UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO

ESCUELA SUPERIOR DE TLAHUELILPAN

SISTEMA DE TELECOMUNICACIÓN EN LA FRECUENCIA DE LOS 2.4 GHZ.

T E S I S

QUE PARA OBTENER EL TÍTULO DE

LICENCIADO EN SISTEMAS COMPUTACIONALES

P R E S E N T A :

DARIEN BERNAVE ORTIZ

JULIÁN DE JESÚS VELÁZQUEZ ARTEAGA

DIRECTORES DE LA TESIS:

LIC. TOMÁS LEÓN QUINTANAR
LIC. GUILLERMO MERA CALLEJAS
M. T. E. VÍCTOR MANUEL SAMPERIO PACHECO

TLAHUELILPAN DE OCAMPO, HGO. DICIEMBRE 2013

Dedicatoria

Julián de Jesús Velázquez Arteaga

A mis profesores que influyeron con sus lecciones y experiencias en formarme como una persona de bien, a mis amigos siempre brindando su apoyo incondicional y en especial a mi mama Josefina Velázquez Arteaga que me preparo para los retos que pone la vida. A todos y cada uno de ellos les dedico cada una de estas páginas de mi tesis.

Darien Bernave Ortiz

A mis padres; ya que gracias a sus enseñanzas de día con día lograron formarme como una persona integral y totalmente independiente, además de estar conmigo en cada uno de mis buenos momentos, en mis malos momentos y si también en los peores momentos de mi carrera. Esta tesis es para ustedes mis padres María Luisa Ortiz Martínez y Jerónimo Bernave Cruz, gracias por todo su apoyo.

Agradecimientos

A nuestro asesor de tesis al Lic. Tomás León Quintanar ya que el confió desde un inicio en nosotros, además de permitirnos conocerlo como amigo de enseñarnos el valor de la lealtad, de la responsabilidad y de siempre estar al pendiente de la tesis con sus puntos de vista, mejoras y consejos.

Al nuestro coasesor el Lic. Guillermo Mera Callejas por sus enseñanzas, dedicación de tiempo en todo momento para la elaboración de nuestra tesis.

A nuestro coasesor el M. T. E. Víctor Manuel Samperio Pacheco por su dedicación de tiempo y sus horas extras que se dedicaba a leer nuestra tesis, para ayudarnos a mejorarla.

Gracias…

Resumen

Hoy en día, gran parte de las empresas tienen problemas como: la fuga de información, el mal uso de la tecnología, la brecha de comunicación, etc., los cuales se traducen en pérdidas. La presente tesis contiene la manera de cómo detectar los problemas dentro de la empresa, cual es impacto negativo para la organización en la ineficiencia del negocio. De la misma manera se habla de una solución que resuelva cada una de las necesidades a consecuencia de dichos problemas.

Todas las empresas para invertir en un nuevo proyecto tienen que realizar un análisis de requisitos, ninguna empresa puede arriesgarse a invertir en un proyecto si este no le es rentable, por tal razón es muy importante realizar un análisis de requisitos el cual depende en gran parte de los recursos humanos, materiales y económicos a participar sobre todo la infraestructura tecnológica con la que cuenta la empresa o si está dispuesta a invertir en tecnología de vanguardia.

En el mundo de los negocios, la transferencia rápida y eficiente de información es sumamente importante, especialmente cuando los datos son transferidos a los clientes. Si el servicio es lento, muchos clientes van a buscar otra opción en otro lugar, ya que creerán que la velocidad de transferencia es un reflejo de la empresa en general. Para compartir información en tiempo real con clientes y compañeros de trabajo la solución perfecta es un sistema de telecomunicación de punto a punto en la frecuencia de los 2.4 GHz.

Abstract

Today, many of the companies have problems such as data leakage, misuse of technology, communication gap, etc., which result in losses. This thesis contains the way how to detect problems within the company, which is negative impact to the organization in business inefficiency. In the same way we speak of a solution that meets each of the requirements as a result of such problems.

All companies to invest in a new project have to perform an analysis of requirements, no company can risk investing in a project if it does not it is profitable, therefore it is very important to conduct a requirements analysis which depends largely human resources, material and financial to participate especially technological infrastructure available to the company or if you are willing to invest in technology.

In the business world, quick and efficient transfer of information is extremely important, especially when the data are transferred to customers. If the service is slow, many customers will look for another option elsewhere because they believe that the transfer rate is a reflection of the overall business. For real- time information, sharing with customers and coworker's perfect solution is a telecommunication system point to point in the frequency of 2.4 GHz

Índice de Contenidos

Lista de cuadros

Lista de figuras

1. Introducción

Las redes inalámbricas se están mostrando en el mundo empresarial como una herramienta muy potente de conectividad; su evolución es constante y también puede ser una útil herramienta en el mundo educativo. [1]

La continua evolución de la tecnología informática y el creciente interés de la administración por alcanzar un desempeño más efectivo, han incrementado el uso de tecnologías de vanguardia como mecanismos para enfrentar la competitividad de manera más eficiente. El manejo de la información, es algo sumamente importante para las empresas hoy en día, las telecomunicaciones juegan un papel muy importante el cual es compartir la información en tiempo real sin importar la distancia a través de dispositivos de alta tecnología. Tales razones explican la gran demanda y variedad de software y herramientas de telecomunicaciones que están dando respuesta a necesidades particulares, en cuanto a la agilización y transmisión de datos que, debidamente interpretados puedan ser útiles para la toma de decisiones certeras.

El mercado tecnológico está siendo transformado por la movilidad, y TP-LINK cuenta con las herramientas necesarias para abastecer tal demanda. [1], [2]

1.1. Antecedentes

En las décadas pasadas las empresas ignoraban la necesidad de cualquier medio de comunicación flexible y seguro a un bajo costo. Hay que tomar en cuenta las muchas ocasiones donde la comunicación a través de una red fracasaron por las fallas tecnológicas pero las actitudes favorables y objetivos alcanzados entre las causa más comunes del fracaso impulso planes estratégicos.

Antes de las redes inalámbricas la creación de una red de computadoras en un negocio, el hogar o la escuela requería tener muchísimos cables con el fin de ofrecer este servicio a todos los usuarios, donde el uso típico profesional y donde el acceso era en puntos específicos, posteriormente este concepto cambio y ahora en las grandes ciudades se ha vuelto una combinación entre los diferentes negocios como: cafés, bibliotecas y puntos de acceso privados que permiten que el cliente pueda utilizar los servicios de internet.

Los puntos de acceso se utilizan comúnmente en redes inalámbricas donde suelen conectarse dispositivos móviles.

1.2. Problema

Actualmente la empresa “Infraestructura y construcción del pacifico S.A. de C.V.” se encuentra ubicada en el estado de Puebla, dedicada a la construcción de carreteras y puentes, misma que tiene un problema critico de comunicación con su más reciente sucursal ubicada en Xicotepec de Juárez, Puebla, por la ubicación geográfica de la sucursal no cuenta con ningún servicio de ISP (proveedor de servicios de internet) para alcanzar una comunicación con las oficinas centrales, lo que a su vez ha provocado buscar alternativas muy costosas y de baja calidad como dispositivos satelitales (BAM), telegramas, teléfonos móviles que solo funcionen fuera de la sucursal. Por lo tanto la empresa no tiene un control riguroso de la documentación para hacer un seguimiento permanente durante la ejecución de una obra, como falta la de un control de inventario, el estatus de la maquinaria, además de que se crea desconfianza con el cliente, la información no llega en tiempo y forma, la supervisión es mínima y todo esto se ve reflejado en pérdidas para la empresa.

La distancia que existe entre la sucursal y las oficinas centrales es de aproximadamente 70 km en línea recta, la falta de este servicio impacta de forma negativa a la empresa ya que el personal tiende a salir para enviar o recibir información o simplemente hacer una llamada, lo que se muestran en pérdidas para la empresa.

Este problema de comunicación genera conflictos y situaciones que alteran gravemente la eficiencia y la productividad en el clima laboral haciendo complicada la posibilidad de mantener la continuidad de la sucursal.

1.3. Justificación

El presente trabajo de investigación tiene como propósito principal eliminar la brecha de comunicación que existe entre la empresa Infraestructura y construcción del pacifico S.A. de C.V. ubicada en Xicotepec de Juárez, Puebla a sus oficinas centrales que se encuentran a una distancia de 70 km aproximadamente en línea recta. Dicha empresa necesita una implementación tecnológica de telecomunicación que comunique, agilice y comparta la información en tiempo real, esta implementación, consiste en configurar una transmisión inalámbrica que trabajará en la frecuencia de los 2.4 GHz., misma que permitirá obtener una comunicación con las oficinas centrales para trasmitir voz, datos y video. Dicho trabajo siguió un tipo de investigación interactiva, con un nivel integrativo, la cual permite crear una solución, apoyada con el uso de los métodos y herramientas teóricamente sustentadas para modificar una situación; con el objetivo de lograr adaptar las mejores estrategias y tecnologías de vanguardia para la implementación tecnológica.

1.4. Objetivos

1.4.1. Objetivo general

Diseñar e implementar un sistema de telecomunicación, el cual consiste en configurar una red inalámbrica bajo el estándar 802.11 en la frecuencia de los 2.4 GHz, misma que vinculará la reciente sucursal con la empresa Infraestructura y construcción del pacifico S.A. de C.V. brindando servicios de comunicación en tiempo real para trasmitir voz, datos y video.

1.4.2. Objetivos específicos

1. Detectar la problemática actual de la empresa
2. Analizar el escenario
3. Diseñar la implementación tecnológica
4. Configurar los dispositivos
5. Implementar sistema de telecomunicación

1.5. Organización de la obra

Capítulo I.- Es una introducción acerca la de tesis donde se abarcarán temas como los antecedentes, el problema que se va a resolver, la justificación a dicho problema y se desglosaran cada uno de los objetivos específicos y claro el objetivo general de la elaboración de esta tesis.

Capítulo II.- Se realizará un análisis del escenario para conocer a detalle la empresa "Infraestructura y construcción del pacifico S.A. de C.V." y su reciente sucursal; en el cual se detectará y se determinará cuál es la problemática real, como es que impacta de forma negativa en la eficiencia de los empleados, asimismo como le repercute a los clientes potenciales de dicha empresa.

Capítulo III.- El análisis de requisitos es la parte más importante para realizar una implementación tecnológica, dependiendo en gran parte de los recursos humanos, materiales y económicos a participar sobre todo la infraestructura tecnológica, con la que cuenta la empresa o si está dispuesta a invertir en tecnología de vanguardia.

Capítulo IV.- Abarca el diseño del sistema de telecomunicación en la frecuencia de los 2.4 GHz. Considerando que es una solución que implementará conexiones en tiempo real a la red, se construirá bajo un diseño de calidad para que cualquier usuario dentro de la sucursal tenga conexión a la empresa y transfiera voz, datos y video sin interrupciones.

Capítulo V.- La configuración de los dispositivos es parte fundamental para lograr una conexión eficiente de punto a punto. Los dispositivos serán configurados de acuerdo a su ubicación, ya que eso determinará si se configuran en modo repetidor o en modo bringe claro cada uno con su respectiva configuración de seguridad de encriptación.

Capítulo VI.- La seguridad en la red es vital para el funcionamiento adecuado de esta misma, para no permitir el acceso a intrusos dentro de la red y exista: interrupción de los procesos empresariales, perdida de datos o riesgo de los mismo, usurpación de identidad, pérdida de ingresos, daño a la confianza de los clientes. Para evitar estas y más amenazas a la empresa se configurarán cada uno de los dispositivos con una clave de encriptación la cual combina

números, letras minúsculas, letras mayúsculas y caracteres lo que permitirá crear una clave de seguridad muy robusta.

Capítulo VII.- Certificación de la empresa TP-link La configuración de los dispositivos es parte fundamental para lograr una conexión eficiente de punto a punto. Los dispositivos serán configurados de acuerdo a su ubicación, ya que eso determinará si se configuran en modo repetidor o en modo ***bringe*** claro cada uno con su respectiva configuración de seguridad.

Capítulo VIII.- Las pruebas realizadas muestran que el sistema de telecomunicación en la frecuencia de los 2.4 GHz está en óptimas condiciones, al igual que responde a las distintas exigencias de la red y de la misma empresa, con las funciones avanzadas en materia de gestión de ancho de banda, control de tráfico, seguridad y acceso etc., todo para brindar una conectividad sólida, eficiente, rentable, fiable para toda la empresa y su reciente sucursal y a toda prueba.

El trabajo de la implementación tecnológica funciona a la perfección, se pueden conectar varios dispositivos de forma simultanea sin importar la marca ni la compañía, ya que la frecuencia es compatible con cada uno de ellos, los directivos están conformes con los resultados de este sistema de telecomunicaciones se logró el objetivo de eliminar la brecha de comunicación. Ahora pueden enviar, recibir y compartir información en tiempo real sin importar el tipo ya sea voz, datos o videos.

2. Análisis del escenario

Hoy en día, gran parte de las empresas tienen problemas como: la fuga de información, el mal uso de la tecnología, la brecha de comunicación, etc., los cuales se traducen en pérdidas. La presente tesis contiene la manera de cómo detectar los problemas dentro de la empresa, cual es impacto negativo para la organización en la ineficiencia del negocio. De la misma manera se habla de una solución que resuelva cada una de las necesidades a consecuencia de dichos problemas.

2.1. Introducción

En este mundo globalizado todas las empresas requieren tecnologías de telecomunicación, mismas que permitan el ágil y eficiente uso de la información, vínculos estrechos con clientes, proveedores y socios comerciales además de una comunicación efectiva y confiable entre los departamentos y sucursales de la misma empresa.

Las redes de telecomunicación tratan de crear medios dedicados que ahorren tiempo evitando el desplazamiento físico, proporcionando así una comunicación eficiente. Cualquier sistema de telecomunicación estable necesita de una infraestructura y unos gastos que sólo pueden ser sufragados por una entidad poderosa. [1]

Por ello los primeros sistemas de telecomunicación eran siempre por y para el servicio del estado. En el pasado los primeros sistemas de telecomunicación aparecen pronto en aquellos

pueblos que por su expansión guerrera se vieron obligados a contar con algún medio de envío rápido de noticias. [1]

El presente trabajo tiene como fin comunicar a una empresa con su reciente sucursal, se realizará la detección del problema, se analizará la forma negativa en que impacta a la empresa y se le brindara una solución tecnológica que se adapte a sus necesidades del problema. [2]

2.2. Importancia de las telecomunicaciones

La información de cualquier red es un recurso corporativo, es decir, todos hacemos uso acorde al nivel de acceso permitido con un fin productivo dentro de la empresa.

Por otro lado, las comunicaciones se han convertido en una herramienta fundamental para las industria y empresas, cada día las transacciones de operaciones son mayores, además de que son agiles y confiables. La comodidad de realizar múltiples aplicaciones dentro de la empresa o sucursales buscan objetivos muy particulares en la tecnología, dado que estas evolucionen vertiginosamente y que dependamos más de ellas. [1]

Una red de telecomunicaciones en la empresa debe resolver las necesidades de comunicación para sus diversas operaciones como: manejo de inventario, almacenamiento, movimientos bancarios y atención a proveedores, tener una comunicación ágil en todos lados y de menor costo es determinante para el sano desarrollo de la empresa. [2]

La información por naturaleza tiene un valor, el cual, dependiendo del contexto en el que se tenga, puede llegar a ser muy grande y las telecomunicaciones no son otra cosa más que sistemas para establecer un puente de comunicación entre dos entidades que se encentran alejadas [3], bajo canales de redes inalámbricas.

Con la llegada de la telefonía móvil, banda ancha y tecnología de satélite las empresas podían tener conexiones de manera muy lenta y costosa ya que existían muchas caídas, el problema de la estática, además que estas en algunas zonas rurales todavía no tienen fácil acceso, cada año estas cifras aumenta lo cual afecta a organizaciones que utilizan este servicio [5]. En la

actualidad existen más opciones a medida que las telecomunicaciones se expanden con métodos de conexión a larga distancia que permiten entre muchas otras aplicaciones llevar los servicios de un lugar a otro como el internet a través de redes inalámbricas para incrementar las comunicaciones[4].

Una de las principales ventajas de las redes inalámbricas es su simplicidad para extender la cobertura de la red local en muy poco tiempo y a bajo costo [4],a través de métodos instantáneos que permiten ahorros hasta más del 50% al compartir recursos entre varias instalaciones relativamente con baja infraestructura de comunicaciones. Además de:

Ventajas comerciales como: eliminación de rentas mensuales, crecimiento de su red, eliminación de cables, movilidad en la conexión de los usuarios, reducción de los costos de operación, reducción de fallas por mantenimiento, la inversión es amortizable en pocos meses.

Ventajas técnicas como: fácil instalación de más equipos, alta velocidad de trasmisión, cobertura más extensa (interna y externa), cobertura uniforme en zonas muertas, nuevas tecnologías para corto, mediano y largo alcance.

Grandes usos como: enlaces que requieran anchos debanda confiable, robustos y amigables, trasmisión de datos entre sucursales, transmisión de datos y video, transmisión de estados críticos en tiempo real, administración del ancho de banda para mayor control.

Aplicaciones como: coordinación con protección civil, proveedores y oficinas centrales [5].

En la transferencia de los datos influye mucho la frecuencia que maneja en ancho de banda, ya que de esta depende la velocidad de la transferencia, entre las más comunes encontramos 2.4 GHz y 5.8 GHz.

No existe una mejor banda para todos los escenarios. La elección entre usar 2.4 o 5 GHz depende de varios factores (el tipo de enlace inalámbrico, interferencia, distancia, línea de visión).

La ventaja de 2.4 GHz: mejor tolerancia a los obstáculos (arboles, puertas, paredes, etc.), son más compartibles con dispositivos móviles (teléfonos Wifi, portátiles y dispositivos IP), no

requieren licencia especial para su uso y la desventaja sufre de interferencia por su alta compatibilidad.

Las ventajas de 5.8 GHz: hay mucha menos interferencia, desventaja: intolerante a obstáculos [6].

Antes de realizar la instalación de un sistema de gran escala puede ser muy útil realizar un análisis del radio del sitio con el fin de determinar cuál es la mejor opción. La coordinación corre a cuenta de la propia tecnología empleada y el modo de acceso múltiple al servicio.

Actualmente ya existen empresas desarrollando comunicaciones unificadas, quienes coinciden en características básicas como la interacción de todos sus departamentos y/o sucursales, la eficiencia de una red basada en una estructura tecnologías de vanguardia muy importante en la trasmisión de la información en tiempo real sin importar la distancia dando respuesta sus necesidades particulares en la ampliación de una red informática inalámbrica. [2], [6]

2.3. Estudiar las causas del problema

La empresa “Infraestructura y construcción del pacifico S.A. de C.V.” se encuentra ubicada en el estado de Puebla, dedicada a la construcción de carreteras y puentes, con su más reciente sucursal ubicada en Xicotepec de Juárez, Puebla, por la ubicación geográfica de la sucursal no cuenta con ningún servicio de ISP (Proveedor de servicios de internet) por tal razón no se cuenta con una línea de internet, el motivo de que la sucursal este en ese lugar, es para poder recibir infraestructura de grandes tamaños como: bigas, estructuras de concreto, ballenas, etc., además de que es un lugar demasiado amplio para trabajar, de la misma manera se utiliza de almacén para la maquinaria pesada.

2.4. Analizar las consecuencias del problema

Brecha de comunicación

- Gastos excesivos en telefonía móvil
- No contar con información en tiempo real
- Ineficiencia de los empleados
- Perder la continuidad del negocio

2.5. ¿Qué ha realizado la empresa?

La empresa ha contratado servicios de internet satelital (BAM), lo cual le ha resultado muy caro, además de que el servicio, depende en gran parte de la recepción de señal satelital para su ideal funcionamiento.

La telefonía móvil tiene un papel importante en la empresa para la comunicación en tiempo real, pero sin embargo carece de un buen servicio a causa de no contar con buena señal en la zona donde se encuentra ubicada la sucursal, de la misma manera resulta muy caro mantener este servicio.

2.6. Determinar una solución

Como se ha mencionado anteriormente la problemática actual de la empresa, es la brecha de comunicación entre la empresa y su reciente sucursal, la solución es el diseño e implementación de un sistema de telecomunicación en la frecuencia de los 2.4 GHz., la cual permitirá eliminar la brecha de comunicación.

3. Análisis de requisitos

En la actualidad las empresas para invertir en un nuevo proyecto tienen que realizar un análisis de requisitos, ninguna empresa puede arriesgarse a invertir en un proyecto si este no le es rentable, por tal razón es muy importante realizar un análisis de requisitos el cual depende en gran parte de los recursos humanos, materiales y económicos a participar sobre todo la infraestructura tecnológica con la que cuenta la empresa o si está dispuesta a invertir en tecnología de vanguardia.

3.1. Introducción

La etapa de Análisis de Requerimientos, es la primera etapa en una implementación tecnológica. Comienza después de que el Cliente ha detectado una ausencia, falla o falta de oportunidad de la información o simplemente, luego que la organización ha determinado un cambio en sus políticas, reglas o tecnologías a aplicar. [7]

En esta etapa, deberemos responder a una pregunta fundamental: ¿Qué es lo que quiere el cliente? y para ello, debe realizar un análisis de requisitos, recopilar los requerimientos del cliente, tanto en relación a la implementación tecnológica, como generales respecto del área informática, es decir la situación ideal, para así poder definir alternativas de solución, según las cuales podremos avanzar desde lo que hoy se posee, hacia el punto que se pretende llegar. [7], [8]

Como parte de nuestro trabajo, deberemos señalar cuál de las alternativas, es a nuestro juicio la más conveniente (y justificarlo) en la propuesta. Hecho lo anterior, el cliente evaluará nuestro trabajo. [7]

3.2. Distancia entre la empresa y su reciente sucursal

Tulancingo de bravo, hidalgo se encuentra ubicada en la parte centro- oriente de México perteneciente al estado de hidalgo, entre una de las regiones geográficas del estado, llamada valle de Tulancingo, formado por llanuras principalmente y por sierra en menor proporción, su topología presenta una superficie semiplano cortada por cañadas, barrancas, cerros y volcanes. El suelo es tipo semidesértico incluye pastos naturales, bosque o selva y riego temporal. El clima es templado- frio, registra una temperatura media anual de 14 grados centígrados, con precipitación de lluvia, prevaleciendo vientos del oeste con una velocidad media anual de 29 Km/h. Altitud 2180 msnm y coordenadas 20°5′9″N 98°21′48″O. [8]

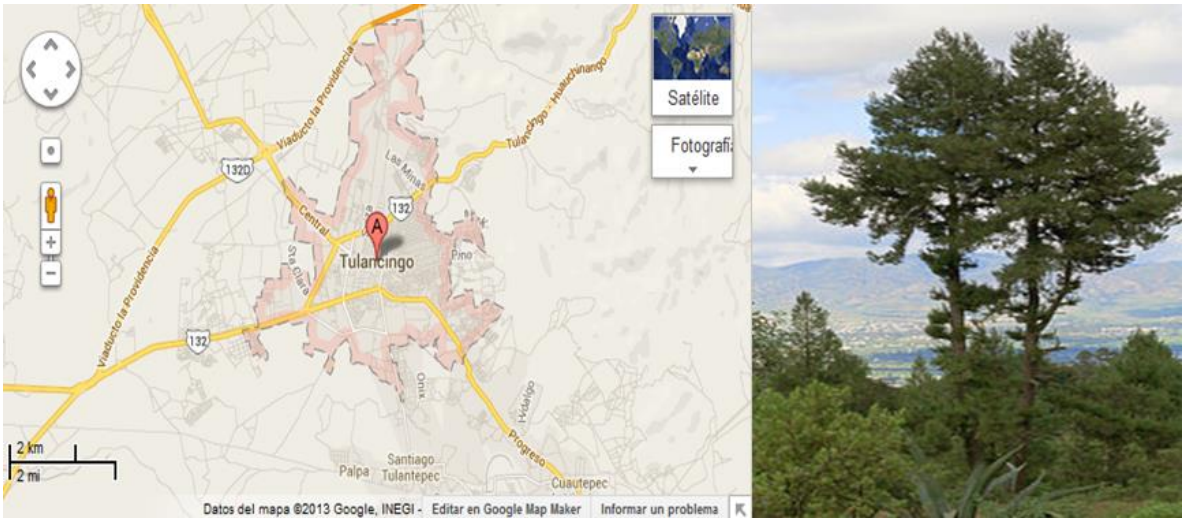


Figura 1. Tulancingo de bravo hidalgo (mapa y foto de la zona)

Xicotepec de Juárez, Puebla uno de los municipios que conforman el estado mexicano de Puebla, dentro de la sierra norte, la altitud de este municipio está comprendida entre los 300 y 1155 msnm, una zona de montañas valles y mesetas, en todo el municipio se aprecian dos formas características de relieve: la zona accidentada que abarca el 90% del municipio y las

zona semiplano solo el 10%. Su clima cálido semihúmedo con temperatura de 0 a 22 grados, tormentas eléctricas, y además en el mes de enero con recurrencia de heladas. Coordenadas: 20°18′0″N 97°58′0″O. [9]

Figura 2. Xicotepec de Juárez puebla (mapa y foto de la zona)

La distancia que existe entre ambos municipios es de 66.4 KM sobre carretera y la distancia en línea recta es de aproximadamente de 64 KM.

