 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-27

**Diseño e implementación de un radio enlace para proveer de servicio de internet inalámbrico gratuito a los habitantes del Barrio Trece de Noviembre de la comuna 8 de Medellín; con autenticación en un portal cautivo.**

Renee Alejandro Díaz Martínez

Wilmar Arley Gonzalez Sierra

Ingeniería en Telecomunicaciones

Fabio León Suárez A.

**INSTITUTO TECNOLÓGICO METROPOLITANO**

**Febrero 2017**

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

## RESUMEN

---

Las redes WLAN son tecnologías que brindan la posibilidad de comunicación sin necesidad de cables o medios físicos, sin lugar a dudas esto brinda beneficios como movilidad, diseño de nuevos espacios, comodidad, escalabilidad, entre otros. Pero en Colombia y en Medellín específicamente, existen zonas desconectadas aún a nivel urbano. El Barrio Trece de Noviembre en la actualidad no cuenta con conexión a internet debido a que es un sector de estrato bajo, y además, por ser una zona con características geográficas que dificultan el despliegue de infraestructuras físicas. El llevar el servicio de internet de forma inalámbrica y gratuita, contribuye a reducir en gran parte la brecha tecnológica en la que viven los habitantes del sector, en pleno siglo XXI. Por eso, el presente proyecto busca por medio de las tecnologías WLAN, ofrecer a los habitantes del Barrio 13 de Noviembre la posibilidad de contar con conexión a Internet de forma gratuita. Para lograr esto, se realizará levantamiento de información del entorno geográfico donde se encuentra asentada esta comunidad, para así tener una visión amplia del rango de cobertura y/o alcance posible con un radio enlace; se pretende hacer una simulación con software especializado (Radio Mobile), para elegir los equipos necesarios; para poder hacer un buen uso del servicio de internet y garantizar la seguridad, se implementará el uso de un portal cautivo y se realizan pruebas de rendimiento. Se implementó un radio enlace que permite brindar Internet inalámbrico gratuito a un barrio en la periferia de Medellín. Los usuarios pueden acceder a un servicio de transferencia de archivos después de autenticarse en un portal cautivo sobre Pfsense.

**Palabras claves:** Brecha tecnológica, Calidad de vida, Ftp, Internet, Portal Cautivo, Radio-enlace, Trece de Noviembre, Wi-fi.

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

## RECONOCIMIENTOS

---

En primer lugar queremos agradecer a Dios por darnos la oportunidad de trabajar en este proyecto, que permite dar un aporte social a una comunidad tan necesitada como los son los habitantes del Barrio 13 de Noviembre.

Queremos agradecer también a los Profesores: Fabio Leon Suárez y Pedro Guerrero, por su orientación y asesorías; a nuestras familias por el apoyo, y por motivarnos a seguir adelante.

Gracias también al Presidente de la Junta de Acción Comunal, Ignacio Arango, por la dedicación y el acompañamiento que nos brindó; su ayuda con toda la información del Sector a intervenir, fue fundamental.

A todos muchas gracias ¡

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

# ACRÓNIMOS

---

*AIRLINK* Herramienta de simulación de Radio Enlaces, Propiedad de Ubiquiti.

*AIRVIEW* Herramienta de Análisis espectral de los equipos Nano Station M.

*ALIASES:* Puede un puerto, un grupo de puertos, una dirección IP o un grupo de direcciones ip, toda una red o un grupo de redes.

*ICMP* Protocolo de mensajes de control de internet

*FTP* Protocolo de transferencia de archivos

*FREEBSD* Es un avanzado Sistema Operativo derivado de BSD y de propiedad de UNIX

*LOS* Hace referencia a que las antenas que intervienen en un radio enlace tienen visión directa

*PING* Utilidad diagnóstica en redes de computadores que comprueba el estado de la comunicación

*POE* Tecnología que incorpora la alimentación eléctrica en infraestructura de redes.

*SNR* Relación señal a ruido en un sistema

*WIFI* Mecanismo de conexión de dispositivos electrónicos de forma inalámbrica

*WLAN* Red de área local cuya interconexión se realiza de forma inalámbrica

 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

## Tabla de Contenido

<b>1. INTRODUCCIÓN .....</b>	<b>6</b>
1.1 Justificación.....	6
1.2 Planteamiento del problema .....	8
1.3 Objetivos .....	9
1.4 Organización del informe.....	9
<b>2. MARCO TEÓRICO .....</b>	<b>10</b>
2.1. Redes Inalámbricas .....	10
2.1.1 Aspectos relacionados con la Capa Física WLAN .....	10
2.1.2 Futuros Estándares en Velocidad de Transmisión.....	11
2.1.3 Aspectos Relacionados con la Capa de Enlace de WLAN .....	11
2.2 Seguridad en las Redes WLAN.....	12
2.2.1 Mecanismo de seguridad WEP .....	12
2.2.2 WPA y WPA2.....	12
2.3 Redes Wi-Fi. ....	13
2.4 Banda de frecuencias no licenciadas en Colombia. ....	13
2.5 Radio Enlaces .....	13
2.6 Topologías de red para entornos inalámbricos.....	14
2.6.1 Punto a Punto .....	14
2.6.2 Punto a Multipunto.....	14
2.6.3 Multipunto a Multipunto .....	14
2.7 Zonas de Fresnel.....	14
2.8 Qué es un Portal Cautivo?.....	15
2.8.1 Tipos de Portal Cautivo .....	15
2.9 Instalación y Configuración del Servidor PfSense.....	16
2.9.1 Configuración del Portal Cautivo .....	20
2.9.2 Creación de los usuarios del Portal Cautivo .....	23
2.9.3 Creación de las Reglas de Navegación para el Portal Cautivo .....	26
2.9.4 Instalación y configuración de servidor FTP sobre Windows server 2012 R2 .....	28
<b>3 METODOLOGÍA.....</b>	<b>34</b>
3.1 Diagrama en Bloque de la Solución .....	34
3.2 Requisitos.....	34
3.3 Diseño Físico y Lógico.....	34
3.4 Simulación y Prueba.....	35
3.5 Implementación del Radio Enlace .....	35
3.5.1 Configuración del Punto de Acceso (ITM Fraternidad) .....	38
3.5.2 Configuración del Equipo Estación (Junta de Acción Comunal, barrio 13 de Noviembre) .....	40
3.6 Monitoreo y Optimización.....	42
<b>4 RESULTADOS Y DISCUSIÓN .....</b>	<b>44</b>
<b>5 CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO .....</b>	<b>48</b>

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

**REFERENCIAS ..... 50**

**APÉNDICE ..... 51**

# 1. INTRODUCCIÓN

---

Las redes inalámbricas han representado un papel muy importante en el mundo, ya que poseen una gran variedad de ventajas, como su facilidad y economía a la hora de realizar una instalación pues se ha suprimido en gran medida el uso de cableado. Otra ventaja muy importante es que permite la comunicación con zonas distantes o de difícil acceso. En la actualidad con el desarrollo de las nuevas tecnologías de la información se ha creado la necesidad de implementar redes inalámbricas aprovechando los diferentes tipos de topologías que están disponibles para que los usuarios se acomoden a sus necesidades. Hay que destacar también que las redes inalámbricas se han convertido también en un objetivo de vulnerabilidad de la seguridad ya que cualquier persona puede tener acceso a las mismas por lo que es muy importante tener en cuenta los lineamientos de seguridad que sean los suficientemente adecuados para evitar las posibles amenazas que se puedan presentar a la red.

En el Barrio 13 de Noviembre, ubicado al nororiente de la ciudad de Medellín, la gran mayoría de sus habitantes pertenece a los estratos 0 y 1, de escasos recursos, vulnerables y muchos de ellos fueron víctimas del conflicto armado, lo que motivó su desplazamiento hacia éste sector. (Dpto. Adtvo. de Planeacion de Medellin, 2008).

En este orden de ideas, se percibe como aún existe una gran desigualdad dentro de la población urbana de Medellín, que ni siquiera cuentan con acceso a los servicios básicos o de primera necesidad; y por supuesto, a la hora de introducirse en un enfoque de la utilización de las nuevas tecnologías de la información, se concluye que aún prevalece una gran brecha tecnológica en este sector de la ciudad. Se debe considerar que en parte también obedece a que es una zona de difícil acceso por debido a sus condiciones topográficas, lo que dificulta el despliegue de infraestructuras físicas.

## 1.1 Justificación

Una vez analizadas las condiciones sociales y económicas de la zona, la cual se encuentra ubicada en la Comuna 8, ver Figura 1, se crea la necesidad de establecer una intervención que contribuya con su desarrollo y la oportunidad a sus habitantes de tener fácil acceso a las nuevas tecnologías de la información; en la implementación de la solución, se utilizó tecnologías inalámbricas ya que se convierten en una solución bastante adecuada comparada con otros medios de transmisión. Por su facilidad de instalación, economía, escalabilidad y estabilidad, dada la cercanía entre los puntos de conexión.

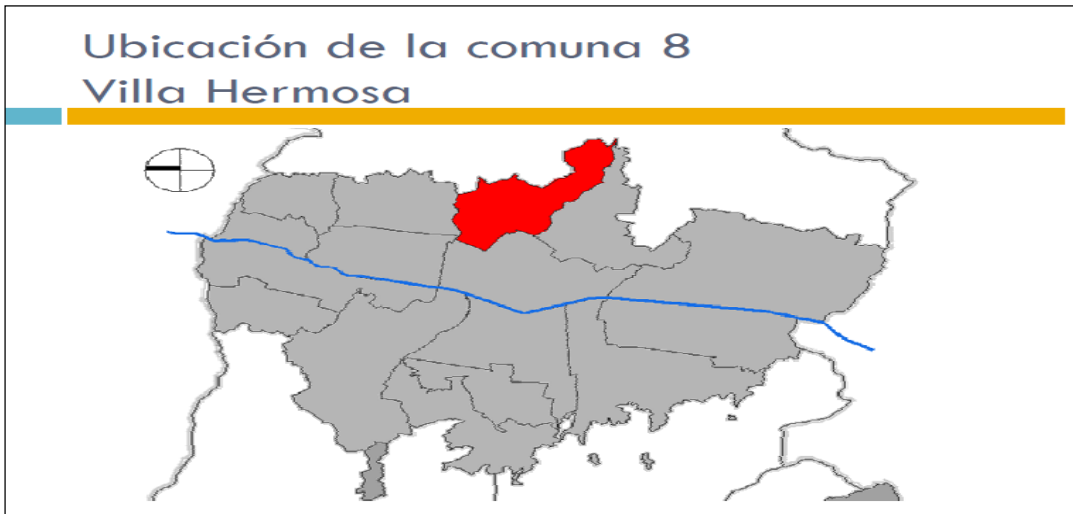


Figura 1. Mapa conformación comuna 8 de Medellín.  
Fuente: Departamento Administrativo de Planeación de Medellín.

Poder ofrecer servicio de internet gratuito permite que muchos de los habitantes del barrio Trece de Noviembre, puedan aprovechar los beneficios que brindan las TICs para aplicarlos al desarrollo de cursos virtuales, investigación, procesos productivos, publicidad, marketing, invención, etc. De esta forma se garantiza que también los jóvenes y habitantes en general, ahorren dinero que pagan por éste concepto (aproximadamente \$1.500 /hora) en dos salas de internet que existen en la actualidad en la zona, (Aguirre, 2015).

Esto contribuye a reducir en gran medida la desigualdad social, la brecha tecnológica y a mejorar la calidad de vida de los habitantes de éste sector.

La Figura 2, muestra la ubicación del ITM Fraternidad en la Comuna 8, y la cercanía que se tiene con el sector a beneficiar con el proyecto.



Figura 2. Mapa de la ubicación del ITM en la comuna 8, con relación al Barrio 13 de Noviembre.  
Fuente: Departamento Administrativo de Planeación de Medellín.

 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

## 1.2 Planteamiento del problema

Como se puede ver en la Tabla 1, el 99 % de los habitantes del sector son estrato socioeconómico 1; lo que pone en evidencia que la mayoría de sus habitantes son de escasos recursos; y no es un secreto que esto también puede reflejar una perspectiva de las condiciones de desigualdad en la que viven.

Tabla 1. Datos Estadísticos Barrio 13 de Noviembre.

Estrato	Personas	%	hogares	%	Viviendas	%	Núcleos familiares	%
1	9920	99%	2190	99,40%	212100	99,30%	2803	99,40%
2	48	0%	10	0,50%	10	0,50%	12	0,40%
3	24	0%	4	0,20%	4	0,20%	6	0,20%
<b>total</b>	<b>9992</b>	<b>1%</b>	<b>2204</b>	<b>100%</b>	<b>2135</b>	<b>100%</b>	<b>2821</b>	<b>100%</b>

Fuente: Departamento Administrativo de Planeación de Medellín. Subdirección Metro información. 2013

Por las condiciones socioeconómicas de los habitantes del sector y por los datos de la Tabla 2, se puede evidenciar como los habitantes escasamente tienen para suplir sus necesidades básicas: Alimentación y pago de los servicios de primera necesidad. El Sector cuenta con redes de telecomunicaciones, pero como se mencionó anteriormente los habitantes no adquieren los servicios, debido a que no cuentan con la capacidad económica para pagarlos.

Tabla 2. Distribución de los Servicios Públicos.

Servicios Públicos Vivienda	SI	NO
Energía Eléctrica	2366	2
Alcantarillado	2219	149
Gas natural domiciliario	28	2340
Teléfono	1923	445
Recolección de basuras	2367	1
Acueducto	2117	251



Fuente: Departamento Administrativo de Planeación de Medellín. Subdirección Metro información. 2013  
Procesamiento: Unidad de Clasificación Socioeconómica y Estratificación.

Todos estos aspectos ocasionan una brecha tecnológica que en pleno siglo XXI resulta difícil de creer; sobre todo en la "Ciudad más innovadora del mundo". Por eso se plantea la pregunta de investigación: *¿Es posible brindar conectividad a internet de forma gratuita a unos 200 usuarios, habitantes del barrio Trece de Noviembre?*



	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

### 1.3 Objetivos

#### General

Diseñar e implementar un radio enlace para proveer servicio de internet gratuito a 200 usuarios, habitantes del Barrio 13 de Noviembre de la comuna 8 de Medellín; con registro y autenticación en un Portal Cautivo.

#### Específicos

Plantear un diseño lógico y físico de la red inalámbrica siguiendo normas estándares de una metodología *Top Down de cisco*, que permita garantizar un radio enlace estable.

Implementar un portal cautivo en un servidor del Laboratorio, para autenticación de usuarios, gestión del sistema y ofrecimiento de servicio basado en el protocolo FTP.

### 1.4 Organización del informe

En el capítulo 1 se encuentra la Introducción, la cual está conformada por las generalidades, pertinencia, justificación, planteamiento del problema abordado y los objetivos del proyecto. En el capítulo 2 se presenta el Marco Teórico, que consiste en el desarrollo de la teoría que permitió fundamentar el proyecto con base al planteamiento del problema; mientras que en el capítulo 3 se presenta la Metodología, y se muestran las tareas vinculadas en pro de alcanzar los objetivos del Proyecto. El capítulo 4 presenta Resultado y las Discusiones, a partir de diversas pruebas que permiten evidencian el logro de los objetivos del proyecto. Por último, el capítulo 5 comprende lo relacionado a las conclusiones, recomendaciones y trabajo futuro que permite orientar al lector de lo que fue logrado con el proyecto, también permite hacer análisis con base a los resultados obtenidos tendientes a mejorar el proyecto, o sirviendo como hoja de ruta para futuros trabajos.

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

## 2. MARCO TEÓRICO

En este capítulo se presentan los fundamentos teóricos que se han adelantado en torno a trabajos similares a éste proyecto y que permiten ubicar en el contexto a los lectores del mismo.

### 2.1. Redes Inalámbricas

Para todos ha sido siempre un gran atractivo poder tener comunicaciones sin el uso de cables. Las comunicaciones inalámbricas han evolucionado con el pasar de los tiempos, en todos los aspectos: velocidades, aplicaciones, coberturas, entre otros. Por otra parte, las comunicaciones inalámbricas brindan la posibilidad de implementar procesos comerciales nuevos y más eficaces que podrían aumentar de manera considerable la capacidad de respuesta a las necesidades particulares.

WLAN, es una red de área local inalámbrica formada por unidades ubicadas en un espacio geográfico de dimensiones reducidas; en una WLAN la conexión se realiza utilizando ondas de radiofrecuencia.

Al ser redes inalámbricas éstas brindan la posibilidad a los usuarios de tener movilidad, ya que no dependen de cables o elementos físicos para permanecer en la red. La ausencia de cables también contribuye a mantener un orden o una organización en la oficina o en cualquier ambiente. La Figura 3, muestra la relación alcance (metros) que son posibles cubrir, teniendo en cuenta el tipo Y/o estándar.

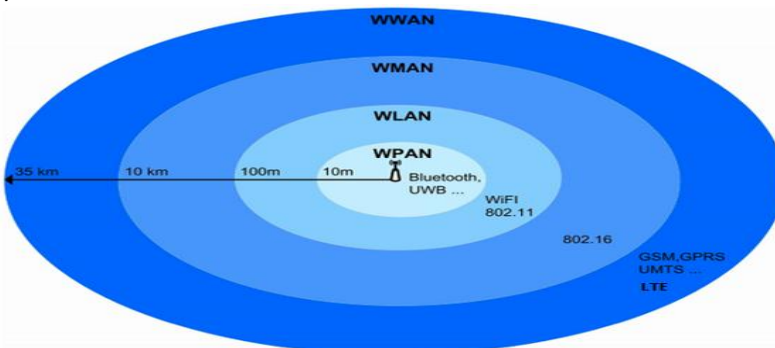


Figura 3. Tipos de redes WLAN.

Fuente: <http://tipstoefl.com/tips-toefl/tips-toefl-mudah/>

#### 2.1.1 Aspectos relacionados con la Capa Física WLAN

**Número de canal:** El número de canal identifica el rango de frecuencias de trabajo. Para 2.4 GHz, estamos hablando de 14 canales, separados por 5 MHz, cada país y zona geográfica aplica sus propias restricciones al número de canales disponibles. Por ejemplo, en Norteamérica tan sólo se utilizan los 11 primeros. Para éste proyecto se utilizó el canal 3 con frecuencia media de trabajo de 2424 MHz, debido a que era el canal que presentaba menos saturación o congestión.

**Potencia de transmisión:** A mayor potencia de transmisión, el punto de acceso tendrá un mayor rango de cobertura, sin embargo, debe evitarse usar más potencia de la necesaria pues aumenta la probabilidad de interferir con otros usuarios. Para la configuración de los equipos se utilizó los valores de potencia que vienen por defecto, los cuales son de 16 dBm, que equivalen a 40mW.

 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

**Velocidad de transmisión:** La tasa de transmisión empleada dependerá del estándar del dispositivo, así para 801.11b el límite superior estará en los 11 Mbps, y para 802.11a y 802.11b en 54 Mbps, empleado en el extremo del usuario final, cuya rata debe ser superior en el radio enlace.

### 2.1.2 Futuros Estándares en Velocidad de Transmisión

**802.11n:** Red inalámbrica que trabaja entre las bandas 2,4 y 5 GHz, con velocidades que alcanzan hasta 600 Mbps.

**802.11ac:** Es un estándar de red inalámbrica que opera por debajo de 6 GHz, permite alcanzar velocidades cercanas a 1 Gbps por segundo.

**802.11ad:** Ofrece un gran performance a frecuencias cercanas a los 60 GHz. Este estándar apunta a ofrecer velocidades de hasta 7 Gbps. Permite alcanzar estas velocidades gracias al uso de la banda ISM de 60 GHz.

**802.11af:** Esta estándar permite utilizar el espectro no utilizado por la frecuencia de TV, o los espacios blancos para transmitir, también se conoce como White-Wi-fi. El sistema general no debe causar interferencia a los usuarios primarios.

**802.11ah:** Es un nuevo estándar que trabaja por debajo de los GHz del espectro de frecuencias. Para lograr esto una nueva capa física y MAC ha sido desarrollado para permitir las comunicaciones en estas frecuencias, aunque a una velocidad menor que la que se puede lograr para la muy alta velocidad 802.11ac y otras variantes Wi-Fi. (Poole, 2014).

**IEEE 802.22:** El estándar IEEE 802.22 WRAN pretende incentivar el uso de dispositivos que no requieran licencia, sobre una base de no interferencia en el espectro que se asigna al servicio televisión. El estándar puede ofrecer velocidades cercanas a las ofrecidas por servicios de DSL / ADSL. (radioelectronics.com)

### 2.1.3 Aspectos Relacionados con la Capa de Enlace de WLAN

**Modos de operación o funcionamiento:** El estándar 802.11 define dos modos operativos, como se observa en la Figura 4. El *modo de infraestructura* en el que los clientes de tecnología inalámbrica se conectan a un punto de acceso y el *modo ad-hoc* en el que los clientes se conectan entre sí sin ningún punto de acceso.

