HERRAMIENTA DE LOCALIZACION DE REDES INALÁMBRICAS PARA GOOGLE MAPS

LAURA VANESSA BERRIO HERNANDEZ
MARIA FERNANDA RAMIREZ HAYEK

POLITÉCNICO GRANCOLOMBIANO INSTITUCIÓN UNIVERSITARIA
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
BOGOTÁ
2009

HERRAMIENTA DE LOCALIZACION DE REDES INALÁMBRICAS PARA GOOGLE MAPS

LAURA VANESSA BERRIO HERNANDEZ
MARIA FERNANDA RAMIREZ HAYEK

TRABAJO DE GRADO PARA OPTAR AL TÍTULO DE INGENIERO DE SISTEMAS

Asesor
Daniel A. Torres Falkonert
Ingeniero de Sistemas

POLITÉCNICO GRANCOLOMBIANO INSTITUCIÓN UNIVERSITARIA
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
BOGOTÁ
2009

Nota de aceptación

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Agradecimientos

El autor expresa su agradecimiento a:

Nuestras familias Berrío Hernández y Ramírez Hayek, por apoyarnos en todo el transcurso de nuestra carrera tanto moral, económica y académicamente para lograr esto.

Julián Meléndez y a Enrique Aranguren, personas especiales en nuestra vidas, por ayudarnos a nuestro crecimiento como personas, por darnos el apoyo y soportarnos en la realización de nuestros esfuerzos.

Mario Barrantes por el haber apoyado en el trabajo laboral a Laura Berrío en sus duros días de trasnocho.

Juan David Castañeda, por ser nuestro compañero y amigo en todo nuestra carreara, apoyándonos y haciéndonos la vida más feliz.

Daniel Torres por creer en nosotras, apoyarnos y asesorarnos para poder realizar esto.

Germán Ulloa por brindarnos su apoyo con el GPS.

Rafael García por brindarnos una mano cuando lo necesitamos y siempre guiándonos por el mejor camino.

Camilo Corena por creer en nosotras y siempre estar pendientes de nuestros esfuerzos, apoyándonos y dándonos los mejores consejos.

Todos nuestros compañeros de carrera cada persona que compartió con nosotros estos momentos de crecimiento personal y académico, dándonos una mano cuando los necesitábamos y aportándonos siempre algo bueno para nuestras vida.

GLOSARIO

GPS: Global Position System, ayuda a encontrar una posición geográfica por medio de satélites.

API: Aplication Programming Interface, Es una biblioteca que define una manera de invocar los diferentes servicios de un programa, cada programa tiene su propio API.

IEEE: Institute Of Electrical Engenieer, Es una asociación de profesionales, son los encargados de hacer los estándares para redes.

Wardriving: Es la técnica de buscar redes inalámbricas empleando un vehiculó en movimiento y utilizando un dispositivo móvil con antena Wi-fi, esto con el fin de detectar las redes.

RESUMEN

Este trabajo pretende generar una herramienta de escaneo la cual permite ejecutar una aplicación cliente en la cual se realiza la identificación de las redes inalámbricas que se encuentran al alcance, adicionalmente permite ejecutar una aplicación web en la cual se grafican o marcan las redes inalámbricas escaneadas y almacenadas. Para la realización de esta aplicación se conto con una investigación completa de la estructura y funcionamiento de las redes inalámbricas.

Dentro de este marco teórico se contemplan las definiciones y conceptos que se deben adquirir para interpretar la información arrojada por la aplicación y el funcionamiento de estas tecnologías.

Este documento plantea el desarrollo de una aplicación para el Escaneo de redes inalámbricas de forma geo-referenciada gracias a la ayuda de Google maps.

Adicionalmente se incluye la documentación básica de diseño de software que soporta la ejecución de la herramienta y un documento de pruebas que refleja una aplicación real del software, estas pruebas son conocidas como wardriving y es la forma capturar redes inalámbricas en un vehículo.

TABLA DE CONTENIDOS

LISTA DE TABLAS

TABLA DE FIGURAS

LISTA DE ANEXOS

1 JUSTIFICACION DEL PROYECTO

La necesidad de tener una conexión a internet es cada vez mayor, razón por la cual el auge de las redes inalámbricas día tras día aumenta. En la actualidad el crecimiento de estas redes es de forma exponencial, ya que constituyen un papel muy importante en la tecnología, la presencia de dispositivos inalámbricos aumenta, esta gran cantidad de dispositivos en el mercado ha forzado el uso de conexión inalámbrica en todo tipo de lugares como aeropuertos, centros comerciales, hoteles, centros médicos, etc.

Actualmente si se ubica en un sector sin importar cual puede encontrar cientos de redes inalámbricas, estas pueden ser de uso personal, públicas, privadas, seguras, inseguras entre otras. Si se desea conectar a alguna red se debe contar con la presencia de un dispositivo portátil y una red, adicionalmente se debe contar con la presencia de una herramienta que identifique las redes cercanas a las cuales podría tener acceso en el sector o zona en la cual se encuentra ubicado, de ahí la razón de satisfacer la necesidad de crear una instrumento que permita identificar todas las redes inalámbricas existentes de una manera más eficiente.

En consecuencia para lograr una conexión solo se debe contar con una red, una herramienta y un equipo, usted puede contar con un software de identificación de redes, pero funcionalmente es mas optima una que le proporcione una ubicación exacta sobre la red y detalles de esta misma. El problema de identificar las redes existentes en el sector donde se encuentra ubicado y el detalle, ubicación, de estas redes constituye un problema de investigación e implementación trivial por esta razón se ha decidido iniciar una investigación dentro del Politécnico Grancolombiano.

Sin embargo no solo existe la necesidad de contar con una herramienta que provea información de las redes si no que es necesario contar con herramientas que aporten a la academia y ofrezcan un valor agregado a las personas que dedican su tiempo a recolectar información para brindar estadísticas de servicios actuales, en este caso las redes inalámbricas. Este sistema de escaneo es ideal para técnicas como wardriving puesto que brinda la información típica que se busca en este tipo de prácticas, adicionalmente plasma la información sobre un mapa sin necesidad de marcar físicamente el lugar donde fue identificada la red.

En la actualidad más que recopilar información para realizar actos ilícitos, corruptos e inmorales existe la necesidad de crear campañas de concientización en las que se capacite a los usuarios, de los tipos de redes actuales, el impacto de tener redes inseguras, de los tipo de cifrado y autenticación que están en auge. La información arrojada por la herramienta aporta en esta necesidad actual.

2 DESCRIPCION DEL PROYECTO

Para implementar este proyecto es necesaria la investigación del funcionamiento básico de las redes inalámbricas con el objetivo de conocer detalles sobre este tipo de redes. Se debe contar con la ayuda de la herramienta google maps lo cual implica utilizar el API de google maps.
Google maps es útil puesto que permite representar y manipular datos geo-referenciados lo que significa que ofrece imágenes y detalles de mapas.

Se desarrolla una herramienta de escaneo de redes inalámbricas que permite graficar estas redes escaneadas sobre un mapa de google maps. Para capturar las redes se contara con dispositivos que permitan rastrear y capturar la señal de estas redes, además se debe contar con tecnología GPS (Global Position System) la cual permite arrojar la posición de cada una de estas redes.

2.1 ALCANCE DEL PROYECTO

Con base en investigaciones se pretende:

- Investigar el funcionamiento básico de las redes inalámbricas
- Investigar el funcionamiento del API de Google Maps
- realizar una integración de la información obtenida por medio de Google Maps y la recopilada por el software desarrollado.
- Desarrollar una herramienta que visualice sobre un mapa de google maps el nombre de las redes inalámbricas capturadas y su ubicación geográfica.
- inicialmente se recogerán datos en la ciudad de Bogotá sin limitar su funcionamiento en cualquier lugar del mundo.
- Los puntos de red que se van a identificar, van a ser capturados en tres tipos de zonas de la cuidad, Zona Residencial, Zona Comercial y Zona de negocios.

Para el desarrollo de lo anterior es claro que se debe contar con la presencia y el conocimiento de tecnología GPS y con dispositivo/s de captura de red.

2.2 OBJETIVO DEL PROYECTO

Satisfacer la necesidad de identificar y visualizar de forma dinámica las redes desde cualquier punto en el que se encuentre.

Utilizar y manipular la documentación (API) de google Maps que permite usar datos geo-referenciados.

Ofrecer un mapa que contenga un marcador con la ubicación y nombre de las redes inalámbricas identificadas. Se pretende facilitar a los usuarios la identificación de este tipo de conexión inalámbrica sobre un mapa global.

Además de brindar el nombre y posición geográfica de la red se pretende generar conciencia de las medidas de seguridad que deben tener en cuenta los usuarios demostrando la cantidad de redes inseguras encontradas en cada sector de la ciudad.

Finalmente con esta herramienta se pretende proveer un sistema de escaneo de redes inalámbricas que adicionalmente tiene la capacidad de graficar estas redes escaneadas sobre un mapa de google maps.

3 ESTADO DEL ARTE

Actualmente existe una cantidad razonable de herramientas de escaneo de redes, estas herramientas ofrecen diversas funcionalidades como, conexión automática a redes abiertas, identificación de la red más cercana, interfaz grafica que permite gestionar las redes y servicios de antivirus entre otros. Durante la búsqueda de sistemas similares que brinden estos mismos servicios, se identifico un sistema con servicios similares, la cual es una herramienta open source que permite escanear redes inalámbricas y las ubica en un mapa de Google Earth.

4 MARCO TEORICO

4.1 RED INALAMBRICA

Una red inalámbrica es un sistema de comunicación de datos que brinda conexión entre equipos situados en la misma área de cobertura. Este tipo de red presenta una gran diferencia y es el mecanismo de conexión, puesto que carece de cables; las redes inalámbricas transmiten y reciben datos a través de ondas electromagnéticas (radio e infrarrojo).
La transmisión de datos entre dos computadores se realiza por medio de un proceso llamado modulación de la portadora. Se tiene un aparato transmisor el cual agrega datos a una onda de radio (es decir la onda portadora). El receptor recibe esta onda, analiza la información y divide la información importante, este receptor debe estar ubicado en una frecuencia (frecuencia portadora).

Las redes inalámbricas son una extensión de las redes cableadas, ya que permiten un intercambio de datos transparente para los usuarios. Entre estos dos tipos de redes no existe una diferencia significativa, a excepción de la flexibilidad. La fácil instalación y flexibilidad que ofrecen este tipo de redes permiten estar presentes en entornos como, equipos de trabajo provisionales, entornos difíciles de cablear, hogares entre otros.

El inicio de las redes inalámbricas fue en el año 1979 en experimentos realizados por IBM, estos experimentos pretendían crear una red local utilizando infrarrojos. En mayo de 1985 el FCC (Federal Communications Commision) asignó bandas 902-928 MHz, 2.400-2.4835 GHz, 5.725-5.859 GHz al estudio científico y médico basadas en spread spectrum.

Desde 1985 hasta 1990 se trabajo en el desarrollo de estas redes inalámbricas. En mayo de 1991 se realizaron las primeras publicaciones con velocidades de 1 Mbps, el mínimo establecido por el IEEE 802 para que realmente se considere una WLAN. El crecimiento de estas redes inicialmente fue lento debido a la falta de estándares y los costos elevados. Sin embargo actualmente su crecimiento es exponencial.

4.1.1 Tipos de Red Según su Cobertura

1. WPAN (Wireless Personal Área Network) Red inalámbrica de ámbito personal este tipo de redes están diseñadas para cubrir un área del tamaño de una alcoba. Tiene la finalidad la conexión de equipos como teléfonos móviles, agendas, pda.
2. WLAN (Wireless Local Área Network) red inalámbrica de ámbito local y son el tipo de redes diseñadas para cubrir una casa u oficina.
3. WWAN (Wireless Wide Área Network) Red inalámbrica extensa cuyo ámbito cubre áreas como las de una ciudad.

4.1.2 IEEE 802.11

El estándar IEEE 802.11 fue creado con el objetivo de sustituir las capas físicas y de acceso del estándar IEEE 802.3 (Ethernet). La mayor diferencia que existe entre Ethernet y una red inalámbrica es el mecanismo de acceso a la red.
Existen tres tipos de redes inalámbricas, cada una está basada en un estándar 802.11X aprobadas por el Instituto de Ingenieros en Electricidad y Electrónica (IEEE).

En la actualidad los estándares con mayor aceptación son IEEE802.11b e IEEE802.11g debido a la banda de 2.4 GHz que está disponible en casi todo el mundo, con una velocidad de hasta 11 Mbps y 54 Mbps.

La familia IEEE 802 incluye especificaciones que son enfocadas sobre dos capas del modelo OSI: capa física y capa de enlace. La capa Mac es el conjunto de reglas que indican como acceder al medio y enviar datos, la capa física es la encargada de la transmisión y recepción.

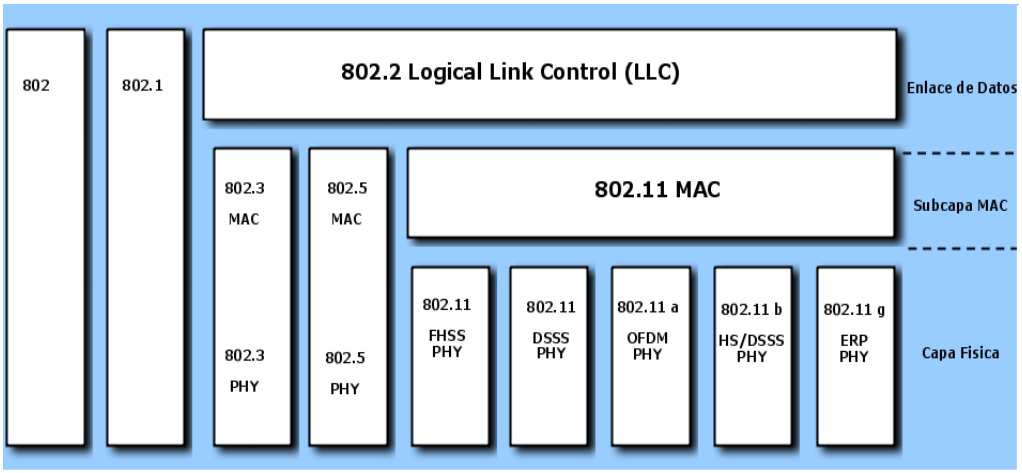


Ilustración 1. Arquitectura IEEE 802[1]

Las versiones siguientes al 802.11 han variado la capa física, 802.11b utiliza espectro ensanchado por secuencia directa de alta tasa (HR/DSSS), 802.11ª y 802.11g una capa física basada en la técnica de multiplicación por división de frecuencias ortogonales (OFDM).

[1]Tecnología Wi-Fi, Ing. Ricardo Alberto Andrade, Ing. Pablo Hernán Salas, Ing. Daniel Santos Paredes. 2008. pag. 13.

La capa física se divide en dos componentes: *Procedimiento de convergencia de la capa (PLCP)* que mapea las tramas MAC sobre el medio y *Physical Medium Dependent (PMD)* que transmite las tramas.

4.1.3 Estándares 802.11

- **IEEE 802.11:** Estándar para LANs inalámbricas (WLANs) en la banda de frecuencia de 2400 MHz a 2484 MHz. Este estándar se diferencia del estándar IEEE 802.3 en sus capas. Presenta tasas de transferencia de 1 y 2 Mbps y utiliza espectro ensanchado por secuencia directa (DSSS).
- **IEEE 802.11a:** Este estándar trabaja en las bandas de Frecuencias de 5 GHz. Utiliza Multiplicación por división de frecuencias ortogonales (OFDM).Ofrece mayor velocidad y menor interferencia.
- **IEEE 802.11b:** Soporta anchos de banda de hasta 11 Mbps, trabaja en la banda de los 2.4 GHz, presenta desventajas en su velocidad, sensibilidad a la interferencia. Este estándar tiene un bajo costo.
- **IEEE 802.11g:** Estándar que soporta anchos de banda de hasta 84 Mbps en la banda de 2.4 GHz. Tiene compatibilidad con el estándar 802.11b, pero es vulnerable a la interferencia de productos que trabajan en la misma banda.
- **IEEE 802.11h:** Estándar con la capacidad de seleccionar dinámicamente la frecuencia (DFS) y controlar la potencia de transmisión (TPC) con el objetivo de solucionar problemas derivados de la coexistencia, utilizadas en su mayoría en sistemas militares.
- **IEEE 802.11j:** Este estándar trabaja en las bandas de Frecuencias de 5 GHz. Tiene la capacidad de seleccionar dinámicamente la frecuencia (DFS) y controlar la potencia de transmisión (TPC) con el objetivo de solucionar problemas derivados de la coexistencia, utilizadas en su mayoría en sistemas militares.
- **IEEE 802.11n:** Estándar que trabaja en las bandas de frecuencia de 2.4GHz y de 5.8GHz.Utiliza la tecnología OFDM y la tecnología múltiples Entradas Múltiples Salidas (MIMO) con tasas de transferencia de hasta 600 Mbps.
- **IEEE 802.11e:** Incluye al estándar 802.11 factores de calidad de servicio (QoS) y así soportar tráfico en tiempo real en todo tipo de entornos.
- **IEEE 802.11i:** Añade a los estándar elementos de seguridad y encriptación. El estándar comprende los protocolos 802.1X, TKIP y AES. Se implementa WPA2.
- **IEEE 802.15:** Estándar para PANs (Personal Área Network en la banda de frecuencias de 2400 MHz a 2484 MHz. Utiliza espectro ensanchado por saltos de Frecuencia (FHSS) con tasas de transferencias del orden 2 Mbps. Este estándar es conocido como Bluetooth. Presenta interferencias con las redes Wi-Fi.

