet. En Alemania existen varias comunidades de este tipo como lo están en: Hamburg, Paderborn and Düsseldorf como principales comunidades. Además, el desarrollo del protocolo B.A.T.M.A.N. está a cargo de la comunidad Freifunk.
- Sudo *Mesh* (Oakland, California) <https://sudoroom.org/wiki/Mesh> comunidad *Mesh* de Oakland.
- RHBMesh, North Yorkshire, UK <http://rhmMesh.net>. Presta servicio de *Wi-Fi* en áreas rurales de Inglaterra con redes Mesh.

Las redes *Mesh* tienen considerablemente varios años de existir como se puede ver en los proyectos antes mencionados, a pesar de ello en El Salvador son poco conocidas y utilizadas.

La red *Mesh* utilizada en UES (Universidad de El Salvador), sede central (San Salvador, El Salvador), es un proyecto existente dentro del campus, dicha red recolecta datos de consumo eléctrico en el Campus de la universidad, proyecto desarrollado por el Ing. Carlos Eugenio Martínez Cruz en colaboración con estudiantes de Ingeniería Eléctrica, dicho proyecto utiliza una red de tipo *Mesh*. La página oficial de dicho proyecto es <http://ues.miconsumodeenergia.com> en dicha página se puede consultar el consumo de energía de los medidores de la universidad de El Salvador por períodos de tiempo.

Se ha montado una red a través de enrutadores diseñados para operar con redes *Mesh*, los cuales trabajan como nodos, dichos nodos se pueden dividir en dos: aquellos que capturan la información (y la transmiten) y los que solamente la reciben.

Los nodos que capturan la información son enrutadores que se encuentran conectados a un medidor de consumo eléctrico en cada transformador que posee el campus central, estos capturan la información a través de un medidor eléctrico que mide el consumo eléctrico en dicho transformador, posteriormente los enrutadores reenvían la información de acuerdo a la mejor ruta que determine la red.

El nodo que recibe la información se encuentra ubicado en la Escuela de Ingeniería Eléctrica, el cual está conectado directamente a una *Raspberry* que emula un servidor local, y esta trasmite los datos al equipo informático (computadora de escritorio)

que almacena la información, posteriormente es cargada a la nube y se puede observar en la aplicación que han desarrollado como equipo de trabajo. Esta red *Mesh* usa el protocolo de enrutamiento dinámico conocido como **BATMAN** (*Better Approach To Mobile Adhoc Networking*).

Este proyecto no es el único que se ha realizado en El Salvador bajo una arquitectura de red *Mesh*, a continuación, se citan los trabajos más destacados en esta rama junto a una pequeña descripción de cada uno:

- **Servicio de respuesta de voz iterativa para el Hospital Nacional Rosales**

“Servicio de respuesta de voz iterativa para el Hospital Nacional Rosales” (**Sánchez, Rony 2012**). Este proyecto realizó un prototipo de una herramienta para proporcionar comunicación sobre protocolo de internet (Voz/IP) para ser usado en el Hospital Nacional Rosales, el sistema utiliza la arquitectura de red *Mesh* para la comunicación entre dispositivos que utilizan software libre.

- **Propuesta de un sistema de comunicaciones de voz y de acceso a Internet para las escuelas del Municipio de Berlín, Usulután.**

“Diseño de una red inalámbrica Wi-Fi para los centros escolares del municipio de Berlín” (**Romero, Edmon 2010**). Consiste en un proyecto en el que se desarrolló una arquitectura de red que proporcionaba internet y telefonía a escuelas del municipio de Berlín, se trataba de una topología de red *Mesh*, el proyecto presentaba la característica de desarrollarse en una zona en la que ya se daba el servicio de internet a las escuelas, por medio de enlaces satelitales de alto costo que financiaba la unión

europea, esto permitió hacer una comparación beneficio-costos que demostró que las redes Mesh son una solución viable a problemas de comunicación actuales con un menor costo. Una de las observaciones más importantes de este proyecto fue: la pobre calidad de la telefonía obtenida.

- **Telefonía inalámbrica y red de acceso a internet para los municipios de Salcoatitán, Juayúa, Apaneca y Ataco.**

“Telefonía inalámbrica y red de acceso a Internet para los municipios de Salcoatitán, Juayúa, Apaneca y Ataco” (Colocho, Luis y Tobías, Román 2011). Similar al proyecto desarrollado en el municipio de Berlín, este proyecto detalla cómo se realizó una arquitectura de red que daba servicio de telefonía e internet a los municipios de Salcoatitán, Juayúa, Apaneca y Ataco apoyándose en una topología de red Mesh con dispositivos que utilizan software libre para la comunicación entre los nodos de la red.

Los proyectos antes citados se basan en el acceso a internet y en la comunicación de voz/IP, aunque se realizaron pruebas durante su desarrollo, dichas redes no están funcionando actualmente, fueron diseñadas o desarrolladas únicamente con fines académicos investigativos.

3 Marco teórico

3.1 Redes informáticas

A partir de la invención de dispositivos capaces de procesar gran cantidad de información, así como también almacenarla surge la necesidad de encontrar una manera de interactuar (comunicar) dos o más dispositivos los cuales pudieran estar en el mismo lugar o a una distancia considerablemente amplia, para cubrir esta necesidad aparecieron las redes informáticas.

Las redes informáticas sirven para poder intercomunicar dos o más dispositivos, estas redes tienen un alcance muy variado, desde una tan sencilla como la conexión directa a través de un cable entre dos dispositivos o una en la que se requiera la interconexión de muchos dispositivos alojados al rededor del mundo, ejemplo de esta, la más conocida comúnmente como internet.

Como ya se dijo anteriormente, para que dos usuarios puedan interactuar se necesita de una red informática y para que esta (red informática) esté funcionando se necesitan 3 componentes esenciales sin los cuales no se podría establecer una conexión. Dichos componentes los encontramos del lado físico (Hardware) como del lado lógico (Software), a partir de esta generalización los definimos en dispositivos, servicios y medios. **(Todd, 2007)**

Dispositivo: Son todos los componentes electrónicos, que tienen una relación directa, por muy mínima que sea con la red informática. Estos componentes electrónicos

se pueden clasificar en dos grandes grupos, dispositivos finales y dispositivos intermedios.

Las computadoras, dispositivos móviles, impresoras, teléfonos IP y cámaras se encuentran en el grupo de dispositivos finales, su nombre se debe a que son los dispositivos con los cuales interactúa el usuario final.

Los *routers*, *hubs*, *switches*, cableado, entre otros, forman el grupo de dispositivos intermedios los cuales se encargan de transmitir y enrutar la información que se envía entre los dispositivos finales. (Todd, 2007)

Servicios: Son los programas que los dispositivos finales ejecutan para el envío de información, en la actualidad se tiene una gran variedad de los mismos, en gran medida se ha tomado mayor importancia a la comunicación a través de internet. En la amplia gama de programas se encuentran los correos electrónicos cuya función es indispensable actualmente en el ámbito empresarial, así como también en el uso personal para el envío y recepción de documentos, además en el mercado se presentan las redes sociales las cuales tienen una aceptación muy elevada por parte de la población mundial, por último, con la aparición de la Web 2.0 tienen mayor relevancia los blogs, wikis, foros, entre otros.

Pero este tipo de programas no son los únicos que se ejecutan en los dispositivos que conforman la red de comunicación, en una red de comunicación se necesitan procesos y operaciones automatizadas. Dichos procesos y operaciones son los encargados de transmitir la información de forma segura y confiable. Estos procesos por lo general se

encuentran alojados en los dispositivos intermedios, cuya función es enrutar y retransmitir la información. (Todd, 2007)

Medio: Para que un mensaje pueda ser llevado de un punto a otro, este debe de ser transportado a través de un medio de desplazamiento cuya función principal es interconectar todos los dispositivos tanto intermediarios como finales. En la actualidad en las redes informáticas encontramos tres tipos de medios: hilos metálicos dentro de cables, fibra óptica y por último tenemos al medio inalámbrico. Cada uno de estos medios tiene sus propias peculiaridades para la transmisión de datos entre dos estaciones, cuando la información es transportada por **hilos metálicos** los dispositivos transforman los bits en pulsos eléctricos, estos pulsos eléctricos son enviados por los cables hasta llegar al receptor el cual deberá convertirlos nuevamente en bits. En cuanto a la **fibra óptica difieren** en el proceso de transformación de los bits, ya que estos dispositivos no los convierten en pulsos eléctricos sino más bien en pulsos de luz o infrarrojos, los cuales llegados a su destino deberán ser reconvertidos a bits. Por último, se deja al **medio inalámbrico**, al contrario que los dos medios anteriores en este medio los bits son convertidos en ondas electromagnéticas las cuales se envían por el aire y deben ser captadas por el dispositivo receptor y como en los demás medios estas llegadas a su destino son reconvertidos a bits para que los programas puedan interpretar el mensaje enviado. (Todd, 2007)

3.1.1 Clasificación de las redes informáticas

Las redes informáticas tienen un impacto muy amplio es por esta razón que tienen usos muy variados, por su diversificación se llegó a crear ciertas categorías las cuales el autor Todd, Lammle las dividió en los siguientes grupos: por el alcance, por su medio y por la ubicación de las redes informáticas. **(Todd, 2007)**

3.1.1.1 Por su alcance

El alcance de una red informática es la extensión del área de cobertura de dicha red, la cual puede involucrar uno o todos los medios de conexión y así tener un mayor alcance. A partir de esto se tienen las siguientes redes:

PAN (*Personal Area Network*): como su nombre lo indica es una red de área local, la cual permite que el usuario pueda comunicar su computadora con otras tecnologías que estén cerca del usuario. Esta red se centra en la persona (usuario) y le permite comunicarse con sus dispositivos personales tales como *Smartphones*, PDAs, tableros digitales, impresoras, fax, escáneres y consolas de videojuegos. Estas redes pueden alámbricas como inalámbricas y tienen un alcance de hasta 10 metros de radio, tomando como origen el punto de conexión a internet. **(Todd, 2007)**

LAN (*Local Area Network*): es una red de área local, su principal característica es que únicamente se puede administrar por los usuarios encargados por organización a la que pertenece, dicha red cubre una única área geográfica en la que proporciona servicios y aplicaciones a los usuarios de la red en una estructura de red común.

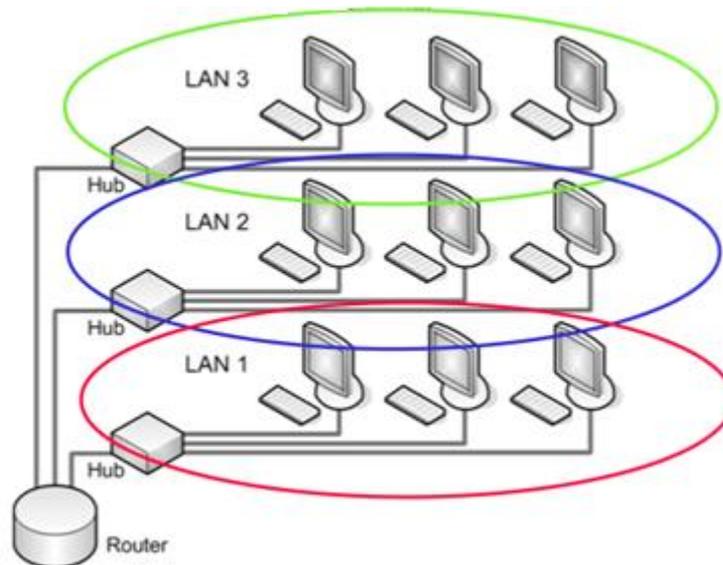


Ilustración 3-1 Red LAN: En la ilustración se observan 3 redes de tipo LAN, las cuales constituyen una sola red WAN.

Esta red es la más fácil de identificar ya que está delimitada geográficamente en una localidad determinada, además que es la que poseen todos los hogares que tienen contratado un servicio de internet. En esta clasificación encontramos edificios, hogares, campus universitarios, la red de una empresa e incluso la red de una región. **(Todd, 2007)**

WAN (Wide Area Network): las redes de área amplia mejor conocidas como WAN, son redes que interconectan redes LAN en áreas geográficas ubicadas en distintas localidades. Las empresas son las que necesitan de este servicio, para interconectar las distintas sucursales que tienen distribuidas a lo largo de una región, país, continente o todo el mundo.

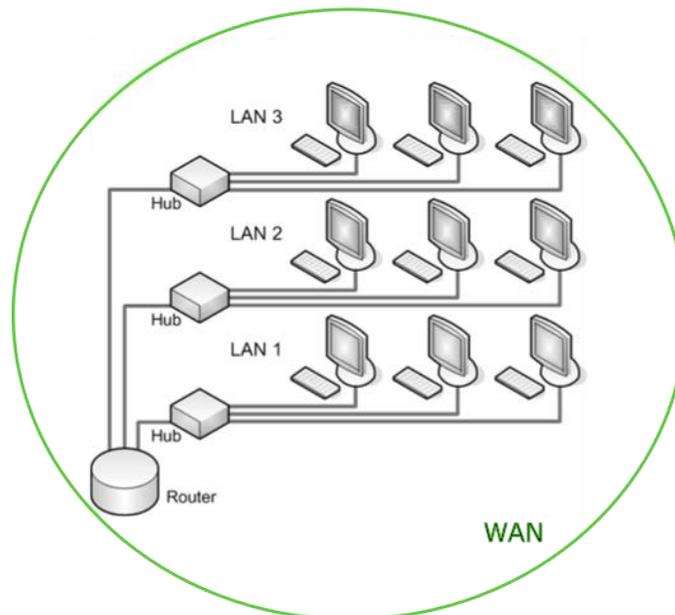


Ilustración 3-2 Red WAN

Las empresas alquilan este servicio a un proveedor de servicio de telecomunicaciones, por consiguiente ellos no pueden administrar la WAN solo tienen la autoridad de administrar cada una de las LAN que interconecta la WAN. (Todd, 2007)

Intranet

A parte de las clasificaciones antes descritas se tiene dos tipos de redes muy usadas *internetwork* e *intranet*, redes de gran alcance, pero cuya diferencia son las personas que tienen acceso a una u otra red.

El concepto de **intranet** es usado para referirse a la conexión privada que uno o más usuarios de una empresa poseen a algunas LAN y WAN que esta empresa posea. Su razón de ser es permitir conexiones de red a los miembros y empleados que posean las

credenciales de seguridad necesarios para acceder a la información que su cargo requiera.

(Todd, 2007)

Internet

En contraparte la **internetwork** es una malla de redes interconectadas globalmente, la cual permite la comunicación entre personas que están en puntos opuestos del globo terráqueo. Algunas de las redes que componen internetwork pertenecen a grandes organizaciones o gobiernos, así como también a los proveedores de servicios de internet.

La internetwork más usada y conocida es el **internet**, es a la que accede el público en general para comunicarse y acceder a información necesaria. Aunque en la actualidad con el avance de la tecnología se ha convertido en una de las actividades de ocio preferidas por sus usuarios, debido a la aparición de las redes sociales y los *Smartphones* con conexiones de buena calidad esta actividad ha tenido una gran evolución. Además, la amplia variedad de videojuegos para estos dispositivos, como para consolas que permiten conexión a internet se convierten en una gran alternativa de diversión para todas las edades. **(Todd, 2007)**

3.1.1.2 Por su medio

Esta categoría se subdivide en dos grandes grupos de acuerdo al canal de comunicación que las redes informáticas ocupan, los cuales son:

Redes cableadas

Red más utilizada desde la aparición de las redes informáticas y aun en la actualidad, son redes cuyos enlaces entre dispositivos de comunicación son cables de red, ya sean hilos metálicos o fibra óptica. Su gran virtud son las altas velocidades de transferencia que se alcanzan con este medio, sus mayores defectos son los costos de mantenimiento de esta red y su poca escalabilidad. (Todd, 2007)

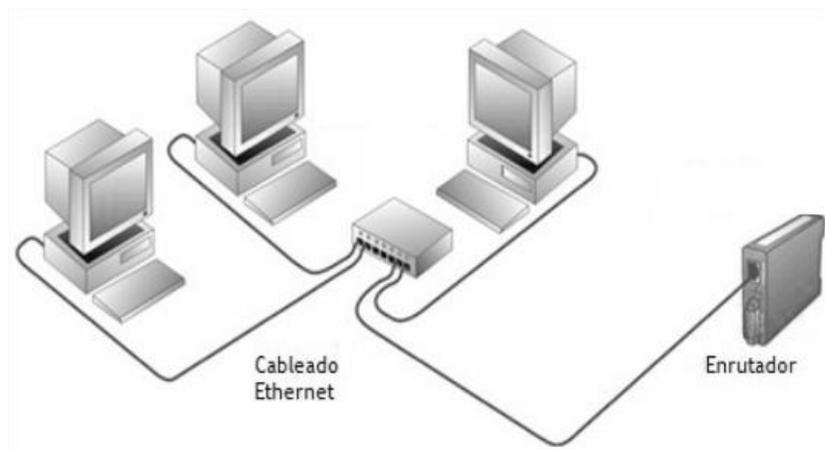


Ilustración 3-3 Red cableada. La imagen muestra una topología básica.

Redes inalámbricas

Este trabajo se enmarca dentro la utilización de este tipo de redes, aprovechando sus cualidades, como lo es su alta escalabilidad con costos bajos de mantenimiento.

Estas están teniendo gran repercusión con la aparición de dispositivos que permiten conexiones inalámbricas, en esta red la información es enviada a través del aire. En cuanto a las virtudes y defectos de esta red son la contraparte de la red cableada,

tienen una gran escalabilidad y bajo costo, en consecuencia, tienen menores tasas de transferencia y más probabilidades de fallos. (Todd, 2007)

Dentro de las redes inalámbricas se tienen redes PAN, LAN y WAN las cuales ya se describieron en la sección anterior, pero cabe resaltar, que utilizando exclusivamente este medio se pueden crear estos tipos de redes informáticas.

Ya se describió el medio por el cual viaja la información de las redes inalámbricas, pero para que esto pueda ocurrir se necesita que el dispositivo que esté usando una red inalámbrica posea una tarjeta de red inalámbrica, esta puede ser una tarjeta de red *Wi-Fi* o una tarjeta de red *bluetooth*, dichas tarjetas permitirán que el dispositivo pueda comunicarse con otros dispositivos que posean este tipo de tarjetas de red.

En el caso de las tarjetas de red Wi-Fi estas están regidas por el estándar 802.11 de la IEEE (el cual se detallará más a profundidad en la sección 3.3 Wi-Fi) y para las tarjetas de red *bluetooth* estas están regidas por el estándar 802.16 de la IEEE.

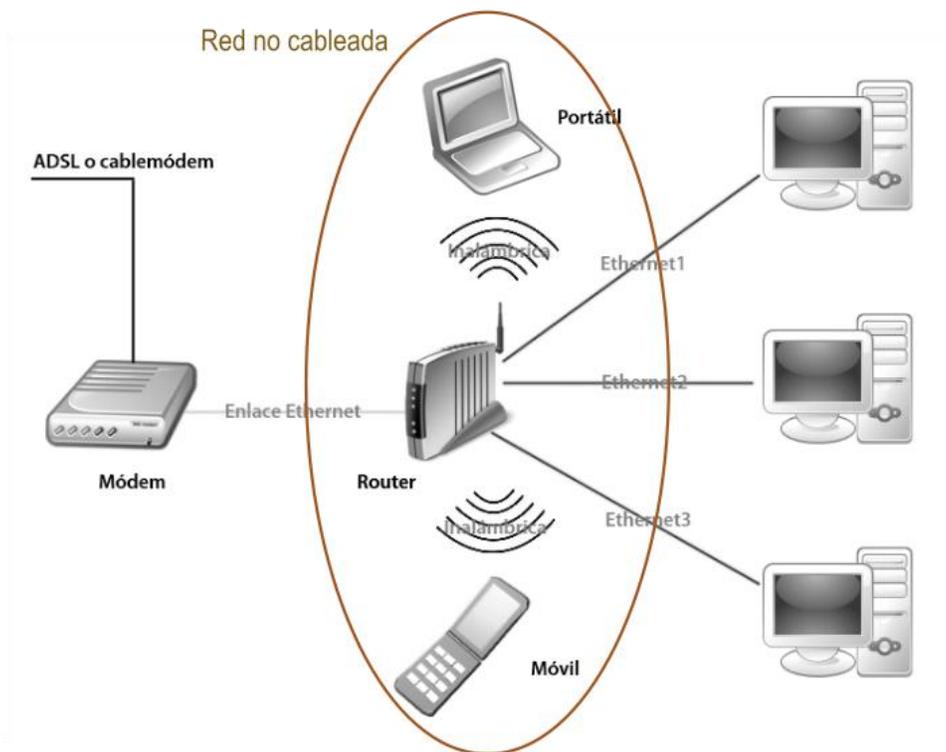


Ilustración 3-4 Red no cableada. Esta imagen muestra un ejemplo de topología de red inalámbrica.

Este tipo de redes presenta una gran oportunidad de disminuir costos con respecto a las otras redes informáticas que utilizan hilos metálicos o fibra óptica, esto la convierte en la opción viable para la investigación que se desarrolla en el presente documento. Esto la convierte en la primera opción para realizar proyectos que requieran gran escalabilidad además de presupuestos muy cortos.

Para comprender de mejor manera el funcionamiento de las redes inalámbricas en la siguiente sección se abordará el comportamiento físico de las ondas.

3.2 Física de ondas

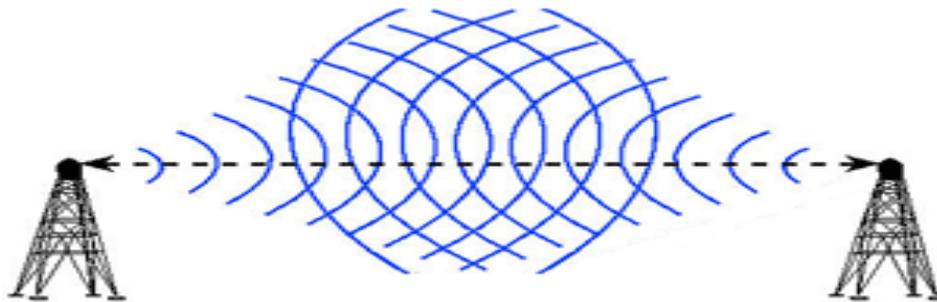


Ilustración 3-5 Comunicación inalámbrica. La ilustración ejemplifica el uso de ondas en las telecomunicaciones.

Para que las conexiones inalámbricas funcionen se necesita que la información que se transmite de una estación a otra, pueda ser enviada por el aire. Esto se logra si la información o mensaje involucrado, se transforma en ondas electromagnéticas que serán enviadas por el aire. Para comprender este proceso se necesita conocer un conjunto de definiciones e interpretaciones sobre que son y cómo funcionan las ondas electromagnéticas.

3.2.1 ¿Qué es una onda?

Todos o casi todos los humanos hemos percibido consciente o inconscientemente las vibraciones u oscilaciones, que se emiten en el día a día de las personas. Dichas oscilaciones pueden ser ocasionadas por vientos u otro tipo de fuerzas, como por ejemplo cuando el viento ejerce una fuerza sobre un árbol, este comienza a mecerse y se mantiene oscilando periódicamente a través del tiempo.

Además del ejemplo antes descrito, este fenómeno se puede observar en péndulos, las cuerdas de guitarra o cuando arrojamamos una piedra sobre el agua observamos como el impacto de la piedra hace que el agua se desplace a través de ondas.

Con los ejemplos antes expuestos podemos definir a una onda como: “es la alteración de un medio (agua, aire, un trozo de metal o incluso el vacío) que se manifiesta como una perturbación (vibración) a través del tiempo”. **(Flikenger, 2008)**

Todas las ondas tienen características muy esenciales que la distinguen, como la velocidad, la frecuencia y la longitud de onda. Matemáticamente estas características están relacionadas por la siguiente formula:

$$\text{Velocidad} = \text{Frecuencia} * \text{Longitud de Onda}$$

La longitud de onda (λ) es: “*la distancia medida desde un punto en una onda hasta la parte equivalente de la siguiente, por ejemplo, desde la cima de un pico hasta el siguiente*” **(Flikenger, 2008)**

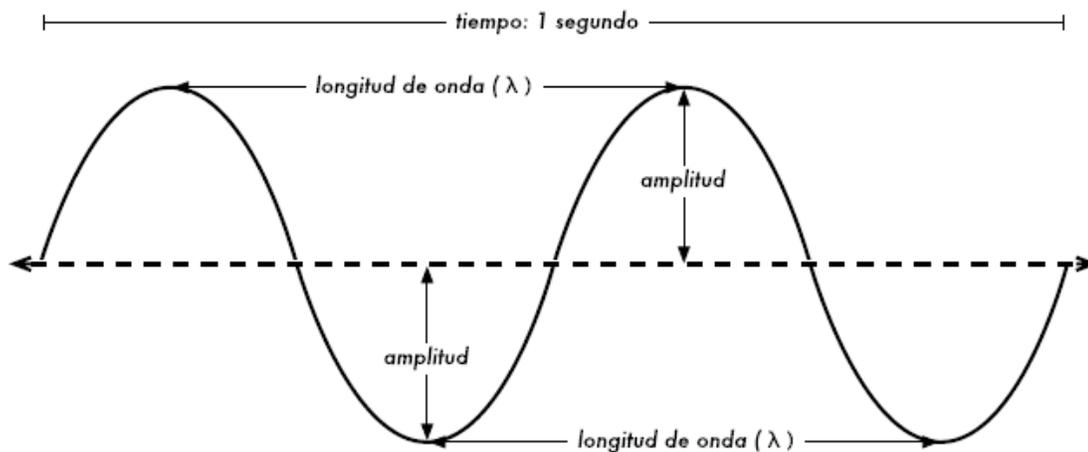


Ilustración 3-6 Longitud de onda. La imagen representa grafica de una onda y sus componentes.

La amplitud (A) como se observa en la imagen anterior, es la distancia entre el centro de la onda y el punto más distante de uno de sus picos. En el ejemplo del agua podemos decir que la amplitud equivale a la altura de la onda de agua.

Otra característica de las ondas es la frecuencia, esta se mide en Hertz (ciclos por segundo) y no es más que la cantidad de ondas completas que pasan por punto específico en un segundo. La velocidad se mide en metros/segundos.

Pero los ejemplos anteriores son fáciles de apreciar para la vista, pero hay unas ondas especiales que no son visibles para el ojo humano, como lo son las ondas electromagnéticas las cuales se detallaran a continuación.

3.2.2 Ondas electromagnéticas

Para entender que son las ondas electromagnéticas, primero se debe conocer que es una fuerza electromagnética, y estas son que fuerzas que ocurren entre corrientes y cargas eléctricas. El ejemplo más sencillo y fácil de observar es cuando llueve y vemos esos destellos de luz que se desplazan de la tormenta a la tierra, este fenómeno conocido como relámpago es ocasionado por una fuerza electromagnética.

En las ondas que antes se describieron, era fácil saber lo que se estaba desplazando y por consiguiente observar la onda cuando se desplazaba sobre la superficie en cuestión, ocurre el caso contrario en las ondas electromagnéticas porque su desplazamiento ocurre en el campo electromagnético, por consiguiente, se complica su observación para el ser humano.

Otro ejemplo de fuerzas electromagnéticas es la **antena dipolo**, la cual se construye al empujar periódicamente electrones de un extremo a otro en un alambre de metal, llegara un momento en que estos electrones estarán en un solo lado con lo cual estará cargado negativamente y el extremo opuesto positivamente. (Flikenger, 2008)

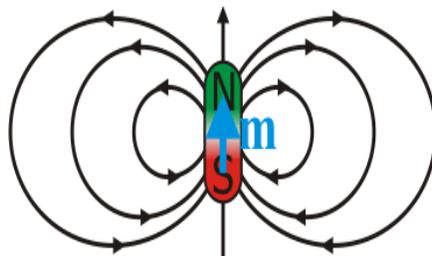


Ilustración 3-7 Antena dipolo

Cuando lo antes descrito ocurre se genera un campo eléctrico que va de positivo a negativo o viceversa dependiendo de que orientación se quiera tomar. Cuando las cargas cambian de lado el campo eléctrico también lo hace, este cambio constante en el campo eléctrico, hace que este se vaya desplazando del alambre y es radiado en el espacio que lo rodea. Cuando este sale al espacio que lo rodea ocasiona movimiento en el espacio electromagnético y es lo que se le conoce como ondas electromagnéticas.

Ya se habló de las características de una onda, pero cabe resaltar que en las ondas electromagnéticas la frecuencia y la longitud de la onda son vitales para comprender el comportamiento de dichas ondas. Si tienen una longitud y una frecuencia determinada cumple con un estándar ya establecido, los cuales se utilizan para la construcción de antenas que se ocupan para la operación de redes inalámbricas.

3.2.2.1 Espectro electromagnético

El espectro electromagnético abarca un gran rango de longitudes y frecuencias de ondas electromagnéticas, el ser humano solo puede percibir algunas porciones de este espectro y es el rango de la luz el cual es visible para el ojo humano. Esta porción está ubicada entre las frecuencias $7.5 \cdot 10^{14}$ Hz y $3.8 \cdot 10^{14}$ Hz, además con una longitud de onda entre los 400 nm. (violeta/azul) y los 800 nm(rojo).

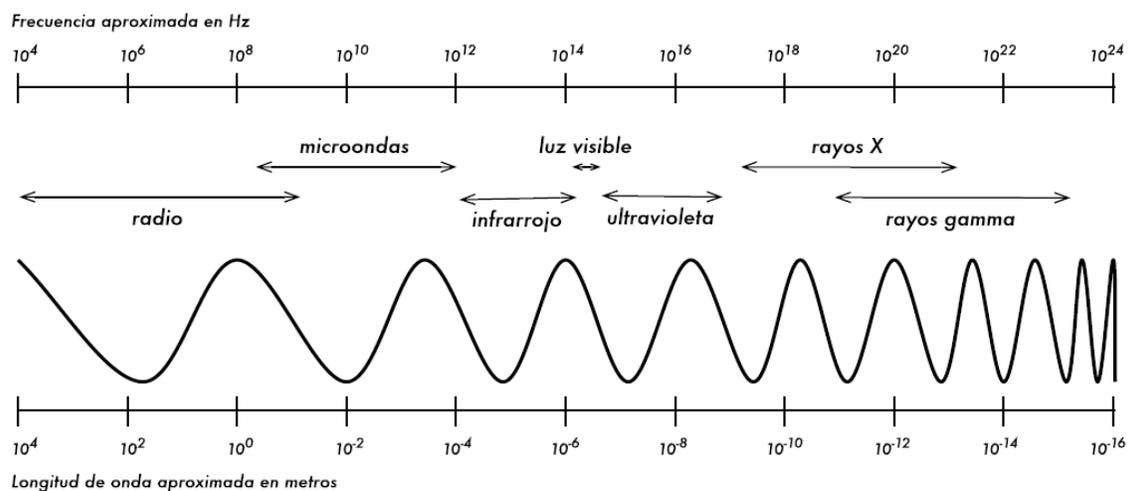


Ilustración 3-8 Frecuencia de ondas. Esta imagen muestra la distribución del espectro de frecuencias de ondas

Aunque solo son percibibles las antes descritas no quiere decir que son las únicas a las que está expuesto el ser humano, entre las más comunes están las **ondas de radio** que van de los 3Hz a los 300GHz, este gran rango del espectro electromagnético se denomina así porque se pueden transmitir ondas electromagnéticas aplicando corriente alterna a una antena. Además de estas se tienen los rayos X, infrarrojo, ultravioleta, el rango donde se transmite la corriente alterna, otra región bastante popular es la de las

microondas esta se encuentra entre frecuencias de 1 GHz y 300 GHz. La region de las microondas y las ondas de radio se encuentra en una region llamada como **banda ISM(Industrial, Cientifica y Medica)**, en esta banda se puede operar sin requerir de una licencia la cual en otras regiones del espectro electromagnetico es requerida, como por ejemplo las regiones donde se puede realizar comunicación de voz y datos, asi como tambien donde se transmite la television y la radio, para estas regiones es necesario contar con una licencia para operar, cuyo principal requisito es monetario razon por la cual no es facil obtener.

Las frecuencias que interesan en este proyecto son las que se encuentran entre los 2400MHz-5000MHz cuyas frecuencias son utilizados por los estantares 802.11(*Wi-Fi*) los cuales se ahondaran mas adelante.

3.2.2.2 Ancho de banda

Este término normalmente es usado para decir la cantidad de datos que se puede enviar o transmitir en la conexión a internet, por ejemplo “mi ancho de banda es de 4Mbps de internet” este término está mal empleado, para referirse a este se debe usar tasa de transferencia de datos.

Pero este ancho de banda no es más que una medida de rango de frecuencia, por ejemplo, si en un dispositivo está usando un rango de 2400 MHz a 2480 MHz, su ancho de banda es de 0.08 GHz o 80 MHz, es la diferencia entre el máximo y menor valor del rango que se está usando. Si el ancho de banda es más grande se pueden enviar más datos en un momento determinado.

3.2.2.3 Frecuencia y canales

Los protocolos 802.11b y 802.11g utilizan la banda 2.4 GHz, la cual está dividida en 14 canales iguales. Estos canales tienen un ancho de 22 MHz además la distancia entre el principio de un canal y su sucesor es de 5 MHz, esto lo podemos apreciar en la ilustración 3-9; con lo anterior se determina que si se usa el canal 1 este se traslapa con su sucesor el canal 2, además de traslaparse con el canal 3 y 4, lo que ocurre cuando dos dispositivos que están cerca utilizan canales que se traslapan es que se crean interferencia el uno con el otro y hace difícil la comunicación inalámbrica. A partir de lo anterior y como se muestra en la imagen para la banda 2.4 GHz los canales que no se traslapan son el 1, 6 y 11 lo que los convierte en los canales ideales para ser utilizados entre nodos cercanos y que no se cree interferencia entre ellos. (Flickenger, 2008)

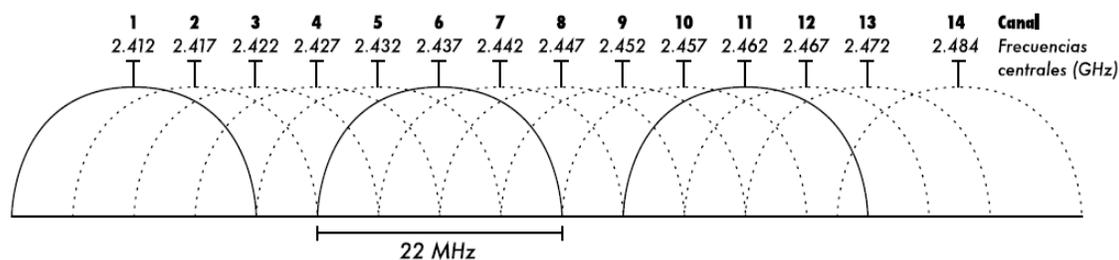


Ilustración 3-9 Canales de la banda 2.4 GHz

A pesar de ser 14 canales no los podemos utilizar todos, como ya se dijo anteriormente crean interferencias si se usan los canales sucesivos. Pero también hay un

nuevo motivo por el cual no se pueden usar, y es por razones geográficas, dependerá de la ubicación donde se necesite utilizar estos canales. En América no se pueden utilizar los canales 12, 13 y 14, en China además de estos no se puede usar el canal 1. En cambio, en Japón se pueden usar todos los canales, al contrario que Israel que es el dominio regulador que menos canales permite solo se pueden usar los canales del 3 al 9. **(Flickenger, 2008)**

A diferencia de la banda 2.4GHz, en la banda **5GHz** cada canal tiene un ancho de 20MHz con una separación de 5 MHz, la distancia entre canales sin superposición pasa de 4 en 2.4GHz a 3 en 5GHz, además esta banda posee 23 canales sin solapamiento que son legales utilizarlos, existen otros canales que no generan solapamiento pero que son ilegales ya que están destinado para el uso militar.

Un punto muy importante en los dispositivos que usan esta banda es que solo permiten configurarlos en los canales que no se superponen, además tiene como curiosidad esta banda que el primer canal configurable es el 36 y el ultimo el 165.