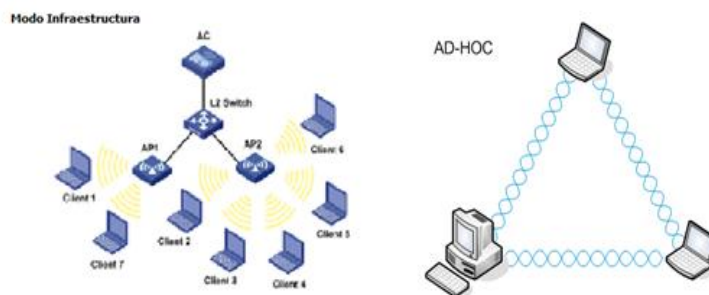


Figura 4. Modos de Funcionamiento, redes WLAN.

Fuente: Poole, AC, 2012

### SSID (Service Set Identifier)

El SSID es el nombre de la LAN inalámbrica. Se trata de una cadena de texto sensible a mayúsculas y minúsculas, que acepta hasta 32 caracteres alfanuméricos y es usada durante el proceso de asociación a una red inalámbrica.

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

## 2.2 Seguridad en las Redes WLAN

Este punto es fundamental, ya que las redes inalámbricas usan ondas de radio y son más susceptibles de ser interceptadas, por lo que se hace casi indispensable proveer de mecanismos de seguridad a nivel de enlace que garanticen la integridad y confiabilidad de los datos.

Los principales mecanismos que intentan o ayudan a garantizar la privacidad, integridad y confidencialidad de la transmisión son: WEP, WPA, filtrado MAC y 802.1x.

### 2.2.1 Mecanismo de seguridad WEP

Su propósito fue brindar un nivel de seguridad comparable al de las redes por cable tradicionales. Se trata de un mecanismo basado en el algoritmo de cifrado RC4, y que utiliza el algoritmo de chequeo de integridad CRC (Chequeo de Redundancia Cíclica).

### 2.2.2 WPA y WPA2

WPA y WPA2 pueden trabajar con y sin un servidor de distribución de llaves. Si no se usa un servidor de llaves, todas las estaciones de la red usan una llave de tipo PSK (*Pre-Shared-Key*), en caso contrario se usa habitualmente un servidor IEEE 802.1x.

### 2.2.3 Protocolo 802.11 x

Este protocolo ofrece un marco para autenticar y controlar el acceso a los puntos de accesos. Sirve como soporte para implementaciones de seguridad sobre servidores de autenticación. El funcionamiento es básicamente el siguiente, el cliente envía una petición al servidor de autenticación a través del AP, quien comprueba el certificado o el nombre de usuario y contraseña utilizando esquemas de autenticación como EAP encargados de la negociación.

En este proyecto se utilizó el estándar de seguridad WPA2-AES y el tipo de autenticación WPA que se usó fue PSK, los cuales se aplicaron para la configuración de los equipos encargados de establecer el radio enlace, es decir los equipos Ubiquiti Nano Station M2.

La Tabla 3 muestra las ventajas y desventajas que ofrecen las redes Wlan

Tabla 3. Ventajas y Desventajas de Redes WLAN.

Ventajas	Desventajas
<ul style="list-style-type: none"> <li>▪ No necesita licencia para su instalación</li> <li>▪ Son más sencillas de instalar</li> <li>▪ Obtenemos conexión sin necesidad de cables.</li> <li>▪ Elimina la necesidad de compartir un espacio físico común.</li> <li>▪ Disponibilidad de información desde diferentes puntos.</li> <li>▪ Permite la movilidad.</li> <li>▪ Comunicación desde cualquier lugar.</li> <li>▪ Mayor economía.</li> </ul>	<ul style="list-style-type: none"> <li>• Menor velocidad de descarga con respecto al cable.</li> <li>• Nivel de seguridad, aún por mejorar.</li> <li>• Presentan interferencia con otros equipos.</li> <li>• Velocidad de transmisión limitada.</li> <li>• Potencia y distancia limitada.</li> <li>• Pueden ser un poco más inestables.</li> </ul>

Fuente: (García, 2012)

 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

### 2.3 Redes Wi-Fi.

Los sistemas basados en Wi-Fi (estándares IEEE 802.11) pueden ser usados para proveer banda ancha inalámbrica. Tiene gran similitud al funcionamiento que posee Ethernet. Wifi se ha popularizado como el estándar de conectividad en hogares, empresas y zonas públicas de hostpots. Aunque también pueden ser utilizadas (bajo ciertas restricciones legales de potencia) en exteriores, utilizando antenas externas, amplificadores adecuados, entre otros.

Los sistemas Wifi han permitido a las comunidades que se encuentran más apartadas, en zonas rurales y sin servicio, a que puedan tener conectividad y un servicio de calidad; wifi ofrece velocidades de datos más altas que los sistemas 3G, gracias a que opera a un ancho de banda de 20MHz.

Las ventajas y desventajas de las redes Wifi, se listan en la Tabla 4.

Tabla 4. Ventajas y Desventajas de redes Wifi.

Ventajas	Desventajas
Uso de frecuencias sin licencia de las bandas ISM 2.4 / 5.8 GHz con ciertas limitaciones de potencia.	Al ser una tecnología creada para redes de corto alcance, hay que solventar ciertos problemas relacionados con su utilización para distancias de decenas de Km
Velocidades desde 1 hasta 54 Mbps, siempre teniendo en cuenta que el throughput <sup>28</sup> neto obtenido está alrededor de un 50-70% de esos valores	
Tecnología con estándar ampliamente conocido y fácil de configurar, lo que favorece los bajos costos de los equipos	El número de colisiones aumenta en relación con el número de usuarios.
Bajo consumo de potencia, menor a 10 W por enrutador	Tiene un número limitado de canales no interferentes, 3 en 2.4 GHz y 8 en 5.8 GHz- .
Un nodo puede adherirse a la red si puede ver a uno de los nodos vecinos (las zonas rurales aisladas normalmente no siguen una distribución geométrica ordenada alrededor de un punto central).	Requiere línea de vista directa (esto podría elevar, en algunos casos, el número de repetidores necesarios aumentando demasiado el costo).
Hardware fácilmente integrable en un sistema impermeable que soporte condiciones meteorológicas adversas.	

Fuente: Grupo de Telecomunicaciones Rurales, Pontificia Universidad Católica del Perú. Redes inalámbricas para zonas Rurales. Lima: GTR-PUCP, 2008. Pag 252. ISBN978-9972-42-843-2.

### 2.4 Banda de frecuencias no licenciadas en Colombia.

En Colombia, el Ministerio de las TICs es el organismo encargado de otorgar los permisos para la operación de los sistemas de acceso inalámbrico y WLAN y atribuir las bandas de frecuencias radioeléctricas de libre utilización para sistemas.

Los rangos de frecuencias más utilizados son los 2,4 GHz y 5 GHz. Las bandas de 2,4 y 5 GHz tienen una característica en común y es que en ellas funcionan los “sistemas de baja potencia y corto alcance”, aplicaciones (ICM)<sup>1</sup>, consideradas como de “uso libre” a nivel mundial. Fue así como nacieron tecnologías como el espectro ensanchado, los sistemas U-NII, los sistemas inalámbricos de área local, etc., y que poco a poco han ido ganando terreno a nivel internacional. (Ministerio de las TICs, 2003)

### 2.5 Radio Enlaces

Se denomina radio enlace a cualquier interconexión entre los terminales de telecomunicaciones efectuados por ondas electromagnéticas. Si los terminales son fijos, el servicio se lo denomina como tal y si algún terminal es móvil, se lo denomina dentro de los servicios de esas características. Los enlaces se hacen básicamente entre puntos visibles, es decir, puntos altos de la

<sup>1</sup> Aplicaciones cuyo fin es el desarrollo de la industria, del sector científico y medico con beneficio general.

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

topografía, para un correcto funcionamiento es necesario que los recorridos entre enlaces tengan una altura libre adecuada para la propagación de la señal. (Technologies, 2003).

En el desarrollo del proyecto se optó por un radio enlace sobre una topología punto a punto. El punto Principal (máster) se ubicó en la terraza del piso 6 del ITM Fraternidad, y la Estación Remota quedó ubicada en la sede de la Junta de Acción Comunal del barrio 13 de noviembre.

## 2.6 Topologías de red para entornos inalámbricos

Las redes inalámbricas se clasifican en tres configuraciones lógicas: enlaces punto a punto, enlaces punto a multipunto, y multipunto a multipunto. El diseño de una red puede hacer uso de estas configuraciones simultáneamente, pero cada enlace va a estar solo dentro de una de esas topologías.

### 2.6.1 Punto a Punto

Los enlaces de este tipo son el legado de los tipos de arquitectura y posiblemente ha sido la topología de red más usada en microondas en los últimos años. Por años e incluso décadas, los operadores de microondas han establecido enlaces punto a punto para extensiones de redes LAN, para conectar sitios remotos con la Red Telefónica Pública Básica Conmutada (RTPBC) y para backhaul<sup>2</sup> celular.

### 2.6.2 Punto a Multipunto

Cada vez que se tiene varios nodos hablando con un único punto de acceso central se trata de una aplicación punto a multipunto. El ejemplo típico de un trazado punto a multipunto es el uso de un punto de acceso inalámbrico que provee conexión a varios computadores portátiles. Los computadores portátiles no se comunican directamente unos con otros, pero deben estar en el rango de cubrimiento del punto de acceso para poder utilizar la red. (Flickenger, Aichele, & Buittrich, 2008).

### 2.6.3 Multipunto a Multipunto

Es conocida como red ad-hoc o en malla, una característica de una red de este tipo es que no hay una autoridad central. Por el contrario, cada nodo de la red transporta el tráfico de tantos otros como sea necesario, y todos ellos se comunican entre sí, una de las ventajas de esta arquitectura que aún si ninguno de los nodos es alcanzable desde el punto de acceso central, igual pueden comunicarse entre sí. (Flickenger, Aichele, & Buittrich, 2008).

## 2.7 Zonas de Fresnel.

Es un elipsoide prolongado que se extiende entre dos antenas. La primera zona de Fresnel es la diferencia entre el camino directo y el camino indirecto que toca un solo punto en la zona de Fresnel (ACB), es decir, es igual a la mitad de la longitud de onda. Como se observa Figura 5.

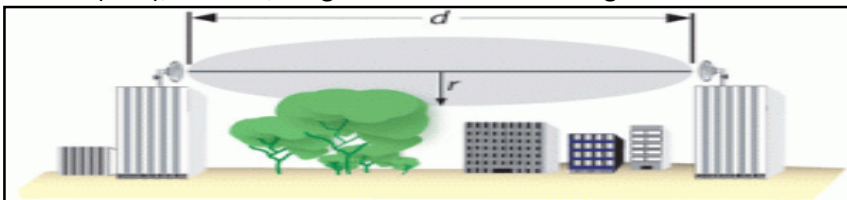


Figura 5. Primera Zona de Fresnel  
Fuente: (Molina, 2015).

<sup>2</sup> Es la porción de una red jerárquica que comprende los enlaces intermedios entre el núcleo y las subredes en sus bordes.

 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Si una porción significativa de la zona de Fresnel es obstruida la potencia de la señal recibida en la antena receptora puede ser atenuada significativamente. Se determina que se necesita por lo menos el 60% de la primera zona se encuentre totalmente despejada de cualquier obstáculo, haciendo parecer como si estuviera en el espacio libre. Para el proyecto se garantizó la primera zona de Fresnel, ya que en la trayectoria del radioenlace no presenta ningún tipo de obstáculo. Como se puede observar en Figura 6.

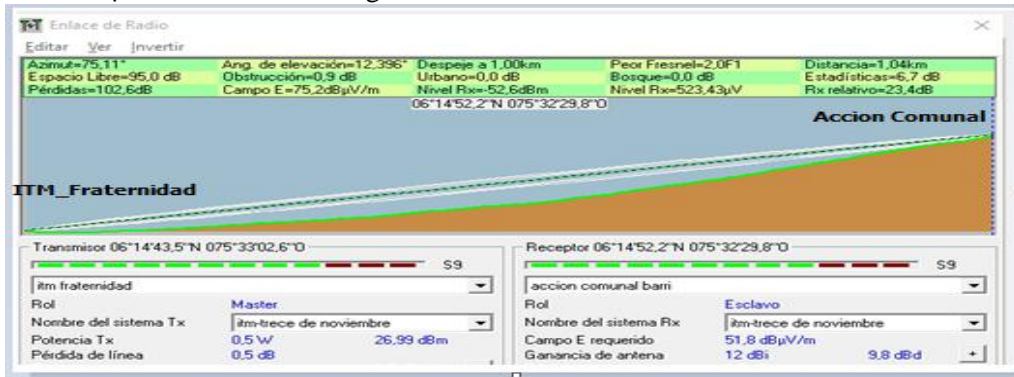


Figura 6. Perfil de Terreno, radioenlace.  
Fuente: Radio Mobile.

## 2.8 Qué es un Portal Cautivo?

Un portal cautivo es una aplicación utilizada generalmente en redes inalámbricas abiertas (*hotspots*) para controlar el acceso a la misma, aunque también puede utilizarse en redes cableadas. Por un lado, se utiliza para presentar al usuario alguna información de interés (información corporativa, políticas de uso, etc.) y por otro le permite al usuario facilitar al sistema sus credenciales de acceso. (Delgado, 2014).

### 2.8.1 Tipos de Portal Cautivo

#### Portales Cautivos por Software:

PepperSpot, NoCatAuth, OpenSplash, PfSense, Easy Captive y ZeroShell.

#### Portales Cautivos por Hardware:

Cisco BBSM-Hotspot, Cisco Site Selection Gateway (SSG), Nomadix Gateway y Aptilo Acces Gateway

Para el proyecto, se usó un Portal Cautivo por Software, llamado *PfSense*.

### 2.8.2 Qué es Pfsense?

PfSense es una distribución basada en FreeBSD, derivada de m0n0wall. Su objetivo es tener unos cortafuegos (firewall) fácilmente configurable a través de una interface web e instalable en cualquier PC. Se trata, por tanto, de una solución muy completa, bajo licencia BSD, es de libre distribución. El cortafuego forma parte del Kernel del sistema. De hecho, se trata del Packet Filter (PF) originario de OpenBSD, considerado como el sistema operativo más seguro del mundo. (García, Quezada, & Bello, 2010).

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

## 2.9 Instalación y Configuración del Servidor PfSense

El proceso de instalación comienza con una pantalla de bienvenida, ver



Figura 7, donde se muestra serie de opciones de arranque; se pulsa la opción 1, para iniciar la instalación ó en su defecto se espera a que el proceso de instalación comience automáticamente.



Figura 7. Inicio Proceso de Instalación PfSense  
Fuente: PfSense.

A continuación, el asistente de instalación pregunta si se desea aceptar las configuraciones de pantalla y teclado que trae por defecto, se selecciona la última opción para aceptar, ver

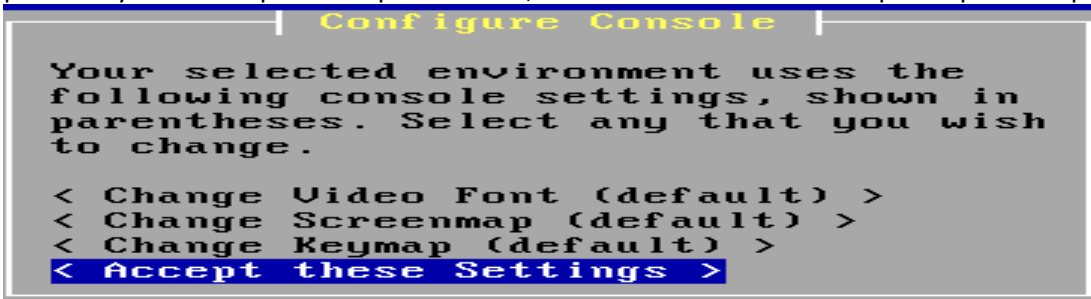


Figura 8.



 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

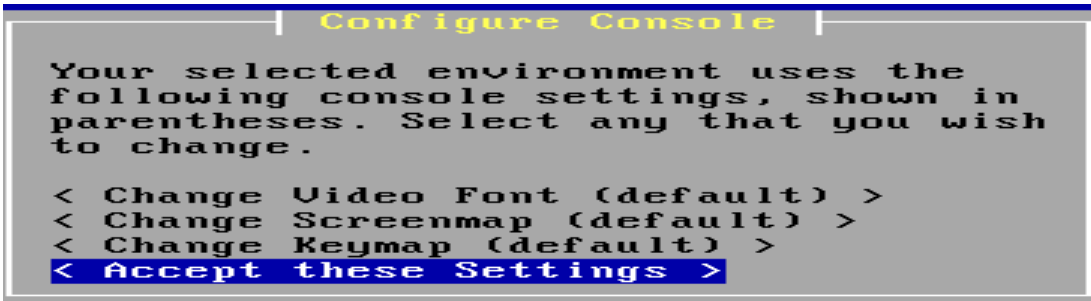


Figura 8. Paso 2, proceso de Instalación PfSense  
 Fuente: PfSense.

En la siguiente pantalla, ver Figura 9, se da clic en la primera opción para aceptar la instalación fácil.

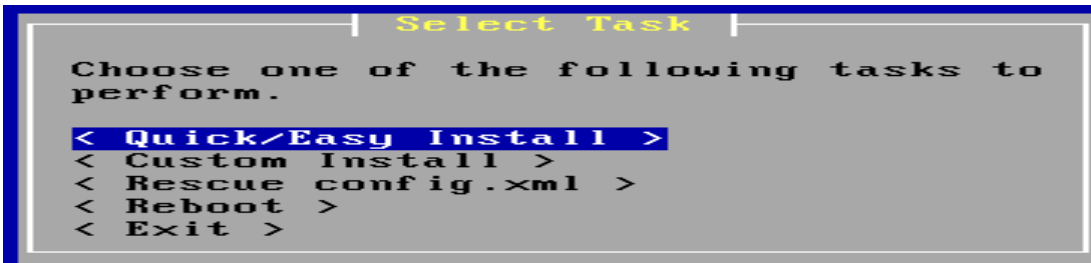


Figura 9. Paso 3, proceso de Instalación PfSense  
 Fuente: PfSense.

Luego comienza el proceso de instalación de Pfsense.

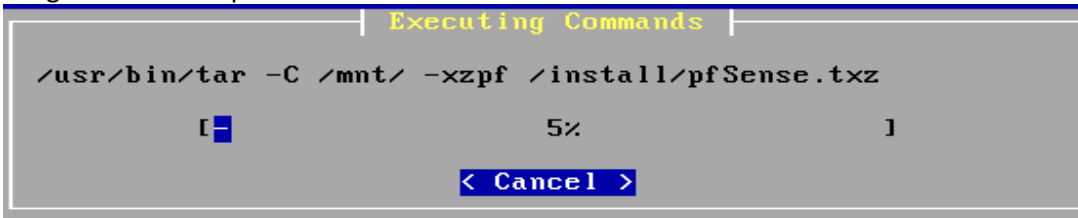


Figura 10.

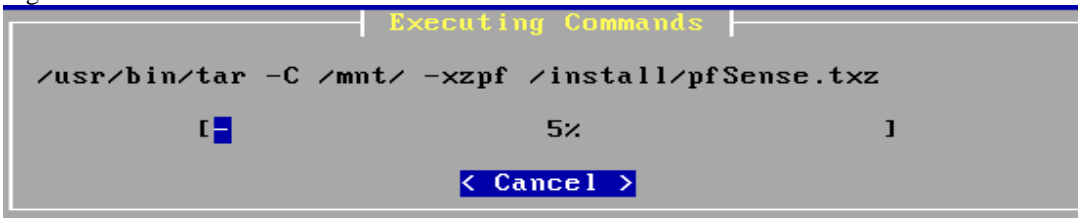


Figura 10. Paso 4, proceso de Instalación PfSense  
 Fuente: PfSense.

 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Luego de la instalación el sistema nos da la opción para reiniciar la máquina, Figura 11.



Figura 11. Finalizando Proceso de Instalación PfSense.

Fuente: PfSense.

Una vez reiniciada la máquina, Pfsense ya está instalado y se puede iniciar el proceso de configuración, ver

Figura 12. Por lo que se debe presionar la tecla F1 o en su defecto el servidor comienza automáticamente.



Figura 12. Inicio Procedimiento de Configuración PfSense

Fuente: PfSense.

A continuación, se muestra una serie de opciones para configurar interfaces y aplicativos para realizar pruebas de conectividad. Y aparte muestra información acerca de que IP tiene las dos interfaces del Firewall tanto la WAN como la LAN, ver Figura 13.

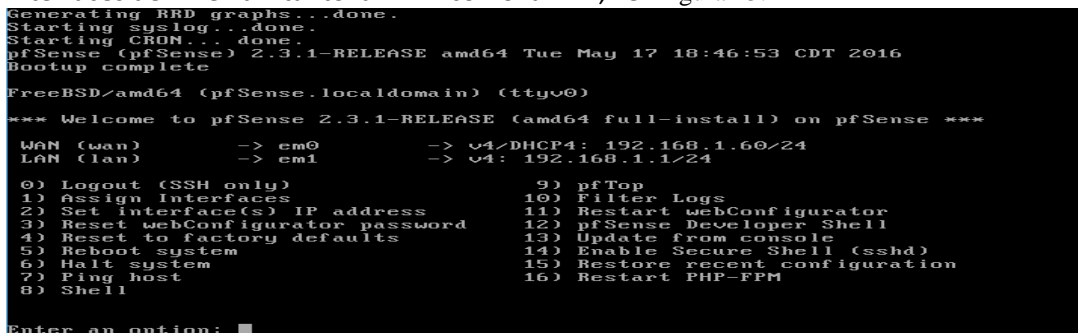


Figura 13. Configuración PfSense.