Norma	*Banda de Frecuencia*	*Modulación*	*Alcance*	*Velocidad Máxima*	*Nº max Canales sin Solap.*
802.11 b	*2.4 GHz*	*DSSS*	*Interiores:40-100m Exteriores:500 - 700m*	*11 Mbps*	*3*
802.11 a	*5 GHz*	*OFDM*	*Interiores:12-50m Exteriores:50-400m*	*54 Mbps*	*12*
801.11 g	*2.4 GHz*	*OFDM*	*Interiores:40-100m Exteriores:500-700m*	*54 Mbps*	*3*

Tabla 1 Estándares 802.11

4.2 ESTRUCTURA DE RED

4.2.1 Topología

Topología hace referencia al patrón de conexión que existe entre los nodos. La topología de red determina únicamente la configuración de las conexiones entre nodos. La distancia que existe entre los nodos, las tasas de transmisión y/o los tipos de señales no hacen parte de la topología de red, pero si pueden afectarse por esta. A la hora de seleccionar una topología se debe tener en cuenta, los costos de encaminamiento, costos entre otros.

Las redes pueden tomar formas diferentes dependiendo de su conexión con los otros nodos. Existen dos tipos de topologías:

- Topología Física: Configuración de cables, computadores, antenas entre otros dispositivos.
- Topología Lógica: Mecanismo de implementar una topología física, de forma eficiente.

4.2.1.1 Topologías de Red Básicas

- Bus o Barra: Los nodos se encuentran conectados a un cable común. Ejemplo: Las redes Ethernet.
- Estrella: Los nodos son conectados directamente a un concentrador central y todos los nodos deben atravesar este concentrador antes de alcanzar el destino.

- Línea: Conjunto de nodos conectados en línea. Cada nodo es conectado a sus dos nodos vecinos excepto el nodo final.
- Anillo: Todos los nodos están conectados entre sí formando un circulo, así cada nodo se conecta a otros dos dispositivos.
- Malla Completa: Existen enlace directo entre todos los nodos de la red.
- Malla Parcial: Ciertos nodos están organizados en una malla completa, pero otros nodos se conectan solo a uno o dos nodos de la red.

Las topologías que aplican en las redes inalámbricas son:

- Estrella: Este tipo de topologías es estándar en las redes inalámbricas.
- Línea: Las líneas de dos puntos se conocen como enlaces Punto a Punto.
- Árbol: Esta topología es utilizada por los Proveedores de Servicios de Internet (ISP).
- Malla Parcial

4.3 ARQUITECTURA

Las redes están compuestas por cuatro elementos:

- **Estaciones**
  Las estaciones son equipos de computación con interfaces de redes inalámbricas, es decir son cualquier dispositivo electrónico que permita interpretar el estándar 802.11.

- **Punto de Acceso (AP)**
  Dispositivo que permite la interconexión entre los dispositivos inalámbricos y las redes. Los puntos de acceso son quienes proveen un cable virtual entre los asociados. Este “cable” conecta a los redes entre ellos y a los clientes con la red cableada. Este tipo de dispositivos puede capturar señales de enrutadores y clientes, ampliándolas para brindar un mayor alcance a la red. Sin embargo los puntos de acceso deben ser transparentes para los dispositivos de la red, es necesario asignarles una dirección IP que permita realizar su configuración.

  Los clientes deben conectarse a los puntos de acceso a través de su nombre. Este mecanismo se conoce como Identificador del Conjunto de Servicio (SSID) y debe ser igual para todos los miembros de una red inalámbrica. Adicionalmente, todos estos puntos de acceso y clientes pertenecen a un mismo Conjunto de Servicios Extendidos (ESS) y deben ser configurados con el mismo ID (ESSID).

- **Medio inalámbrico**
  La transmisión de datos se debe realizar a través de un medio inalámbrico, entre estos se encuentran las señales de radio y las emisiones infrarrojo.

- **Sistema de Distribución**
  Los puntos de acceso (AP), deben ser conectados a sistemas de distribución que permiten un área de cobertura superior. Significa que ofrece mayor movilidad. Todos los puntos de acceso que se encuentren en un sistema de distribución inalámbrico deben ser configurados de tal forma que utilicen el mismo canal de radio.

  El Sistema de distribución puede realizar funciones de puente y de punto de acceso pero reduce la velocidad de transferencia a la mitad.

4.4 TIPOS DE RED

4.4.1 Peer to Peer

Este esquema también es conocido como redes ad-hoc, permiten la visibilidad entre equipos inalámbricos a través de señales de radio sin utilizar un punto de acceso.

Las redes Peer to Peer presentan la configuración más simple, solo es necesario contar con terminales que incluyan adaptadores de redes inalámbricas. En este tipo de redes solo es necesario usar el mismo canal de radio y un identificador, llamado SSID en “Modo ad-Hoc”.

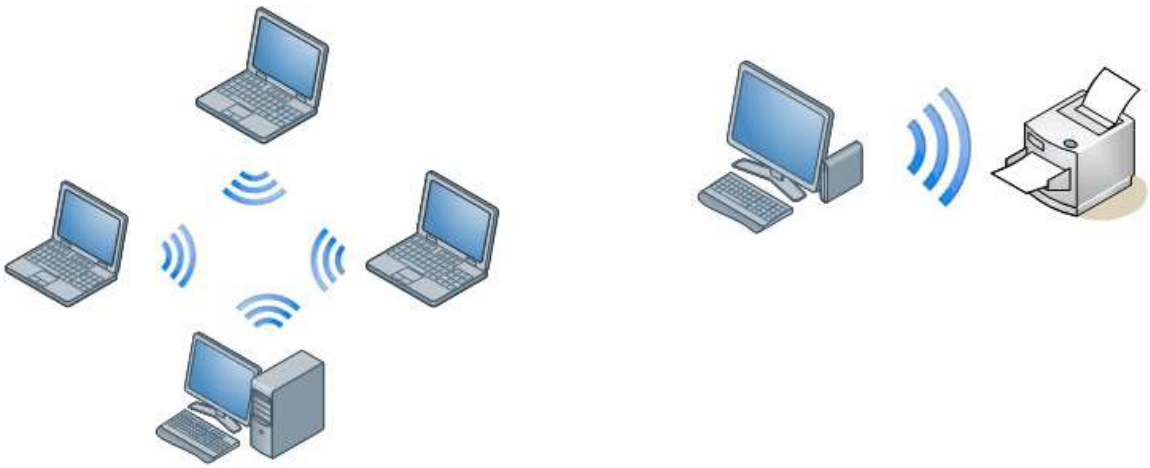


Ilustración 2. Peer to Peer

4.5 PUNTO DE ACCESO

Los puntos de acceso son “Concentradores inalámbricos”, su principal función es la de conectar dispositivos inalámbricos con dispositivos que utilizan cables. En este tipo de redes los computadores que tiene conexión inalámbrica pueden tener acceso a los mismos servicios que los computadores conectados a través de cables.

En este tipo de red se debe contar con una unidad base que se pueda conectar a los equipos sin cable y adicionalmente una tarjeta de red típica. Cabe aclarar, que a diferencia de las redes peer to peer, los equipos inalámbricos no se hablan entre sí, lo hacen a través de la unidad base que ofrece mayor seguridad y conectividad con los equipos conectados a la red cableada.

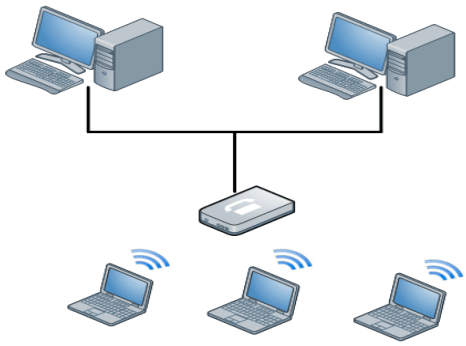


Ilustración 3. Punto de Acceso

Los puntos de acceso se ubican en lugares altos con el objetivo de brindar mayor cobertura a los equipos que soporta. Un único punto de acceso soporta un pequeño grupo de usuarios en un rango entre treinta y cien metros.

4.6 ROAMING

Si el área que se desea cubrir es muy amplia, se utiliza este tipo de redes y así permitir a los usuarios desplazarse entre las diferentes áreas de cobertura sin sufrir interrupciones en la conexión, una de las características más interesantes de las redes inalámbricas. Esta facilidad es conocida como itinerancia o roaming.

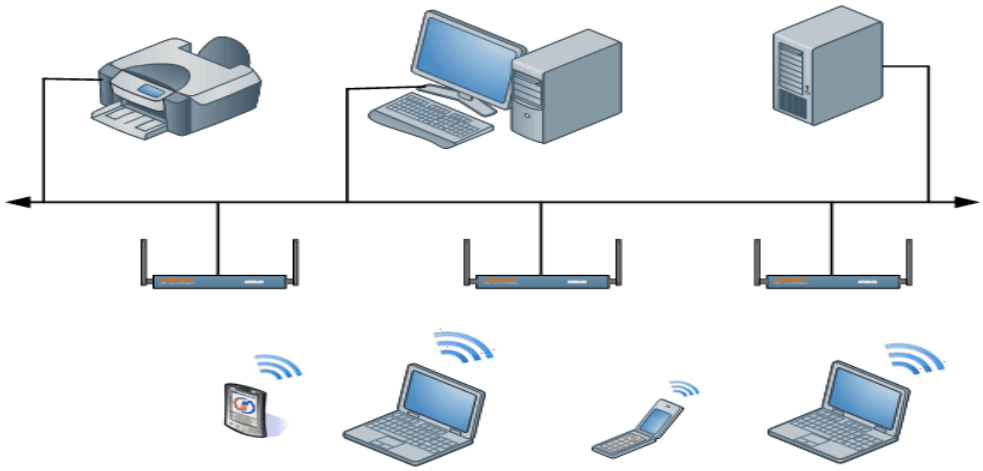


Ilustración 4. Roaming

4.6.1 Servicios De red

Hay un conjunto de servicios que deben existir para la capa MAC, estos servicios se dividen en dos categorías SS (Station Service) y DSS (Distribution System Service).

4.6.1.1 Servicios de Estación (SS)

Grupo de servicios que soportan el transporte de MSDUs (MAC Service Data Unit) dentro de un BSS.

Servicios:

- **Autenticación:** Es uno de los servicios más importantes debido a que está basado en la seguridad de una red inalámbrica. Este servicio es utilizado para la identificación y autorización de las redes inalámbricas y no tiene un esquema predeterminado.

- Desautenticación: Este servicio finaliza una autenticación que tenga la red inalámbrica. Caso contrario a la autenticación.

- Privacidad: Servicio que ayuda a mantener la confidencialidad de los datos, con el objetivo de evitar que estaciones que no sean autorizadas accedan a WLAN, para esto este servicio se hace uso de WEP (Wired Equivalent Privacy) que implementa la privacidad.

- Entrega de MSDU: Servicio que indica que se quiere entregar paquetes fragmentados desde la capa LLC hasta la capa Física.

4.6.1.2 Servicio de Sistema de Distribución (DSS)

Este grupo de servicios se utilizan para superar limitaciones lógicas, las cuales son ofrecidas por el medio y el espacio de direcciones, se presenta cuando una estación sale y entra del área de cobertura.

Servicios:

-**Asociación:** Servicio que asegura que la petición sea reconocida por un punto de acceso, para ser o no aceptada por este. Se realiza para cada petición a un único punto de acceso.

-**Disociación:** Servicio que termina una Asociación de una estación.

-**Reasociación:** Servicio que permite que las estaciones cambien el punto de acceso por otro, cuando esto ocurre el sistema de distribución es actualizado.

-**Distribución:** Servicio que indica que una petición ya fue aceptada por un punto de acceso. Se utiliza un sistema de distribución con el fin de enviar al destino. Es usado para poder tener comunicación con las diferentes estaciones.

-**integración:** Servicio que le permite a redes que no tengan estándar IEEE 802.22 trasferir información con otra que si tenga este estándar.

4.7 CAPA DE ACCESO AL MEDIO (MAC)

La subcapa Mac se encuentra en la parte inferior de la capa de enlace de datos y se define como una de las capas más importantes del estándar 802.11. Cabe señalar que esta subcapa MAC varía dependiendo de la capa física (Ej: Ethernet, WLAN). Esta subcapa se puede describir como la manera de llevar una tarjeta de red a un medio físico, o tener una manera de acceder al medio físico por medio de una red inalámbrica utilizando un intercambio de datos. Esta subcapa puede actuar de forma distribuida, significa que todas las estaciones cooperan para poder determinar quién y cuándo debe acceder a la red.

Entre las funciones que realiza esta subcapa se encuentran:

- Controlar el acceso al medio físico
- Controlar la transmisión de datos del usuario al medio inalámbrico.
- Controlar sincronización y algoritmos de distribución

- Eliminar tramas duplicadas o erróneas
- Detectar y corregir errores de transmisión

4.7.1 Problemas y Retos de la capa Mac

Calidad del enlace de radio: La frecuencia en un enlace de radio presenta ruido, interferencias y adicionalmente no tiene licencia, por esta razón no se debe asumir que las tramas que son enviadas fueron recibidas por los destinatarios; la propagación de las ondas puede ocasionar la perdida de la recepción de las ondas.

Por estas razones es necesario tener tramas que confirmen la recepción de cada uno de los datos enviados. Todas las tramas que son enviadas tienen que ser reconocidas, si no es así son consideradas perdidas y se procede a reenviar la trama de nuevo.

Nodo Oculto: A diferencia de las redes cableadas, las redes inalámbricas tienen los límites menos definidos, razón por la cual en cierto momento una estación puede estar por fuera del alcance de otra, de forma que no se pueden comunicar. El problema se puede observar en la Ilustración 5. problema nodo oculto: La estación 1 y estación 3 no pueden comunicarse entre sí, las dos estaciones pueden transmitir al mismo tiempo, lo que genera una colisión que no es detectada por estas estaciones, pues la colisión se produce en la estación 2.
Con el objetivo de evitar esto el 802.11 implementa un sistema de Request to Send (RST) y su respuesta Clear to Send (CTS) que permite que las estaciones usen señales de requerimiento y aceptación para el envío de datos. De esta forma un nodo puede cerciorarse que otro está listo para recibir tramas.

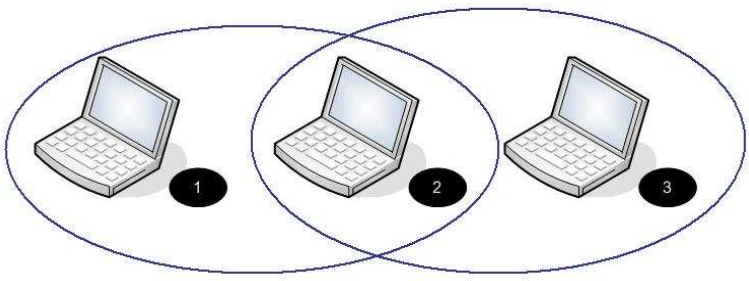


Ilustración 5. Problema Nodo Oculto[2]

[2] Tecnología Wi-Fi, Ing. Ricardo Alberto Andrade, Ing. Pablo Hernán Salas, Ing. Daniel Santos Paredes. 2008. Pág. 27.

El proceso de transmisión de datos se puede observar en la Ilustración 6, solución nodo oculto: La estación 1 va a transmitir una trama, significa que debe iniciar el proceso enviando una trama RTS. Al llegar la estación destino este responde con una trama CTS produciendo silencio en las otras estaciones vecinas. Luego la trama CTS es enviada por la estación 1 y la estación 2 luego de recibirla envía una trama de ACK.

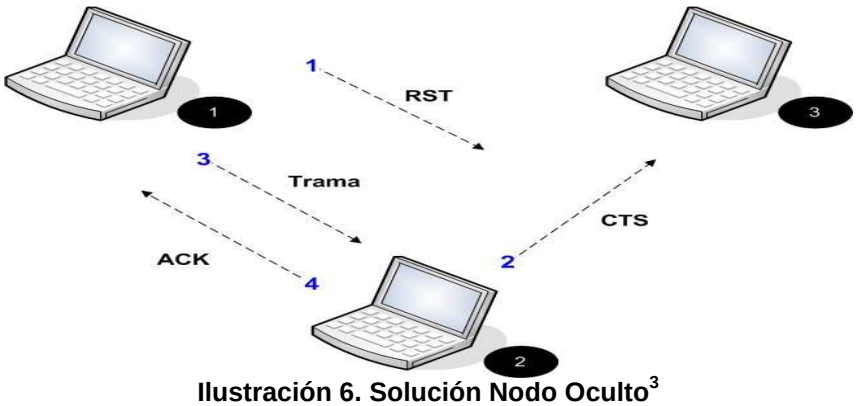


Ilustración 6. Solución Nodo Oculto[3]

4.7.2 Mecanismos de Acceso MAC

El acceso al medio es controlado por funciones de coordinación. De la misma forma que Ethernet, el acceso CSMA/AC es administrado por la *Función de Coordinación Distribuida* (DCF) y adicionalmente se encuentra la *Función Punto de Coordinación (PFC)* el cual es soportado por el servicio DCF. *Ver Ilustración 7. Arquitectura capa MAC.*

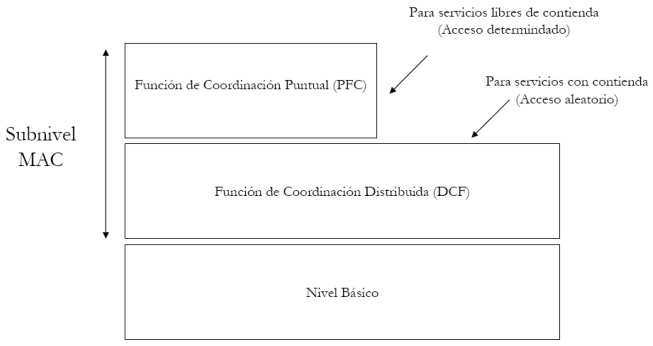


Ilustración 7. Arquitectura Capa MAC[4]

[3] Tecnología Wi-Fi, Ing. Ricardo Alberto Andrade, Ing. Pablo Hernán Salas, Ing. Daniel Santos Paredes. 2008. Pág. 28.