3.2.3 Comportamiento de las ondas electromagnéticas

Las ondas electromagnéticas poseen un comportamiento único con respecto a otro tipo de ondas, entre ellos encontramos algunos enunciados que son de mucha ayuda para determinar los dispositivos que se usan o se desean usar para la elaboración de una red inalámbrica.

Además de los comportamientos que ya se mencionaron, se encuentran otros los cuales se aplican cuando una onda electromagnética viaja. Estos comportamientos ayudan a identificar las interferencias a las cuales son sometidas las redes inalámbricas y poder elegir el lugar óptimo para la posición de las antenas. Si la onda electromagnética es más grande que un obstáculo presente esta lo rodeara, pero puede ocurrir el caso opuesto y tenga que impactar con el obstáculo. A partir de este choque pueden darse muchas situaciones que se describirán a continuación.

3.2.3.1 Absorción

Cuando una onda electromagnética viaja a través del espectro, esta deberá atravesar ciertos cuerpos que estarán presentes en el medio. Cuando una onda choca con un cuerpo esta puede desaparecer (ser absorbida por el cuerpo) o atravesarlo, esto dependerá del material por el cual este compuesto dicho cuerpo.

Si hablamos de absorción hay dos tipos de materiales que se pueden considerar como absorbentes perfectos, los cuales son el agua y los metales. Estos materiales por su composición anulan la energía de una onda, logran anularlo porque los electrones en este tipo de cuerpos pueden moverse libremente, por consiguiente, ese movimiento anula la energía que los quiere atravesar.

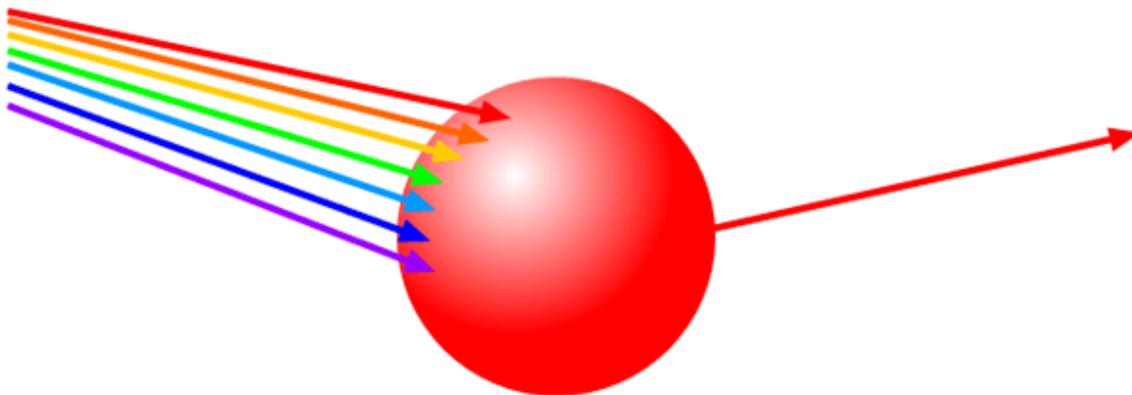


Ilustración 3-10 Ejemplo de absorción

Además de estos elementos en una zona geográfica donde se quiera construir un enlace de red inalámbrica, se encuentran muchos más elementos que componen el ambiente de la misma entre ellos tenemos árboles, paredes, vidrios, animales, personas, entre otros. Los árboles si su composición es seca tienen una absorción muy baja, por el contrario, si es árbol que tienen mucha agua su absorción es grande. Los vidrios se pueden considerar con absorción nula, al contrario que los humanos que tenemos una absorción muy grande, esto es debido a que nuestro cuerpo está compuesto mayormente por agua.

Por último, se debe de tener en consideración la altura a la que se pondrá el enlace de red inalámbrica, para que las ondas que sean enviadas no sean absorbidas por los elementos antes descritos. Así como también se debe considerar el material con el cual se protegerá el equipo que transmitirá la onda de radio, se deben usar materiales que sean atravesados fácilmente por estas y no pierda energía, si se utiliza plástico este debe probarse para que no interfiera con la potencia de las antenas.

3.2.3.2 Reflexión

Además de la absorción cuando una onda debe atravesar un cuerpo sufre otro fenómeno, este comportamiento es el de reflexión ocurre cuando una onda choca con un cuerpo esta no puede atravesarlo y es disparada en sentido contrario, pero con el mismo ángulo con el cual intercepto con el cuerpo reflectante.

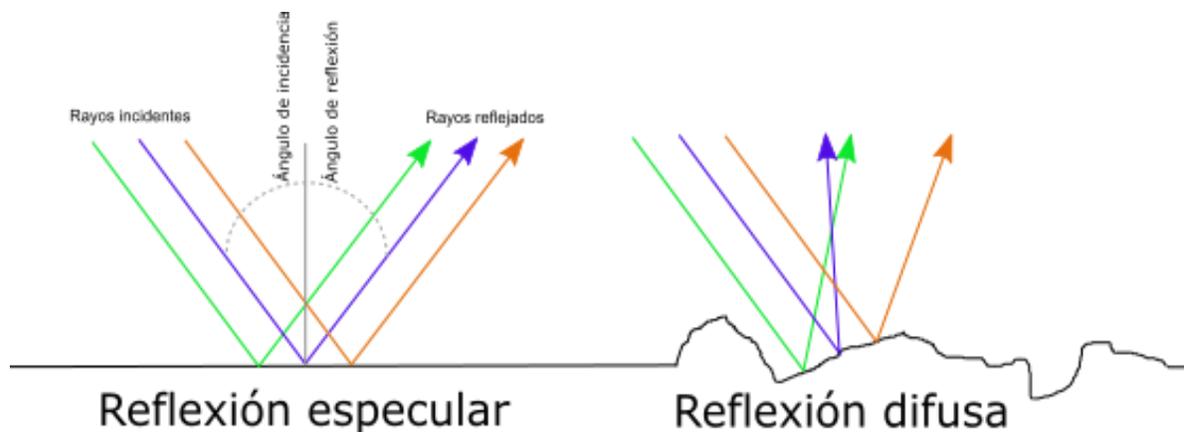


Ilustración 3-11 Reflexión de ondas

Al igual que en la absorción en la reflexión los materiales que más afectan este fenómeno son los metales y el agua, cuando una onda se encuentra en un medio compuesto por muchos metales es difícil saber la trayectoria que esta tomara, porque esta se ira reflejando en los diferentes elementos y tomara muchos caminos probables para llegar a un mismo punto.

3.2.3.3 Difracción

Como ya se mencionó cuando una viaja se puede encontrar con obstáculos y uno de ellos puede ser una barrera, pero además esta barrera puede tener una pequeña abertura donde puede salir una porción de la onda. Esta barrera la podemos imaginar como una pared que posee una pequeña puerta, cuando la onda impacte con la pared esta se detendrá, pero por la zona donde se encuentra la puerta esta comenzara una trayectoria circular como si se tratara de una nueva onda electromagnética.

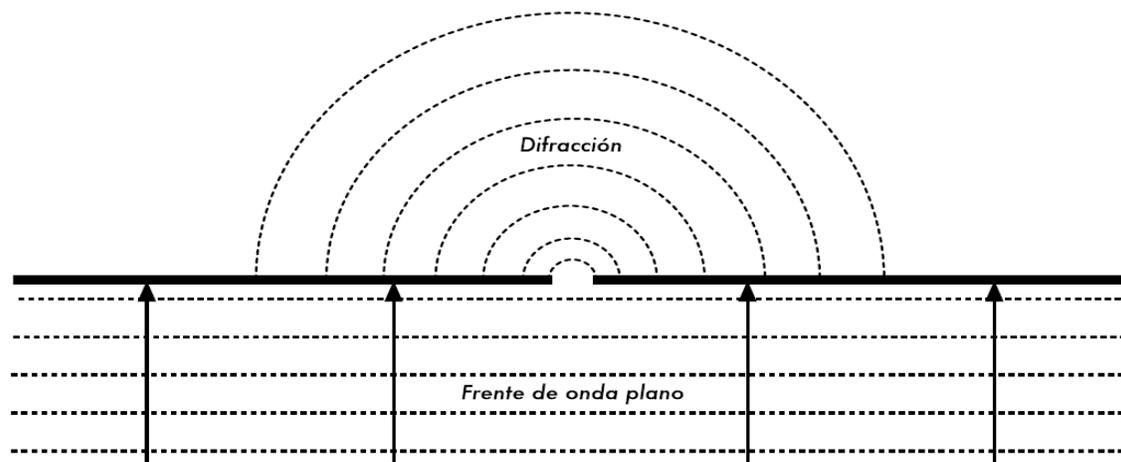


Ilustración 3-12 Difracción de ondas

Una de las ventajas que ocurre la difracción, es que la onda alcanzara puntos más allá de la zona donde se encuentre el punto de apertura. En contra parte cuando una onda sufre difracción pierde potencia.

3.2.3.4 Interferencia

Las ondas tienen comportamientos muy inusuales como ya se describió anteriormente, por esta misma razón hay muchas razones por las cuales perciben

interferencias. Una de ellas es cuando más ondas se encuentran en el espectro electromagnético, debido a que la suma de dos ondas no siempre da como resultado una onda de mayor amplitud, en algunos casos la suma de esas ondas nos puede llevar a un resultado nulo. Esto ocurre cuando un pico de una onda se alinea con un valle de otra onda, como resultado nos da un resultado nulo esto se conoce como **interferencia destructiva**. El caso opuesto es cuando el pico de una onda se alinea con el pico de otra onda nos da como resultado 2 este fenómeno se conoce como **interferencia constructiva**.

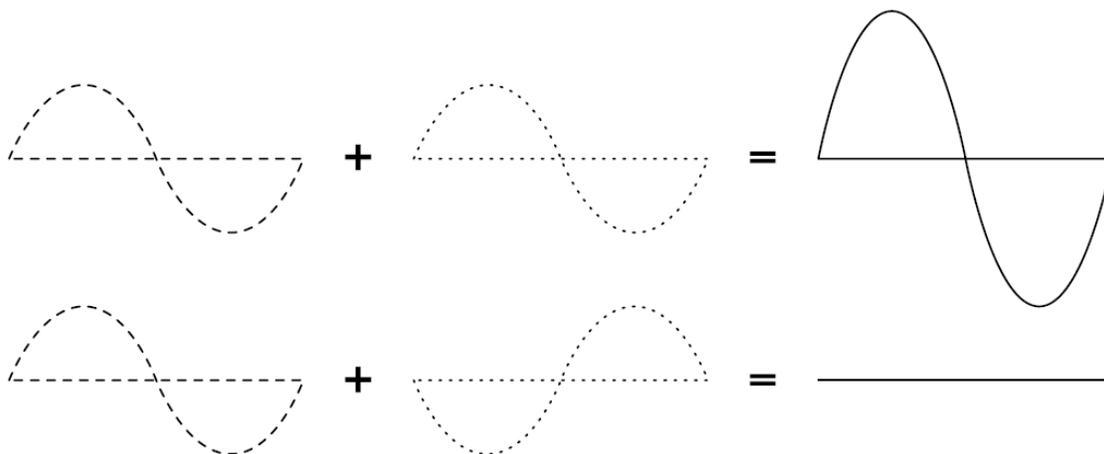


Ilustración 3-13 Interferencia de ondas

Además, cuando dos ondas chocan se puede tener un tercer resultado y es que cuando estas se combinen generen una nueva onda, la cual no podrá ser interpretada por el dispositivo receptor.

3.2.4 Antenas

Como ya se mencionó anteriormente una antena es, un medio capaz de transmitir ondas electromagnéticas si se le aplica corriente alterna. Esta empieza a emitir ondas electromagnéticas cuando su campo eléctrico está cambiando periódicamente, este fenómeno hace que el campo eléctrico comience a abandonar la antena y a desplazar esa energía por el campo electromagnético.

Las antenas comúnmente se catalogan como: débiles o de gran potencia, la potencia se mide en **decibeles** (dB) esta una unidad no tiene dimensiones. El cálculo de los dB se apoya en la siguiente formula: $dB = 10 * \log (P1/P0)$, donde P1 y P0 serán las potencias que se quieren comparar.

Otra medida que a menudo encontramos son los **dBi**, la cual se usa para medir la potencia de una antena isotrópica. Esta antena es la que transmite la potencia de forma uniforme en todas las direcciones, pero esta no es más que una antena idealizada porque no existe. El hecho de que esta antena no existe nos lleva al siguiente término la **polarización**, esta característica describe la dirección en la cual se están transmitiendo las ondas. Debido a esto debemos alinear correctamente las antenas, porque de no hacerlo esta no podrá alcanzar con sus ondas a la antena que estará recibiendo la información.

En la actualidad cuando se habla de antenas y la dirección a la cual pueden transmitir sus ondas encontramos las antenas **direccionales** y **omnidireccionales**.

3.2.4.1 Antenas direccionales

Esta antena tiene un alcance máximo de 60 grados en el plano horizontal (coordenadas polares). Esta concentración de su alcance, le permite potenciar toda su energía y concentrarla en un mismo punto, este punto generalmente es donde se encuentra otra antena. Esta característica la hace propicia para establecer una conexión de red entre dos puntos separados por una distancia considerablemente amplia.

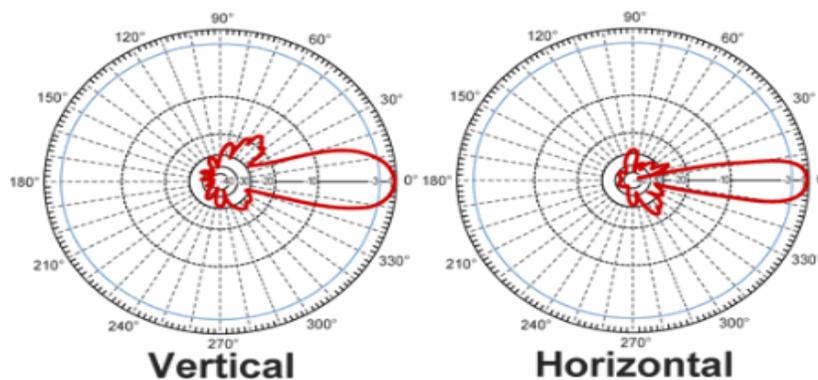


Ilustración 3-14 Alcance de las antenas direccionales

A pesar de lo antes mencionado también se usan para otro tipo de funciones, ya sea para brindar servicios de internet u otro tipo de conexiones a distancias cortas, pero en las que se requiere concentrar su alcance un punto específico.

3.2.4.2 Antenas omnidireccionales

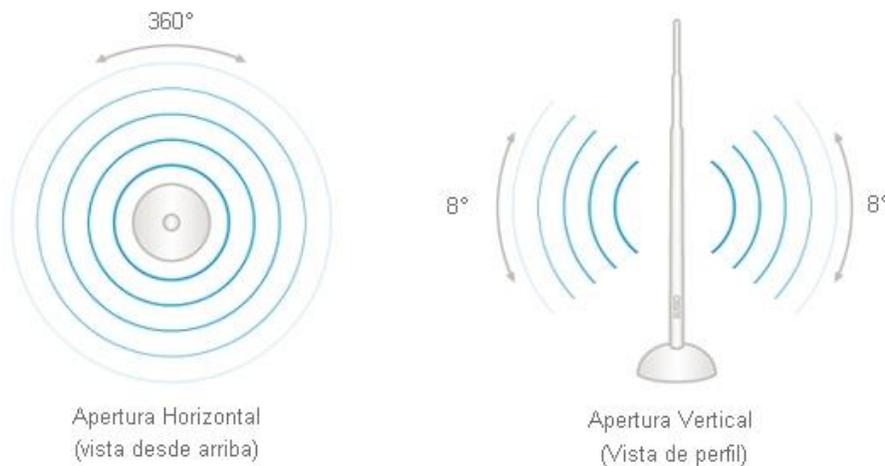


Ilustración 3-15 Alcance de las antenas omnidireccionales

A diferencia de las antenas direccionales, este tipo de antenas envían sus ondas de radio a través de los 360 grados del plano horizontal (coordenadas polares). Dicho de otra forma, esta antena envía las ondas de radio aproximadamente con la misma intensidad en todas direcciones posibles en el plano horizontal.

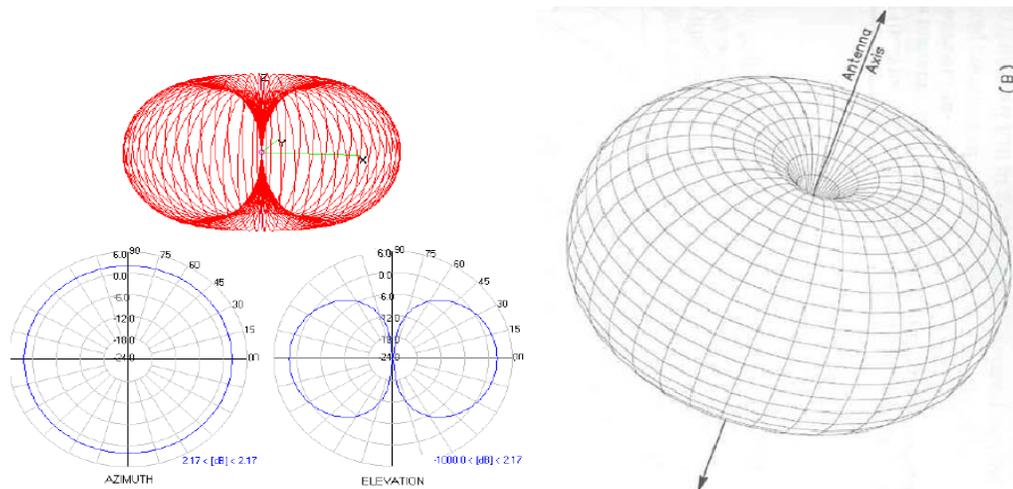


Ilustración 3-16 Ondas de una antena omnidireccional

A pesar de que su nombre es omnidireccional, esto solo se cumple en el plano horizontal, ya que en el vertical no es así. Se aclara, porque la mayoría de personas se imagina, que las ondas de radio que una antena omnidireccional emite, se pueden dibujar en el espacio como una esfera, pero esto es incorrecto. La representación que se aproxima más a estas ondas de radio de las antenas omnidireccionales es una dona, esto ocurre porque en el punto superior e inferior de la antena no se están emitiendo ondas de radio.

3.3 Estándar IEEE 802.11 (Wi-Fi)

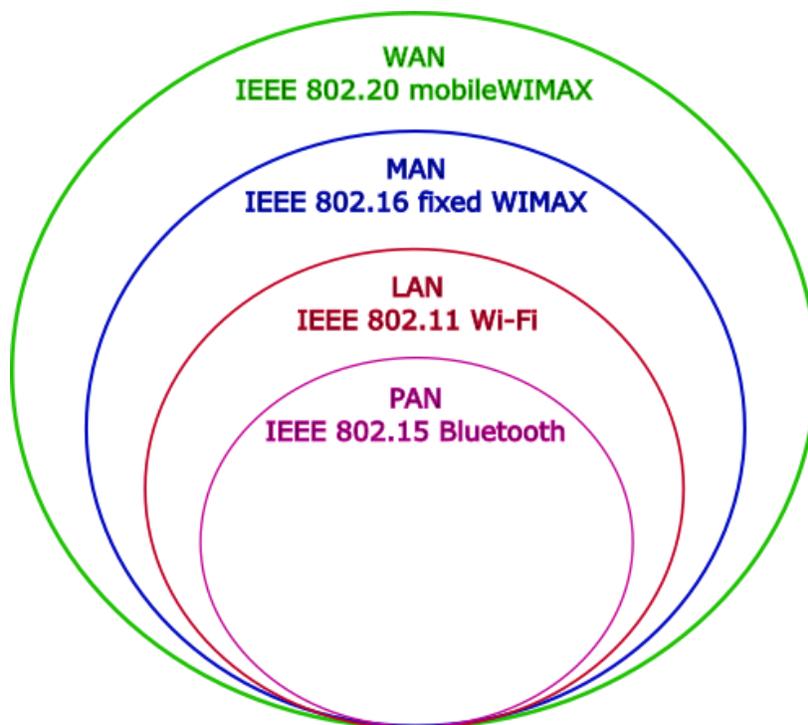


Ilustración 3-17 Ubicación del protocolo Wi-Fi: Enmarcado de esta forma según el alcance de la red, WAN < 150 Km., MAN < 50 Km., Wi-Fi < 150 mts., Bluetooth < 10 mts.

La tecnología de conexiones inalámbricas se impulsó de manera notoria desde la creación del estándar 802.11 mejor conocido como *Wi-Fi*, 802.11 es un conjunto de estándares de la IEEE para la implementación de redes inalámbricas de computadoras, este estándar apareció en 1999 incorporando los protocolos 802.11a y el 802.11b, los cuales no son los únicos ya que actualmente se tiene una amplia gama de protocolos de la familia 802.11, ver *Tabla 3-1*, este proyecto se enmarca en la utilización de interfaces de red inalámbricas bajo el protocolo 802.11n, se amplía el estudio de este protocolo en el siguiente apartado. 802.11 tiene una serie de estándares que trabajan con diferentes

frecuencias, anchos de banda, tecnologías de Hardware, entre otros aspectos, que hacen que cada uno de diferentes resultados en la comunicación, siendo el principal aspecto medido, la tasa de transferencias que se alcanza con cada uno de estos estándares.

Tabla 3-1 Versiones del protocolo 802.11

<i>Lanzamiento</i>	<i>Estándar</i>	<i>Banda</i>	<i>Ancho de banda</i>	<i>Modulación</i>	<i>Tecnologías avanzadas de antenas</i>	<i>Tasa máxima de transferencia</i>
<i>1997</i>	802.11	2.4	20	DSSS, FHSS	-	2 Mbits/s
<i>1999</i>	802.11b	2.4	20	DSSS	-	11 Mbits/s
<i>1999</i>	802.11a	5	20	OFDM	-	54 Mbits/s
<i>2003</i>	802.11g	2.4	20	DSSS, OFDM	-	54 Mbits/s
<i>2009</i>	802.11n	2.4, 5	20,40	OFDM	MIMO, hasta cuatro corrientes espaciales	600 Mbits/s
<i>2012</i>	802.11ad	60	2160	SC, OFDM	<i>Beamforming</i>	6.76 Gbits/s
<i>2013</i>	802.11ac	5	40,80,160	OFDM	MIMO, MU-MIMO, hasta ocho corrientes espaciales	6.93 Gbits/s

3.3.1 802.11n

802.11n es una mejora a los estándares previos 802.11a y 802.11g, teniendo como principal aspecto el incremento en la tasa de transferencia de 54MBps de sus predecesores a hasta 600MBps según las condiciones que permita de Hardware y de la presencia de otras radiofrecuencias que puedan generar ruido. Dentro de las mejoras que incluye este estándar están, el uso de MIMO, *Multiple-Input Multiple-Output*, diversidad de antenas y multiplexado espacial, uso de tramas en la capa MAC y la unión de interfaces de red.

Con el uso de MIMO se logra el uso de más de una antena, hasta cuatro, para la emisión y recepción de datos, logrando que se envíe mucha más información que con los protocolos predecesores que solo permiten una antena. Para lograr esto se utiliza la multiplicación espacial SDM, que hace que se puedan generar múltiples flujos de transferencia de información a la vez, para que esto funcione se necesita una antena para cada flujo de transferencia. De modo que, si el emisor cuenta con tres antenas, pero el receptor solo con dos, la comunicación solo se llevara a cabo con dos antenas.

Otra de las mejoras es el uso de canales que operan con 40MHz de ancho, anteriormente a este estándar se utilizaba solo el de 20MHz, por lo que con el estándar n se puede transmitir el doble con el mismo canal. Esto se puede lograr tanto con las bandas de frecuencia a de 5GHz o la de 2.4GHz que permite el estándar, aunque en 2.4GHz es

poco viable en zonas urbanas debido a que no debe haber ningún ruido que interfiera con el canal usado, en cambio 5GHz tiene más canales libres.

3.3.2 802.11ac

802.11ac es un estándar de la IEEE para conexiones inalámbricas, es más reciente que el anteriormente mencionado 802.11n. Este estándar permite conexiones de al menos 500Mbps de tasa de transferencia y logrando hasta los 1.69 Gbps, logrando así tasas de transferencias muy superiores al estándar 802.11n.

Al igual que con 802.11n los factores que hacen la diferencia principalmente son, el uso de más antenas a la vez y el incremento del ancho del canal de comunicación. Con 802.11ac se pueden llegar a utilizar hasta ocho antenas en simultáneo, siempre apoyando con MIMO para lograr transmitir por todas ellas a la vez. Pero además permite recibir datos de diferentes clientes con diferentes antenas, con lo que se da mejor uso a las antenas disponibles, con el uso de multiMIMO, que es una variante de MIMO para trabajar con múltiples clientes usando MIMO con cada uno de ellos.

El otro aspecto fundamental es que trabaja en la frecuencia de los 5GHz con un ancho de banda de canal de 80MHz, hasta los 160MHz, duplicando o cuadruplicando así el máximo de su predecesor 802.11n que trabajaba con canales de hasta 40 MHz.

La combinación de antenas, anchos de banda y la mejora de la tecnología para la transmisión y recepción de las frecuencias logran que 802.11ac tenga tasas de transferencia que tiene, muy superiores a estándares anteriores.

3.3.3 Modos Wi-Fi

Todos los dispositivos *Wi-Fi* pueden ser configurados para que actúen de una forma u otra dependiendo de qué es lo que se necesite, cabe aclarar que no todos los protocolos que existen pueden operar en todos los modos que se describirán a continuación. Estas configuraciones son 4: modo master o de infraestructura, modo administrativo, modo *ad-hoc* y modo monitor.

3.3.3.1 Modo master o de infraestructura

Una tarjeta en modo master ofrece un servicio de red que parece ser un punto de acceso (AP) tradicional, dicho de otra forma, crea una red inalámbrica que por lo general permite la conexión a internet a los usuarios de esta. Para que este modo pueda operar se le debe configurar un canal y un nombre de red, dicho nombre es conocido como SSID. La asignación del canal debe de ser asignado procurando que no se vea afectado por otros dispositivos que estén actuando con este mismo modo y estén utilizando el mismo canal de comunicación o uno que lo traslape. Otra característica de este modo es que no pueden comunicarse con los demás dispositivos configurados con este mismo modo, en cambio brindan conexiones a los dispositivos configurados en modo administrativo.

3.3.3.2 Modo administrativo

Este es el modo por defecto en los dispositivos comerciales con *Wi-Fi*, en este modo el dispositivo solo se podrá conectar a una red creada por otro dispositivo en modo master, por esta razón es que este modo se le conoce además con el nombre de modo cliente.

Para que este modo funcione se le deben enviar las credenciales (validaciones) de ser necesarias, si estas credenciales son válidas el dispositivo que está brindando la conexión de red las aceptara y se podrá establecer la conexión de red. Al igual que en el modo master dos dispositivos configurados con el mismo modo administrativo no se podrán comunicar de forma directa.

3.3.3.3 Modo ad-hoc

Una red *ad-hoc* inalámbrica es aquella en las que no hacen falta nodos especiales que encaminen y gestionen el tráfico, sino que cada nodo tiene la capacidad de reenviar paquetes dirigidos a otros nodos de la red. Dicho de otra forma, se puede tener una red de dispositivos que se comuniquen sin necesidad de enrutadores o puntos de acceso. Este es el modo fundamental para la creación de las redes Mesh que tanto se mencionan en este proyecto, pero las cuales serán explicadas más adelante.

3.3.3.4 Modo monitor

Este es un modo especialmente usado por aplicaciones, las cuales son utilizadas para monitorizar el tráfico de radio en un canal dado. En este modo no se transmiten datos, ya que solo se utilizan para analizar problemas en enlaces inalámbricos o para observar el uso de la red. Con lo anterior se puede concluir que no es un modo usado para la comunicación entre dos usuarios finales.

3.4 Red Mesh

Las redes *Mesh*, redes en malla o redes *ad-hoc* como las denomina el estándar 802.11 de la IEEE, son redes que funcionan multipunto a multipunto, es decir no tienen una topología estructurada como la redes comunes, por consiguiente la comunicación no pasa por un dispositivo central que organiza la comunicación, sino que se trata de una serie de nodos que se encargan de hacer la red y utilizar estos servicios, en la mayoría de casos se efectúan estos dos procesos simultáneamente aunque ocasionalmente simplemente algunos nodos podrían simplemente servir para conformar la red a modo de enrutadores.

Este tipo de red tiene un nivel de complejidad mayor que las punto a multipunto comunes en lo que al reto tecnológico respecta, ya que la coordinación que se necesita para llevar a cabo la comunicación es mucho más compleja porque no se tiene un punto que organice la topología, sino que esta se va conformando a medida los nodos se van uniendo a la red. (Butler, 2013)

3.4.1 Funcionamiento

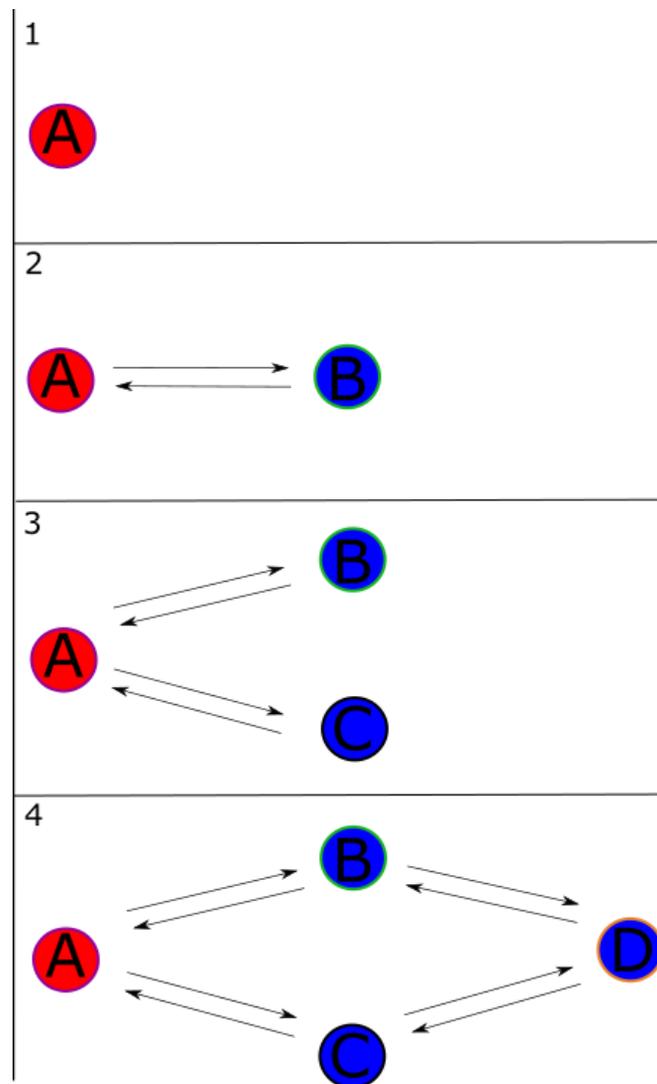


Ilustración 3-18 Topología Mesh

La topología de red se va conformando con la interconexión de nodos con sus vecinos alcanzables, de modo que, al agregar un nodo solitario, este genera una celda (1). Luego al agregar otro nodo que se encuentre en su rango de alcance, este lo reconoce y genera un enlace similar a una conexión punto a punto (2). Al agregar un nuevo nodo

cercano al primero y a la vez al segundo se generan 2 nuevos enlaces entre estos (3). Si se agrega un cuarto nodo lejano al primero, pero en el rango del segundo y tercer nodo se generan 2 enlaces, pero el primer nodo siempre es capaz de comunicarse con el cuarto porque puede llegar a este a través del segundo o desde el tercer nodo (4). Incluso si se pierde comunicación con el segundo o el tercer nodo, la comunicación seguiría existiendo ya que siempre habría una ruta disponible para llevar a cabo la comunicación.

Esta es la razón por la cual las redes Mesh se convierten en una red escalable y a la vez altamente confiable, mientras más nodos se agregan esta red va ganando robustez por poseer más redundancia. El hecho que haya más redundancia no significa que un paquete dará muchos más saltos antes de llegar a su destino, para ello el protocolo de enrutamiento ejecuta algoritmos para determinar la mejor ruta entre 2 nodos que requieran comunicarse. **(Butler, 2013)**

3.4.2 Protocolos de enrutamiento para redes Mesh

Para las redes Mesh como para cualquier tipo de red existen muchos protocolos de enrutamiento, que ayudan a mantener la red comunicada entre sí o con otras redes, de los cuales muchos ya no están vigentes, otros están en desarrollo y otros han logrado actualizarse para ser utilizados en la actualidad.

Estos numerosos protocolos existentes, se clasifican de acuerdo a ciertos criterios, como lo son su alcance, su modo de descubrir las rutas o el algoritmo que emplean;

Como se describe en (**Doumenc, Hélène 2008**) los cuales se clasifican de la siguiente manera.

Por su alcance:

- *Los protocolos unicast* son los que transmiten información de un único destino a un único receptor.
- *Los protocolos multicast* consisten en mandar simultáneamente información a múltiples destinos, usando la estrategia más eficiente para el envío de los mensajes sobre cada enlace de red.

Basado en el modo de descubrimiento de rutas

- *Los protocolos proactivos* intentan tener en cada momento, e independientemente de las necesidades de encaminamiento, una visión precisa del estado de la red. Se busca mantener actualizadas las tablas de encaminamiento a través del envío de mensajes de forma periódica. Esta característica procura una respuesta rápida ante solicitudes de ruta y suele ofrecer un buen comportamiento en los escenarios de movilidad alta. Sin embargo, para mantener una actualización permanente de las rutas, se introduce una sobrecarga importante de la red con los mensajes de control.
- *Los protocolos reactivos*, solo obtienen información de encaminamiento cuando es necesario. Son protocolos bajo demanda que buscan la ruta hacia un destino en el momento en el que se quiere mandar información a ese destino. Obviamente, en las redes que usan esos tipos de protocolos la sobrecarga es menor que para los

protocolos proactivos. Sin embargo, los retardos al establecimiento de las comunicaciones son mayores.

- *Los protocolos híbridos* que combinan esos dos esquemas utilizando, por ejemplo, proactividad en las cercanías del nodo considerado, pero buscando las rutas bajo demanda para los nodos más alejados.

Basado en el algoritmo implementado por el protocolo

- Protocolo basado en el vector de distancia, cada nodo mantiene una tabla de encaminamiento y periódicamente, cada nodo pasa su tabla a sus vecinos. Con la información recibida, cada nodo recalcula su tabla.
- Por otro lado, se encuentran los *protocolos basados en el estado del enlace*. En los cuales todos los nodos mantienen una tabla del mapa completo de la red. Cada nodo envía periódicamente el estado del enlace con sus nodos vecinos y a partir de esta información se actualizan o no las tablas de cada nodo.