Figura 3. Distancia de los dos municipios (vista satelital)

Ambos municipios cuentan con diferentes formas de corteza terrestre, rodeados de valles y montañas, fuertes corrientes de aire, msnm uno menor de otro, además que la humedad que existe es mucha con riesgo de tormentas eléctricas, así como altas y bajas temperaturas.

3.3. Elección de un dispositivo

El CPE inalámbrico de alta potencia de 2.4 GHz. Para exteriores se dedica a la solución de redes inalámbricas de larga distancia. Integra las funciones de punto de acceso inalámbrico, cliente WIPS, antena de alta ganancia y carcasa resistente a la intemperie. Cuenta con una antena de 12dBi, alta sensibilidad significativamente RX, puede ampliar el rango de transmisión para ofrecer una conexión inalámbrica más estable. Compatible con IEEE 802.11, con una red inalámbrica de hasta 54 Mbps. Lo que es ideal para navegar por internet y el intercambio de archivos.

Está diseñado para difíciles ambientes exteriores, construido con una carcasa impermeable al aire libre y duradero de alta de la temperatura (-30 ° C a 70 ° C) podría trabajar en lugares con condiciones extremas de mal tiempo. Además que incorpora protección contra rayos de 4000v. y el diseño también ayuda a evitar las sobre tenciones de una tormenta garantizando un funcionamiento fiable.

Figura 4. Dispositivo TP-LINK

El dispositivo cuenta con potencia para velocidades más altas dándole a su red flexibilidad para ir más allá. Degradación de la señal al viajar largas distancias se atenúa con el significado de alta sensibilidad RX que usted puede conseguir una mayor velocidad en distancias más larga, permitiendo que el AP para detectar y recibir a los más débiles señales, dos aspectos de trabajo en conjunto garantizar la las señales pueden ir más allá y llevar una mayor velocidad a la misma distancia que las normales.

Múltiples aplicaciones.

El dispositivo es compatible con:

- AP cliente.
- Router cliente.
- Puente.
- Repetidor.
- AP

Diferentes modos de operación de puerta de enlace que permitir varias aplicaciones inalámbricas para ofrecer al usuario una experiencia más dinámica y completa.

PoE compatible para la implementación más flexible.

Dispositivo capaz de ser alimentado mediante un cable Ethernet para enviar simultáneamente datos y electricidad a cualquier lugar su punto de acceso pueden estar ubicados hasta 200 metros de distancia. Esta función multiplica sus opciones de lo que permite colocar al AP en una posición que sea más conveniente para obtener la mejor señal posible, como en la pared o en el techo de su oficina. [10]

Figura 5. Edificio TP-LINK

4. Diseño de la implementación tecnológica

Hoy en día, en el mundo de los negocios, la transferencia rápida y eficiente de información es sumamente importante, especialmente cuando los datos son transferidos a los clientes. Si el servicio es lento, muchos clientes van a buscar otra opción en otro lugar, ya que creerán que la velocidad de transferencia es un reflejo de la empresa en general. Para compartir información en tiempo real con clientes y compañeros de trabajo la solución perfecta es un sistema de telecomunicación de punto a punto.

4.1. Introducción

Las redes punto a punto se aplican para un tipo de arquitectura de red específica, en la que cada canal de datos se usa para comunicar únicamente dos nodos. Los dispositivos AP Y CPE soportan el modo de punto de acceso y de modo de estación o transmisión, por lo tanto una conexión punto a punto puede ser creada a partir de AP y CPE o del 2 CPE o del 2 de AP, de acuerdo al diseño de red. [11]

PPP son las siglas de Point to Point Protocol, Protocolo Punto a Punto. Esto significa, que la conexión se realiza, obviamente, siempre entre dos hosts (integrantes de la conexión) o puntos de conexión. Siempre un integrante de la conexión es cliente y el otro servidor. Este cliente va a ser el host que se quiere conectar a Internet (nosotros), y el servidor va a ser el ISP. [11], [12]

Este protocolo se utiliza bajo líneas telefónicas, por eso se la denomina conexión dialup (dial en inglés es llamar). PPP es una evolución de un protocolo anterior, SLIP (Serial Line IP, Protocolo de Internet por Línea Serie -así se llama a las líneas en las cuales se conectan los módems), y su diferencia principal es que PPP es un protocolo que permite el transporte de otros protocolos, valga la redundancia, además de TCP/IP (Protocolo de Control de Transmisión), como IPX (de Novell), etc. SLIP solamente estaba diseñado para TCP/IP. [12]

4.2. Acceso a internet (ISP)

Los sistemas de comunicación se presentan utilizando distintas combinaciones de tecnologías de redes de telecomunicaciones. Las tecnologías se apoyan en infraestructura de comunicación y pueden sustituir o complementar mutuamente en función de cada caso. Cada tecnología cuenta con características distintas dependiendo de su capacidad y las posibilidades de la red. [11]

4.2.1. ISP

Proveedor de servicios de internet (ISP) es una compañía que ofrece acceso a internet, normalmente por una cuota, tiene su lugar a través de una conexión de acceso telefónico, estos a su vez ofrecen servicios adicionales como cuentas de correo electrónico, exploradores web y espacio para crear sus propios sitios web. [12]

4.2.2. ¿Por qué utilizar un ISP?

Al menos que se cuente con una línea especializada no es posible conectarse directamente a internet utilizando solo la línea telefónica ya que no fue diseñada para esto. Ya que esta solo transfería voz en una frecuencia de modulación en el rango de la voz humana. Entonces, el ISP es un intermediario que proporciona el acceso a internet por medio del modem que permite que se establezca esta conexión dentro de esta frecuencia.

4.2.3. ¿Cómo establecer la conexión en ISP?

Se establece con un sencillo protocolo (PPP) que permite que dos ordenadores remotos puedan comunicarse sin tener una dirección IP. Sin embargo, una de estas direcciones IP es necesaria para poder acceder a Internet, principalmente porque el protocolo utilizado en Internet es el protocolo TCP/IP que permite que un gran número de usuarios ubicados por medio de estas direcciones se comuniquen. Una vez ya conectado el ISP proporciona una dirección IP que se conserva durante este periodo en el que se encuentra conectado por lo tanto no son fijas ya que en la siguiente conexión este proporcionara una distinta según ya la capacidad de tal proveedor. [12]

4.2.4. Elección de un ISP

La elección de un ISP depende de distintos criterios entre ellos son:

- Cobertura: algunos ISP ofrecen cobertura en grandes ciudades o nacionales.
- Ancho de banda: es la velocidad total que ofrece en proveedor.
- Precio: este factor depende del ISP y del tipo de paquete elegido.
- Acceso: se considera el tiempo de la conexión.
- Servicios técnicos: el equipo que se encarga de responder a los problemas técnicos.
- Servicios adicionales. [13]

4.3. Diseño

El diseño debe ofrecer soluciones, que proporcionan análisis de la red LAN inalámbrica para la solución rápida y eficaz de problemas, la elección de dispositivos no vulnerables. La visión inteligente del nivel de la red permite identificar el origen de los problemas que plantean riesgos o interrumpen el rendimiento como: [14]

- Interferencias: la propagación de ondas electromagnéticas.
- Inestabilidad del medio físico: propagación de ondas electromagnéticas a través del aire un fenómeno altamente complejo, presencia del ruido, modificaciones del medio físico.
- Velocidad de trasferencia o retardos: menor velocidad en la transmisión mayores retrasos en la información.
- Seguridad: los datos transmitidos por la interfaz son venerables.

[11]

Dentro del diseño Las soluciones garantizan que las aplicaciones WLAN, tales como voz datos y videos obre red inalámbrica, mantengan la integridad a lo largo de las fases de implementación y expansión resaltando y aumentado las ventajas como:

- Flexibilidad: son flexibles ya que permiten interconectar dispositivos en ubicaciones complicadas
- Escalabilidad: la cualidad que permite la posibilidad de adaptarse en cobertura y ancho de banda.
- Rapidez: el despliegue de una re suele ser por lo general bastante rápido e todo si existe ya un equipamiento o una infraestructura previa (torres de comunicación ubicados a grandes alturas) que pueda ser aprovechada para llevar a cabo la instalación.
- Costes reducidos: Dependerá del caso, pero en general resulta menos costoso el despliegue de una red inalámbrica que una cableada.

[14]

Para la ampliación de una red inalámbrica se debe tomar en cuenta el ISP ya que de este dependerá del entorno que se pretenda ampliar, es decir el uso sobretodo el coste de esta. Los ISP proporcionan flexibilidad y adaptación en las instalaciones en el sentido que

proporcionan un ancho de banda pero muy tenues cuando se incrementa la distancia, un buen diseño de la ampliación de esta permite hacer despliegues rápidos y una mayor facilidad en el ajuste dentro de la instalación física, teniendo un entorno ideal de aplicación en terrenos complicados, como las que se pueden dar en los entornos rurales. [11]

4.4. Enlace punto a punto

Los enlaces punto a punto generalmente se usa para conectarse a internet donde dicho acceso no está disponible de otra forma. Uno de los lados del enlace punto a punto estará conectado a internet, mientras que el otro utiliza el enlace para acceder al mismo. [12]

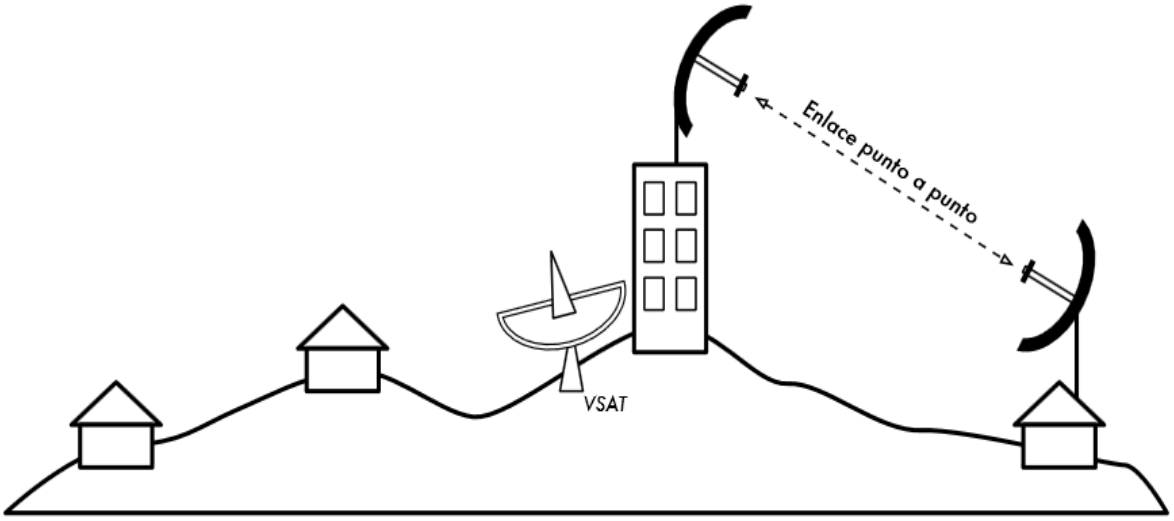
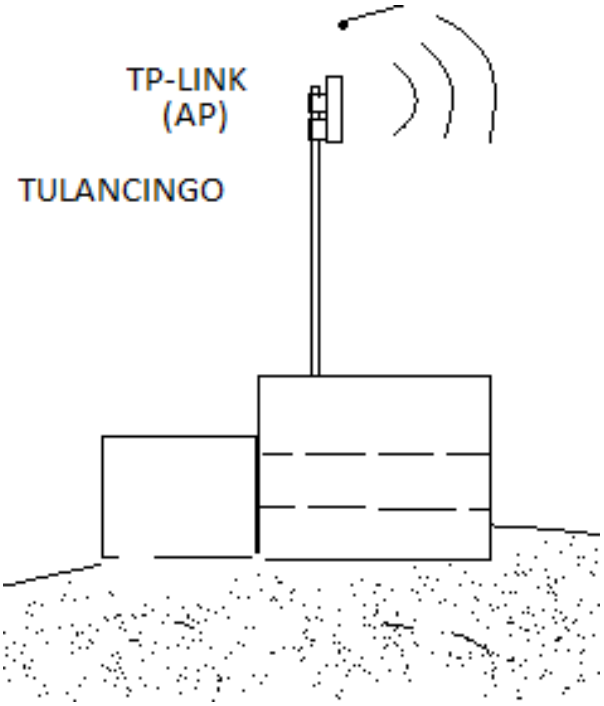


Figura 6. Enlace punto a punto

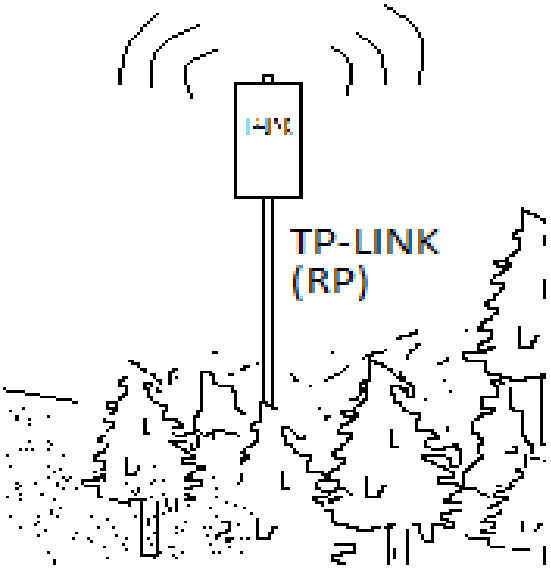
Los diseños de la red inalámbrica de alta eficiencia son difíciles ya que su capacidad debe ser el suficiente para las necesidades máximas que exige la empresa, independientemente del rango el conjunto de enlaces debe dar servicio en la fracción total del área. El aislamiento de la sucursal debe ser con antenas omnidireccionales que pueden incluir factores de reusó o con más espacio libre. La distancia del aislamiento trabaja muy bien con altos porcentajes de atenuación media. Dependiendo lo disperso del ambiente, la distancia del aislamiento (algunos casos de interferencia) y por lo tanto menor cobertura. Dentro del análisis que se realizó se eligieron cuidadosamente los dispositivos y la frecuencia que evitara este tipo de problemas. [12]

4.5. Ubicación de los dispositivos



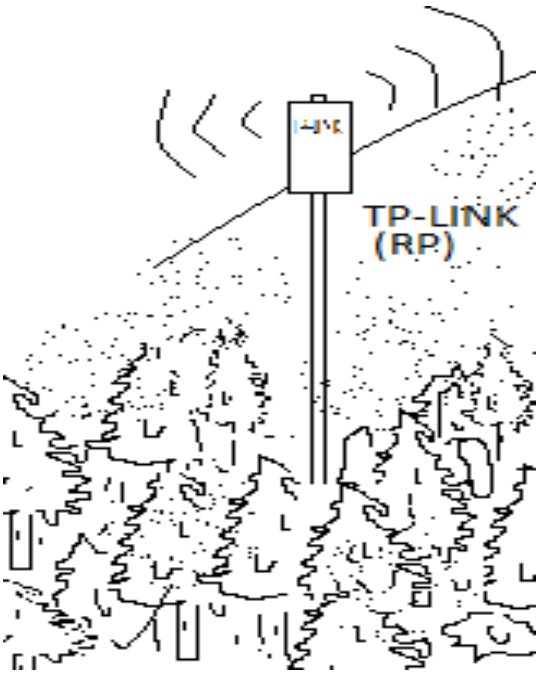
PRIMER AP UBICADO EN LA EMPRESA

Figura 7. TP-LINK Tulancingo de Juárez



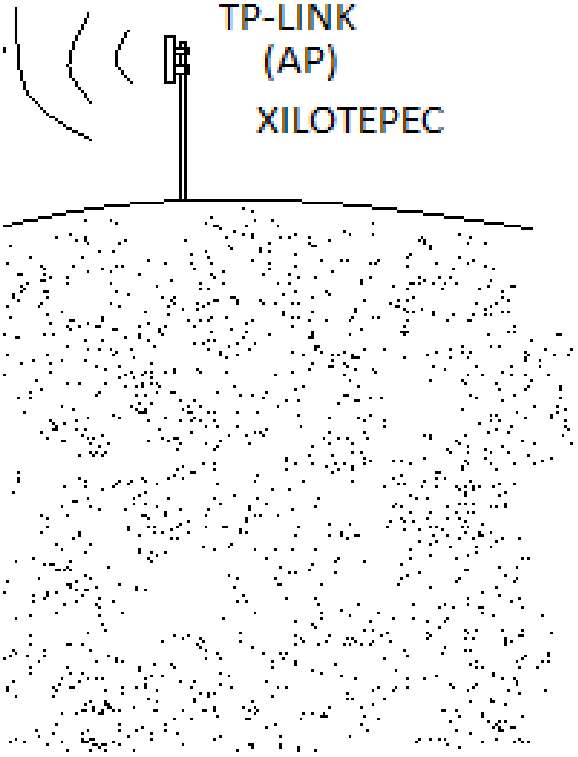
SEGUNDO AP UBICADO APROXIMADAMENTE A 22 KM DE LA EMPRESA

Figura 8. Primer repetidor



TERCER AP UBICADO APROXIMADAMENTE A 44 KM DE LA EMPRESA

Figura 9. Segundo repetidor



CUARTO AP UBICADO EN LA SUCURSAL

Figura 10. TP-LINK Xicotepec

Figura 11. Diseño general de la implementación

5. Configuración de los dispositivos

Hoy en día, en el mundo de los negocios, la transferencia rápida y eficiente de información es sumamente importante, especialmente cuando los datos son transferidos a los clientes. Si el servicio es lento, muchos clientes van a buscar otra opción en otro lugar, ya que creerán que la velocidad de transferencia es un reflejo de la empresa en general. Para compartir información en tiempo real con clientes y compañeros de trabajo la solución perfecta es un sistema de telecomunicación de punto a punto.

5.1. Introducción

Las redes punto a punto se aplican para un tipo de arquitectura de red específica, en la que cada canal de datos se usa para comunicar únicamente dos nodos. Los dispositivos AP Y CPE soportan el modo de punto de acceso y de modo de estación o transmisión, por lo tanto una conexión punto a punto puede ser creada a partir de AP y CPE o del 2 CPE o del 2 de AP, de acuerdo al diseño de red. [15]

PPP son las siglas de Point to Point Protocol, Protocolo Punto a Punto. Esto significa, que la conexión se realiza, obviamente, siempre entre dos hosts (integrantes de la conexión) o puntos de conexión. Siempre un integrante de la conexión es cliente y el otro servidor. Este cliente va a ser el host que se quiere conectar a Internet (nosotros), y el servidor va a ser el ISP. [15], [16]

Este protocolo se utiliza bajo líneas telefónicas, por eso se la denomina conexión dialup (dial en inglés es llamar). PPP es una evolución de un protocolo anterior, SLIP (Serial Line IP,

Protocolo de Internet por Línea Serie -así se llama a las líneas en las cuales se conectan los módems), y su diferencia principal es que PPP es un protocolo que permite el transporte de otros protocolos, valga la redundancia, además de TCP/IP (Transmisión Control Protocol, Protocolo de Control de Transmisión), como IPX (de Novell), etc. SLIP solamente estaba diseñado para TCP/IP. [16]

5.2. Conexión física de cada dispositivo

Figura 12. Inyector POE

Para poder lograr los de imagen anterior se tienen que seguir los siguientes pasos.

1. Primero será conocer cada conexión del dispositivo.

   - DC.- También conocida como corriente directa, esta conexión sirve para suministrar energía eléctrica al dispositivo.

   - POE.- Este puerto sirve para comunicar al dispositivo con la red.

   - LAN.- Por sus siglas en ingles significa Local Area Network (Red de Área Local) este puerto como su nombre lo dice nos permitirá crear una red local para conectar uno o más equipos simultáneamente. [17]

5.3. Datos de configuración

El AP de TP-link TL-WA5210G es muy poco conocido, que funciona como: Access Point, Cliente, Repetidor, con un inyector POE y fuente de 12v, tiene en la parte posterior lets indicadores del nivel de señal, además de un botón reset y un conector adicional de puesta a tierra que jamás se había visto en este tipo de dispositivos. Si se le conecta una antena de mayor ganancia tipo parabólica o de rejilla a través de su conector complementario de antena rompe las limitaciones de la distancia en condiciones normales. [18]

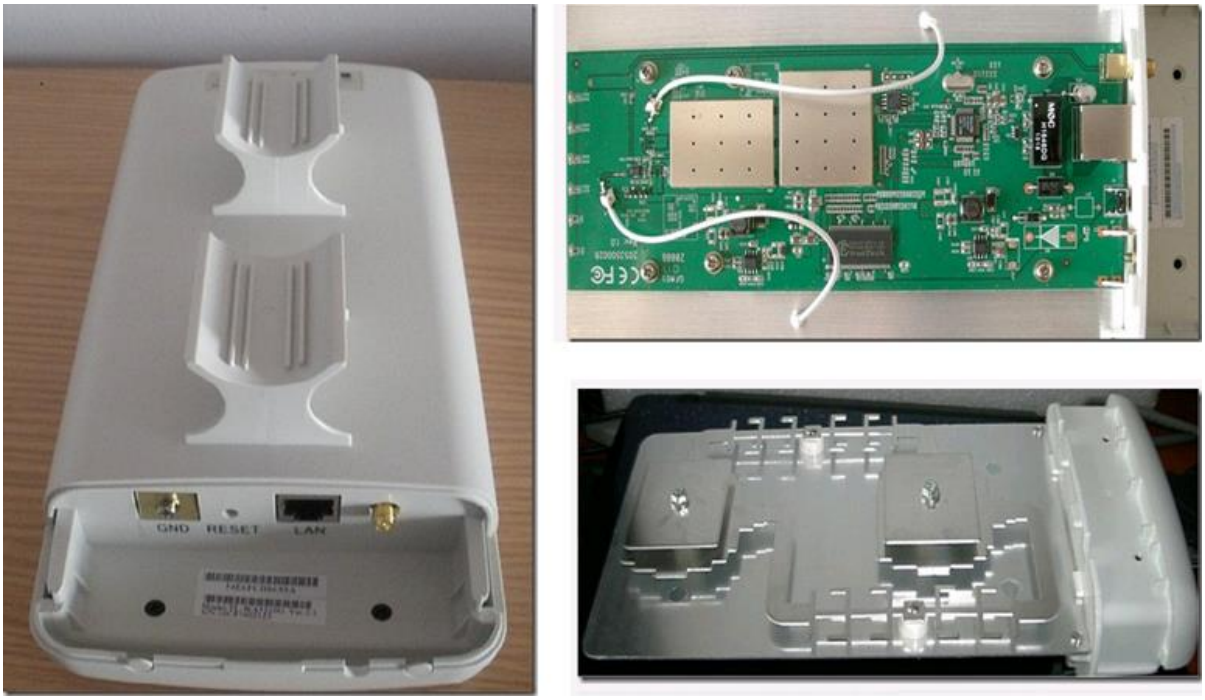


Figura 13. Vistas del dispositivo

Al conectar el dispositivo al equipo de cómputo a través de un cable Ethernet, este se alimentara de forma automática, ya que se aprovecha el voltaje de la toma LAN de la tarjeta de red. [19]

La dirección IP: un número único e irrepetible con el cual se identifica el dispositivo conectado a una red [20]. Es un valor entre 192.168.1.2 a 192.168.1.253 solo cambia la última cifra de 2 a 253 y no se debe repetir este número para otra conexión que este habilitada. [18]

Puerta de enlace predeterminada: dispositivo que conecta y dirige el tráfico de datos entre dos redes o más [22], es siempre 192.168.1.254 es la opción más importante de todas para acceder a la configuración del AP. [18]

Servidor DNS preferido: el sistema para asignar nombres a equipos y servicios de la red que se organizan en una jerarquía de dominios. [23]

Servidor DNS alternativo: el sistema para asignar nombres a equipos y servicios de la red que se organizan en una jerarquía de dominios cualquier otro valido. [23]