Fuente: PfSense.

La interface WAN por defecto viene activada para recibir una dirección IP DHCP en este caso se asigna una dirección estática tanto en la interface WAN como en la LAN. La idea es que las dos interfaces queden en diferentes subredes. Para esto se digita el número 2 en la ventana de comandos y se presiona Enter, para configurar las dos interfaces, ver Figura 14.



Figura 14. Configuración PfSense.

Fuente: PfSense.

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

El asistente pregunta cuál de las dos interfaces se desea configurar por lo cual se debe presionar la tecla 1 correspondiente a la interface WAN. Luego de esto pregunta si se desea que la interface obtenga una IP por DHCP, se selecciona “no”, para configurar una dirección estática, ver Figura 15.

```
Enter the number of the interface you wish to configure: 1
Configure IPv4 address WAN interface via DHCP? (y/n) n
```

Figura 15. Configuración Interfaces de Red PfSense.  
Fuente: PfSense.

Luego de esto el asistente de configuración solicita el ingreso de la dirección estática que le será asignada a la interface WAN del servidor, la cual es 192.168.125.6/30, y la puerta de enlace que es la 192.168.125.5/30. Ver Figura 16.

```
Enter the number of the interface you wish to configure: 1
Configure IPv4 address WAN interface via DHCP? (y/n) n
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.125.6
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0    = 8
Enter the new WAN IPv4 subnet bit count (1 to 31):
> 30
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.125.5
```

Figura 16. Configuración Interfaces de Red PfSense.  
Fuente: PfSense.

Luego de esto, el asistente pregunta si se desea configurar una dirección IP para el protocolo IPV6 a la cual se presiona ENTER para omitir y continuar. Ver Figura 17.

```
Configure IPv6 address WAN interface via DHCP6? (y/n) n
Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Please wait while the changes are saved to WAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
The IPv4 WAN address has been set to 192.168.125.6/30
Press <ENTER> to continue.
```

Figura 17. Configuración Pfsense.  
Fuente: PfSense.

El asistente de configuración envía nuevamente la pantalla de inicio en donde se selecciona nuevamente la opción 2, para configurar la interface LAN se escoge la opción 2; ver Figura 18.

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.31.0.1
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0    = 8
Enter the new LAN IPv4 subnet bit count (1 to 31):
> 22
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 172.31.0.1
```

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Figura 18. Configuración interfaces de Red PfSense LAN.  
Fuente: PfSense.

Igual que en la WAN se configura una IP estática 172.31.0.1/22 y se le indica la puerta de enlace es la 172.31.0.1. Luego de esto se presiona la tecla ENTER para omitir la configuración del protocolo IPV6.

A continuación, el asistente pregunta si se desea activar el servicio de DHCP para esta interface, se selecciona “yes” para que los equipos que se conecten a esta interface obtengan direccionamiento automáticamente; y seguidamente se asigna un rango de IP para el servicio de DHCP, ver

Figura 19, como se pretende conectar unos 200 hosts simultáneamente, se selecciona el rango desde la dirección IP 172.31.0.200 en adelante. Con el direccionamiento que se tiene (máscara de 22), se logran tener equipos conectados hasta la IP 172.31.3.254.

```
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 172.31.0.200
Enter the end address of the IPv4 client address range: 172.31.3.254

Please wait while the changes are saved to LAN...
Reloading filter...
```

Figura 19. Configuración del Servicio DHCP – LAN  
Fuente: PfSense.

Seguido de esto se activa la administración vía WEB para poder tener administración desde cualquier equipo conectado a la interfaz de la red LAN. Y con este último proceso se tienen configuradas las interfaces de red del servidor. El asistente indica que ya se tiene gestión vía web a través de la dirección [HTTP://172.31.0.1/](http://172.31.0.1/). Ver

Figura 20.

```
The IPv4 LAN address has been set to 172.31.0.1/22
You can now access the webConfigurator by opening the following URL in your web browser:

    http://172.31.0.1/

Press <ENTER> to continue.
*** Welcome to pfSense 2.3.2-RELEASE (i386 full-install) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.125.6/30
LAN (lan)      -> em1      -> v4: 172.31.0.1/22
```

Figura 20. Notificación de Administración Web del PfSense.  
Fuente: PfSense.

Se ingresan las credenciales que por defecto son “admin” para el usuario y “Proyectoitm2016” la contraseña; ambos datos se puede cambiar más adelante. Ver Figura 21.

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

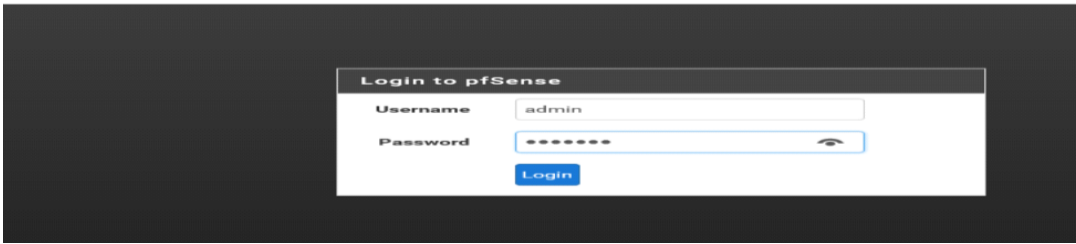


Figura 21. Acceso Web PfSense

Fuente: PfSense.

Una vez ingresados los datos de login, aparece un asistente de configuración automática, el cual se cancela para poder configurar las preferencias de manera manual. Ver Figura 22.



Figura 22. Asistente de Configuración Web del PfSense.

Fuente: PfSense.

### 2.9.1 Configuración del Portal Cautivo

Para proceder con la configuración del portal cautivo se ingresa al menú. Ver Figura 23.

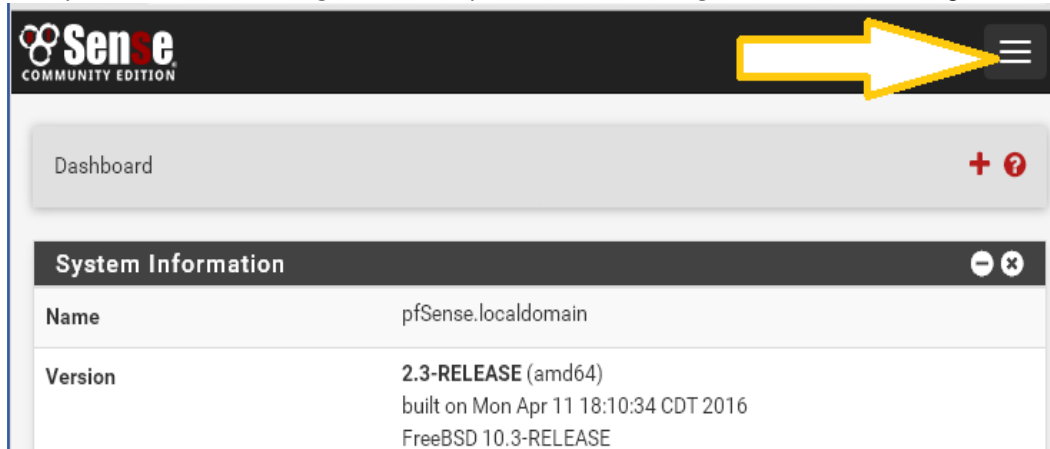


Figura 23. Paso 1 para Configurar el Portal Cautivo.

Fuente: PfSense.

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Se ingresa a “Services” y luego la opción *Captive Portal*. Ver Figura 24.

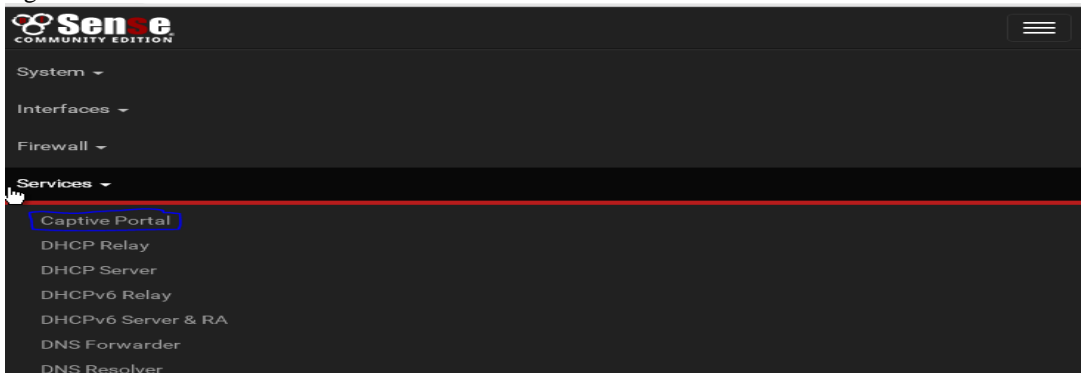


Figura 24. Paso 2 para Configurar el Portal Cautivo.  
 Fuente: PfSense.

Luego se debe crear la Zona, para ello se da clic en “Add”, ver Figura 25.

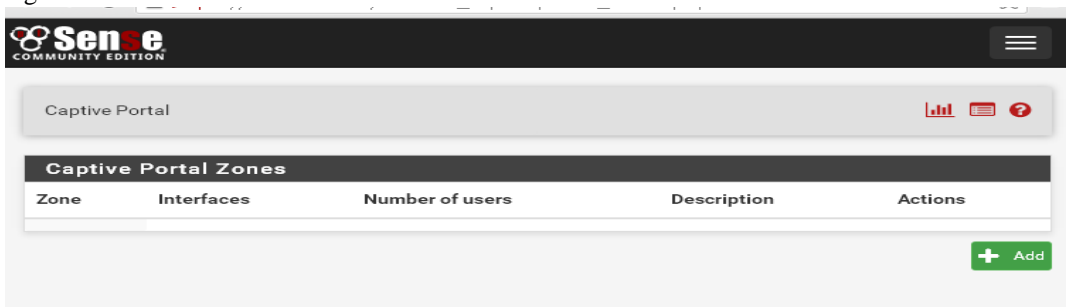


Figura 25. Creando la Zona del Portal Cautivo.  
 Fuente: PfSense.

Se asigna el Nombre de “*Internet Gratis*” y en Descripción “13\_Noviembre”. Se guarda y continúa. Ver

Figura 26.

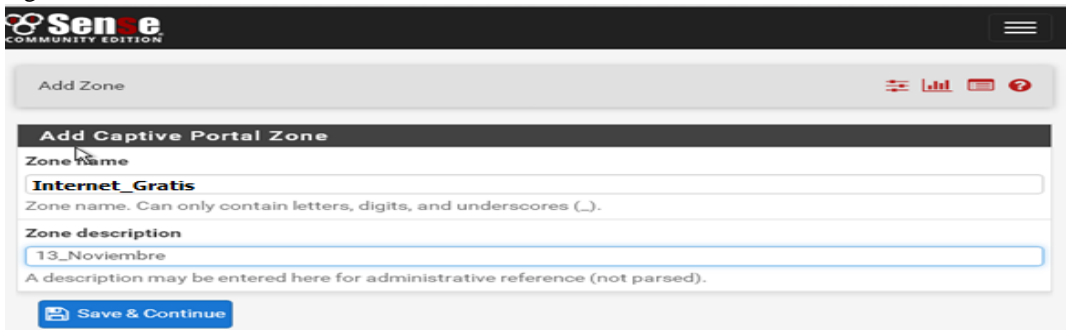
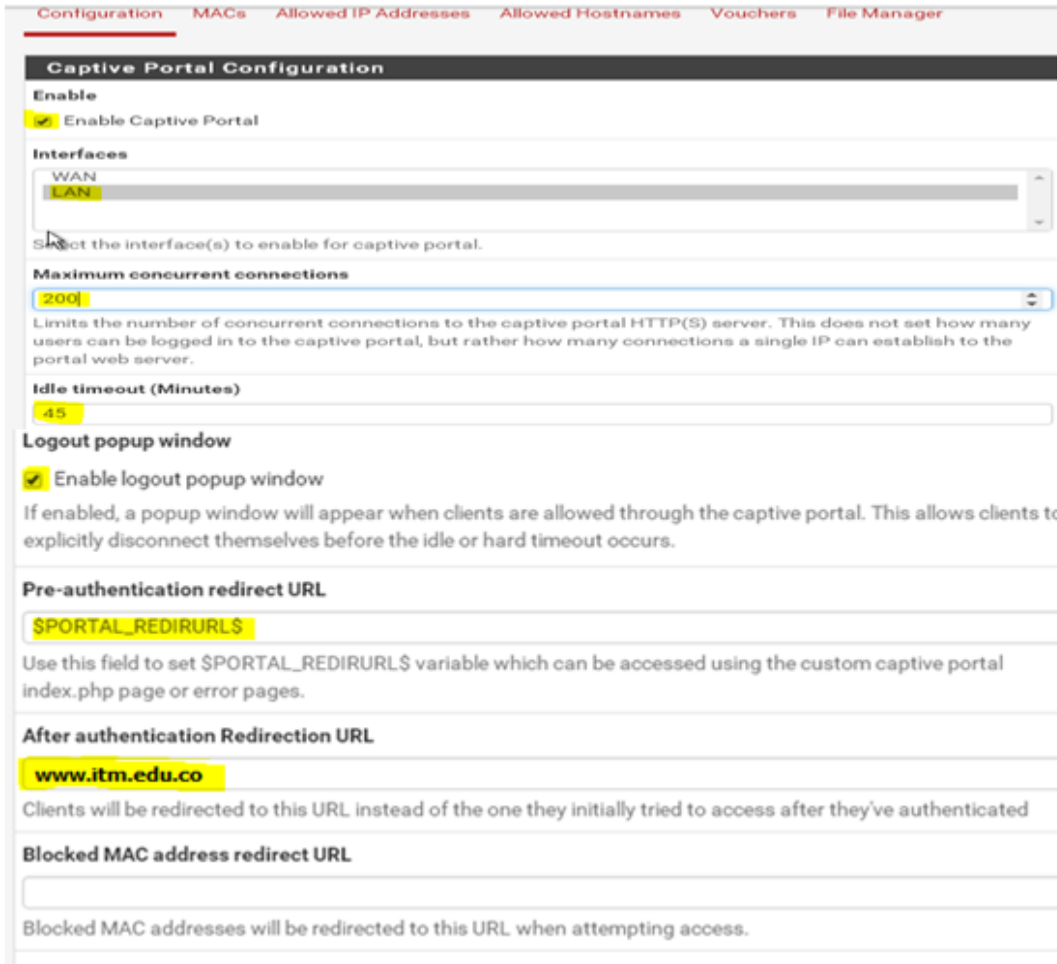


Figura 26. Configurando la Zona del Portal Cautivo.  
 Fuente: PfSense.

En la

 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Figura 27, se habilita el Portal Cautivo para la interfaz LAN, que será la red de los usuarios beneficiados, se indica el número de conexiones y el tiempo de conexión que tendrán los usuarios por cada autenticación, se muestra que se habilita la ventana emergente de autenticación (pasados los 45 Min), la web a la cual será direccionado el usuario después de autenticarse es [www.itm.edu.co](http://www.itm.edu.co)



The screenshot shows the 'Captive Portal Configuration' page in PfSense. The 'Enable' section has 'Enable Captive Portal' checked. Under 'Interfaces', 'LAN' is selected. 'Maximum concurrent connections' is set to 200. 'Idle timeout (Minutes)' is set to 45. 'Logout popup window' is checked. 'Pre-authentication redirect URL' is set to '\$PORTAL\_REDIRURLS'. 'After authentication Redirection URL' is set to 'www.itm.edu.co'. 'Blocked MAC address redirect URL' is empty.

Figura 27. Habilitando y Configurando el Portal Cautivo.  
Fuente: PfSense.

Se habilita el login a través de protocolo web seguro, se indica el nombre o la IP del servidor y se utiliza el certificado SSL por defecto. Ver Figura 28.

 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

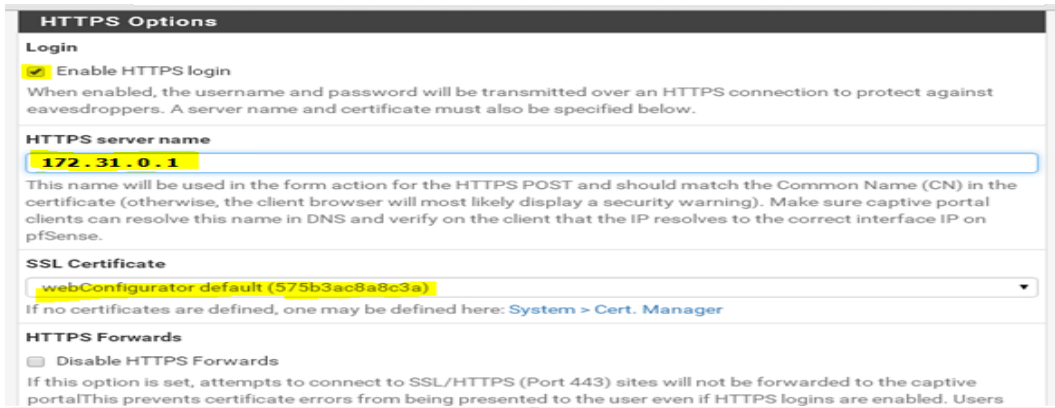


Figura 28. Últimos pasos de Configuración del Portal Cautivo.  
Fuente: PfSense.

Finalizada la configuración, se guardan los cambios al dar click sobre el botón “Save”. Se observa en la Figura 29 como queda creada la zona donde se implementará el portal cautivo.

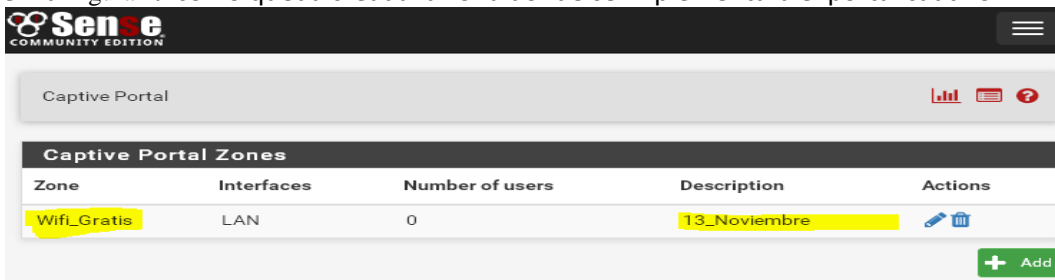


Figura 29. Se crea la Zona de Influencia del Portal Cautivo.  
Fuente: PfSense.

### 2.9.2 Creación de los usuarios del Portal Cautivo

Se ingresa a través menú/System/user Manager, para crear los usuarios Portal Cautivo que se podrán autenticar y navegar de forma gratuita. Ver Figura 30.

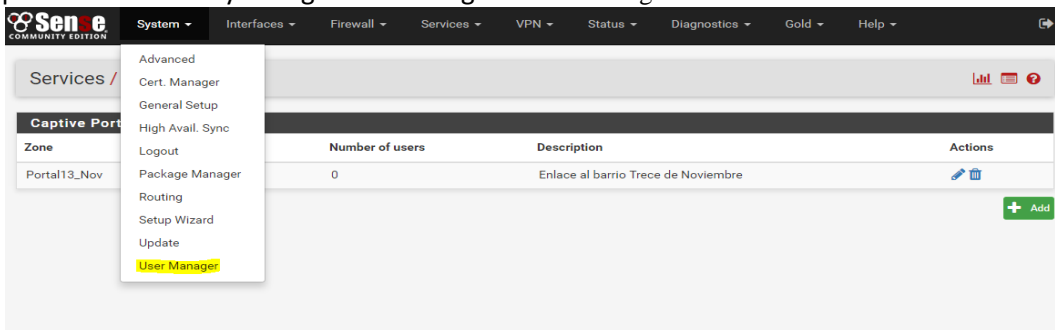


Figura 30. Creación de los Usuarios del Portal Cautivo.  
Fuente: PfSense.

Primero se debe crear el Grupo donde van a estar los usuarios que van a tener el servicio gratuito. Se da clic en “Add”. Ver Figura 31.



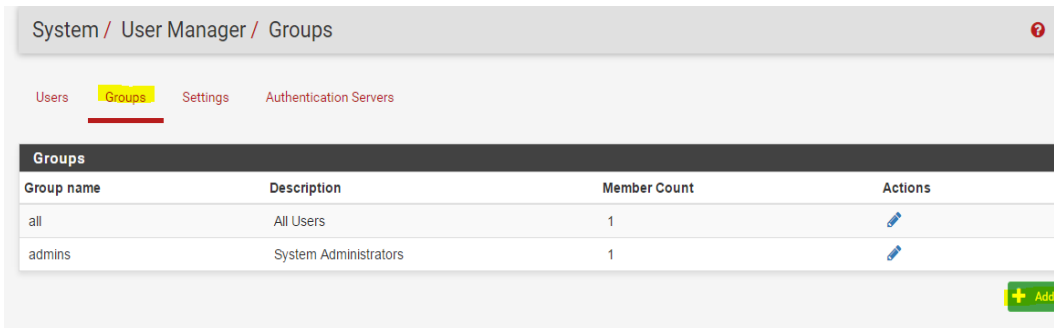


Figura 31. Creando Grupo de Usuarios del Portal Cautivo.

Fuente: PfSense.

Se crea el Grupo “*Usuarios\_13Nov*” y la descripción “*Usuarios del Enlace al Barrio Trece de Noviembre*”, luego se da clic en guardar, ver Figura 32.

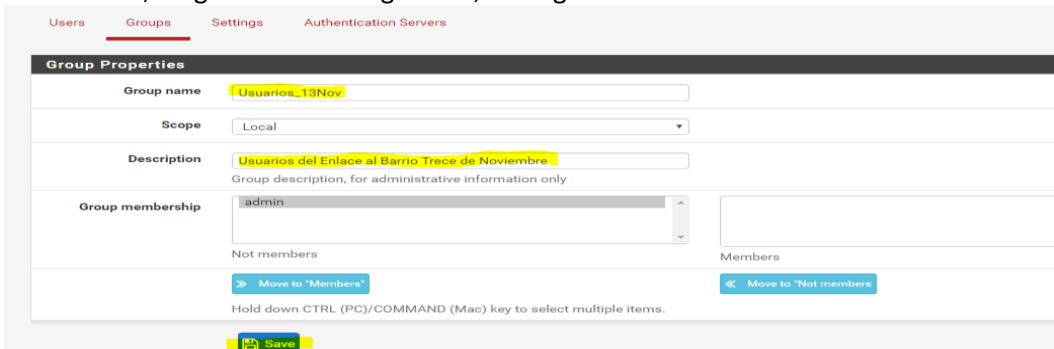


Figura 32. Creando Grupo de Usuarios del Portal Cautivo.

Fuente: PfSense.

De esta forma queda creado el Grupo de Usuarios del Portal Cautivo, ver Figura 33.

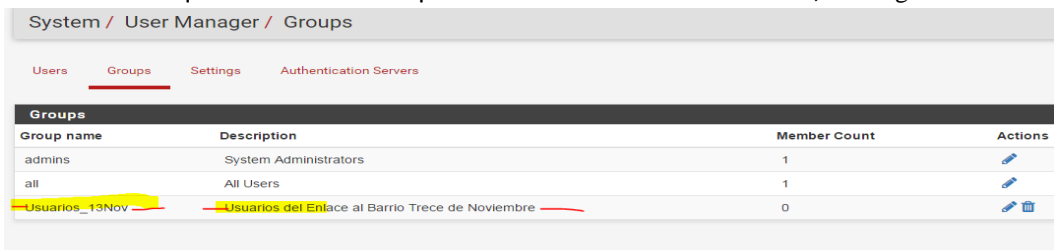
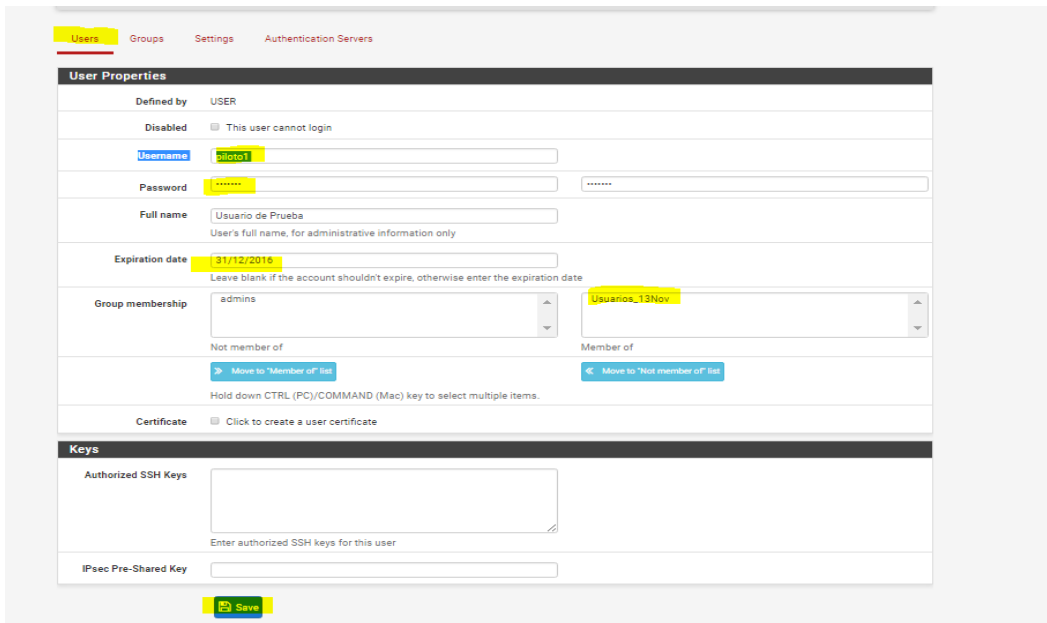


Figura 33. Queda creado el Grupo del Portal Cautivo.

Fuente: PfSense.

Ahora se deben crear el (los) usuario (s) que estará haciendo parte del Grupo “*Usuarios\_13Nov*” y que podrán autenticarse; para ello se ingresa al menú “Users”, ver Figura 34. Se crea el usuario, “*Piloto1*”, se asigna una descripción, una contraseña y se asocia al grupo creado anteriormente. Se guardan los cambios.

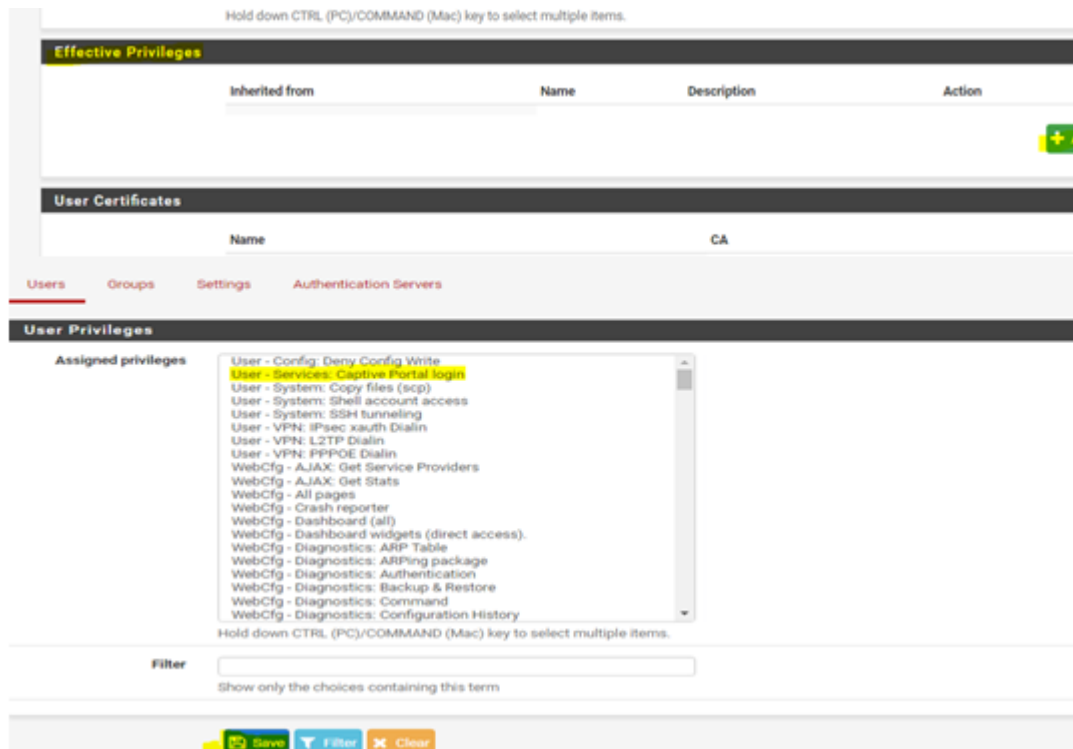


The screenshot shows the 'User Properties' configuration page in PfSense. The 'User Properties' section includes fields for 'Defined by' (USER), 'Disabled' (checkbox), 'Username' (piloto1), 'Password' (masked), 'Full name' (Usuario de Prueba), 'Expiration date' (31/12/2016), 'Group membership' (admins), and 'Certificate' (checkbox). The 'Keys' section includes 'Authorized SSH Keys' and 'IPsec Pre-Shared Key'. A 'Save' button is visible at the bottom.

Figura 34. Creación de Usuarios del Portal Cautivo.

Fuente: PfSense.

Para terminar de crear al usuario. Se debe asociar el "Privilegio" que va a tener éste usuario. Se edita el usuario creado. Ver



The screenshot shows the 'User Privileges' configuration page in PfSense. It features a table for 'Effective Privileges' with columns for 'Inherited from', 'Name', 'Description', and 'Action'. Below this is the 'User Certificates' section. The 'Assigned privileges' section contains a list of privileges, with 'User - Services: Captive Portal login' highlighted. A 'Filter' input field is present at the bottom, along with 'Save', 'Filter', and 'Clear' buttons.

Figura 35.

 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22



En la parte de “Effective Privileges”, se adiciona el privilegio que tendrá el usuario “User-Services: Captive Portal Login” que le otorga acceso a internet después de autenticarse en el portal.

Figura 35. Asociando el Usuario al Grupo del Portal Cautivo.  
Fuente: PfSense.

Para probar la creación del usuario y sus privilegios se trató de acceder a Internet, aparece la página web de autenticación del Portal Cautivo, ver Figura 36. Se autentica con el usuario: “Piloto1” y la clave: “123456”

**INTERNET GRATIS BARRIO TRECE DE NOVIEMBRE.**



Figura 36. Página de Autenticación en el Portal Cautivo.  
Fuente: PfSense.

Una vez autenticados en el Portal Cautivo, el usuario es redireccionado a la página de inicio [www.itm.edu.co](http://www.itm.edu.co), que fue configurada.

 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22



### 2.9.3 Creación de las Reglas de Navegación para el Portal Cautivo

Con el fin de garantizar la seguridad, eficiencia y evitar el uso indebido del servicio de internet se configuran algunas reglas que van a impedir el acceso a páginas de contenido pornográfico. Se crea igualmente una regla para evitar el acceso a Youtube, ya que ésta página consume mucho ancho de banda. Se accede al Servidor a través del navegador de internet, ingresando la ip de administración <http://172.31.0.1>. Se procede a la autenticación del usuario administrador y se ubica en el menú la opción Firewall / Aliases. Ver Figura 37.

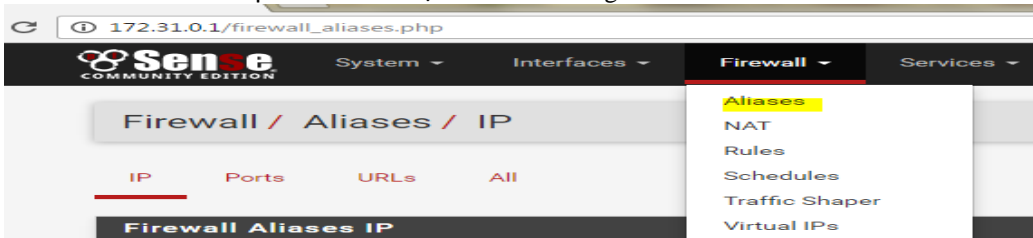


Figura 37. Configuración de Aliases  
Fuente: Pfsense