3.4.2.1 OLSR

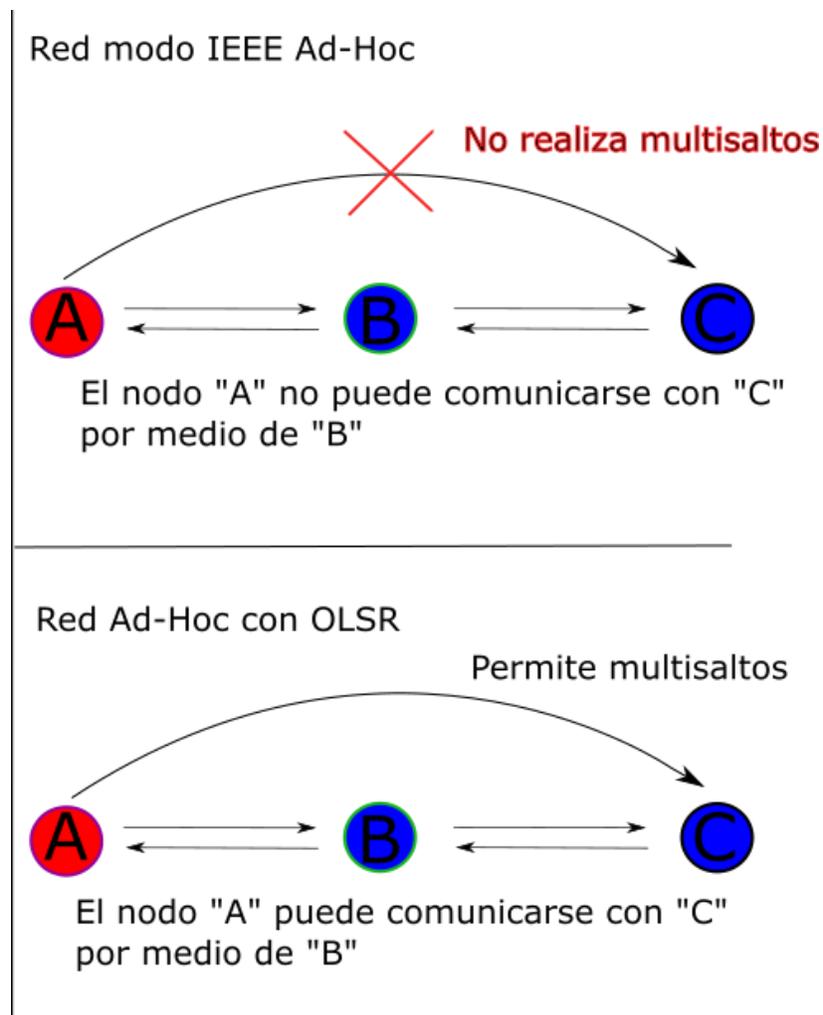


Ilustración 3-19 Muestra de posibilidad de comunicación ampliada con OLSR

OLSR (*optimized link state route*), es un protocolo diseñado para trabajar con redes ad-hoc que también son conocidas como MANETs (*Mobile ad hoc network*). Se trata de un protocolo proactivo, es decir que actualiza la información de la topología de red con otros *routers* regularmente. El protocolo busca identificar todos los destinos de la red, identificar un subconjunto suficiente de enlaces en la red, con el fin de que las rutas

más cortas a todos los destinos disponibles se puedan calcular y proporcionar un conjunto de enrutamiento que contenga las rutas más cortas desde un *router* a todos los destinos.

La clave del funcionamiento esta en los *MPRs (multipoint relays)*, que son los encargados de reenviar la información. Cada *router* de la topología escoge 2 grupos de *MPRs* vecinos que se encuentren a no más de 2 saltos y que tengan enlaces simétricos, es decir que sean enlaces bidireccionales¹. Estos 2 grupos son los *MPRs* de inundación y los *MPRs* de ruteo. Con el uso de estos se permite la reducción de inundaciones y de topología.

La reducción de inundaciones se logra con el uso de *MPRs* de inundación, ya que un router solo necesita enviar el control de tráfico que es recibido por primera vez directamente desde uno de sus routers de inundación selectores (los asociados a él como *MPR* de inundación), así la cantidad de retransmisiones necesarias se vuelve menor.

La disminución de la topología apoyándose en los *MPRs* de ruteo que son los que reciben la información del estado de los enlaces de sus *MPRs* selectores y luego solo son ellos los encargados de difundirla por la red, evitando que cada router deba enviar el estado de sus enlaces a todos los demás *routers* cercanos. Es de recordar que el saber el

¹ Enlace bidireccional: Que es capaz de transmitir en ambos sentidos.

estado de los enlaces es fundamental para generar luego las rutas óptimas para el envío de datos.

Los objetivos del protocolo se logran haciendo que cada router:

- Identifique vecinos simétricos a uno y 2 saltos
- Reporte su participación en OLSR y que desea ser *MPR* de inundación y *MPR* de ruteo, mediante el envío de mensajes HELLO y la adición de un mensaje TLV *MPR_WILLING*.
- Extienda los mensajes HELLO para permitir la adición de enlaces de métricas direccionales a enlaces anunciados con otros *routers* que participan en OLSRv2 e indicar con qué tipo de métrica de enlace está siendo usado por estos *routers*.
- Seleccionando los *MPRs* de inundación y los *MPRs* de ruteo de entre los vecinos de un salto dispuestos de tal modo que, para cada grupo de *MPRs*, todos los vecinos simétricos de 2 saltos sean accesibles directamente o a través de al menos un *MPR* selector, usando una ruta de métrica total mínima para al menos la selección del *MPR* de ruteo.
- Señalando su *MPR* de ruteo y *MPR* de inundación seleccionado, extendiendo un mensaje HELLO para reportar esta información mediante la adición de *MPR* Address Block TLV(s) asociadas a las direcciones de red apropiadas.
- Extrayendo sus *MPRs* de inundación selectores y *MPRs* de ruteo selectores desde los mensajes HELLO recibidos, usando la *MPR* Address Block TLV(s) incluida.

-Definiendo un mensaje tipo TC (*topology control*). Los mensajes TC se usan periódicamente entre *MPRs* de ruteo selectores y en si toda la MANET. Esta señalización incluye las métricas direccionales de vecinos adecuadas (la mejor métrica de enlace es la dirección entre estos *routers*).

-Permitiendo que estos mensajes TC, así como los mensajes HELLO, sean incluidos en paquetes usados en el protocolo ip de la MANET o en el puerto UDP.

-Difundiendo los mensajes TC usando el mecanismo de reducción de inundación denotado MPR *flooding*. (**IETF-RFC7181, 2014**)

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Reserved										Htime										Willigness											
Link Code					Reserved					Link Message Size																					
Neighbor Interface Address																															
Neighbor Interface Address																															
...																															
Link Code					Reserved					Link Message Size																					
Neighbor Interface Address																															
Neighbor Interface Address																															

Ilustración 3-20 Estructura de un mensaje HELLO de OLSR

0										1										2										3			
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1		
ANSN																				Reserved													
Advertised Neighbor Main Address																																	
Advertised Neighbor Main Address																																	

Ilustración 3-21 Estructura de un mensaje TC de OLSR

3.4.2.2 BATMAN

Better Approach To Mobile Adhoc Networking mejor conocido como B.A.T.M.A.N. es un protocolo de comunicación para redes *ad hoc* al igual que OLSR, aunque este protocolo tiene como objetivo solucionar los problemas que presenta OLSR. A pesar que tiene poco tiempo de estar en el mercado -en comparación con OLSR- está siendo muy aceptado por la comunidad dedicada al área de redes inalámbricas.

Este protocolo aun esta en desarrollo, sus creadores son la Comunidad “Freinfuk” cuya idea se originó en el año 2007. Dichos desarrolladores hicieron pruebas para hacer posible el enrutamiento en la capa 2 del modelo OSI (capa Ethernet) en lugar de la capa 3 como tradicionalmente se ha realizado.

BATMAN conserva ciertos aspectos que utilizan otros protocolos de enrutamiento, entre los cuales se pueden destacar: encontrar nodos BATMAN además de encontrar la mejor ruta a dichos nodos. Otro aspecto es el poder detectar los nuevos nodos y enviar información sobre estos a sus nodos vecinos.

Este protocolo de comunicación utiliza un mensaje especial de comunicación llamado “emisión”, el cual se está enviando de forma periódica para informar a sus vecinos que aún está activo. Cuando los vecinos reciben dicho mensaje, estos lo reenvían

a sus vecinos y así sucesivamente a los demás nodos de la red. La función de este mensaje es llevar la información a cada nodo de la red con el fin de poder encontrar la mejor ruta para un nodo BATMAN.

Lo antes descrito es una de las premisas por las cuales fue creado BATMAN la cual consiste en descentralizar la información de ruteo de un solo nodo y llevándola a todos los nodos de la red, dicha premisa busca eliminar la difusión de información relativa de los cambios de la red a todos los nodos que la componen. Con esta premisa el nodo solo envía datos de una “dirección” solo si recibe información de esta, esto conlleva a que la información sea enviada de nodo a nodo y se obtienen paquetes de rutas individuales, dichos paquetes se crean de forma dinámica.

El comportamiento en el envío de paquetes en BATMAN funciona de la siguiente forma: un paquete tiene como origen un nodo el cual determina la ruta óptima para el destino, a diferencia de los protocolos de estado de enlace BATMAN no trata de determinar la ruta completa que el paquete debe seguir hasta llegar a su destino, dicho de otra forma, cada nodo BATMAN utiliza un algoritmo para determinar la mejor ruta hacia el destino del paquete. **(Butler, 2013)**

3.5 Prototipo

Según Ecured define un prototipo como: “Los prototipos son un método de validación ampliamente utilizado en muchas disciplinas, y en todos los casos, los principios son los mismos: el prototipo consiste en la creación de una maqueta o versión

del producto final. Los objetivos de los prototipos varían en función de la disciplina.” (Ecured, 2015).

Dicho de otra forma, un prototipo es una muestra de lo que se pretende implementar, estos sirven para advertir eventuales fallos en el funcionamiento y descubrir falencias.

3.5.1 Prototipo tecnológico

De acuerdo a la siguiente se puede definir como: “Un prototipo es también un modelo a escala o facsímil de lo real, pero no tan funcional como para que equivalga a un producto final, ya que no lleva a cabo la totalidad de las funciones necesarias del sistema final, proporcionando una retroalimentación temprana por parte de los usuarios acerca del sistema”. (Ecured, 2015)

3.5.2 Prototipo de red

Un prototipo de red puede ser virtual o real. La principal diferencia es que en el virtual se simula una arquitectura de red, a través de software especializado para esta función, tales como: GNS3, Packet Tracer, NetFPGA entre otros. En esta simulación se puede interactuar con la red en un escenario ideal, debido a que no se presentan interferencias en la transmisión de datos causadas por el entorno de toda la arquitectura de red (CL, 2015).

En cambio en el real se utiliza hardware que se pueda configurar a través de un firmware y pueda trabajar de forma óptima de acuerdo a las funciones que deba de

realizar, este hardware puede ir desde interfaces de red así como *switches*, routers, servidores entre otros (CL, 2015).

La mayor limitante que presenta este prototipo es el económico ya que para poder elaborarlo debemos de contar con todo el hardware necesario para hacerlo, así como también en caso de ser requerido adquirir licencias de software, para que el hardware pueda funcionar.

La mayor ventaja que presenta el prototipo real es que se hacen las pruebas en el lugar físico donde se quiere implementar la red, con esto se identifican las interferencias que deben de ser corregidas, así como los demás errores que se encuentren. (CL, 2015)

3.6 Videovigilancia

En la actualidad existen dos tipos de sistemas de videovigilancia, *Sistemas CCTV* y los *Sistemas de videovigilancia basados en IP*, a estos dos tipos se les unen los *Sistemas de videovigilancia Híbridos*, que es la aplicación de los dos sistemas anteriores en una misma solución de videovigilancia.

3.6.1 Sistemas CCTV

Circuito cerrado de televisión o CCTV (siglas en inglés de *Closed Circuit Television*). Es una tecnología de videovigilancia diseñada para supervisar una diversidad de ambientes y actividades. Es un sistema no tan moderno donde las cámaras CCTV se adaptan para poder estar controladas remotamente desde una sala de control, donde se puede configurar su panorámica, inclinación y zoom. En efecto, con la videovigilancia

digital es posible monitorear remotamente, por medio de Internet, todas las cámaras conectadas a un DVR (Grabador de Video Digital), realizando las configuraciones necesarias según sea la arquitectura de la red, dicha configuración queda fuera del alcance de este trabajo.

Beneficios de los sistemas CCTV

- ✓ Según la instalación y el tamaño de la misma, puede ser más económica una solución digital a una solución IP.
- ✓ Facilidad de uso.
- ✓ Grabación y visualización simultáneas.
- ✓ Mejoras constantes en la tecnología de compresión y el almacenamiento.
- ✓ Alta calidad en la imagen.
- ✓ Alertas automáticas

Sistemas CCTV con DVR

El DVR es un dispositivo interactivo de grabación de video en formato digital que se utiliza en video seguridad para diversas funcionalidades como el tratamiento de las secuencias de video recibidas, acceso a guías de programación, búsquedas avanzadas de contenidos, conexión a Internet, entre otras.



Ilustración 3-22 DVR Swann modelo DVR4-2600

Beneficios de los sistemas CCTV con DVR

- Equipo diseñado completamente para monitoreo.
- Nivel de desarrollo más alto que sistemas basados en PC
- Si se corta la energía, el DVR vuelve a iniciar automáticamente cuando la energía vuelva sin necesidad de inicio manual.
- Inmune a virus por carecer de sistema operativo convencional y trabajar con uno propietario especializado para el requerimiento.
- Monitoreo 24 horas 7 días a la semana, sin recalentamientos ni fallas.
- Seguridad en la información guardada.
- Software integrado

3.6.2 *Sistemas de videovigilancia basados en IP*

La videovigilancia IP es aquella que aprovecha la red informática empresarial sin necesidad de desplegar una infraestructura de cableado coaxial específica para la red de videovigilancia. Así se utiliza el mismo cableado o el medio que se utilice para la red actual que se emplea para la comunicación de datos, acceso a Internet o correo electrónico. Las migraciones al sistema IP son cada vez más comunes debido a sus ventajas, este es el tipo de sistema de videovigilancia en el que se centrará la investigación de este trabajo de graduación por lo que se explica con más detalle en el apartado **3.7 *Videovigilancia IP***.

3.6.3 *Sistemas de videovigilancia Híbridos*

Un sistema de videovigilancia híbrido, es aquel que soporta un sistema CCTV análogo y video vigilancia IP, dicho sistema puede ser una gran alternativa según las necesidades específicas y particulares de cada usuario. Cuando se habla de un sistema híbrido se refiere a adaptaciones que se llevan a cabo desde el grabador, hasta el tipo de transmisión utilizada. Se puede tener un sistema inicial híbrido con un NDVR²

² NVDR *Network Digital Video Recorder*: Es un videograbador híbrido, ya que combina ambas tecnologías (analógica y digital). Se incluye en entornos donde se aprovechan instalaciones analógicas y se recurre a la tecnología IP.

(*Network Digital Video Recorder* – Grabador de video en Red y Digital), el cual podría integrar cámaras IP y cámaras CCTV análogas bajo un mismo grabador y reproductor de video.

Es posible considerar un sistema híbrido al realizar la migración de un sistema CCTV análogo a un sistema de seguridad IP, utilizando la misma infraestructura en cableado coaxial existente para transmitir video digital desde cámaras IP. Esto sería una solución magnífica si actualmente se cuenta con un sistema análogo y se quiere actualizar, o simplemente pasar a un sistema de seguridad IP, sin generar sobrecostos.

También se pueden mantener las cámaras CCTV análogas y empezar a utilizar cámaras IP, integrando todo bajo una misma plataforma.

Ventajas al Implementar Video Vigilancia Híbrida

Al combinar un sistema analógico de circuito cerrado de televisión con un sistema de vigilancia IP, se adquiere todas las funcionalidades y ventajas que ofrece la tecnología digital, reduciendo costos al utilizar la infraestructura análoga.

- ✓ Accesibilidad remota
- ✓ Fácil integración y funcionalidad actualizable
- ✓ Escalabilidad y flexibilidad
- ✓ Rentabilidad
- ✓ Inteligencia distribuida

- ✓ Mejor calidad de imagen
- ✓ Combina las ventajas de la tecnología analógica de circuito cerrado de televisión con la flexibilidad y facilidad de acceso proporcionados por la tecnología IP.

3.7 Videovigilancia IP

Como ya se describió antes de manera breve la videovigilancia IP es un sistema de vigilancia visual digital, que actualmente está dominando el mercado de seguridad, dejando a un lado la videovigilancia CCTV. A continuación, se profundiza un poco más en cuanto a sus componentes tecnológicos.

Arquitectura



Ilustración 3-23 Arquitectura de la videovigilancia IP

Se pueden identificar tres elementos básicos que todo sistema de videovigilancia IP debe poseer: Cámaras o dispositivos IP que permitan el *streaming* de video, medios por los cuales se transmite dicho *streaming* de video y por el ultimo el software y todo el equipo de hardware que permite el monitoreo de las cámaras IP. Estos elementos se estudian con mucho más detalle a continuación.

3.7.1 Cámara IP



Ilustración 3-24 Cámara IP

Captura el vídeo y el audio (en caso de incorporar entrada y salida de audio) y puede ser fijas o móviles, estando conectadas por cable o en modo inalámbrico a una red de datos IP, a través de la cual se puede controlar y almacenarla información en NVRs (Network Video Recorder) o servidores de vídeo en red.

Características principales

- Resolución megapíxel: Mayor resolución lo que se traduce en poder visualizar detalles imposibles de ver con cámaras analógicas y/o VGA tradicionales.
- Zoom óptico: Acercamiento de imagen mediante el objetivo y sin pérdida de calidad de imagen.
- Zoom digital: Ampliación/acercamiento de una imagen mediante técnicas digital con una consiguiente disminución de la resolución de la imagen.
- 3GPP video streaming: Permite visualizar remotamente vídeo online de una cámara IP en un teléfono 3G o *smartphone*.
- Conector I/O (entrada/salida): Diseñados para conectar dispositivos externos a la cámara tales como sirenas/alarmas, detector de movimientos, sensores de temperatura, iluminador externo, etc.
- Barrido progresivo: Consigue una mayor nitidez y claridad en la grabación y visualización de imágenes en movimiento.

Funcionamiento básico

Este trabajo de graduación no tiene por objetivo ahondar tanto en detalles técnicos del funcionamiento de las cámaras, sino más bien, su aplicación en una solución como videovigilancia, es por esto que se limita a brindar un conocimiento general de estas tecnologías.

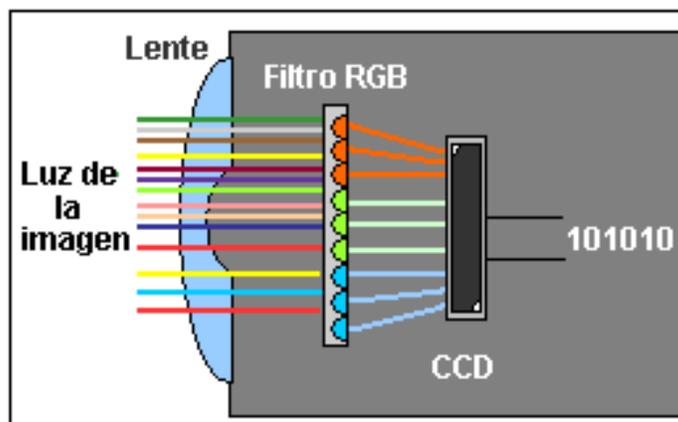


Ilustración 3-25 Funcionamiento de una Cámara IP

La luz de la imagen pasa por la lente, esta se refleja en un filtro RGB (Red-Green-Blue), el cuál descompone la luz en tres colores básicos: rojo, verde y azul. Esta división de rayos se concentra en un chip sensible a la luz denominado CCD ("Charged Coupled Device"), el cuál asigna valores binarios a cada píxel y envía los datos digitales para su codificación en video y posterior envío a través de Internet o la red local hasta el dispositivo (celular moderno, Desktop o Laptop), desde el cuál se monitorea la cámara.

Partes de una cámara IP

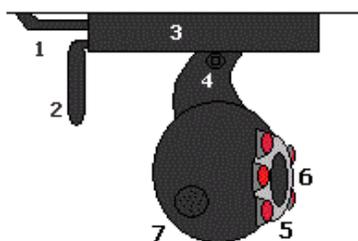


Ilustración 3-26 Esquema partes externas de una Cámara IP

1. Panel trasero: suministra de energía eléctrica al dispositivo y cuenta con el puerto RJ11 para conectividad por medio de cable UTP.
2. Antena: permite una mejor señal de red inalámbrica.
3. Base giratoria horizontal: permite colocar la cámara en la posición horizontal que el usuario decida.
4. Brazo giratorio vertical: permite colocar la cámara en la posición vertical que el usuario decida.
5. Visor digital: se encarga de captar las imágenes a transmitir y grabar vía Internet. En caso de contar con la característica, pueden tener LED's infrarrojos, que permiten visualizar en la oscuridad.
6. LED's: permiten visualizar, incluso cuando no hay luz visible.
7. Micrófono: se encarga de grabar el audio.

Resolución en cámaras IP

La resolución de una cámara indica el grado de detalle con que esta puede obtener una imagen, es decir que a mayor resolución mayor detalle tendrá la imagen capturada, mayor serán la cantidad de detalles que se pueden distinguir en un acercamiento digital.

La unidad con que se mide la resolución es *El Pixel*

Pixel

Un píxel o pixel, plural píxeles (acrónimo del inglés *picture element*, ‘elemento de imagen’), por definición es la menor unidad homogénea en color que forma parte de una imagen digital.

Concepto de Pixel

Ampliando lo suficiente una imagen (zoom) en la pantalla de una computadora, como puede observarse en la *ilustración 3 – 25*, pueden observarse los píxeles que componen la imagen. Los píxeles son los puntos de color (siendo la escala de grises una gama de color monocromática). Las imágenes se forman como una sucesión de píxeles. La sucesión marca la coherencia de la información presentada, siendo su conjunto una matriz coherente de información para el uso digital. El área donde se proyectan estas matrices suele ser rectangular. La representación del píxel en pantalla, al punto de ser accesible a la vista por unidad, forma un área homogénea en cuanto a la variación del color y densidad por pulgada, siendo esta variación nula, y definiendo cada punto sobre la base de la densidad, en lo referente al área. **(Wikipedia, 2016)**

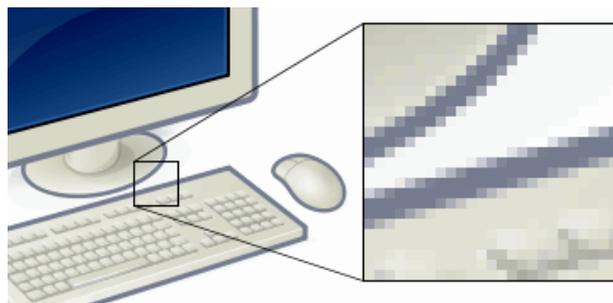


Ilustración 3-27Ejemplo de un píxel, en una imagen ampliada digitalmente

Si bien el pixel es la unidad fundamental, se utiliza el múltiplo **Megapíxel** como la unidad más habitual para denotar la resolución de una cámara o de una imagen, así como también la resolución de un video. Un megapíxel (Mpx) equivale a 1 millón de píxeles, a diferencia de otras medidas usadas en la computación en donde se suele utilizar la base de 1024 para los prefijos, en lugar de 1024 se utiliza la base 1000, debido a su conveniencia respecto del uso del sistema binario. Usualmente se utiliza esta unidad para expresar la resolución de imagen de cámaras digitales; por ejemplo, una cámara que puede tomar fotografías con una resolución de 2048×1536 píxeles se dice que tiene 3,1 megapíxeles ($2048 \times 1536 = 3.145.728$).

La cantidad de megapíxeles que tenga una cámara digital define el tamaño de las fotografías que puede tomar y el tamaño de las impresiones que se pueden realizar; sin embargo, hay que tener en cuenta que la matriz de puntos está siendo distribuida en un área bidimensional y, por tanto, la diferencia de la calidad de la imagen no crece proporcionalmente con la cantidad de megapíxeles que tenga una cámara.

La videovigilancia se está moviendo hacia megapíxeles de resolución para la vigilancia de vídeo de alta definición. Hoy en día, se puede encontrar una amplia selección de cámaras de megapíxeles de resolución que adopta la tecnología analógica o digital de la tecnología IP. Actualmente, los formatos de resolución más comunes de megapíxeles son: 1.3, 2 y 3 megapíxeles, así como 5, 6 y 8 megapíxeles¹ (ver *tabla 3-1*).

¹ Nota: 6 megapíxeles y cámaras IP de megapíxeles 8 están todavía en desarrollo

Tabla 3-2 Tabla de resoluciones más conocidas y utilizadas

Nombre	Ancho (píxeles)	Altura (píxeles)	Total (píxeles)
1MP / 720P	1280	720	921,600
QVGA / 960P	1280	960	1228,800
1.3MP	1280	1024	1310,720
2MP / 1080P	1920	1080	2073,600
2.3MP	1920	1200	2304,000
3MP	2048	1536	3145,728
5MP	2560	1920	4915,200
6MP	3032	2008	6088,256
8MP	3264	2448	7990,272

En orden de dejar más claro este concepto se presenta la siguiente ilustración comparativa de 4 formatos bien conocidos, en la cual se aprecia la diferencia de tamaño y en las imágenes (ver *ilustración 3-28*).



Ilustración 3-28 Comparación entre distintas resoluciones

Es natural suponer que al aumentar la resolución de las imágenes estas aumente de tamaño de almacenaje, lo que provoca una sobrecarga en la red al momento de transmitir las, no es lo mismo transmitir una secuencia de imágenes con resolución QVGA a transmitir una secuencia de imágenes a 1080P, para solucionar este problema surgieron los códec de video de alta compresión que se estudia de manera general y en específico el códec H.264 en el siguiente apartado.

Códec de video

Un códec de video es un tipo de códec que permite comprimir y descomprimir video digital. Normalmente los algoritmos de compresión empleados conllevan una pérdida de información.

El problema que se pretende acometer con los códec es que la información de video es bastante ingente en relación a lo que un ordenador normal es capaz de manejar. Es así como un par de segundos de video en una resolución apenas aceptable puede ocupar un lugar respetable en un medio de almacenamiento típico (disco duro, Cd, DVD) y su manejo (copia, edición, visualización) puede llevar fácilmente a sobrepasar las posibilidades de dicho ordenador o llevarlo a su límite.

Es así como se ha preferido construir y ocupar estos algoritmos de compresión y descompresión en tiempo real: los códec. Su finalidad es obtener un almacenamiento sustancialmente menor de la información de vídeo. Esta se comprime en el momento de guardar la información hacia un archivo y se descomprime, en tiempo real, durante la visualización. Se pretende, por otro lado, que el proceso sea transparente para el usuario, es decir, que no intervenga o lo haga lo menos posible.

Existe un complicado equilibrio entre la calidad de video, la cantidad de datos necesarios para representarlo (también conocida como tasa de bits¹), la complejidad de los algoritmos de codificación y decodificación, la robustez frente a las pérdidas de datos

¹ En informática y telecomunicaciones, el término tasa de bits define el número de bits que se transmiten por unidad de tiempo a través de un sistema de transmisión digital o entre dos dispositivos digitales. Así pues, es la velocidad de transferencia de datos.

y errores, la facilidad de edición, la posibilidad de acceder directamente a los *frames*, y otros factores.

Códec H.264

H.264 o MPEG-4 parte 10 es una norma que define un códec de vídeo de alta compresión, desarrollada conjuntamente por el ITU-T Video Coding Experts Group (VCEG) y el ISO/IEC Moving Picture Experts Group (MPEG). La intención del proyecto H.264/AVC fue la de crear un estándar capaz de proporcionar una buena calidad de imagen con tasas binarias notablemente inferiores a los estándares previos (MPEG-2, H.263 o MPEG-4 parte 2), además de no incrementar la complejidad de su diseño (**Wikipedia, 2016**).

Para garantizar un ágil desarrollo de la misma, la ITU-T y la ISO/IEC acordaron unirse para desarrollar conjuntamente la siguiente generación de códecs de vídeo. El Joint Video Team (JVT) estaba formado por expertos del VCEG y MPEG y nació en diciembre de 2001 con el objetivo de completar el desarrollo técnico del estándar hacia 2003. La ITU-T planeó adoptar el estándar bajo el nombre de ITU-T H.264 e ISO/IEC bajo el nombre de MPEG-4 Parte 10 Códec de Vídeo Avanzado (AVC) y de aquí surgió el nombre híbrido de H.264/MPEG-4 AVC. Para empezar a programar el código del nuevo estándar adoptaron las siguientes premisas:

- La estructura DCT + Compensación de Movimiento de las versiones anteriores era superior a otros estándares y por esto no había ninguna necesidad de hacer cambios fundamentales en la estructura.

- Algunas formas de codificación de vídeo que habían sido excluidas en el pasado debido a su complejidad y su alto coste de implementación se volverían a examinar para su inclusión puesto que la tecnología VLSI había sufrido un adelanto considerable y una bajada de costes de implementación.
- Para permitir una libertad máxima en la codificación y evitar restricciones que comprometan la eficiencia, no se contempla mantener la compatibilidad con normas anteriores.

3.7.2 Medio de comunicación

Se refiere a al medio físico por el cual es transmitida la información, toda la información referente a este apartado ya fue cubierta previamente en el punto *3.1 Redes informáticas*.

3.7.3 Software de la estación de monitoreo

Es todo aquel software que permite la decodificación de las transmisiones, así como su visualización en tiempo real, existen diversidad de software que permiten dicho objetivo, pero este trabajo se enmarca en el uso exclusivo de software libre, por lo cual se centra en dicho software como lo es *ZoneMinder*, *Motion*, *Blue Iris*.

ZoneMinder

ZoneMinder es un conjunto de aplicaciones que conjuntamente proporcionan una completa solución de video vigilancia permitiendo capturar, analizar, grabar y monitorizar cualquier cámara CCTV, Cámaras IP, Webcam, etcétera conectada a una

máquina basada en Linux. Está diseñado para ejecutarse en distribuciones de Linux que soporten la interfaz Video For Linux (V4L) y puede soportar múltiples cámaras sin pérdida aparente de rendimiento. ZoneMinder requiere MySQL y PHP y se apoya en un servidor web como Apache.

4 Objetivos

4.1 Objetivo General

Determinar la factibilidad técnica y financiera de la aplicación de las redes *Mesh* en el área de la videovigilancia en zonas públicas y ampliación de zonas *Wi-Fi* de la alcaldía San José Las Flores.

4.2 Objetivos específicos

- Realizar una investigación de los componentes de hardware y software necesarios para desarrollar una red *Mesh*, un sistema de videovigilancia y una zona *Wi-Fi*, en función de las necesidades que debe cumplir el prototipo a realizar, para funcionar bajo las condiciones que el municipio de San José Las Flores necesita.
- Realizar una selección de componentes a utilizar para el desarrollo del prototipo y documentar el porqué de dicha selección basándose en coste del componente, calidad del servicio, robustez (durabilidad y adaptabilidad).
- Adquirir los componentes de hardware seleccionados e implementar en ellos el software libre seleccionado para el posterior desarrollo del prototipo.
- Desarrollar un prototipo funcional brindando los servicios, videovigilancia y ampliación de zonas *Wi-Fi*, con los componentes seleccionados; basados en el municipio sujeto a estudio.
- Realizar comparación de costos entre el modelo de sistemas de vigilancia y zona *Wi-Fi* soportado por red *Mesh* (en base al prototipo) y modelos que utilicen otro tipo de dispositivos y topologías de red existentes en el mercado.

5 Metodología de la investigación

La investigación busca determinar la factibilidad que puedan llegar a tener las redes inalámbricas tipo Mesh, como alternativa de comunicación para soportar servicios de videovigilancia y acceso a internet en zonas públicas a cargo de instituciones públicas.

La investigación conlleva dos instrumentos para la obtención de información, un instrumento para la recolección de datos relevantes a la población afectada con el proyecto y un instrumento enfocado a la evaluación de aspectos tecnológicos. El centro de la investigación está en el desarrollo, observación y evaluación del instrumento tecnológico, siendo el desarrollo y estudio del prototipo funcional la base de este instrumento.

Para la investigación se necesitó el estudio de diversos factores que conllevan una mezcla de métodos de medición de resultados tanto cuantitativos como cualitativos.

5.1 Diseño del instrumento de recolección de datos

Este instrumento busca obtener la apreciación de la necesidad y funcionalidad de desarrollar el proyecto de parte de la población que se verá afectada con el mismo, conocer la expectativa y grado de apoyo de la institución hacia el proyecto, obtener otros datos relacionados a la factibilidad del proyecto como obtención de presupuestos institucionales para desarrollo de proyectos, registro de proyectos similares en instituciones del mismo tipo.

La investigación requiere del instrumento la utilización de diversos métodos de investigación según el tipo de información que se necesita medir.

5.1.1 Cálculo del universo

Para la determinación de la percepción poblacional del municipio con respecto al proyecto se utilizará el siguiente universo y muestra.

Tabla 5-1 Población del municipio San José Las Flores

Municipio	Total	Mujeres	Hombres
San José Las Flores	585	291	294

Resultados Oficiales de los Censos Nacionales VI de Población y V de Vivienda 2007 para el casco urbano del municipio.

Con una población total de 585 en el casco urbano del municipio y con una incertidumbre de menos 40 o 30 debido a la discriminación de todos los infantes y jóvenes que no hayan cumplido los 15 años, se trabajara con las cantidades siguientes.

Universo: Todo aquel habitante del municipio San José Las Flores con 15 años sin límite de edad ni distinción de sexo o discapacidad física.

Muestra: 66 habitantes, la muestra fue calculada en base a un nivel de confianza del 95% y un porcentaje de error de un 5%.

Formula obtención de muestra:

$$n = \frac{k^2 * p * q * N}{(e^2 * (N-1)) + k^2 * p * q}$$

En donde:

N = tamaño de la población, 585

K = nivel de confianza, valor a usar 1.96 correspondiente al 95%

p= probabilidad de éxito, o proporción esperada, 95%

q = probabilidad de fracaso 5%

e = error muestral 5%

Con la muestra se llevarán a cabo las técnicas de recolección de datos de **entrevista** para luego hacer una **medición** de los datos y determinar la existencia de una necesidad.

5.1.2 Métodos cuantitativos

Los métodos cuantitativos en el instrumento de recolección de datos de la investigación son necesarios para obtener la apreciación de la necesidad y funcionalidad de desarrollar el proyecto de parte de los ciudadanos del municipio.

Para ello utilizara una encuesta, a realizarse en una cantidad de habitantes acorde a la proporción de toda la población necesaria para que la investigación sea objetiva. La encuesta contendrá una serie de ítems que esperan saber de la población, el conocimiento previo de lo que es la videovigilancia y el Wi-Fi, apreciación sobre la necesidad de

videovigilancia y acceso a internet en zonas públicas, posibilidad de acceso a internet.

Los ítems específicos y la razón de estos en la encuesta son:

- Edad, sexo y ocupación: Necesarios para clasificar la población encuestada.
- ¿Sabe lo que es un sistema de videovigilancia?, pregunta cerrada opciones de respuesta: si o no, esta pregunta recabara información si se conoce el término de videovigilancia entre los ciudadanos del municipio.
- ¿Alguna vez ha oído hablar de un sistema de videovigilancia para su comunidad?, pregunta cerrada opciones de respuesta: si o no, esta pregunta pretenderá obtener información, sobre antecedentes (si es que se tiene) o si se está desarrollando un proyecto de este tipo en el municipio.
- ¿Conoce los costos de un sistema de videovigilancia?, pregunta cerrada opciones de respuesta: si o no, el objetivo de esta pregunta es conocer la noción que puedan tener los ciudadanos de la inversión que implica desarrollar un proyecto de este tipo.
- ¿Cree usted necesario un sistema de videovigilancia en su comunidad?, pregunta cerrada opciones de respuesta: si o no, esta pregunta buscara dar a conocer si la población realmente considera útil tener este servicio en su municipio.
- ¿Diría que, San José las Flores es una ciudad moderna?, pregunta cerrada opciones de respuesta: si o no, el objetivo de esta pregunta es recolectar

información sobre la percepción que tienen los ciudadanos del municipio sobre el desarrollo que tiene actualmente dicho municipio.

- ¿Considera que la modernización de su comunidad es importante?, pregunta cerrada opciones de respuesta: si o no, esta pregunta buscara recolectar información de los habitantes sobre la importancia que tiene la modernización del municipio, si quieren que siga la línea de modernización si cundieran que ya es un municipio moderno, con respecto a aspectos tecnológicos o si consideran que debe modernizarse porque actualmente no lo está.
- ¿Cuánto es lo máximo que debe invertir su gobierno local (alcaldía) en términos monetarios (\$) en la seguridad pública de su municipio?, pregunta abierta, buscara obtener información sobre el presupuesto que consideren necesario los ciudadanos para desarrollar proyectos de seguridad en el municipio, con lo cual se comparara si los costos del proyecto se encuentran entre los rangos aceptados por los habitantes.
- ¿Cuánto vale (\$) su seguridad?, es una pregunta abierta que intentara conocer el valor que le puedan dar los habitantes a su seguridad. No sirve como parámetro monetario, sino más bien como un parámetro de si consideran la inversión en seguridad importante o no.
- ¿Cómo cree usted, que un sistema de videovigilancia podría ayudar a su comunidad?, las opciones de respuesta disponibles son, reacción, prevención, sensación y no sabe. Con esto se buscará saber que efecto

crea la población que podría tener en su entorno un sistema de videovigilancia.