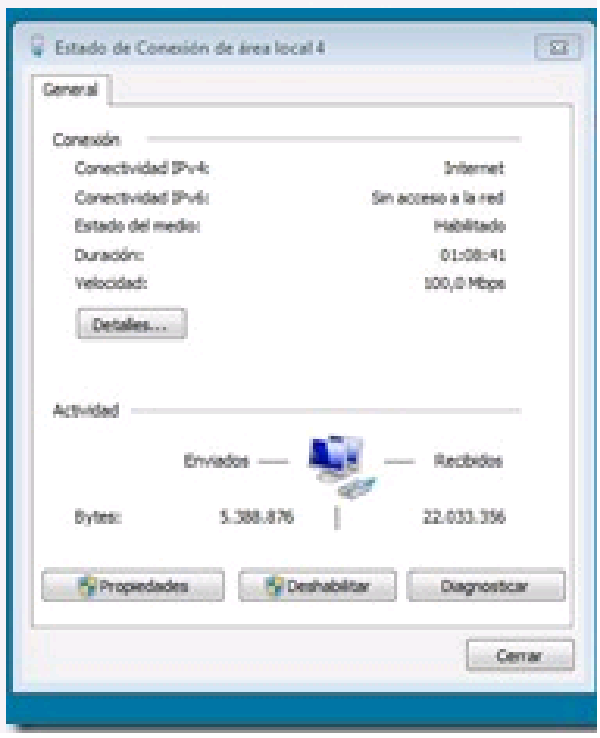


Figura 14. Estado de la conexion

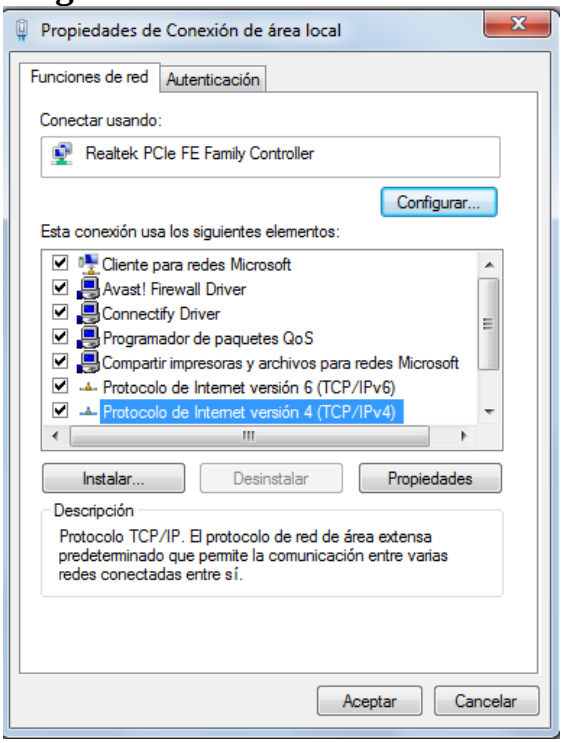


Figura 15. Protocolo ipV4

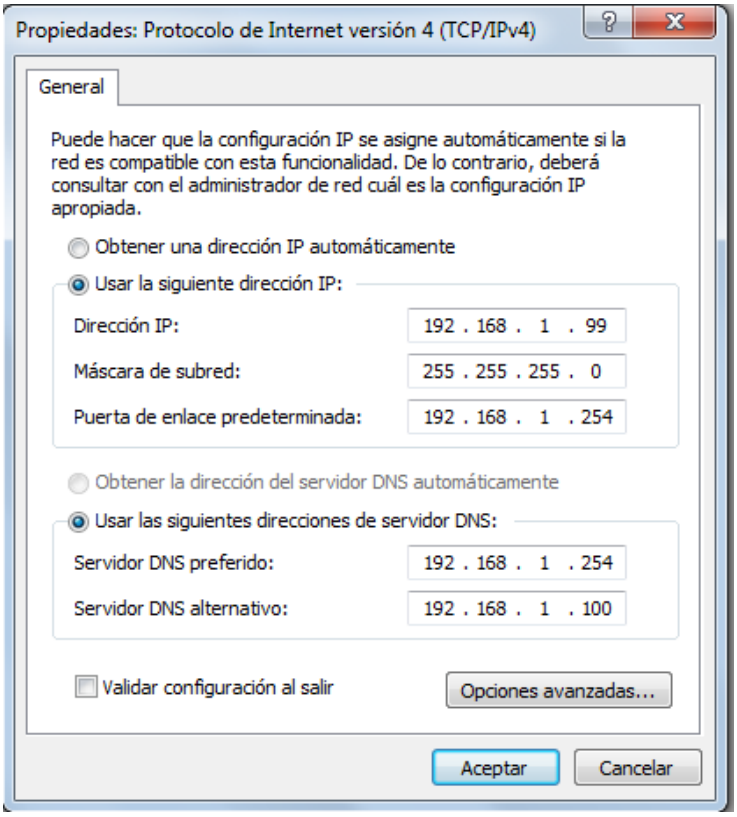


Figura 16. Ip fija

CPE inalámbrico de alta potencia de 2.4 GHz, TP-LINK TL-WA5210G.

Dispositivo que interconecta dispositivos de comunicación inalámbrica para transmitir datos, permite la conexión de dispositivos móviles delegando la tarea de ruteo, direccionamiento a servidores y swiches, este sigue el estándar de comunicación 802.11 de la IEEE lo que permite esta variedad de equipos inalámbricos, incluyen tareas como la configuración de la función de ruteo, de direccionamiento de puertos, seguridad y administración de usuarios con una completa zona de acceso donde los clientes pueden conectarse sin importar las redes a las que se han adjuntado por el momento.

Hay que destacar que posee una sensibilidad de recepción increíble, con la seguridad inalámbrica el TL-WA5210G proporciona 64 bit LAN inalámbrica de seguridad WEP de cifrado y autenticación WPA/WPA2 y WPA-PSK/WPA2-PSK, así como de seguridad TKIP / AES.

5.4. Configuración de AP modo Bridge emisor

A. Para realizar la configuración en modo BRIDGE o mejor conocida como point to point se tiene que configurar previamente en modo local. Conectado el dispositivo solo a una máquina.

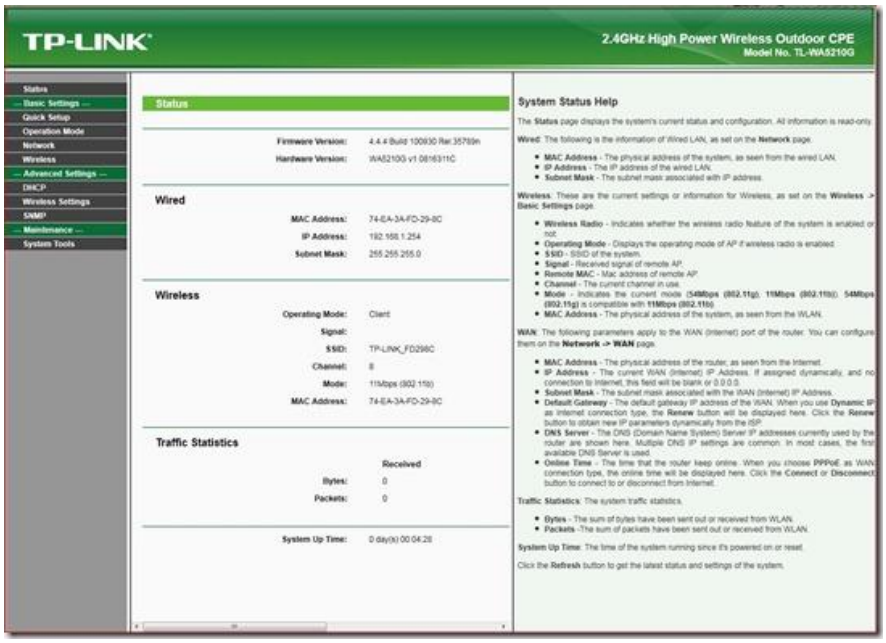


Figura 17. Pantalla principal TP-LINK

B. Una vez conectado entrar a la configuración del dispositivo de la siguiente manera: abrir cualquier navegador, insertar la siguiente dirección ip 192.168.1.254 y presionar enter.

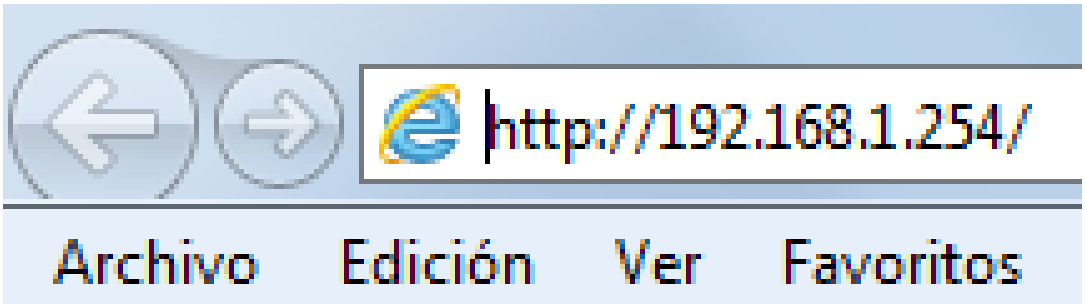


Figura 18. Dirección ip en el navegador

C. Ahora aparecerá esta nueva ventada donde pide usuario y password.

Figura 19. Seguridad del dispositivo

D. Por default es admin en los dos campos.

E. Este es el software de configuración del dispositivo.

Figura 20. Ingreso de datos

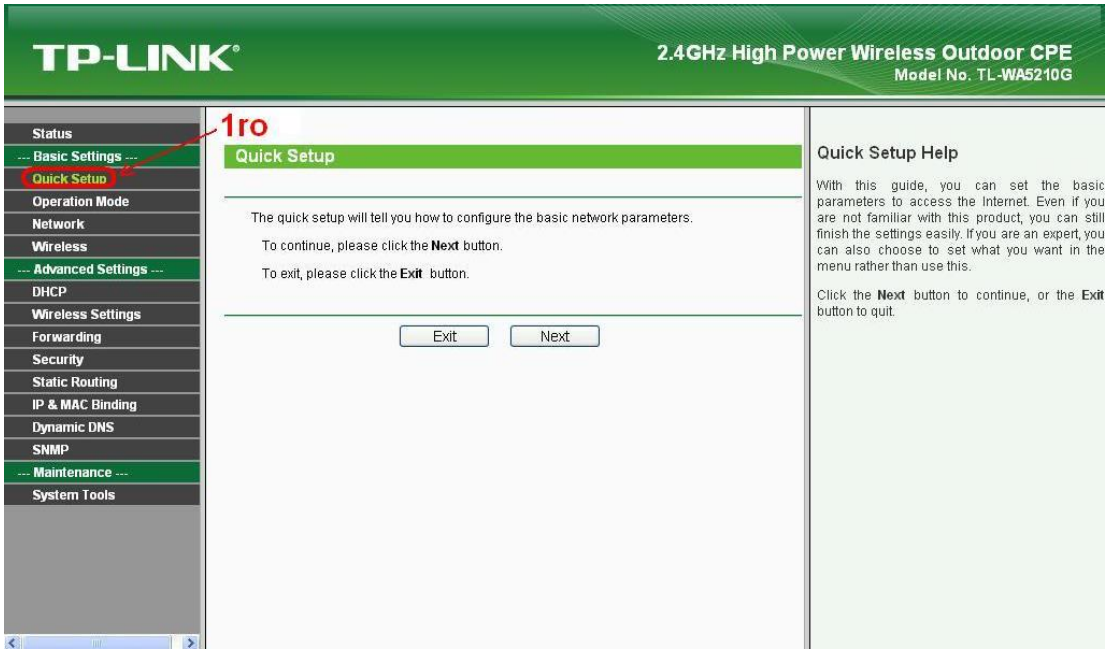


Figura 21. 1er paso

F. Lo primero que se tiene que realizar es cambiar la dirección ip del dispositivo, eso se hace de la siguiente manera entrando a la opción de Wireless Settings.

Figura 22. LAN

G. Ahora ingresamos la nueva dirección ip de nuestro dispositivo y damos clic en Save. (Cada dirección ip que se asigne a los dispositivos no se puede repetir)

Figura 23. Nueva dirección

H. Esperar hasta que el dispositivo se reinicie, tendrá que salir esta pantalla.

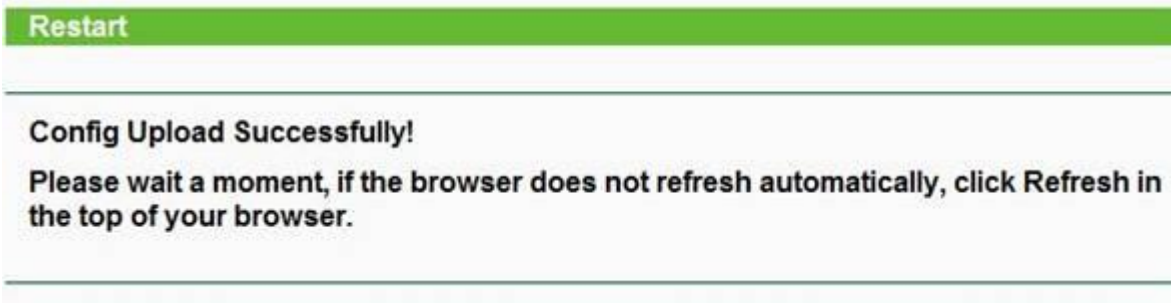


Figura 24. Reset

I. Se tendrá que ingresas con la nueva dirección ip al dispositivo. (Ahora ya se puede configurar el dispositivo conectado a internet)

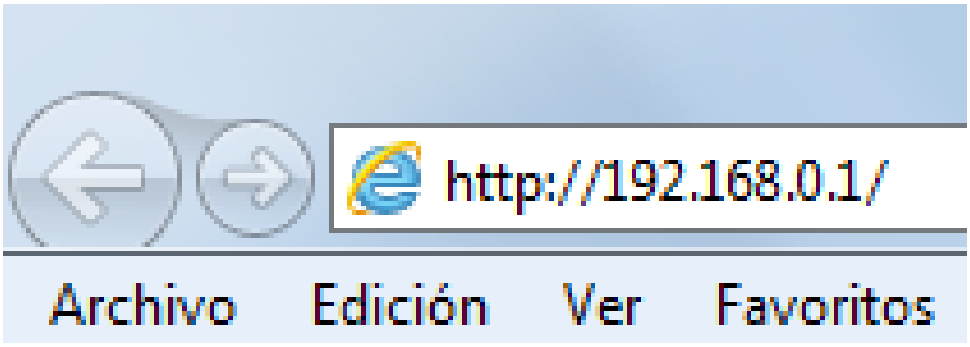


Figura 25. Ip nueva

J. Una vez cargado el software del dispositivo seleccionar Operation Mode (Modo de Operación) → Access Point (Punto de Acceso) y dar clic en Save.

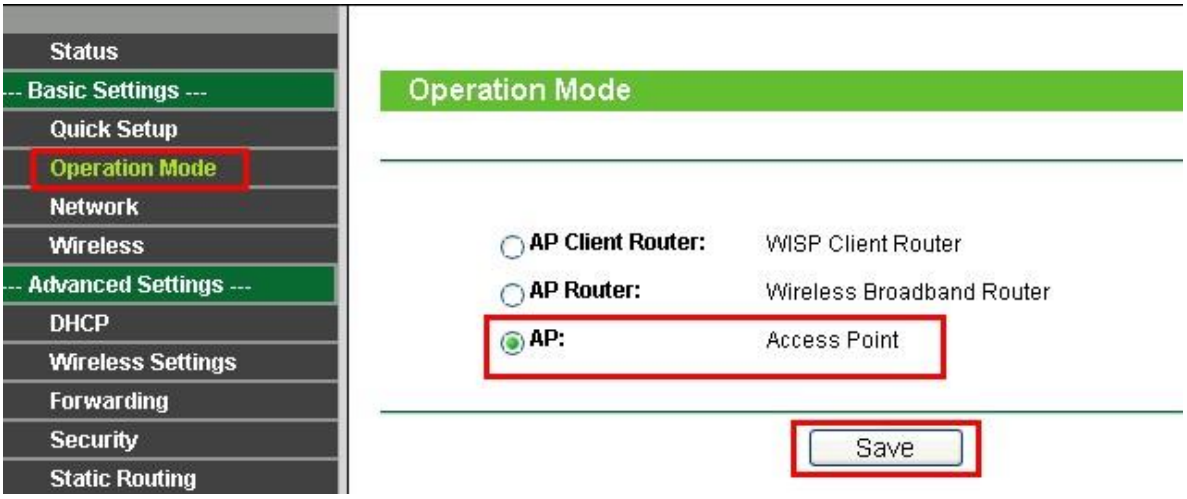


Figura 26. Modo de operación

K. Nuevamente esperar que se guarde la configuración y envié esta pantalla.

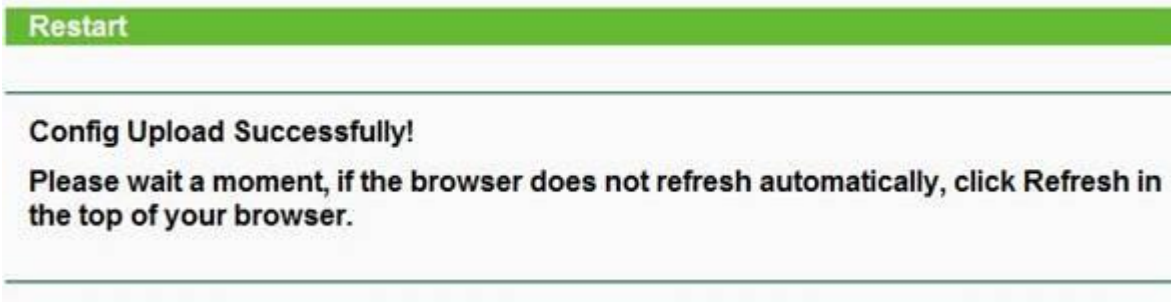


Figura 27. Reset 2

L. Seleccionar Wireless → Wireless Mode → Bridge (Point to Point) por ultimo seleccionar save.

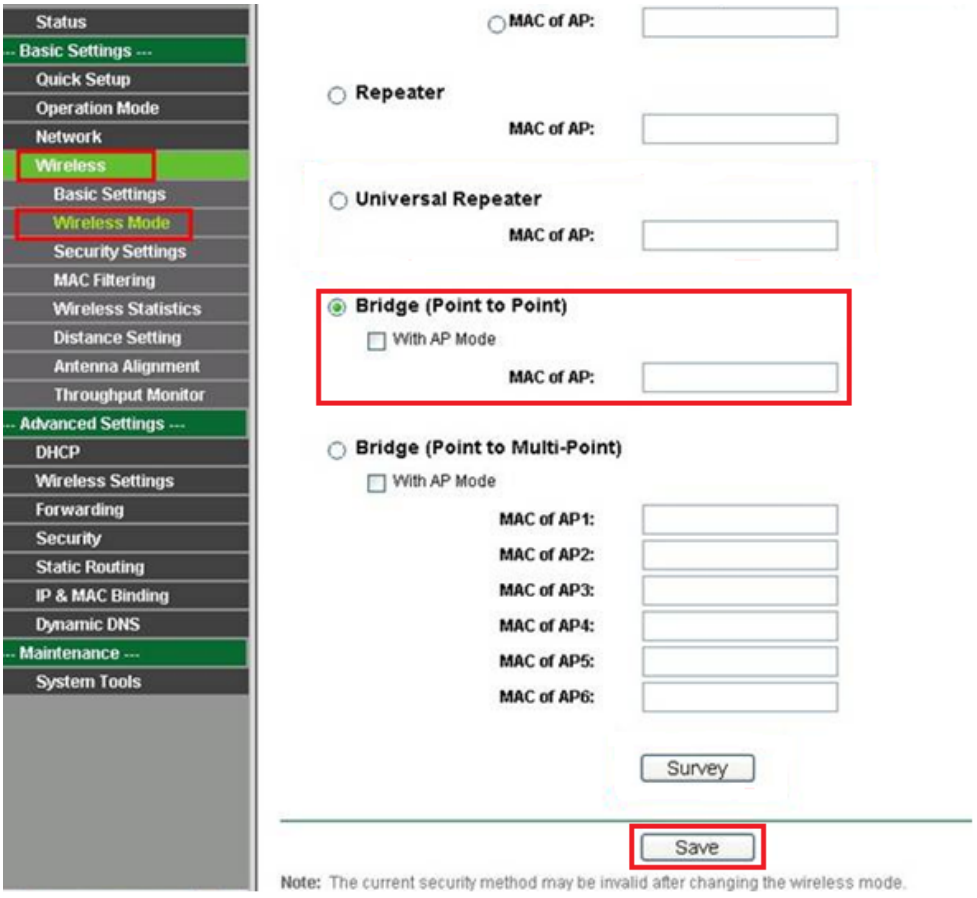


Figura 28. Wireless

M. Se reiniciará nuevamente el dispositivo.

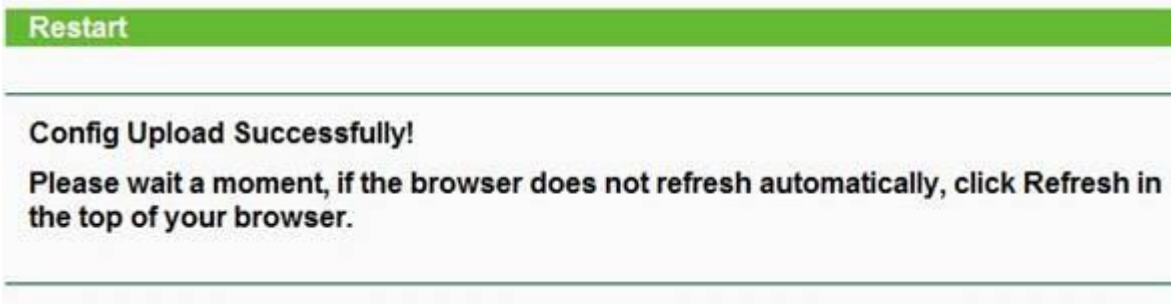


Figura 29. Reset 3

Nota: Esta configuración se realizará en otro dispositivo a diferencia de que se tendrá que agregar los siguientes pasos para lograr la conexión de punto a punto.

N. Se necesita detectar la red a la cual nos vamos a conectar en este caso el módem.

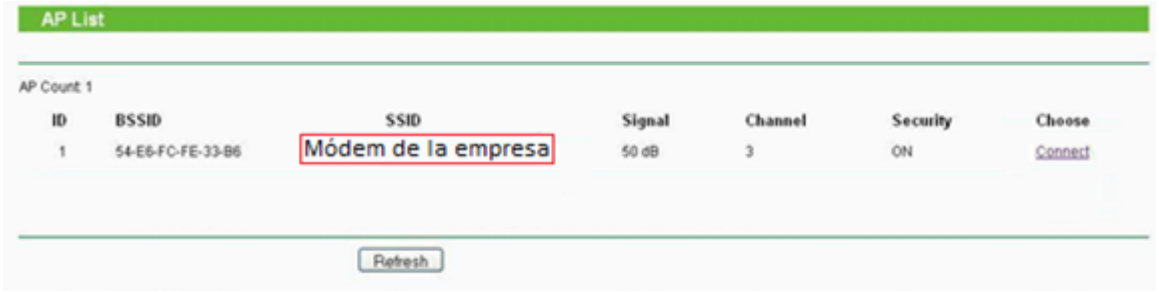


Figura 30. Modem de la empresa

O. Una vez detectada la red solo seleccionamos Connect.

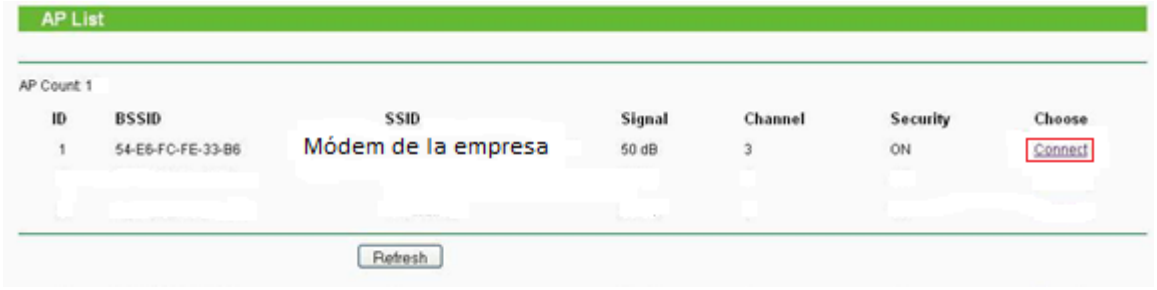


Figura 31. connect

P. Después se ingresara la contraseña del módem la cual por motivos de seguridad no se mostrará. La contraseña es de tipo wpa+wpa2 psk. Para introducir la contraseña se seguirá la siguiente ruta Wireless → Security Settings.