Luego se ubica la opción “IP” para adicionar las IPs de las páginas que se desean bloquear; estas IPs se pueden consultar con algunas de las herramientas en línea que hay en la web. Se da click en ADD. Aparecerá una ventana como la siguiente, ver Figura 38, donde se coloca una descripción al Alias y se procede agregar las IPs a Bloquear.

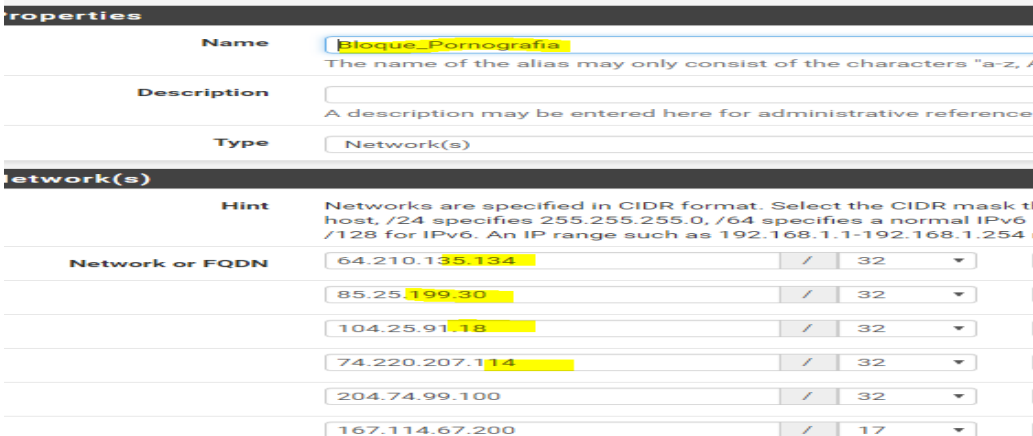
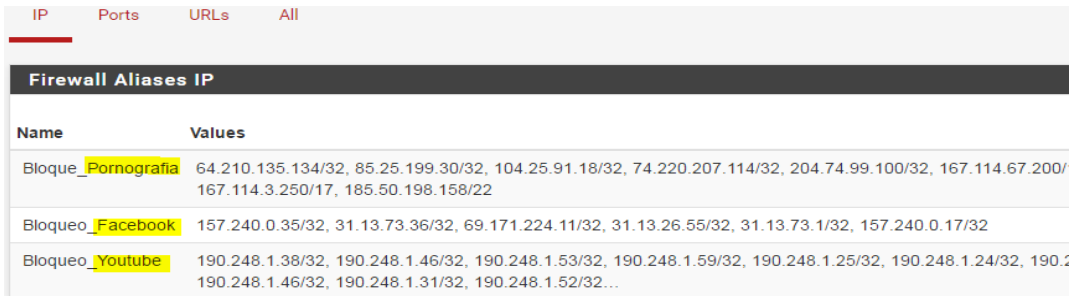


Figura 38. Parámetros de los Aliases.  
Fuente: Pfsense

Al finalizar, se da click en “Save”. Para el desarrollo del proyecto se crearon Alias para Facebook, Youtube y página de contenido sexual o pornográfico. Ver Figura 39.

 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22



Name	Values
Bloqueo_Pornografia	64.210.135.134/32, 85.25.199.30/32, 104.25.91.18/32, 74.220.207.114/32, 204.74.99.100/32, 167.114.67.200/32, 167.114.3.250/17, 185.50.198.158/22
Bloqueo_Facebook	157.240.0.35/32, 31.13.73.36/32, 69.171.224.11/32, 31.13.26.55/32, 31.13.73.1/32, 157.240.0.17/32
Bloqueo_Youtube	190.248.1.38/32, 190.248.1.46/32, 190.248.1.53/32, 190.248.1.59/32, 190.248.1.25/32, 190.248.1.24/32, 190.248.1.46/32, 190.248.1.31/32, 190.248.1.52/32...

Figura 39. Alias configurados para el Proyecto  
Fuente: Pfsense

Después de creados las Aliases, se crean las “Reglas” que aplicará el firewall de Pfsense para el bloqueo de los “Alias” creados anteriormente. Para ello, se busca en el menú /firewall/Rules. Ver Figura 40.

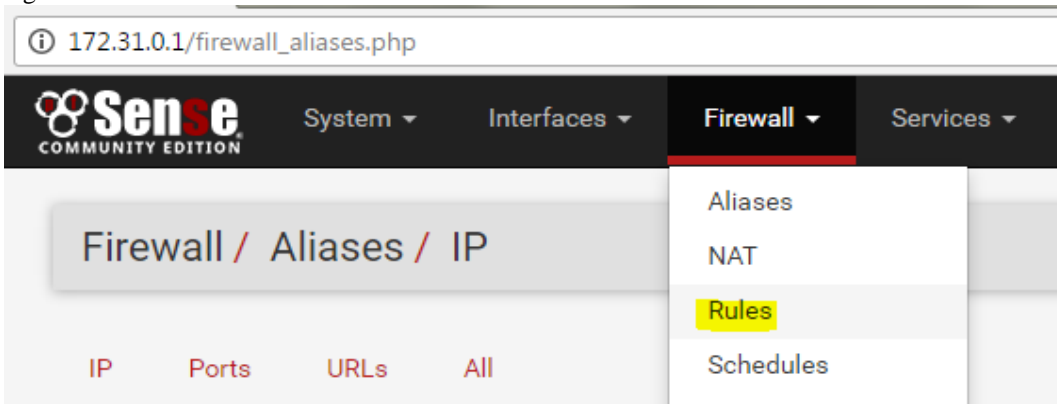


Figura 40. Configuración de las Reglas  
Fuente: Pfsense

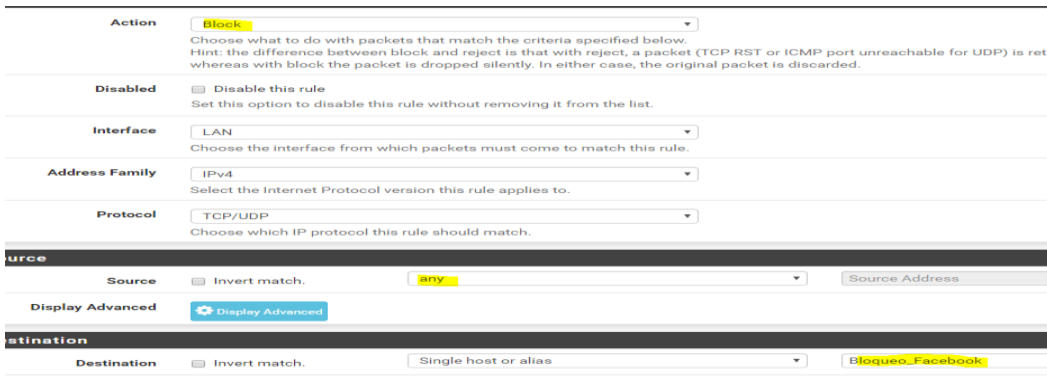
Se selecciona la interfaz de red, donde se quiere aplicar la regla. En este caso la red LAN. Y se da click en “ADD”. Ver Figura 41.



Figura 41. Interfaz de red a la que se le aplica la regla.  
Fuente: Pfsense

Aparecerá una ventana donde se selecciona el tipo de restricción a aplicar (Pass, reject, o Block). En la parte de Source, se selecciona la opción “Any”, en la parte de Destination se selecciona “Single host or alias” y se asocia el Alias que se creó anteriormente, ver Figura 42. Este proceso se debe hacer para cada uno de los Aliases que se crearon para el bloqueo de las páginas, en este caso de Facebook, Youtube y las de contenido pornográfico.

 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22



The screenshot shows the configuration of a firewall rule in pfSense. The 'Action' is set to 'Block'. The 'Interface' is 'LAN'. The 'Address Family' is 'IPv4'. The 'Protocol' is 'TCP/UDP'. The 'Source' is set to 'any'. The 'Destination' is set to 'Bloqueo\_Facebook'. The 'Display Advanced' button is visible.

Figura 42. Bloqueo de Páginas.  
Fuente: Pfsense

Después de bloqueada la página, se hacen pruebas de acceso y se verifica que no se puede acceder a la misma. Ver Figura 43.



Figura 43. Bloqueo exitoso.  
Fuente: Navegador Web.

#### 2.9.4 Instalación y configuración de servidor FTP sobre Windows server 2012 R2

Lo primero que se debe tener en cuenta es que como se trata de un servidor éste debe tener una dirección IP. Para el caso en particular, se asignó la IP 172.31.0.2. Ver Figura 44.

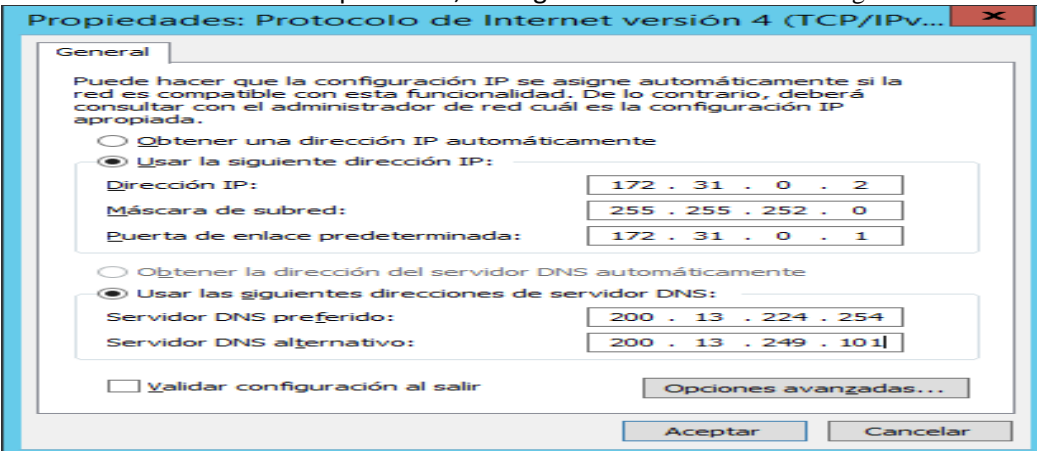


Figura 44. Configuración tarjeta de red.  
Fuente: Servidor Windows

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Lo primero que se hace es crear una carpeta en el disco local “D” del servidor, con el nombre de “Servidor FTP”. Ver Figura 45.

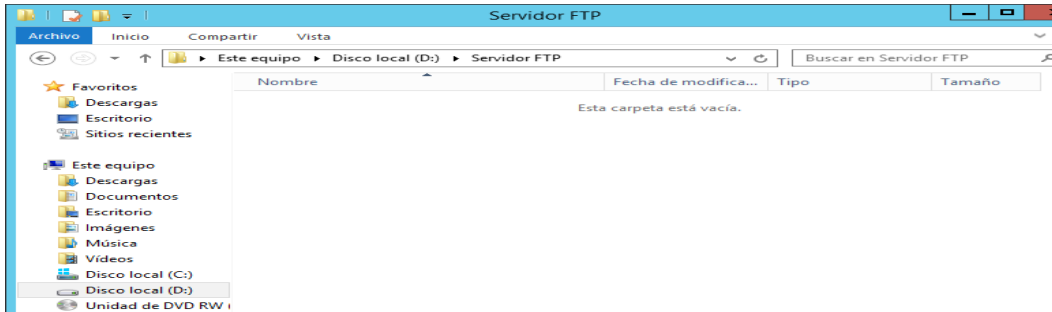


Figura 45. Creación de carpeta en Servidor FTP  
Fuente: Servidor Windows.

La Figura 46 muestra como instalar y configurar el servicio FTP. Para esto se debe ingresar a la administración del servidor, en la opción agregar roles y características; seguido de esto la opción, Tipo de instalación y se selecciona la opción Instalación basada en características y roles.

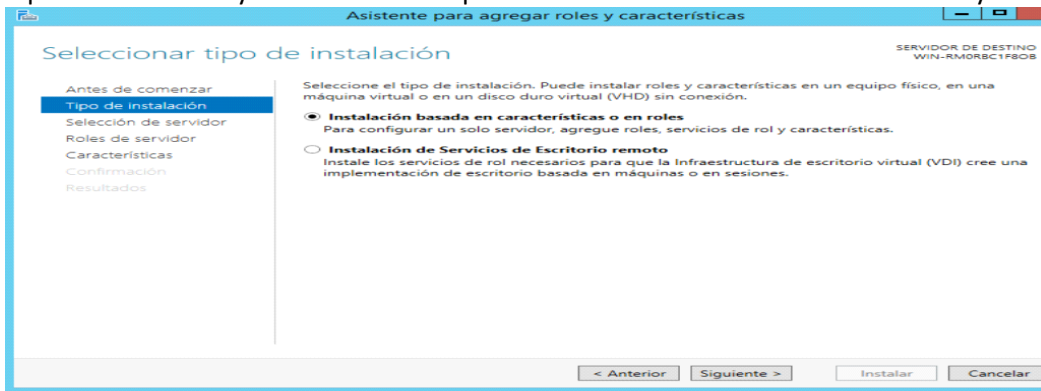


Figura 46. Instalación Servicio FTP.  
Fuente: Servidor Windows.

Después de dar clic en siguiente se pasa a la opción “Selección de servidor” en donde por defecto ya se encuentra seleccionada la opción Seleccionar un servidor del grupo de servidores, Ver Figura 47.

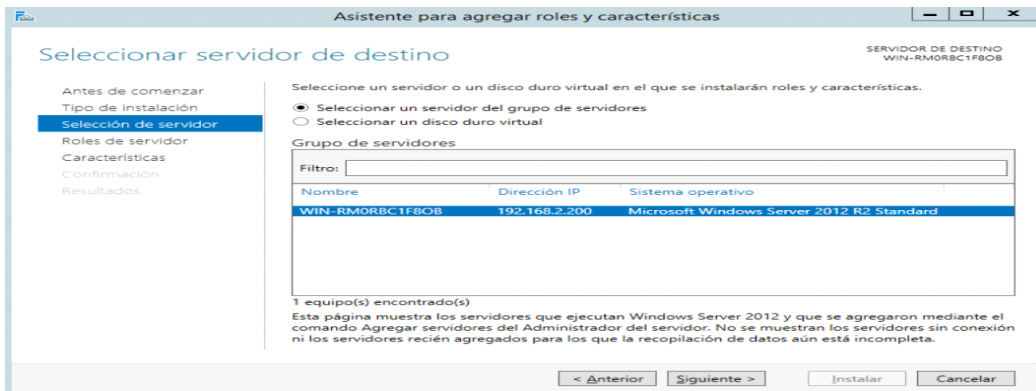


Figura 47. Configuración servicio FTP  
Fuente: Servidor Windows.

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Al hacer clic en Siguiente, se muestra una serie de roles del servidor, ver Figura 48 en donde se escoge la opción Servidor WEB(IIS) y se da clic en agregar.

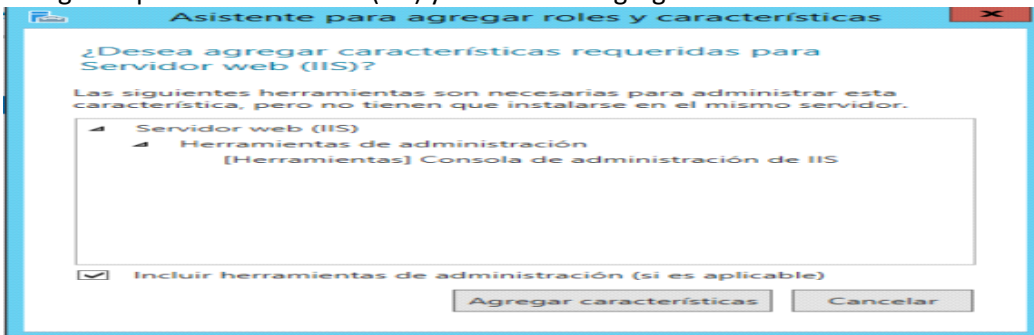


Figura 48. Configuración de Roles, servidor FTP.  
Fuente: Servidor Windows.

En la siguiente opción “Características” se da clic en siguiente, y a continuación aparece un mensaje que muestra cuáles serán las características del servidor WEB, a continuación, se da clic en Siguiente, ver Figura 49.

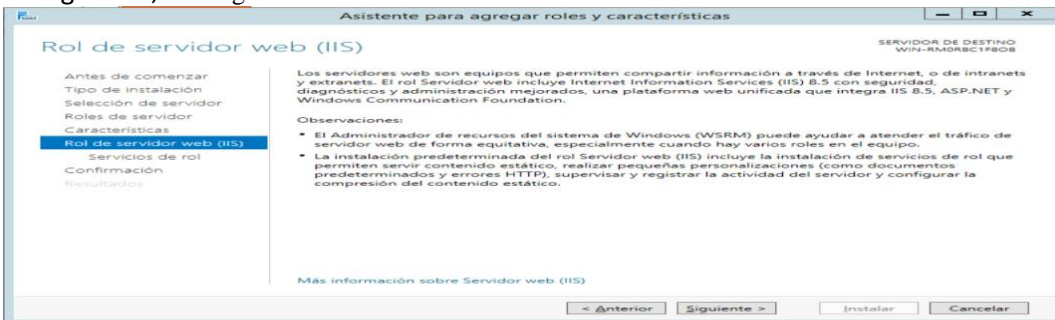


Figura 49. Rol de Servidor Web (IIS)  
Fuente: Servidor Windows.

La Figura 50 muestra la opción llamada “Servicios de rol” se escoge el servicio requerido que en el caso particular es Servidor FTP, en donde se activa el servicio FTP y extensibilidad FTP.

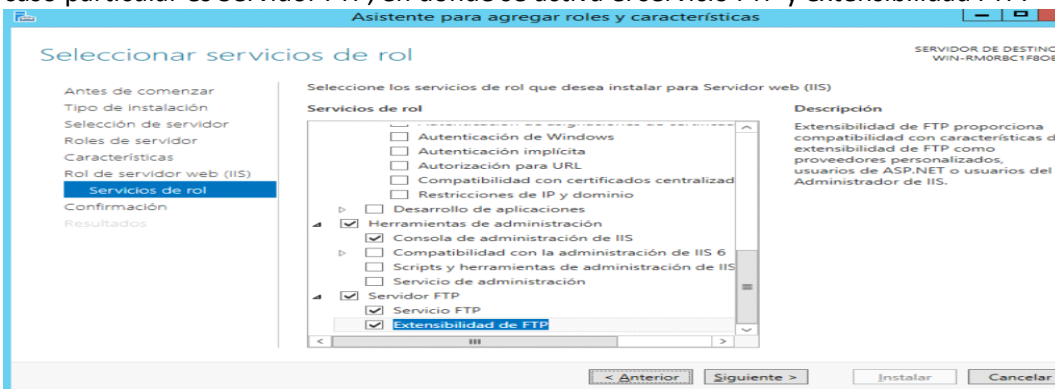


Figura 50. Configuración de Servicios de Rol.  
Fuente: Servidor Windows.



	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Una vez que se ha dado clic, en siguiente marcamos la opción reiniciar el servidor en caso de ser necesario y se da clic en instalar. Ver Figura 51.

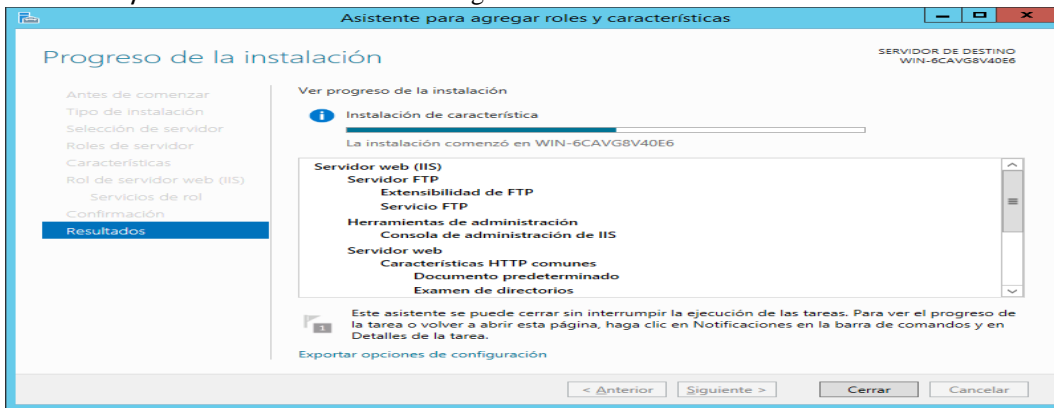


Figura 51. Finalizando Proceso de Instalación.

Fuente: Servidor Windows.

Una vez terminada la instalación se da clic en cerrar. Luego se ingresa por el menú herramientas y seleccionamos la opción "Administrador de Internet Information services (IIS)". Ver Figura 52.

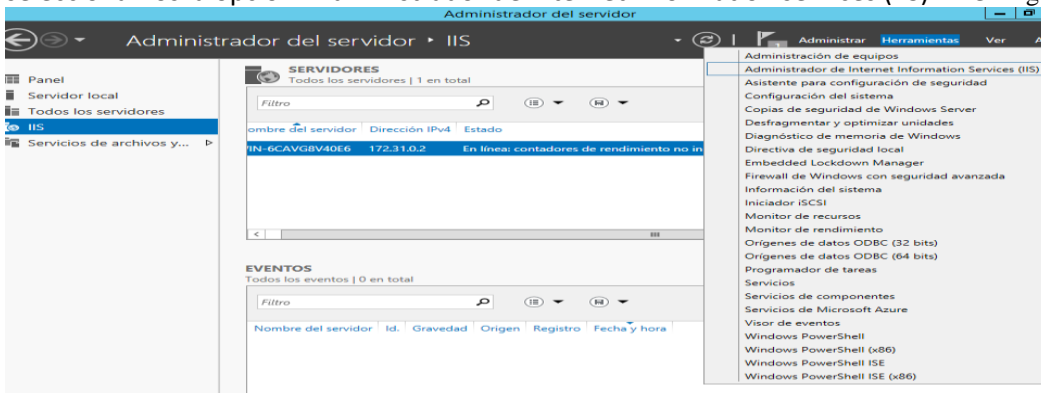


Figura 52. Configurando el servicio IIS.

Fuente: Servidor Windows.

En la parte izquierda de la ventana, ver Figura 53, se puede observar que ya se encuentra el servicio (ISS). Se debe dar clic derecho en sitios y agregar sitio FTP.

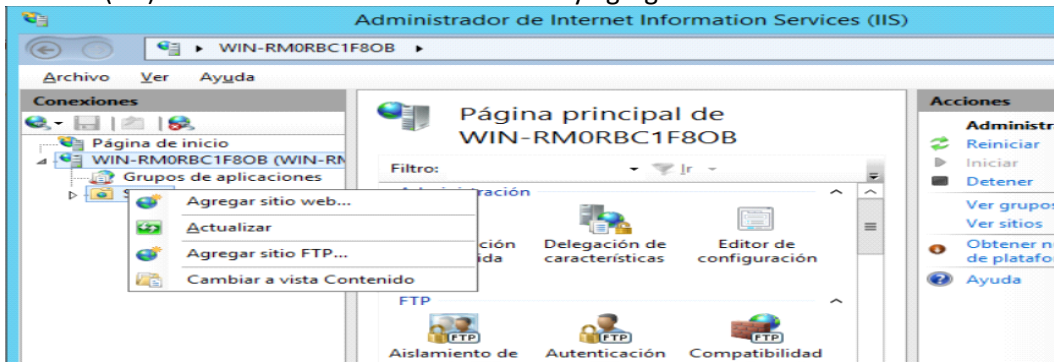


Figura 53. Agregando el Sitio FTP.

Fuente: Servidor Windows.

 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

La Figura 54 muestra la ventana en donde se debe asignar un nombre al servicio y agregar la ruta física de la carpeta que fue creada anteriormente en el disco local.

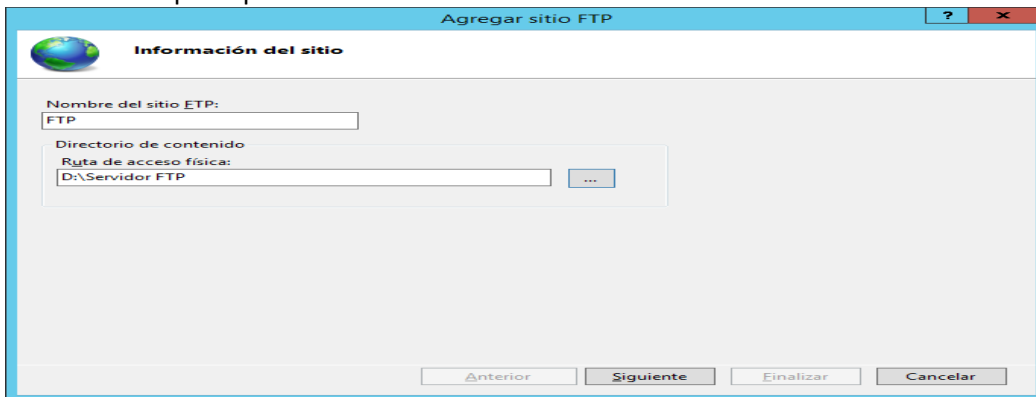


Figura 54. Asociando carpeta al servicio FTP.  
Fuente: Servidor Windows.

En la Figura 55, se selecciona la dirección IP estática que se asignó a la tarjeta de red, que para el caso en particular es la 172.31.0.2, se escoge la opción sin SSL y se da clic en siguiente.

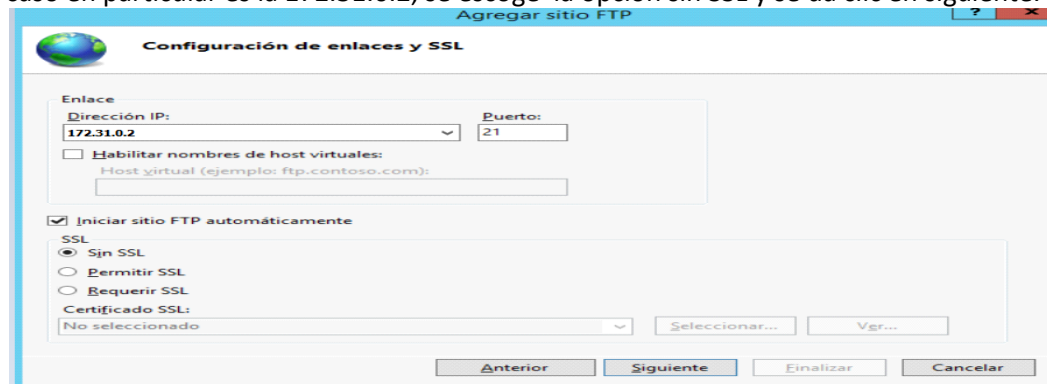


Figura 55. Configuración de Enlaces y SSL.  
Fuente: Servidor Windows.

En la Figura 56 se encuentran las opciones de autenticación en donde se activa la opción “Básica” y se otorgan el tipo de permisos que tendrán los usuarios, se asignan permisos de lectura y escritura. Se da clic en finalizar, con esto se ha creado el sitio FTP.

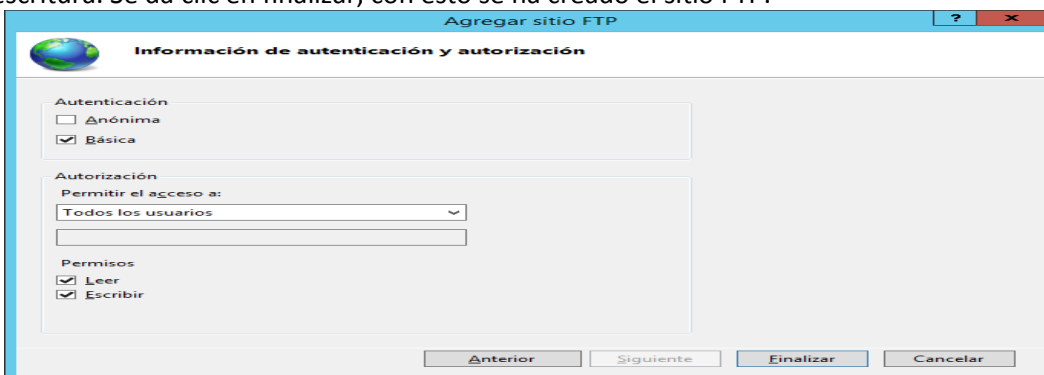


Figura 56. Autenticación y Autorización  
Fuente: Servidor Windows.

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

A continuación, se hacen una serie de pruebas para garantizar que realmente el servicio de FTP está funcionando correctamente.

En el explorador de Windows se ingresa la dirección <ftp://172.31.0.2> que es la dirección del servidor FTP, la Figura 57 muestra una ventana en donde se debe realizar la autenticación. Usuario: administrador y clave: Proyectoitm2016

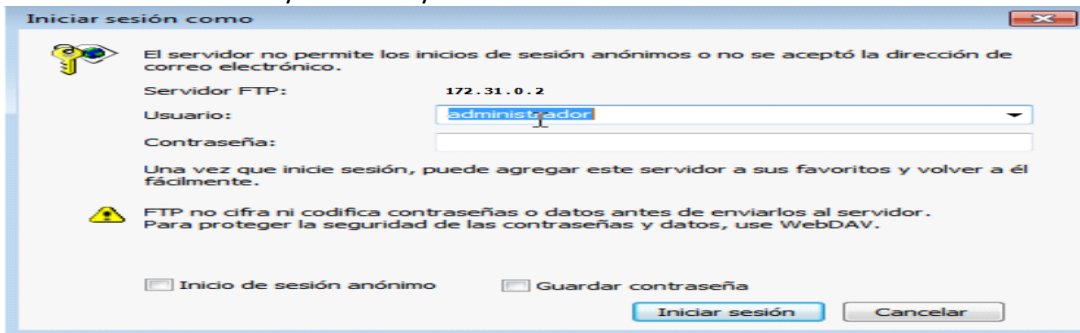


Figura 57. Pruebas de servicio FTP.

Fuente: Servidor Windows.

Si la autenticación es correcta, se tiene acceso a la carpeta del servidor FTP. Como se observa en la Figura 58.