- ¿Sabe lo que es *Wi-Fi*? pregunta cerrada opciones de respuesta: si o no, esta pregunta buscara saber, si se conoce el termino entre los habitantes del municipio.
- ¿Posee una conexión inalámbrica (*Wi-Fi*) a internet en su hogar?, pregunta cerrada, se utilizará para saber qué porcentaje de la población tiene acceso a internet a través de una conexión *Wi-Fi* en su hogar, la pregunta es útil para evaluar si no se está ofreciendo un servicio que en realidad ya está cubierto, aunque no sea directamente en zonas públicas.
- ¿En la actualidad, es necesario el internet para la educación?, pregunta cerrada la cual pretenderá conocer que tanto relacionan internet con educación los habitantes del municipio.
- ¿Es económicamente capaz de adquirir una conexión a internet personal? Pregunta cerrada que intentara conocer si los habitantes pueden tener acceso a internet si lo desean, con el factor económico que esto implica. De considerar realmente importante el internet la población, el número de encuestados que dicen poder pagar una conexión a internet debería de coincidir con los que dicen poseerla.
- ¿De qué manera le ayudaría tener acceso gratuito a internet de forma inalámbrica?, pregunta de múltiples opciones que contempla comunicación, investigación, no sabe, tareas y tareas y comunicación

como sus posibles respuestas. Con esta pregunta se esperará conocer con qué fin podrían aprovechar la población el acceso a internet.

- ¿Necesita internet inalámbrico en lugares públicos (un parque, un comedor público) ?, pregunta cerrada que buscara saber la necesidad de prestar el servicio de *Wi-Fi*.

5.1.3 Métodos cualitativos

Para los aspectos cualitativos se recurrirá a la entrevista al alcalde o al director de proyectos de la alcaldía, por ser los que pueden estar directamente involucrados con el proyecto. En la entrevista se espera saber la expectativa que tiene la institución del proyecto, como consideran que es su alcaldía, si consideran que prestar los servicios de videovigilancia y Wi-Fi es importante, adonde desean que se instalen las cámaras de videovigilancia, que zonas esperan cubrir con el Wi-Fi, con qué recursos cuentan para dar soporte al proyecto y que grado de implicación tendrán con el proyecto, este último punto es muy importante porque con este se espera saber si la alcaldía está dispuesta a financiar el proyecto o no.

5.1.4 Documentos institucionales

La investigación requiere la obtención de información previa, como lo es, el presupuesto de la alcaldía para el desarrollo de proyectos, este aspecto se puede solventar con la consulta del presupuesto para desarrollo que otorga el gobierno a la alcaldía en la que se realizara el proyecto, para luego poder compararlo con el costo que determine la

investigación que tiene implementar el proyecto, y ver si está acorde a lo que se puede permitir una institución como la alcaldía en la que se desarrollara el proyecto.

Obtención de información de proyectos de videovigilancia realizados en otras alcaldías, con el fin de poder comparar el costo del proyecto desarrollado con otros realizados previamente, como posible punto de factibilidad del proyecto.

5.2 Diseño del instrumento tecnológico

La investigación conlleva un instrumento tecnológico que es el prototipo funcional, este permitirá la obtención de datos relacionados con la viabilidad técnica del proyecto. El prototipo debe cumplir con los requerimientos del entorno físico en el que la institución indique que debe funcionar, con los requerimientos que implican los servicios que va a prestar y con la tecnología de comunicación que se ha ofertado. En base al cumplimiento de estos requerimientos se evaluará la viabilidad del proyecto.

El prototipo consiste en una serie de nodos conformados por elementos de Hardware y Software configurados para prestar servicios captura de video y funcionalidad de punto de acceso a red inalámbrica, que se comunican entre sí a través de una red inalámbrica Ad-Hoc tipo Mesh, y están conectados a una fuente de acceso a internet. Conformando un sistema de videovigilancia y puntos de acceso inalámbrico a internet diseñado para trabajar en una zona pública a cargo de la institución para la que se realiza el proyecto.

La realización del prototipo a un nivel general se hará de la siguiente forma:

1. **Elección de componentes**, implica la elección de componentes de Hardware y Software que se utilizaran en el prototipo, basándose en los servicios que este debe prestar.
2. **Diseño**, etapa en la que, a partir de los componentes obtenidos, requerimientos de los servicios a prestar y del entorno en el que debe funcionar el prototipo, se desarrollan los lineamientos a seguir para la posterior construcción del prototipo.
3. **Desarrollo**, en el desarrollo se llevará a cabo la realización del prototipo como tal, esto conlleva el armado físico de los componentes de Hardware para conformar los nodos, instalaciones de Software, pruebas de funcionamiento, corrección de fallas, entre otros relacionados a la realización del prototipo. En esta etapa puede haber algunas desviaciones respecto al diseño, debido a que no se sabe con certeza si lo diseñado será funcional al momento de realizar el prototipo.
4. **Obtención de resultados**, en esta etapa se obtendrán a partir del prototipo ya funcionando datos relevantes para la realización de las factibilidades del proyecto. Además, se obtendrá lo que es capaz de hacer realmente el prototipo.

Cada etapa tendrá su metodología de realización, para las etapas de elección de componentes, diseño y obtención de resultados, se detalla su metodología en este apartado, en el caso del desarrollo su metodología se especificará en el diseño del prototipo.

5.2.1 Elección de componentes

La elección de componentes debe seguir con una serie de lineamientos según las funciones que deban cumplir los componentes, siempre en función de los servicios a prestar. Los componentes del prototipo a evaluar son Hardware, Software y Protocolos. La etapa de elección de componentes se apoyará en la investigación y contemplará los aspectos necesarios que cada componente necesita, la investigación se realizará a través de diferentes fuentes como internet, consultas a proveedores o cualquier otro medio viable para obtención de información.

5.2.1.1 Componentes de Hardware

Para la elección de los componentes de Hardware se tienen que evaluar 3 componentes, placa base, cámara e interfaces inalámbricas. Se debe tomar en cuenta que puede haber algún componente que sea capaz de englobar a más de uno de estos componentes a la vez, de ser ese el caso la elección de cámara o interfaces inalámbricas podría omitirse si se elige un componente que englobe a la placa con uno o ambos componentes adicionales.

Para el desarrollo del prototipo se ha optado por 2 opciones iniciales, las cuales consisten en armar el prototipo a partir de una placa base que permita la adición de dispositivos de hardware adicionales o algún tipo de Hardware ya prefabricado al que se le puedan adicionar dispositivos a través de algún puerto de comunicación y que se le pueda cambiar su Firmware para adecuarlo a lo que se necesita.

En el caso de usar una placa base se piensa en un Hardware que permita una personalización de los nodos, se trata de una placa base no diseñada inicialmente para cumplir las funciones que requiere el prototipo, a pesar de esto se le puedan agregar los dispositivos de Hardware adicionales que mejor se adapten a las necesidades del prototipo, además de poder instalar una amplia gama de sistemas operativos y Software que permita el funcionamiento de los servicios con el Hardware. Con esta opción se debe evaluar aparte de la placa, los dispositivos adicionales que se puedan necesitar.

La otra opción es un Hardware ya prefabricado, este término se usará para referirse a dispositivos que ya cumplan todas o parte de las funciones que debe hacer el prototipo, en caso de cumplir con algunas funciones se necesitará buscar una forma de adicionar dispositivos que permitan terminar de cumplir las funciones que requiere el prototipo.

Se deben evaluar una serie de **aspectos** tanto para la **placa base** como para un **Hardware prefabricado**, para luego poder llevar a cabo la elección del mejor Hardware disponible. Los aspectos a evaluar son:

- **Diseño original:** Se busca saber cuál es la función para la que se desarrolló el Hardware.
- **Soporte de sistema operativo:** Los nodos necesitan soportar diversos servicios que muy rara vez se encuentran listos para funcionar en un software ya preinstalado, pero un sistema operativo presenta una gama de posibilidades más amplia para poder soportar estos servicios.

- **Soporte a dispositivos adicionales:** Se habla de poder soportar Hardware adicional al que ya viene, con esto se busca poder ampliar las posibilidades que se puedan tener, en lo que respecta al Hardware. Ya que aunque el Software pueda soportar la adición de nuevas funciones, si no se cuenta con el Hardware necesario tampoco será útil, en ese sentido es fundamental que el Hardware que se obtenga permita la adición y funcionamiento de otro Hardware adicional, a menos que se obtenga un hardware que ya cuente con todas las funciones que se van a necesitar, pero eso corta el desarrollo del proyecto hasta cierto punto, ya que usualmente los productos de este tipo suelen ser más cerrados en cuanto a personalización y no suelen ser de código abierto.
- **Capacidad de procesamiento:** Se necesita que los nodos procesen el Streaming de video y el tráfico de internet, además de los aspectos de comunicación, lo que vendría a ser una especie de *Router* con cámara incluida, por ello se necesita un hardware que sea capaz de realizar procesos que consuman grandes cantidades de recursos.
- **Documentación en la Web:** Para llevar a cabo un proyecto investigativo es fundamental tener una base de la cual partir, por ello mientras más información se tenga de proyectos similares, mejor se podrá desarrollar este. En ese sentido se ha evaluado si el Hardware tiene soporte por parte de comunidades en la Web, a las cuales se pueda hacer consultas para el desarrollo de este proyecto.
- **Capacidad de escalar:** se hace referencia a la capacidad de mejorar el Hardware que ya se tiene, expandirlo, no necesariamente añadiéndole nuevas funciones,

sino mejorando las que ya tiene, como poder mejorar el procesador, reemplazándolo por uno mejor, poder aumentar la cantidad de memoria RAM, poder mejorar la capacidad de almacenamiento. Se evalúa este aspecto porque durante el desarrollo del proyecto se presente la necesidad de mejorar el rendimiento del Hardware y no se tengan opciones que impliquen software para lograrlo. Sin embargo, con un Hardware lo suficientemente potente, este aspecto puede no ser importante, de lo contrario se tendría un problema muy difícil de resolver.

- **Funcionalidades que puede cumplir del prototipo (únicamente para el Hardware prefabricado):** Se debe evaluar cuáles de los servicios de red inalámbrica, red Mesh o captura de video puede prestar ya el Hardware.

Respecto a la cámara los requerimientos a evaluar son **compatibilidad con la placa base, facilidad de obtención de controladores** para los posibles sistemas operativos a usar, **resolución**. Los primeros dos puntos a evaluar caen por su propio peso, ya que un problema de compatibilidad podría no ser solucionable e implicaría la utilización de otro Hardware, y en lo que respecta a la resolución es de vital importancia ya que al prestarse un servicio de video vigilancia, la calidad de imagen que se debe prestar debe ser lo suficientemente nítida para poder identificar rostros, placas de vehículos, entro otros detalles visuales de relevancia que podrían interesar a la hora de prestar el servicio.

En el caso de las interfaces inalámbricas, sus requisitos van en el sentido de los modos que puedan soportar, otro aspecto a evaluar sería la compatibilidad con los posibles sistemas operativos a utilizar. El primer requisito que se necesita para estas interfaces de red inalámbricas, es que se puedan funcionar en **modo AP** el cual servirá para poder prestar el servicio de internet. El segundo requisito y no menos importante es que la interfaz de red pueda soportar el **modo Ad-Hoc** el cual se utilizara para la construcción de la red Mesh. Estos dos modos son soportados por una pequeña cantidad de interfaces de red que se encuentran en el mercado.

5.2.1.2 Elección de Software

Al hablar del software se hace referencia al sistema operativo o programa que controlara la placa base y sus componentes para el funcionamiento de los nodos, el sistema operativo debe ser de **código abierto, compatible** con la placa base y los dispositivos adicionales.

5.2.1.3 Elección de protocolos

Los protocolos a utilizar son muchos, pero se debe prestar especial atención a dos en específico, como lo son el protocolo de enrutamiento para la red Mesh y el de transmisión para el Streaming de video.

Para el protocolo de **enrutamiento en la red Mesh**, los dos principales factores a tomar en cuenta son, compatibilidad con el sistema operativo, eficiencia, uso extendido y cantidad de documentación disponible del protocolo. Que sea un protocolo de uso extendido, en el sentido de que es muy usado, suele ser sinónimo de que tiene buen

soporte, además de ser protocolos de funcionamiento comprobado, esto no asegura que sea el mejor protocolo, pero sí que es un protocolo que funciona. La cantidad de documentación disponible es muy importante porque eso permite una mayor cantidad de fuentes de información en las cuales buscar a la hora de desarrollar el prototipo. La eficiencia del protocolo es fundamental para tener una comunicación lo más óptima posible, ya que puede que la comunicación se pueda establecer con varios protocolos, pero se debe elegir el mejor para la topología.

El protocolo de Streaming de video se encuentra un poco más explotado que el de enrutamiento Mesh, por lo que la documentación y compatibilidad no presentan factores de importancia. El factor determinante para la elección de este protocolo será la eficiencia, al tratarse de Streaming en tiempo real es necesario que el protocolo para la transmisión de video sea el que permita mayor y mejor transferencia de datos.

5.2.2 Diseño

Para el diseño del prototipo se deberá tomar en cuenta siempre los servicios a ofrecer, el entorno en el que deberá funcionar, los componentes de Hardware y software seleccionados. En esta etapa del desarrollo del prototipo se deberá detallar las condiciones en las que trabajara el prototipo, como estará compuesto cada nodo, como se comunicaran los nodos y como se prestaran los servicios.

5.2.3 Obtención de resultados

En la obtención de resultados del prototipo se deberá medir una serie de factores para conocer los alcances y limitaciones del prototipo. Los factores a medir son:

- Tasa de transferencia máxima entre nodos.
- Degradación de tasas de transferencia entre saltos
- Mayor resolución de imagen de las cámaras posible de obtener
- Cantidad de nodos posibles de soportar en la red Mesh
- Cantidad de clientes posibles de soportar en la red de acceso a internet
- Cantidad de cámaras posibles de soportar y la resolución con la que podrían trabajar.

5.3 Factores de influencia

- Acceso a internet en la alcaldía, para saber con qué recursos se cuentan para prestar el servicio de Wi-Fi.
- Presupuesto de la alcaldía, para tener un parámetro de la capacidad de inversión de la alcaldía en un proyecto como el que se desea llevar a cabo, aunque esto no implique que ellos van a absorber esos costos directamente para el prototipo.
- Aspectos del entorno del lugar como topología, cantidad de redes inalámbricas activas, estructuras físicas disponibles para el montaje del prototipo, distribución del alambrado eléctrico, entre otros, para que el

prototipo cumpla con los requerimientos del entorno en el que trabajara y saber en qué se puede apoyar el prototipo para su funcionamiento.

- Alternativas de Hardware disponibles para el desarrollo del prototipo, para poder hacer uso del hardware que ofrezca una buena combinación entre buen rendimiento, bajo costo, versatilidad y facilidad de manejo, según los requerimientos de los servicios que se ofertaron.
- Alternativas de Software posibles para el Hardware elegido, para elegir la que mejor soporte pueda prestar a los servicios ofertados, cumpliendo con la premisa del menor costo.
- Rendimiento del prototipo en aspectos técnicos como tasas de transferencia, calidad de imagen por parte de las cámaras, entre otros, para poder hacer mejores elecciones en configuraciones del prototipo.
- Costo del prototipo, para saber si es viable o no la adquisición de este tipo de elementos.

5.4 Presentación de resultados

Luego de llevar a cabo la investigación se obtendrá como resultado la viabilidad del proyecto en las condiciones de para las que fue desarrollado, quedando plasmado en un documento final que contenga todos los aspectos relacionados al desarrollo de la investigación además del prototipo funcional que se obtendrá físicamente y podrá ser observado funcionando si el resultado de la investigación fue favorable.

El documento contendrá el desarrollo de los instrumentos que se necesitaron para la realización de la investigación, el lineamiento para la replicación del instrumento

tecnológico, la evaluación de los resultados obtenidos por los instrumentos y las factibilidades del proyecto en base a la evaluación de los resultados obtenidos. Además de los aspectos ambientales en los que se llevó a cabo la investigación. Sin embargo los aspectos principales a tomar en cuenta en el resultado son la obtención de **factibilidades, el prototipo funcional y los lineamientos para su desarrollo.**

6 Análisis

6.1 Análisis de datos

En esta sección del documento se analizarán los resultados obtenidos a través de los métodos de recolección de datos que se planificaron en la metodología de la investigación.

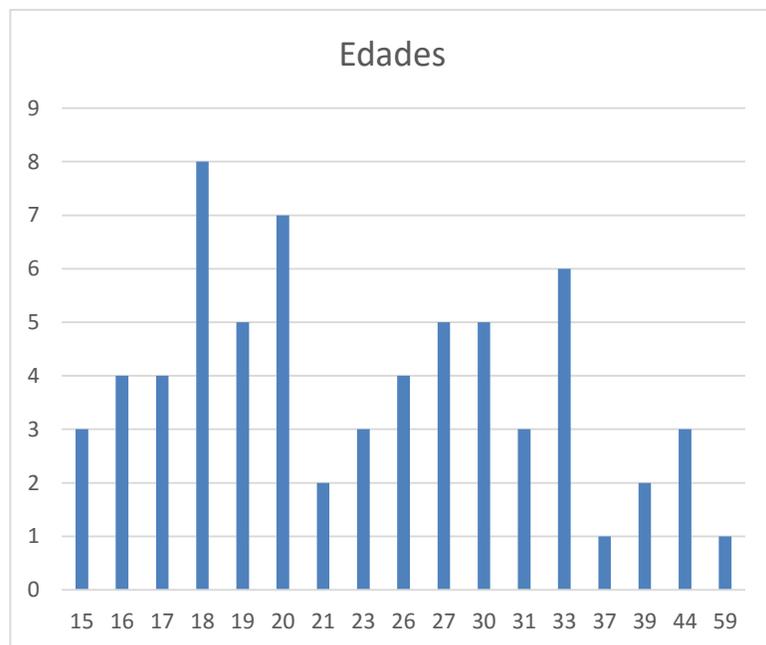
6.1.1 Investigación social

En este apartado se analizarán los datos obtenidos a través de los métodos cuantitativos como cualitativos de la investigación social que se contempla en el proyecto.

6.1.1.1 Encuesta

✓ Edad

Edad	Cantidad
15	3
16	4
17	4
18	8
19	5
20	7
21	2
23	3
26	4
27	5
30	5
31	3
33	6
37	1
39	2

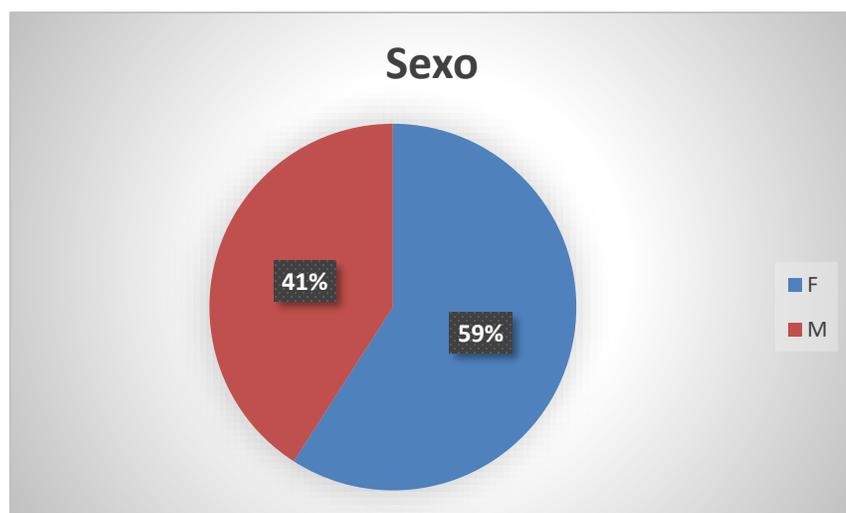


44	3
59	1

Como se puede observar en el grafico se solicitó llenar la encuesta a personas mayores de 15, sin distinción de máxima edad. Además, se puede observar que la mayor cantidad de personas encuestadas se encuentran entre el rango de los 16 hasta los 33 años de edad.

✓ Sexo

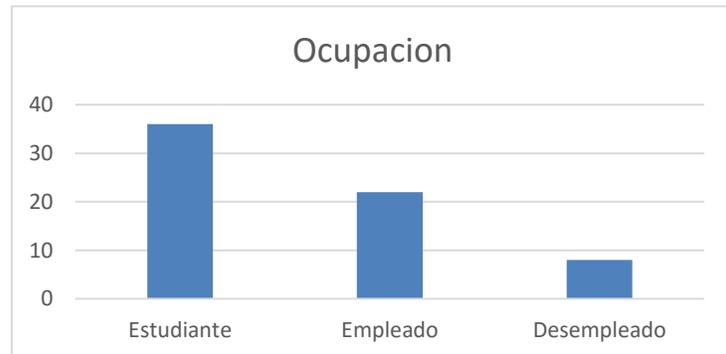
Sexo	Cantidad
F	39
M	27



Como los datos lo reflejan no se tomó discriminación de sexo para pasar la encuesta, como muestran los datos la encuesta se pasó casi a partes iguales entre sexo masculina y femenino.

✓ Ocupación

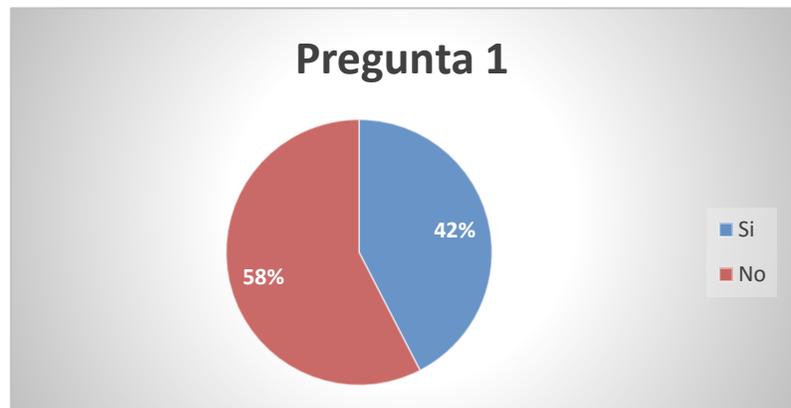
Ocupación	Cantidad
Estudiante	36
Empleado	22
Desempleado	8



Entre los datos obtenidos a través de esta pregunta se puede observar que en su mayoría los habitantes encuestados se encuentran actualmente estudiando, como segunda mayor frecuencia se tiene a habitantes con empleo y por ultimo a habitantes desempleados.

✓ ¿Sabe lo que es un sistema de videovigilancia?

Pregunta 1	Cantidad
Si	28
No	38

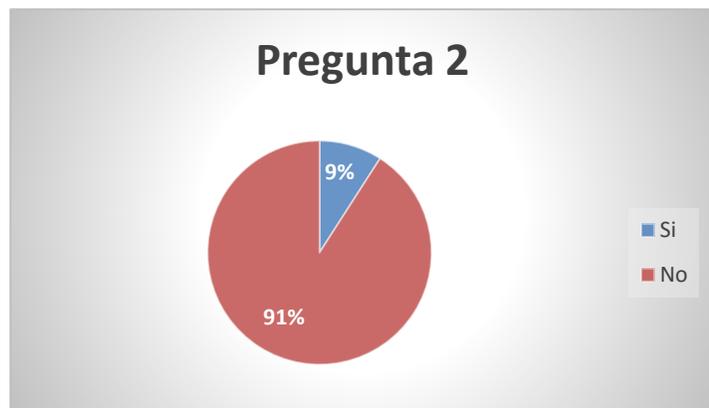


Esta pregunta lanzo un resultado negativo en cuanto al número de personas que conocen el término de sistema de videovigilancia. Se dice que es un resultado negativo,

porque la mayoría de los habitantes encuestados no conocen el término, 57% por ciento de los habitantes respondieron No y 53% respondieron Si.

- ✓ **¿Alguna vez ha oído hablar de un sistema de videovigilancia para su comunidad? (videovigilancia pública)**

Pregunta 2	Cantidad
Si	6
No	60



Estos resultados muestran que la población no conoce ningún antecedente ni sabe que un proyecto de esta índole se esté llevando a cabo en el municipio, 91% respondieron No y solamente un 9% respondieron Si.

- ✓ **¿Conoce los costos de un sistema de videovigilancia?**

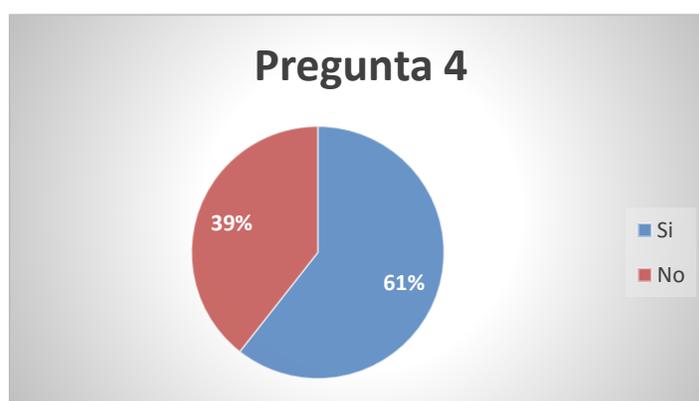
Pregunta 3	Cantidad
Si	2
No	64



Los resultados que lanzo esta pregunta son casi unánimes, apenas un 3% de los encuestados conocen el costo que tienen los sistemas de videovigilancia.

✓ **¿Cree usted necesario un sistema de videovigilancia en su comunidad?**

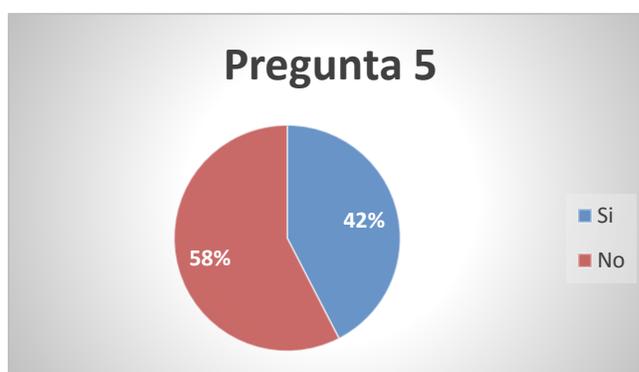
Pregunta 4	Cantidad
Si	40
No	26



La mayoría de los habitantes encuestados considera necesario el desarrollo de un proyecto para la creación de un sistema de videovigilancia, 61% de los habitantes encuestados respondieron Si y un 39% respondieron No.

✓ **¿Diría que, San José las Flores es una ciudad moderna?**

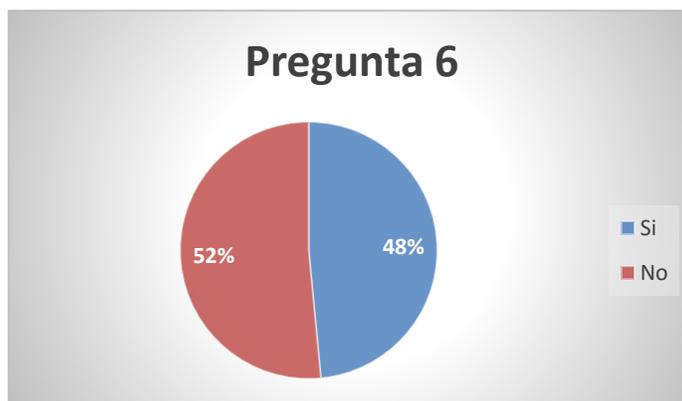
Pregunta 5	Cantidad
Si	28
No	38



Los datos obtenidos por esta pregunta muestran que en su mayoría los habitantes encuestados no consideran a San José Las Flores un municipio moderno, 57% de los habitantes encuestados respondieron No y un 43% respondieron No.

- ✓ **¿Considera que la modernización de su comunidad es importante? con modernización nos referimos al hecho de utilizar tecnologías emergentes o nuevas que puedan ayudar a su comunidad.**

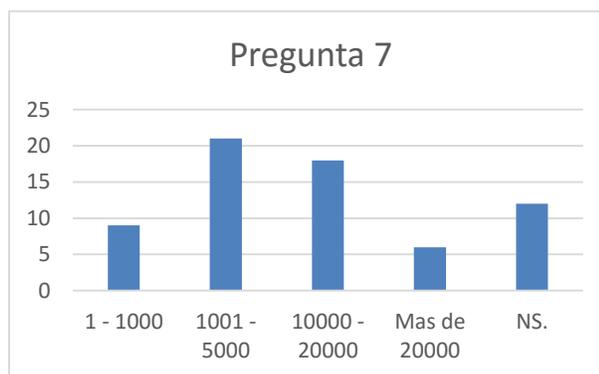
Pregunta 6	Cantidad
Si	32
No	34



Esta pregunta lanzo resultados muy divididos con respecto a la necesidad de modernizar el municipio en aspectos de tecnologías emergentes que puedan ayudar a la población, 52% de los habitantes hicieron que predominara el No en los resultados y un 48% respondieron Si.

- ✓ **¿Cuánto es lo máximo que debe invertir su gobierno local (alcaldía) en términos monetarios (\$) en la seguridad pública de su municipio?**

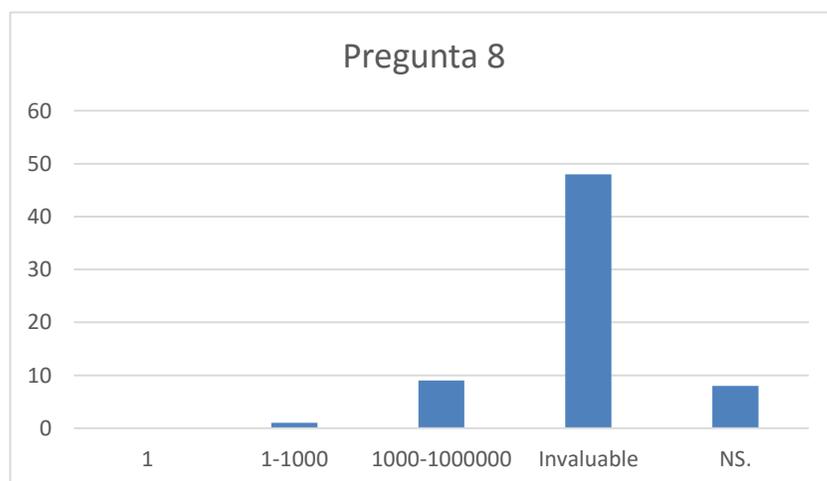
Pregunta 7	Cantidad
1 - 1000	9
1001 - 5000	21
5000 - 20000	18
Más de 20000	6
NS.	12



Los resultados de esta pregunta lanzan como rango predominante entre los \$1000 y los \$20000, que debe invertir la alcaldía en proyectos de seguridad.

- ✓ **¿Cuánto vale (\$) su seguridad?**

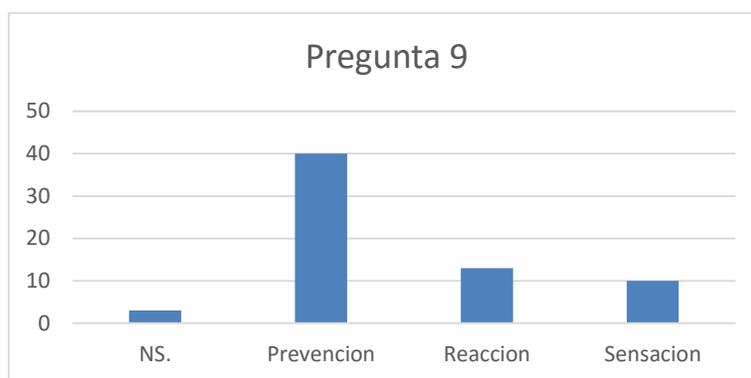
Pregunta 8	Cantidad
1	0
1-1000	1
1000-1000000	9
Invaluable	48
NS.	8



Como era de esperar los datos obtenidos en esta pregunta muestran un 72% de los habitantes encuestados considera invaluable la seguridad personal.

✓ **¿Cómo cree usted, que un sistema de videovigilancia podría ayudar a su comunidad?**

Pregunta 9	Cantidad
NS.	3
Prevención	40
Reacción	13
Sensación	10



Los resultados obtenidos por esta pregunta reflejan que el 61% de los habitantes encuestados consideran que un sistema de videovigilancia ayudaría a la prevención de hechos vandálicos dentro del municipio.

✓ **¿Sabe lo que es Wi-Fi?**

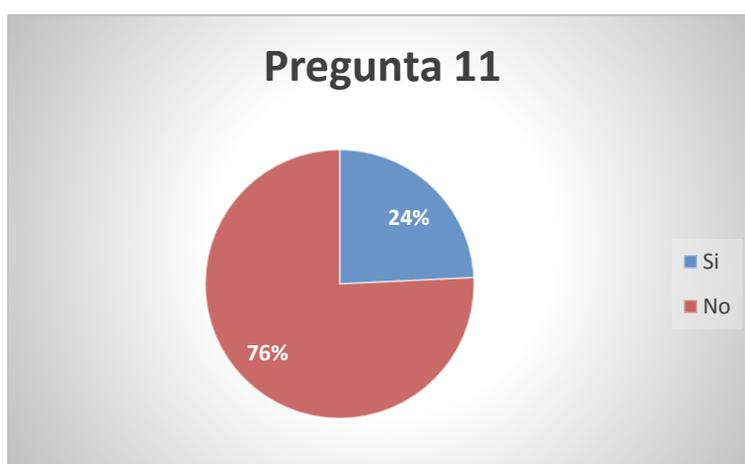
Pregunta 10	Cantidad
No	16
Si	50



Los datos recabados por esta pregunta muestran que el 76% de los habitantes encuestados conocen lo que es *Wi-Fi*.

✓ **¿Posee una conexión inalámbrica (*Wi-Fi*) a internet en su hogar?**

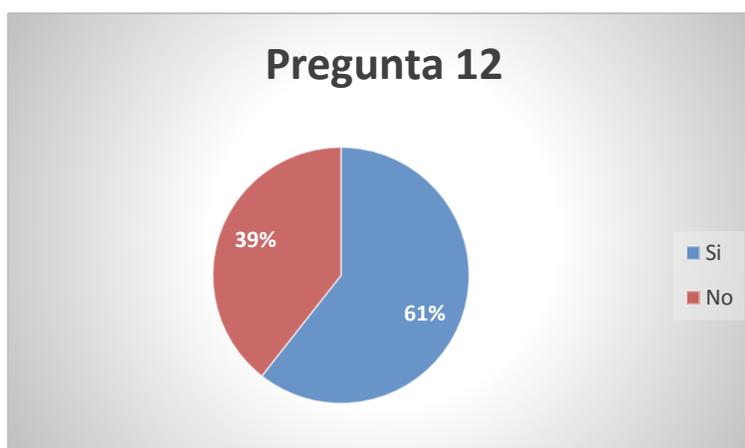
Pregunta 11	Cantidad
No	50
Si	16



Como muestra el grafico apenas un 24% de los encuestados poseen una conexión inalámbrica a internet en sus hogares.

✓ **¿En la actualidad, es necesario el internet para la educación?**

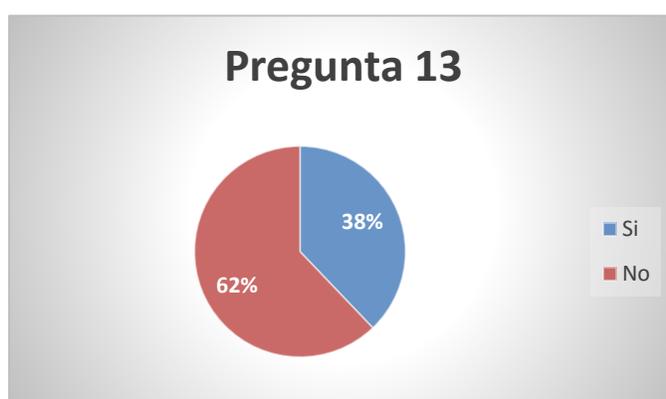
Pregunta 12	Cantidad
No	26
Si	40



Un 61% de los habitantes encuestados consideran que el internet es necesario para la educación y aprendizaje.