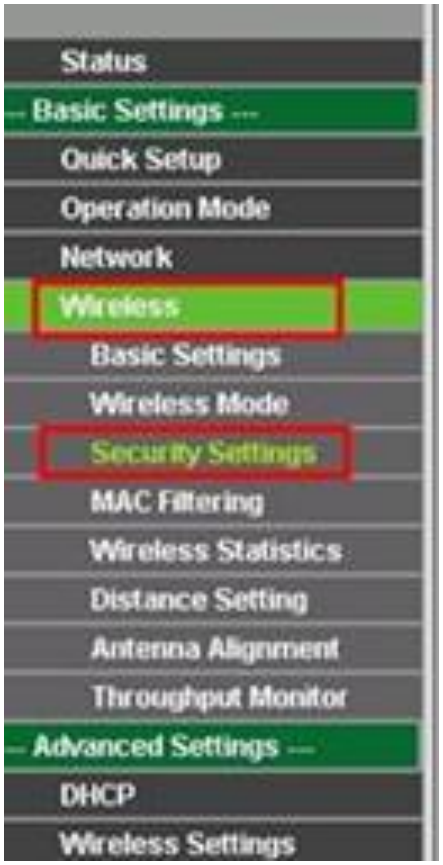


Figura 32. Security settings

Figura 33. Clave WPA2

Nota: Si se realiza alguna mala configuración solo se reinicia el dispositivo y regresara a su configuración de fábrica.

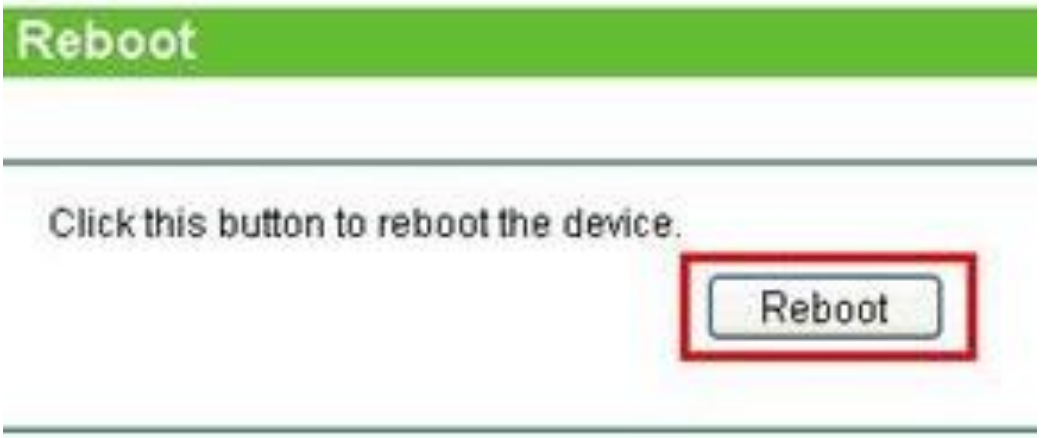


Figura 34. Reset 4

5.5. Configuración de AP modo Universal Repeater

A. Para realizar la configuración en modo Universal Repeater o mejor conocida como repetidor universal se tiene que configurar previamente en modo local. Conectado el dispositivo solo a una máquina.

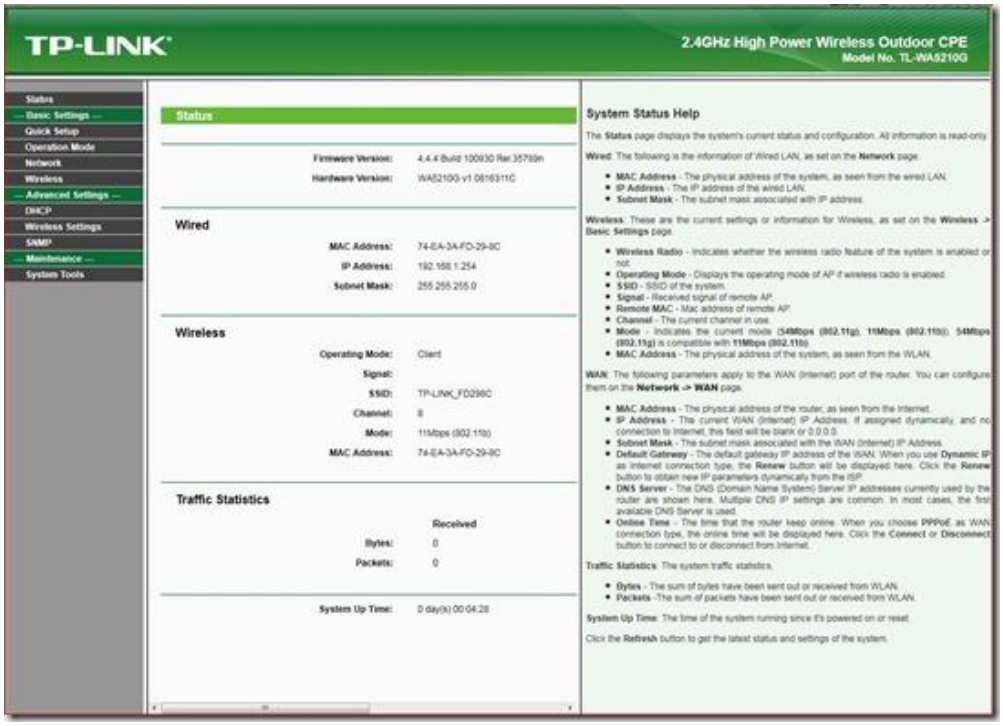


Figura 35. Principal 2

B. Una vez conectado entrar a la configuración del dispositivo de la siguiente manera: abrir cualquier navegador, insertar la siguiente dirección ip 192.168.1.254 y presionar enter.

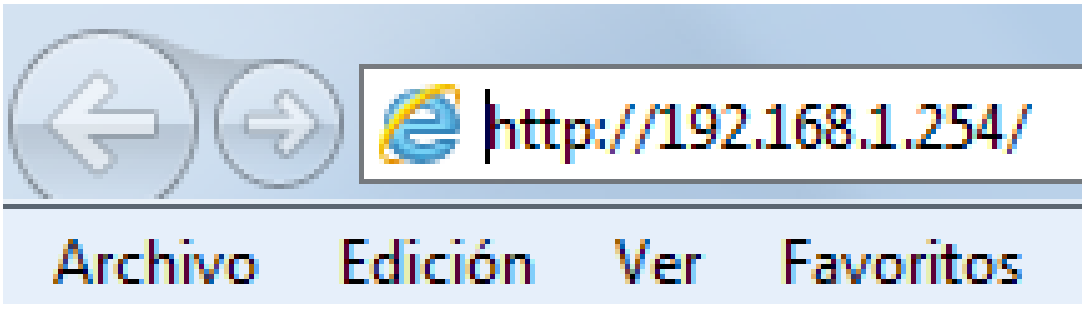


Figura 36. Dirección ip

C. Ahora aparecerá esta nueva ventada donde pide usuario y password.

Figura 37. Seguridad WIN

D. Por default es admin en los dos campos.

Figura 38. Ingreso de datos

E. Este es el software de configuración del dispositivo.

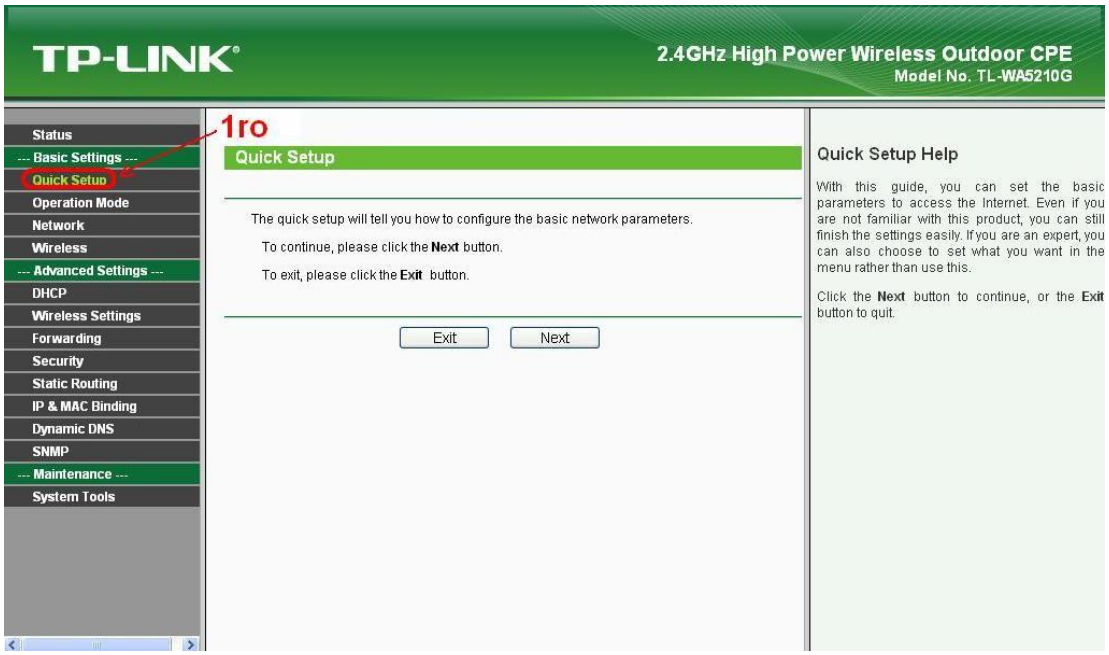


Figura 39. Quick setup

F. Lo primero que se tiene que realizar es cambiar la dirección ip del dispositivo, eso se hace de la siguiente manera entrando a la opción de Wireless Settings.

Figura 40. LAN

G. Ahora ingresamos la nueva dirección ip de nuestro dispositivo y damos clic en Save. (Cada dirección ip que se asigne a los dispositivos no se puede repetir)

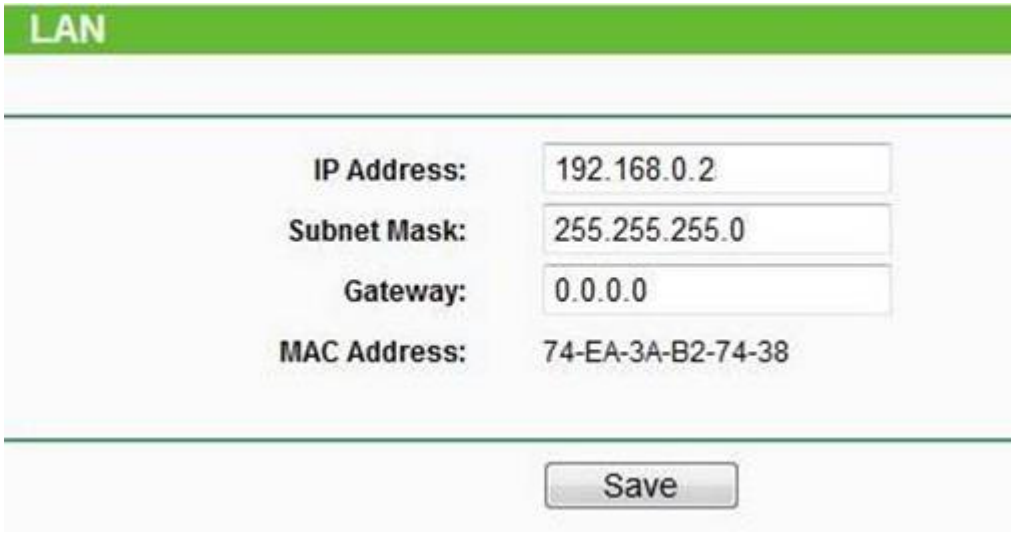


Figura 41. Save LAN

H. Esperar hasta que el dispositivo se reinicie, tendrá que salir esta pantalla.

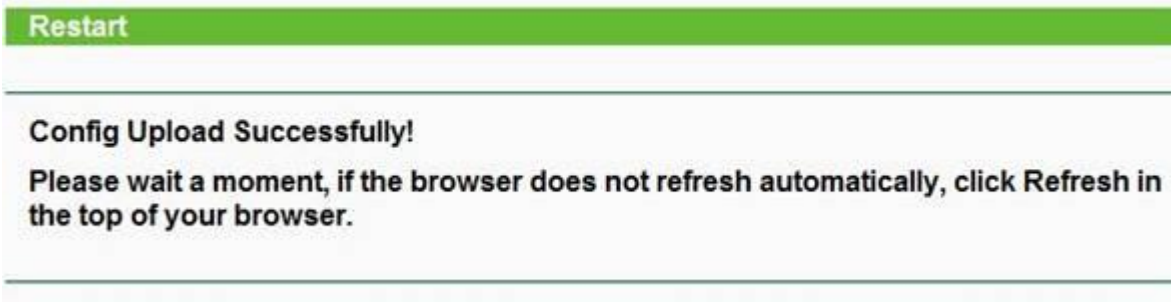


Figura 42. Reset 4

I. Se tendrá que ingresas con la nueva dirección ip al dispositivo. (Ahora ya se puede configurar el dispositivo conectado a internet)

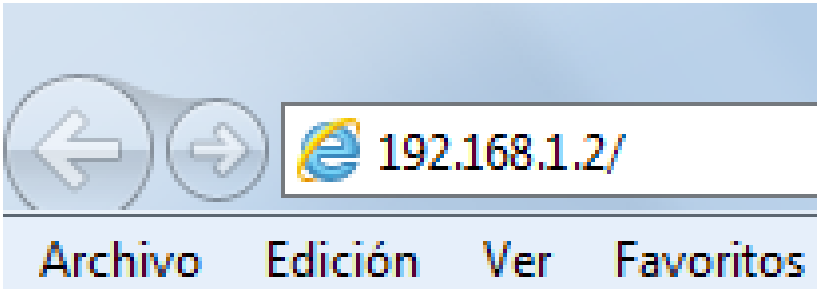


Figura 43. Ip nueva

J. Una vez cargado el software del dispositivo seleccionar Operation Mode (Modo de Operación) → Access Point (Punto de Acceso) y dar clic en Save.

.

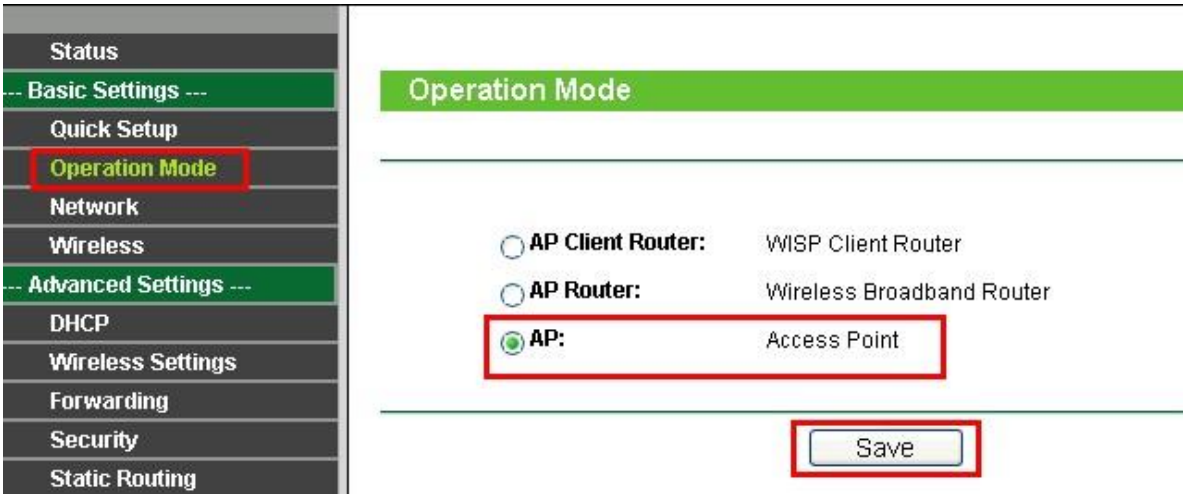


Figura 44. Operation mode

K. Nuevamente esperar que se guarde la configuración y envié esta pantalla.

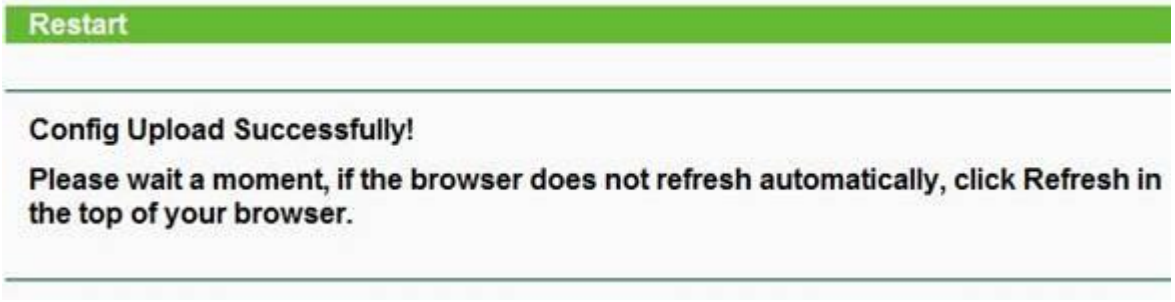


Figura 45. Reset 5

L. Seleccionar Wireless → Wireless Mode → Universal Repeater por último seleccionar save.

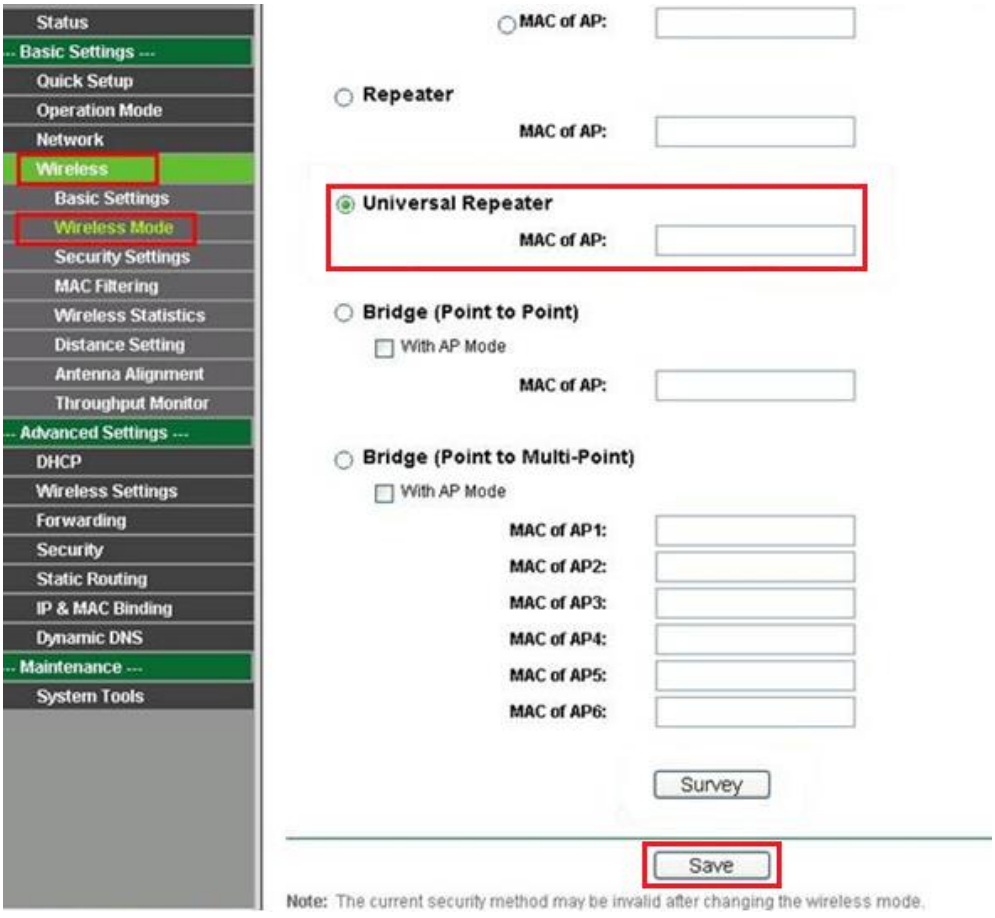


Figura 46.universal repeater

M. Es muy importante configurar la distancia de recepción para poder transmitir

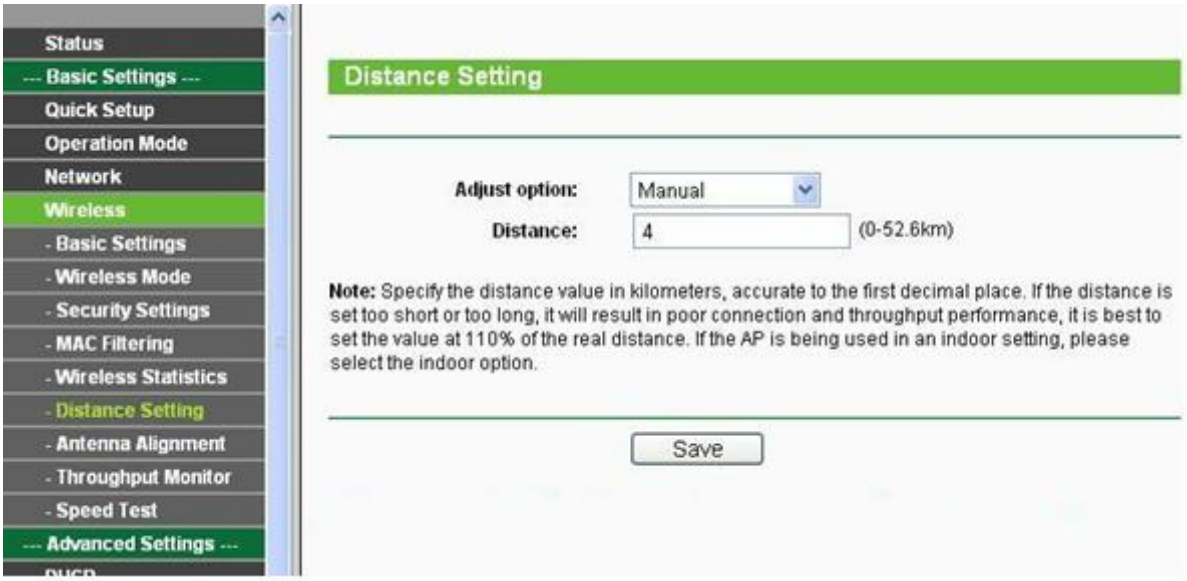


Figura 47. Distance setting

Nota: Esta configuración se tendrá que realizar en otro dispositivo ya que también será utilizado como repetidor universal.

5.6. Como conectar un dispositivo a la red

Para poder accesar a la red desde cualquier dispositivo solo se tiene que activar su tarjeta de red en las laptops, en los dispositivos móviles será su wifi para que detecten la red de la empresa, una vez detectada la única red se ingresa la contraseña de seguridad la cual es de encriptación wpa+wpa2 psk y se podrá disfrutar de todos los servicios que nos provee el internet y para los equipos de escritorio solamente conectándolos por medio del cableado utp tendrán acceso a internet.

El acceso a internet desde la sucursal podrá ser desde dispositivos inalámbricos cubriendo totalmente la zona de los trabajadores

Figura 48. Trabajadores

Figura 49. Modos de conexión

Cualquier dispositivo con la frecuencia correcta se podrá conectar de forma alámbrica y configurar para su utilización de la empresa

Figura 50. Cámara ip

Figura 51. Conexiones

La conexión a internet es exitosa

Figura 52. Conexión rj45

Figura 53. Internet en pc 1

Figura 54. Internet pc 2

Dispositivos inalámbricos conectados

Figura 55. Teléfonos móviles conectados a internet

Figura 56. Teléfono móvil conectado a internet distancia más larga

Figura 57. Tablet conectada a internet

Llamadas por ip.

Figura 58. Llamada en sucursal teléfono IP

Figura 59. Llamada simulador de teléfono IP oficinas centrales

Video Llamadas en tiempo real

Figura 60. Video llamada en tiempo real (sucursal- oficinas centrales)

6. Seguridad en la red

La Wi-Fi es una de las tecnologías líderes en la comunicación inalámbrica. El soporte para Wi-Fi se está incorporando cada vez en más aparatos: portátiles, celulares, tabletas y dispositivos para la trasferencia de todo tipos de datos. Hay un aspecto que en demasiadas ocasiones pasa desapercibido: la seguridad, aquellos métodos de encriptación utilizados para el nivel de esta.