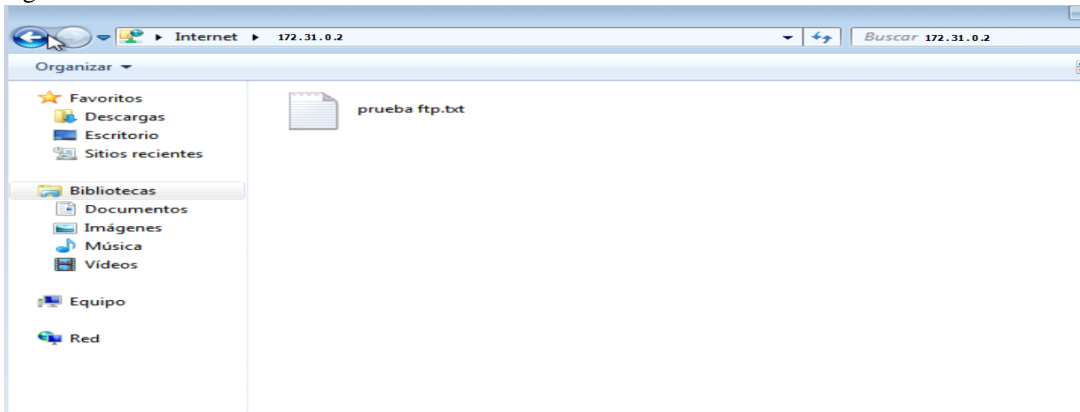


Figura 58. Acceso exitoso, servidor FTP.

Fuente: Servidor Windows.

## 3 METODOLOGÍA

Se presenta la forma como se trabajó en pro de lograr los objetivos del proyecto.

### 3.1 Diagrama en Bloque de la Solución

El proyecto se desarrolló siguiendo la metodología de diseño Top-Down recomendada por Cisco, la cual se resume en los siguientes pasos:

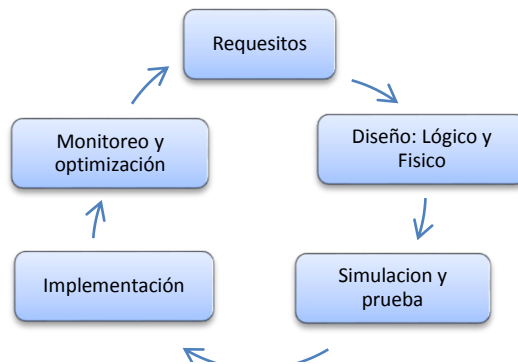


Figura 59. Diagrama de Procesos, modelo Top-Down.  
Fuente: (Oppenheimer, 2012)

### 3.2 Requisitos

Se solicitó un radio enlace que permitiera ofrecer servicio de Internet inalámbrico gratuito a cerca de 200 usuarios, habitantes del Barrio 13 de Noviembre; que los usuarios para poder disfrutar del servicio se debían autenticar en un portal cautivo; también se requirió poder ofrecer servicio de transferencia de archivos (FTP).

### 3.3 Diseño Físico y Lógico

El radio enlace mostrado en la Figura 60 se implementó utilizando radios Nano Station M2 de Ubiquiti Networks, cuyas especificaciones se muestran en el Apéndice 2.

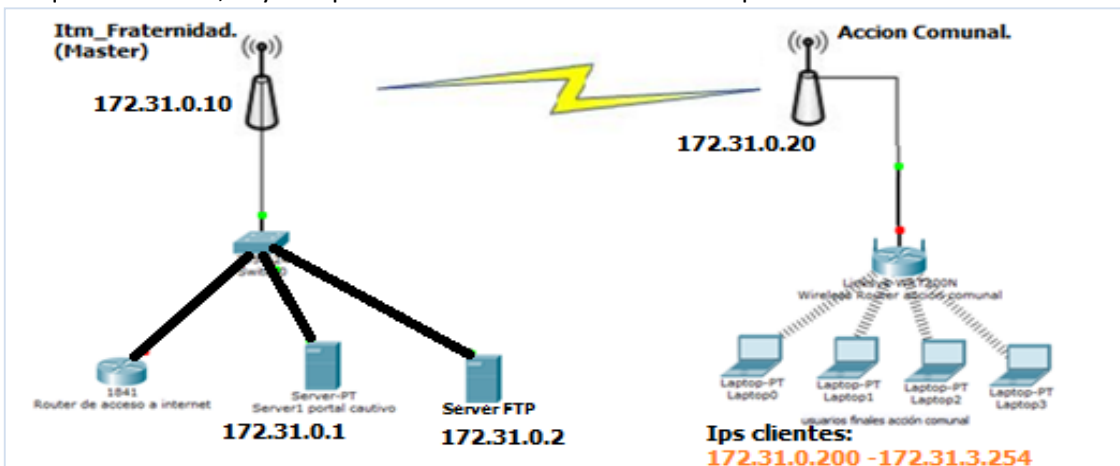


Figura 60. Diseño del Radioenlace.  
Diseño del Radioenlace con Software Packet Tracer.

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

### 3.4 Simulación y Prueba.

Con la ayuda del programa Radio Mobile y AirLink, se realizó la simulación del radioenlace que se implementó en la zona beneficiada.

En la Figura 61 se presenta la disposición de las antenas en terreno.

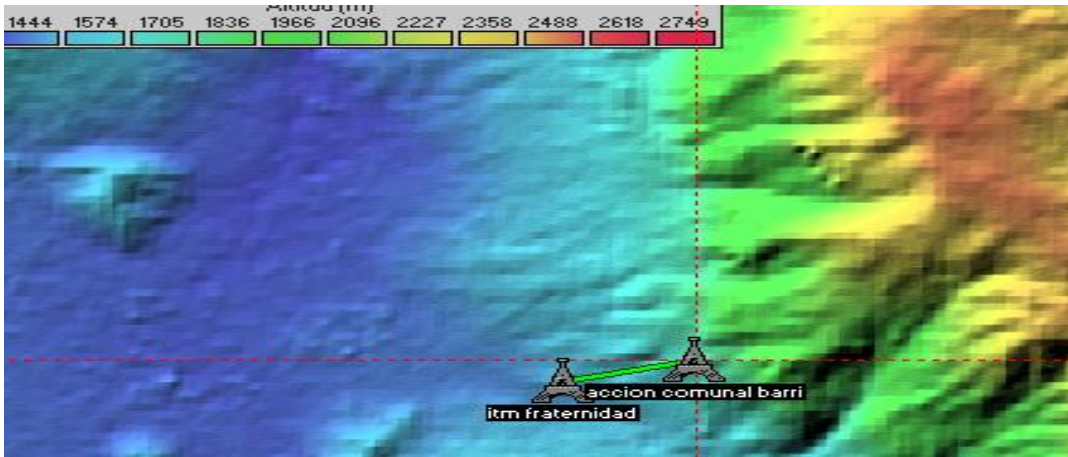


Figura 61. Disposición en Terreno del Radioenlace.

Fuente: Software Radio Mobile.

### 3.5 Implementación del Radio Enlace

Con la ayuda de la herramienta GooleEarth se ubicaron los dos puntos de referencia, el Equipo Máster, en la sede del ITM Fraternidad, ver Figura 62.

Coordenadas de ITM FRATERNIDAD, ubicación equipo Máster:

6°, 14', 43.50" Latitud Norte.

-75°, 33', 2.65" Longitud Oeste.

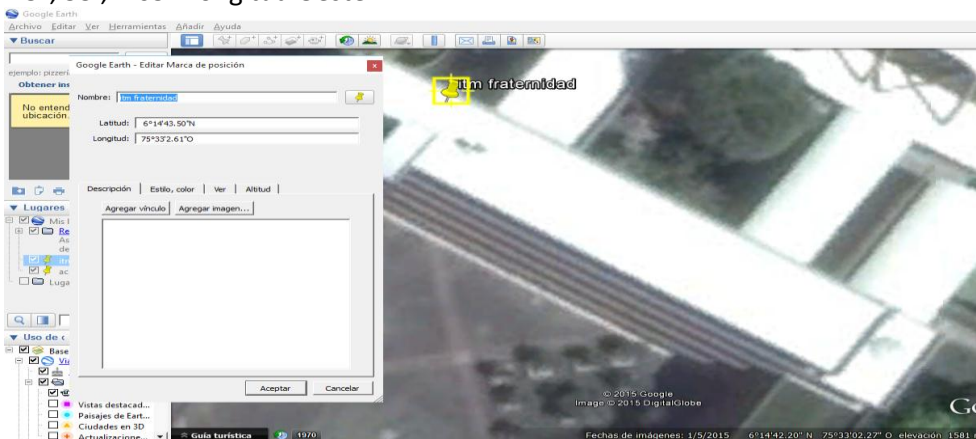


Figura 62. Coordenadas del Equipo Máster

Fuente: Google Earth, 2015

La Figura 63 muestra las coordenadas de la Sede de la Junta de Acción Comunal Barrio 13 de Noviembre.

6°, 14', 52.17" Latitud Norte.

75°, 32", 29.84" Longitud Oeste.

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

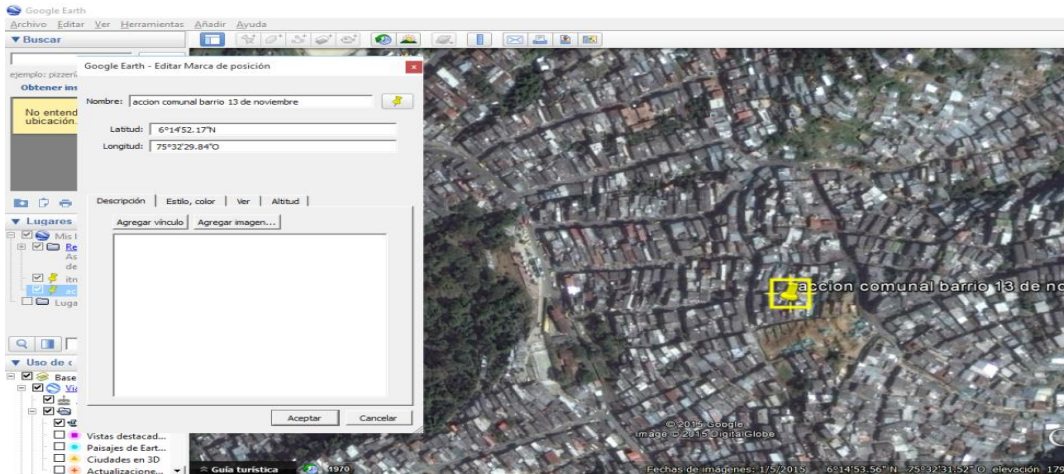


Figura 63. Coordenadas del equipo remoto.

Fuente: Google Earth, 2015

Con la ayuda de la herramienta AirLink se simuló el radio enlace entre los dos puntos y se observó que es perfectamente confiable, como lo muestra el trazo color verde; ver Figura 64.



Figura 64. Simulación del radio enlace.

Fuente: Airlink Ubiquiti 2015.

Al configurar los parámetros de ubicación geográfica del radio enlace, se obtuvo una distancia aproximada de 1.15 kilómetros, la misma herramienta AirLink permitió simular los dispositivos de radio seleccionados, evidenciando como se muestra en la Figura 65, que se ajustan a las necesidades pues se tiene línea de vista clara hacia la estación remota y los niveles de potencia recibida en los extremos se encuentran en rangos

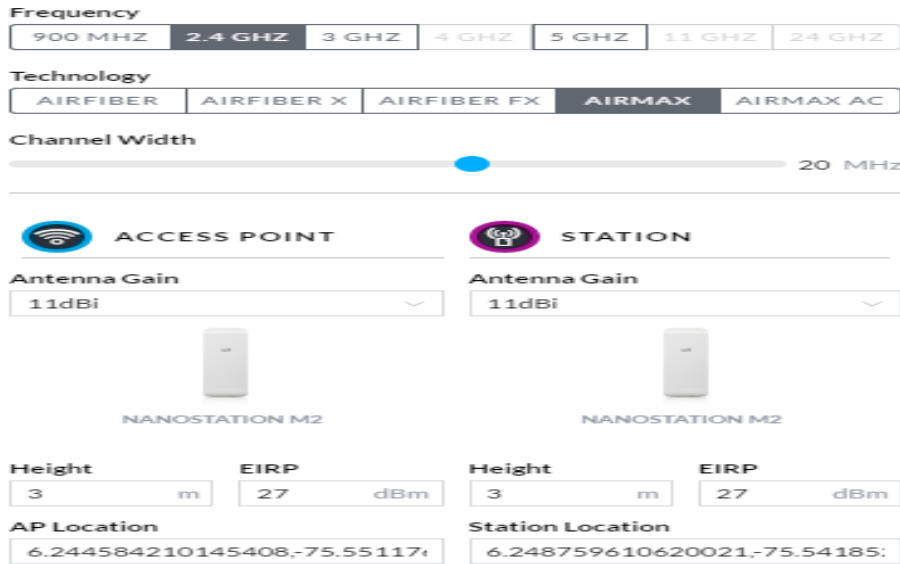


Figura 65. Simulación utilizando los equipos seleccionados (Nano station M2).  
 Fuente: AirLink Ubuquiti 2016.

La Figura 66 muestra parámetros como la potencia de la señal del transmisor y el receptor, la capacidad total del canal y el tipo de modulación utilizada dentro de rangos aceptables.

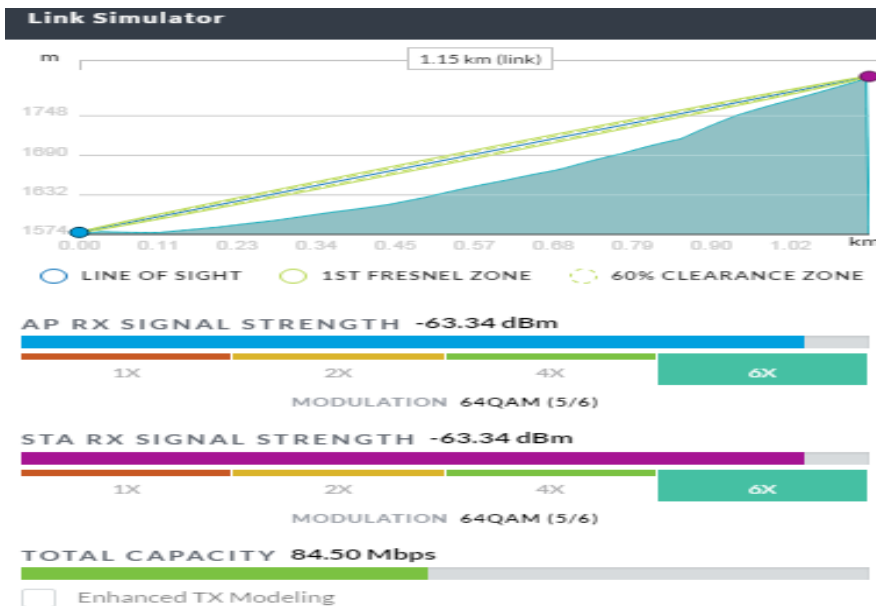


Figura 66. Resultados de la simulación del enlace con los equipos seleccionados.  
 Fuente: AirLink Ubuquiti 2016.

 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

### 3.5.1 Configuración del Punto de Acceso (ITM Fraternidad)

Se accede al equipo a través del navegador de Internet, por medio de la IP <http://172.31.0.10>; con el usuario “admin” y la contraseña “wifi13”. La Figura 67 muestra los parámetros de configuración de la pestaña “Main” del Equipo Máster, que estará instalado en el ITM Fraternidad.

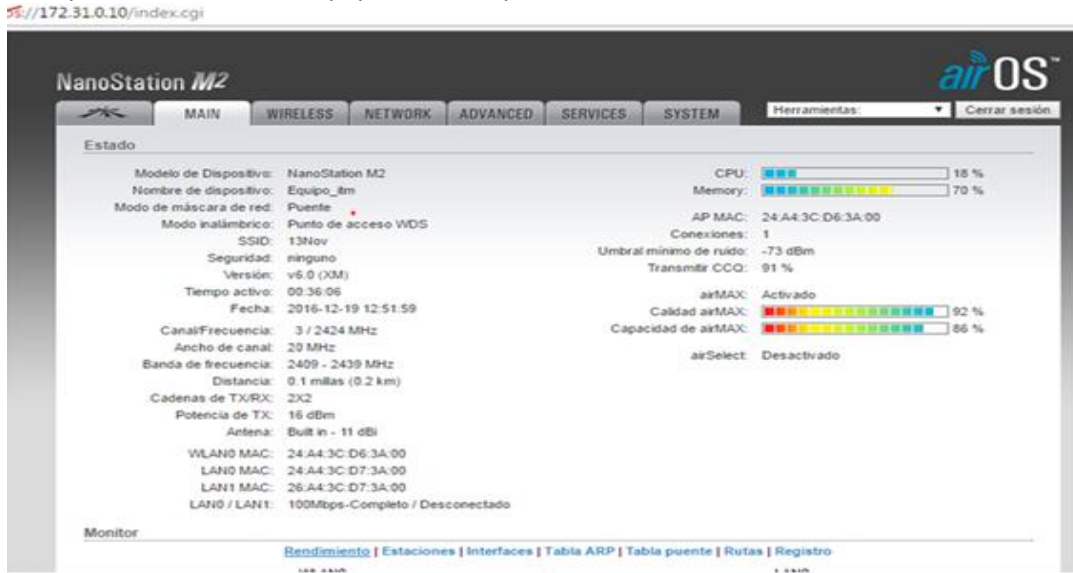


Figura 67. Configuración pestaña “Main” del Equipo Máster.

Fuente: NanoStation M2. 2016

La Figura 68 muestra la forma como se configura los parámetros en la pestaña “Wireless”. Se observa el Modo de Inalámbrico, el SSID (13Nov) de la red, ancho de banda del canal, la frecuencia de trabajo, la cual se estableció fija y el tipo de Seguridad que tendrá el Radio enlace.

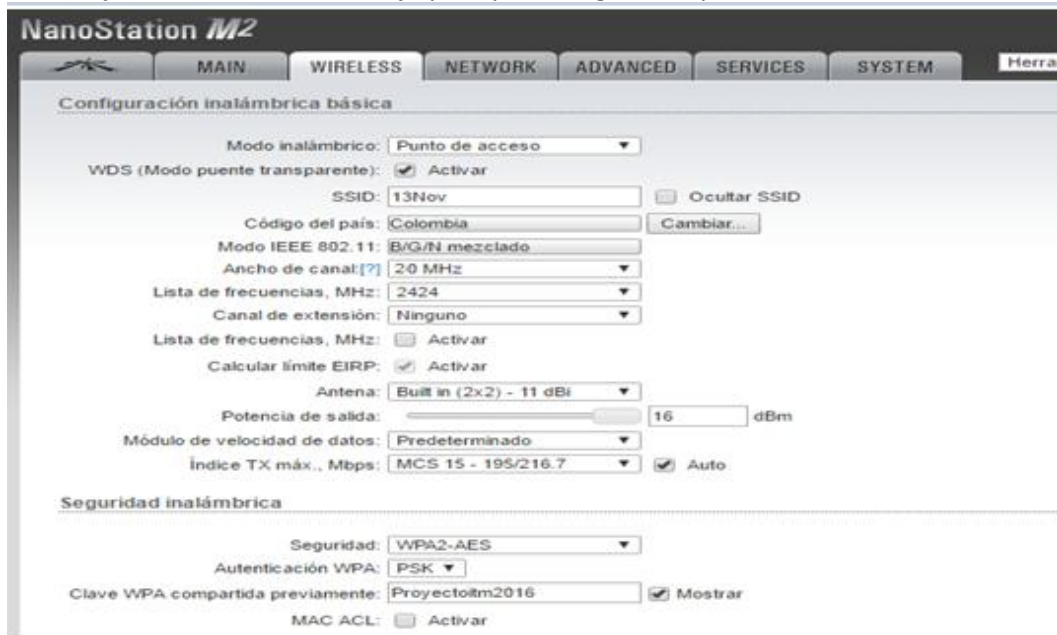


Figura 68. Pestaña de Wireless en la configuración del Equipo Máster.

Fuente: NanoStation M2. 2016



 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

La Figura 69 muestra la forma como se configuró la pestaña “Network” del Equipo Máster.

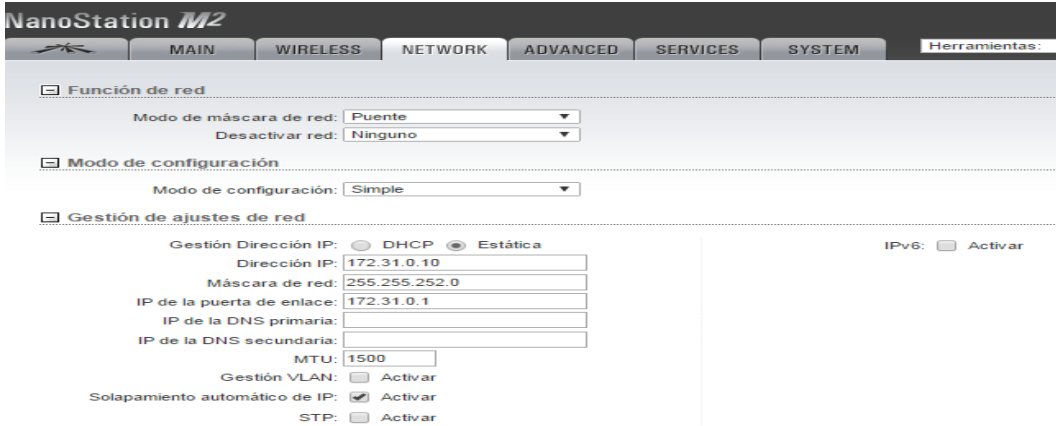


Figura 69. Pestaña de Network en la Configuración del Equipo Máster.  
Fuente: NanoStation M2. 2016.

La Figura 70 muestra la pestaña “Advanced” del Equipo Máster.

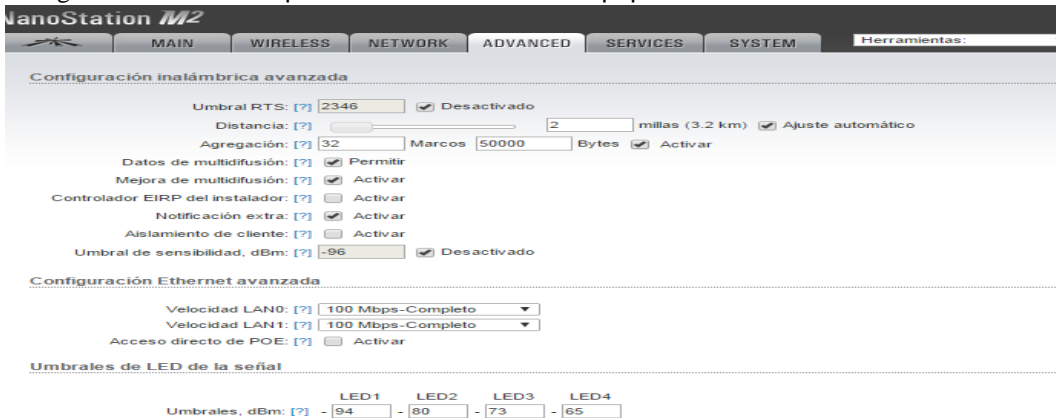


Figura 70. Pestaña de Configuración Advanced del Equipo Máster.  
Fuente: NanoStation M2. 2016.

La Figura 71 muestra la forma como se configura la pestaña “Services” en el Equipo Máster.

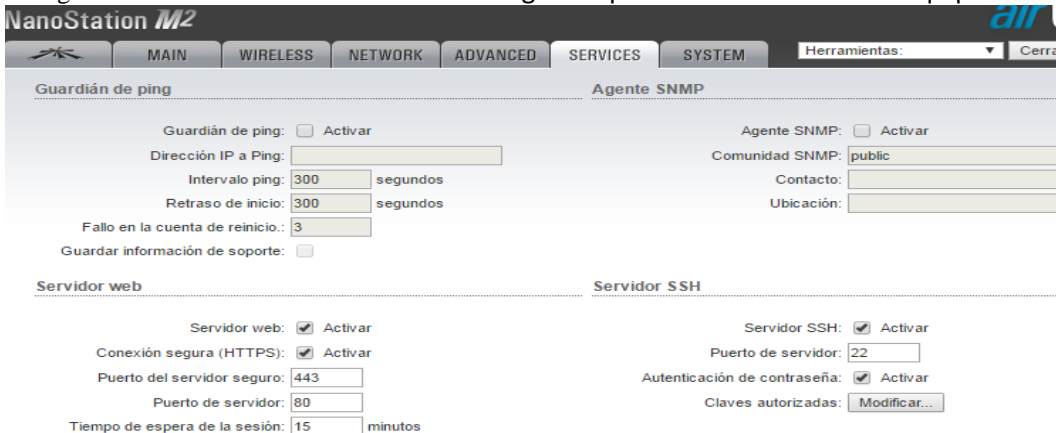


Figura 71. Pestaña de Configuración Services del Equipo Máster.  
Fuente: NanoStation M2. 2016.

 <b>Institución Universitaria</b>	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

La Figura 72 presenta la forma como se deja la configuración de la pestaña “System”.

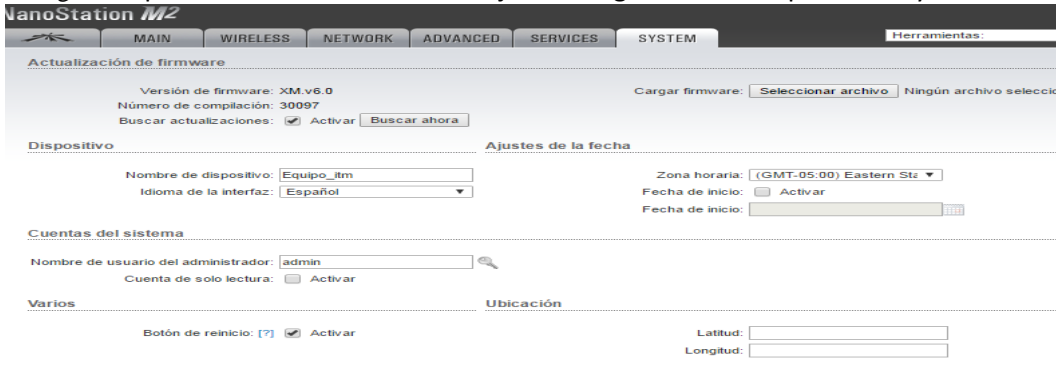


Figura 72. Pestaña de Configuración System del Equipo Máster.  
Fuente: NanoStation M2. 2016.

### 3.5.2 Configuración del Equipo Estación (Junta de Acción Comunal, barrio 13 de Noviembre)

Se accede al equipo a través del navegador de Internet, por medio de la Ip <http://172.31.0.20>; con el usuario “admin” y la contraseña “wifi13”. La Figura 73 muestra la pestaña Equipo remoto o Estación, que se encuentra en el Barrio 13 de Noviembre.



Figura 73. Pestaña de Configuración Main del Equipo Estación.  
Fuente: NanoStation M2. 2016.

La Figura 74 muestra la forma de cómo se configura el apartado “Wireless” del Equipo Estación.

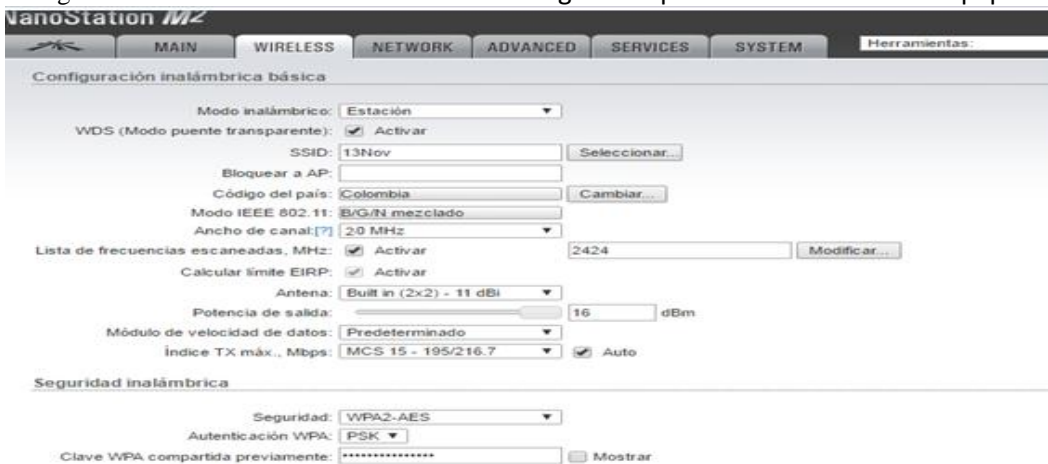


Figura 74. Pestaña de Configuración Wireless del Equipo Estación.  
Fuente: NanoStation M2. 2016.

 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

La Figura 75 muestra la forma de cómo se configura el apartado “Network” del Equipo remoto o Estación, que se encuentra en el Barrio 13 de Noviembre.

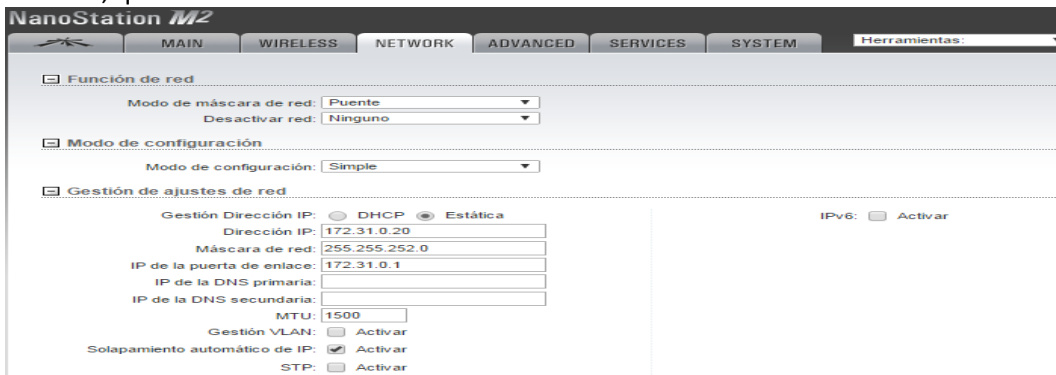


Figura 75. Pestaña de Configuración Network del Equipo Estación.  
Fuente: NanoStation M2. 2016.

La Figura 76 muestra la forma de cómo se configura el apartado “Advanced” del Equipo Estación.

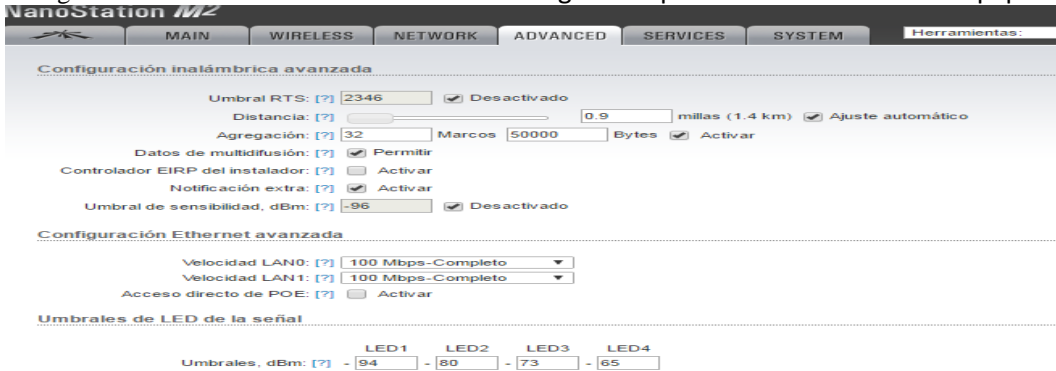


Figura 76. Pestaña de Configuración Advanced del Equipo Estación.  
Fuente: NanoStation M2. 2016.

La Figura 77 muestra la forma de cómo se configura el apartado “Services” del Equipo Estación.

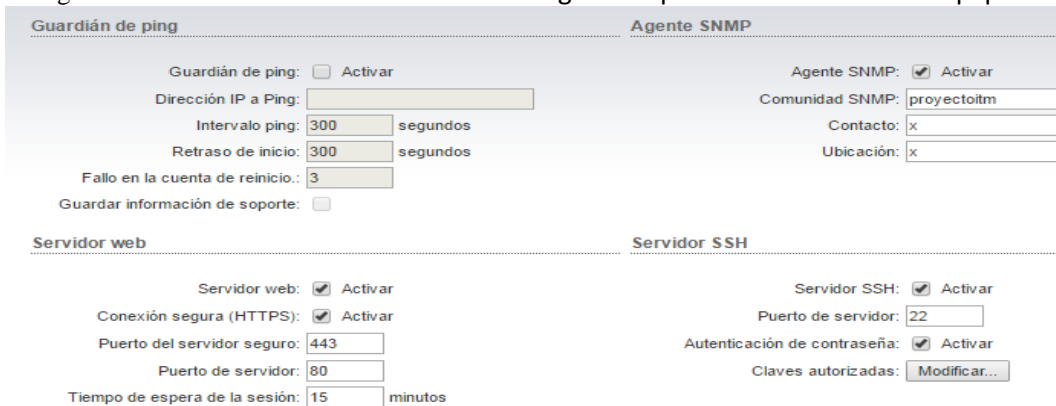


Figura 77. Pestaña de Configuración Services del Equipo Estación.  
Fuente: NanoStation M2. 2016.

La Figura 78 muestra la forma de cómo se configura el apartado “System” del Equipo Estación.

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

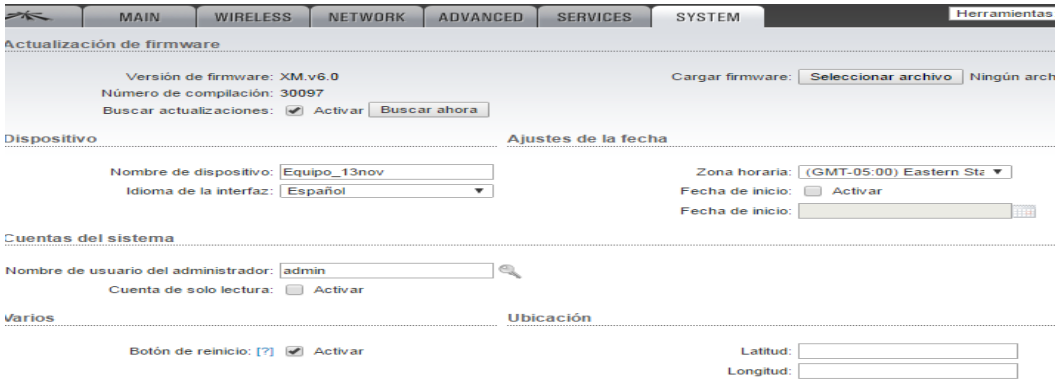
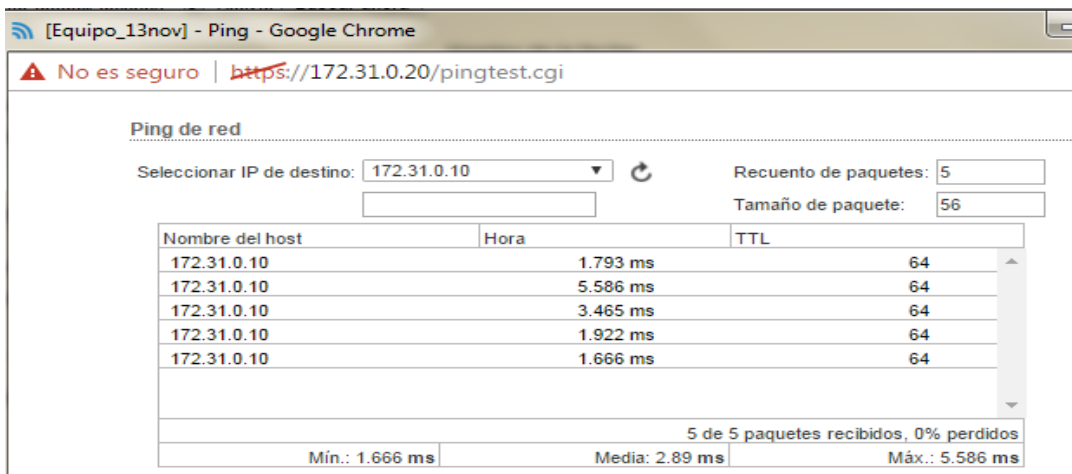


Figura 78. Pestaña de Configuración System del Equipo Estación.  
Fuente: NanoStation M2. 2016.