- ✓ **¿Es económicamente capaz de adquirir una conexión a internet personal (para uso personal, instalada en su casa alámbrica o inalámbrica)?**

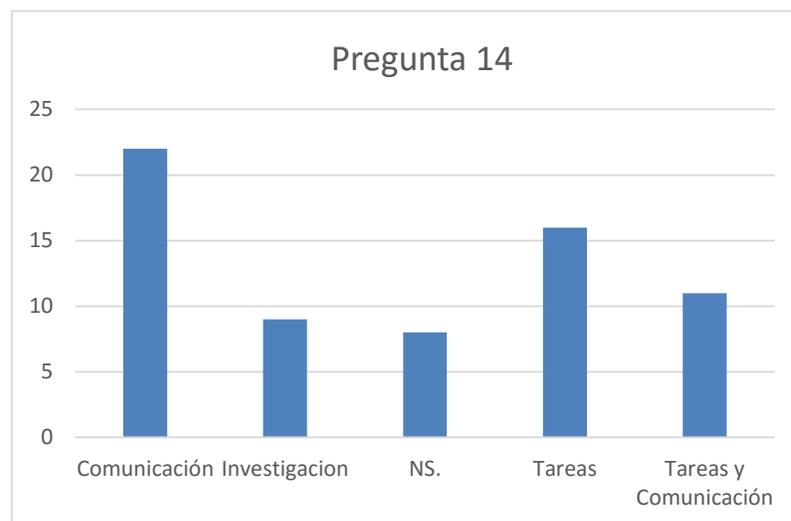
Pregunta 13	Cantidad
No	41
Si	25



Como se puede observar en el gráfico solo un 38% de los habitantes encuestados pueden costear un servicio de internet en sus hogares, mientras que el 62% restante no se puede costear este servicio.

- ✓ **¿De qué manera le ayudaría tener acceso gratuito a internet de forma inalámbrica?**

Pregunta 14	Cantidad
Comunicación	22
Investigación	9
NS.	8
Tareas	16
Tareas y Comunicación	11



Los datos muestran que el uso que los habitantes encuestados le darían al servicio de internet inalámbrico es muy variado, estos usos van desde actividades de ocio como la comunicación, así como también a uso didáctico el cual involucra la realización de tareas.

- ✓ **¿Necesita internet inalámbrico en lugares públicos (un parque, un comedor público)?**

Pregunta 15	Cantidad
No	25
Si	41



Los datos obtenidos de la última pregunta de la encuesta muestran como un 62% de los habitantes encuestados necesitan accesos a internet de forma inalámbrica en lugares públicos del municipio, lo que refleja una evidente necesidad del servicio en cuestión.

6.1.1.2 Entrevista

Se llevó a cabo una entrevista a Darwin David Serrano Guardado, administrador de proyecto de la alcaldía de San José las Flores, luego de hacer el análisis al texto de la transcripción de la entrevista, se resume en el cuadro que se muestra a continuación, la información de recabada durante la entrevista de mayor interés.

Tabla 6-1 Resumen de la información obtenida en la entrevista.

Aspecto	Resultado(✓ si, ✗ no)
Cuenta la alcaldía con algún tipo de servicio de videovigilancia	✗
Despierta interés para la alcaldía desarrollar un proyecto de implementación de videovigilancia	✓
Ofrece la alcaldía algún tipo de servicio de acceso a internet para los habitantes del municipio	✓
Despierta interés para la alcaldía desarrollar un proyecto para mejorar el servicio de internet a la comunidad	✓
Cuenta la alcaldía actualmente con los fondos para apoyar el desarrollo del proyecto	✗
Podría llegar a contar con los fondos para implementar el proyecto en el futuro	✓
Cuenta la alcaldía con una conexión a internet que pueda ser compartida con los habitantes del municipio	✓

La entrevista se centró en los aspectos referentes a los servicios que prestara el sistema, si se cuenta con ellos, si se desea contar con ellos y si se podría financiar un proyecto de este tipo.

De la entrevista se obtuvo que la alcaldía está interesada en desarrollar el proyecto, aunque actualmente no cuenta con los fondos, si podría llegar a contar con ellos. De los servicios que se espera que preste el sistema, ya se cuenta con un servicio de acceso a internet para los habitantes, pero es deficiente.

6.2 Decisiones sobre prototipo

En esta sección del documento se analizarán los componentes tecnológicos que involucra el prototipo que pretende desarrollar este proyecto, como primer punto se analizaran los dispositivos que pueden ser seleccionados para la elaboración de cada nodo del prototipo. Posteriormente en base al dispositivo seleccionado en el análisis anterior, se realizará un nuevo análisis, pero con respecto a los sistemas operativos que este dispositivo seleccionado pueda soportar. Y por último se realizará un análisis de los protocolos que se usaran para brindar los servicios de *Wi-Fi* y videovigilancia.

6.2.1 Elección del Hardware

Para poder desarrollar el prototipo como primer punto se necesitó establecer los requerimientos de Hardware necesarios en base a los servicios que el prototipo pretende brindar. Como ya se mencionó en el párrafo anterior los servicios a prestar son

videovigilancia y *Wi-Fi*, además que se debe establecer una red de comunicación tipo Mesh. En base a estos requerimientos se necesitan los siguientes componentes de hardware por cada nodo:

- 2 redes inalámbrica, se necesita una para el *Wi-Fi* y otra para la red Mesh.
- Enrutamiento de paquetes de red.
- Captura de video.
- Soporte a la intemperie.

6.2.1.1 Elección del dispositivo base

La elección del dispositivo base se divide en dos, primero se evaluarán placas base y luego posibles dispositivos prefabricados que puedan cumplir con todas o la mayoría de características del prototipo.

6.2.1.1.1 Placa base

Para la placa base eligieron como base los siguientes dispositivos el Arduino UNO, Odroid C1 y Raspberry Pi 2 B. En el caso del Arduino UNO y de la Raspberry PI 2 B, se eligieron por ser los que predominan en las preferencias de los desarrolladores de soluciones a la medida que implican Hardware de código en el entorno local.

Para el caso del Odroid C1 se eligió porque tiene una capacidad parecida a la de la Raspberry PI 2 B, aunque sea menos conocida. Todas las opciones permiten un alto grado de personalización de soluciones.

En la siguiente tabla se encuentran las especificaciones técnicas de la Raspberry Pi 2 B, Arduino Uno y Odroid C1.

Tabla 6-2 Comparativa entre Raspberry, Arduino y Odroid C1

Aspecto	Raspberry	Arduino	Odroid C1
Soporte de sistema operativo	✓	✗	✓
Soporte a dispositivos adicionales	✓	✓	✓
Puertos USB	✓	✗	✓
Capacidad de procesamiento	Alta	Baja	Alta
Documentación en la web	Alta	Alta	Media
Diseño original	Educativo	Educativo	Educativo
Capacidad de modificar el hardware	✗	✗	✗
CPU	4 núcleos a 900MHz	1 núcleo a 16MHz	4 núcleos a 1.5 GHz
RAM	1 GB	0.002 MB	1 GB
Precio*	\$50.00	\$60.00	\$50.00

*Precio promedio según Amazon consultado 15 de agosto 2015.

Luego de la investigación sobre placas base se pudo determinar de cada Hardware lo siguiente:

Tabla 6-3 Características de Hardware de los dispositivos Raspberry, Arduino y Odroid

Raspberry Pi 2B



*Ilustración 6-1 Placa
Raspberry Pi 2B*

Es una computadora de placa reducida que puede soportar los servicios que requiere el proyecto, ya que según las especificaciones obtenidas puede adicionarse tanto el hardware como el Software necesario. Un posible inconveniente podría ser la potencia en el procesamiento, pero también dependería de la optimización del software. Tiene buenas prestaciones de procesamiento y ofrece flexibilidad en cuanto al Hardware y el Software que puede soportar. Un aspecto interesante es que dentro del Hardware adicional que soporta puede ser por conexión USB, por lo que se trata de Hardware bastante comercial del que se puede obtener con relativa facilidad los controladores y software necesario para operarlo. El hecho de que soporte diversos sistemas operativos Linux ofrece mucha versatilidad, porque se puede elegir dentro de las

distribuciones soportadas la que mejores prestaciones ofrezca para el soporte de los servicios.

Arduino UNO



*Ilustración 6-2 Placa
Arduino UNO*

Es un microcontrolador al que se le puede agregar hardware específico para Arduino, esto es un inconveniente porque no se puede contar con Hardware comercial para adicionárselo, sin embargo, el hardware que se le puede adicionar si tiene sus controladores para Arduino. En lo que respecta a procesamiento es inviable ya que tiene características muy limitadas. No puede funcionar como una computadora y solo puede realizar un proceso a la vez, y el proyecto requiere que los nodos ejecuten más de un proceso a la vez, ya que los servicios deben trabajar simultáneamente.

Odroid C1



*Ilustración 6-3
Odroid C1*

Es una computadora de placa reducida que puede soportar los servicios que el proyecto requiere, ya que según las especificaciones obtenidas puede incorporar tanto el software como el hardware requerido. La mayor de sus desventajas es el poco soporte que cuenta por la comunidad web. Su mayor virtud es que cuenta con las prestaciones más altas de hardware de las placas base analizadas. Otro

punto favorable es que dentro del Hardware adicional que soporta puede ser por conexión USB, con lo cual se trataría de Hardware altamente comercial. Además, esta placa base soporta diversos sistemas operativos Linux los cuales ofrecen mucha versatilidad y se podría elegir la mejor opción para desarrollar el prototipo.

Análisis: En base a la evaluación individual de cada uno de los dispositivos antes descrito se pudo determinar que la **Raspberry PI 2 B y Odroid C1** son los Hardware que mejor se adaptan a las necesidades que el proyecto requiere. En la *tabla 6-1* se puede determinar que el mejor procesador de los tres dispositivos es el del Odroid C1, en segundo lugar, se encuentra el procesador de la *Raspberry Pi 2 B* y por último se tiene el procesador del Arduino UNO. En lo que respecta a la memoria RAM la Raspberry Pi 2 B y Odroid C1 cuentan con la misma cantidad y además poseen 500,000,000 veces más memoria RAM que el Arduino UNO. Otra característica muy importante es si las placas poseen puertos USB entre sus prestaciones, la Raspberry PI 2 B y el Odroid C1 cuentan con 4 puertos de este tipo, mientras que el Arduino Uno no posee ninguno. En cuanto a poseer un puerto específico para la adición de cámara de video solo la Raspberry Pi 2 B lo posee, mientras que el Odroid C1 y el Arduino Uno no cuentan con un puerto de este tipo. Otro punto a tener en cuenta y además muy importante, es la documentación y soporte que estas placas poseen por parte de la comunidad web, este punto favorece

ampliamente a la Raspberry Pi 2 B, debido a la popularidad de esta placa en el mercado internacional.

La razón por la cual se eligió la **Raspberry Pi 2 B** como la mejor opción es debido a la basta documentación encontrada con respecto a proyectos similares, además de la experiencia que el equipo de trabajo posee con esta placa en proyectos educativos. Por ultimo cabe mencionar que esta placa soporta una amplia gama de software, con software nos referimos a sistemas operativos de distribuciones Open Source como distribuciones de paga, así como también nos referimos a los distintos programas, protocolos y configuraciones de software que permiten instalar los diferentes sistemas operativos.

La elección de esta placa base conlleva la elección de dos componentes de Hardware adicionales no planificados en la metodología, debido, a que la elección genera la necesidad, una tarjeta SD para el almacenamiento y una fuente de alimentación eléctrica, estos componentes se evaluarán más adelante luego de los componentes de Hardware previstos en la metodología.

6.2.1.1.2 Dispositivos prefabricados

Para los dispositivos prefabricados se eligieron en base a la preferencia por ser los dispositivos que predominan para construir una red Mesh, entre ellos se encuentran Mesh Potato, DLink DIR 310 y Open Mesh OM2P. En el caso de Mesh Potato se eligió por la utilización de los dispositivos en el desarrollo de proyectos similares los cuales fueron

citados en el Capítulo de Antecedentes, sección 2.2.2 Redes Mesh pag.9 del presente documento.

Para los dispositivos prefabricados se eligieron Mesh Potato, Open-Mesh OM2P y D-Link DIR-320:

Tabla 6-4 Comparativa entre D-Link DIR320, Open-Mesh OM2P y Mesh Potato

Aspecto	D-Link DIR-320	Open-Mesh OM2P	Mesh Potato
Soporte de sistema operativo	✓	✓	✓
Soporte a dispositivos adicionales	✗	✗	✗
Puertos USB	✓	✗	✗
Capacidad de procesamiento	Baja	Baja	Baja.
Documentación en la web	Baja	Baja	Baja
Diseño original	✓	✓	✓
Capacidad de modificar el hardware	✗	✗	✗
CPU	RaLink RT5350 SoC	400 MHz QCA9331 MIPS 24K	MIPS 4K de 180MHz
RAM	32Mbytes	64 MB	16 MB
Precio*	\$50.00	\$60.00	\$35.00
Funcionalidades que puede cumplir del prototipo	Wi-Fi.	Red Mesh y Wi-Fi.	Red Mesh y Wi-Fi.

*Precio promedio según Amazon consultado 22 de enero 2016.

Tabla 6-5 Características de hardware de D-Link DIR320, Open-Mesh OM2P y Mesh Potato

Dlink DIR 320



Ilustración 6-4

Router Dlink DIR 320

Es una computadora de placa reducida que trabaja como un *Router*, trabaja con 2 redes inalámbricas, la Mesh que utiliza para la interconexión de los nodos y la red *Wi-Fi* para brindar conexión inalámbrica a los clientes. Estos son exactamente 2 de los servicios que debe prestar el prototipo, sin embargo, no tiene posibilidades de soportar una cámara instalada directamente en el nodo. Podría funcionar poniendo una cámara IP conectada al puerto Ethernet que esta posee. Pero el nodo directamente ya no sería una sola unidad que presta todos los servicios y los costos se incrementarían considerablemente, además las prestaciones de procesamiento no son muy buenas para poder procesar el Streaming de video en los nodos.

Mesh Potato



Ilustración 6-5

Dispositivo Mesh Potato

Es una computadora de placa reducida que trabaja como un *Router*, trabaja con 2 rede inalámbricas, la Mesh que utiliza para la interconexión de los nodos y la red *Wi-Fi* para brindar conexión inalámbrica a los clientes. Estos son exactamente 2 de los servicios que debe prestar el prototipo, sin embargo, no tiene posibilidades de soportar una cámara instalada directamente en el nodo. Podría funcionar poniendo

una cámara IP conectada al puerto Ethernet que esta posee. Pero el nodo directamente ya no sería una sola unidad que presta todos los servicios y los costos se incrementarían considerablemente, además las prestaciones de procesamiento no son muy buenas para poder procesar el Streaming de video en los nodos.

Open Mesh OM2P

Ilustración 6-6

Dispositivo Open Mesh OM2P

Es un dispositivo para la ampliación de redes inalámbricas que retransmite redes estructuradas a través de una red Mesh entre los repetidores Open Mesh. Se trata de un dispositivo para fines comerciales que se maneja desde un ambiente Web, el uso de estos dispositivos permitiría el soporte de las dos redes de comunicación que requiere el proyecto, pero no permite la transmisión de video porque no tiene forma de añadirle más componentes al Hardware original, a menos que se conecte una cámara IP. El dispositivo tiene un precio relativamente alto respecto a los demás dispositivos prefabricados evaluados.

Análisis: En base a las características de los dispositivos se pudo determinar que la funcionalidad total del prototipo no se puede obtener con los dispositivos investigados y que directamente no se pueden adicionar dispositivos al Hardware prefabricado para adicionar la funcionalidad de forma que todo trabaje directamente en el nodo. Se puede

lograr adicionar dispositivos como cámaras IP que transmitan a través del nodo, pero el planteamiento es hacer nodos que cumplan directamente las funciones de videovigilancia, red Mesh y acceso inalámbrico a internet y con los dispositivos investigados no se pueden realizar todas estas funciones como nodos únicos.

De los dispositivos prefabricados se obtuvo que el mejor para el proyecto es el **MeshPotato** porque cumple con dos de las funciones del prototipo al igual que el OpenMesh, pero a un precio menor, el Dlink se descartó porque solo soporta una red inalámbrica a la vez, con lo que no se pueden dar directamente los dos servicios de comunicación a la vez.

6.2.1.1.3 Especificaciones técnicas del dispositivo elegido

Como se menciona en el análisis de los dispositivos prefabricados, ninguno está preparado para conformar el nodo ofertado en el proyecto, por lo que el mejor Hardware para el prototipo es la placa base Raspberry PI 2 B, apoyándose en el análisis de las placas bases.

Ya habiendo elegido la **Raspberry PI 2 B** como el dispositivo que se usara para el desarrollo de este proyecto se listan las especificaciones de hardware con las cuales cuenta esta placa de microcomputadoras, dichas prestaciones estarán disponibles para poder utilizarlas si son necesarias para el desarrollo del prototipo:

- Un procesador de 4 núcleos de 900MHz ARM Cortex-A7
- Memoria RAM de 1GB
- 4 puertos USB

- 1 conjunto de pines GPIO
- 1 puerto HDMI
- 1 puerto Ethernet 10/100
- 1 puerto de sonido de 3.5mm
- 1 interfaz de cámara
- 1 interfaz para pantalla
- 1 puerto para memoria micro SD
- Un procesador de video VideoCore IV 3D

Con estas características se puede soportar la ejecución de un sistema operativo Linux y agregar el Hardware para dar los servicios de captura de video y transmisión de datos por las 2 redes inalámbricas.

6.2.1.2 Elección de la cámara

Para la cámara se pensó en la cámara que se ha desarrollado específicamente para la **Raspberry Pi**, porque tiene una resolución de 1080p además que dicha cámara se desarrolló para ser utilizada en este hardware en particular, es por este motivo que la **Raspberry** cuenta con puerto especial en el cual se conecta esta cámara.

Esta cámara soporta imágenes de video de 5 megapíxeles y una resolución de 1080p30 para fotografías. Esta cámara se puede encontrar en 2 tipos diferentes, la primera es una cámara básica con las especificaciones antes mencionadas y otra versión llamada NoIR la cual tiene una función especial, esta función permite hacer tomas

nocturnas. Pensando en el tipo de servicio que se prestara se optó por la segunda opción. Con esta elección ya se tiene el Hardware que brindara el streaming¹ de video.

6.2.1.3 Elección de las interfaces inalámbricas

Como ya menciono anteriormente cada nodo requiere 2 interfaces de red inalámbricas y observando las características que posee la **Raspberry Pi** seleccionada, esta cuenta con 4 puertos USB a través de los cuales se pueden conectar directamente las interfaces de red. Como cualquier dispositivo que se necesita agregar a esta placa, estas interfaces de red deben de cumplir con una serie de requisitos para poder funcionar de forma óptima.

El primer requisito que se necesita para estas interfaces de red inalámbricas es que se puedan poner en **modo AP** el cual servirá para poder prestar el servicio de internet. El segundo requisito y no menos importante es que la interfaz de red pueda soportar el **modo Ad-Hoc** el cual se utilizara para la construcción de la red Mesh. Estos dos modos son soportados por una pequeña cantidad de interfaces de red que se encuentran en el mercado, es por ello que se tomó de apoyo la página web wikidevi.com, la cual muestra el listado de Chipsets y los modos que estos soportan, a partir de esta información buscar interfaces de red que cuenten con estos chipsets.

¹ Streaming: es la distribución digital de multimedia a través de una red de computadoras, de manera que el usuario consume el producto (generalmente archivo de vídeo o audio) en paralelo mientras se descarga. (**Wikipedia streaming, 2016**)

Se buscó las interfaces de red inalámbricas que fueran accesibles para nosotros en el mercado local o internacional, se encontró una amplia gama de interfaces de red y de muy diversas marcas de comerciantes, pero lo realmente importante era encontrar interfaces de red que contaran con el Chipset indicado.

Se buscó una gama de dispositivos en páginas de venta de artículos en línea, como lo son amazon.com y ebay.com, en tiendas del área metropolitana local además del Hardware a disposición de cada uno de los miembros del equipo de trabajo. Las interfaces que se escogieron fueron las siguientes, LB-Link BL-WN155A, Netis WF2120, D-Link DWA-123, D-Link DWA-125. Todas estas interfaces cuentan con el protocolo 802.11n la razón por la cual se eligió este protocolo y no el 802.11ac se deben, a la diferencia de costos monetarios entre las interfaces que poseen 802.11n y 802.11ac ya que estas últimas triplican y en algunos quintuplican el valor de una interfaz 802.11n. A pesar de ello se recomienda el uso de interfaces 802.11ac ya que estas pueden establecer un enlace de red con mayor distancia de separación entre los nodos, así como también brindan mayor velocidad de transferencia de datos.

A continuación, se detalla porque se escogió cada Hardware:

- LB-Link BL-WN155A, según la oferta en Amazon.com (se revisó el 20 de agosto de 2015), el dispositivo viene preparado para trabajar con modo ad-hoc además tiene soporte para Linux. Su chipset es el Ralink RT5370 o RT5372, no está claro cuál es que trae específicamente según la página del fabricante, pero según la web de wikidevi.com ambos chipsets soportan el modo AP y el modo Ad-Hoc. Además, soporta los protocolos 802.11b/g/n, permitiendo una tasa de

transferencia de hasta 150Mbps. Tiene una antena de 5dBi omnidireccional. Posee una antena externa a diferencia de las demás interfaces investigadas. (**Wiki RT5370, 2015**)

- Netis WF2120, fue buscado en Amazon.com pero también se encontró en tiendas locales, su chipset es el RTL8188CUS, pero su driver en Linux puede ser el RTL8192CU, ambos soportan el modo AP, pero el modo ad-hoc lo tiene como incógnita según la página wikidevi.com, ósea que podría o no soportarlo, como punto positivo soporta el modo AP para dar el servicio de. Una razón importante para adquirir este Hardware es que utiliza un Chipset muy común en nuestro medio, por lo que, en caso de algún fallo, podría ser reemplazado por otro Hardware con facilidad, ya que sería fácil de encontrar un sustituto con el mismo Chipset. Soporta los protocolos 802.11b/g/n, permite una tasa de transferencia de hasta 150Mbps. (**Wiki RTL8188CUS, 2015**)
- D-Link DWA-123 D1, fue buscado en las tiendas locales, utiliza un Chipset RTL8188eu, el cual soporta modo AP, en la investigación realizada sobre este chipset no se pudo determinar si soporta el modo Ad-Hoc. A pesar de esto no se descartó, por lo que muy probablemente lo soportara, además de ser un Hardware muy común en el mercado local, por lo que se podía encontrar un sustituto con facilidad en caso de daño. Soporta los protocolos 802.11b/g/n, permite una tasa de transferencia de hasta 150Mbps. (**Wiki RTL8188EU, 2015**)
- D-Link DWA-125 A2, este Hardware utiliza un Chipset Ralink RT3070 soporta tanto el modo AP como el modo Ad-Hoc, por lo que es ideal para desarrollar el

proyecto, el inconveniente con este Hardware es que es difícil de encontrar tanto en el mercado local como en internet, el que se ha obtenido es por acceso de uno de los miembros del equipo. Soporta los protocolos 802.11b/g/n, permite una tasa de transferencia de hasta 150Mbps. **(Wiki RT3070, 2015)**

Se adquirirán todos los Hardware antes mencionados, porque se necesitará hacer pruebas y puede que no todos funcionen con los servicios de AP y modo Ad-Hoc el cual se utilizará en la creación de la red Mesh que necesita el proyecto. Solo se tiene certeza de que el Hardware D-Link DWA-125 A2 soporta todos los servicios que se necesitan, sin embargo, no se ha podido obtener un proveedor para adquirir el Hardware, por lo que solo se cuenta con las 3 que ya tiene el equipo y se necesitan más interfaces para llevar a cabo el proyecto. En el desarrollo del proyecto se irán obteniendo los resultados de cada Hardware y se trabajara con los que mejor funcionen.

6.2.1.4 Elección de memoria SD

Para el almacenamiento del sistema operativo que maneja la placa base se necesita una memoria SD, en el mercado se encuentran muchas de varios tipos, pero según las especificaciones de la Raspberry Pi 2 B, soporta tarjetas de memoria micro SD desde los 4GB categoría 4 hasta categoría 10, siendo la categoría lo que determina la velocidad de escritura en MB/s que puede alcanzar la memoria, aunque esto no implique que en general funcionara mejor una memoria categoría 10 sobre una categoría 4. (www.raspberrypi.org, 2016)

Siendo estas las condiciones se tomaron en cuenta las memorias SD más vendidas en amazon.com cuando se hizo la búsqueda de la placa base y luego se consultó en el mercado local, para determinar la facilidad de acceso a estas, para luego poder elegir la de mejor desempeño y que fuera fácil de encontrar.

Tabla 6-6 Comparativa de memorias SD según amazon.com

Marca	Capacidad de almacenamiento (GBs)	Categoría	Facilidad de acceso en el mercado local	Precio USD	Evaluación
San Disk	8	10	No	\$6.75	Excelente
Kingston	8	4	Si	\$3.99	Excelente
PNY	16	10	No	\$6.99	Buena
Trascend	16	10	No	\$5.99	Buena

Teniendo en cuenta el rendimiento y el precio se determinó que la mejor opción de memoria es la **San Disk** porque tiene la capacidad necesaria para soportar el sistema operativo, tiene una buena evaluación en las reseñas de los usuarios y la velocidad de escritura más alta posible. El tamaño no es factor determinante porque la capacidad mínima evaluada sobrepasa por mucho lo que se necesita en el prototipo porque no se necesita mucho almacenamiento en los nodos.

A pesar de haber hecho una elección sobre el almacenamiento, solo se toma como una referencia y no es determinante usar este Hardware en específico porque el prototipo

puede funcionar con otro tipo de tarjeta siempre y cuando cumpla con las especificaciones impuestas por la Raspberry Pi 2 B.

6.2.1.5 Elección de Fuente de alimentación

Se necesita determinar la fuente de alimentación que utilizara la placa base con todos los dispositivos necesarios instalados, se determinó que se podría llegar el siguiente amperaje en el caso de mayor necesidad de conexión de dispositivos. Los datos parten de las especificaciones del sitio de Raspberry Pi. (www.raspberrypi.org, 2016)

Tabla 6-7 Listado de componentes de Hardware del nodo y su consumo eléctrico

Componente	Amperaje a consumir (mA)
Placa base	500
Cámara	250
Interfaz de red (2)	100-500

Según los componentes posibles el máximo amperaje necesitado puede llegar a ser de 1750mA, por ello se necesitará utilizar una fuente de alimentación de 2000mA porque pueden permitir un margen de error si se necesitara más corriente. El voltaje no se ha tomado en cuenta porque la placa base solo trabaja con 5V por lo que la fuente debe ser de 5V y 2000mA.

Según los foros de Raspberry Pi si la alimentación no es la necesaria, la placa base no lograra funcionar adecuadamente o simplemente no trabajara (www.raspberrypi.org, 2012). En cuanto a marcas y modelos no se ha ahondado porque dependerá de lo que se encuentre en el mercado local.

6.2.2 Elección del sistema operativo

Se necesita definir el sistema operativo con el que se manejara el Hardware adquirido, por defecto la Raspberry Pi 2 B soporta los siguientes sistemas operativos según la página de Raspberry:

Tabla 6-7 Comparativa de Sistemas operativos disponibles

Sistema Operativo	Reseña
Raspbian	Es el sistema operativo por excelencia para la Raspberry Pi 2 B, es una distribución de Linux derivada de Debian. En la web se encuentra mucha información de proyectos realizados con la Raspberry Pi y este sistema operativo.
Ubuntu MATE	Es una distribución de Ubuntu para equipos de poca capacidad, es una distribución bastante amigable con el usuario. Existe una versión adaptada para la Raspberry Pi
SNAPPY Ubuntu CORE	Es una distribución de Ubuntu pensada en desarrolladores.
Windows 10 OIT Core	Distribución de Windows para ordenadores de placa

	reducida.
OSMC	Sistema operativo Linux, Desarrollado para montar un centro de medios con la Raspberry Pi y algunos otros Hardware.
OPENELEC	Sistema operativo Linux, Desarrollado para montar un centro de entretenimiento diversos ordenadores de placa reducida.
RISC OS	Una distribución no Linux para desarrolladores, utilizada para el desarrollo de proyectos de Hardware.

Además de estos sistemas operativos cabe destacar otro que también es soportado por la Raspberry Pi 2 B, aunque no está en la página oficial del Raspberry, este sistema operativo es el OpenWRT, que merece especial atención porque es una distribución de Linux diseñada para trabajar con comunicaciones y ampliamente usado para las redes Mesh como la que se desea llevar a cabo.

Teniendo en cuenta los sistemas operativos disponibles para la placa Raspberry Pi 2 B, se determinó que **el sistema operativo más idóneo es el OpenWRT**, por ser directamente orientado a las comunicaciones y por haber proyectos en los que también se le utiliza con video vigilancia, un inconveniente que se puede llegar a tener, es la falta de documentación, ya que no es muy amplia la cantidad de información existente con proyectos realizados con este sistema operativo y este Hardware. Es por ello que con este

sistema operativo solo se hicieron pruebas de cómo establecer una red Mesh, mas sin embargo no se logró llevar a cabo los otros servicios que necesitaba cada nodo.

Como segunda se eligió al sistema operativo Raspbian sistema con el cual se desarrollará el sistema operativo ya que ofrece mayor flexibilidad y documentación para la implementación de los servicios que pretende ofrecer el prototipo. Además, con Raspbian se han desarrollado muchos proyectos documentados en la Web, los controladores pueden son más fáciles de obtener y resulta relativamente amigable de trabajar según las reseñas de internet.

6.2.3 Elección de protocolos

Ahora que se tienen los posibles sistemas operativos con los que se trabajara, se puede empezar a elegir los protocolos que se utilizaran para, establecer comunicación con una red Mesh y enrutar los paquetes a través de la misma, transmitir video de las cámaras a través de la red Mesh, controlar remotamente los nodos, establecer comunicación de red.

6.2.3.1 Elección de protocolo de comunicación para la red Mesh

Según la investigación sobre proyectos similares, los protocolos más comunes que se utilizan son BATMAN y OLSR, incluso el más utilizado es BATMAN según una apreciación subjetiva de parte del equipo a partir de la cantidad de proyectos desarrollados con cada protocolo que se ha encontrado en la web, aunque no presenten grandes diferencias de rendimiento según algunas fuentes, tal como lo indica el ingeniero en ciencias y computación del instituto nacional de tecnología Puducherry de Karaikal

India, el Dr. Narendran Rajagopalan en su publicación a una revista informática (**Rajagolapan, 2013**). El artículo presenta una comparación de los protocolos BATMAN y OLSR, la comparación se basa en una serie de estudios experimentales realizados a los protocolos, concluyendo que OLSR se comporta levemente mejor que BATMAN pero que las diferencias son muy bajas para dar un veredicto concluyente.

Por ello se hizo una comparación teórica de los protocolos basándose en el artículo anterior y en la publicación en la web “Redes inalámbricas de uso comunitario: un Análisis comparativo de protocolos” de E. Rodríguez disponible en la Biblioteca Digital de la Universidad Católica Argentina, que recomienda el estudio de la topología para la elección del protocolo.

Tabla 6-8 Comparativa entre los protocolos OLSR y BATMAN

Clasificación del protocolo	OLSR	BATMAN
Modo de descubrimiento de rutas	Proactivo	Proactivo
Algoritmo implementado	Estado de enlace	Vector distancia
Tablas de enrutamiento	El protocolo hace que cada nodo sepa toda la red, posiblemente sobrecargando la capacidad de los nodos si es una red muy grande, pero	El protocolo hace que cada nodo solo almacene la información referente a su siguiente salto por lo que no necesita saber toda la red cada

haciéndola más eficiente si es una red pequeña y no está en constante cambio.	nodo, esto permite que los nodos no se sobrecarguen pero que deban hacer una determinación de la ruta a la hora de transmitir, en lugar de saberla de antemano.
---	---

En base a las características descritas en la última tabla se determinó que era mejor utilizar OLSR, ya que los nodos de la red son pocos y la red no estará en constante cambio al tratarse de una red de cámaras y puntos de acceso a internet, si por el contrario fuera a tratarse de una red de clientes que directamente formaran una red de internet entre ellos, posiblemente sería una mejor opción BATMAN, pero dadas las circunstancias se optó por OLSR. Pero siempre se mantiene al BATMAN como opción si OLSR no da el rendimiento necesario para prestar el servicio de enrutamiento en la red Mesh.

6.2.3.2 Elección de protocolo para transmisión de video

Para la transferencia de video existen diversos protocolos para el Streaming de video, como lo son la familia de protocolos RTP¹, RTMP², HTTP³, HLS⁴, DASH⁵, Shoutcast⁶ y otros, pero los más comunes son RTP y HTTP, por ello nos decantamos por cualquiera de estos 2 protocolos para dar soporte al Streaming, pero de entre estos 2 se debe escoger cual es el que mejor trabajaría según lo que requiere el servicio de Streaming en tiempo real.

RTP trabaja con UDP como protocolo a nivel de capa de transporte, lo que implica que la transmisión no requiere confirmación de entrega de paquetes, permitiendo una transferencia más rápida pero sensible a fallas, ya que, si algún paquete falta, este ya no tiene posibilidad de ser reincorporado a los paquetes recibidos y los datos recibidos quedan incompletos.

¹ RTP: Es un protocolo de nivel de sesión utilizado para la transmisión de información en tiempo real, como por ejemplo audio y vídeo en una video-conferencia. **(Wikipedia RTP, 2016)**

² RTMP: inicialmente fue un protocolo con propiedad y desarrollado por Macromedia para el streaming de audio, vídeo y datos a través de Internet, entre un reproductor Flash y un servidor. **(Wikipedia RTMP, 2016)**

³ HTTP: es el protocolo de comunicación que permite las transferencias de información en la World Wide Web. **(Wikipedia HTTP, 2016)**

⁴ HLS: es un protocolo de comunicaciones de streaming basado en HTTP implementado por Apple Inc. como parte de su QuickTime, Safari, OS X, y el software IOS. **(Wikipedia HSL, 2016)**

⁵ DASH: también conocido como MPEG-DASH, es una técnica de transmisión con velocidad de transmisión adaptable que permite el streaming de alta calidad de contenido multimedia a través de Internet entregado desde los servidores web HTTP convencionales. **(Wikipedia DASH, 2016)**

⁶ Shoutcast: es una tecnología de streaming auditiva freeware, desarrollada por Nullsoft. SHOUTcast utiliza la codificación MP3 o AAC de contenido auditivo y http (Hyper Text Transfer Protocol) como protocolo (también se puede utilizar multicast) para transmitir radio por internet. **(Wikipedia Shoutcast, 2016)**

Mientras tanto http trabaja con TCP en su capa de transporte, lo que hace que la transferencia se más lenta pero más confiable porque los paquetes si reciben confirmación y reenvió de ser necesario.

Teniendo en cuenta esto, es lógico decir que nos conviene más el uso de RTP para el Streaming de video, porque es más viable para la transmisión de video en tiempo real, tal como Microsoft lo sugiere en su artículo “Comparing HTTP Streaming Protocol with RTSP” (**Microsoft, 2010**), si se tratase de transferencia de video previamente grabado que no se estuviese transfiriendo en tiempo real HTTP sería la mejor opción, pero la necesidad de hacer la transferencia en tiempo real no lleva a decantarnos por RTP como primera opción para el Streaming de video, manteniendo a HTTP como una segunda opción en caso de no poder implementar RTP.

7 Desarrollo

7.1 Diseño del prototipo

7.1.1 Diseño del prototipo

El prototipo está basado en una red *mesh* de cuatro nodos, uno de estos conectado alámbricamente a la red de la alcaldía, la cual cuenta con acceso a internet; mismo acceso que se utilizara para brindar el servicio AP o expansión de zonas de zonas Wi-Fi, utilizando la red interna de la alcaldía para transmitir las imágenes de video desde los cuatro nodos hasta el centro de monitoreo ubicado en la alcaldía.