En cuando a las medidas de seguridad en los aparatos Wi-Fi, se utiliza un protocolo de encriptación como WEP, WPA y WPA2. Examinaremos las debilidades del el protocolo resaltando la necesidad de una nueva arquitectura de seguridad en el estándar 802.11i, por lo que también estudiaremos la puesta en práctica en estos dispositivos junto a sus primeras vulnerabilidades menores y su integración en los sistemas operativos.

6.1. Introducción

La mayoría de las redes son vulnerables e inseguras principalmente las redes inalámbricas con cifrado WEP y facilidad con que se pueden recuperar claves WEP mediante técnicas de reinyección de tráfico, autentificación falsa y captura de datos, se nos plantea el reto de comprobar la seguridad de las redes WPA y WPA2. Existen varias formas de seguridad vía WPA-PSK, pero hablemos de las más usadas por la mayoría de las redes domésticas del tipo WPA-PSK si entrar en servidores RADIUS. La configuración mediante encriptación WEP no depende de una buena configuración, simplemente son inseguras. Las WPA-PSK suelen ser muy seguras, pero siempre que estén bien configuradas. Ahora las WPA2-PSK

son las más seguras hoy en día ya que su encriptación es mucho más completa que las anteriores versiones; ya que se puede configurar una contraseña con números, letras (mayúsculas y minúsculas) además de caracteres. [24]

6.2. Seguridad WEP

Descripción WEP (Privacidad Equivalente a Cableado), fue el primer protocolo de encriptación introducido en el primer estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite, proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits o de 128.

Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas, de ser captados con relativa facilidad. El sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada, varias debilidades serias fueron identificadas por analistas criptográficos. Como consecuencia, hoy en día una protección WEP puede ser violada con software fácilmente accesible en pocos minutos. [24]

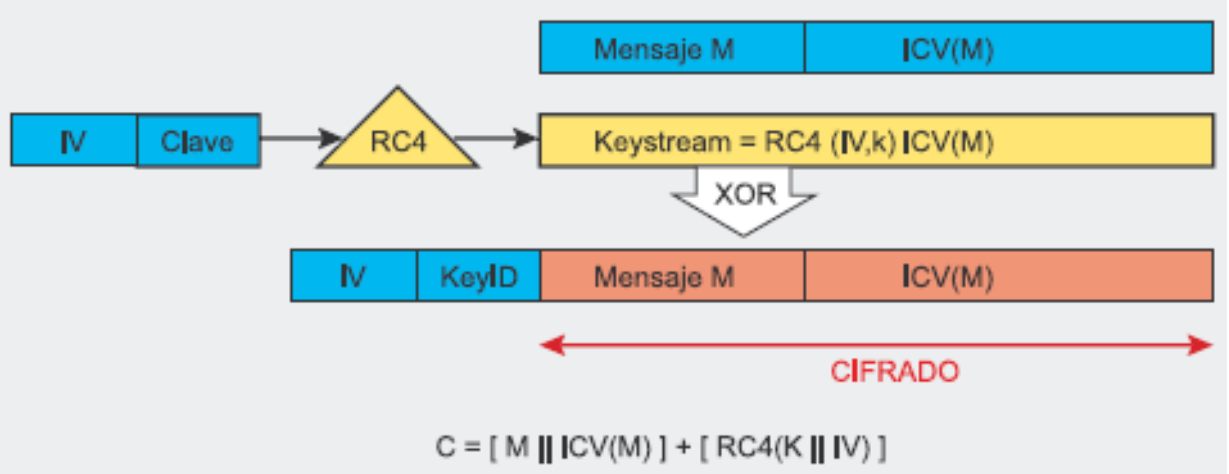


Figura 61. Seguridad WEP

El IEEE creó la nueva corrección de seguridad 802.11i para neutralizar los problemas, la Wi-Fi Alliance anunció que WEP había sido reemplazado por Wi-Fi Protected Access

(WPA). Finalmente, con la ratificación del estándar completo 802.11i (conocido como WPA2), el IEEE declaró que tanto WEP-40 como WEP-104 fueron revocados por presentar fallos en su propósito de ofrecer seguridad, A pesar de sus debilidades de WEP sigue siendo utilizado, ya que es a menudo la primera opción de seguridad que se presenta a los usuarios por las herramientas de configuración de los routers aun cuando sólo proporciona un nivel de seguridad que puede disuadir del uso sin autorización de una red privada, pero sin proporcionar verdadera protección. Fue desaprobado como un mecanismo de privacidad inalámbrico en 2004, pero todavía está documentado en el estándar actual.

WEP fue incluido como el método para asegurar la privacidad del estándar original IEEE 802.11, WEP usa el algoritmo de cifrado RC4 para la confidencialidad, mientras que el CRC-32 proporciona la integridad. El RC4 funciona expandiendo como una semilla para generar una secuencia de números pseudoaleatorios de mayor tamaño. Esta secuencia de números se unifica con el mensaje mediante una operación XOR para obtener un mensaje cifrado. Uno de los problemas de este tipo de algoritmos de cifrado es que no se debe usar la misma para cifrar dos mensajes diferentes, ya que obtener la clave sería trivial a partir de los dos textos cifrados resultantes. Para evitar esto, WEP especifica un vector de iniciación (IV) de 24 bits que se modifica regularmente y se concatena a la contraseña (a través de esta concatenación se genera la semilla que sirve de entrada al algoritmo).

Una clave WEP de 128 bits consiste casi siempre en una cadena de 26 caracteres hexadecimales (0-9, a-f) introducidos por el usuario. Cada carácter representa 4 bits de la clave (4 x 26 = 104 bits). Añadiendo el IV de 24 bits obtenemos lo que conocemos como "Clave WEP de 128 bits". Un sistema WEP de 256 bits está disponible para algunos desarrolladores, y como en el sistema anterior, 24 bits de la clave pertenecen a IV, dejando 232 bits para la protección. Consiste generalmente en 58 caracteres hexadecimales. (58 x 4 = 232 bits) + 24 bits IV = 256 bits de protección WEP. [25]

El tamaño de clave no es la única limitación de WEP. Cracker una clave larga requiere interceptar más paquetes, pero hay modos de ataque que incrementan el tráfico necesario. Hay otras debilidades en WEP, como por ejemplo la posibilidad de colisión de IV's o los paquetes alterados, problemas que no se solucionan con claves más largas.

En el sistema WEP se pueden utilizar dos métodos de autenticación: Sistema Abierto y Clave Compartida.

Para más claridad hablaremos de la autenticación WEP en el modo de Infraestructura (por ejemplo, entre un cliente WLAN y un Punto de Acceso), pero se puede aplicar también al modo Ad-Hoc.

Autenticación de Sistema Abierto: el cliente WLAN no se tiene que identificar en el Punto de Acceso durante la autenticación. Así, cualquier cliente, independientemente de su clave WEP, puede verificarse en el Punto de Acceso y luego intentar conectarse. En efecto, la no autenticación (en el sentido estricto del término) ocurre. Después de la autenticación y la asociación, el sistema WEP puede ser usado para cifrar los paquetes de datos. En este punto, el cliente tiene que tener las claves correctas. [26]

Autenticación mediante Clave Compartida: WEP es usado para la autenticación. Este método se puede dividir en cuatro fases:

I) La estación cliente envía una petición de autenticación al Punto de Acceso.

II) El punto de acceso envía de vuelta un texto modelo.

III) El cliente tiene que cifrar el texto modelo usando la clave WEP ya configurada, y reenviarlo al Punto de Acceso en otra petición de autenticación.

IV) El Punto de Acceso descifra el texto codificado y lo compara con el texto modelo que había enviado. Dependiendo del éxito de esta comparación, el Punto de Acceso envía una confirmación o una denegación. Después de la autenticación y la asociación, WEP puede ser usado para cifrar los paquetes de datos.

A primera vista podría parecer que la autenticación por Clave Compartida es más segura que la autenticación por Sistema Abierto, ya que éste no ofrece ninguna autenticación real. Sin embargo, es posible averiguar la clave WEP estática interceptando los cuatro paquetes de cada una de las fases de la autenticación con Clave Compartida. Por lo tanto es

aconsejable usar la autenticación de Sistema Abierto para la autenticación WEP (nótese que ambos mecanismos de autenticación son débiles).

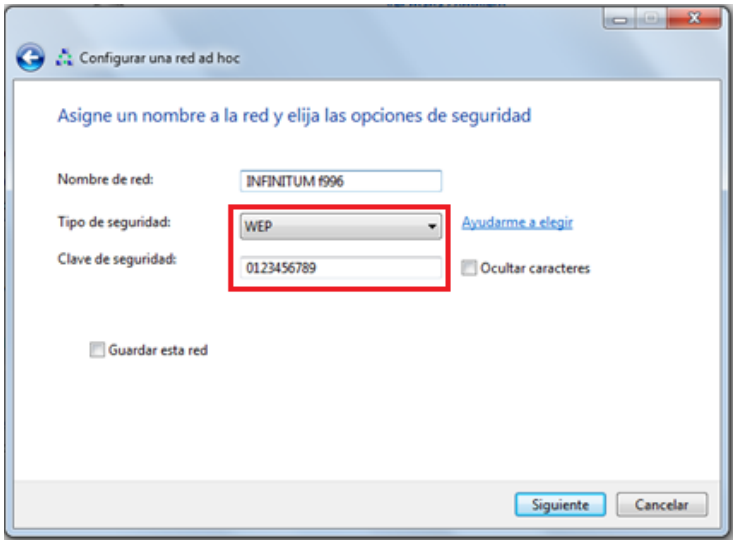


Figura 62. Configuración wep

6.2.1. WEB Plus

Es una mejora WEP desarrollada por Agere Systems (anteriormente una filial de Lucent Technologies) que mejora la seguridad WEP evitando "IV's débiles". Este protocolo es completamente eficaz únicamente cuando es usado a ambos extremos de la conexión inalámbrica. Como esto no es fácil de conseguir, representa una seria limitación. Es posible que tarde o temprano se logren ataques con éxito al sistema WEP+. Además no previene necesariamente los ataques de Replay. [27]

6.2.2. WEB Dinámico

En este caso las claves WEP cambian de forma dinámica. Cada cliente utiliza dos claves: una de asignación y una predeterminada. La clave de asignación se comparte entre el cliente y el punto de acceso, y protege las tramas unidifusión. La clave predeterminada es compartida por todos los clientes para proteger las tramas de difusión y multidifusión. WEP de clave dinámica ofrece ventajas significativas sobre las soluciones de WEP con clave estática. La más importante se refiere a que reduce el ámbito de cada clave. Las claves se

utilizan con menos frecuencia y se reduce el compromiso de la clave utilizándola para proteger menos tráfico. Otra ventaja es que a intervalos periódicos las claves se actualizan en el punto de acceso. Es un sistema distribuido por algunas marcas comerciales como 3Com.

La idea del cambio dinámico se hizo dentro de 802.11i como parte de TKIP, pero no para el actual algoritmo WEP. [27]

6.3. Seguridad WPA-PSK

Es un nivel más alto de seguridad que el WEP que combina la codificación y la autentificación para crear un nivel inquebrantable de protección. Una WPA-PSK (clave compartida en WPAPm) es configurada para cada dispositivo de red, para que los paquetes enviados sobre una red inalámbrica sean codificados usando TKIP (Protocolo de Integridad de Clave Temporal) o EAS (Estándar de cifrado avanzado). WPA es un sistema para proteger las redes inalámbricas (Wi-Fi). Creado para corregir las deficiencias del sistema previo, WEP Los investigadores han encontrado varias debilidades en el algoritmo WEP (tales como la reutilización del vector de inicialización (IV), del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. PSK: Claves pre-compartidas: Un método que realiza claves creadas manualmente y estáticas, utiliza el que configura la red inalámbrica para identificarse a un Ordenador PSK.

WPA adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red. Para no obligar al uso de tal servidor para el despliegue de redes, WPA permite la autenticación mediante una clave pre-compartida, que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red.

WPA fue diseñado para utilizar un servidor de autenticación (normalmente un servidor RADIUS), que distribuye claves diferentes a cada usuario (a través del protocolo 802.1x);

sin embargo, también se puede utilizar en un modo menos seguro de clave pre compartida para usuarios de casa o pequeña oficina.[2] [3] La información es cifrada utilizando el algoritmo RC4 (debido a que WPA no elimina el proceso de cifrado WEP, sólo lo fortalece), con una clave de 128 bits y un vector de inicialización de 48 bits. [28]

Una de las mejoras sobre WEP, es la implementación del Protocolo de Integridad de Clave Temporal (TKIP - Temporal Key Integrity Protocol), que cambia claves dinámicamente a medida que el sistema es utilizado. Cuando esto se combina con un vector de inicialización (IV) mucho más grande, evita los ataques de recuperación de clave (ataques estadísticos) a los que es susceptible WEP.

Adicionalmente a la autenticación y cifrado, WPA también mejora la integridad de la información cifrada. La comprobación de redundancia cíclica (CRC - Cyclic Redundancy Check) utilizado en WEP es inseguro, ya que es posible alterar la información y actualizar la CRC del mensaje sin conocer la clave WEP. WPA implementa un código de integridad del mensaje (MIC - Message Integrity Code), también conocido como "Michael". Además, WPA incluye protección contra ataques de "repetición" (replay attacks), ya que incluye un contador de tramas.

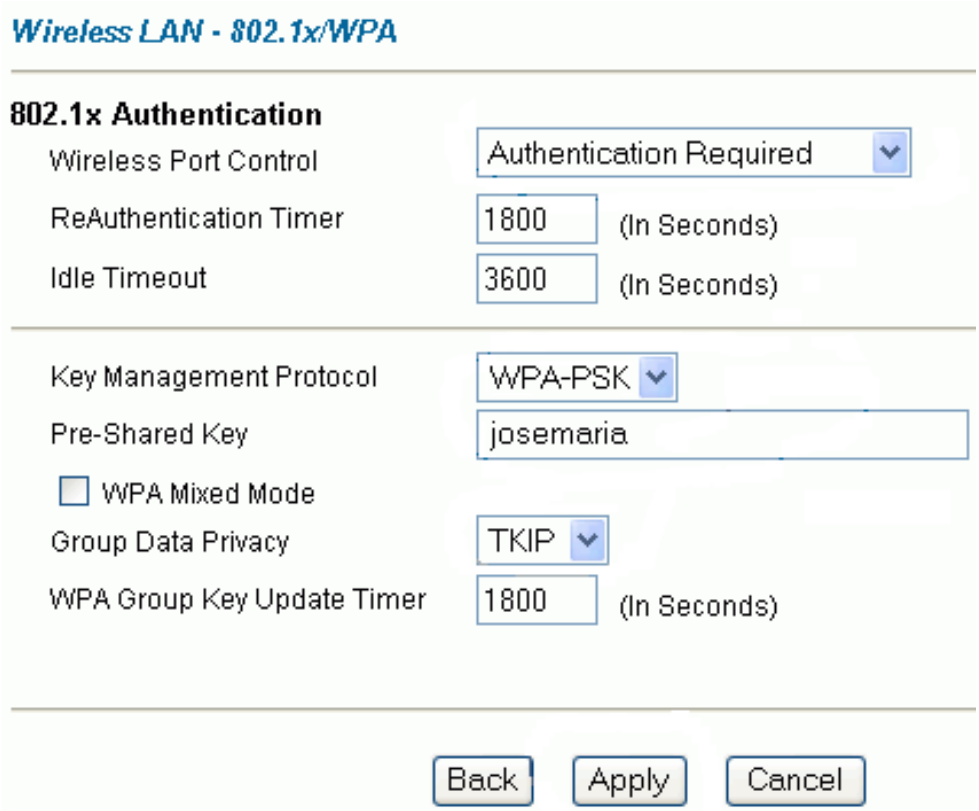


Figura 63. Wireless LAN

Al incrementar el tamaño de las claves, el número de llaves en uso, y al agregar un sistema de verificación de mensajes, WPA hace que la entrada no autorizada a redes inalámbricas sea mucho más difícil. El algoritmo Michael fue el más fuerte que los diseñadores de WPA pudieron crear, bajo la premisa de que debía funcionar en las tarjetas de red inalámbricas más viejas; sin embargo es susceptible a ataques. Para limitar este riesgo, los drivers de las estaciones se desconectarán un tiempo definido por el fabricante, si reciben dos colisiones Michael en menos de 60 segundos, podrán tomar medidas, como por ejemplo reenviar las claves o dejar de responder durante un tiempo específico. [29]

6.4. WPA2-PSK

Se tiene la idea de que las redes inalámbricas 802.11 cuentan con un nivel de protección alto cuando se encuentran configuradas mediante un cifrado WPA/WPA2, sin embargo, es importante hacer tres observaciones con respecto a este tema.

La primera se relaciona con la protección establecida por estos protocolos, debido a que principalmente se refieren a la autenticación, por lo que otros elementos básicos de seguridad, como la disponibilidad, no son cubiertos por el control, lo que implica la implementación de un conjunto de medidas adicionales para proporcionar un nivel de seguridad aceptable.

Por otro lado, la combinación de estos protocolos en conjunto con WPS (Wi-Fi Protected Setup), no da el resultado esperado, sino que se expone información debido a que existen vulnerabilidades que eliminan la protección brindada por la fortaleza de estos protocolos. De lo anterior se deriva la herramienta Reaver, muy popular en los últimos meses, la cual aprovecha la divulgación para vulnerar redes inalámbricas del tipo de cifrado WPA/WPA2.

Finalmente, la fortaleza que se utiliza es WPA/WPA2 está dada por el nivel de robustez de la contraseña, por lo que las contraseñas sin la fortaleza suficiente o configuradas por defecto por los fabricantes, son vulnerables a ataques de fuerza bruta. [30]

WPA2 (Acceso Protegido Wi-Fi 2) es un sistema para proteger las redes inalámbricas, creado para corregir las vulnerabilidades detectadas en WPA, WPA2 está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i.

La Wi-Fi Alliance llama a la versión de clave pre-compartida WPA-Personal y WPA2-Personal y a la versión con autenticación 802.1x/EAP como WPA-Enterprise y WPA2-Enterprise.Los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard). Con este algoritmo será posible cumplir con los requerimientos de seguridad del gobierno de USA - FIPS140-2. "WPA2 está idealmente pensado para empresas tanto del sector privado cómo del público. Los productos que son certificados para WPA2 le dan a los gestores de TI la seguridad que la tecnología cumple con estándares de interoperatividad" declaró Frank Hazlik Managing Director de la Wi-Fi Alliance. Si bien parte de las organizaciones estaban aguardando esta nueva generación de

productos basados en AES es importante resaltar que los productos certificados para WPA siguen siendo seguros de acuerdo a lo establecido en el estándar 802.11i.

WEP2 usa cifrado y vector de iniciación de 128-bits. Esta mejora de WEP fue presentada tras los primeros modelos 802.11i. Éste se podía desarrollar sobre algunos (no todos) tipos de hardware que no eran capaces de manejar WPA o WPA2. Se esperaba que eliminase la deficiencia del duplicado de IV así como ataques a las claves por fuerza bruta. Sin embargo, como todavía se basaba en el algoritmo de cifrado RC4, aún mantenía las mismas vulnerabilidades que WEP.

Después de que quedara claro que el algoritmo WEP era deficiente y requeriría aún más correcciones, tanto WEP2 como el algoritmo original fueron desechados. Las dos longitudes de clave ampliadas formaron lo que más adelante se conocería como TKIP del WPA.

Tanto la versión 1 de WPA, como la denominada versión 2, se basan en la transmisión de las autenticaciones soportadas en el elemento de información correspondiente. En el caso de WPA 1, en el tag propietario de Microsoft, y en el caso de WPA2 en el tag estándar 802.11i RSN. [31]

Durante el intercambio de información en el proceso de conexión RSN, si el cliente no soporta las autenticaciones que especifica el AP (access point, punto de acceso), será desconectado pudiendo sufrir de esta manera un ataque DoS específico a WPA. Además, también existe la posibilidad de capturar el 4-way handshake que se intercambia durante el proceso de autenticación en una red con seguridad robusta. Las claves PSK (precompartidas) son vulnerables a ataques de diccionario (no así las empresariales, ya que el servidor RADIUS generará de manera aleatoria dichas claves), existen proyectos libres que utilizan GPU con lenguajes específicos como CUDA (NVIDIA) y Stream (AMD) para realizar ataques de fuerza bruta hasta cien veces más rápido que con computadoras ordinarias.

El protocolo Address Resolution Protocol (ARP – RFC826) es usado para traducir una dirección IP de 32-bits a una dirección Ethernet de 48-bits (las redes Wi-Fi también utilizan

el protocolo ethernet). Para ilustrarlo, cuando un host A (192.168.1.1) quiere comunicarse con un host B (192.168.1.2), la dirección IP conocida debe ser traducida a una dirección MAC utilizando el protocolo ARP. Para hacerlo, el host A envía un mensaje broadcast conteniendo la dirección IP del host B (¿Quién tiene 192.168.1.2? Decírselo a 192.168.1.1). El host objetivo, reconociendo que la dirección IP en los paquetes coincide con la suya propia, devuelve una respuesta (192.168.1.2 está en 01:23:45: 67:89:0A). La respuesta es típicamente almacenada en la caché.

El protocolo de autenticación IEEE 802.1X (también conocido como Port-Based Network Access Control) es un entorno desarrollado originalmente para redes de cable, y posee mecanismos de autenticación, autorización y distribución de claves y además incorpora controles de acceso para los usuarios que se unan a la red. La arquitectura IEEE 802.1X está compuesta por tres entidades funcionales:

- El suplicante que se une a la red.
- El autenticador que hace el control de acceso.
- El servidor de autenticación que toma las decisiones de autorización.

En las redes inalámbricas, el punto de acceso sirve de autenticador. Cada puerto físico (puerto virtual en las redes inalámbricas) se divide en dos puertos lógicos, formando la PAE (Port Access Entity). La PAE de autenticación está siempre abierta y permite el paso de procesos de autenticación, mientras que el PAE de servicio sólo se abre tras una autenticación exitosa (por ejemplo, una autorización) por un tiempo limitado (3600 segundos por defecto). La decisión de permitir acceso está hecha por lo general por la tercera entidad, el servidor de autenticación (que puede ser un servidor Radius dedicado o – por ejemplo en las redes domésticas – un simple proceso funcionando en el punto de acceso). La Figura 3 ilustra el modo de comunicación entre estas entidades. [30]

El estándar 802.11i hace pequeñas modificaciones a IEEE 802.1X para que las redes inalámbricas estén protegidas frente al robo de identidades. La autenticación de mensajes se ha incorporado para asegurarse de que tanto el suplicante como el autenticador calculan sus claves secretas y activan la encriptación antes de acceder a la red.

Normalmente los routers protegidos con una encriptación WPA2-PSK son más seguros que las encriptaciones WEP y WPA. La clave WPA2-PSK soporta hasta 64 caracteres. Así que este tipo de contraseña es más robusta que cualquier otra, usando letras minúsculas, mayúsculas, números y caracteres simultáneamente. Para generar una clave "dura" fácilmente se puede usar una frase, un refrán, un estribillo de una canción para después modificarlo. Una manera sencilla de modificarlo es sustituir las vocales por sus números más parecidos y la vocal a por @. Por ejemplo: Usaremos el siguiente refrán que dice: "no por mucho madrugar amanece más temprano". Si cambiamos las vocales por números y símbolos, y los espacios por signos, nos podría quedar la clave así:

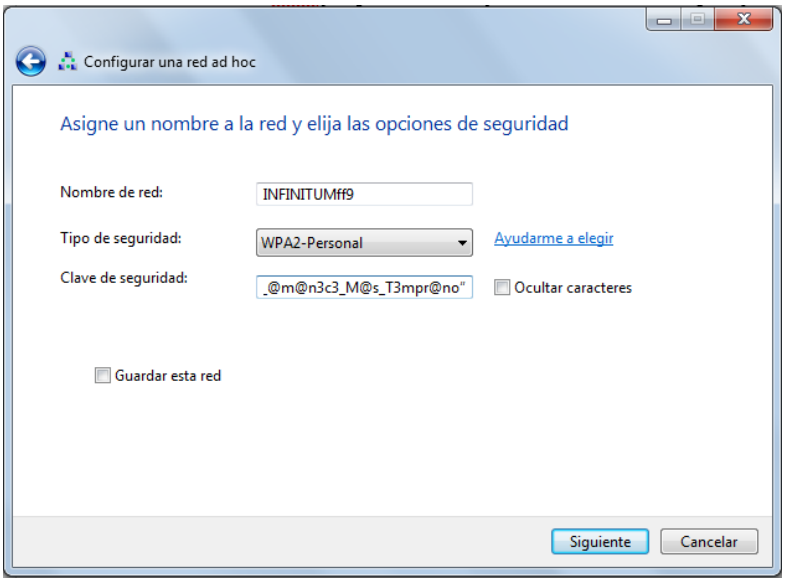


Figura 64. Configuración del host

Se ha generado una contraseña de encriptación muy robusta, además de ser una frase fácil de recordar a prueba de ataques por fuerza bruta. [31]

6.4.1. WPS

Wi-Fi Protected Setup™ es un programa opcional de certificación que proporciona la Wi-Fi Alliance [31], diseñado para facilitar la instalación y configuración de seguridad en redes inalámbricas de área local 802.11. Este programa fue presentado por la Wi-Fi Alliance a principios de 2007, proporciona un conjunto de soluciones de configuración de red para hogares y pequeñas oficinas. Permite administrar y configurar de manera segura los

elementos de una red inalámbrica pequeña sin necesidad de tener conocimientos avanzados en el tema. [32]

En WPS existen dos opciones principales de configuración de seguridad, Personal Identification Number (PIN) y Push Button Configuration (PBC), los Access Point deben ofrecer ambas opciones y los clientes deben ofrecer, al menos, la opción de seguridad PIN

6.4.2. ¿Cómo funciona el WPS?