4.7.2.1 Función de Coordinación Distribuida (DCF)

El método de acceso más importante de 820.11 es esta función DCF también conocida como el mecanismo de acceso básico del estándar *Acceso Múltiple por Censado de Portadora con Colisión Evitable* (CSMA/CA).

Es claro que el medio por el que viajan las redes inalámbricas es bastante ruidoso, debido a las interferencias de otros dispositivos en la frecuencia incluyendo su propio ruido. Por esta razón la necesidad de tener una confirmación de la recepción de una trama a través del ACK. Si el emisor no recibe el ACK en un determinado intervalo se considera que la trama se ha perdido y es enviada de nuevo.

El estándar 802.11 diseñó un parámetro denominado *ACK Timeout,* es el tiempo que el emisor espera antes de considerar una trama perdida.

Una estación antes de realizar la transmisión debe censar el medio para identificar si otra estación se encuentra transmitiendo. Si el medio está ocupado aplazará la transmisión, hasta que el medio esté libre.

Si el medio se encuentra libre, luego de haber aplazado la transmisión o después de una transmisión exitosa, el protocolo CSMA/CA establece técnicas para evitar las colisiones. Una de las técnicas que utiliza es la definir la duración de los tiempos entre tramas, denominados **IFS**.

IFS: Esta técnica pretende asignar prioridades en el instante que se accede al medio dependiendo del tipo de trama y del modo de coordinación en el que se está trabajando (DCF o PCF).

El modo de enviar una trama por el protocolo CSMA/CA, es el siguiente:

1. Prueba si el estado del canal está ocupado o libre.
2. Si el canal esta libre este espera un tiempo, este tiempo se le llama espacio entre tramas distribuido (DIFS).
3. Luego de esto se envía una trama, la cual va hacer la solicitud de trasmisión (RTS).
4. Ahora el destino recibe la trama y espera un tiempo, este tiempo es llamado espacio corto entre tramas (SIFS) y envía una contestación.
5. Si la contestación es afirmativa, el origen espera un tiempo SIFS, y con esto transmite una trama de datos (DATA).

---

[4] WLAN Red Inalámbrica de Área Local [En línea]. Disponible en: http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/valle_i_lf/capitulo1.pdf. Pág.6.

6. Si lo datos llegaron correctamente al destino, este tiene que esperar un tiempo SIFS y enviar una confirmación positiva (ACK).
7. Si sucede lo contrario a lo anterior entonces enviaría una confirmación negativa (NAK).si sucede esto el origen trataran de enviarlo de nuevo.
8. Se repite el proceso varias veces.

4.7.2.2 Función Punto de Coordinación (PFC)

La PFC brinda servicios libres de contienda. Existen estaciones especiales llamadas PC (Point Coordinators) que aseguran que el canal es entregado sin contienda. Estas estaciones se encuentran ubicadas en los Puntos de Acceso (AP), lo que significa que el servicio está disponible en redes de tipo infraestructura. Con el objetivo de brindar un beneficio adicional, PFC permite a las estaciones transmitir después de un intervalo de tiempo corto, pero este benefició depende del Computador.

Los periodos libres de contienda se alternan en periodos y los computadores son los encargados de alternar dichos periodos. El PCF transmite información en los frames llamados Beacon al principio del periodo, esta trama contiene la duración máxima del periodo, CFMaxDuration; Estos Beacon obtienen el control del medio estableciendo un NAV (Network Allocation Vector).

Después de acceder al medio, el AP crea una lista que incluyen las estaciones que desean transmitir, estas estaciones deben demostrar que pueden mantener la comunicación con el AP y deben realizar una solicitud a través de una trama específica.

La norma 802.22 no estableció este tipo de acceso obligatorio, por esta razón existe una gran mayoría de APs comerciales que no tienen incluida esta función.

4.7.3 Tipos de Tramas

- *Tramas de Control:* Las tramas de control son utilizadas para el control de acceso al medio (Ejemplo: RST,ACK,CTS)
- *Tramas de Datos:* La trama de datos es usada para la transmisión de datos.
- *Tramas de Gestión:* La trama de Gestión es transmitida para intercambiar información de transmisión (Ejemplo: Beacon).

4.7.3.1 Formato de Trama

Ilustración 8. Formato de Trama

Cada tipo de trama está compuesta de la siguiente forma:
Preámbulo (96 bits de sincronización):

- Synch: Este campo contiene una secuencia de bits (unos y ceros) que son usados para lograr sincronización del receptor, la selección de antena y corregir el desvió de frecuencia del receptor.
- SFD: Bits que permiten la delimitación del inicio de trama.

PLCP Header: Encabezado que contiene información importante para el proceso de decodificación en el nivel físico.

- PLCP Signaling Field (PSF): Contiene la velocidad de la información.
- PLCP PDU Length (PLW): Contiene el número de bytes contenidos en el paquete. Es utilizado por la capa física para identificar el fin del paquete.
- Header Error Check Field (HEC): Campo que utiliza un código de redundancia con el objetivo de detectar errores en el PLCP Header.

MAC Data: Campo que contiene información del nivel de enlace.

4.7.3.2 Trama MAC

Ilustración 9.Trama MAC

Control de Trama: Indica el inicio de la trama y está compuesto por 2 bytes:

- *Versión de Protocolo:* Este campo de 2 bits indica la versión de 802.11 MAC que se encuentra en la trama. La primera versión tiene valor 0.
- *Tipo:* Campo de 2 bits que indica el tipo de trama que puede ser: gestión, control o datos.

- *Subtipo:* Este campo de 4 bits asociados al tipo indican cada una de las acciones de las tramas (Por Ejemplo: Asociación, autenticación, RST, ACK…).
- *A DS:* Campo de 1 bit que indica si el frame desea reenviarse usando un AP. Si una estación envía una trama a un punto de acceso este campo se establece en 1.
- *De DS:* Campo de 1 bit que indica que el mensaje fue enviado usando un AP. ES decir, si los campos *A DS y De DS en 0, la comunicación viaja entre dos estaciones (modo ad hoc)*
- *Más Fragmentación:* Campo que indica si hacen falta fragmentos por transmitir. Todos los fragmentos excepto el último contienen este bit en 1.
- *Reintento:* Campo que indica si una trama fue retransmitida, de esta forma ayuda a la estación receptora a eliminar tramas duplicadas.
- *Control Potencia:* Con el objetivo de conservar la vida de batería, ciertos dispositivos eliminan la energización a la interface de red. Las estaciones pueden estar en modo de ahorro de energía o activos.
- *Más Datos:* El AP utiliza este bit, en modo de ahorro de energía, con el objetivo de indicar a una estación que existen tramas adicionales en espera.
- *Seguridad:* Campo que indica si la trama está protegida por un protocolo de seguridad de la capa de datos.
- *Orden:* Indica si las tramas y fragmentos van a ser transmitidas en un orden especifico.

Duración / ID: Este campo puede tener dos significados diferentes:

- El Id de la estación para el mensaje (ahorro de energía).
- Duración del canal de transmisión.

Direcciones: Las tramas pueden contener hasta 4 direcciones dependiendo de los bits definidos en el campo de control:

- Dirección 1: Dirección del receptor. Si él *A DS* se encuentra activado entonces esta dirección es del AP y desactivado es la dirección de la estación.
- Dirección 2: Dirección del transmisor. Si *De DS* se encuentra activado es la dirección del AP y desactivado es la dirección de la estación.
- Dirección 3: Contiene la dirección de la fuente de origen si tiene una trama De DS. Si la trama tiene A DS corresponde a la dirección de destino.
- Dirección 4: Este campo de dirección es utilizado cuando las tramas son trasmitidas desde un AP a otro.

Control de Secuencias: Campo que representa el orden de los diferentes fragmentos dentro de una misma trama. Está compuesto por el número de

fragmentos y numero de secuencia, quienes identifican la trama y le numero de fragmento de la trama.

Cuerpo Trama: Campo que contiene la información

FCS: Campo contenido en un CRC (Control de redundancia cíclica) que permite la detección de errores en la trama.

4.8 CAPA FISICA

La capa física del estándar 802.11 define diferentes técnicas de transmisión, las cuales fueron publicadas en 1997:

- Espectro Ensanchado por Salto de Frecuencia (FHSS)
- Espectro Ensanchado por Secuencia Directa (DSSS)
- Infrarrojo (IR)

Durante el avance de las redes fueron desarrolladas otras capas basadas en tecnologías de radio:

- 802.11a:Multiplexación por División de Frecuencias Ortogonales (OFDM)
- 802.11b:Espectro Ensanchado por Secuencia Directa de Alta Tasa (HR/DSSS)
- 802.11g:Multiplexación por División de Frecuencias Ortogonales (OFDM)

En 1985 el FCC (Federal Communications Comission), la Agencia Federal del Gobierno de Estados Unidos encargado de regular y administrar el tema de telecomunicaciones asigno las bandas IMS (Industrial Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en espectro ensanchado. Existen dos tipos de tecnologías que usan radiofrecuencia, banda ancha y banda estrecha, la tecnología de espectro ensanchado usa todo el ancho de banda disponible

4.8.1 Espectro Ensanchado por Salto de Frecuencia (FHSS)

Esta tecnología de espectro ensanchado tiene como objetivo transmitir una porción de información a través de una frecuencia determinada durante un intervalo corto de tiempo, pasado este tiempo se salta a una frecuencia diferente y se sigue trasmitiendo a otra frecuencia. Significa que cada tramo es transmitido en una frecuencia distinta durante un tiempo corto.
El grupo de posibles frecuencias se llaman “hopset”. Cada banda de frecuencias asignadas se divide en sub-bandas de menor frecuencia llamadas canales, cada canal está definido como una región espectral con una frecuencia central en el “hopset” con un tamaño de ancho de banda igual y suficiente para incluir la mayor cantidad de energía en una ráfaga de modulación de banda estrecha (FSK).

Los saltos de frecuencia son determinados por una secuencia aleatoria almacenada en tablas. Si dos comunicaciones distintas usan diferentes frecuencias en un mismo instante de tiempo la tecnología FHSS permite tener más de un punto de acceso en la misma zona geográfica sin interrupciones.
Aunque se cambia de canal físico y la sincronización en los saltos de frecuencia se mantiene, a nivel lógico permanece un solo canal por el que se realiza la comunicación.

4.8.1.1 Modulación

El estándar IEEE 802.11 define esta tecnología FHSS mediante la modulación de frecuencia FSK (Frequency Shift Keying), con velocidades de 1Mbps hasta 2Mbps. El rango de frecuencias empleadas en la banda de 2,4 GHz es:

Límite Inferior	**Limite Superior**	**Rango regulatorio**	**Área geográfica**
2.402 GHZ	2.480 GHz	2.400- 2.4835 GHz	América del Norte
2.402 GHZ	2.480 GHz	2.400- 2.4835 GHz	Europa
2.473 GHZ	2.495 GHz	2.471- 2.497 GHz	Japón
2.447 GHZ	2.473 GHz	2.445- 2.475 GHz	España
2.448 GHZ	2.482 GHz	2.4465- 2.4835 GHz	Francia

Tabla 2 Rango de Frecuencias Empleadas en FHSS

El tiempo máximo en una frecuencia es de 400 ms cada 30 segundos.
La banda de 2.4 GHz se organiza en 79 canales con un ancho de banda de 1 MHz sin superposición.

4.8.2 Espectro Ensanchado por Secuencia Directa (DSSS)

Técnica de espectro ensanchado por secuencia directa (DSSS) consiste en modular la señal a transmitir con una secuencia de bits de alta velocidad, conocidos como chips y Secuencia de Barker, código de dispersión o ruido pseudoaleatorio (código PN) del cual resulta una expansión de la señal.

La señal transmitida se amplia y su potencia disminuye considerablemente, de esta forma se tiene una señal menos sensible al ruido puesto que la interferencia solo afecta a algunos bits de la señal original. Para recuperar la señal original el receptor debe conocer el código de ruido utilizado.

El ancho de la Banda Típica es de 22 MHz, siendo la canalización cada 5 MHz (desde el canal 1, centrado en 2412 MHz, hasta el canal 13, centrado en 2472 MHz). Únicamente Japón usa el Canal 14, centrado en 2484 MHz.

IEEE 820.11 utiliza espectro ensanchado por secuencia directa (DSSS) y tiene tasas de transferencia de 1 y 2 Mbps, a diferencia de IEEE 802.11b, que utiliza espectro ensanchado por secuencia directa de alta tasa (HR/DSSS) con tasas de transferencia de 5,5 y 11 Mbps.

4.8.3 Infrarrojos

Los infrarrojos son ondas electromagnéticas que se propagan en línea rectal esos sistemas infrarrojos se ubican en altas frecuencias, bajo el rango de las frecuencias de la luz visible. Por esta razón las propiedades de los infrarrojos son las mismas que tiene la luz visible. Esta tecnología es susceptible de ser interrumpida por cuerpos opacos pero se permite reflejarse en ciertas superficies.
Las velocidades de transmisión que existen en esta tecnología son:

- 1 y 2 Mbps infrarrojos en modulación Directa.
- Mbps a través de infrarrojos portadora modulada.
- 10 Mbps Infrarrojos con modulación de múltiples portadoras.

4.8.3.1 Clasificación

De acuerdo al Angulo de apertura con que se emite la información en el transmisor, los sistemas infrarrojos tienen diferentes clasificaciones:

- Sistema infrarrojo de corta apertura: Están compuestos por un cono de infrarrojo direccional, funciona de manera similar a los controles de televisión, el emisor debe orientar hacia el receptor antes de transferir información. Esta tecnología es un poco complicada utilizarla, pues se debe tener muy presente la orientación del dispositivo.La tecnología de infrarrojos es considerada como un sistema inalámbrico pero no móvil y es útil en enlaces punto a punto.
- Sistemas de gran apertura: No es necesario que el emisor y el receptor estén sincronizados. La dispersión que se utiliza en este tipo de red permite rebotar en techos y paredes, generando un efecto de interferencia en el receptor. Por esta razón la velocidad de transmisión disminuye.

La tecnología de infrarrojo es importante en la implementación de WLANs por presentar características como:

- Amplio ancho de banda
- Longitud de onda cercana a la luz
- Fuerte resistencia a las interferencias electromagnéticas (Ejemplo: motores, luces, etc.)

- No se requiere autorización especial de algún país para transmitir con laser o diodos.
- Utiliza un protocolo simple y de bajo consumo de potencia.

Las limitaciones que se encuentran en esta tecnología son:

- Sensibilidad a objetos móviles que interfieren en la comunicación entre el emisor y receptor.
- Restricción en la potencia de transmisión
- Sensibilidad a la luz directa, lámparas y en general a fuentes de luz brillantes.
- Transmisiones de datos bajas.

La capa física de esta tecnología es la encargada de gestionar el establecimiento, mantenimiento y finalización del enlace entre los dos equipos. Su funcionamiento es simple: el emisor emite luz que se propaga en el espacio, el receptor recibe los impulsos de luz y los convierte en señales eléctricas.
Algunos dispositivos con tecnología infrarroja son:

- Impresoras
- Teléfonos Celulares
- Palms
- Mouse
- Teclados

4.9 PROTOCOLOS CRIPTOGRAFICOS

4.9.1. WEP: WIRED EQUIVALENT PRIVACY

WEP es un algoritmo que hace parte del estándar 802.11 y fue creado con el objetivo de proteger la información transmitida en una red inalámbrica. El protocolo WEP se basa en dos componentes que permiten cifrar las tramas de la red, el algoritmo de cifrado RC4 y el algoritmo de chequeo de integridad CRC.

El algoritmo de cifrado WEP se aplica sobre la capa MAC. Inicialmente se genera una semilla. La semilla está formada por una clave y un vector de inicialización, la clave es generada manualmente y la debe tener el receptor y emisor; el vector de inicialización de 24 bits es generado de forma aleatoria.

Una vez generada la semilla, se forma una cadena de longitud igual al payload del frame. Este proceso se lleva a cabo a través de un algoritmo de cifrado llamado RC4.Por ultimo se combina la clave de cifrado (keystream) y el payload a través de una XOR.

Origen								Destino				
Datos				*Keystream*		*Cipher Stream*		*Keystream*				*Datos*
0				1		1		1				0
1				1		0		1				1
0	←	XOR	→	1	→	1	→	1	→	XOR	→	0
1				0		1		0				1
1				0		1		0				1
0				1		1		1				0

Ilustración 10. Operación de Cifrado

Uno de los grandes problemas en la implementación de este algoritmo es el tamaño de los vectores de iniciación. Estos vectores de iniciación pueden ser identificados a través de las tramas que pasan por los puntos de acceso.