7.1.2 Esquema del prototipo

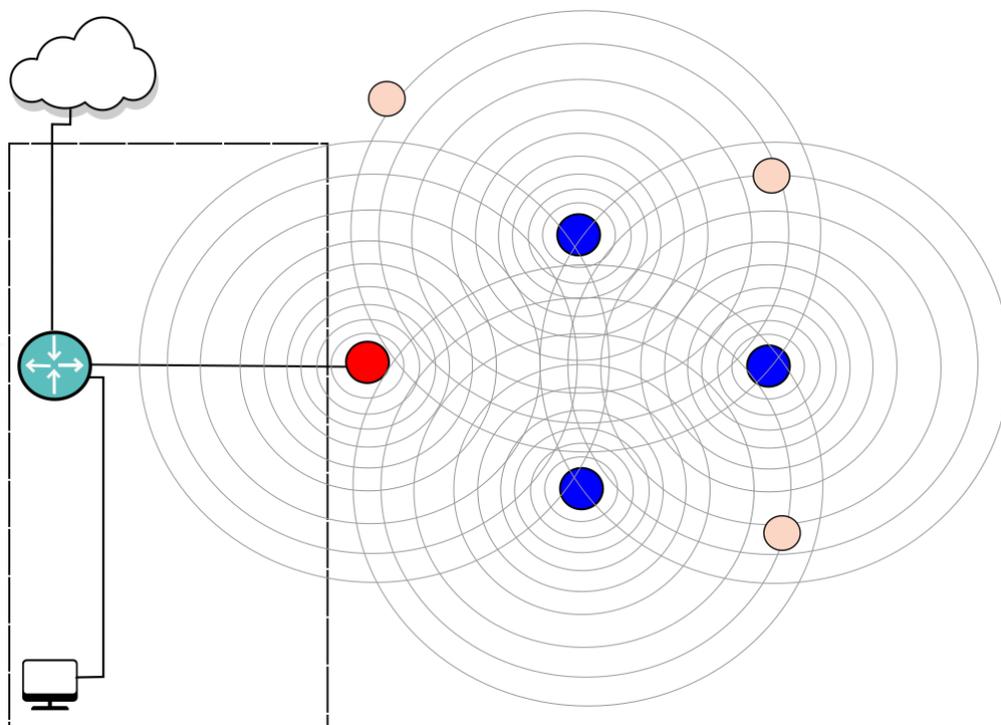


Ilustración 7-1 Diseño del prototipo

El rectángulo de líneas discontinuas representa la localidad de la alcaldía que a su vez delimita la frontera entre las redes, la red *mesh* del prototipo y la red interna de la alcaldía; El diseño de este prototipo no está basado en condiciones precisas de ninguna municipalidad por lo que puede ser utilizado en cualquier otra que cumpla con los requisitos para ello (*factibilidad operativa*), dividiendo así el esquema en dos grandes partes, la red *mesh* del prototipo y la red interna de la alcaldía.

Los círculos rosados representan posibles nodos que se podrían añadir con el tiempo, pensando en la expansión de la red, los cuales pueden compartir sus recursos si así lo desean, como el acceso a internet haciendo crecer el ancho de banda disponible al público en general. Dichos nodos tentativos pueden ser aportados por la misma comunidad que quiera compartir su acceso a internet haciendo crecer la red *mesh* y fortaleciendo la misma, al tener más opciones de salida a internet.

7.1.3 Red *mesh* del prototipo

Constituida por cuatro nodos de dos tipos:

- ✓ **Nodo Centinela (3):** Representado en color azul, es el nodo que brinda los servicios de videovigilancia y *AP*, el cual posee dos interfaces de red inalámbrica, una capaz de soportar el modo *Ad-Hoc* y otra capaz de soportar el modo *master*, y una cámara para la transmisión de video streaming.

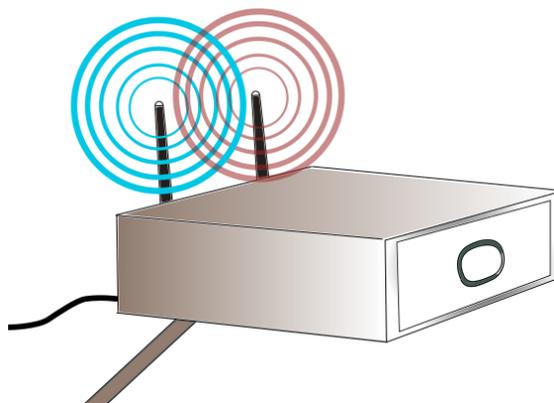


Ilustración 7-2 Cámara IP del prototipo

- ✓ **Nodo Frontera (1):** Representado de color rojo, es el nodo que permite la comunicación entre la red *mesh* y la red interna de la comuna por medio de una conexión alámbrica, y que además tiene todas las características de un Nodo Centinela. Este es el nodo responsable de la transmisión de toda la información desde la red Mesh y el centro de vigilancia, así como también garantizar el acceso a Internet desde la red Mesh.

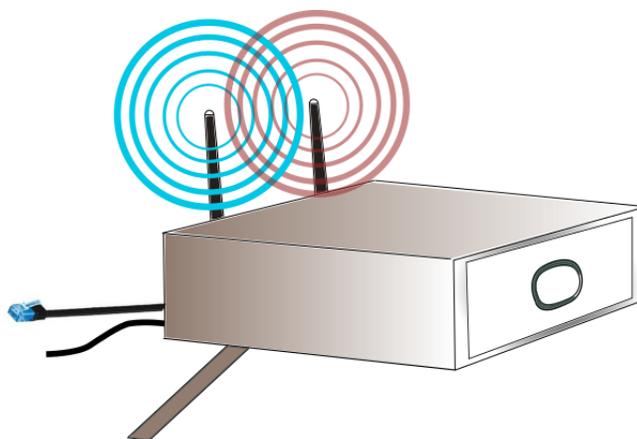


Ilustración 7-3 Cámara IP del prototipo

7.1.4 Red interna de la Alcaldía.

El diseño de esta red queda fuera del alcance de este trabajo de graduación, sin embargo, dicha red debe garantizar:

- Acceso a Internet (Nube en el diagrama): Debe tener una conexión a internet, la cual será utilizada por el Nodo Frontera para enviar y recibir todos los paquetes desde y hacia la red Mesh.
- Comunicación estable hacia el centro de monitoreo (Computadora en el diagrama): El centro de monitoreo es ya sea un computador potente como un servidor dedicado o compartido, el cual recibe todo el streaming de video desde la red Mesh emitido por cada uno de los Nodo Centinela.

Esta red cuenta con al menos un router que es el encargado de dirigir todos los paquetes ya sea desde la misma red, así como desde la red Mesh, representado por un circulo de color gris con flechas en el centro, es el dispositivo que está conectado a el Nodo Frontera ya sea directamente o a través de un Switch.

7.2 Comunicación de la red Mesh

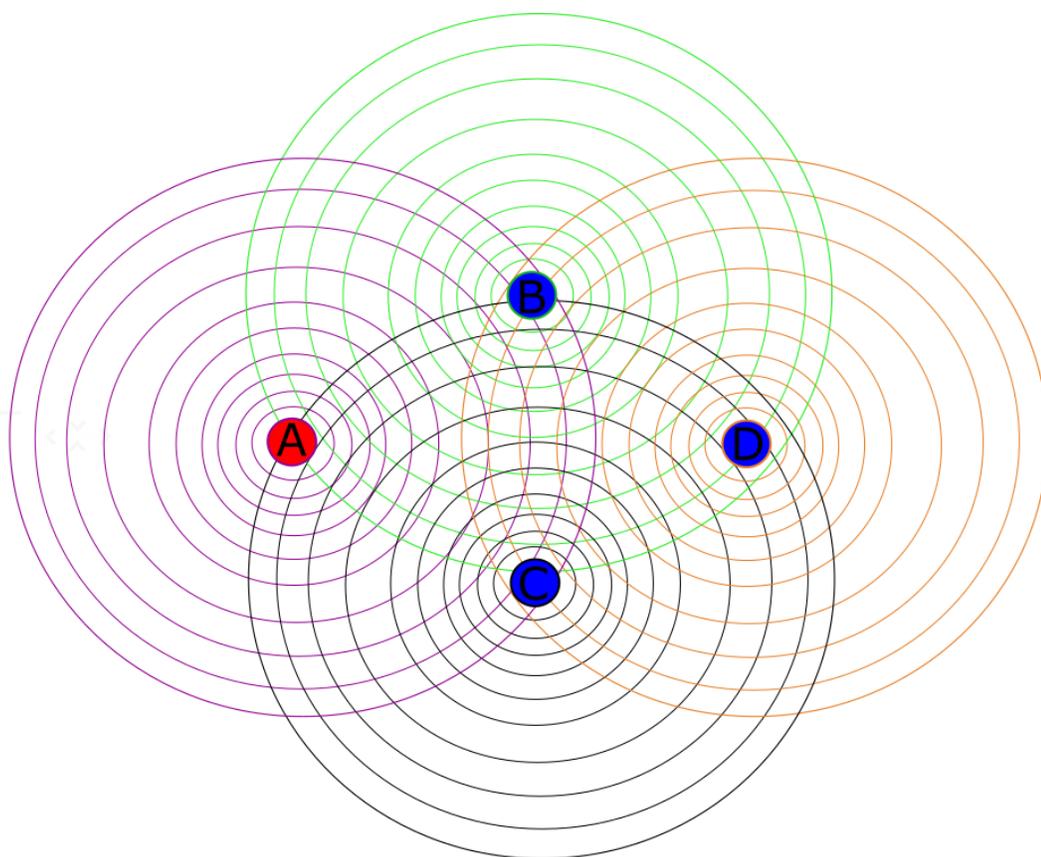


Ilustración 7-4 Comunicación entre nodos de la red Mesh

De color azul los Nodos Centinelas y de color rojo el Nodo Frontera, cada uno emitiendo un radio de alcance de su señal inalámbrica detectando vecinos en la red se obtienen los siguientes enlaces de comunicación.

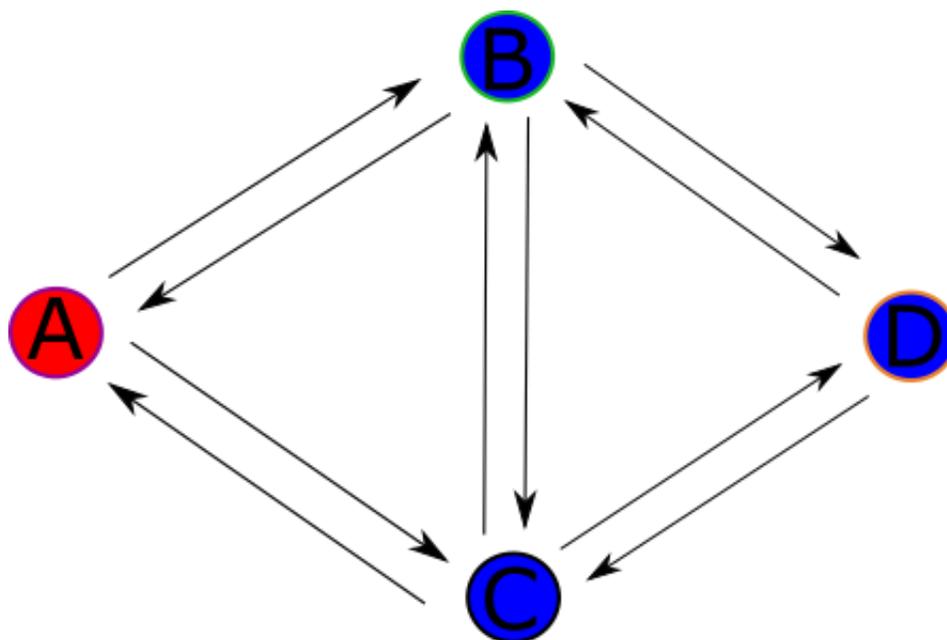


Ilustración 7-5 Rutas entre los nodos del prototipo

Con este diseño de red Mesh se generan 5 enlaces bidireccionales (una vez establecido el enlace se puede recibir o enviar datos al otro extremo del enlace) los cuales sirven de rutas para el envío de información, en este caso en específico el streaming de video, el cual es generado por los cuatro nodos y todo el tráfico de información generado desde los clientes de los AP instalados en cada uno de los nodos.

7.2.1 Nodos “B” y “C” como puente

Llamados así por su función, pasar la información desde el lado izquierdo del mallado hacia el derecho o viceversa. Con esto se aporta robustez al diseño, con más posibles formas de alcanzar un nodo desde otro distante, así pues, si llegase a fallar el nodo “B” perfectamente el nodo “C” sigue garantizando la comunicación entre “A” y

“D” igual en el caso contrario en el que “C” fallara el nodo “B” se encarga de comunicar a los demás nodos entre sí.

7.2.2 Rutas en la red Mesh

Tabla 7-1 Posibles saltos de los nodos en la red Mesh

Origen	Destino	Saltos	Ruta	
A	B	1	A - B	
		2	A - C - B	
		3	A - C - D - B	
	C	1	A - C	
		2	A - B - C	
		3	A - B - D - C	
	D	2	2	A - B - D
			2	A - C - D
		3	3	A - B - C - D
3			A - C - B - D	
B	A	1	B - A	
		2	B - C - A	
		3	B - D - C - A	
	C	1	B - C	
		2	B - A - C	
		2	B - D - C	
	D	1	B - D	
		2	B - C - D	
		3	B - A - C - D	
C	A	1	C - A	
		2	C - B - A	
		3	C - D - B - A	
	B	1	C - B	
		2	C - A - B	
		2	C - D - B	
	D	1	C - D	
		2	C - B - D	
		3	C - A - B - D	
D	B	1	D - B	
		2	D - C - B	
		3	D - C - A - B	
	C	1	D - C	

		2	D – B – C
		3	D – B – A – C
	A	2	D – B – A
		2	D – C – A
		3	D – B – C – A
		3	D – C – B – A

Estas rutas serán elegidas por el protocolo de enrutamiento, el cual debe elegir la ruta más óptima según sean las condiciones en ese momento. Estas son las posibles rutas por las cuales un paquete puede alcanzar su destino, existiendo un mínimo de 3 rutas; lo cual vuelve robusta la red Mesh, la cual es más robusta a medida se agregan más nodos, puesto que son más las posibilidades para enviar un paquete.

7.3 Diseño de servicios

7.3.1 Diseño del servicio de expansión de zonas Wi-Fi

Cada nodo de la red Mesh está dotado con una interfaz de red capaz de soportar el modo Master el cual permite la creación de un ACCESS POINT o AP por sus siglas, el cual permite a distintos dispositivos conectarse a él, brindando un acceso a internet a través de la red Mesh, la cual esta suministrada de dicho acceso por el Nodo Frontera que se encuentra conectado a la red interna de la comuna donde se encuentra la salida a internet, al cual será compartida por los demás usuarios de la comunidad para evitar los tiempos de ocio de dicho recurso.

7.4 Diseño del caso de estudio

La alcaldía de San José las Flores decidió que los servicios se prestaran en la zona del parque que esta frente a la alcaldía y sus alrededores, por ser donde suele haber una alta afluencia de personas, principalmente jóvenes que pueden hacer uso del servicio de acceso a internet. Además, les pareció una buena zona para iniciar con la videovigilancia por ser una zona concurrida y con establecimientos comerciales y de interés a los alrededores.

A continuación, se detallan los puntos de interés que se desean vigilar.

Tabla 7-2 Puntos de interés para el prototipo.

Punto de interés	Razón
<p>Frente de la alcaldía</p> 	<p>La fachada de la alcaldía fue presentada como un punto de vigilancia importante porque se desea vigilar quienes entran a la alcaldía. Se planea que se ubique un nodo en la esquina del parte que esta frente a la alcaldía, o en la glorieta si los arboles lo permiten.</p>

Glorieta del parque



En la glorieta del parque se suelen reunir jóvenes a hacer tareas o pasar tiempos libres, por lo que es bueno que haya acceso a internet ahí, además se consideró buena idea que haya vigilancia por la propia seguridad de los jóvenes.

Tienda comunal



La comuna cuenta con una tienda, la cual se desea vigilar, además tiene un gimnasio comunal a la par también, por lo que la zona en sí se podría abarcar con una sola cámara.

A continuación, se muestra la distribución de donde se determinó que se debían poner los nodos y hacia donde debían de apuntar las cámaras, además se muestran los puntos de interés seleccionados por la alcaldía y fuentes de recursos influyentes al sistema.

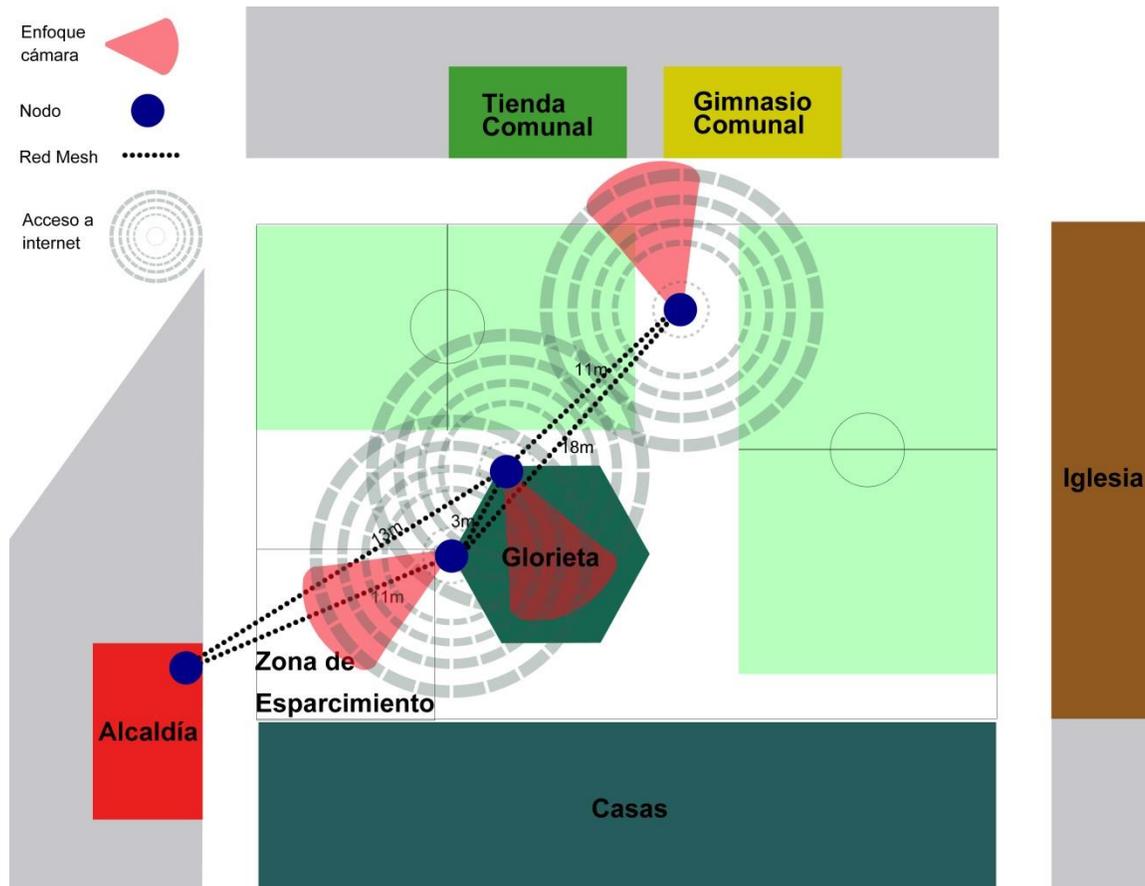


Ilustración 7-6 Distribución física del prototipo

7.5 Configuraciones

7.5.1 Instalar sistema operativo (Raspbian Wheezy)

Recursos necesarios:

- Tarjeta micro SD: Es recomendable una tarjeta clase 10 de al menos 8 GB, si no se dispone de este modelo puede utilizar una de clase 4 con capacidad mínima de 4GB.

- Una computadora con lector de tarjeta micro SD y sistema operativo Linux (Ubuntu o Debian), para la instalación de la imagen de S.O en computadoras con Windows ver Anexo1. Si no dispone de lector de tarjetas micro SD utilice un adaptador de tarjetas SD a USB.

Software necesario

- Archivo con la imagen de Raspbian Wheezy

7.5.1.1 Paso 1: Descargar la imagen

Ingresar a la siguiente URL: <https://www.raspberrypi.org/downloads/raspbian/> y descargar al archivo de la imagen de Raspbian en la computadora en un directorio al cual se pueda acceder fácilmente.

7.5.1.2 Paso 2: Instalar Raspbian con la herramienta 'dd'

Esta es herramienta en muy poderosa en cuanto a sus usos, por lo cual tener mucho cuidado con las sentencias que se ejecuten a continuación.

Ejecutar **df -h** para visualizar los dispositivos montados en la computadora actualmente. Si la computadora posee un slot para tarjetas SDs, insertar la SD en dicho slot; caso contrario puede utilizar un adaptador SD-USB.

Una vez dentro la memoria SD, ejecutar nuevamente el comando **df -h**, el nuevo dispositivo que ha aparecido es la tarjeta SD. La columna de la izquierda proporciona el

nombre de la tarjeta SD, mostrara algo parecido a `/dev/mmcblk0p1` o `/dev/ssd1`. La última parte (`p1` o `1` respectivamente) es el número de la partición, pero se busca grabar la imagen la tarjeta completa, para esto quitar el `p1` o `1` del nombre, obteniendo algo por ejemplo como `/dev/mmcblk0` o `/dev/sdd`. Esto es necesario ya que las imágenes de Raspberry Pi poseen más de una partición.

Ahora que ya se tiene el nombre de la tarjeta SD dada por el sistema, es necesario desmontarla, para evitar que sea leída o algún otro proceso intente escribir sobre ella. Para ello ejecute el siguiente comando.

```
- umount /dev/sdd1
```

Reemplazar **ssd1** por cualquiera que sea el nombre del dispositivo SD que se haya detectado en el paso anterior (incluyendo el número de la partición). Si la tarjeta SD posee más de una partición, todas estas particiones deberán ser desmontadas, siguiendo los mismos comandos.

El siguiente comando, es el comando `dd`, el cual deberá ser ejecutado ya sea desde un usuario **root** o agregando el prefijo **sudo** a la orden siguiente.

```
dd bs=4M if=2016-03-18-raspbian-jessie.img of=/dev/sdd
```

Ejecutar el comando anterior en una terminal, escribe la imagen *if="Nombre de la imagen"* en el dispositivo *of="nombre del dispositivo"*. Cambiar estos datos por los

obtenidos en los pasos anteriores, si se ejecuta el comando `dd` dentro de la carpeta que contiene el archivo basta con el nombre de dicho archivo, si se ejecuta desde otro directorio, especificar la dirección completa del archivo ejemplo: `/home/usr/Descargas/2016-03-18-raspbian-jessie.img`.

El tamaño de bloque en 4M trabajara correctamente en la mayoría del tiempo, si no es así, intentar con 1M.

El comando `dd` no provee ningún tipo de información de estado o progreso, y podría parecer que la computadora o la terminal se ha congelado, pero no es así, este proceso podría tardar entre 5 a 20 minutos dependiendo de la computadora que se está utilizando.

Correr el comando **`sync`**, el cual se encarga de asegurarse que es seguro extraer la SD de la computadora. Ahora ya es seguro extraer la SD con la imagen escrita correctamente.

7.5.1.3 Paso 3: Configurar la primera ejecución del sistema operativo

Al iniciar el sistema operativo por primera vez, se presentará una pantalla de configuración inicial como se muestra en la imagen, en esta configuración se deberá elegir las siguientes opciones:

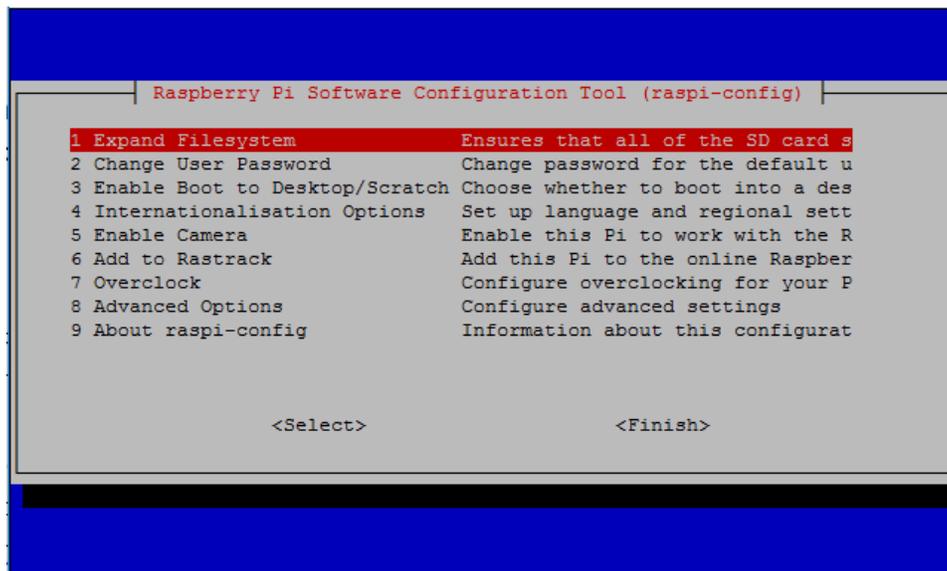


Ilustración 7-7 Interfaz de configuración de Raspberry

Entrar a la opción expand filesystem, al acceder el sistema permitirá utilizar todo el espacio de la memoria SD, al realizarlo se mostrará una pantalla como la que se muestra en la figura.

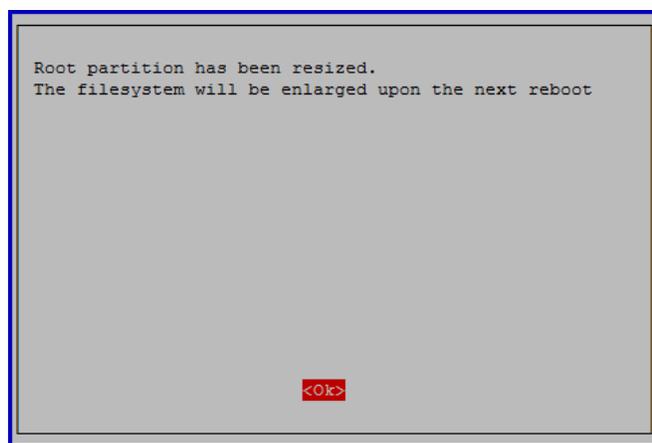


Ilustración 7-8 Confirmación de expansión de disco

Modificar la contraseña, en esta opción se modifica la contraseña del usuario pi que es el usuario por defecto.

Mostrará un mensaje para avisar que se procederá a preguntar por la contraseña, presionar OK para continuar

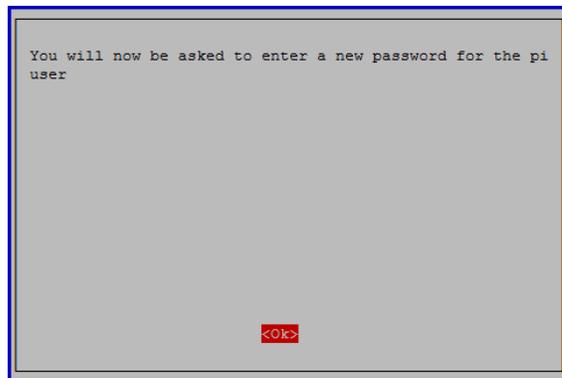


Ilustración 7-9 Interfaz de cambio de contraseña

En la línea de comando en la que pregunta la contraseña, ingresar la contraseña que se desea poner al usuario.

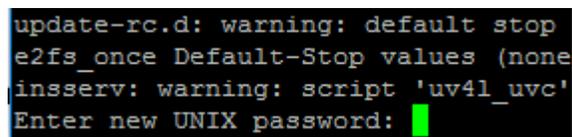


Ilustración 7-10 Línea de comandos, cambio de contraseña

Luego de ingresarla volverá a preguntar por una confirmación de la contraseña, volver a escribirla tal cual la escribió previamente.

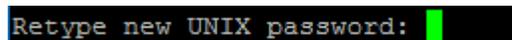


Ilustración 7-11 Confirmación del cambio de contraseña

Si la confirmación fue la correcta se mostrará un mensaje como el que se muestra en la imagen, presione OK para volver al menú principal.

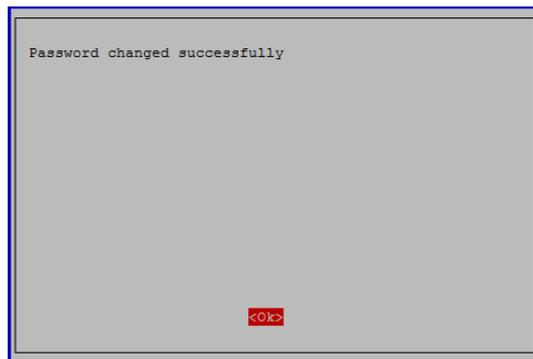


Ilustración 7-12 Ventana de confirmación

En caso de no coincidir las contraseñas mostrará un mensaje de error y volverá al menú principal.

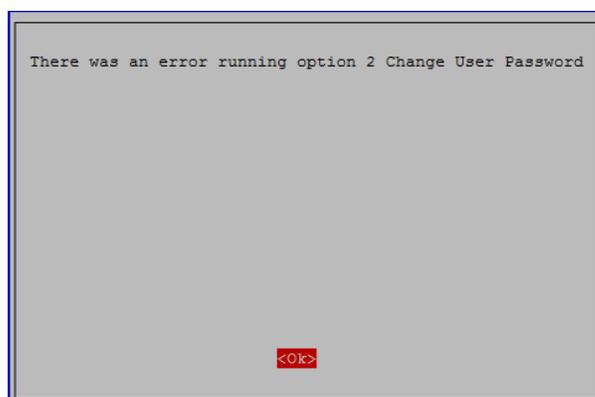


Ilustración 7-13 Mensaje de error

Acceder a la opción 3 del menú para elegir que el sistema iniciara en modo línea de comando siempre.

Por defecto accederá en modo línea de comando como se muestra en la imagen, presionar ENTER para continuar y regresar al menú principal

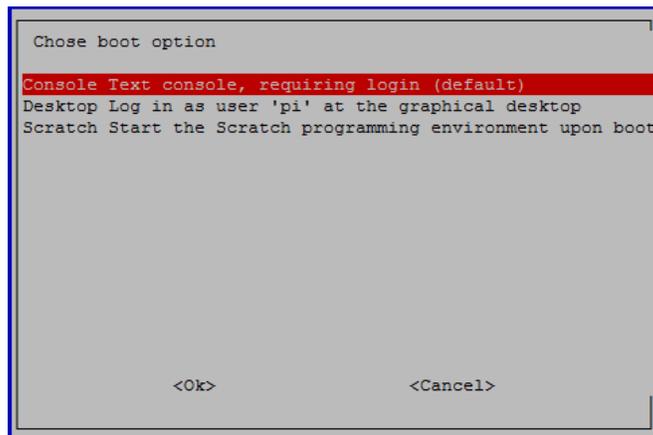


Ilustración 7-14 Interfaz de configuración de Raspberry

Habilitar la cámara accediendo a la opción 5 del menú.

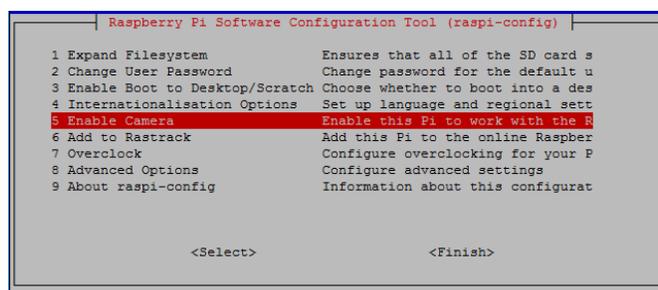


Ilustración 7-15 Interfaz de configuración de Raspberry

Escoger la opción "Enable" y presione ENTER para volver al menú principal.

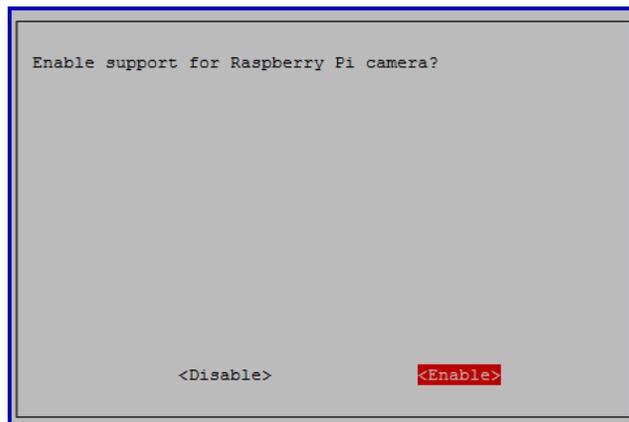


Ilustración 7-16 Ventana de habilitación de la cámara

Acceder a la opción 8 en la que se encuentran las opciones avanzadas.

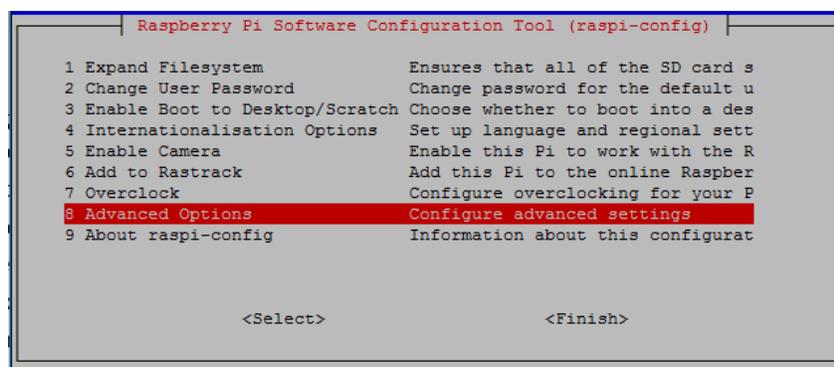


Ilustración 7-17 Interfaz de configuración de Raspberry

Dentro encontrará otro submenú, dentro escoger la opción A4 para habilitar el protocolo SSH que permitirá un posterior acceso a la Raspberry desde un ordenador vía LAN.

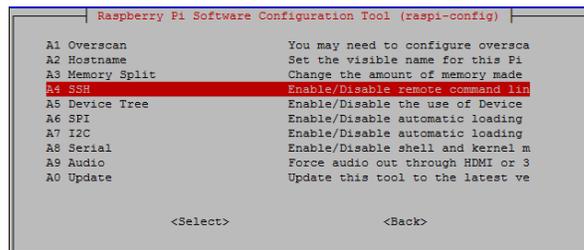


Ilustración 7-18 Interfaz de configuración de Raspberry

Marcar como “Enable” y presionar ENTER.

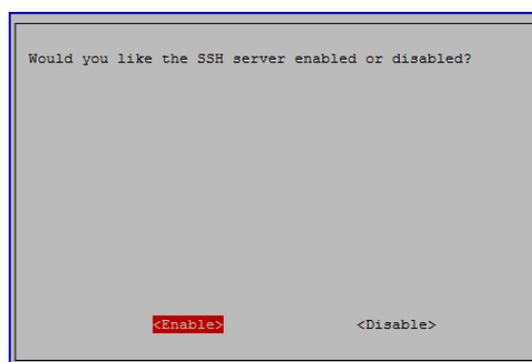


Ilustración 7-19 Interfaz de habilitación

Se mostrará una pantalla de confirmación, presionar OK para volver al menú principal.

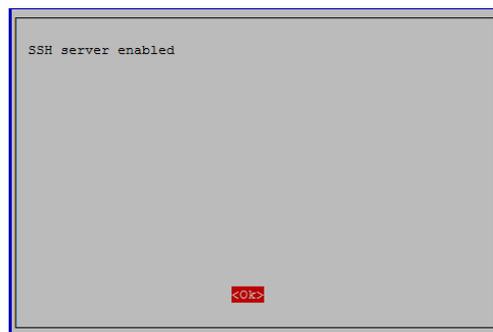


Ilustración 7-20 Ventana de confirmación

Presionar “Finish” para aceptar todas las configuraciones anteriores.