WPS proporciona un procedimiento simple y consistente para agregar nuevos dispositivos a redes Wi-Fi, este procedimiento está basado en un protocolo de detección homogéneo por parte de los fabricantes. El procedimiento utiliza automáticamente un elemento para expedir credenciales a los dispositivos que están asociados en la red. Todos los Access Point certificados con WPS poseen capacidad de registro de nuevos dispositivos. Además, el elemento que registra puede residir en cualquier dispositivo de la red. Un elemento de registro que reside en el Access Point se conoce como Internal Registrar o elemento de registro interno. Un elemento de registro que reside en otro dispositivo de la red se conoce como External Registrar o elemento de registro externo. WPS puede admitir varios elementos de registro en una sola red [33].

El proceso para la configuración de un nuevo dispositivo en la WLAN comienza con una acción iniciada por el asistente de configuración e introduce el PIN o presiona el botón PBC. Ésta es la etapa donde el usuario pretende acceder a la red. WPS inicia el intercambio de información entre el dispositivo y el elemento de registro. Este último expide las credenciales de red (SSID y clave de seguridad) que autorizan al cliente a unirse a ésta. Una vez otorgado el acceso, el nuevo dispositivo puede comunicarse de forma segura transmitiendo datos a través de la red y evitando accesos no autorizados. Una vez que WPS ha finalizado y concede el acceso, la configuración es guardada, por lo que el usuario no tiene que realizar el procedimiento cada vez que quiera acceder. El dispositivo, una vez encendido, realizará una búsqueda automática para asociarse a la red.

WPS puede cifrar los datos y autenticar cada dispositivo, también puede ser utilizado en una red abierta, sin cifrado. El intercambio de credenciales de red e información

inalámbricas se realiza mediante el protocolo de autenticación extensible (EAP-WSC), uno de los protocolos de autenticación utilizados en WPA. Se establece un handshake en el que los dispositivos se autentican mutuamente y de ese modo un cliente es aceptado en la red, pues el elemento de registro comunica el SSID y la clave WPA2 previamente compartida (PSK). El uso de un PSK al azar mejora la seguridad al eliminar el uso de contraseñas que pueden ser previsibles y fáciles de obtener.

Por otro lado, en el método de instalación tradicional, el usuario debe configurar manualmente el Access Point para soportar el tipo de cifrado con PSK y, a continuación, debe introducir manualmente el SSID y PSK tanto en el AP como en el cliente. Este enfoque está sujeto a errores del usuario a través de una mala escritura de PSK y SSID. Con WPS, el proceso de intercambio de credenciales requiere poca intervención del usuario, solo hasta que se ha completado la primera acción de configuración (introducir el PIN o presionar el botón PBC), ya que la red emite el nombre y PSK.

La mayoría de los fabricantes, incluyendo Cisco/Linksys, Netgear, D-Link, Belkin, Buffalo, ZyXEL y Technicolor tienen dispositivos certificados en WPS, otros proveedores como TP-Link no están certificados pero cuentan con soporte para WPS.

6.4.3. Método PBC

Proveedor de servicios de internet (ISP) es una compañía que ofrece acceso a internet, normalmente por una cuota, tiene su lugar a través de una conexión de acceso telefónico, estos a su vez ofrecen servicios adicionales como cuentas de correo electrónico, exploradores web y espacio para crear sus propios sitios web. [35]

7. Empresa TP-LINK

TP-LINK es un proveedor global de productos para redes SOHO y N º 1 de la participación en el mercado en China, con productos traducidos a más de 100 países a decenas de millones de clientes. Comprometidos a una I + D poderosa, producción efectiva y gestión de calidad estricta, TP-LINK sigue ofreciendo productos premiados de redes de comunicación inalámbrica, ADSL, Routers, Switches, cámaras IP, adaptadores Powerline, servidores de impresión, convertidores de medios y los adaptadores de red para los usuarios finales del mundo.

Basado en la confianza de decenas de millones de clientes, TP-LINK está creciendo para convertirse en uno de los proveedores más competitivos de productos de red con aspiraciones de convertirse en una de las 3 marcas de redes y luchar por la mayor participación del mercado mundial, al avanzar en el mundo de las redes para servir mejor a nuestros clientes más valiosos con un producto que facilita la vida.

7.1. Introducción

TP-LINK se compromete a fabricar los productos de la mayor calidad para nuestros clientes finales de forma económica para que el ahorro en la fabricación llegue al cliente de forma que el producto resulte más atractivo en líneas generales. TP-LINK emplea las mejores técnicas de gestión y control de calidad para fabricar productos de calidad de la forma más eficiente posible.

Una autoridad de certificados (CA) es una autoridad (servidor de seguridad) en una red, o una entidad de terceros, que los problemas y administra las credenciales de seguridad y claves públicas para el mensaje cifrado y descifrado. Como parte de una infraestructura de clave pública (PKI), una entidad emisora comprueba con una autoridad de registro (RA) para verificar la información facilitada por el solicitante de un certificado digital. Si el RA verifica la información del solicitante, la entidad puede emitir un certificado.

En lo que respecta a la seguridad de la red Wi-Fi, un certificado es un identificador digital utilizado para autenticar una máquina o un usuario a una red. Ambos pueden ser necesarias para algunos métodos de autenticación. Un certificado contiene información sobre quién es el propietario del certificado, emisor del certificado, un número de serie único u otra identificación única, fechas de vencimiento y cifra la información que se puede utilizar para verificar la información de que disponen en el certificado. Dicha autenticación es más segura que un nombre de usuario o contraseña.

7.2. Certificación

Hardware.- El análisis de compatibilidad electromagnética e integridad de señal total garantiza que incluso con altos niveles de volumen de producción la calidad del producto mantiene la uniformidad y la estabilidad de rendimiento.

Software.- El completo control del código fuente del producto asegura que TP-LINK mantiene un fuerte control del rendimiento y funcionamiento del producto, tal como desarrollo del producto y capacidades de resolución de problemas

Nuestros productos han obtenido distintos certificados oficiales a nivel mundial:

Figura 65. Certificación

Producto completo.- TP-LINK prueba los productos completados basándose en el desgaste a largo plazo en todos los entornos, incluso la temperatura y humedad, sostenibilidad de la fuente de alimentación y las vibraciones. Esta comprobación asegura que el producto es duradero y mantiene el mismo rendimiento a lo largo de toda su vida útil.

Los productos TP-LINK cuentan con la mejor tecnología de proveedores de chipset reconocidos a nivel mundial, para proporcionar los mejores productos posibles a nuestros clientes alrededor del mundo.

7.2.1. Control de calidad

TP-LINK mantiene un estricto control de calidad en la manufactura de nuestros productos para mantener nuestras cifras RMA (devolución de material) al mínimo posible para beneficiar tanto a los distribuidores como a los revendedores y especialmente a los clientes finales.

Estricto sistema de control de calidad

- Sistema de Calidad Corporativo: ISO 9001 - 2000
- 22 puntos de control de calidad (5 puntos de control de calidad para la sección SMT)

Objetivos de Calidad:

- Índice de aprobación IQC: ≥98.20%
- Índice de aprobación en la primera: ≥99.10%
- Índice de aprobación FQA: ≥98.50%
- Satisfacción del Cliente: 97.00%

7.3. Acerca de TP-LINK

TP-LINK ha crecido de manera rápida en los últimos años y no solamente en la industria de las redes, sino en la industria IT en general. En el año 2011, los envíos de CPEs inalámbricos y de banda ancha de TP-LINK fueron el NO.1 a nivel mundial con el 32.12% y el 27.48% respectivamente para el 3er trimestre del año 2011, basado en un reporte de industria de dispositivos de terminales de redes, dicho reporte provino de una de las organizaciones de investigación de industrias líderes en el mundo – In-Stat*

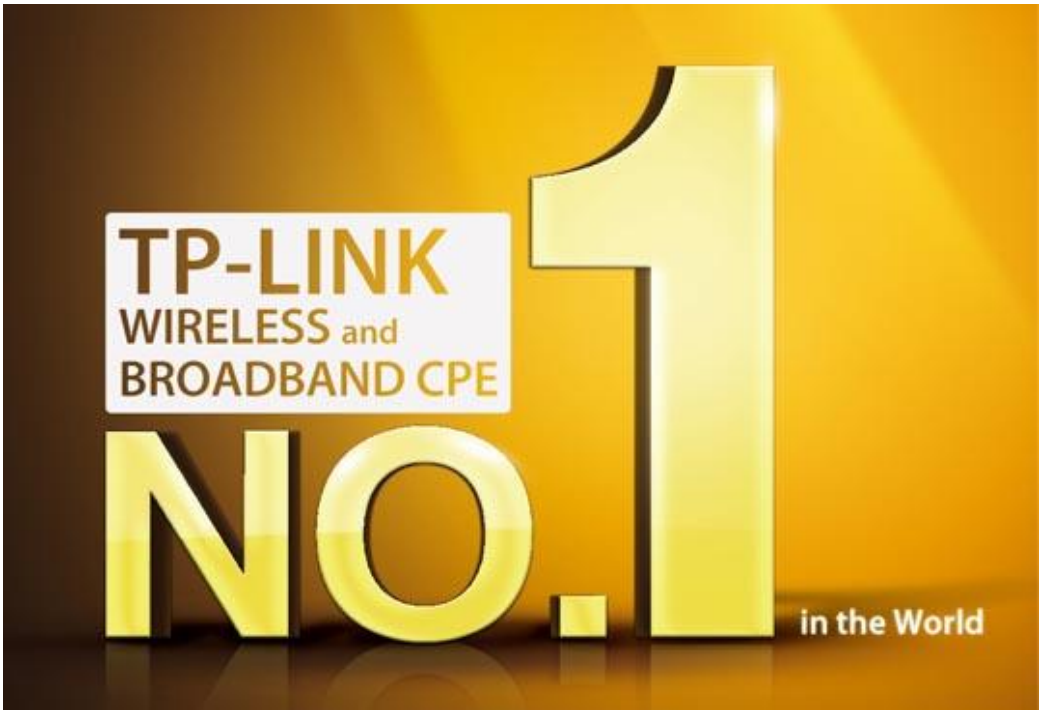


Figura 66. No.1

Desde su entrada en el mercado internacional en 2005, TP-LINK se ha vuelto más y más interesado en el mercado internacional. Nuestros productos se distribuyen en más de 100 países y sirven a más de mil millones de usuarios en todo el mundo.

En 2009, el 41.8% de nuestros ingresos anuales fue del mercado internacional, y hemos iniciado con éxito nuestras primeras cuatro sucursales del extranjero en Singapur, Alemania, EE.UU. e India, con planes para nuestras oficinas en el Reino Unido, Rusia, Italia y Vietnam ya en vigor con el fin de proporcionar un servicio rápido y completo a nuestros clientes.

Figura 67. Países

Desde que iniciamos en el Mercado mundial en el 2005, TP-LINK ha sufrido un crecimiento notable y dramático alimentado por excelentes productos y prácticas de negocios. Con una velocidad de crecimiento promedio anual del 44.7% en los últimos 7 años, Los ingresos de ventas de TP-LINK alcanzaron los mil millones de dólares (USD) en el año 2011. [36]

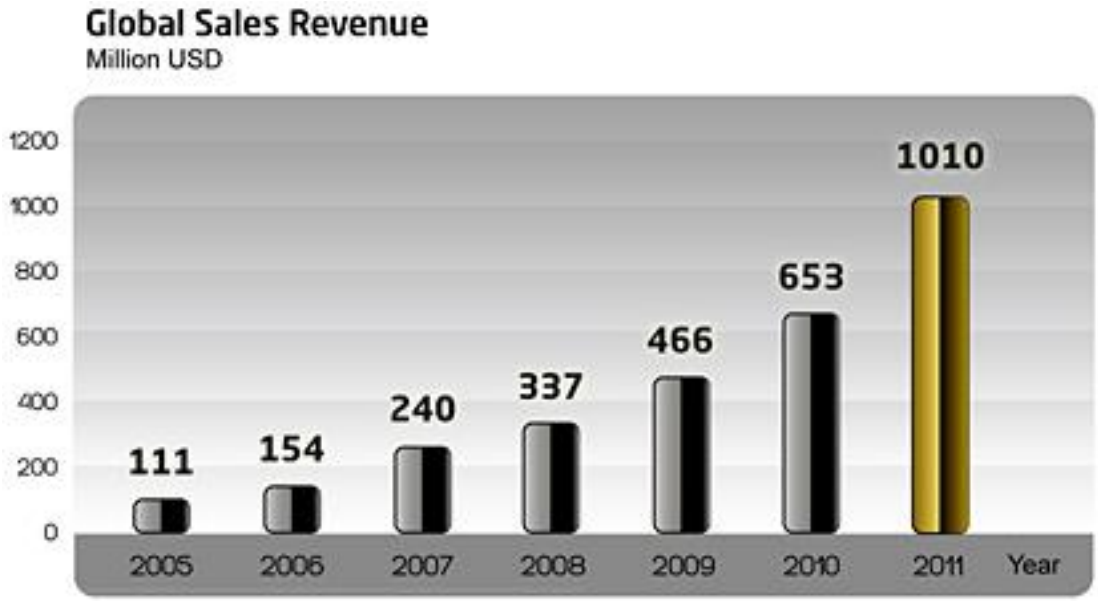


Figura 68. Global sales revenue

7.3.1. Principios fundamentales de TP-LINK

El cliente es primero

TP-LINK se esfuerza para asegurar que trabajamos de manera que facilitemos las vidas de nuestros clientes, para asegurar una relación comercial duradera y beneficiosa para ambas partes

Nuestra Base es la Calidad

Los cimientos sobre los que se levanta TP-LINK son la calidad en el producto y, especialmente, la calidad en el servicio. Nuestro objetivo es proporcionar los mejores productos que podamos y complementarlos con un servicio que esté a la altura de la calidad que nos esforzamos por proporcionar a nuestros clientes.

Empresa honesta

TP-LINK intenta ser lo más transparente, honrada y confiable que sea posible, tanto dentro de la empresa con los empleados, como con nuestros clientes y colaboradores, para mantener un crecimiento constante basado en estos sólidos principios.

Enfoque mantenido

TP-LINK se esfuerza por crecer al ritmo de la industria de las redes y la comunicación, mejorando constantemente sin desviarnos de nuestros objetivos clave y nuestro sector de productos. De esta forma esperamos alcanzar la excelencia en nuestro sector y ser líderes por consiguiente.

7.4. Beneficios de contar con certificación TP-LINK

El departamento de Investigación y desarrollo (R&D por sus siglas en inglés) de TP-LINK es la clave de nuestros productos y como tal es una gran parte del éxito actual y futuro de TP-LINK en la industria mundial de redes. El Departamento de R&D de TP-LINK está formado por un gran equipo de gente altamente instruida que utilizan el equipo y técnicas más avanzadas brindando a TP-LINK productos innovadores de alta calidad.

El equipo de R&D de TP-LINK es el motor que mueve la capacidad e ingenio de TP-LINK y está formada por más de 800 ingenieros experimentados de R&D, la mayor parte de los cuales, son graduados de las mejores universidades de China. Para apegarse a los estrictos requisitos de control de calidad de TP-LINK, 400 o la mitad de nuestros 800 empleados de R&D están dedicados exclusivamente a probar los productos para garantizar la mejor calidad de los mismos. [36]

Con nuestros servicios de certificación Wi-Fi, usted puede estar seguro de:

- Los dispositivos Wi-Fi han sido sometidos a pruebas de interoperabilidad para mejorar la experiencia del usuario
- La interoperabilidad certificada soporta bajas tasas de retorno, reduce los costos, proporciona una mayor satisfacción de los consumidores y mayores volúmenes comercializados
- Aseguramiento de pruebas en numerosas configuraciones y con una muestra diversa de otros dispositivos para asegurar la compatibilidad con otros equipos Wi-Fi CERTIFIED

- Entrada inmediata el mercado
- Servicios de Expertos de pruebas Wi-Fi
- Una ventaja frente a la competencia con un sello de auditoría
- Tiempos rapidos de las auditorias gracias a nuestra gran experiencia
- Servicio de ventanilla única exclusivo de TÜV Rheinland
- Cumplimiento con los requisitos legales de los gobiernos locales

Nuestros Servicios de Wi-Fi

TP-LINK ofrece la pre-certificación la certificación oficial de los siguientes planes de pruebas Wi-Fi:

- 802.11n Draft 2.0.
- WPA/WPA2 – 802.11a/b/g.
- WMM®.
- WMM – Power Save.
- WPA/WPA2 – 802.11h/d.
- WPA/ WPA2 – 802.11a/b/g.
- WPA/WPA2 – Dual Band a/g – a/b. [36]

8. Implementación del sistema de telecomunicación

Las pruebas se realizan con el fin de cumplir con los objetivos ya establecidos, en este caso se realizó un análisis del tráfico de los datos, velocidad de respuesta envió y recepción de paquetes entre otros, ya que la red es la base que soporta el negocio, una carretera que cada vez trasmite más información y aplicaciones que soporten esos datos y es que la convergencia hoy es una realidad donde múltiples servicios conviven en una misma plataforma.

8.1. Introducción

El estudio de la telecomunicaciones han desarrollado nuevas y novedosas técnicas capaces de entregar una mayor información sobre los procesos que en ella se desarrollan, esta contante búsqueda se ha extendido con el fin de lograr los objetivos ya fijados en el comportamiento de las redes, [1] y es así como el alcance de una red traspasa la integración de soluciones de voz, video y datos, pues bajo una misma estructura convergen sistemas IP, seguridad, conexiones inalámbricas, internet y mucho más[2].

La amplitud de estos temas permite que sean tratadas y evaluadas desde varias perspectivas [1], por lo mismo la importancia de la estructura de equipamiento (AP, repetidores y Reuters) es vital a la hora de implementar cualquier tipo de solución tecnológica ya que será la base para garantizar su performance y funcionamiento. Será esta estructura la que permita que PC´s y otros dispositivos instalados en una determinada red puedan comunicarse entre sí [2].

8.2. Colocación de los AP

La colocación del AP

Figura 69. Colocación AP

Figura 70.colocacion tp-link

Lugar donde se colocó el primer repetidor

Figura 71. Perspectiva 1

Perspectiva del primer repetidor

Figura 72. Perspectiva 2

Lugar de colocación del segundo repetidor

Figura 73. Perspectiva 3

Figura 74. Lugar de la sucursal

Figura 75. Llegada a la sucursal

Figura 76. Llegada a la sucursal 2

Lugar donde se colocó el segundo AP

Figura 77. Llegada a la sucursal 3

8.3. Pruebas de conexión

El objetivo de las pruebas realizadas fue comprobar la cobertura ofrecida por el dispositivo y localizar las ubicaciones más propicias para desarrollar una excelente cobertura, debido a la orografía del terreno y para evitar pérdidas adicionales debidas a la vegetación, los únicos puntos accesibles para la ubicación del router se encuentran a lo largo de las instalaciones de la constructora.

Se estableció un primer punto de pruebas en el entorno con el objetivo de comprobar el correcto funcionamiento de los equipos de comunicaciones.

Figura 78. Pruebas de conexión con celulares

Partiendo de ese punto, se realizaron pruebas en otros puntos de las aumentando la distancia al router con el objeto de localizar el punto más alejado desde el cual sea posible establecer la comunicación.

Para estos puntos extremos se realizaron pruebas bajo configuraciones del router en modo 11b+g, con objeto de establecer las idoneidad de la utilización.

Las pruebas consistió en la realización de cuatro mediciones con el adaptador inalámbrico del ordenador portátil: intensidad de señal recibida y comprobación de la posibilidad de asociarse al punto de acceso, velocidad nominal de la asociación, tiempo de ida y vuelta al igual la velocidad real de transmisión de datos; así como el establecimiento de la comunicación entre el ordenador personal del dispositivo.

Para realizar las mediciones de la intensidad de la señal se utilizó la aplicación de software libre Network Stumbler, que muestra gráficamente el nivel detectado en el adaptador inalámbrico en todo instante, calculando el valor máximo y mínimo recibido. Con esta prueba se comprueban las diferencias con el cálculo teórico del balance de potencia, a la vez que permite orientar la antena de manera óptima.

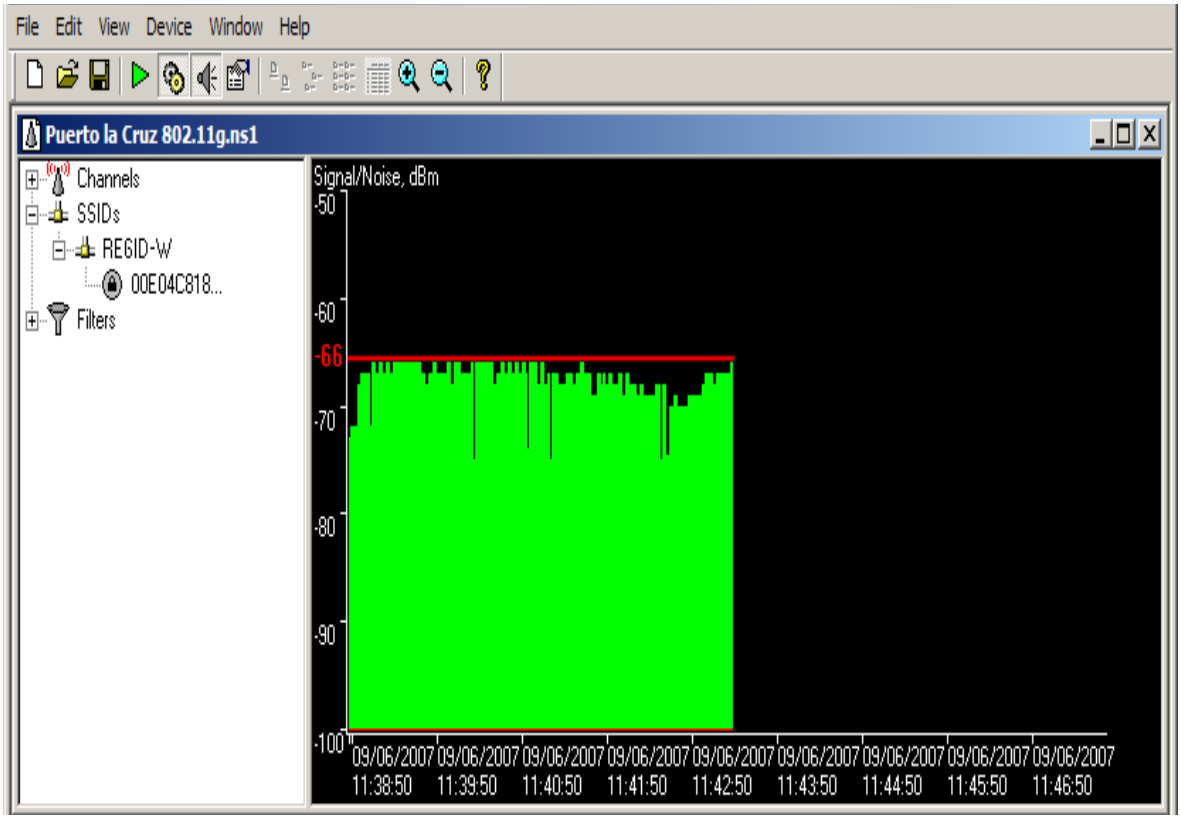


Figura 79. Intensidad de señal 1

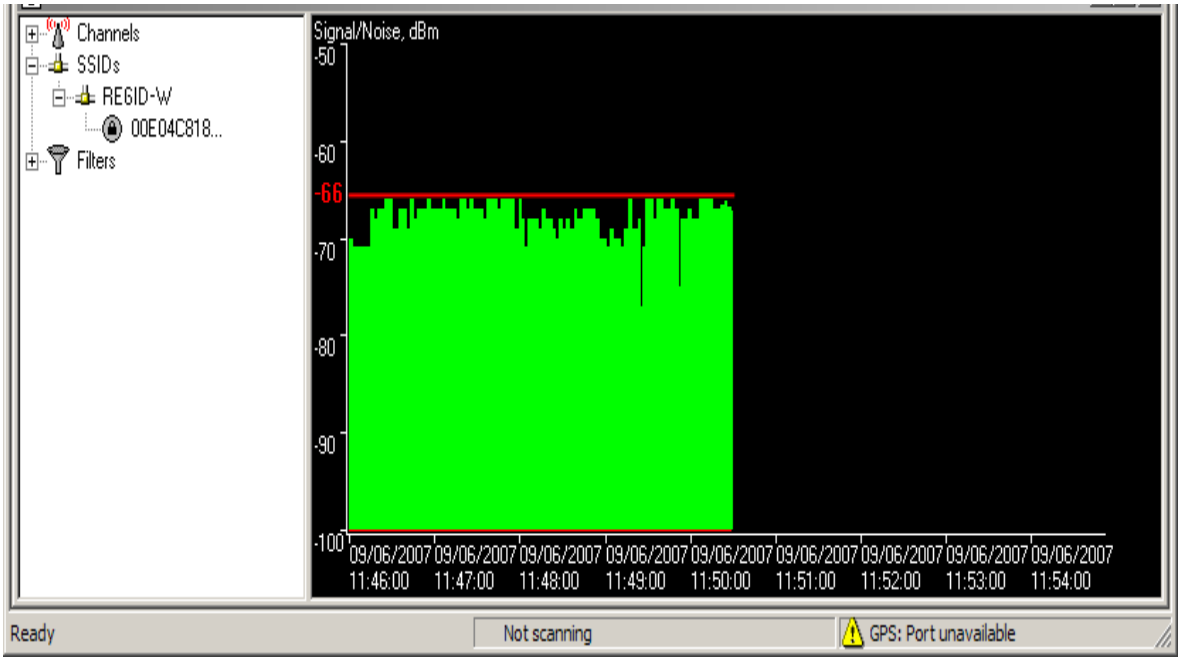


Figura 80. Intensidad de señal 2

Una vez orientada la antena, se verificó que el ordenador portátil podía asociarse al dispositivo, introduciendo previamente las claves WPA2 requeridas.