El vector de inicialización (IV) presenta problemas de seguridad, el estándar 802.11 no especifica el manejo de este vector de inicialización. La única indicación que se proporciona es la de realizar un cambio del IV en cada trama, indicación que permite a los fabricantes modificar el vector de inicialización de diversas formas.
Dado que no existe una restricción fuerte sobre la frecuencia de los vectores de inicialización, es posible que estos se repitan en corto tiempo. La cantidad de veces que se repite un vector de inicialización depende de la implementación de los fabricantes y la carga de la red.
El protocolo WEP es inseguro pues permite identificar fácilmente el vector de inicialización lo cual permite deducir la clave total.WEP es un protocolo que no presenta autenticación de usuarios, lo que significa que es un protocolo que no brinda autenticación y no cumple con unos de los objetivos más importantes.

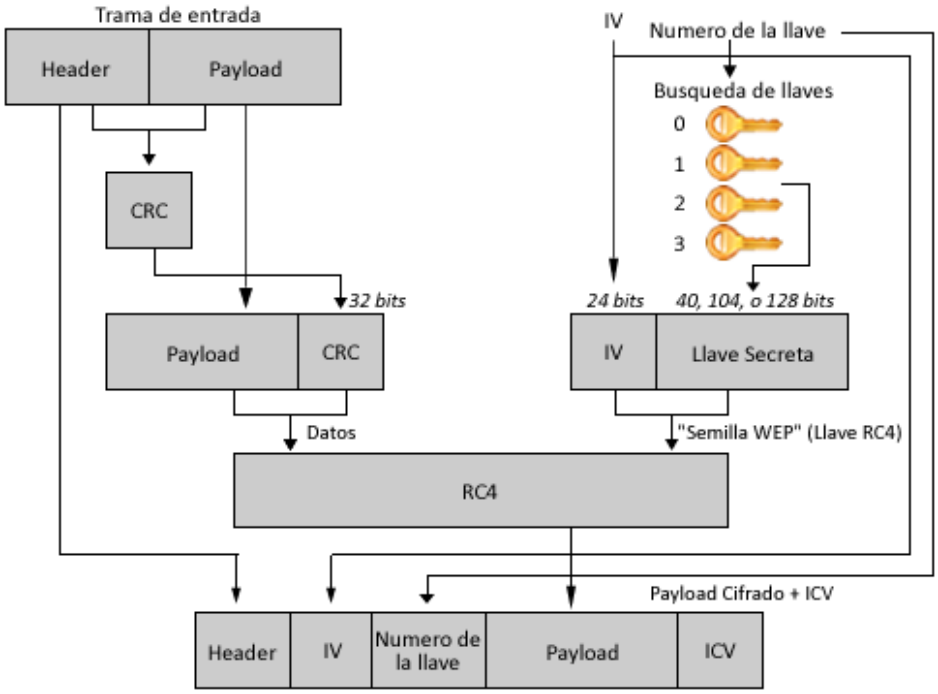


Ilustración 11. Funcionamiento WEP

Durante un estudio realizado por el ISAAC (Internet Security, Aplicación, Autenticación) se concluyo que las principales debilidades del protocolo WEP son:

- Repetición de las claves
- Fácil obtención de la claves a través del trafico
- Autenticación en la red sin clave
- Longitud de claves
- Algoritmos de cifrado vulnerables

4.9.1.1. Algoritmo RC4

El algoritmo RC4 fue creado por Ron Rivest en 1987.Este algoritmo es conocido como ARCFOUR y hace parte de WEP y WAP.
RC4 es un generador de número aleatorios inicializados con una llave privada superior a los 256 bytes. El algoritmo es bastante sencillo pues básicamente su función es generar una clave de flujo y cifrar el flujo ejecutando un XOR. Utiliza 256 bytes de memoria para cada uno de los estados del arreglo, n bytes de memoria para la llave y variables enteras.
El algoritmo está compuesto por dos partes, la inicialización de la llave (KSA) y el cifrado y descifrado. Debido a la sencillez y funcionamiento de este algoritmo se presentan las siguientes debilidades:

- La clave secreta se puede recuperar
- Los bytes del keystream dependen de algunos bits de las clave
- El numero de la clave se puede deducir si 3 elementos no se modifican

4.9.1.2. Algoritmo de chequeo CRC

El algoritmo de chequeo CRC permite verificar la integridad de los datos de trasmisión, de acuerdo al estándar IEEE-802.
La información que envia a través de una red se puede asegurar utilizando sumas de verificación (checksums).Es posible validar un archivo y su valor luego de ser enviado. Si las sumas de verificación son iguales significa que el archivo no fue modificado.
Los códigos de redundancia cíclica (CRC) son necesarios para calcular las sumas de verificación y la detección de errores en grandes secuencias de datos. Estos CRC están basados en el uso de polinomios generados G(x) de grado r y n bits de datos binarios que representan los coeficientes de polinomio de orden n-1.A cada uno de estos bits se les debe añadir r bits de redundancia y así obtener un polinomio divisible por el polinomio generador. El receptor debe verificar si el polinomio recibido es divisible por G(x), si no lo es, significa que hubo un error en la transmisión.

WEP utiliza el CRC32 para verificar la integridad de la información, la suma de verificación que resulta del CRC32 es conocido con ICV

4.9.1.3. Ataque de fuerza bruta

Es posible obtener la semilla de 32 bits que utiliza el PRNG (Generador de números pseudoaleatorios de WEP) a partir de la contraseña. Si la contraseña contiene caracteres ASCII el bit más alto de cada carácter es cero. Si se realiza un XOR de los bits también resulta un cero lo cual reduce la entropía de la fuente. De 32 bits que utiliza la semilla solo se desde el 16 al 13 bits. El LGC de modulo 2^32 genera que los bits más bajos sean “menos aleatorios” que los más altos, significa que, el bit 0 tiene longitud del ciclo de 2^1, 2^2, 2^3 etc. La longitud total de clico es 2^24.
Por esta razón solo es necesario considerar las semillas desde 00:00:00:00 hasta 00:7F:7F:7F significa que entropía total queda reducida a 21 bits. Este tipo de datos proporciona la posibilidad de realizar un ataque de fuerza bruta reducida a 21 bits. Principalmente se puede observar que con este tipo de conocimiento es posible utilizar un directorio para genera las semillas que aparecen el diccionario y de esta manera si las contraseña está incluida en el diccionario, reducir el tiempo necesario para identificar la contraseña es menor.

4.9.2. WPA (Acceso Protegido de Fidelidad inalámbrica)

WAP es un protocolo desarrollado con el objetivo de eliminar las vulnerabilidades del WEP. Este protocolo está diseñado para ser compatible con dispositivos 802.11, incluyendo 802.11b, 802.11a y 802.11g.
En este nuevo estándar se propone un nuevo protocolo de cifrado, llamado TKIP (Temporary Key Intregrity Protocol), protocolo encargado de realizar el intercambio de llaves entre un punto de acceso y el cliente. El protocolo TKIP utiliza el algoritmo RC4 para encriptar y el CRC antes de transmitir, pero utilizan IB de 48 bits lo que disminuye significativamente la posibilidad de romper la encriptación.

Automáticamente WPA genera llaves de encriptación únicas, lo cual evita la repetición de claves como sucedía en WEP. El protocolo WPA implementa el MIC (Message Integrity Code) Código de Integridad del mensaje con el cual se evita que se le logre la modificación de ICV, por esta razón el MIC de 8 bytes es utilizado en la comprobación de la integridad de los mensajes antes del ICV.

WPA en el proceso de autenticación utiliza una serie de sistemas abierto y 802.11x.El cliente es autenticado con el punto de acceso, el cual autoriza el envió de paquetes. El protocolo WPA procede a realizar la autenticación del cliente haciendo uso de 801.1x, sin embargo sirve de interfaz para un servidor de autenticación como RADIUS o LDAP, si no se dispone de un servidor de autenticación, es posible utilizar PSK. Una vez se ha verificado la autenticidad del usuario, el servidor de autenticación crea un par de claves maestras (PMK) que se distribuyen mediante los algoritmos de encriptación YKIP o AES con los que se protege el trafico entre el cliente y el punto de acceso.

WPA tiene dos funcionalidades: autenticación y encriptación de datos. La autenticación la realiza haciendo uso de 802.1x/ EAP o PSK y la encriptación utilizando el algoritmo TKIP, específicamente AES. Los puntos de acceso compatibles con WPA pueden ser:

- Modalidad red empresarial: En este caso el punto de acceso utiliza un servidor RADIUS y 802.11X y EAP para la autenticación. El servidor RADIUS asigna las claves compartidas para cifrar los datos.
- Modalidad red casera o PSK: Esta modalidad es implementada cuando no se dispone de un servidor RADIUS. Por esta razón es necesario asignar una contraseña compartida en el punto de acceso y los dispositivos móviles. De esta forma solo se puede acceder si la contraseña del punto de acceso y el dispositivo coincide. Luego de obtener el acceso, TKIP es quien asegura el acceso.

Cabe destacar que WPA sigue siendo vulnerable a ataques de denegación de servicio, el envió de paquetes consecutivos en un mismo intervalo de tiempo utilizando una clave errónea, el punto de acceso elimina todas las conexiones de los usuarios.

WAP implementa un código de integridad del mensaje conocido como “Michel” e incluye protección contra ataques de repetición.
El estándar WPA fue liberado en abril de 2003 y empezó a ser obligatorio para todos los miembros de Wi-fi a partir finales de 2003. Todo equipo de red inalámbrica que contenga el sello “Wi-Fi Certified” podrá ser actualizado para cumplir con las especificaciones de WPA.
La versión mejorada es (WPA2) y está basada en el estándar 802.11 (802.11x, TKIP y AES).

4.9.3. WPA2

En Junio de 2004 fue entregada la edición final de este estándar WPA2. El estándar fue creado con el principal objetivo de mejorar las deficiencias de WEP y WPA, como la separación de la autenticación de usuario de la integridad y privacidad de los mensajes, brindando una arquitectura robusta y escalable .La arquitectura de las redes inalámbricas es llamada Robust Security Network (RSN) y utiliza autenticación 802.1X, distribución de claves robustas y mecanismos de integridad y privacidad.
RSN brinda seguridad, escalabilidad y una red transicional de seguridad (TSN), permitiendo a un usuario actualizar su equipo. Si el proceso de autenticación o asociación utiliza 4-way handshake, la asociación recibe el nombre de RSNA *(Robust Security Network Association).*

Un contexto seguro de comunicación consta de cuatro fases:

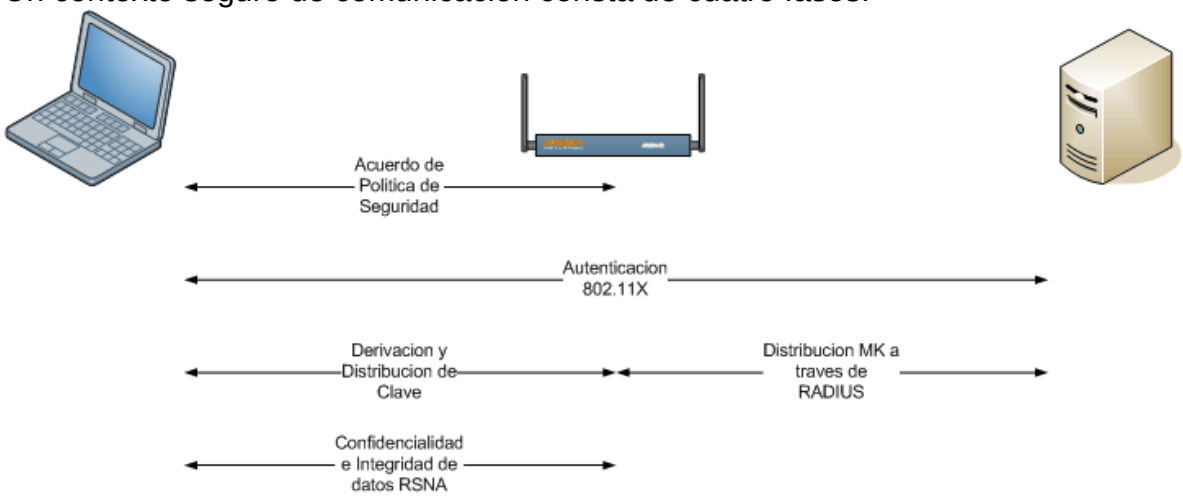


Ilustración 12. Fases WPA2

Fase 1:
Durante esta fase los participantes deben estar de acuerdo sobre la política de seguridad a utilizar. La política de seguridad se envía en el campo RSN IE *(Information Element)* y describe:

- Métodos de autenticación soportados (802.1X, PSK)
- Protocolos de seguridad (CCMP,TKIP)

- Soporte para la pre-autenticación

Fase 2:
La segunda fase hace pertenece a la autenticación 802.1X basada en EAP y el método específico como: EAP/TLS, EAP/TTLS o PEAP. Esta autenticación se inicia en el instante que el punto de acceso solicita los datos de identidad al cliente y la respuesta del cliente incluye algún método de autenticación especifico.

Fase 3:
Durante la fase 3 se realiza la generación y el intercambio de calves. Durante la derivación de la clave, se producen dos handshakes:

- *4-Way Handshake* para la derivación de la PTK (Pairwise Transient Key) y GTK (Gropu Trasient Key).
- *Group Key Handshake* para la renovación de GTK

Este *4-Way Handshake*, permite:

- Confirmar que el cliente conoce la PMK
- Generar una nueva PTK
- Instalar claves de cifrado e integridad
- Cifrar el transporte de la GTK
- Confirmar la selección de la suite de cifrado

Fase 4:
Las claves generadas en la fase 3 son utilizadas en protocolos que soportan la confidencialidad e integridad de datos RSNA:

- TKIP (Temporal Key Hash)
- CCMP
- WRAP

4.9.4. TKIP (Temporal Key Integrity Protocol)

Este protocolo pretende resolver las debilidades del algoritmo WEP y la compatibilidad con el hardware utilizando el firmware.
El protocolo está compuesto así:

- Un código de integración de mensajes (MIC), encripta el checksum y las direcciones físicas (MAC) de origen, destino y datos en texto claro de la trama 802.11.
- Contramedidas que minimizan la probabilidad de ser atacados.
- Un IV (vector de Inicialización) de 48 bits llamado TSC (TKIP Sequence Counter) que previenen ataques por repetición.

La estructura de encriptación TKIP propuesta por 802.11i es la siguiente:

Ilustración 13. Estructura TKIP

El uso del TSC amplia la vida útil de la llave temporal y elimina la recodificación de la llave temporal. Es posible intercambiar 2^48 paquetes utilizando una sola llave temporal antes de utilizarse de nuevo. El proceso de encapsulación TKIP es el siguiente:

- La llave temporal, la dirección del emisor y el TSC se combina en dos fases para así obtener una llave de 128 bits por paquete, dividido en una llave RC4 de 104 bits y en una IV de 24 bits para la próxima encapsulación WEP.
- El MIC final es calculado sobre la dirección física origen, destino y el MSDU después de ser segmentado por la llave MIC y el TSC. La función MIC utiliza una función hash unidireccional.
- El TSC es examinado con el objetivo de identificar que el paquete recibido tiene valor TSC mayor que el anterior. Luego de ser calculado el valor del MIC basado en MSDU recibido y desencriptado, el valor calculado del MIC es comparado con el valor recibido.

4.9.5. 802.1X

802.1X es una adaptación del framework EAP (Extensible Authentication Protocol) que pertenece a la capa de enlace. En vez de especificar como autenticar a los usuarios, EAP permite a los diseñadores del protocolo construir sus propios *métodos EAP*, estos son subprotocolos que realizan las transacciones de autenticación. EAP es usado para seleccionar un mecanismo específico de autenticación luego de que el autenticador solicita información para determinar el mecanismo específico que usar. En ver de actualizar al autenticador con nuevos mecanismos de autenticación a medida que aparecen, EAP permite el uso de un servidor de autenticación que puede implementar los métodos de autenticación, de esta forma el autenticador funciona como un puerto de entrada para todos los métodos disponibles. Esto permite que los métodos EAP usen diferentes métodos para autenticar a los usuarios dependiendo de los requerimientos de una situación particular.

4.9.5.1. EAP

EAP es una encapsulación que puede funcionar sobre cualquier capa de enlace y usar cualquier método de autenticación disponible, a pesar de que se ha usado en su mayoría sobre enlaces PPP. La siguiente Ilustración muestra la arquitectura básica de EAP.