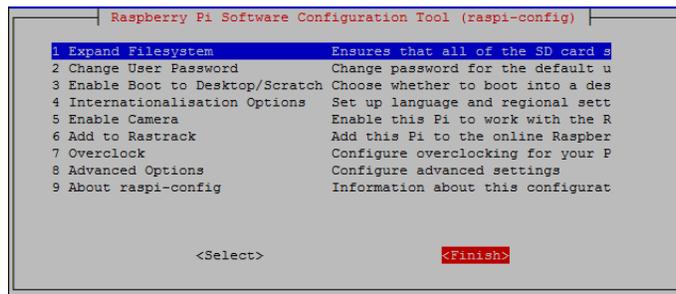


Ilustración 7-21 Interfaz de configuración de Raspberry

Preguntara si se desea reiniciar, escoja que si con la opción “Yes” presionando ENTER.



Ilustración 7-22 Aviso de reinicio del sistema

7.5.2 Primer inicio al sistema

7.5.2.1 Preparación para trabajar con SSH

Las configuraciones siguientes, se pueden realizar directamente en cada Raspberry (directamente desde el teclado conectado al dispositivo y un monitor asociado al mismo) o bien desde un acceso remoto, en caso que se quiera realizar las configuraciones directamente salte este paso, para ejecutar un comando basta con presionar enter desde la terminal.

Para trabajar más cómodamente con los dispositivos se recomienda habilitar y configurar el SSH.

- Identificar la red LAN: Identificar la red, la máscara y el Gateway de red en la cual está desarrollando el prototipo.
- Configurar estáticamente la interfaz eth0 de la Raspberry: Modificando el archivo interfaces dentro del cual están las configuraciones de las interfaces.
- Reiniciar el servicio de Networking de la Raspberry para aplicar los cambios realizados.

Realizar los pasos anteriores con cada una de las Raspberries asignando una IP distinta a cada una, ya que cada una se identificará con esa IP y es por medio de la cual será establecida la conexión SSH; a continuación se muestran los pasos realizados para la configuración de este prototipo, tener en cuenta que las direcciones IP utilizadas para las interfaces eth0 son del ambiente de desarrollo de este grupo de trabajo de graduación, para que este paso tenga éxito se deberá sustituir estas direcciones por las de su ambiente de desarrollo.

7.6 Desarrollo del prototipo

7.6.1 Configuración de IPs estáticas a la interfaz eth0

Se le asignó una IP distinta a cada Raspberry, basada en la red LAN del ambiente de desarrollo de la siguiente forma.

Tabla 7-3 Dirección de la red alámbrica

Red	Mascara de Red	Gateway
192.168.0.0	255.255.255.0	192.168.0.1

Se le asignó una IP a cada nodo.

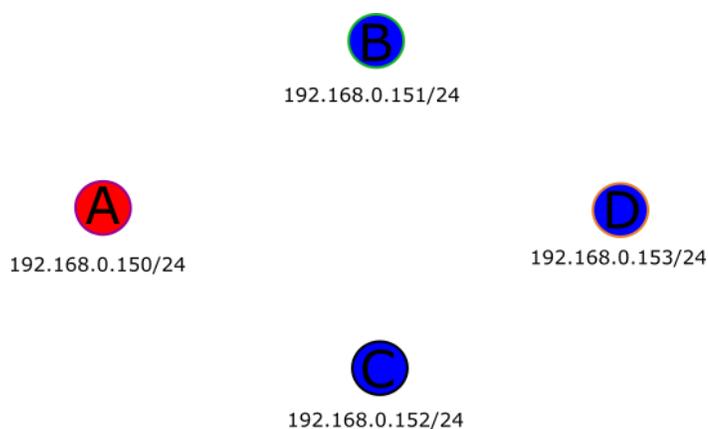


Ilustración 7-23 Distribución de Ips dentro de la red

7.6.1.1 Comandos para configurar una IP estática

Modificar el archivo interfaces ubicado en `/etc/network/interfaces`. Para poder modificar este archivo es necesario ser un usuario root o anteponer el prefijo sudo, el editor de texto usado en esta guía es **nano**, este archivo contiene toda la configuración de las interfaces del dispositivo, agregar las siguientes líneas, borrando la configuración que ya está escrita para la interfaz eth0.

```
nano /etc/network/interfaces
```

```
auto eth0
allow-hotplug eth0
iface eth0 inet static
    address 192.168.0.150
    netmask 255.255.255.0
    gateway 192.168.0.1
```

La configuración anterior es la configuración del Nodo Frontera, realizar los cambios respectivos adaptando la configuración a la LAN ya sea de desarrollo o producción.

```
Ctrl + O //Guardar el documento
Ctrl + X //salir
```

Una vez modificado el archivo de configuración, es necesario reiniciar el servicio networking para que estos cambios sean efectivos, seguir el siguiente comando para ello.

7.6.1.2 Comandos para reiniciar el servicio networking

```
/etc/init.d/networking restart
```

El servicio será reiniciado y las configuraciones hechas anteriormente serán aplicadas.

Los pasos anteriores se repitieron en los cuatro nodos del prototipo, cambiando las direcciones por las correspondientes en el diagrama *Ilustración 7 - 33*

7.6.2 Red Mesh y OLSR (Interfaz Wlan0)

Para levantar la red Mesh, es necesario establecer la interfaz inalámbrica (Wlan0) en modo Ad-Hoc y definir una red para la red *Mesh*, así como un único ESSID y un canal, esta información tiene que ser la misma en todos los dispositivos para que se puedan unir a una misma célula, caso contrario no estarán en una misma red Mesh, la configuración será la misma en todos los dispositivos con la única diferencia que la dirección IP de cada interfaz inalámbrica será distinta pero dentro la misma red. Debido al comportamiento de la red *Mesh*, no es necesario definir un Gateway por defecto, ya que cada nodo tiene la capacidad de enrutar los paquetes hacia su destino, más adelante se definirá un Gateway de salida hacia Internet para toda la red *mesh* por medio del protocolo OLSR.

Tabla 7-4 Dirección Ip de la red MESH

Red Mesh	Mascara de Red	Gateway
192.168.3.0	255.255.255.0	-

Distribución de IPs

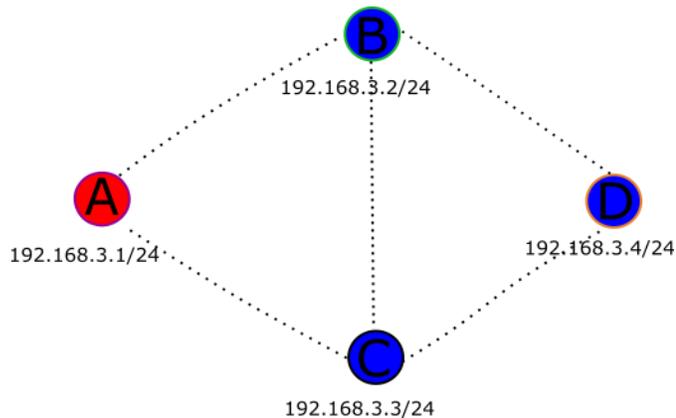


Ilustración 7-24 Distribución de Ips dentro de la red MESH

7.6.2.1 Comandos para la configuración de la interfaz Wlan0 (Red Mesh)

```
nano /etc/network/interfaces
```

Modificar el archivo interfaces ubicado en **/etc/network/interfaces**. Borrando la configuración que ya está escrita para la interfaz wlan0.

```
auto wlan0
allow-hotplug wlan0
iface wlan0 inet static
    address 192.168.3.1
    netmask 255.255.255.0
    wireless-channel 11
    wireless-ssid VMesh
    wireless-mode ad-hoc
```

7.6.2.2 Comandos para configurar el servicio ifplugd

Este paso es de suma importancia para poder aplicar los cambios realizados, en caso de omitirlo no se aplicará ninguna configuración realizada. Detener el servicio ifplugd:

```
service ifplugd stop
```

Modificar el archivo ifplugd ubicado en `/etc/default/ifplugd` de la siguiente manera:

```
GNU nano 2.2.6 File: /etc/default/ifplugd
# This file may be changed either manually or by running dpkg-reconfigure.
#
# N.B.: dpkg-reconfigure deletes everything from this file except for
# the assignments to variables INTERFACES, HOTPLUG_INTERFACES, ARGS and
# SUSPEND_ACTION. When run it uses the current values of those variables
# as their default values, thus preserving the administrator's changes.
#
# This file is sourced by both the init script /etc/init.d/ifplugd and
# the udev script /lib/udev/ifplugd.agent to give default values.
# The init script starts ifplugd for all interfaces listed in
# INTERFACES, and the udev script starts ifplugd for all interfaces
# listed in HOTPLUG_INTERFACES. The special value all starts one
# ifplugd for all interfaces being present.
INTERFACES="eth0"
HOTPLUG_INTERFACES="eth0"
ARGS="-q -f -u0 -d10 -w -I"
SUSPEND_ACTION="stop"
```

Ilustración 7-25 Archivo "ifplugd" de Raspbian

```
Ctrl + O //Guardar el documento
Ctrl + X //salir
```

```
/etc/init.d/ifplugd restart
```

Este comando reiniciará el servicio ifplugd aplicando las configuraciones realizadas.

```
/etc/init.d/networking restart
```

Esto permitirá que las modificaciones realizadas en la interfaz wlan0 se hagan efectivas, en este punto ya está levantada la red Mesh con un solo nodo.

7.6.2.3 Comandos para instalar y configurar OLSR

```
apt-get update
```

El update es opcional, pero se recomienda.

```
apt-get install olsrd
```

Modificar el archivo olsrd.conf, ubicado en **/etc/olsrd/olsrd.conf** indicando la interfaz en la cual se requiere que trabaje el protocolo. Por defecto si el sistema le asigna el nombre wlan0 a la primera interfaz que se conecta a la Raspberry.

```

GNU nano 2.2.6                               File: /etc/olsrd/olsrd.conf
#
# olsr.org OLSR daemon config file
#
# Lines starting with a # are discarded
#
# This file was shipped with the debian olsrd package
#
#
# This file is an example of a typical
# configuration for a mostly static
# network(regarding mobility) using
# the LQ extention
#
# Debug level(0-9)
# If set to 0 the daemon runs in the background
DebugLevel      0
#
# Interfaces and their rules
# Omitted options will be set to the
# default values. Multiple interfaces
# can be specified in the same block
# and multiple blocks can be set.
#
# !!CHANGE THE INTERFACE LABEL(s) TO MATCH YOUR INTERFACE(s)!!
# (eg. wlan0 or eth1):
#
# this is (in most cases) the only configuration you need to change
#Interface "eth1" "eth0" "wlan0" "wlan1" "ath0" "ath1"
Interface "wlan0"
{
#
# IPv4 broadcast address to use. The
# one usefull example would be 255.255.255.255
# If not defined the broadcastaddress
# every card is configured with is used

```

Ilustración 7-26 Archivo de configuración de OLSRD

Ctrl + o //Guardar el documento

Ctrl + x //salir

Modificar el archivo olsrd ubicado en **/etc/default/olsrd**, para que se inicie el proceso desde el arranque del dispositivo. Para ello descomentar (quitar el numeral del inicio de la oración) la siguiente línea:

START_OLSRD="YES"

```
Ctrl + O //Guardar el documento  
Ctrl + X //salir
```

```
/etc/init.d/olsrd start
```

Este comando inicia el proceso de olsrd.

Hasta acá, la red Mesh se encuentra activa y el protocolo de enrutamiento olsr se encuentra corriendo.

7.6.3 Acceso a internet a la red Mesh y AP

Lo primero que se debe hacer es identificar el Gateway de salida de la red *mesh*, dicho en otras palabras, el nodo que tendrá acceso a internet y que está conectado a la red local de la alcaldía.

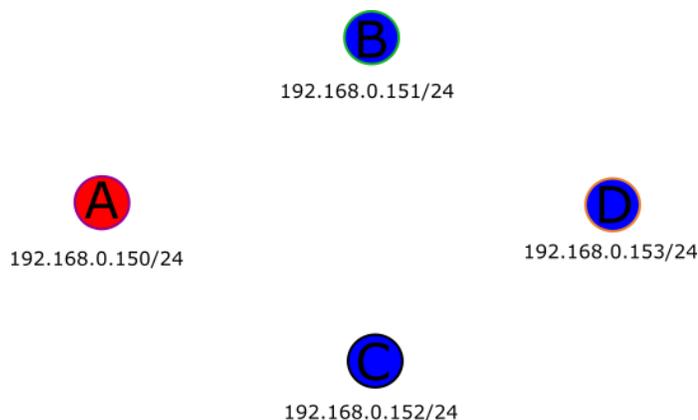


Ilustración 7-27 Diseño de la red MESH

En el diseño de este trabajo, el nodo que servirá de Gateway es el nodo, el cual está conectado alámbricamente con la red local de la alcaldía por medio de la interfaz eth0 y también pertenece a la red *mesh* antes configurada por la interfaz wlan0, es

necesario informar a la red, que este nodo es el Gateway de la red, para esto, se configura el archivo `olsrd.conf`

7.6.3.1 Comandos para definir Gateway de la red en el protocolo OLSR

Modificar el documento `olsrd.conf` ubicado en `/etc/olsrd/olsrd.conf`, buscar la sección de `Hna4` y descomentar la siguiente línea, en dado caso de no estar, agréguela.

```
GNU nano 2.2.6      File: /etc/olsrd/olsrd.conf
# syntax: netaddr netmask
# Example Internet gateway:
# 0.0.0.0 0.0.0.0

Hna4
{
#   Internet gateway:
0.0.0.0 0.0.0.0
#   more entries can be added:
#   192.168.64.0 255.255.255.0
}

# HNA IPv6 routes
# syntax: netaddr prefix
# Example Internet gateway:
Hna6
{
#   Internet gateway:
#   ::          0
```

Ilustración 7-28 Archivo de configuración de OLSRD

Para descomentar solo borre el símbolo de numeral, #.

Es necesario que solo este nodo tenga esta configuración, por ende, repita estos pasos en los otros nodos, comentando o borrando esta línea en sus respectivos archivos de configuración, con esto la red ya posee un Gateway, pero todavía no tiene acceso a internet, para ellos es necesario activar el NAT, como se muestra a continuación.

7.6.3.2 Comandos para activar NAT

La red tiene acceso a internet por el nodo “A”, NAT (Network Address Translation), ayudara a dirigir todo el tráfico de la red *Mesh* hacia la interfaz eth0, dando acceso a internet. Esta configuración solo se realizará en el nodo “A” (Nodo que está conectado directamente a la red local de alcaldía).

Modificar el archivo sysctl.con ubicado en `/etc/sysctl.conf`, en este archivo buscar la línea “`net.ipv4.ip_forward=1`” y descomentarla, en el caso que no esté agréguela al final del archivo

```
Ctrl + O //Guardar el documento
Ctrl + X //salir
```

Para que la configuración surja efecto inmediatamente ejecutamos el siguiente comando.

```
sudo sh -c "echo 1 > /proc/sys/net/ipv4/ip_forward"
```

Configurar el NAT para recibir todas las peticiones por la interfaz wlan0 y reenviarlas por la interfaz eth0 así mismo recibir sus respuestas por la eth0 y dirigirlas a la red *mesh*, con los siguientes comandos.

```
sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE (enter)
sudo iptables -A FORWARD -i eth0 -o wlan0 -m state --state
RELATED,ESTABLISHED -j ACCEPT (enter)
sudo iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT (enter)
```

Para guardar la configuración de iptables y no tener la necesidad que repetirlos en cada inicio de los dispositivos, realizamos la siguiente configuración.

```
sudo sh -c "iptables-save > /etc/iptables.ipv4.nat"
```

El cual crea un archivo de respaldo de toda la configuración actual de iptables, ahora configurar el dispositivo para que con cada reinicio cargue esta misma configuración, para ellos modificar el archivo interfaces de la siguiente manera en el archivo interfaces ubicado en **/etc/network/**.

Agregar la siguiente línea al final del archivo

```
up iptables-restore < /etc/iptables.ipv4.nat
```

```
Ctrl + O //Guardar el documento
```

```
Ctrl + X //salir
```

El archivo debería estar de la siguiente forma

```
GNU nano 2.2.6      File: /etc/network/interfaces
auto wlan0
allow-hotplug wlan0
iface wlan0 inet static
    address 192.168.3.1
    netmask 255.255.255.0
    wireless-channel 11
    wireless-essid VVMesh
    wireless-mode ad-hoc
#wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf
up iptables-restore < /etc/iptables.ipv4.nat
```

Ilustración 7-29 Ejemplo de configuración de NAT desde boot

Ahora el dispositivo cargará dicha configuración al momento de levantar la red y sus interfaces. Reiniciar todos los dispositivos y asegurarse que todo funcione bien hasta el momento con el siguiente comando.

```
sudo reboot
```

7.6.3.3 Comandos para instalar HOSTAPD e ISC-DHCP-SERVER

Las siguientes configuraciones serán realizadas en cada uno de los nodos que no son frontera, es decir nodo B, C y D.

Instalación de ISC-DHCP-SERVER

```
sudo apt-get install isc-dhcp-server
```

Configuración de ISC-DHCP-SERVER. Toda la configuración se realiza en el archivo `dhcpd.conf` ubicado en `/etc/dhcp/`. En este archivo comentar o borrar las siguientes líneas:

```
option domain-name "example.org";  
option domain-name-servers ns1.example.org, ns2.example.org;
```

En la sección de abajo descomentar `authoritative`:

```
#If this DHCP server is the official DHCP server for the local  
#network, the authoritative directive should be uncommented.  
authoritative;
```

Ahora el archivo debe lucir de la siguiente manera

```

GNU nano 2.2.6      File: /etc/dhcp/dhcpd.conf      Modified
#
# Sample configuration file for ISC dhcpd for Debian
#
#
# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# option definitions common to all supported networks...
#option domain-name "example.org";
#option domain-name-servers ns1.example.org, ns2.example.org;

default-lease-time 600;
max-lease-time 7200;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page  ^U UnCut Text ^T To Spell

```

Ilustración 7-30 Archivo de configuración de isc-dhcp-server

Ahora definir la red y el rango de redes que el servidor proporcionara a las peticiones DHCP para ello escribir lo siguiente al final de este archivo

```
subnet 192.168.10.0 netmask 255.255.255.0 {  
    range 192.168.10.10 192.168.10.50;  
    option broadcast-address 192.168.10.255;  
    option routers 192.168.10.1;  
    default-lease-time 600;  
    max-lease-time 7200;  
    option domain-name "local-network";  
    option domain-name-servers 8.8.8.8, 8.8.4.4;  
}
```

Con lo anterior se le está configurando de tal manera que todo aquel dispositivo que solicite DHCP al servidor se le otorgara una IP dentro del rango de 192.168.10.10 y 192.168.100.50, dando un máximo de hasta 40 direcciones IPs, pertenecientes a la red 192.168.10.0 y que usara los servidores DNS de Google el 8.8.8.8 o el 8.8.4.4. Una vez realizadas todas las modificaciones a los archivos guárdelo con el comando Ctrl + O y salga del editor nano con Ctrl + X.

Configurar la interfaz por la cual el servidor escuchara las peticiones DHCP, para esto, editar el archivo `isc-dhcp-server` ubicado en `/etc/default/`

Buscar la línea “INTERFACES” y colocar el nombre de la interfaz por la cual escuchara las peticiones, en todo caso será la otra interfaz de red inalámbrica que posea, recordar que por una interfaz se conectara a la red Mesh y por la otra dará el servicio AP,

es por la interfaz que brindara el servicio AP que escuchara las peticiones. Para este tutorial ocupamos la interfaz Wlan3 en el nodo C, para obtener el identificador de su interfaz de red ejecute el comando iwconfig desde la terminal, y el archivo queda de la siguiente manera.

```
GNU nano 2.2.6 File: /etc/default/isc-dhcp-server
# Defaults for isc-dhcp-server initscript
# sourced by /etc/init.d/isc-dhcp-server
# installed at /etc/default/isc-dhcp-server by the maintainer scripts
#
# This is a POSIX shell fragment
#
# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPD_CONF=/etc/dhcp/dhcpd.conf
#
# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPD_PID=/var/run/dhcpd.pid
#
# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""
#
# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACES="wlan3"
```

Ilustración 7-31 Archivo de configuración por default de isc-dhcp-server

7.6.3.3.1 Configuración de IP estática de la interfaz inalámbrica

Para que el servidor DHCP funcione correctamente es necesario que la interfaz por la cual escuchara posea una configuración de IP estática y esto ayudara también para levantar el hostapd más adelante. Para esto seguir los siguientes pasos para configurar una IP estática en la interfaz de red.

En el archivo interfaces ubicado en /etc/network/, buscar la configuración de su interfaz en este archivo, comentar o borrar completamente dicha configuración y digitar lo siguiente:

```
auto wlan3
allow-hotplug wlan3
iface wlan3 inet static
    address 192.168.11.1
    netmask 255.255.255.0
#    wireless-mode master
#wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf
up iptables-restore < /etc/iptables.ipv4.nat
```

Ilustración 7-32 Configuración estática de una interfaz inalámbrica

Comentar la línea que inicia con wpa, o borrarla.

Con esto es suficiente para configurar la IP estática de su interfaz de red que servirá como AP, no olvide que la IP de esta interfaz debe coincidir con la del archivo de configuración del servidor dhcp, siendo esta el router o Gateway de esa configuración DHCP.

7.6.3.3.2 Instalando HOSTAPD

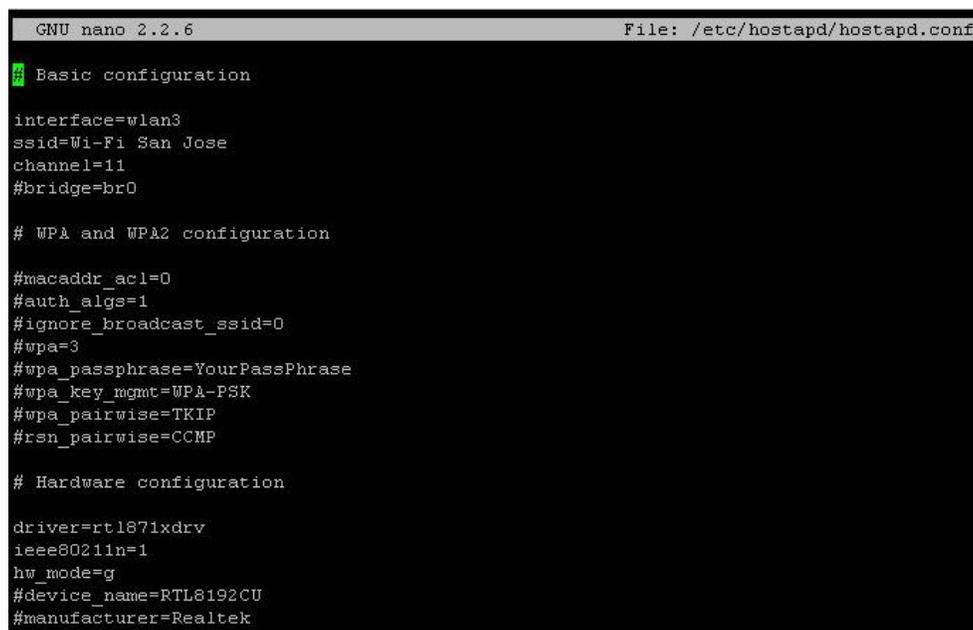
Esta instalación se realizó basada en el chipset de las interfaces de este prototipo, RTL8188, el cual no posee el driver en el paquete que se encuentra en el repositorio oficial por lo cual se instala desde una versión compilada por Jens Segers colaborador de la comunidad de software libre, de la siguiente manera, si se posee otro chipset de igual manera funcionara con esta versión.

```
wget https://github.com/jenssegers/RTL8188-  
hostapd/archive/v1.1.tar.gz  
tar -zxvf v1.1.tar.gz  
cd RTL8188-hostapd-1.1/hostapd  
sudo make  
sudo make install
```

Con esto ya se encuentra instalado el software HOSTAPD.

7.6.3.3 Configurando HOSTAPD

Por defecto la instalación ya tiene una configuración, modificarla de la siguiente manera.



```
GNU nano 2.2.6 File: /etc/hostapd/hostapd.conf  
# Basic configuration  
  
interface=wlan3  
ssid=Wi-Fi San Jose  
channel=11  
#bridge=br0  
  
# WPA and WPA2 configuration  
  
#macaddr_acl=0  
#auth_algs=1  
#ignore_broadcast_ssid=0  
#wpa=3  
#wpa_passphrase=YourPassPhrase  
#wpa_key_mgmt=WPA-PSK  
#wpa_pairwise=TKIP  
#rsn_pairwise=CCMP  
  
# Hardware configuration  
  
driver=rtl871xdrv  
ieee80211n=1  
hw_mode=g  
#device_name=RTL8192CU  
#manufacturer=Realtek
```

Ilustración 7-33 Archivo de configuración de HOSTAPD

Nota: Asegurase de configurar bien la interfaz y el canal que usara para la red AP, no utilice le mismo canal de la red mesh para evitar interferencia, este canal dependerá de su diseño, escoger canales que no se solapen con redes vecinas.

7.6.3.3.4 *Habilitar NAT*

Para esto realizar los pasos del apartado anterior, COMANDOS PARA ACTIVAR NAT, con unos ligeros cambios, en lugar de eth0, escribir la interfaz de red que utiliza para su red mesh en ese dispositivo y en lugar de wlan0 reemplazarlo por la interfaz de red de la interfaz AP. Y luego seguir exactamente igual hasta el final.

7.6.3.3.5 *Arrancar servicios*

```
sudo service isc-dhcp-server start
sudo service hostapd start
```

7.6.3.3.6 *Finalizando configuración del servicio de expansión de zonas Wi-Fi*

Para que todo esto surja efecto desde el arranque del dispositivo y no se tenga la necesidad de arrancar manualmente los servicios ejecutar los siguientes comandos

```
sudo update-rc.d hostapd enable
sudo update-rc.d isc-dhcp-server enable
```

Con esto se iniciarán los servicios desde el arranque de su Raspberry Pi.

7.6.4 Streaming de video en la Raspberry

Habilitar la cámara desde la configuración de Raspbian, desde el inicio del sistema por primera vez o accediendo al menú de configuración con el siguiente comando. Si ya se hizo previamente ignore este paso, y muévase al siguiente.

```
sudo raspi-config
```

Crear un link falso al dispositivo ya que por la versión de Raspbian cambio su manejo. Para solucionar esto ejecute la siguiente línea de comandos.

```
sudo ln -s /usr/include/linux/videodev2.h
```

Ya que se utilizará una herramienta nativa para la generación del streaming no es necesario instalarla, como lo es RASPIVID, pero si hay que instalar vlc para poder enviar dicho streaming en formato RTSP por medio de un puerto específico, para ello instalar vlc de la siguiente manera.

```
sudo apt-get install vlc /usr/include/linux/videodev.h
```

Con esto ya está instalado VLC y se puede empezar a transmitir video, corriendo el siguiente comando.

```
raspivid -o - -t 0 -n -w 640 -h 480 -fps 30 | cvlc stream://stdin --sout '#rtp(sdp=rtsp://:8554/)' :demux=h264
```

7.6.4.1 Configurando Zoneminder.

Configurar *Zoneminder* es relativamente sencillo, pues solo indicaremos por donde y como escuchara el streaming de video, para ello siga los siguientes pasos.

Nota: La instalación de *Zoneminder* queda fuera del contenido de este trabajo, si quiere puede documentarse en la página oficial de este proyecto: <https://zoneminder.com/>

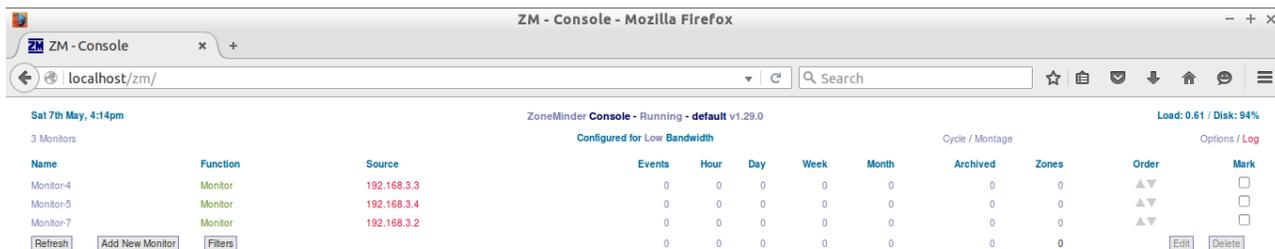


Ilustración 7-34 Interfaz de ZoneMinder

Para agregar un monitor a *Zoneminder*, haga clic en Add New Monitor, lo cual desplegara la siguiente ventana emergente, en la cual se configura como detectar y presentar el streaming de video.

Monitor - Monitor-8	
Name	Monitor-8
Server	None
Source Type	Local
Function	Monitor
Enabled	<input checked="" type="checkbox"/>
Linked Monitors	Monitor-4 Monitor-5 Monitor-7
Analysis FPS	
Maximum FPS (?)	
Alarm Maximum FPS (?)	
Reference Image Blend %ge	6.25% (Indoor)
AlmReflImageBlendPct	6.25%
Triggers	None available

Ilustración 7-35 Ventana emergente para agregar un monitor

Esta es la configuración que trae por defecto ZM, la cual se deberá cambiar por la siguiente, para que acepte el protocolo RTSP. La pestaña General quedara de la siguiente manera. En esta pestaña puede definir el nombre del monitor a su gusto, lo demás si debe estar de la forma en que se muestra.

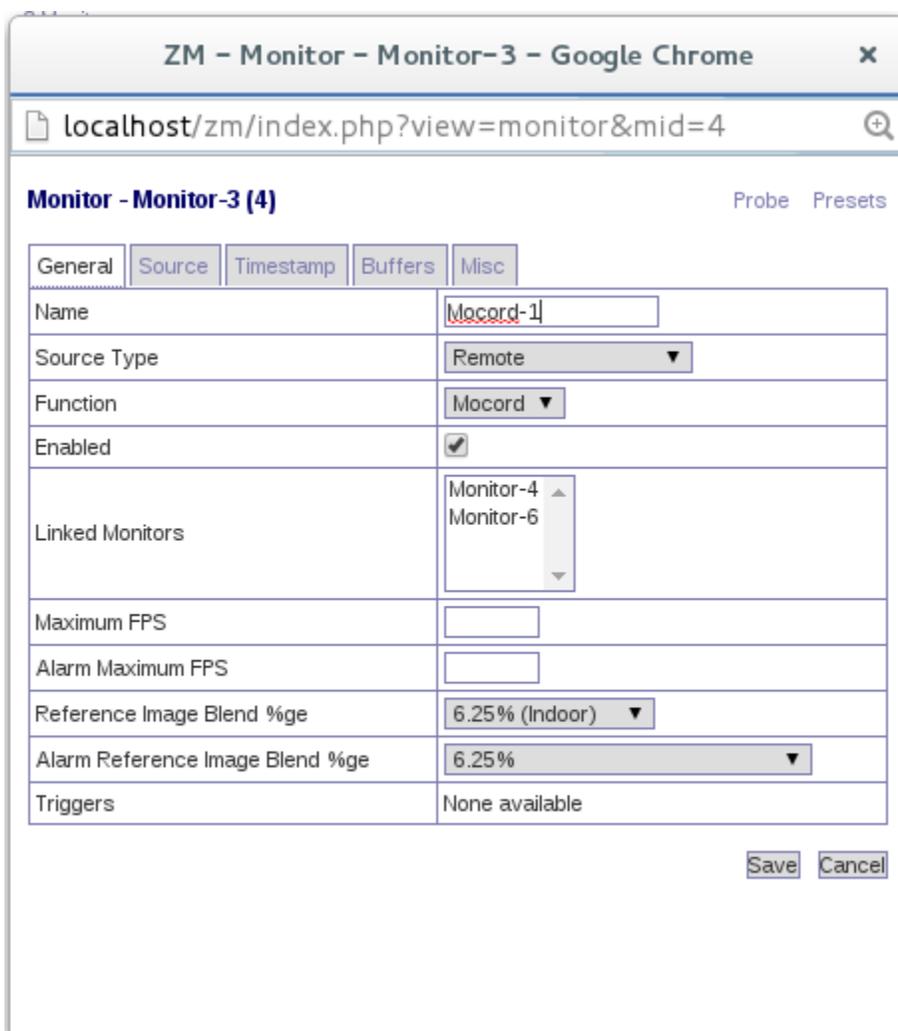
Monitor - Monitor-4 (4)		Probe	Presets
<div style="display: flex; justify-content: space-between;"> General Source Timestamp Buffers Control Misc </div>			
Name	Monitor-4		
Server	None		
Source Type	Remote		
Function	Monitor		
Enabled	<input checked="" type="checkbox"/>		
Linked Monitors	<div style="border: 1px solid gray; padding: 2px;"> Monitor-5 Monitor-7 </div>		
Analysis FPS	<input type="text"/>		
Maximum FPS (?)	<input type="text"/>		
Alarm Maximum FPS (?)	<input type="text"/>		
Reference Image Blend %ge	6.25% (Indoor)		
AlmReflmageBlendPct	6.25%		
Triggers	None available		
<input type="button" value="Save"/> <input type="button" value="Cancel"/>			

Ilustración 7-36 Configuración de un monitor remoto

Almacenar streaming de video en ZoneMinder

ZoneMinder es una herramienta muy completa de videovigilancia, proponderante en el software OpenSource, el cual permite realizar muchas de las tareas de videovigilancia, una de ellas es el almacenamiento de la transmisión de las cámaras, para ello se debe configurar el Monitor en modo Mocord, lo cual le permitirá visualizar y almacenar lo que se está visualizando. Para realizar eso se debe configurar la pestaña General de la siguiente manera. En la cual el único cambio respecto a la imagen anterior

es la opción **Function**, cambiando de **Monitor** (opción por defecto) a **Mocord** ZoneMinder almacena todo el streaming de video que esta recibiendo. La configuración de las otras pestañas es la misma, ya sea un Monitor o un Mocord, la utilización completa de ZoneMinder y todas sus funciones, queda fuera del alcance de este trabajo, pero si se dese documentar más acerca de esta herramienta, su documentación se encuentra en el siguiente enlace: <http://zoneminder.readthedocs.io/en/latest/userguide/index.html>



ZM - Monitor - Monitor-3 - Google Chrome

localhost/zm/index.php?view=monitor&mid=4

Monitor - Monitor-3 (4) Probe Presets

General	Source	Timestamp	Buffers	Misc
Name	Mocord-1			
Source Type	Remote			
Function	Mocord			
Enabled	<input checked="" type="checkbox"/>			
Linked Monitors	Monitor-4 Monitor-6			
Maximum FPS				
Alarm Maximum FPS				
Reference Image Blend %ge	6.25% (Indoor)			
Alarm Reference Image Blend %ge	6.25%			
Triggers	None available			

Save Cancel

Ilustración 7-37 Configuración para guardar streaming de video.

En la pestaña Source realizar las siguientes modificaciones.

Monitor - Monitor-4 (4)		Probe	Presets
General Source Timestamp Buffers Control Misc			
Remote Protocol	RTSP		
Remote Method	RTP/Unicast		
Remote Host Name	192.168.3.3		
Remote Host Port	8554		
Remote Host Path			
Target colorspace	24 bit colour		
Capture Width (pixels)	640		
Capture Height (pixels)	480		
Preserve Aspect Ratio	<input type="checkbox"/>		
Orientation	Normal		
Deinterlacing	Disabled		
Use RTSP Response Media URL (?)	<input type="checkbox"/>		
		Save	Cancel

Ilustración 7-38 Configuración de un monitor remoto

Es posible modificar la resolución a capturar, pero esta debe ser igual a la que se está transmitiendo desde el dispositivo, por cada monitor deberá cambiar la IP, por la IP que utiliza el dispositivo en la interfaz inalámbrica con la cual se conecta a la red *Mesh*.

ZoneMinder Console - Running - default v1.29.0

Configured for Low Bandwidth

Cycle / Montage

Events	Hour	Day	Week	Month	Archived	Zones
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0

Ilustración 7-39 Configuración básica de ZoneMinder

Para una mejor transmisión configurar el uso del ancho de banda que hace Zoneminder en su red, para ello puede hacer clic en LOW y escoger entre LOW, MEDIUM o HIGH. Recomendamos usar HIGH para obtener mejor resultados, pero esto dependerá de cada caso en particular. El uso de ZM u otro software para la videovigilancia queda a discreción del encargado del proyecto.