.

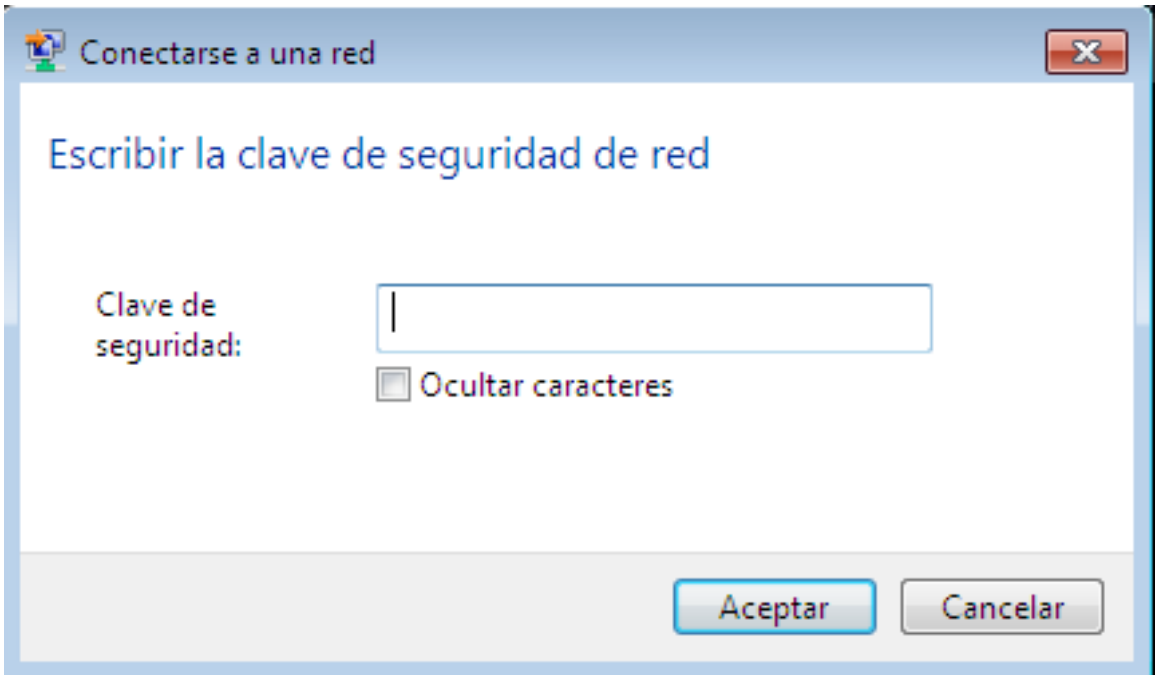


Figura 81. Prueba de seguridad

El sistema operativo indicó la velocidad nominal de la asociación. Esta prueba muestra la calidad del enlace, desde el punto de vista del sistema operativo.

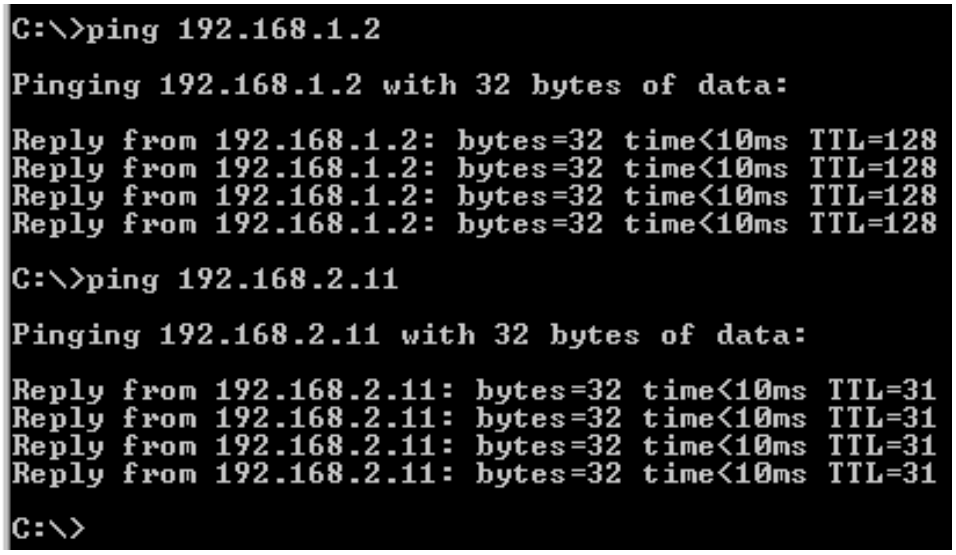


Figura 82. Prueba de transferencia de datos

Par el cálculo del RTT se utilizó el comando ping, que realiza el envío consecutivo de una serie de paquetes IP al equipo indicado y muestra el tiempo que tarda en obtener la respuesta del otro extremo de la comunicación. Con este parámetro se comprueba la estabilidad del radioenlace y la posible pérdida de datos durante la comunicación.

Figura 83. Prueba de velocidad 1

Figura 84. Prueba de velocidad 2

Para medir la velocidad real de transmisión, se realizaron transferencias de ficheros entre el ordenador personal del dispositivo y el ordenador, se calcularon las velocidades de transferencia. Con esta última prueba, se verifica cómo se comporta realmente el enlace a la hora de realizar una transferencia de datos.

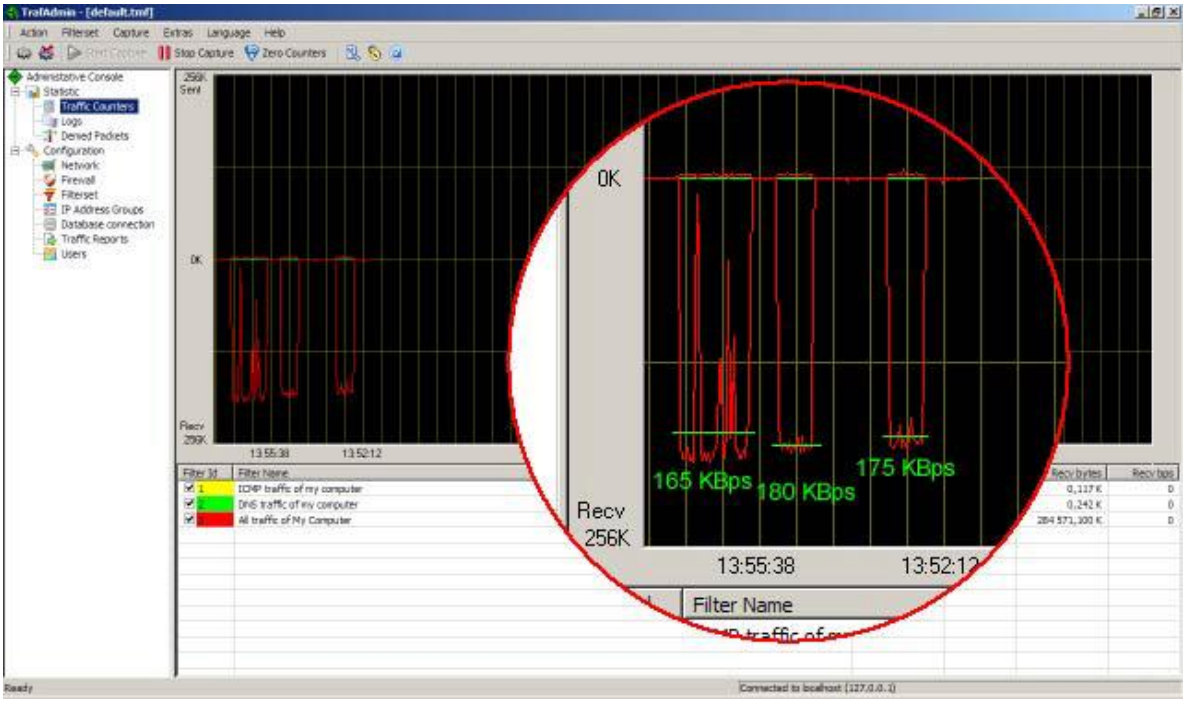


Figura 85. Medida de velocidad 1

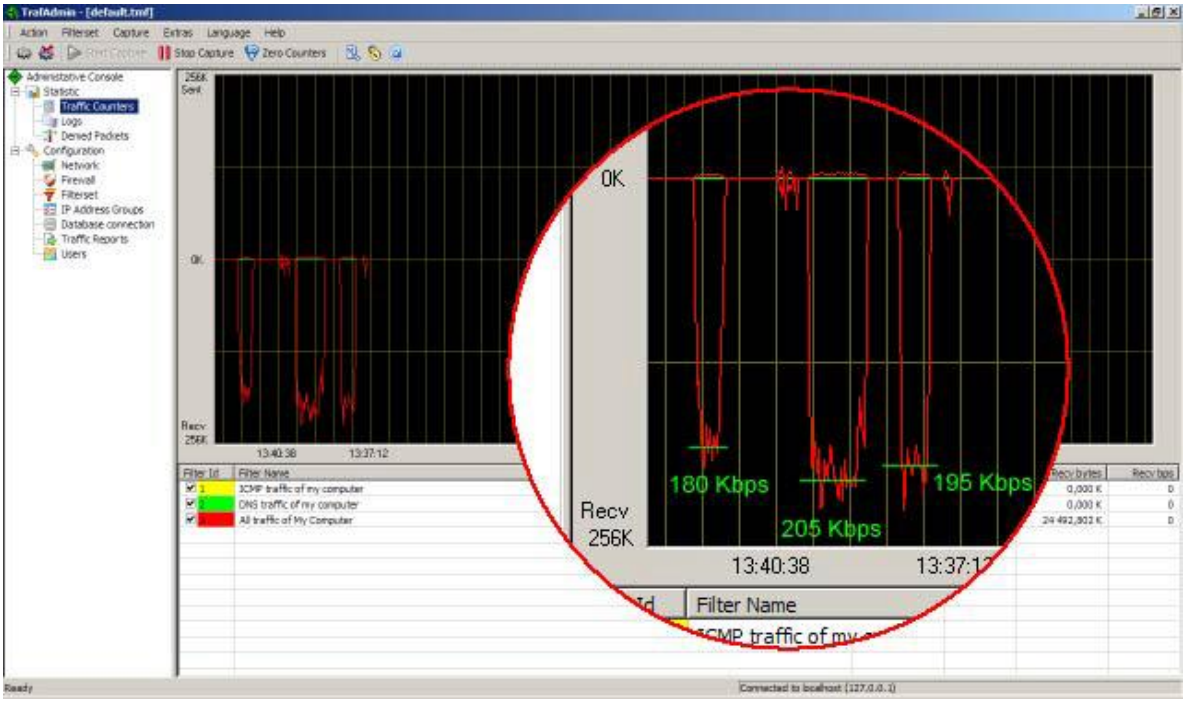


Figura 86. Medida de velocidad 2

Conclusiones

Para detectar el problema se tuvo que seguir una metodología, así mismo para brindar una solución, la cual es la implementación de un sistema de telecomunicación en la frecuencia de los 2.4 GHz.

Para un verdadero despliegue de una red inalámbrica en necesario pensar en un enfoque conceptual y la valoración objetiva, los análisis que se realizan son necesarios para conocer el valor real de la ampliación de una red, además de conocer los escenarios y dispositivos que están adaptados para las situaciones climatológicas, así mismo comprender que los beneficios son muy factibles compensando esos puntos débiles que presentan pérdidas para la empresa.

En el diseño de un sistema de telecomunicaciones es fundamental un buen conocimiento en las características y limitaciones de los dispositivos, escenarios y proveedores de internet, para poder hacer una adecuada distribución en conjunto de los mismos, así mismo localizar las ventajas y debilidades con un análisis previo, aumentando la calidad, ampliando la cobertura de este sistema de telecomunicación adaptándose a las condiciones y necesidades de la empresa.

Conocer el dispositivo es una gran ventaja para su configuración, logrando un desarrollo inalámbrico en la empresa, ya que a su vez esta recuperara el control de su reciente sucursal, algo muy importante que se viene preparando desde tiempo atrás, con ayuda de un análisis de dispositivos configurados y en puntos estratégicos (diseño) esto se lograra.

Trabajo futuro

Nosotros como responsables conocemos que el mantenimiento puede ser una tarea muy ardua, con continuas caídas y degradaciones en el funcionamiento. Las razones de ello son múltiples: la primera de ellas y principal factor es partir desde el primer momento con un diseño e implantación inicial de la red incorrecta, defectuosa o no adecuadamente dimensionado. Suele seguir un importante descuido en las labores de mantenimiento, las cuales evitarían la mayoría de las incidencias posteriores, y no se implantan las herramientas necesarias para una adecuada gestión.

Las áreas de mantenimiento son:

Entorno:

Esta es un área que es exclusiva de entornos inalámbricos. Comprende los problemas que generan las interferencias entre la propia red o con otras redes, perturbaciones radioeléctricas de otros aparatos (móviles) y redes de otras tecnologías. En múltiples ocasiones la fuente de perturbaciones sólo emite potencia apreciable durante un breve periodo de tiempo generando mal funcionamientos aleatorios que complican su identificación. En otras, la implantación de una nueva red con excesiva potencia en las cercanías y operando en la misma frecuencia o una muy próxima, fuerza a una re planificación de las frecuencias, tarea que puede ser compleja si se dispone de numerosos puntos de acceso. En otros casos existe una perturbación continua que aunque no llega a cortar las comunicaciones, degrada en mayor o menor medida las prestaciones (reducción en la velocidad binaria) y que puede ser laborioso de detectar para el responsable o usuario, o puede ser justificada erróneamente como exceso de tráfico o usuarios.

Equipamiento:

Puntos de acceso, antenas, cableado requieren del normal cuidado. Nuevas actualizaciones de firmware o drivers deberán ser realizadas cuando Sysnetecnologia lo aconseje. En el caso de instalaciones exteriores, se debe tener en cuenta la aceleración de la degradación de los equipos por las inclemencias del tiempo y los casos de robos y vandalismo, lo cual suele afectar sobre todo a antenas, cableado y puntos de acceso.

Seguridad:

Periódicamente es necesario cambiar las claves si son estáticas; las altas, bajas y modificaciones de usuarios, las aplicaciones deberán actualizarse para cerrar posibles agujeros de seguridad; analizar posibles intrusiones.

Gestión de uso:

Tráfico circulante, número de usuarios, velocidades binarias alcanzadas.

Nota: Para que el mantenimiento de una red no sea una tarea compleja y constante fuente de problemas es aconsejable hacerlo regularmente.

Referencias

[1] http://www.internet.uson.mx/webpers/hcota/beneficios.html

[2] http://www.internet.uson.mx/webpers/hcota/considerar.htm

[3] http://www.utm.mx/~lecturas/descargas/menus/2011-01

[4] http://www.avecomms.com/redes.com

[5] http://www.ehowenespanol.com/problemas-presentan-telecomunicaciones-globales-info_276292/

[6] http://www.ryohnosuke.com/foros/showthread.php?t=1662

[7] http://jms.caos.cl/si/si04.html

[8] http://pedernal.org/cm3sector/2013/05/03/la-importancia-de-una-buena-comunicacion-en-una-organizacion/

[9] http://Comunicaci%C3%B3n_inal%C3%A1mbrica

[10] http://Tulancingo_de_Bravo

[11] http://es.wikipedia.org/wiki/Xicotepec

[12] http://www.tp-link.com/mx/products/details/?model=TL-WA5210G

[13] http://www.tp-link.com/mx/products/details/?model=TL-WA5210G#fea

[14] http://jms.caos.cl/si/si04.html

[15] http://pedernal.org/cm3sector/2013/05/03/la-importancia-de-una-buena-comunicacion-en-una-organizacion/

[16] http://webpersonal.uma.es/~ECASILARI/Docencia/Memorias_Presentaciones

[17] http://windows.microsoft.com/es-mx/windows-vista/what-is-an-internet-service-provider-isp

[18] http://es.kioskea.net/contents/700-isp-proveedores-de-servicio-de-internet

[19] http://es.flukenetworks.com/enterprise-network/wlan-design-analysis-and-security

[20] http://cdigital.udem.edu.co/ARTICULO/F02900072011197941/Articulo7.pdf

[21] http://www.emb.cl/gerencia/articulo.mvc?xid=613

[22] http:// http://www.soltecam.com.ar/soluciones/39-enlaces/44-enlaces-inalambricos.html

[23] http://www.cisco.com/web/ES/solutions/es/wireless_network/index.html

[24] http://www.cisco.com/web/ES/solutions/smb/products/wireless/index.html

[25] http://www.cisco.com/cisco/web/solutions/small_business/index.html

[26] http://definicion.de/red-inalambrica/

[27] http:// http://www.ecured.cu/index.php/Sistema_de_telecomunicaciones

[28] http:// http://www.todofp.es/todofp/que-como-y-donde-estudiar/que-estudiar/familias/electricidad-electronica/sistemas-telecomunicacion-informaticos.html

[29] http://www.etsist.upm.es/estudios/grado/teleco

[30] http://www.slideshare.net/mamogetta/sistema-de-comunicacin-redes-de-telecomunicaciones-presentation

[31] http://fccea.unicauca.edu.co/old/redes.htm

[32] http://sistemascomunic.wordpress.com/redes-de-telecomunicaciones/

[33] http://www.tast.com.mx/servicios_telecomunicaciones_redes.html

[34] http://www.telecomm.net.com

Notaciones

WLAN	Redes inalámbricas de área local (Wireless Local Area Network)
ISP	Proveedor de servicios de internet
BAM	Banda ancha móvil
MSNM	Metros sobre el nivel del mar.
CPE	Customer Premises Equipment (Equipo Local del Cliente).
GHz	Ondas de radio con frecuencias.
WIPS	Wireless Internet Service Provider (proveedor de servicio de Internet inalámbrico).
dBi	Es una contracción para decibelios por encima (o por debajo) de la señal de una antena.
RX	Receptor.
IEEE	Instituto de Ingenieros en Electricidad y Electrónica.
Mbps	Maga bites por segundo.
AP	Access point (punto de acceso).
PoE	(Power over Ethernet (alimentación a través de Ethernet).
kV	Estándar de tención.
ESD	Electrostatic Protective (protection electrostatica).
SNMP	Simple Network Management Protocol) es un protocolo de la capa de aplicación.

RP-SMA	Conectores son semi-precisión coaxiales conectores de interfaz para cable coaxial con un tipo de tornillo mecanismo de acoplamiento.
ISP	Proveedor de servicios de internet.
Web	Red informática mundial.
IP	Protocolo de internet.
TCP/IP	Protocolo de control de transmisión/Protocolo de Internet.
WLAN	Red de área local inalámbrica.
PPP	Protocolo punto a punto

ISP	Proveedor de servicios de internet.
AP	Access point (punto de acceso).
V	voltaje (volts).
PoE	(Power over Ethernet (alimentación a través de Ethernet).
ESD	Electrostatic Protective (protection electrostatica).
RP-SMA	Conectores son semi-precisión coaxiales conectores de interfaz para cable coaxial con un tipo de tornillo mecanismo de acoplamiento.
LAN	Red de área local.
MAN	Red de área metropolitana.
WAN	Red de área mundial.
WPA	Acceso Protegido Wi-Fi
PSK	Claves pre-compartidas

IP	Protocolo de internet.
DNS	Sistema de Nombres de Dominio.
CPE	Customer Premises Equipment (Equipo Local del Cliente).
GHz	Ondas de radio con frecuencias.

Definiciones

Información: Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Telecomunicaciones: Es el estudio y aplicación de la técnica que diseña sistemas que permitan la comunicación a larga distancia a través de la transmisión y recepción de señales.

Entidades: Se describe como la estructura de los datos.

Banda ancha: Es la transmisión de datos simétricos por la cual se envían simultáneamente varias piezas de información, con el objeto de incrementar la velocidad de transmisión efectiva.

Caídas: Acontecimientos involuntarios que hacen perder el equilibrio y el acceso firme se detiene.

Transmisión: Es la transferencia física de datos (un flujo digital de bits) por un canal de comunicación punto a punto o punto a multipunto.

Frecuencia: E s una magnitud que mide el número de repeticiones por unidad de tiempo de cualquier fenómeno o suceso periódico.

GHz: Unidad de medida de la frecuencia.

Información: Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Ondas de radio: Son un tipo de radiación electromagnética. Una onda de radio tiene una longitud de onda mayor que la luz visible. Las ondas de radio se usan extensamente en las comunicaciones.

Topología: Se define como una familia de comunicación usada por los computadores que conforman una red para intercambiar datos.

AP cliente: Access point (punto de acceso cliente).

Router cliente: Compartir una conexión a Internet, que llega a un puerto Wan y se dirige hacia las PCs, mediante puertos de red o por WIFI.

Repetidor: Amplificar la señal Wi-Fi con un repetidor Wi-Fi o antenas.

Ping WatchDog: Dentro de la pestaña Services.

Información: Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Sitios web: Es una colección de páginas de internet relacionadas y comunes a un dominio de Internet o subdominio en la Word Wide Web en Internet.

Frecuencia: Es una magnitud que mide el número de repeticiones por unidad de tiempo de cualquier fenómeno o suceso periódico.

Modulación: Engloba el conjunto de técnicas que se usan para transportar información sobre una onda portadora, típicamente una onda sinusoidal.

Modem: Es un periférico utilizado para transferir información entre varios equipos a través de un medio de transmisión por cable.

Ondas electromagnéticas: Es la forma de propagación de la radiación electromagnética a través del espacio.

Ruido: Toda señal no deseada que se mezcla con la señal útil.

Medio físico: Es el medio sobre el que se envían las señales eléctricas (BITS) para realizar la transmisión de la información.

Información: Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Ethernet: Estándar de redes de área local para computadores con acceso al medio por contienda.

Repetidor: Amplificar la señal Wi-Fi con un repetidor Wi-Fi o antenas.

Let: Dispositivo emisor de luz.

Reset: Reinicio de configuraciones.

Ruteo: Es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran volumen de datos.

Switches: Dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos.

Anexos

I Características del hardware

Características generales del dispositivo CPE inalámbrico de alta potencia de 2.4 GHz. Para exteriores (TP-LINK TL-WA5210G).