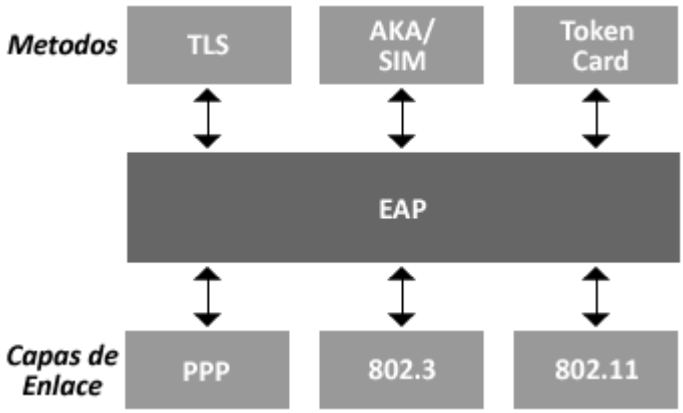


Ilustración 14. Arquitectura EAP

9.4.5.1.1. Paquete EAP

Un paquete EAP está compuesto por los siguientes campos:

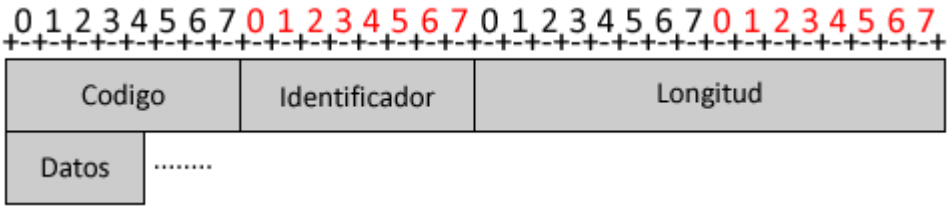


Ilustración 15.Paquete EAP

1. Código
   Es de un byte de largo e identifica el tipo de paquete EAP, los códigos están definidos de la siguiente forma:
   - Request
     Un paquete de tipo *request* es enviado por el autenticador al punto. Cada solicitud tiene un tipo asociado que indica que tipo de información se está solicitando. Cualquier paquete de tipo *request* adicional deberá ser enviado luego de haber recibido el paquete *response* correspondiente, o de que se reciba en mensaje de error de una capa inferior.

     El formato de un paquete de tipo *request* se muestra a continuación:

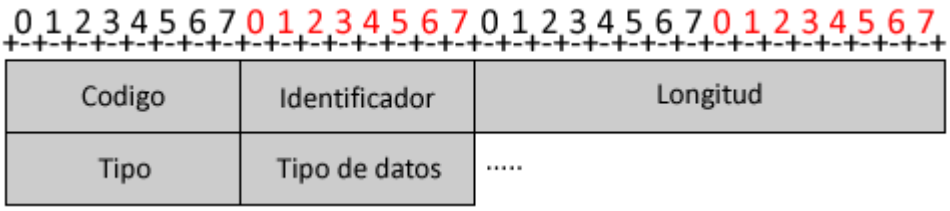


Ilustración 16. Formato paquete *request*

- Código
  El código mide un byte y tiene el valor de 1 en el caso de un paquete de tipo *request* y 2 para un paquete de tipo *response*.
- Identificador
  La longitud de este campo es de un byte. El identificador debe ser el mismo si el paquete se retransmitio, una retransmision de un paquete de tipo *request* se origina debido a que no se recibe el paquete *response* asociado en el tiempo definido.
- Longitud
  La longitud es de dos octetos e indica la longitud del paquete incluyendo los campos de *codigo*, *identificador*, *longitud*, *tipo* y *tipo de datos*.
- Tipo
  El campo *tipo* es de un octeto e indica el tipo de solicitud o respuesta. Se debe indicar un tipo especifico para cada *request* o *response* EAP.
- Tipo de datos
  El campo tipo de datos varia de acuerdo al tipo de *request* y el *response* asociado.
  - Identidad: El autenticador usa el tipo identidad para indicar que esta intentando establecer algun nombre de usuario a autenticar.
  - Notificacion: El autenticador puede usar este tipo de datos para enviar un mensaje al usuario. Esto mensajes pueden incluir informacion como que la contraseña va a expirar o los motivos por los que una cuenta esta bloqueada.
  - NAK: Los Null Acknowledgments se usan para sugerir un nuevo metodo de autenticacion. La siguiente tabla muestra los metodos de autenticacion:

Tipo de codigo	Protocolo de autenticacion	Descripcion
4	Challenge MD5	Autenticacion tipo CHAP en EAP
6	GTC	Diseñado para trabajar con tokens OTP como RSA SecurID
13	EAP-TLS	Autenticacion mutua con certificados digitales
21	TTLS	Tunel TLS, sirve para proteger metodos de autenticacion debiles con encripcion TLS
25	PEAP	EAP Protegido, protege metodos EAP debiles con encripcion TLS
18	EAP-SIM	Autenticacion mediante SIM Card
29	MS-CHAP-V2	Autenticacion mediante password cifrado de Microsoft, compatible con dominios Windows.

Tabla 3. Métodos de autenticación

- Response
  Los paquetes de tipo *response* son enviados por el punto como respuesta a un paquete *request* valido.

  El formato de un paquete de tipo *response* es el mismo usado por los mensajes de tipo *request*.

- Success
  Al final de un intercambio EAP el usuario se ha autenticado satisfactoriamente o ha fallado en el proceso, una vez el autenticador determina que el intercambio esta completo, emite un mensaje con un código de *success* o de *failure* con el fin de terminar el intercambio.

  El formato de una trama de tipo *success* es el siguiente:

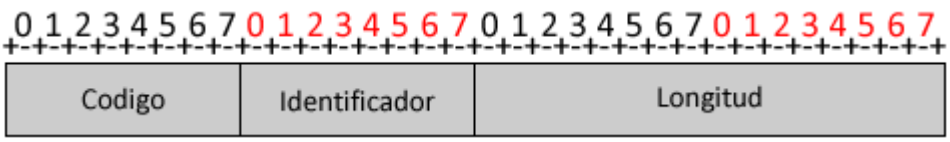


Ilustración 17. Formato trama *success*

- Código: El código ocupa un byte de largo y toma el valor de 3 si el mensaje es de tipo *Success* y 4 si es de tipo *failure.*
- Identificador: el valor de este campo corresponde con el identificador asociado al intercambio EAP que se esté realizando.
- Longitud: Este campo ocupa dos bytes de largo y corresponde a la suma de los campos código, identificador y longitud.

- Failure
  El autenticador envía un mensaje de tipo failure cuando se ha fallado en el proceso de autenticación, la estructura de este paquete es la misma descrita en el campo *success.*

2. Identificador
   Tiene un byte de largo, es un entero usado para mantener una correspondencia entre una solicitud y su respuesta correspondiente.
3. Longitud
   Este campo mide dos bytes e indica la longitud en octetos del paquete EAP, incluyendo los campos de *código*, *identificador*, *longitud* y *datos*. Los octetos por fuera del rango de este campo deben ser tratados como parte del enlace de datos y deben ser ignorados después de su recepción. Un mensaje con una longitud mayor que el número de octetos recibidos debe ser descartado de forma silenciosa.
4. Datos
   El campo de datos puede ser de cero o más octetos. El formato de este campo está determinado por el campo de código.

9.4.5.1.2. Métodos EAP

La extensibilidad permite a un protocolo desarrollar nuevas características a medida que se presentan nuevos requerimientos, esto permite el desarrollo de nuevos métodos para usar en redes inalámbricas.
La selección de un método EAP está relacionada con el sistema de autenticación que se esté usando. Los primeros métodos se centraban en establecer un canal para comunicarse con el servidor de autenticación. Los métodos actuales además de establecer el canal cumplen las siguientes metas:

1. Ofrecer una protección criptográfica fuerte de las credenciales de usuario
   Dada la naturaleza abierta de las redes inalámbricas, cualquier dato que se envié por estas ser protegido si se quiere mantener seguro. La mayoría de los métodos EAP diseñados para redes inalámbricas usan TLS para ofrecer protección a las credenciales de usuario.
2. Ofrecer un mecanismo de autenticación mutua

Debido a que cualquier atacante puede desplegar puntos de acceso falsos para capturar las credenciales de usuario, debe existir una manera de validar que los usuarios se están conectando a la red correcta.

3. Ofrecer una función de derivación de llaves
   Las llaves definidas por los usuarios ofrecen muy poca protección frente a ataques de diccionario, un protocolo de seguridad fuerte debe usar llaves dinámicas generadas de forma aleatoria.

4.9.5.3. 802.1X

802.1X define tres componentes para realizar el proceso de autenticación, el *supplicant* es la maquina del usuario que está intentando acceder a algún recurso de red. El acceso a la red es controlado por el *autenticador*, sin embargo este no mantiene ninguna información del usuario. Todas las solicitudes recibidas se pasan al *servidor de autenticación* para el procesamiento de las credenciales.

El proceso de autenticación es realizado entre el *supplicant* y el *servidor de autenticación* con el *autenticador* funcionando como puente entre los dos. El protocolo usado entre el *supplicant* y el *autenticador* es EAP, mientras que desde el *autenticador* al *servidor de autenticación* el tráfico se transporta en paquetes RADIUS.

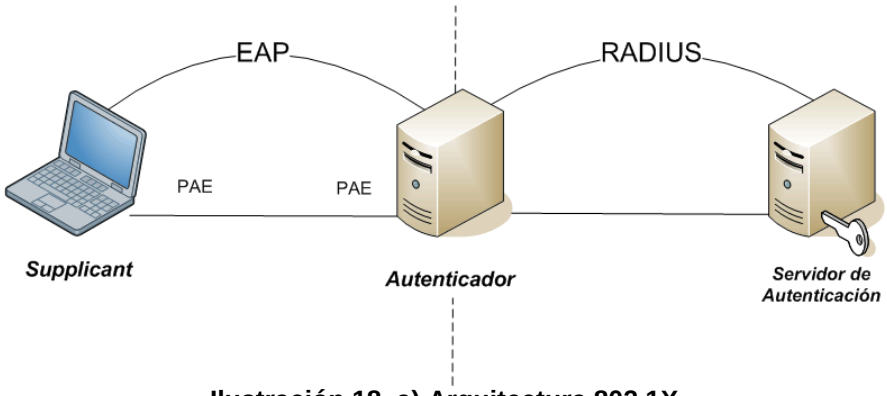


Ilustración 18. a) Arquitectura 802.1X

En resumen en el proceso de autenticación el *supplicant* realiza un intercambio EAP con un servidor RADIUS. Las ventajas de usar RADIUS es que tiene soporte para varias bases de datos, LDAP, NIS, PAM, Cerberos y cuentas de usuario de Windows entre otros.

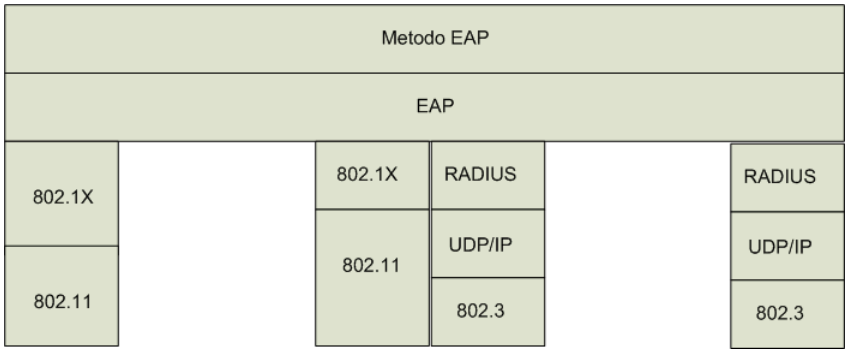


Ilustración 19. b) Arquitectura 802.1X

802.1X es un framework, debido a esto el mecanismo de autenticación es implementado por el *servidor de autenticación*. El framework ofrece una forma de generar *challenges* o de confirmar y denegar el acceso a los recursos de red, mas nunca toma decisiones de acuerdo a las credenciales ingresadas por el usuario.

4.9.6 WEP: WIRED EQUIVALENT PRIVACY

WEP es un algoritmo que hace parte del estándar 802.22 y fue creado con el objetivo de proteger la información transmitida en una red inalámbrica. Este algoritmo es basado en el algoritmo de cifrado RC4 y utiliza claves de 64bits o de 128 bits. A través del tiempo se ha identificado que WEP no es un algoritmo seguro. WEP utiliza claves de cifrado estáticas, lo que permitiría a un atacante almacenar cadenas de texto cifrado con la misma clave con el objetivo de realizar un ataque por fuerza bruta

4.10 SEGURIDAD

4.10.6 Filtrado direcciones MAC

El filtrado de direcciones MAC es un método que permite la creación de una tabla de datos en cada uno de los Acces Point. Esta tabla está compuesta por las direcciones MAC de las tarjetas inalámbricas que tienen permiso de acceder al Acces Point.
Este tipo no brinda confidencialidad de la información, pues no hace uso del cifrado de los datos, en este caso la información de la MAC.
.

4.10.7 VPN

Una Red privada Virtual (VPN) crea un canal virtual sobre una red. Esta red ofrece un túnel por el que viajan los datos totalmente cifrados de un lado a otro. A diferencia de otros protocolos, este túnel representa un área virtual dedicada entre dos puntos.

Las VPNs proveen los servicios de cifrado, autenticación, integridad y encapsulamiento de los datos. Adicionalmente utilizan protocolos que permiten otorgar acceso a servicios privados de una empresa o cierto personal autorizado. La definición más clara de una red virtual privada es, una estructura de red creada sobre una red de transmisión publica que usa las mismas políticas de acceso que se utiliza normalmente en las redes privadas.

4.11 ESTRUCTURA DE DATOS GEOGRAFICOS

Estas estructuras de datos son utilizadas para realizar consultas más eficientes acerca de datos geográficos, manejan datos mono dimensionales, es decir los datos de asocian a un único atributo.

4.11.1 Estructura de datos Árbol-R

Existen diferentes estructuras de datos para manejar esta clase de atributos espaciales como lo son los árboles tipo R, los cuales son utilizados en métodos de acceso espacial. Significa que indexan información multidimensional, esta información se puede definir como las coordenadas que existen en algún lugar geográfico .Un problema real puede ser: “Encontrar todas las redes inalámbricas en un radio de 100 metros alrededor de la posición actual”.

Los arboles-R se encuentran divididos de forma jerárquica en conjuntos, utilizados para almacenar y borrar datos en tiempo logarítmico. Los algoritmos de búsqueda hacen uso de los conjuntos límite para identificar en que nodo buscar .De esta forma el tipo de arboles (Arboles-B) son ideales para el trabajo con bases de datos. Los conjuntos límite aseguran que los elementos cercanos se encuentran localizados en la misma hoja, cada hoja contiene un identificador del elemento actual y el conjunto limite del elemento.

(I, tupla-identificador)

I está definido como un intervalo [a, b], donde n es el número de dimensiones.

$$\mathbf{I= (I_0 , I_1, I_2, I_3,\ldots,I_{n-1})}$$

Ahora cada nodo que no es hoja se compone de un registro que incluye la dirección del nodo inferior del árbol, I se define como los rectángulos que se encuentran en los nodos inferiores. Como se muestra a continuación:

(I, puntero-hijo)

De esta manera se puede representar gráficamente lo dicho anteriormente: Ilustración 20.

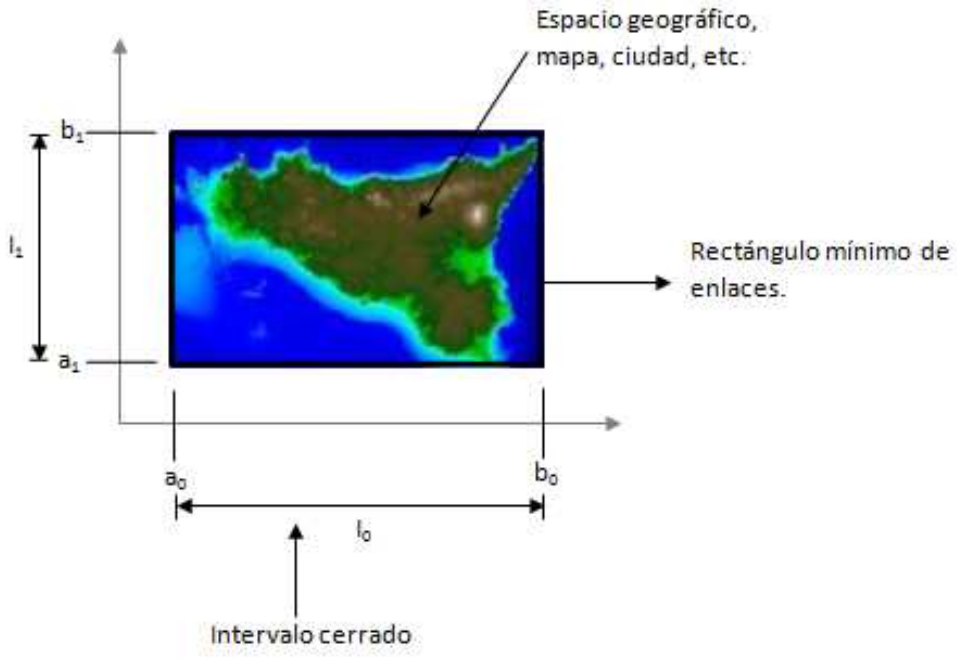


Ilustración 20. Representación grafica Árbol-R

4.11.1.1 Propiedades de los Arboles-R

Se tiene que M es el máximo número que existen de entradas en un nodo, existe un m que es $m \leq M/2$ el cual es el mínimo de entradas que se encuentran en un nodo, dicho lo anterior se deben cumplir las siguientes propiedades:

1. Cada hoja, contiene un intervalo de m y M registros indexados.
2. Cada uno de los nodos no hojas, contiene un intervalo de m y M de nodos hijos.
3. El nodo principal tiene por lo menos dos hijos.
4. Los nodos hojas se encuentran al mismo nivel.
5. La altura de un árbol –R es de $[\log_m N]-1$.