7.7 Obtención de resultados

Tras la culminación del desarrollo del prototipo se pudieron obtener los datos necesarios para determinar el rendimiento y alcance de este. A continuación, se describirán los aspectos técnicos que más influyen en el prototipo.

Luego de hacer una serie de experimentos con software para medición de tasas de transferencia se logró observar que las tasas reales varían según cuatro factores principales externos, distancia entre nodos, interferencia en la radiofrecuencia y número de saltos entre nodos para establecer un enlace.

7.7.1 Distancia

Para el factor distancia se llevaron a cabo una serie de mediciones a diferentes distancias con el software *Iperf* y los datos obtenidos se muestran en la siguiente tabla. En la tabla se muestra la distancia a la que se hizo la medición y la tasa de transferencia promedio de un total de 5 mediciones por cada distancia. En ciertos tramos de la medición se notó que había interferencia en la radiofrecuencia que estaba utilizando.

Tabla 7-5 Tasa de transferencia de datos por distancia entre nodos

Distancia (metros)	Tasa de transferencia promedio(Mb/s)
5	18
10	14.8
15	11.7
20	6.8
25	2.7
30	1.23
35	0.450

Como se puede observar en las mediciones las tasas de transferencia bajan considerablemente con la distancia, aun si estas son cortas, además se pudo determinar que **los nodos no pueden estar a más de 25 metros** para que haya una comunicación aceptable entre ellos.

7.7.2 Interferencia en la radiofrecuencia

La **interferencia en la radiofrecuencia** como factor determinante se logró observar por medio de una prueba en la que se tenían dos nodos en un cuarto cerrado de 4x4 metros y se lograba una tasa de transferencia de 17.8 Mb/s, luego se le agrego una señal inalámbrica generada por un *Router* inalámbrico en el mismo canal que el que se utilizaba para hacer la comunicación entre nodos y la tasa de transferencia bajo a 12.8 Mb/s.

7.7.3 Saltos entre nodos

Los saltos entre nodos son el otro factor que afecta la tasa de transferencia en el envío de datos. Se pudo observar que la tasa de transferencia bajaba a aproximadamente la mitad luego de cada salto y para que haya un salto se notó que se necesitaba una distancia de al menos 17 metros y la tasa de transferencia que se logra a esa distancia es de alrededor de los 6 Mb/s, con esto se pudo determinar que no se pueden dar más de dos saltos si se requiere una transmisión aceptable.

7.7.4 Número de clientes por AP

Otro dato muy importante era el conocer la cantidad de clientes que puede soportar cada AP para ello se fueron conectando dispositivos inalámbricos a un solo AP hasta que este dejó de responder, el número recomendado de clientes por nodo es de 20.

7.7.5 Tasa de transferencia en el Streaming de video

Tasa de transferencia del Streaming de video, el Streaming de video se probó con dos protocolos de transferencia HTTP que trabaja a través de TCP y con RTP que trabaja con UDP, en la siguiente tabla se muestran las tasas de transferencia promedio que se lograron con cada protocolo y con las diferentes resoluciones que se utilizaron.

Tabla 7-6 Consumo de red acorde a la resolución de la cámara

Resolución	Tasa de transferencia/HTTP	Tasa de transferencia/RTP
640x480	8Mbps	3Mbps
720x480	14Mbps	6Mbps
1080x720	25Mbps	13Mbps

8 Factibilidades

8.1 Técnica

Con el desarrollo del prototipo funcional se ha demostrado la factibilidad técnica del proyecto bajo estas características:

- 4 nodos involucrados en el sistema.
- 3 nodos prestando el servicio de videovigilancia a través del envío de fotogramas a un intervalo de 30 marcos por segundo, con una resolución VGA de 640x480 pixeles y transfiriendo por un protocolo RSTP.
- 3 nodos prestando acceso a internet con la posibilidad de agregar hasta 20 clientes por nodo y compartiendo entre todos el ancho de banda que ofrece el ISP de la alcaldía.
- Todos los nodos interconectados a través de una red Mesh con una tasa de transferencia de 18Mb/s de carga y 54 Mb/s de descarga en cada enlace directo entre nodos en un ambiente con poca interferencia y a una distancia menor a los 20 metros.

Los nodos están físicamente distribuidos de modo que dos nodos se conectan directamente (nodos intermedios) con el nodo frontera y un cuarto nodo se comunica con cualquiera de los dos nodos intermedios para llegar al nodo frontera, y del nodo frontera llega la comunicación al centro de vigilancia, tal como está plasmado en el diseño del prototipo.

Del prototipo se obtuvo el siguiente funcionamiento:

Tasa de transferencia red Mesh, la tasa de transferencia del enlace entre dos nodos directamente enlazados fue de 18Mbps de carga y 54 Mbps de descarga, pero esta velocidad se reduce a la mitad por cada salto que da el mensaje para llegar a su nodo destino además de las pérdidas generadas por las distancias entre enlaces., de modo que entre el nodo frontera y el nodo más alejado físicamente la tasa de transferencia fue de 6Mbps/20Mbps de carga y descarga respectivamente, porque la conexión necesitaba pasar por un solo nodo intermedio, pero si se necesitase pasar por dos el resultado fue de 3.1Mbps/11.5Mbps de carga y descarga respectivamente de tasa de transferencia y así sucesivamente a medida se van agregando saltos.

Tasa de transferencia del Streaming de video fue de 3Mb/s en promedio bajo las características de una transferencia de 30 fotogramas por segundo, bajo a una resolución de 640x480 pixeles, un formato de compresión H.264 y realizando la transferencia a través del protocolo RSTP, pero esta tasa de transferencia puede fluctuar según la cantidad de colores que se presenten en la captura e incrementar la tasa de transferencia o se puede llegar a reducir si se presenta una captura oscura o con pocos colores, aunque se logró observar que si el ancho de banda no es suficiente, el Streaming baja su tasa de transferencia.

La **tasa de transferencia del servicio de acceso a internet** se ve limitada directamente a lo que el ISP de la alcaldía ofrece, siendo esta una tasa de 4Mb/s que se debe compartir entre tantos clientes de acceso a internet tenga el sistema y tantos usuarios

de la alcaldía estén conectados, para cada nodo que presta el servicio de acceso a internet el límite de clientes para los que puede funcionar es de hasta 20, esto solo para el funcionamiento correcto del nodo pero el buen funcionamiento de la red de acceso a internet también depende de que tanto se esté utilizando el ancho de banda total del ISP.

Uniendo estos datos para cada nodo se obtuvo la tabla de consumo de tasa de transferencia siguiente:

Tabla 8-1 Tasas de transferencia utilizadas en el prototipo

Descripción nodo	Tasas de transferencia (Mb/s)			
	Streaming de Video	Acceso a internet	Total consumo	Conexión centro de monitoreo
Nodo frontera, recibe el tráfico de todos los nodos (3) pero directamente solo tiene dos conectados.	9	4	13	100
Nodo intermedio*, recibe el tráfico del nodo más alejado al nodo frontera y genera el propio.	6	4	10	14.8
Nodo más alejado al nodo frontera, solo genera su propio tráfico.	3	4	7	6

El instrumento tecnológico demostró que el uso de las redes Mesh es viable para prestar los servicios de videovigilancia y acceso a internet bajo las características en las que se desarrolló el instrumento, pero no es útil para un alcance más extenso porque se encontró con las limitantes de la distancia entre nodos, la interferencia de la radio frecuencia por la que se comunican y las bajas tasas de transferencia que se puedan alcanzar. Estas limitantes están directamente asociadas al tipo de interfaces de red que se utilizaron, pero para un funcionamiento óptimo se deben utilizar interfaces tipo AC y antenas direccionales para la red Mesh y omnidireccionales de alta potencia para prestar el servicio de acceso a internet.

Para **guardar el streaming de video** se necesitara de un disco duro que sea capaz de guardar días, semanas incluso más de un mes de video de las 3 cámaras que conforman el nodo. Es por ello que se optó por el disco duro seagate de 4TB, el cual está capacitado para guardar 176 días de video continuo con una resolución de 704x480 utilizando el codex H.264 mismo que se ocupa en el prototipo. Si este dato lo divididos entre las 3 cámaras, nos da un total de 58 días de video continuo para las 3 cámaras y es un valor más que razonable para establecer una política de almacenaje por parte de la alcaldía. **(Seagate, 2016)**

8.2 Económica

8.2.1 Prototipo

En el aspecto económico es importante conocer y puntualizar, el costo total del prototipo, así como también el costo total de un nodo Mesh para poder adherirse al prototipo como tal.

Nodo externo

Tabla 8-2 Costo de nodo externo

Dispositivo	Cantidad	Costo	Sub total
Raspberry Pi 2 B	1	\$50.00	\$50.00
Adaptador Wireless 802.11n	2	\$10.00	\$20.00
Micro sd de 8 Gb clase 10	1	\$5.00	\$5.00
Adaptador de corriente de 2 Amperios	1	\$5.00	\$5.00
Cámara	1	\$35.00	\$35.00
Case	1	\$25	\$25
Total			\$140.00

Fuente: Los precios de referencia han sido tomados de eBay.

Los datos planteados en el cuadro anterior, nos muestran el costo total que tendrá cada nodo que este transmitiendo el Streaming de video, así como también estará brindado Wi-Fi a las personas que lo deseen. De estos nodos según el prototipo que se desarrolló se necesitan 3 lo cual nos da un monto de \$420.00.

Nodo frontera

Tabla 8-3 Costo de nodo frontera

Dispositivo	Cantidad	Costo	Sub total
Raspberry Pi 2 B	1	\$50.00	\$50.00
Adaptador Wireless 802.11n	1	\$10.00	\$10.00
Micro SD de 8 Gb clase 10	1	\$5.00	\$5.00
Adaptador de corriente de 2 Amperios	1	\$5.00	\$5.00
Case de plástico para Raspberry PI	1	\$5	\$5
Total			\$75.00

Fuente: Los precios de referencia han sido tomados de eBay.

Según los datos del cuadro anterior el nodo frontera necesitara de una inversión de \$75.00, si a esto le sumamos \$420.00 de los nodos externos obtenemos un total de \$495.00 para la adquisición de todo el hardware necesario para la creación del prototipo.

8.2.2 Centro de monitoreo

Para el centro de monitoreo el único gasto al cual debe incurrir la alcaldía es en la compra de un disco duro, en dicho disco duro se guardará el streaming de video que se esté transmitiendo por cada nodo del prototipo.

Para el almacenamiento se recomienda un disco duro Seagate 4tb 3.5 (stbd4000400) cuyo precio en ebay.com es de \$162.00. **(Ebay, 2016).**

8.2.3 Alcaldía

Conociendo los costos que totales que se tendrían en el prototipo también es importante indagar si la alcaldía cuenta con los recursos necesarios para poder realizar dicha inversión, para ello nos guiaremos de los datos económicos que percibe la alcaldía a través del FODES (Fondo de Desarrollo Económico y Social de los Municipios de El Salvador). Dicho fondo está destinado un 75% para la inversión y un 25% en la administración el presupuesto, el monto que recibió la alcaldía de San José Las Flores en 2014 es de \$458,066.79 de los cuales \$343,550.09 fueron destinados para inversión en todo el municipio (**FODES, 2014**).

Si los \$343,550.09 los dividimos de forma equitativa entre los 12 meses del año nos da un total de \$28,629.17 y esto lo dividimos entre 30 días nos da un total de \$954.30 con lo cual podemos observar que el prototipo puede ser comprado con el dinero que está destinado para ser invertido en un día.

8.2.4 Costo de oportunidad

Conociendo el monto total del prototipo y que además la alcaldía cuenta con los recursos necesarios para la adquisición de los dispositivos se planteara el costo de oportunidad que este proyecto generaría.

San José Las Flores es un municipio pequeño y además muy seguro, pero nunca está de más ser previsoros y tomar medidas de seguridad antes de que sea un problema, ya que se encuentra en un departamento de Chalatenango en el que solo de Enero a Agosto de 2015 se reportaron 69 homicidios, 206 hurtos y 44 robos, según datos oficiales

de la PNC (Sub-Dirección de Seguridad Pública, 2015). Además se tiene la certeza de que la videovigilancia puede ser un factor de minimización de delitos y facilitador de capturas, como se ha obtenido por parte de los datos de la PNC de capturas logradas en San Salvador por la intervención del sistema de videovigilancia (Sub-Dirección de Seguridad Pública, 2015) que revelan hasta 146 detenciones sólo en 2014, además de afirmar que cumplen un papel preventivo.

Teniendo en cuenta que una solución común por parte de las municipalidades para el problema de seguridad es contratar agentes municipales, se podría plantear un supuesto en el que se puedan llegar a necesitar 2 agentes municipales si no se tuviese prevención a la delincuencia, bajo ese supuesto se tiene que estos ganan alrededor de \$346.50 al mes en alcaldías localizadas en zonas cercanas a San José Las Flores como es el caso de la alcaldía de Nueva Concepción (Alcaldía Municipal de Nueva Concepción, 2016) haciendo un valor de \$693 mensuales si se llegaran a necesitar. Este supuesto está sujeto al hecho de que el uso de los agentes se previno, no a que el sistema pueda ser sustituto de estos si fueran necesarios.

Respecto a prestar el servicio de acceso a internet, la alcaldía ya cuenta con un servicio de acceso a internet que según el director de proyectos de la alcaldía se encuentra subutilizado la mayor parte del tiempo, debido a que solo se utiliza para prestar funciones básicas como recepción y envío de documentos por parte del personal de la alcaldía. Si se tiene en cuenta que el costo por cada MB de navegación utilizado es de \$0.0067 según

Claro y Tigo para planes prepago de 150MBs con duración de un día a un costo de 1\$ diario, y el sistema está diseñado para permitir el consumo de hasta 4Mb/s, suponiendo que la alcaldía utiliza permanentemente 1Mb/s de ancho de banda, quedan libres 3Mb/s haciendo 259,200 Mb/s de navegación en un día, con lo que en un supuesto en el que se utiliza el ancho de banda al máximo por parte de los clientes del sistema, los habitantes, se podrían suplir hasta 1,728 paquetes de navegación. Sin embargo el sistema solo está preparado para suplir nominalmente hasta 60 usuarios, haciendo un ahorro de hasta \$60 por día en el entendido de que solo 60 clientes se conectan al sistema, y hasta \$21,600 en un año. Pero al tratarse de un sistema en el que los usuarios conectados van rotando y que las tasas de transferencia que pueden alcanzar son mayores que lo que pueden obtener con paquetes de navegación móvil, el ahorro podría llegar a ser aún mayor.

Además de los datos antes determinados se estima que el tiempo de vida útil del prototipo en el peor de los casos es de 1 año cuyo monto asciende a los \$495.00, se calculara el costo de oportunidad.

Costo anual del prototipo: \$495.00.

Costo de disco duro para almacenamiento: \$162.00.

Costo anual de dos agentes del CAM: \$8,316.

Ahorro anual en servicio de acceso a internet: \$21,600

Con estos datos se puede determinar que tan solo en el primer año de vida del sistema se pueden llegar a tener beneficios de hasta \$29,259.

8.3 Operativa

Para la construcción del prototipo de red planteado en este documento se requerirá de una serie de perfiles de recurso humano necesarios para desarrollarlo de forma correcta, en la siguiente tabla se describirán los puestos y las funciones sobre el desarrollo y puesta en marcha del prototipo.

Tabla 8-4 Operadores involucrados en el sistema

Puesto	Descripción
Técnico informático	Técnico informático con conocimientos básicos sobre redes informáticas. Sus funciones sobre el prototipo serán: Conectar todos los componentes de hardware que el prototipo necesita. Además, deberá seguir de manera ordenada el manual de desarrollo brindado en el presente documento, en el cual se detalla como configurar todo el software necesario para el funcionamiento óptimo del prototipo.
Técnico electricista	Sus funciones serán la creación de los puntos de corriente eléctrica donde se deberán conectar las fuentes de alimentación de todos los nodos del prototipo.
Encargado del centro de monitoreo	Sus funciones serán la de observar el streaming de video en el centro de monitoreo y en caso de ser necesario realizar copias de seguridad del streaming de video

	guardado en el disco duro del centro de monitoreo destinado para esta tarea.
--	--

En la alcaldía de San José Las Flores la cual es nuestro caso de estudio los puestos antes descritos ya se cuentan en el personal disponible por la alcaldía, con esto se tienen todos los insumos necesarios para la elaboración y puesta en marcha del prototipo con lo que se determina que este proyecto es totalmente factible.

9 Conclusiones

La aplicación de redes Mesh para videovigilancia y expansión de zonas Wi-Fi se demostró que es completamente factible basados en el prototipo realizado en San José Las Flores, Chalatenango.

La videovigilancia aporta una percepción de seguridad a los habitantes de la comunidad de San José Las Flores, Chalatenango.

El uso de tecnologías como las redes mesh hacen asequibles servicios como videovigilancia y acceso a internet a comunidades que no cuentan con grandes recursos económicos, optimizando la utilización de recursos y la distribución de los mismos.

La innovación tecnológica es tal que, a la culminación de este trabajo de graduación ya se cuentan con tecnologías superiores a las utilizados en el desarrollo del prototipo tales como dispositivos Raspberry pi 3 que ofrece mejores prestaciones y protocolos más avanzados como 802.11AC, respaldando la idea del uso de tecnologías económicas y robustas en el uso de redes mesh para la prestación de servicios como videovigilancia y acceso a internet público.

10 Recomendaciones

Como se pudo observar en el desarrollo del proyecto, la tecnología de red Mesh es totalmente funcional para prestar los servicios de videovigilancia y acceso a internet que inicialmente se plantearon al diseñar el proyecto. Seguir al pie de la letra el diseño y las instrucciones de configuración garantizan el funcionamiento del sistema, teniendo en cuenta que los factores distancia e interferencia son los que podrían generar degradación en el sistema. Por ello hacer que los enlaces directos entre nodos no tengan más 15 metros de distancia, que no haya redes en el mismo canal de radiofrecuencia y que los enlaces entre nodos sean directamente visibles, que no haya ningún cuerpo o estructura que interfiera el enlace de la comunicación, es fundamental para un correcto funcionamiento del sistema.

Para que el sistema sea más robusto y se puedan soportar enlaces de mejor calidad, se debe utilizar interfaces con el protocolo 802.11AC y antenas direccionales para soportar la red Mesh. Con esta mejora se podrían agregar más cámaras al sistema, o utilizarse mejores resoluciones en las cámaras ya existentes.

Para hacer más robusto el sistema en el servicio de acceso a internet, se deben agregar nuevos servidores que presten el servicio, como lo podrían ser vecinos aledaños a las zonas en las que funcione el sistema que compartan su acceso a internet y de este modo hacer que el ancho de banda disponible sea aún mayor e incluso los clientes puedan

tener una salida a internet más corta si se encuentran más cerca del servidor de acceso a internet de un vecino que el de la alcaldía.

11 Lista de referencias

(Flickenger, 2008): Flickenger, Rob. (2008). Redes inalámbricas en los países en desarrollo. Gran Bretaña: Hacker Friendly LLC.

(Todd, 2007): Todd, Lammle. (2007). CCNA Exploration 4.0 Aspectos básicos de networking. 4º Edición.

(Sanchez, Rony 2012): Sánchez Morales, Rony Stalyn. (2012). Servicio de respuesta de voz iterativa para el Hospital Nacional Rosales. Tesis de ingeniería eléctrica, Universidad de El Salvador, San Salvador.

(Doumenc, Hélène 2008): Doumenc, Hélène. (2008). Estudio comparativo de protocolos de encaminamiento en redes VANET. Proyecto fin de carrera Facultad de Informática, Universidad politécnica de Madrid, Madrid, España.

(Romero, Edmon 2010): Romero Moreno, Edmon Osmani. (2010). Diseño de una red inalámbrica Wi-Fi para los centros escolares del municipio de Berlín. Tesis de ingeniería eléctrica, Universidad de El Salvador, San Salvador.

(Colocho, Luis y Tobías, Román 2011): Colocho Susaña, Luis Alonso y Tobías Vides, Román Abad. (2011). Telefonía inalámbrica y red de acceso a Internet

para los Municipios de Salcoatitán, Juayúa, Apaneca y Ataco. Tesis de ingeniería eléctrica, Universidad de El Salvador, San Salvador.

(Arnoldo, Pablo 2010): Arnoldo, Pablo. (2010). Diccionario Geográfico de El Salvador. San Salvador: Instituto Geográfico Nacional.

(DYGESTIC, 2007): DYGESTIC. (2007). VI Censo de población y V de vivienda.

(FISDL, 2006): FISDL. (2006). San José Las Flores. Consultado el 17 de Mayo de 2015 a través de <http://goo.gl/Uspbje>

(Wikipedia vigilancia, 2015): Wikipedia. (2015). Vigilancia. Consultado el 18 de Mayo de 2015 a través de <https://goo.gl/Ycmwf3>

(Wikipedia, Freifunk 2015): Wikipedia. (2015). Freifunk. Consultado el 13 de Mayo de 2015 a través de <http://goo.gl/Uap0hu>

(FISDL, 2005): FISDL. (2005). Mapa Nacional de Extrema Pobreza. Consultado el 18 de Mayo de 2015 a través de <http://goo.gl/tLR6h2>

(El diario de Hoy, 2015): El diario de Hoy. (2015). Sistema de videovigilancia opera a medias en La Unión. Consultado el 8 de Mayo de 2015 a través de <http://goo.gl/qpWCJt>

(FISDL, 2009): FISDL. (2009). Estado del Desarrollo humano en municipios de El Salvador 2009. Consultado el 7 de Mayo de 2015 a través de <http://goo.gl/jzCbv5>

(La prensa Gráfica, 2015): La Prensa Gráfica. (2015). Sistema de video vigilancia costará entre \$30 y \$40 mill: Bukele. Consultado el 17 de Mayo de 2015 a través de <http://goo.gl/LLfSwW>

(Wikipedia ISP, 2016): Wikipedia. (2016). Proveedor de servicios de internet. Consultado el 6 de marzo de 2016 a través de https://es.wikipedia.org/wiki/Proveedor_de_servicios_de_Internet

(Wikipedia router, 2016): Wikipedia. (2016). Router. Consultado el 6 de marzo de 2016 a través de <https://es.wikipedia.org/wiki/Router>

(Wikipedia Ethernet, 2016): Wikipedia. (2016). Ethernet. Consultado el 6 de marzo de 2016 a través de <https://es.wikipedia.org/wiki/Ethernet>

(FODES, 2014): FODES. (2014). Documento consultado el 8 de Mayo de 2015 a través de <http://goo.gl/rJJ7iM>

(Alcaldía Municipal de Nueva Concepción, 2016): Documento institucional de Alcaldía Municipal de Nueva Concepción. (2016). Estructura presupuestaria año 2016. Chalatenango.

(Sub-Dirección de Seguridad Pública, 2015): Documento institucional, Personas detenidas utilizando tecnología de video vigilancia en San Salvador. Policía Nacional Civil, División de emergencias 911, San Salvador.

(Ebay, 2016): Ebay. (2016). Consultado el 23 de Mayo de 2016 a través de <http://www.ebay.com/itm/NEW-Seagate-4TB-3-5-Inch-Internal-Desktop-Hard-Disk-Drive-Kit-STBD4000400-/151165694756?hash=item23322d7324:g:PMUAAOxy4t1Sg8j9>

(Seagate, 2016): Seagate. (2016). Consultado el 23 de Mayo de 2016 a través de <http://www.seagate.com/la/es/tech-insights/how-much-video-surveillance-storage-is-enough-master-ti/>

12 Anexos

12.1 Anexo 1

Instalar sistema operativo (Raspbian Wheezy)

Recursos necesarios:

- Tarjeta micro SD: Es recomendable una tarjeta clase 10 de al menos 8 GB, si no se dispone de este modelo puede utilizar una de clase 4 con capacidad mínima de 4GB.
- Una computadora con lector de tarjeta micro SD y sistema operativo Windows 7 en adelante: Si no dispone de lector de tarjetas micro SD utilice un adaptador de tarjetas SD a USB.

Software necesario

- Archivo con la imagen de Raspbian Wheezy
- Win32 Disk Imager versión 0.9.5

Paso 1: Descargar la imagen y descomprimir

Ingrese a la siguiente URL: <https://www.raspberrypi.org/downloads/raspbian/> y descargue al archivo de la imagen de Raspbian en su ordenador, una vez descargado descomprima el archivo y guárdelo en una ubicación conocida para su uso posterior.

Paso 2: Instalar Win32 Disk Imager

Descargar el programa Win32 Disk Imager de la URL: <https://sourceforge.net/projects/win32diskimager/>, en la página presione el botón descargar, como se ve en la imagen



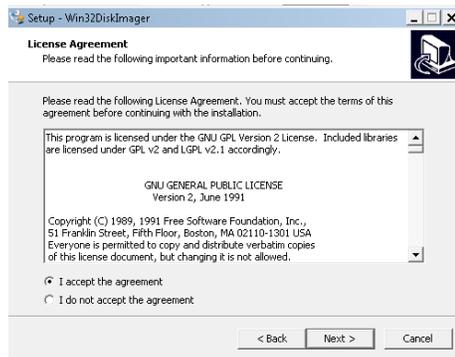
Abra el archivo descargado, de preferencia ejecútelo como administrador.



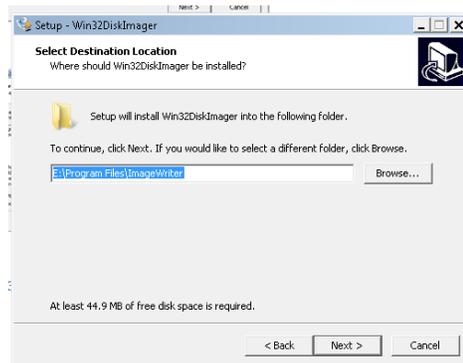
En la primera pantalla solo se necesita continuar al siguiente paso presionando el botón "Next".



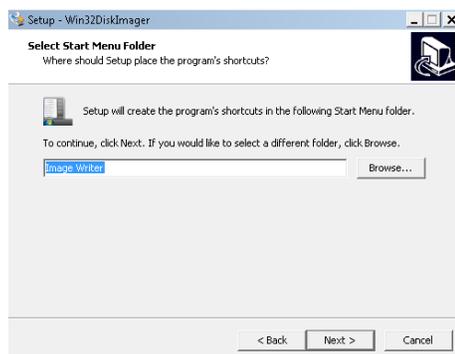
Presione aceptar a los términos de instalación del Software y continuar.



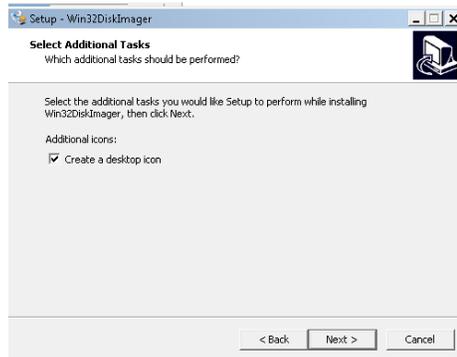
Escoja el directorio en el que va a instalar el programa, se puede dejar con el directorio por defecto.



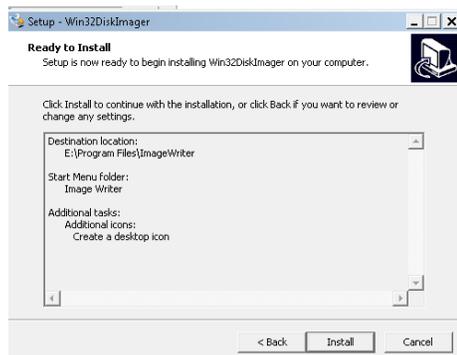
Escoja en que menú se va a mostrar el programa, se puede dejar con el menú por defecto.



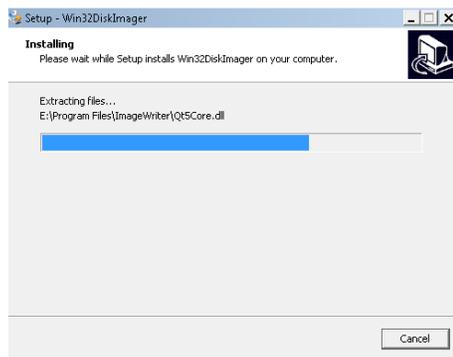
Escoja si dese tener un acceso directo en el escritorio.



Luego de estos pasos se mostrará una pantalla con la confirmación de las preferencias escogidas, presione instalar para proceder con la instalación.



Se mostrará una barra de estado con el proceso de la instalación, espere a que termine.

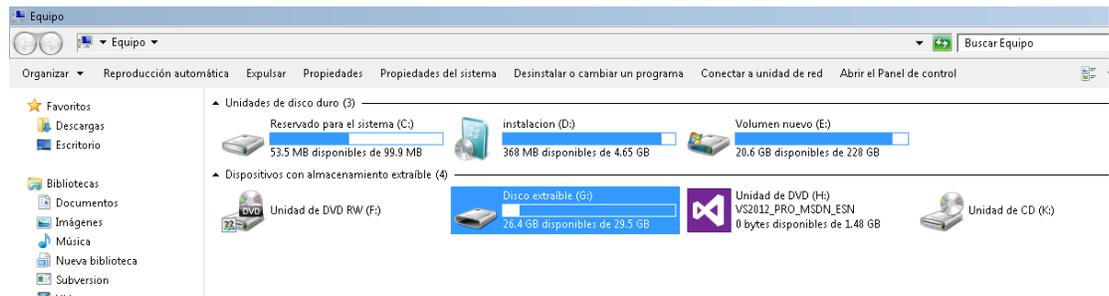


Se mostrará una pantalla con la confirmación de la instalación en la que se podrá escoger si se desea leer el archivo de la post instalación o si lo desea ejecutar directamente, escoja lo que desea hacer y presione finalizar.



Paso 3: Montar la imagen en la memoria SD

Inserte la memoria SD en su equipo, ya sea con el lector SD o con su adaptador USB e identifique la unidad que se le asigne. Para conocer la unidad entrar en equipo e identificar la unidad que le corresponde a la memoria SD tal como se muestra en la imagen. En “Equipo” (Clic en inicio y luego “Equipo”) podrá observar todos sus medios de almacenamiento interno y externos



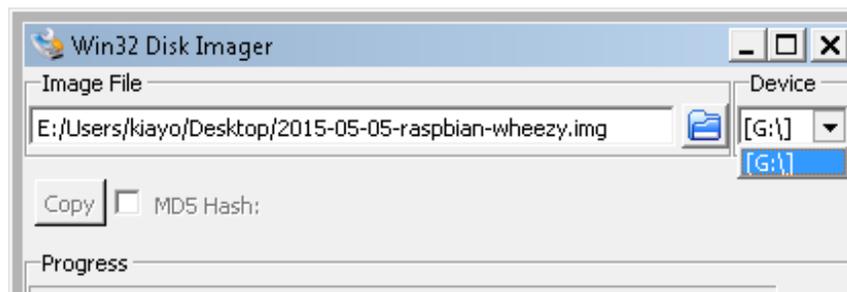
Ejecutar Win32 Disk Manager.

Clic en la imagen de la carpeta.

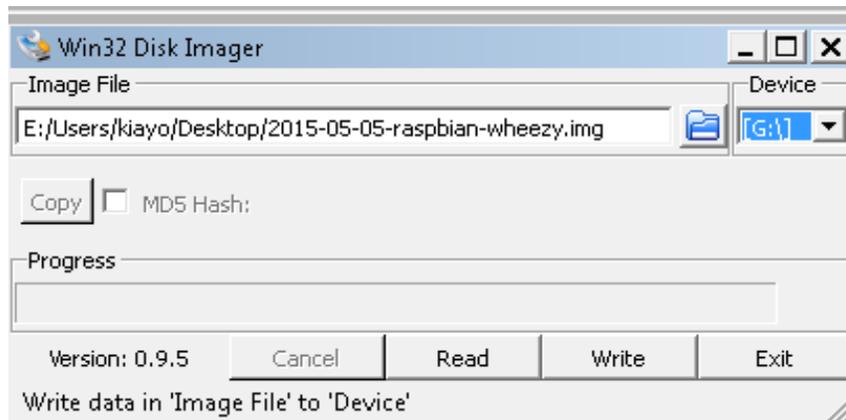


En el recuadro emergente busque el archivo de la imagen de Raspbian que descargo y luego clic en “abrir”.

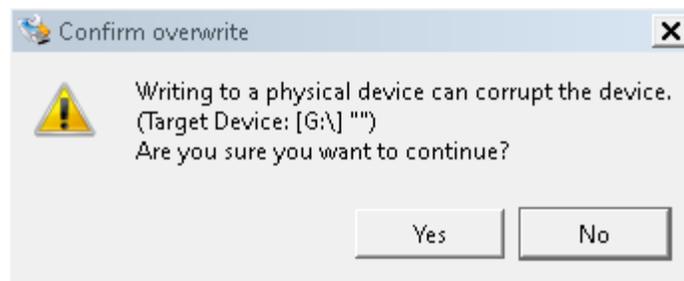
Debajo de la opción “Device” despliegue la lista de dispositivos disponibles y seleccione la letra que identifica a la memoria SD previamente reconocido; Si su tarjeta no aparece en el listado, extráigala y vuelva a insertarla, si el problema persiste cambie el adaptador o asegúrese que la tarjeta está en buen estado.



Una vez seleccionado el dispositivo correcto clic en “Write”.

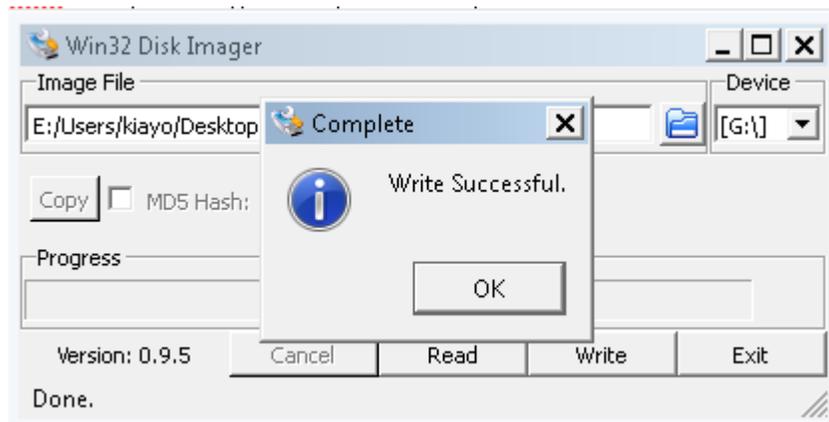


En la advertencia que aparecerá haga clic en “Yes” para proceder con la grabación de la imagen, esta advertencia sirve para asegurarse que es el dispositivo correcto el seleccionado y no tiene ningún tipo de error en el proceso.



La duración de esta operación dependerá de las capacidades de su computadora, pero en promedio tarda entre 20 a 45 minutos.

Al finalizar la grabación de la imagen verá un mensaje como el siguiente indicando que su grabación ha culminado con éxito. La memoria micro SD ahora contiene el sistema operativo necesario para la Raspberry Pi 2.



12.2 Anexo 2



ALCALDÍA MUNICIPAL SAN JOSÉ LAS FLORES

DEPARTAMENTO DE CHALATENANGO, EL SALVADOR

Barrio El Centro, San José Las Flores, Chalatenango, Telefax 2354-9005. Correo Electrónico Secretaría: alcaldiasanjoselasflores@gmail.com



San José Las Flores, 20 de mayo de 2016.

A QUIEN CORRESPONDA

Presente

Reciba un cordial Saludo esperando se encuentre cosechando éxitos en las labores que día con día realiza.

Por este medio se hace constar que como institución no podremos asistir a la Defensa pública de Tesis que se desarrollara este Sábado 21 de Mayo, por motivos de fuerza mayor, pero damos fe de que los Jóvenes Heber Jonathan López Guardado, Fernando José Agurto Armero y Mario David Hernández Rivas, Realizaron la demostración y explicación del funcionamiento de la aplicación de redes mesh, que contempla un sistema de video vigilancia y ampliación de zonas wifi. Como municipalidad vemos de mucho interés este tipo de proyectos que ayudan a la mejora de la seguridad, el acceso al internet, la reducción de costos y la facilidad de su implantación y expansión.

Sin más que agregar me suscribo a usted no sin antes hacer mis muestras de consideración y estima.

Atentamente



José Felipe Tobar Arce
Alcalde Municipal