### 3.6 Monitoreo y Optimización

Luego de la implementación del radio enlace se usaron herramientas de monitoreo como AirView, pruebas de Ping y test de velocidad; que permitieron obtener métricas y estadísticas del radio enlace con el fin de garantizar un óptimo funcionamiento del mismo. En la Figura 79 se muestra una captura del resultado del Ping entre la Estación remota y el Máster, y se pudo apreciar que no se presentan pérdidas de paquetes, la media del tiempo de envío y recepción del Ping es de 2.89 ms, lo que garantiza la conectividad.



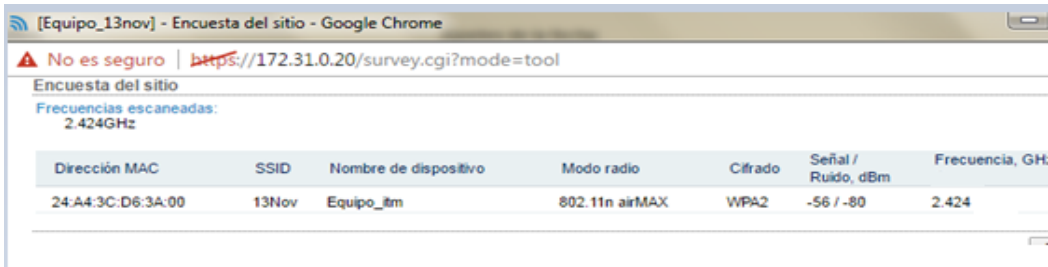
Nombre del host	Hora	TTL
172.31.0.10	1.793 ms	64
172.31.0.10	5.586 ms	64
172.31.0.10	3.465 ms	64
172.31.0.10	1.922 ms	64
172.31.0.10	1.666 ms	64

5 de 5 paquetes recibidos, 0% perdidos  
Mín.: 1.666 ms      Media: 2.89 ms      Máx.: 5.586 ms

Figura 79. Resultados de la prueba de Ping desde la Estación hacia el Equipo Máster.  
Fuente: Herramientas del NanoStation M2. 2016.

La Figura 80 muestra los resultados de la medición de la relación señal a ruido en el sistema. Se puede apreciar que S/N es de -56/-80 dBm, que resultan ser aceptable para el enlace implementado.

 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22



Dirección MAC	SSID	Nombre de dispositivo	Modo radio	Cifrado	Señal / Ruido, dBm	Frecuencia, GHz
24:A4:3C:D6:3A:00	13Nov	Equipo_itm	802.11n airMAX	WPA2	-56 / -80	2.424

Figura 80. Resultados relación Señal a Ruido (S/N) del Sistema.  
 Fuente: Herramientas del NanoStation M2. 2016.

La Figura 81 muestra el resultado de la prueba práctica de velocidad del radio enlace, donde se obtuvieron valores cercanos a los 55.16 Mbps, si se tiene en cuenta que en la simulación realizada, ver Figura 65, se tenía una capacidad del canal de 84.5 Mbps; la prueba se realizó desde la Estación Remota hacia el Equipo Máster.



<https://172.31.0.20/sptest.cgi>

**Prueba de velocidad de red**

Seleccionar IP de destino:

Usuario:

Contraseña:

Puerto WEB remoto:

**Resultados de la prueba**

RX: 36.58 Mbps

TX: 18.58 Mbps

Total: 55.16 Mbps

Figura 81. Resultados de la prueba de velocidad del Sistema.  
 Fuente: Herramientas del NanoStation M2. 2016.

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

## 4 RESULTADOS Y DISCUSIÓN

A partir de las pruebas realizadas se logró configurar un radio enlace que trabaja en la banda ICM de frecuencias libre de 2.4 GHz; presentó una conectividad estable como se pudo observar en la prueba de ping realizada, ya que no se presentaron pérdidas de paquetes y la tasa media de envío y recepción del ping es 2.89 ms, ver Figura 79.

El radio enlace quedó establecido entre la Sede del ITM Fraternidad como Equipo Máster, y la Sede de la Junta de Acción Comunal del Barrio 13 de Noviembre como Estación Remota, con una distancia aproximada de 1.2 Km.

La Figura 82 muestra la disposición final de las antenas, superpuestas en una brújula para apreciar el ángulo de elevación ( $22^\circ$ , Equipo Máster) y de inclinación ( $248^\circ$ , Estación Remota).

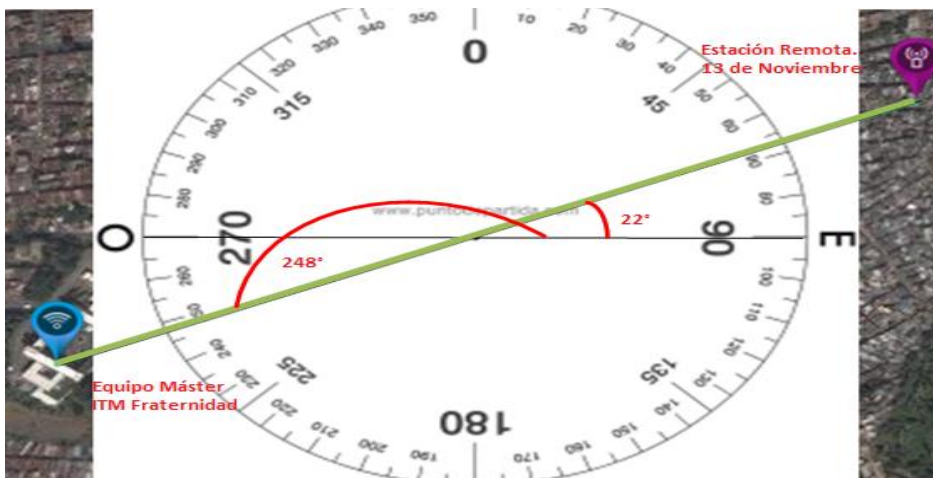


Figura 82. Ángulos de Elevación e Inclinación de las antenas dispuestas.

Fuente: Herramienta AirLink, Nano Station, 2016. Superposición, Autor.

Ubicar el mejor rango de frecuencias también jugó un papel fundamental, con la herramienta AirView se logró evidenciar qué tan saturado se encontraba el espectro electromagnético y permitió seleccionar el rango de frecuencias con menor saturación; para el proyecto se escogió el valor de 2.424 GHz como frecuencia central, tal y como se observa en la Figura 83, los colores fríos (azul y violeta) reflejan el espectro con menor saturación, mientras que los colores cálidos (amarillo y rojo) representan el espectro más ocupado.

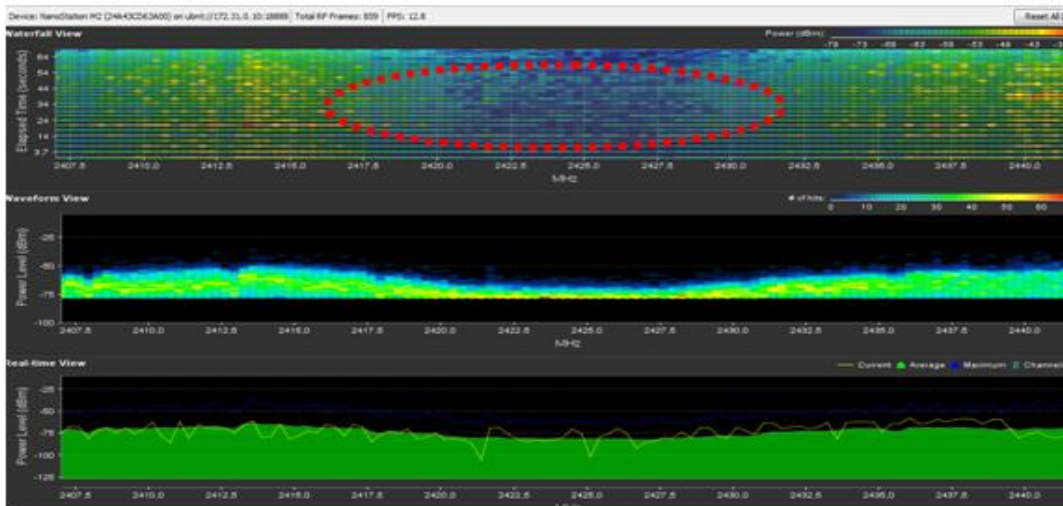


Figura 83. Saturación del espectro electromagnético.  
 Fuente: Herramienta AirView Nano Station M2, 2016.

De forma similar, pero a nivel de canales se observa en la Figura 84, por lo que se determinó utilizar el Canal 3, con un ancho de banda de 20 MHz, ya que éste solo presentó un uso de 20.2%.

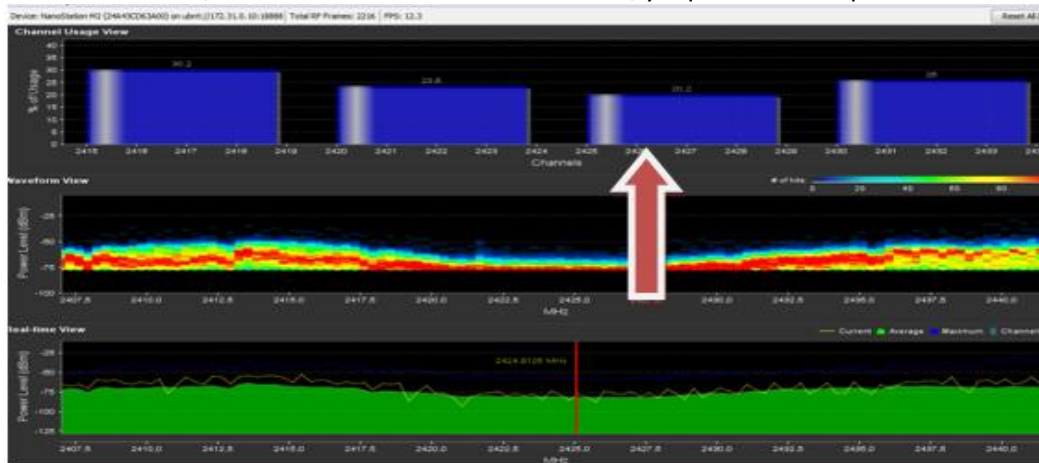


Figura 84. Porcentaje de utilización de los Canales.  
 Fuente: Herramienta Airview, Nano Station M2, 2016.

Al tener en cuenta factores que afectan directamente las comunicaciones inalámbricas y en particular las bandas de frecuencias libres de 2.4 GHz, se pudo lograr una solución aceptable al problema planteado, ya que en la práctica se logró obtener una velocidad de 55.16 Mbps, como se mostró anteriormente y que representa más del 65% de la capacidad real del canal, según el resultado de la simulación del radio enlace que se presentó en la Figura 66.

En la Figura 80, se presenta el resultado de la relación señal a ruido, cuyo valor fue de -56/-80 dBm, lo que quiere decir que se tienen 24 dB, que pueden ser suficientes para lograr velocidades mayores a los 20 Mbps, según la tabla publicada en el sitio web:

<https://www.nireleku.com/2013/01/entendiendo-la-relacion-senal-ruido-y-la-atenuacion/>

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

El diseño físico del proyecto quedó dispuesto de la siguiente manera: Para la conexión a Internet, desde el ITM Fraternidad se utilizó el puerto 2, del Router Mikrotik CCR1009-8G-1S-1S+ Giga Ethernet, Ver Figura 85.



Figura 85. Puerto del router Mikrotik utilizado para la conexión a Internet.  
Fuente: Mikrotik.

Desde el Router Mikrotik CCR1009-8G-1S-1S+, se establece una conexión a través del puerto Giga Ethernet “G1” Troncal, del Switch D-Link Des-3010 F. Ver Figura 86.



Figura 86. Puerto de conexión entre router Mikrotik y Switch D-Link.  
Fuente: Autor.

Para llevar la conexión de Internet hasta la interfaz WAN del servidor PfSense, desde el mismo Switch D-Link Des-3010F se utilizó el puerto 1 mostrado en la Figura 87.



Figura 87. Puerto de conexión hacia la interfaz Wan del Pfsense.  
Fuente: Autor.



 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Se lleva luego la conexión a la interfaz LAN del PfSense por medio del Puerto 1 del switch Cisco Catalyst 2960 de 24 Puertos. Desde el mismo Switch también se establecen conexiones para el Equipo Máster por medio del Puerto 2, y para el servidor FTP desde el Puerto 3.



Figura 88. Puertos de conexión para la interfaz LAN del Pfsense y los demás equipos.  
Fuente: Autor.

Gráficamente se pueden observar estas conexiones físicas en la Figura 89

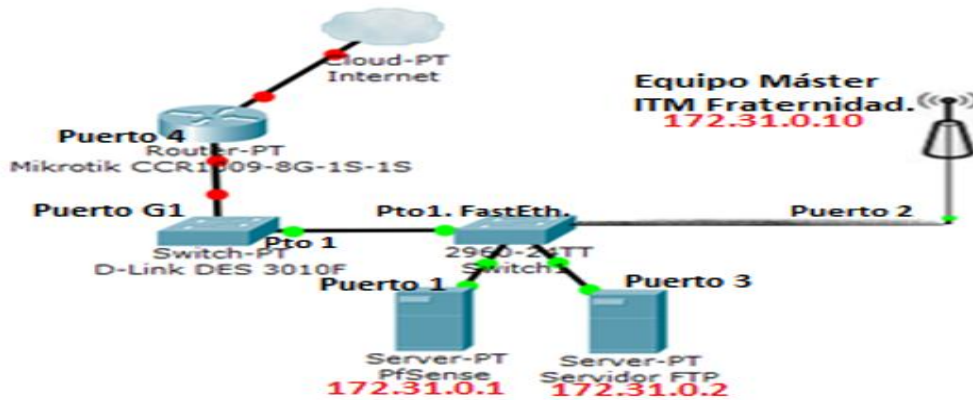


Figura 89. Conexión física de equipos en el laboratorio del ITM  
Fuente: Autor.

La disposición final en campo de los equipos del radio enlace, se puede ver en la Figura 90.



Figura 90. Disposición en terreno de los equipos del radio enlace: Estación Remota y Equipo Máster.  
Fuente: Autor.

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

## 5 CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

---

### CONCLUSIONES.

Se diseñó e implementó un radio enlace que utiliza radios Ubiquiti Nano Station M2, que previamente simulado indicó que se podía alcanzar una velocidad de 84.50Mbps, pero que en la práctica, finalmente quedó transmitiendo a 55.16 Mbps, sin pérdida de paquetes como lo demuestran las pruebas de conectividad realizadas con el comando ping. Además, mediante pruebas de monitoreo se obtuvo una relación señal a ruido aceptable para brindar acceso a Internet gratuito a los usuarios del barrio Trece de Noviembre, ubicado en la comuna 8 de Medellín, a 1.2 km de la sede Fraternidad del ITM. Para que los usuarios accedan al servicio, deben autenticarse previamente con un usuario y contraseña válidos a través de un portal cautivo PFSense implementado por software.