4.11.2 Estructura de datos X-tree

Esta estructura de datos es utilizada para datos con altas dimensiones, está basada en arboles-R. Si existe un gran número de coordenadas esta estructura llega a un punto de deterioro de ahí la necesidad de crear la estructura de Árbol X-tree.
Dentro de este existe el 2D-tree, en el cual cada registro tiene dos campos espaciales. Como se muestra en la siguiente figura:

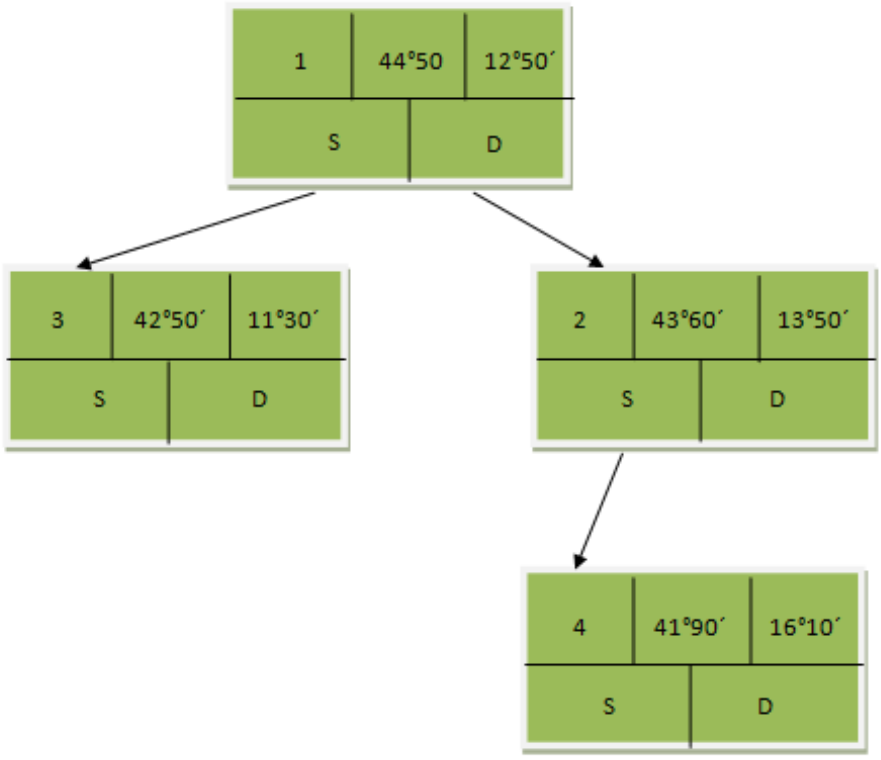


Ilustración 21. Estructura de datos 2D-tree

La estructura representa el id de las coordenadas, latitud y longitud de cada punto. Cada uno de los puntos es insertado con su respectiva información.

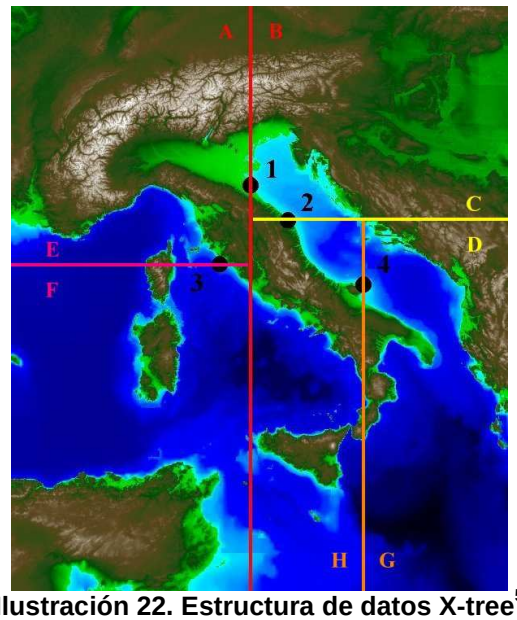


Ilustración 22. Estructura de datos X-tree[5]

[5] Geographic Data Structures, María Antonia Brovelli, Politécnico di Milano, http://geomatica.como.polimi.it/corsi/geog_info_system/l10_geographicdatastructures.pdf, pág. 36.

Existe el quadTree, en este caso se utilizan cuatro cuadrantes para cada nodo, pero representan puntos de dos dimensiones, los cuadrantes son divididos como: NO (norte- Oeste), SO (sur-oeste), NE (norte –oeste) y SE(sur-este), la manera de representarlo es la siguiente:

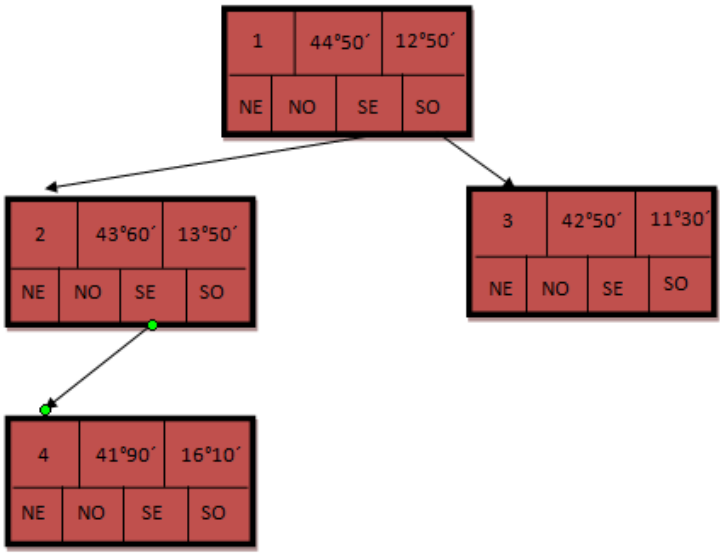


Ilustración 23. Estructura de datos quadTree

Geográficamente esta estructura hace las particiones de la siguiente manera:

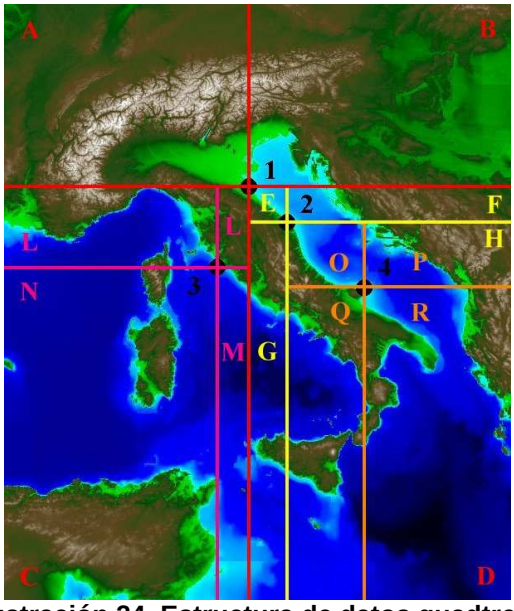


Ilustración 24. Estructura de datos quadtree[6]

[6] Geographic Data Structures, María Antonia Brovelli, Politécnico di Milano, http://geomatica.como.polimi.it/corsi/geog_info_system/l10_geographicdatastructures.pdf, pág. 56.

4.11.3 Estructura de datos HHCODE

Estructura de datos que almacena datos espaciales a través de una codificación en n-dimensiones con un valor unidimensional, se realiza por medio de un nuevo tipo de datos helicoidal, esta estructura se basa en una descomposición recursiva del espacio, determinada región es divida en dos dimensiones y se divide en cuatro cuadrantes a estos se les asigna un código de 0 a 3.

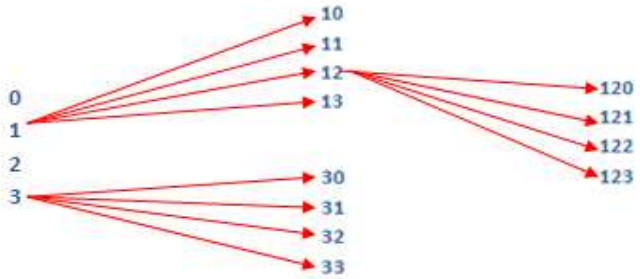


Ilustración 25. Estructura de datos HHCODE[3]

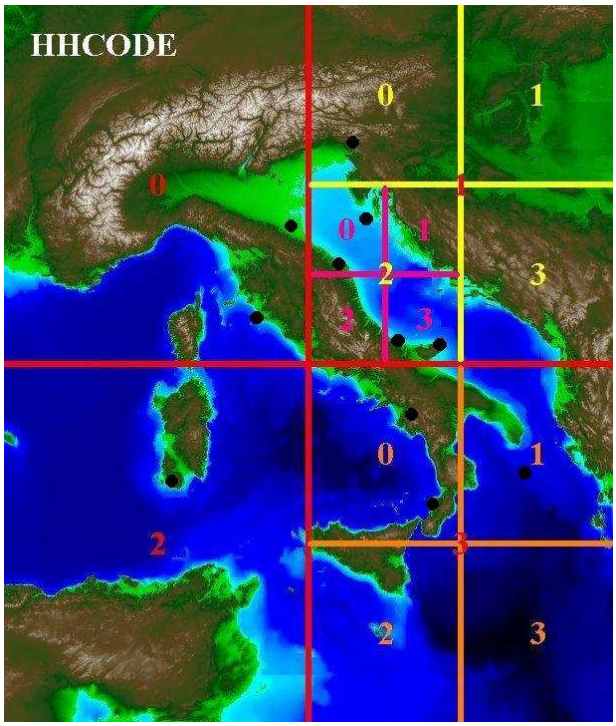


Ilustración 26. Partición estructura de datos HHCODE[7]

[7] Geographic Data Structures, María Antonia Brovelli, Politécnico di Milano, http://geomatica.como.polimi.it/corsi/geog_info_system/l10_geographicdatastructures.pdf, pág. 45.

4.12 Hardware

Existen dispositivos que permitan interconectar elementos Wireless. Entre estos se encuentran los routers, puntos de acceso, computadores, tarjetas PCI o USB.

- **Routers:** Es una dispositivo de Hardware que permite interconectar segmentos de red y enviar paquetes de datos entre redes, el router elige que camino debe escoger de tal forma que el envió sea más rápido para proceder a buscar el punto de llegada del paquete. Estos dispositivos se encargan del control de errores, extracción de la información, distribución de la señal.

- **Repetidores**: Los repetidores son los encargados de ampliar la señal, teniendo en cuenta que la señal sea la más adecuada adicionalmente repite las diferentes señales de los segmentos a los otros que se encuentran conectados a un repetidor.

- **Switches:** Los switches son los encargados de analizar los diferentes frame que van llegando, cuando llega un frame lo revisa y decide según su contenido como debería reenviarlo a su destino final.

- **Gateway:** Es un punto de la red, lo que hace es que permite que una red entre a otra red, como por ejemplos los proxy server, los firewall o servicios que dejan pasar un correo de un lado a otro.

4.12.1 Obstáculos que causan interferencia en la señal

Existen varios obstáculos que pueden interferir en la señal de una red inalámbrica esto hace que la señal llegue más baja, inclusive estando a pocos metros de distancia. Estas interferencias son:

1. Existen los obstáculos que retienen la señal como lo son, las paredes, el suelo, los muebles, y demás objetos., cuando la red inalámbrica este mas lejos de obstáculos de este tipo, su señal tendrá una mayor cobertura.
2. Los objetos que pueden modificar la señal de una red inalámbrica son en su mayoría metálicos, puesto que estos objetos reflejan la onda y la llenan de ruido, por esta razón es recomendable tener obstáculos de este tipo y así tener mayor cobertura.
3. Y por último los obstáculos que compiten por la señal, son objetos que requieren de la misma frecuencia, un ejemplo a esto son los Router y una de las formas de solucionar este problema es conseguir routers que manejen una frecuencia distinta de 2.4GHz.

Las señales de radiofrecuencia pueden interrumpirse por la acción de ciertos materiales ambientales. Los siguientes materiales provocan interferencia en las señales inalámbricas.

• **Materiales**	• **Ejemplo**	• **Interferencia**
• Madera	• Puertas	• Baja
• Vidrio	• Ventanas	• Baja
• Yeso	• Paredes Interiores	• Baja
• Asbesto	• Techos	• Baja
• Hojas	• Arboles	• Media
• Ladrillo	• Paredes	• Media
• Cerámica	• Tejas	• Alta
• Papel	• Rollos de Papel	• Alta
• Vidrio	• Ventanas	• Alta
• Metal	• Viga	• Muy Alta

Tabla 4. Materiales interruptores de Señal

4.13 EFECTO FRESNEL

Aparte de los obstáculos nombrados anteriormente, se puede hablar de un problema que se llama efecto de Fresnel, esto se refiere a crear una línea visual , entre dos puntos , esto quiere decir que si un punto puede observar a otro; si esto se hace en el día , esta línea es más fácil de observar cosa que no pasa en la noche , entonces para esto pueden existir unos obstáculos como lo son las montañas, la curvatura de la tierra, edificios, arboles , etc., hasta llegar a un punto de bloquear esta línea. Esto es con respecto a la visibilidad pero esto también ocurre con una señal de red inalámbrica, ya que puede reducir la potencia de señal.

Para esta línea existe un área llamada zona Fresnel, esto depende de la longitud de línea y de la frecuencia de la señal. Entonces si algún objeto queda dentro de esta zona hace que ocurra una difracción, esto se refiere a que la señal llegue a la antena un poco después de lo que debería llegar, esto puede hacer que la señal sea un poco más baja, y a veces se pierda.

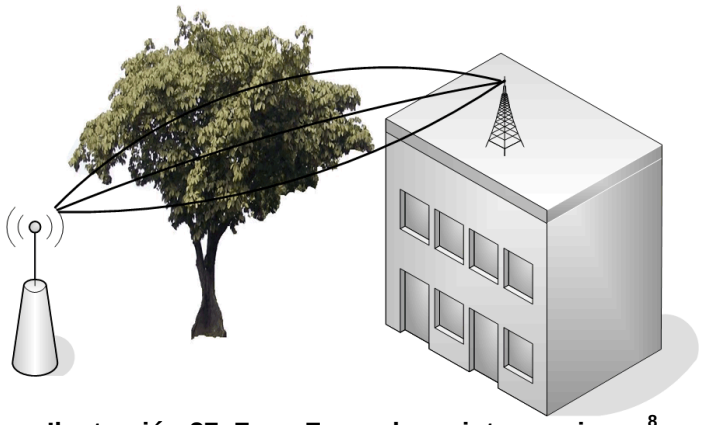


Ilustración 27. Zona Fresnel con interrupciones[8]

Si los obstáculos que aparecen no son tan fuertes para bloquear una señal, como por ejemplo los arboles, lo que hace la señal es atenuarse, pero esto hace que su calidad se reduzca. Algunas veces para que todo lo anterior no ocurra elevan las antenas para que ya la línea de visión entre estos punto sea directa.

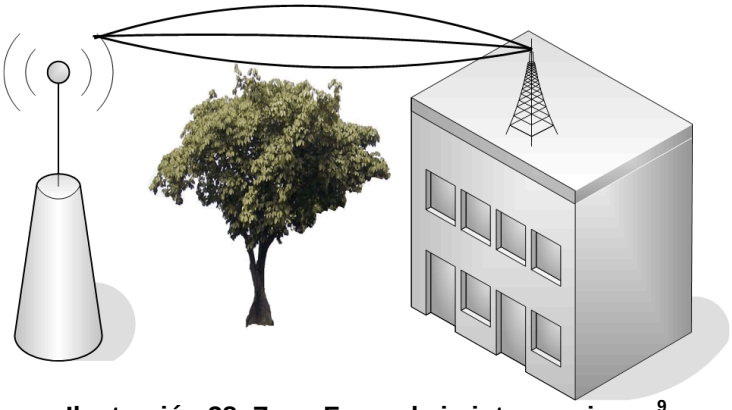


Ilustración 28. Zona Fresnel sin interrupciones[9]

4.14 GOOGLE MAPS

Es un servidor de aplicaciones de mapas web, servicio que google presta gratuito, la función que realiza es generar fotos satelitales del mundo y rutas entre diferentes ubicaciones, con el fin de poder visualizar de una manera diferente ubicaciones geográficas, sea cual sea el motivo, google maps ofrece diferentes servicios, como localizar restaurantes, hoteles, museos, etc. Y también pueden servir como guía turístico.

En el caso de esta aplicación lo que se quiere es que el usuario pueda visualizar las diferentes redes inalámbricas que se encuentran en cualquier lugar donde se quiera capturar las redes.

[8] Estándares y Topologías inalámbricos (pasado, presente y futuro de las redes wireless) [Paper]. Pág. 11.
[9] Estándares y Topologías inalámbricos (pasado, presente y futuro de las redes wireless) [Paper]. Pág. 11.

4.14.6 Funcionamiento

Google maps utiliza gran cantidad de archivos javascript y XML, con el objetivo de brindar al usuario un mapa interactivo. Ejemplo realizar acercamientos, adicionalmente desplazarse en cualquier ubicación. Si un usuario realiza una búsqueda, la ubicación de esta es marcada por un indicador que se convierte en un pin, este pin es una imagen que se encuentra en formato PNG; este proceso es transparente para el usuario.