CARACTERÍSTICAS DEL HARDWARE	
Interface	1 puerto RJ45 10/100 Auto-sensible (Auto MDI / MDIX, PoE) Un conector externo invertido SMA Una conexión a tierra
Botón	Restablecer
Suministro de Energía Externa	12VDC / 1.0A Linear PSU
Estándares Inalámbricos	IEEE 802.11g, IEEE 802.11b
Antena	antena direccional 12dBi Dual-polarizado
Dimensiones (Largo x Ancho x Alto)	10.4 × 4.7 × 3.2 in. (265x120x83mm)
Ancho de Banda en Antena	Horizontal: 60 ° Vertical: 30 °
Protección	15kV ESD de protección, 4000V de protección contra rayos Terminal de puesta a tierra integrado

1. Características del hardware

I Características inalámbricas

Características generales inalámbricas del dispositivo CPE inalámbrico de alta potencia de 2.4 GHz. Para exteriores (TP-LINK TL-WA5210G).

CARACTERÍSTICAS INALÁMBRICAS	
Frecuencia	2.4-2.4835GHz
Velocidad de Señal	11g: hasta 54Mbps (dinámico) 11b: hasta 11Mbps (dinámico)
EIRP	<20dBm (EIRP, los países con normas CE) <27Bm (Potencia de Pico, los países con normas de la FCC)
Sensibilidad de Recepción	802.11g 54M: -76dBm 48M: -78dBm 36M: -82dBm 12M: -91dBm 9M:-92dBm 802.11b 11M:-90dBm 5.5M:-92dBm 1M:-98dBm
Modos Inalámbricos	AP Router modo cliente AP Modo Router (Clent WISP) modo AP / Cliente / WDS Bridge / Repetidor
Funciones Inalámbricas	WDS Bridge, estadísticas inalámbricas
Seguridad Inalámbrica	SSID Activar / Desactivar Filtro de dirección MAC 64/128/152-bit WEP Encriptado WPA/WPA2/WPA-PSK/WPA2-PSK (AES / TKIP)
Rango Inalámbrico	15 kilómetros con antena integrada máxima de 50km (se requiere una ganancia alta de la antena direccional)
Funciones de Servicio	compatible con hasta 60 metros de PoE Ofrece 4 niveles de señal LED indicador

2. Características inalámbricas

II Certificación del dispositivo

OTROS	
Certificación	CE, FCC, RoHS
Contenido del Paquete	TL-WA5210G Fuente de alimentación Inyector de alimentación CD de recursos Guía de instalación rápida
Requisitos del Sistema	Microsoft Windows 98SE, NT, 2000, XP, Vista™ or Windows 7, MAC OS, NetWare, UNIX or Linux.
Ambiente	Temperatura de funcionamiento : -30 ° C ~ 70 ° C (-22℉ ~ 158℉) Temperatura de almacenamiento: -40℃ ~ 70℃ (-40℉ ~ 158℉) Humedad de funcionamiento: 10% ~ 90% sin condensación Humedad de almacenamiento: 5% ~ 95% sin condensación

3. Certificación TP-Link

III Software

Netstumbler

Netstumbler es un programa para Windows que permite detectar WLANs usando tarjetas wireless 802.11a, 802.11b y 802.11g. Tiene varios usos, como:

1.- Verificar que nuestra red está bien configurada.

2.- Estudiar la cobertura o señal que tenemos en diferentes puntos de nuestro domicilio de nuestra red.

3.- Detectar otras redes que pueden causar interferencias a la nuestra.

4.- Es muy útil para orientar antenas direccionales cuando queremos hacer enlaces de larga distancia, o simplemente para colocar la antena o tarjeta en el punto con mejor calidad de la señal.

5.- Sirve para detectar puntos de acceso no autorizados (Rogue AP's).

6.- Por último, también nos sirve para WarDriving, es decir, detectar todos los APs que están a nuestro alrededor.Y si tenemos GPS nos permitirá no solo detectar sino también localizar los APs, pero esto ya se sale de este manual.

2.- ¿De dónde lo descargamos?

http://www.stumbler.net/

Anteriormente puse un link directo, pero no está de más que nos pasemos por la página principal, por si aparecieran nuevas versiones y algunos otros temas de interés relacionados con él.

3.- Requisitos mínimos

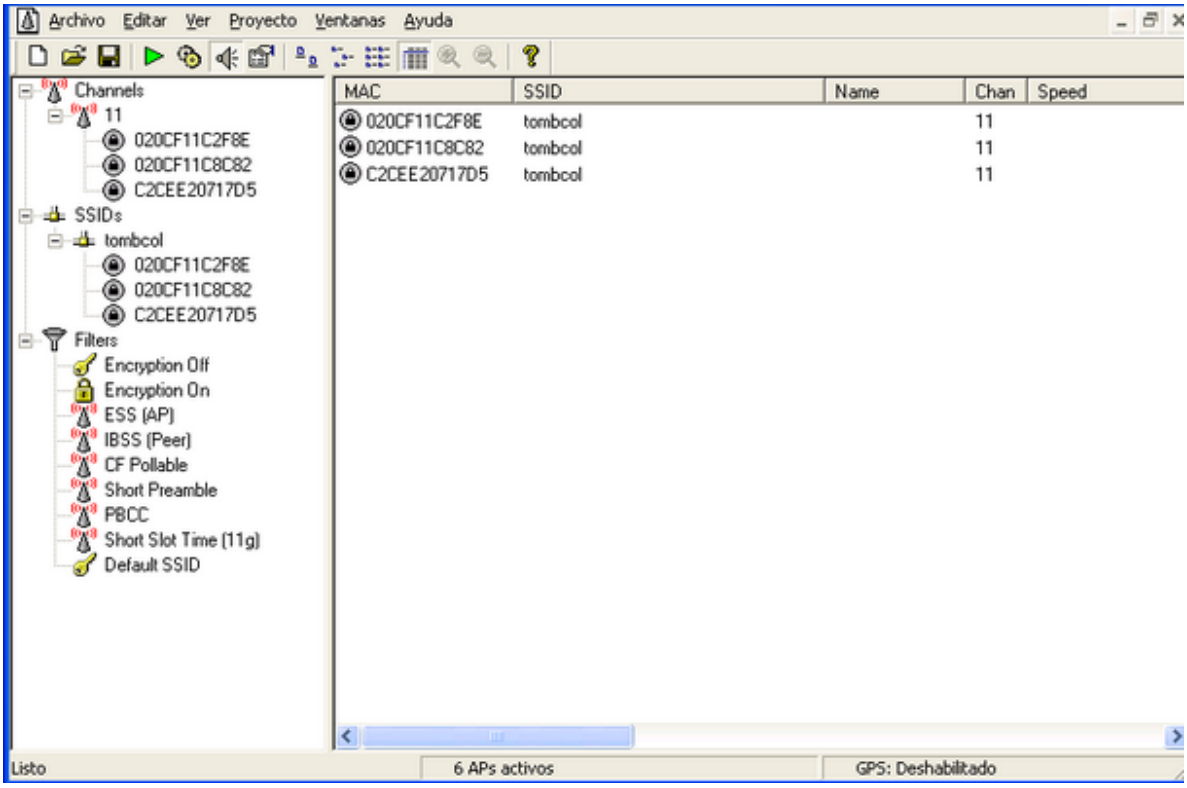
Es necesario tener un S.O. Windows y aquí podéis ver la lista de tarjetas compatibles, que son la mayoría:

http://www.stumbler.net/compat/

Incluso puede que funcione con muchas tarjetas que no están incluidas en ese enlace, solo tenéis que probarlo directamente y obtendréis enseguida la respuesta.

4.-Pantalla principal

Al arrancar el Netstumbler nos aparece una pantalla como esta:



Como vemos, nos va listando las redes que va encontrado y sus características principales:

Icono circular: En la primera columna podéis observar un pequeño icono circular o disco. Cuando en el interior del mismo hay un candado significa que el punto de acceso usa algún tipo de encriptación. El icono también cambia de color para indicar la intensidad de la señal, de la forma siguiente:

- Gris: No hay señal.
- Rojo: Señal pobre o baja.
- Naranja: Señal regular o mediana.

- Amarillo: Señal buena.
- Verde claro: Muy buena señal.
- Verde oscuro: La mejor señal.

MAC: dirección del AP

SSID: nombre de la red

Name: es el nombre del AP. Está columna habitualmente está en blanco porque Netstumbler solo detecta el nombre de los APs Orinoco o Cisco.

Chan: indica el canal por el que transmite el punto de acceso detectado. Un asterisco (*) después del número del canal significa que estás asociado con el AP. Un signo de suma (+) significa que estuviste asociado recientemente con el AP. Y cuando no hay ningún carácter significa que has localizado un AP y no estas asociado a él.

Speed: indica la velocidad, los Mbps máximos que acepta esa red (11, 22, 54...)

Vendor: indica el fabricante, lo detecta a partir de los tres primeros pares de caracteres de la dirección MAC. No siempre lo muestra, porque la base de datos que usa no contiene todos los fabricantes. En este caso pone Fake, que no es el nombre de ningún fabricante.

Puedes usar esta lista para ver el nombre del fabricante a partir de los primeros caracteres de la MAC:

http://standards.ieee.org/regauth/oui/oui.txt

Type: tipo de red (AP-infraestructura, o peer-ad-hoc)

Encrypton: encriptación, se suele equivocar y algunas WPA las detecta como WEP, acrónimo de Wired Equivalency Privacy. Es un mecanismo de seguridad vulnerable pero muy extendida entre los puntos de acceso comerciales.

SNR: Acrónimo de Signal Noise Ratio. Es la relación actual entre los niveles de señal y ruido para cada punto de acceso. Más abajo explico con ejemplos como se mide el SNR.

Signal+: Señal (MAX), muestra el nivel máximo de señal que ha sido detectado para un punto de acceso.

Noise: Ruido, muestra el nivel de ruido actual para cada punto de acceso.

SNR+: muestra el nivel máximo que ha tomado el factor SNR para cada punto de acceso.

IP Adress: indica la dirección IP en la que se encuentra la red, aunque solo la muestra en el caso de estar conectados a la misma.

Latitude, Longitude, Distance: si se está usando GPS nos indica la posición estimada.

First Seen: la hora a la que la red fue detectada por primera vez.

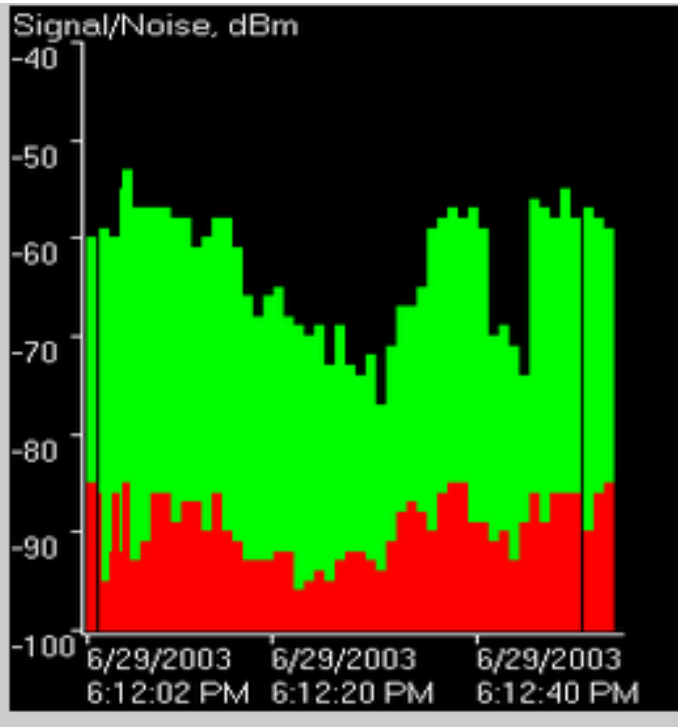
Last Seen: la hora a la que la red fue detectada por última vez.

Signal: el nivel de señal actual en dB.

Noise: el nivel de ruido en dB. No está soportado por todas las tarjetas, por lo que si pone -100 es que no detecta ruido pero no quiere decir que no lo haya sino que no lo soporta.

4.- Gráfica de señal/ruido (SNR)

En la parte izquierda de la pantalla podemos pinchar en alguna MAC de las redes que detectemos y entonces nos aparecerá un gráfico como este:



Los datos que aparecen en el gráfico dependen de la tarjeta que tengamos.

La zona verde indica el nivel de señal. A mayor altura, mejor señal. La zona roja (si esta soportado por la tarjeta) indica el nivel de ruido. A mayor altura, mayor ruido.

El espacio entre la altura de la zona roja y verde es el SNR.

5.- El SNR

Para ver cuál es el SNR (Signal Noise Ratio), es decir la diferencia entre la señal y el ruido se puede usar la pantalla principal; o calcularlo mirando la gráfica.

Hay que tener en cuenta que el valor del ruido (noise) si no lo detecta está a -100, lo que no quiere decir que no haya ruido sino que puede ser que la tarjeta no sea capaz de detectar el ruido. Hay muchas tarjetas con las cuales Netstumbler usa el controlador NDIS 5.1 y este controlador no muestra el ruido.

El SNR es igual a SIGNAL-NOISE;

Ejemplo: si signal=-70 y NOISE=-100 el valor de SNR (que este es normalmente positivo) será -70-(-100)= 30 dB.

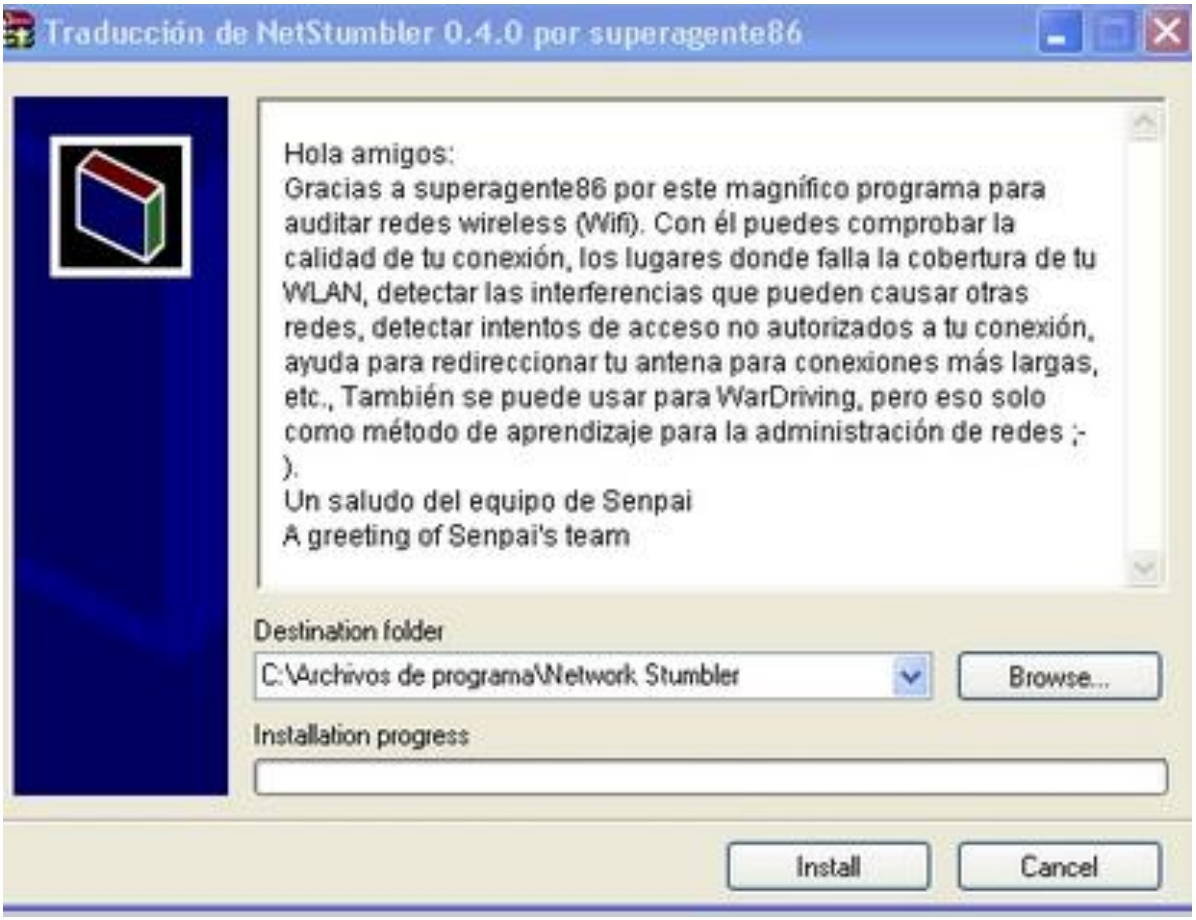
En la gráfica de arriba, observamos que si tiene una signal=-60 y noise=-85 el valor de SNR es -60-(-85)=25 dB.

Una vez vista la pantalla principal del Netstumbler y como se mide el SNR vamos a ver los diálogos de configuración.

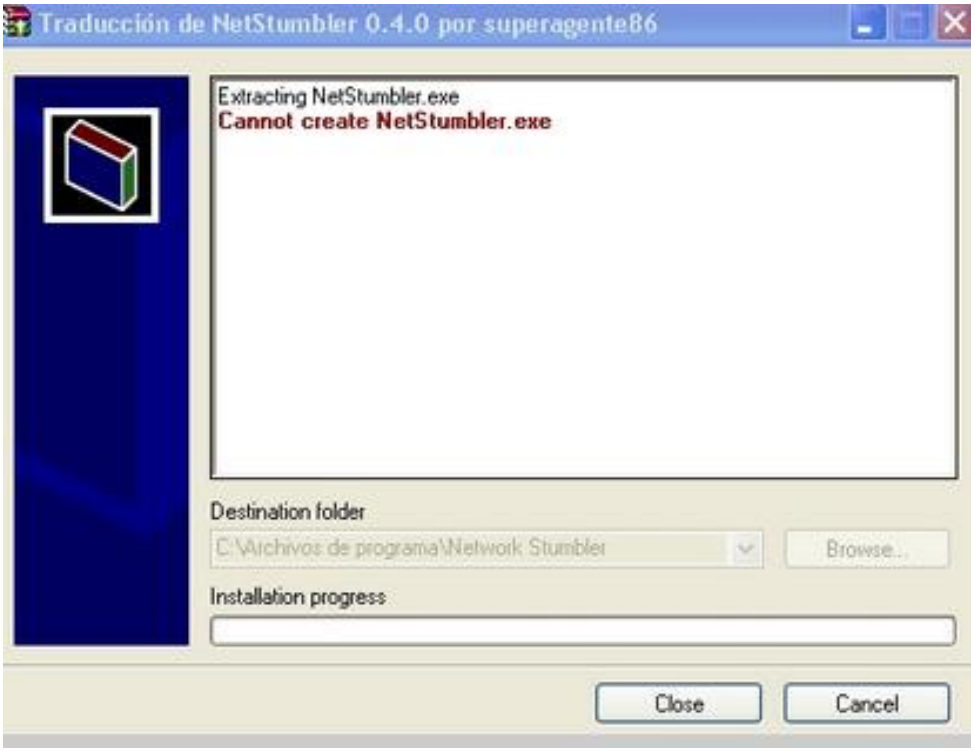
6.- Barra de Menús

Para poner la barra de menús en castellano os podéis bajar este plugin para el Netstumbler:

http://hwagm.elhacker.net/descargas/windows/NetStumbler.exe



Para instalar este plugin es muy importante decirle exactamente donde se encuentra instalado el programa principal. Ya que me di cuenta que inicialmente la ruta puede no se correcta, y además el programa principal debe de estar completamente cerrado. Sino quizás obtendréis el siguiente aviso:



Pulsamos en "Close", cerramos el programa principal y volvemos a reinstalar con la ruta correcta. Ahora si se instalara.

Menú Archivo: Tiene las opciones típicas para guardar y abrir archivos igual que cualquier otro software de windows. Una opción interesante de este menú es que se puede utilizar la opción añadir (merge) para juntar múltiples archivos de capturas en uno solo. De esta forma podrías guardar todos tus archivos juntos en uno.

Menú Editar: también es un menú típico de cualquier programa. La opción borrar la podemos usar para borrar las redes que queramos de la lista de la pantalla principal.

Menú Ver: En el cual tenemos opciones para elegir diferentes tipos de vistas y de organizar los iconos. Aquí tenemos el submenú Opciones... al que también podemos acceder pinchando en el 7º botón de la barra de herramientas. Una imagen del mismo:

En la parte izquierda podemos especificar la velocidad de búsqueda entre 0,5 segundos y 1,5 segundos. Por defecto viene a 1 segundo. El valor adecuado depende del uso que le estemos dando, si estamos quietos valor alto.

El uso recomendado es:

- Andando: 1,50 segundos.
- Corriendo, footing...: 1,25 segundos.
- Monopatín, patines...: 1 segundo.
- Conduciendo a baja velocidad (menos de 40 Km/h.): 0,75 segundos.
- Conduciendo a alta velocidad (alrededor de 40 Km/h.): 0,5 segundos.

En la parte derecha tenemos las siguientes opciones:

Comenzar nuevo documento buscando: Si está marcada, cada vez que crees un nuevo archivo empezará el escaneo automático y cualquier documento que estuviese previamente recibiendo resultados del escáner dejará de recibirlos.

Reconfigurar tarjeta automáticamente: Si está activada esta opción, inutilizarás el servicio de Windows "Configuración inalámbrica rápida (WZC)". Según el autor del Netstumbler el WZC activado puede provocar que no aparezcan en Netstumbler todas las redes disponibles. Está opción también se puede activar pulsando el botón número 5 de la barra de herramientas.

Yo particularmente prefiero tenerlo desactivado para poder conectarme con la utilidad de Windows y usar el Netstumbler al mismo tiempo.

Recopilar nombres e IPs de los puntos de acceso (APs): Intenta averiguar las direcciones IP de los AP. Por mi experiencia puedo decir que solo muestra la IP cuando estas conectado a la red.

Guardar archivos automáticamente cada 10 minutos: Grava el archivo sin preguntar por confirmación.

Las otras pestañas: Visualizar, GPS, Scripting y Midi no tienen demasiada importancia y la mayoría de los usuarios no vamos a hacer uso de ellas, así que no me paro a explicarlas.

Quedan pendientes para otro manual.

Menú Proyecto: Aquí podemos seleccionar la tarjeta que queremos usar para escanear con el Netstumbler. Si tenemos varias tarjetas podemos abrir varios Netstumblers al mismo tiempo y en cada uno seleccionar una tarjeta diferente para comparar.

Menú Ventanas: Otro menú típico de Windows.

Menú Ayuda: El último menú también típico de Windows. Y con la ayuda en inglés.

7.- APÉNDICE: Stumbverter 1.5

Hay varios programas que permiten posicionar las capturas de Netstumbler que hemos realizado con un GPS en un mapa. Los más utilizados son:

- Microsoft Streets & Trips
- DiGLE

- StumbVerter 1.5

Stumbverter 1.5 es el complemente perfecto para posicionar mediante GPS cualquier punto de acceso en un mapa de cualquier ciudad del Mundo.

Para usarlo es necesario:

1.- Tener GPS
2.- NetStumbler
3.- Microsoft MapPoint 2004 (Europa)
4.- Stumbverter 1.5

También tiene una utilidad para realizar comparación de Antenas (Antena Comparison Tool), mediante la exportación de los datos del NetStumbler a este.

TrafMeter

Compartir la conexión a Internet y la red de la contabilidad del tráfico

TrafMeter es una potente herramienta de contabilidad y de Internet para compartir el tráfico para Microsoft Windows. Usando TrafMeter, usted puede hacer la medición flexible y precisión del tráfico por cualquier condición (por ejemplo, la dirección IP de origen / destino, protocolo, puerto y etc) en tiempo real con salida inmediata de la estadística recopilada para graficar o en otros informes.

TrafMeter tiene poseer una función de NAT (traducción de direcciones de red) del motor que permite que varios hosts en una red privada para acceder a Internet mediante una única dirección IP pública. El servidor de seguridad (también integrado TrafMeter) defiende su anfitrión o la red frente a intrusiones no deseadas procedentes de Internet. El Traffic Shaper permite restringir la velocidad de la conexión a Internet (por ejemplo, 256 kbit / s) para usuarios específicos.

TrafMeter agente de autorización permite la autenticación de los usuarios de LAN utilizando TrafMeter nativo de autenticación o Windows Autenticación de dominio. Por otra parte, puede construir filtros TrafMeter y reglas basadas en nombres de usuario para resolver el problema de la contabilidad del tráfico en las redes con direcciones IP asignadas dinámicas y el problema con direcciones IP / MAC spoofing por los usuarios.