Siguiendo la metodología Top Down de Cisco, se definieron los requisitos iniciales y se planteó un diseño lógico con direcciones IP Privadas clase B con máscara de 22, cuyo rango es: 172.31.0.200 a 172.31.3.254 para los clientes que se conectarán a través de los Access Points en la Estación Remota. Se estableció una IP estática para el Equipo Máster que fue 172.31.0.10 y otra para la Estación Remota (172.31.0.20). Para el diseño físico, se utilizaron equipos Ubiquiti Nano Station M2, cuya ganancia es de 11dBi, trabajando a una frecuencia fija de 2.424 GHz, y con ancho de banda de 20 MHz para el canal. El radio enlace se simuló utilizando la herramienta AirLink, y se realizaron pruebas de monitoreo como test de velocidad, relación señal a ruido de -56/-80dBm y análisis espectral con la herramienta AirView.

También se implementó un Portal Cautivo tipo software, llamado Pfsense, por medio del cual los usuarios se autentican para disfrutar del servicio de Internet gratuito. La versión del Pfsense instalada fue la 2.3.1-Release (Amd 64); cuya arquitectura está basada en el Sistema Operativo FreeBSD. El Pfsense también ofrece funcionalidades como Firewall, Proxy, Lista de Control de Acceso (ACL); igualmente herramientas de gestión como asignación de ancho de banda, prioridad de tráfico, log de eventos, QoS, entre otras.

Para el servicio de transferencia de archivos (FTP), se utilizó un Windows Server 2012 R2, al cual se le asignó la IP estática 172.31.0.2; éste tiene una capacidad de almacenamiento en disco disponible de 150 GB. Para este servicio, los usuarios deben ingresar también con un usuario y contraseña.

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

## **RECOMENDACIONES**

Si bien no se probó la capacidad que pueda tener el radio enlace para otorgar conectividad Wifi a 200 usuarios de forma simultánea es probable que esto se pueda lograr segmentándolos, de tal manera que accedan por medio de distintos Access Points, conectados a través de un Switch de la Estación Remota. También se podrían utilizar platos en cada antena, con el fin de concentrar mejor la cantidad de energía irradiada, lo que representa mayor directividad y por ende una mejor ganancia.

Sería bueno que para los proyectos posteriores y en particular de aquellos que surjan de una idea de un Docente, se defina el alcance o los aportes por parte del Docente y/o la Institución, en nuestro caso en particular hubo algunos inconvenientes al momento de definir los aportes económicos del Docente y/o de la institución, lo que sin lugar a dudas representa pérdida de tiempo, vital para el desarrollo satisfactorio de los proyectos.

Se evidenciaron falencias igualmente en la asignación de los recursos que eran la materia prima del proyecto, como lo era la asignación del canal de internet y las estaciones de trabajos (Servidores) requeridas para la implementación del proyecto.

## **TRABAJO FUTURO**

Se espera que este proyecto sirva como hoja de ruta para continuar implementando nuevos enlaces de radio, que permitan a otros sectores aledaños al Trece de Noviembre disfrutar del servicio gratuito de Internet, de esta forma se continúa reduciendo la brecha tecnológica que padecen estos sectores marginados de la ciudad.

Se espera que futuros proyectos implementen enlaces hacia otros puntos, cambiando a una topología Punto-Multipunto más elaborada, que permita llegar a más lugares como: parques, plazoletas o zonas comunes.

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

## REFERENCIAS

---

- Aguirre, D. (19 de 11 de 2015). Habitante y Comerciante del Sector. (W. S. Renee Diaz, Entrevistador)
- Andrews, J. (2007). Fundamentals of WiMAX: understanding broadband wireless. Estados Unidos: Prentice Hall.
- Delgado, V. M. (20 de 05 de 2014). AULA DE SOFTWARE LIBRE. Obtenido de <https://www.uco.es/aulasoftwarelibre/375-implementacion-de-un-portal-cautivo-con-wifidog/>
- Dpto. Adtvo. de Planeacion de Medellin. (2008). la comuna 8 memoria y territorio.
- Flickenger, R., Aichele, C., & Buittrich, S. (2008). Redes Inalámbricas en Paises en Desarrollo. Hacker Friendly.
- Garces Cardona, F. (2008). Medellin.
- Garcia, C., Quezada, C., & Bello, D. (14 de 07 de 2010). slideshare.net. Obtenido de <http://es.slideshare.net/valericio1/portal-cautivo>
- Garcia, R. J. (2012). instalaciones de radiocomunicaciones. En G. M. Santiago. Madrid: ediciones paraninfo.
- Ministerio de las TICs. (2003). Bandas radioeléctricas sin licencia. Tecnologías Wi-Fi, 75.
- Molina, F. (04 de 01 de 2015). Calculos primera zona de fresnel. Obtenido de <http://www.franciscomolina.cl/2015/01/04/calculos-primera-zona-de-fresnel/>
- Oppenheimer, P. (2012). Top-Down Network Design Third Edition. Indianapolis, IN 46240 USA: Cisco Press.
- Poole, A. C. (1 de 08 de 2014). Radio-Electronics.com. Obtenido de <http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11-standards-tutorial.php>
- Sweeney, D. (2006). Wimax:Operator´s Manual. New York: Apress.
- Technologies, G. I.-I. (02 de 01 de 2003). Grupo IRC. Obtenido de <http://www.radiocomunicaciones.net/radio-enlaces.html>
- Wi-Fi, N. I. (s.f.). radio comunicaciones. Obtenido de <http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11-standards-tutorial.php>

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

# APÉNDICE

## Apéndice A.

### Calculando la Zona de Fresnel

Fórmula sin obstáculos:

$$r = 17,32 * \sqrt{(d/4f)}$$

**d** = Distancia total entre transmisor y receptor (km).

**f** = Frecuencia (GHz).

**r** = Altura en metros que deben tener las antenas.

- **Ejemplo con frecuencia de 2,4 GHz**

Para una distancia de 1.1 km. (Nuestro caso)

$$r = 17,32 * \text{raíz}((1.1\text{Km} / (4 * 2,4 \text{ GHz}))) \rightarrow r = 5.8 \text{ m.}$$

Esto quiere decir que para el caso en particular, el radio *ideal* de la zona de Fresnel es de **5.8 m.**

Sabiendo que las condiciones “ideales” no se cumplen, y para un radio enlace óptimo, se espera garantizar libertad de obstáculos por lo menos el 80% **“Primera zona de Fresnel”**; esto es:

- **Calculando la Primera zona de Fresnel:**

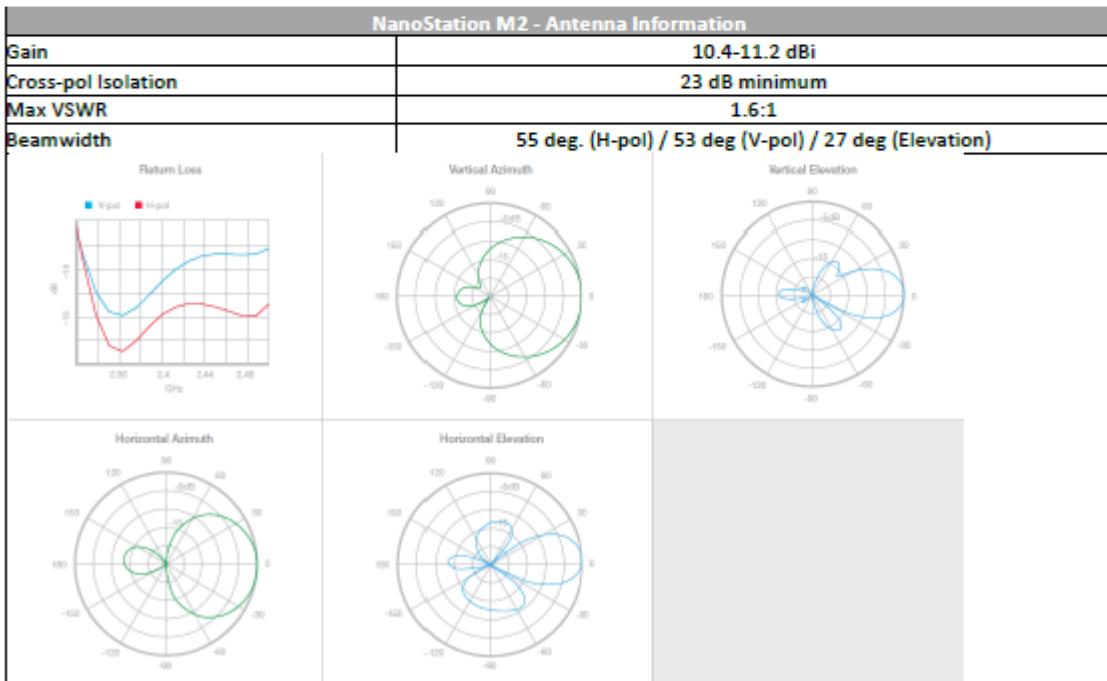
$$r = 5.86 \text{ m} * 80\% \rightarrow r = 4.68 \text{ m, radio primera zona de Fresnel.}$$

Lo que quiere decir que con **4.68 m** de radio despejado entre ambas antenas, tenemos un radio enlace óptimo y estable.

**Apéndice B.**

Especificaciones técnicas del radio Nano Station M2.

NanoStation M2 - Operating Frequency 2412-2462 MHz							
OUTPUT POWER: 28 dBm							
2.4 GHz TX POWER SPECIFICATIONS				2.4 GHz RX POWER SPECIFICATIONS			
	DataRate	Avg. TX	Tolerance		DataRate	Avg. TX	Tolerance
<b>11b / g</b>	1-24 Mbps	28 dBm	+/- 2 dB	<b>11b / g</b>	1-24 Mbps	-97 dBm min	+/- 2 dB
	36 Mbps	26 dBm	+/- 2 dB		36 Mbps	-80 dBm	+/- 2 dB
	48 Mbps	25 dBm	+/- 2 dB		48 Mbps	-77 dBm	+/- 2 dB
	54 Mbps	24 dBm	+/- 2 dB		54 Mbps	-75 dBm	+/- 2 dB
<b>11n</b>	MCS0	28 dBm	+/- 2 dB	<b>11n</b>	MCS0	-96 dBm	+/- 2 dB
	MCS1	28 dBm	+/- 2 dB		MCS1	-95 dBm	+/- 2 dB
	MCS2	28 dBm	+/- 2 dB		MCS2	-92 dBm	+/- 2 dB
	MCS3	28 dBm	+/- 2 dB		MCS3	-90 dBm	+/- 2 dB
	MCS4	27 dBm	+/- 2 dB		MCS4	-86 dBm	+/- 2 dB
	MCS5	25 dBm	+/- 2 dB		MCS5	-83 dBm	+/- 2 dB
	MCS6	23 dBm	+/- 2 dB		MCS6	-77 dBm	+/- 2 dB
	MCS7	22 dBm	+/- 2 dB		MCS7	-74 dBm	+/- 2 dB
	MCS8	28 dBm	+/- 2 dB		MCS8	-95 dBm	+/- 2 dB
	MCS9	28 dBm	+/- 2 dB		MCS9	-93 dBm	+/- 2 dB
	MCS10	28 dBm	+/- 2 dB		MCS10	-90 dBm	+/- 2 dB
	MCS11	28 dBm	+/- 2 dB		MCS11	-87 dBm	+/- 2 dB
	MCS12	27 dBm	+/- 2 dB		MCS12	-84 dBm	+/- 2 dB
	MCS13	25 dBm	+/- 2 dB		MCS13	-79 dBm	+/- 2 dB
	MCS14	23 dBm	+/- 2 dB		MCS14	-78 dBm	+/- 2 dB
MCS15	22 dBm	+/- 2 dB	MCS15	-75 dBm	+/- 2 dB		



(From: Ubiquiti Networks, Inc.)

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

FIRMA ESTUDIANTES	 <hr/>  <hr/>
FIRMA ASESOR	 <hr/>
Entrega del informe final para enviar al jurado evaluador.	
FECHA ENTREGA: <u>27/02/2017</u>	

FIRMA COMITÉ TRABAJO DE GRADO DE LA FACULTAD _____
RECHAZADO ___      ACEPTADO ___      ACEPTADO CON MODIFICACIONES ___
ACTA NO. _____ FECHA ENTREGA: _____

FIRMA CONSEJO DE FACULTAD _____
ACTA NO. _____ FECHA ENTREGA: _____