4.14.7 API Google maps

El api de google maps, es la forma de insertar los mapas a páginas Web, lo primero que se debe hacer es crear una llave para poder interactuar con este API, cuando se interactúa con la programación de los mapas se deben seguir las siguientes instrucciones:

1) Se puede comenzar creando un mapa de 500 x 300 y se puede centrar en las coordenadas que se desee.
2) Luego de esto se carga el código del API por medio de una etiqueta script, como se muestra a continuación, en esta dirección se encuentra el código javascript , que contiene todo lo necesario para utilizar el API.

```
<script src="http://maps.google.com/maps?file=api&v=2&key=abcdefg&sensor=true_or_false"
        type="text/javascript">
</script>
```

3) Ahora se crea un elemento div, en donde se coloca el nombre de map_canvas , esto se hace para crear un espacio en la página web , únicamente para el mapa que se va a cargar.

```
<div id="map_canvas" style="width: 500px; height: 300px"></div>
```

4) Se crea un objeto llamado Gmap2, la clase javascript que representa los mapas, cada objeto de esta clase solo define a un único mapa. Se utilizaron aspectos de las operaciones del mapa.

```
var map = new GMap2(document.getElementById("map_canvas"));
```

5) Se le asigna las coordenadas donde se quiere centrar el mapa, esto se hace a través de un método llamado setCenter ().Para utilizar este método se necesita conocer una coordenada GLatLng, objeto que hace referencia a una ubicación dentro de él, los parámetros son latitud y longitud. Adicionalmente se le asigna un nivel de acercamiento. antes de manipular cualquier objeto en el mapa.

```
map.setCenter(new GLatLng(37.4419, -122.1419), 13);
```

6) Ahora lo que se hace es introducir un evento que permite que el mapa se cargue antes de ser visualizado, con el fin de evitar imprevistos y tener un control de cómo se está dibujando lo solicitado.

```
<body onload="initialize()" onunload="GUnload()">
```

Las anteriores son las instrucciones que se deben llevar a cabo para ubicar un mapa de google maps en una página web e interactuar con el API.
Google Maps también permite el manejo de ventanas de información de tipo GInfowindow, quienes muestran un contenido HTML en una ventana flotante sobre el mapa. En este caso se utilizo para mostrar la información de cada una de las redes como: MAC, ESSID, CHANNEL, QUALITY, ENCRYPTION, AUTHENTICACTION, LATITUD y LONGITUD. Esta ventana se crea automáticamente cuando se crea un mapa, debido a que no tiene un constructor especifico.

5 GPS (Sistema de posicionamiento global)

Las siglas GPS significan **G**lobal **P**ositioning **S**ystem (sistema global de posicionamiento), es un sistema de navegación compuesto de 24 satélites puestos en órbita por el Departamento de Defensa de los Estados Unidos, y sus estaciones en tierra. Estos satélites envían señales de radio a la superficie de la tierra, son llamados NAVSTAR y tiene 5 estaciones repartidas en la superficie terrestre, se encuentran en Hawai, Isla de Ascensión, Diego Gracia, Atolón de Kwajalein y Colorado Springs, estas estaciones tienen como función monitorear el estado de los satélites y su posición.

5.1 Historia

El GPS nació debido a la necesidad de tener un sistema de navegación preciso. El desarrollo de relojes atómicos y el progreso de la tecnología espacial hicieron posible el GPS. La precisión de los relojes es importante puesto que el GPS depende del tiempo que toma las señales de los satélites en llegar a los receptores en la tierra para identificar la posición y los tiempos de viaje de estas señales.
En 1948, la Oficina Nacional de Normas de Estados Unidos fabrico el primer reloj atómico ineficiente, que utilizaba moléculas de amoniaco y tubo de cobre.
En 1956 se fabrico un reloj portable “Atomichron”. Estos nuevo relojes que se fueron creando con el tiempo, empleaban frecuencias resonantes de cesio, rubidio, máser de hidrogeno y moléculas de amoniaco.
Durante los 60’s diversas fuerzas armadas de Estados Unidos trabajaron en sistemas de navegación por satélite, “Navstar” fue el resultado de estos estudios, el cual depende de satélites que transportan relojes atómicos, estaciones terrestres que controlan el sistema y posicionadores (receptores).En el año 1978 fue lanzado el primer satélite y en el año 1995 se envió la totalidad de los satélites de GPS.

5.2 Funcionamiento del GPS

El GPS depende de la transmisión de la posición y señal de tiempo exacta enviada por los satélites. Luego de obtener esta información, los receptores GPS pueden calcular su distancia al satélite, utilizando la información de cuatro satélites, el receptor puede calcular la posición exacta.
Las coordenadas que ofrece el GPS son latitud, longitud y altura sobre el elipsoide WGS84.Este elipsoide es un modelo matemático de la forma de la tierra. Como se nombro anteriormente, este sistema está formado por una constelación de 24 satélites, que orbitan la tierra a una altura de 20.200 Kilómetros, emitiendo ondas de radio. Los satélites emiten ondas en dos frecuencias y s encuentran moduladas con un código binario.

Para determinar la posición (latitud, longitud y altura) el receptor GPS calcula la intersección de tres esferas cuyos centros son la posición de cada satélite y cuyos radios son las distancias entre el receptor y satélite. Por esta razón el GPS se basa en la medición de distancias entre el receptor y satélite.

5.2.1 Triangulación y Trilateración

Con frecuencia se usa el término triangulación para hacer referencia al proceso mediante el cual el GPS determina la posición de un receptor en la tierra.

A pesar de que la triangulación también se usa para obtener la ubicación de un punto a partir de la ubicación de otros puntos conocidos, existen algunas diferencias que se explicaran a continuación entre este procedimiento y el usado por un GPS.

5.2.1.1 Triangulación

La triangulación es el proceso de determinar la ubicación de un punto midiendo los ángulos que se forman entre él, dos puntos conocidos y ubicados en los extremos de una línea imaginaria.

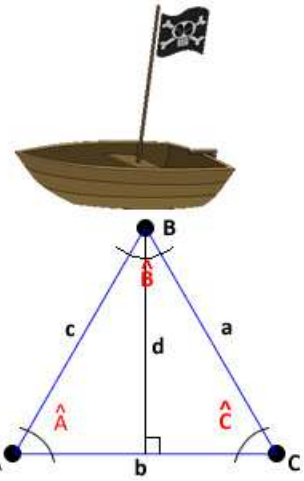


Ilustración 29. Triangulación

Por ejemplo, un observador ubicado en el punto A mide el ángulo $\hat{A}$ formado entre la base del triangulo y el barco, mientras que un observador en el punto C hace lo mismo para el ángulo $\hat{C}$. Si se tiene la longitud b entre A y B, se puede usar la ley de los senos para encontrar la distancia d de la siguiente manera:

$$\frac{\sin \hat{A}}{a} = \frac{\sin \hat{B}}{b} = \frac{\sin \hat{C}}{c}$$

Como b es conocida, podemos reescribir las longitudes a y c de la siguiente forma:

$$a = \frac{b \sin \hat{A}}{\sin \hat{B}}$$

$$c = \frac{b \sin \hat{C}}{\sin \hat{B}}$$

La distancia d puede ser calculada usando el seno de $\hat{A}$ o el de $\hat{C}$, para la demostración se usara el seno de $\hat{A}$:

$$\sin \hat{A} = \frac{d}{c}$$

Despejando d obtenemos la siguiente ecuación:

$$d = c \sin \hat{A}$$

Reemplazando el valor de c en la ecuación anterior obtenemos:

$$d = \frac{b \sin \hat{A} \sin \hat{C}}{\sin \hat{B}}$$

Sabemos que:

$$\hat{B} = 180° - \hat{A} - \hat{C}$$

Debido a que $\sin \theta = \sin 180 - \theta = \sin 180 - (\hat{A} + \hat{C})$, podemos sustituir $\sin \hat{B}$ por $\sin(\hat{A} + \hat{C})$ para obtener:

$$d = \frac{b \sin \hat{A} \sin \hat{C}}{\sin(\hat{A} + \hat{C})}$$

Para obtener las coordenadas del punto B con las distancias c y a obtenidas de los cálculos anteriores, se puede usar el seno y el coseno de cualquiera de los dos puntos de observación $\hat{A}$ o $\hat{C}$ para obtener la desviación respecto a los ejes norte-sur y oriente-occidente, respectivamente.

5.2.1.2 Trilateración:

El método usado por los sistemas de GPS para obtener la ubicación de un punto en la tierra se conoce como **trilateración**. Este usa las ubicaciones conocidas de varios puntos de referencia, como los satélites, la distancia entre cada uno de estos puntos y el punto a ubicar.

Geométricamente hablando se necesitan 4 puntos de referencia para ubicar un punto en el espacio de forma correcta, sin embargo con tres puntos se obtienen dos posibles ubicaciones de las que generalmente se puede descartar una. (*Ver Funcionamiento del GPS*).

El problema de la trilateración tridimensional se formula mediante el sistema de ecuaciones conformado por las ecuaciones de las tres esferas. Para esto se imponen tres restricciones sobre las ecuaciones para facilitar su solución:

1. Todas las esferas están en el plano $Z = 0$.
2. Una esfera debe estar en el origen.
3. Otra esfera debe estar sobre el eje X.

La siguiente grafica muestra un ejemplo de las condiciones impuestas sobre las esferas:

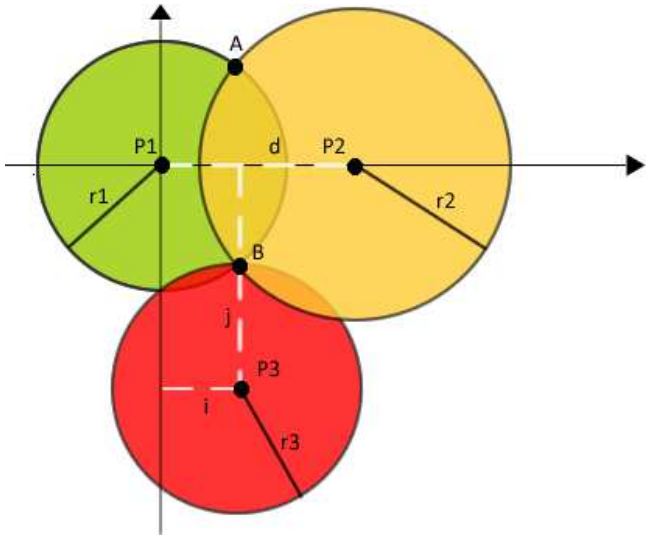


Ilustración 30. Condición de las esferas en trilateración

Por medio de traslaciones cualquier conjunto de puntos en el espacio se puede mover para cumplir estas condiciones, encontrar la solución y devolver las traslaciones realizadas para obtener la solución en el sistema de coordenadas original.

Las ecuaciones de las tres esferas de acuerdo a la imagen anterior son:

$$(1)\ r_1^2 = x^2 + y^2 + z^2$$

$$(2)\ r_2^2 = (x-d)^2 + y^2 + z^2$$

$$(3)\ r_3^2 = (x-i)^2 + (y-j)^2 + z^2$$

Igualando las dos primeras ecuaciones y resolviendo para X tenemos:

$$r_1^2 - x^2 - y^2 - z^2 = r_2^2 - (x-d)^2 - y^2 - z^2$$

$$r_1^2 - x^2 = r_2^2 - x^2 + 2xd - d^2$$

$$r_1^2 = r_2^2 + 2xd - d^2$$

$$(4)\ x = \frac{r_1^2 - r_2^2 + d^2}{2d}$$

Al sustituir este resultado en la primera ecuación obtenemos la formula de un círculo, correspondiente a la intersección entre las dos primeras esferas:

$$(5)\ r_1^2 - \frac{(r_1^2 - r_2^2 + d^2)^2}{4d^2} = y^2 + z^2$$

Ahora sustituyendo la ecuación (4) en la ecuación (5) tenemos:

$$(6)\ r_1^2 - x^2 = y^2 + z^2$$

Reemplazando la ecuación (6) en la ecuación de la tercera esfera tenemos:

$$r_3^2 = (x-i)^2 + (y-j)^2 + r_1^2 - x^2 - y^2$$

$$r_3^2 = x^2 - 2ix + i^2 + y^2 - 2jy + j^2 + r_1^2 - x^2 - y^2$$

$$r_3^2 = -2ix + i^2 - 2jy + j^2 + r_1^2$$

$$2jy = r_1^2 - r_3^2 + i^2 + j^2 + 2ix$$

$$(7)\ y = \frac{r_1^2 - r_3^2 + i^2 + j^2}{2j} + \frac{i}{j}x$$

Ahora con las coordenadas X (Ecuación 4) e Y (Ecuación 7), se puede despejar Z de la formula de la primera esfera:

$$r_1^2 = x^2 + y^2 + z^2$$

$$z = \sqrt[2]{r_1^2 - x^2 - y^2}$$

Debido a que Z se expresa como una raíz cuadrada, se pueden tener cero, una o dos soluciones al problema. Esto se puede ver como si se tomara el círculo correspondiente a la intersección de la primera y segunda esfera e interceptarlo con la tercera esfera.

Si el círculo no interseca a la esfera la solución no es real (la raíz cuadrada de un valor negativo).

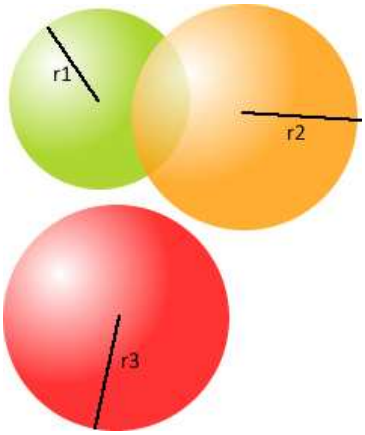


Ilustración 31. Solución no real de intersección de esferas

Si el circulo toca la esfera en un único punto entonces Z=0 y se tendría una única solución.

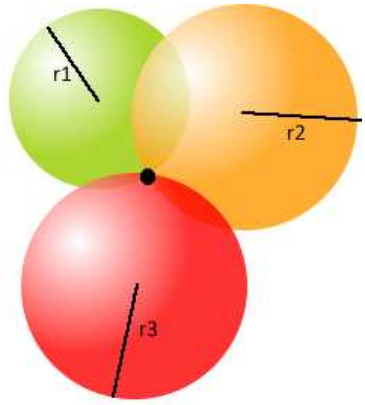


Ilustración 32. Única solución de intersección de esferas

Si el círculo toca a la esfera en dos puntos entonces Z es igual al valor positivo o negativo de la raíz cuadrada de un número positivo y existirían dos soluciones al problema.

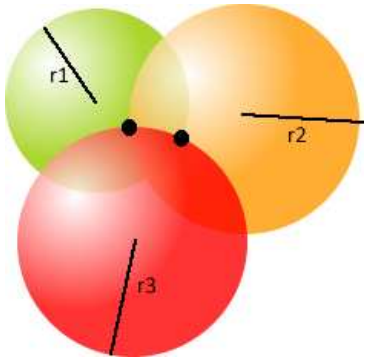


Ilustración 33. Doble solución de intersección de esferas

Debido a la trayectoria esférica de los satélites del sistema GPS y a la facilidad de medir la distancia entre estos y un receptor, es que se usa la trilateración como el método para geolocalizar al receptor GPS.

5.2.2 Triangulación del GPS

El funcionamiento del GPS se basa primordialmente en un principio básico de triangulación, por esta razón es necesario conocer la distancia exacta entre el satélite y el GPS.

El principio básico de triangulación ayuda a dar el punto o lugar en donde se encuentra el objeto, este emplea círculos o líneas rectas creando esferas imaginarias, las cuales se crean inmediatamente que el GPS detecta la señal de radiofrecuencia, cuando esto sucede el receptor mide la distancia entre el satélite y el GPS, significa que el punto se encuentra en algún lugar del circulo.

- Inicialmente se mide la distancia entre el satélite y la posición actual del receptor.

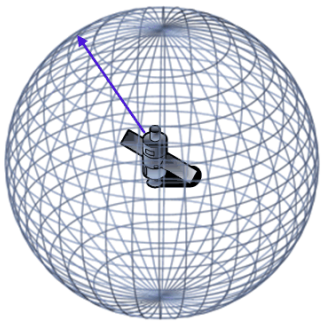


Ilustración 34. Distancia satélite – receptor[10]

[10] GPS Fácil, uso del sistema de posicionamiento global, autor: Lawrence Letham, editorial: Paidotribo , 2001. Pág. 12.

- A continuación se realiza el mismo procedimiento con un segundo satélite, esto reduce las posibles ubicaciones del receptor al área correspondiente a la intersección entre las dos esferas.

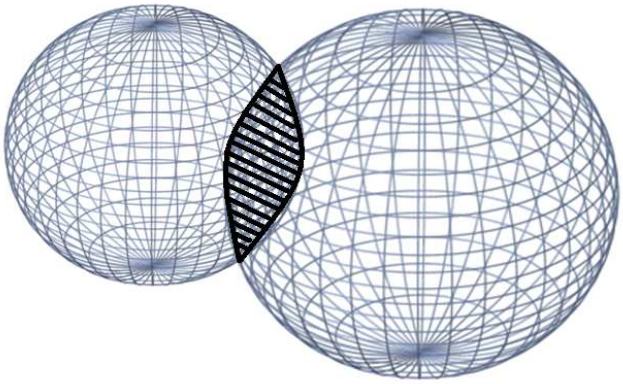


Ilustración 35. Intersección entre las dos esferas[11]

- Finalmente se mide la distancia a un tercer satélite, de esta forma solo quedan dos posibles puntos en los que el receptor puede estar ubicado.

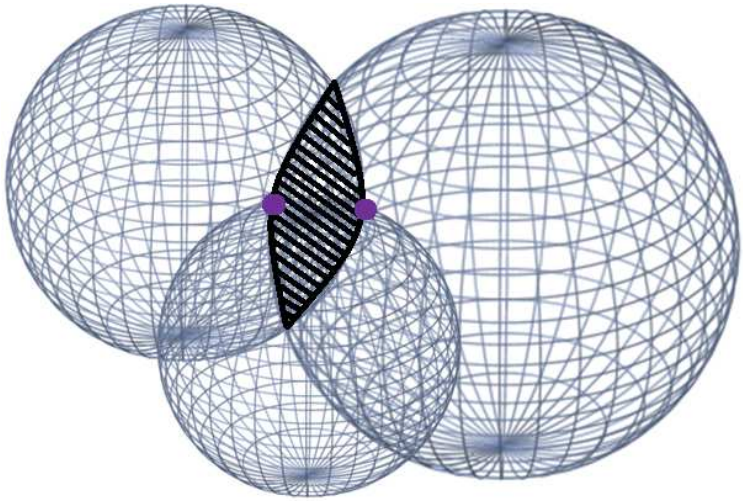


Ilustración 36. Puntos donde el receptor puede estar ubicado[12]

- Se puede realizar una medición a un cuarto satélite para obtener la ubicación exacta del receptor, aunque usualmente solo se utilizan tres

[11] GPS Fácil, uso del sistema de posicionamiento global, autor: Lawrence Letham, editorial: Paidotribo , 2001. Pág. 12.

[12] GPS Fácil, uso del sistema de posicionamiento global, autor: Lawrence Letham, editorial: Paidotribo , 2001. Pág. 12.

mediciones debido a que uno de los dos puntos se puede descartar pues representa una posición absurda para el receptor.

5.2.2.1 Geométricamente

Básicamente se basa en saber cuál es el ángulo de cada una de las señales que emite los satélites de esta manera ya se puede saber el punto de medición.

Ahora se calcula el radio de cada una de las esferas este radio es la distancia desde el satélite hasta la superficie de la esfera virtual, la cual es la misma del receptor al satélite, esta distancia se calcula con la siguiente ecuación.
Distancia = Tiempo * Velocidad

Velocidad = velocidad de las ondas electromagnéticas en el vacío. Velocidad de la luz que es 3 x 10^5 Km/s.
Tiempo = es el tiempo en el que viaja la señal.

Para saber este tiempo es necesario saber el tiempo que transcurrió en el momento de la emisión y el tiempo transcurrido hasta su recepción, pero esto solo se puede saber con la sincronización de los relojes del receptor y del satélite, el satélite posee un reloj atómico de cesio, estos relojes son muy exactos, mientras que el GPS posee un reloj de cuarzo los cuales no son tan exactos.
Para poder sincronizar estos dos el satélite envía una señal digital cada intervalo de tiempo esto lo hace junto a una señal de radiofrecuencia, lo que hace esta señal es llegar al receptor con un retardo esto con el fin de que este retraso será igual entre los dos relojes cuando este viajando al receptor.

A lo anterior lo podemos llamar pseudotelemetrizacion , esta técnica se utilizan códigos PRN(C/A y P), esto se hace sobre unas portadoras llamadas L1(19 cm de longitud de onda) y L2(24 cm de longitud de onda),por las cuales se transmite información esto los posee los satélites NAVSTAR , con una variación del tiempo (Δt) esto para la llegada de los códigos , como se dijo anteriormente esto se maneja con unos relojes los cuales no se pueden sincronizar de una manera fácil por esta razón se maneja una técnica llamada pseudodistancia ; esta técnica es la que más se utiliza ya que es la que da una mejor precisión respecto a la ubicación del receptor.

Como esta distancia no es exacta se resuelve un sistema de cuatro ecuaciones para poder encontrar las coordenadas exactas del receptor, estas ecuaciones se describen de la siguiente manera:

$$(x-x_1)^2+(y-y_1)^2+(z-z_1)^2=D_1{}^2$$
$$(x-x_2)^2+(y-y_2)^2+(z-z_2)^2=D_2{}^2$$
$$(x-x_3)^2+(y-y_3)^2+(z-z_3)^2=D_3{}^2$$

$$(x - x_4)^2 + (y - y_4)^2 + (z - z_4)^2 = \square_4^2$$

Siendo (x_0, y_0, z_C) las coordenadas que queremos encontrar.

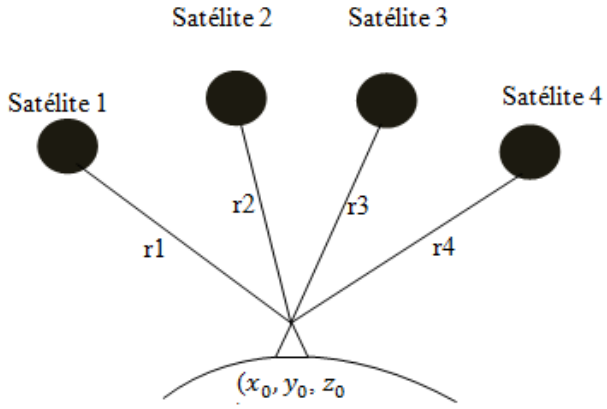


Ilustración 37. Ubicación de los Satélites

De esta manera podemos saber de forma más exacta la posición del receptor, puesto que en esta se necesito de cuatro satélites y no tres ya que con el cuarto se puede tener una mayor precisión del tiempo y la distancia.

Como se dijo anteriormente, este sistema no es un 100% exacto de acuerdo a su medición por esta razón para un sistema de dos dimensiones la longitud de un error se denota por $\bar{e}$, para calcular este error se utiliza el teorema de Pitágoras de la siguiente manera.

$$\bar{e} = \sqrt{x^2 + y^2}$$

De esta manera se podrá saber una posición verdadera partiendo de que los puntos son conocidos.

5.2.2.2 Solución de las ecuaciones para encontrar un punto en la tierra mediante la triangulación.

Como se dijo anteriormente los diferentes satélites forman diferentes circunferencias cada una tiene diferentes puntos de ubicación y diferentes radios, partiendo de esto tenemos:

$$Satelite\ 1 = S_1(x_1, y_1, z_1)$$
$$Satelite\ 2 = S_2(x_2, y_2, z_2)$$
$$Satelite\ 3 = S_3(x_3, y_3, z_3)$$
$$Satelite\ 4 = S_4(x_4, y_4, z_4)$$

Con lo anterior podemos desarrollar las siguientes ecuaciones:

$$(x - x_1)^2 + (y - y_1)^2 + (z - z_1)^2 = {D_1}^2$$
$$(x - x_2)^2 + (y - y_2)^2 + (z - z_2)^2 = {D_2}^2$$
$$(x - x_3)^2 + (y - y_3)^2 + (z - z_3)^2 = {D_3}^2$$
$$(x - x_4)^2 + (y - y_4)^2 + (z - z_4)^2 = {D_4}^2$$

La solución de estas ecuaciones se solucionan de la misma forma que el método descrito en la sección (*5.2.1.2 Trilateración.)*

Solucionando lo anterior se puede decir que los objetos están en vacio como se dijo anteriormente, por esta razón influye mucho el clima y muchos factores de donde sale la señal del GPS, para que esta sea clara y exacta.

5.2.3 Fases de códigos y portadoras

Se sabe que los satélites y los georeceptores tienen que estar sincronizados para esto generar un mismo código, luego de esto se mira en qué momento el georeceptor recibió el código, de esta forma se encuentra la diferencia de tiempo esto quiere decir que es el tiempo que se demoro la señal para llegar a la tierra.

Para esto existen unas fases mientras la señal está siendo transmitida las cuales son:

1. Código
2. CD (Tt)= Ttsv fcD
3. Portadora CR(Tt) = Ttsv fcR

T = el tiempo de un sistema de un solo satélite
t = tiempo del receptor
Cuando el subíndice es t esto quiere decir que la señal es la que se trasmite.
Cuando el subíndice es r esto quiere decir que la señal es la que se recibe.
fcD = es la frecuencia del código .
fcR = es la frecuencia de la portadora.

5.2.3.1 Medidas de las fases de los códigos

Cuando hablamos de la fase de código hablamos de la generada por el receptor y la cual es desplazada progresivamente según la secuencia que está generando el satélite, esto se hace hasta que se puede obtener una máxima correlación.
Con esta fase se puede obtener la época de la transmisión Tt esto en estado del código.
Entonces dicho lo anterior se puede encontrar la diferencia entre ambas lecturas del código, esto es llamado pseudodistancia, dicho anteriormente, la cual se expresa de la siguiente manera.

PR= c (tr – Tt)

Ahora se pueden obtener más detalles de esta ecuación de la siguiente manera:

PRCD = c(tr –Tt)= R + cdtu + cdta + cdts + eR

dts=Esto represente el error que existe en el reloj del satélite con respecto al del GPS.
dtu= esto representa el error de sincronización del reloj.
dta= esto representa el retraso que sucede por la atmosfera.
eR= esto representa el ruido que puede existir en la transmisión.
R= esto representa la distancia inclinada de la señal.

Ahora se evalúa la fase portadora, se quiere es encontrar la diferencia entre la fase portadora transmitida CR(Tt) , esto se llamaría la fase relativa la cual se puede hallar de la siguiente manera:

PRcR = R + cdtu + cdta + cdts + c(N/fcR) + eR

De esta manera se completarían las diferentes fases y se podría transmitir información de posicionamiento de navegación.

5.2.4. Errores en un GPS

En el mundo existen muchos factores que pueden hacer que la señal de un GPS se dañe, como la distancia entre el satélite y el GPS. Esta señal tiene que pasar por la ionosfera y luego por el vapor del agua llamado troposfera, con estos factores permiten que se pierda la velocidad para llegar a su destino. Una solución a este problema es verificar las condiciones atmosféricas y predecir si la señal llega en un tiempo preciso o presenta un retardo, existen retardos que no son significativos, por esta razón el punto de la ubicación dada por el GPS es casi exacto.

Otro problema que se puede encontrar es en los satélites aunque sean muy sofisticados y de una precisión muy alta, son las variaciones en los tiempos de los relojes atómicos lo cual puede dañar la medición del tiempo entre el satélite y el GPS, pero como se dijo anteriormente son resultados exactos que estos pequeños errores no afectarían en su respuesta.

6 INGENIERIA DE SOFTWARE

6.1 REQUERIMIENTOS

6.1.6 Requerimientos funcionales

6.1.6.1 Requerimiento funcional 001

Identificador RF-001	**Nombre** Conectar GPS al sistema de escaneo.	**Sistema** Sistema de escaneo.
Categoría No visible	**Tipo** Necesario	**Prioridad** Alta
Requerimiento que lo utiliza RF-002	**Critico** Si	
Actor o Rol Aplicación.		
Entradas Ninguna	**Salidas** Mensaje de información indicando el estado del GPS (Conectado/No conectado).	
Descripción Se inicia la aplicación, a continuación se inicia la búsqueda de un dispositivo GPS bluetooth con el cual se obtienen las coordenadas de la ubicación geográfica de las redes inalámbricas encontradas.		
Curso de eventos 1. Se inicia la aplicación. 2. El sistema intenta emparejarse con el dispositivo GPS. 3. Se muestra un mensaje de éxito o fracaso de la conexión.		
Precondiciones Se inicia la aplicación.		
Pos condiciones El sistema se encuentra emparejado con un dispositivo GPS.		
Manejo de situaciones anormales (Casos de excepción) Si el sistema no encuentra un dispositivo GPS con el cual emparejarse, este mostrara un mensaje de información al usuario.		
Criterios de aceptación El sistema se encuentra emparejado con un dispositivo GPS.		

6.1.6.2 Requerimiento funcional 002

Identificador RF-002	**Nombre** Iniciar escaneo de redes.	**Sistema** Sistema de escaneo.
Categoría Visible	**Tipo** Necesario	**Prioridad** Alta
Requerimiento que lo utiliza RF-003 RF-004 RF-005 RF-006	**Critico** Si	
Actor o Rol Usuario del sistema		
Entradas Evento de clic sobre el botón “Escanear”.	**Salidas** Listado con la información de las redes inalámbricas asociadas.	
Descripción Para iniciar el escaneo el usuario debe hacer clic sobre el botón “Escanear”, a continuación se selecciona la frecuencia con la que se ejecutara el escaneo. Finalmente el usuario hace clic sobre el botón “Iniciar escaneo” para comenzar la búsqueda de las redes inalámbricas.		
Curso de eventos 1. El usuario hace clic sobre el botón “Escanear”. 2. Luego debe indicar la frecuencia del escaneo que se desea ejecutar, los valores son “Escanear una vez” o escanear “Periódicamente”. 3. Si se selecciona la opción de escanear de forma periódica, es necesario indicar un intervalo de tiempo, cada vez que ese intervalo se complete el escaneo se ejecutara de nuevo. 4. Se inicia el escaneo dando clic en el botón “Iniciar Escaneo”		
Precondiciones La aplicación se está ejecutando.		
Pos condiciones Se obtiene un listado con las redes inalámbricas encontradas y la información asociada a cada una de estas.		
Manejo de situaciones anormales (Casos de excepción) Si el sistema no encuentra ninguna red inalámbrica se muestra un mensaje de advertencia informando esta situación.		
Criterios de aceptación Se tiene una lista con la información de las redes inalámbricas encontradas.		

6.1.6.3 Requerimiento funcional 003

Identificador RF-003	**Nombre** Listar redes inalámbricas.	**Sistema** Sistema de escaneo.
Categoría Visible	**Tipo** Necesario	**Prioridad** Alta
Requerimiento que lo utiliza RF-004 RF-005	**Critico** Si	
Actor o Rol Aplicación.		
Entradas Finalización exitosa del requerimiento RF-002	**Salidas** La aplicación muestra el listado creado en el requerimiento anterior en la interfaz grafica de usuario.	
Descripción Si el requerimiento RF-002 termina exitosamente, se muestran las redes encontradas en la interfaz grafica de usuario.		
Curso de eventos 1. RF-002 termina exitosamente. 2. Se muestran las redes encontradas en la interfaz grafica de usuario.		
Precondiciones RF-002 termina exitosamente.		
Pos condiciones La interfaz grafica de usuario muestra un listado con las redes inalámbricas encontradas.		
Manejo de situaciones anormales (Casos de excepción) Si RF-002 no termino correctamente, no se muestra ningún tipo de información.		
Criterios de aceptación La interfaz grafica de usuario muestra un listado con las redes inalámbricas encontradas.		

6.1.6.4 Requerimiento funcional 004

Identificador RF-004	**Nombre** Guardar resultados del escaneo.	**Sistema** Sistema de escaneo.
Categoría Visible	**Tipo** Necesario	**Prioridad** Alta
Requerimiento que lo utiliza RF-006 RF-007	**Critico** Si	
Actor o Rol Usuario del sistema.		
Entradas Evento de clic sobre el botón “Guardar Resultados”.	**Salidas** Archivo de extensión .wns con la información de las redes inalámbricas escaneadas.	
Descripción Después que el proceso de escaneo descrito en el RF-002 finaliza correctamente, el usuario puede guardar los resultados del escaneo para un análisis posterior.		
Curso de eventos 1. El usuario hace clic en el botón “Guardar Resultados”. 2. El usuario selecciona la ubicación donde desea almacenar el archivo. 3. El usuario ingresa el nombre del archivo. 4. El usuario hace clic en el botón “Guardar”.		
Precondiciones RF-002 termina exitosamente.		
Pos condiciones El sistema crea un archivo de extensión .wns que contiene la información de las redes inalámbricas escaneadas.		
Manejo de situaciones anormales (Casos de excepción) Si en el proceso de escaneo no se encontró ninguna red, el sistema muestra un mensaje indicando que no existen redes a guardar.		
Criterios de aceptación El archivo se encuentra en el directorio especificado y su contenido corresponde al último escaneo ejecutado.		

6.1.6.5 Requerimiento funcional 005

Identificador RF-005	**Nombre** Seleccionar red para ver información.	**Sistema** Sistema de escaneo.
Categoría Visible	**Tipo** Necesario	**Prioridad** Alta
Requerimiento que lo utiliza	**Critico** Si	
Actor o Rol Usuario del sistema.		
Entradas Evento de clic sobre el SSID que se muestra en la lista generada en RF-003	**Salidas** Información detallada de la red inalámbrica identificada por el SSID seleccionado.	
Descripción El usuario hace clic sobre el SSID con el objetivo de visualizar la información detallada de la red inalámbrica asociada a este.		
Curso de eventos 1. El usuario hace clic sobre el SSID de alguna de las redes inalámbricas identificadas. 2. El sistema muestra toda la información de la red seleccionada.		
Precondiciones RF-002 termino exitosamente.		
Pos condiciones Se muestra toda la información asociada al SSID seleccionado.		
Manejo de situaciones anormales (Casos de excepción)		
Criterios de aceptación El sistema muestra toda la información de la red.		

6.1.6.6 Requerimiento funcional 006

Identificador RF-006	**Nombre** Abrir archivo wns	**Sistema** Sistema de escaneo.
Categoría Visible	**Tipo** Opcional	**Prioridad** Baja
Requerimiento que lo utiliza	**Critico** No	
Actor o Rol Usuario del sistema.		
Entradas Evento de clic sobre el botón “Abrir archivo”.	**Salidas** Todo el contenido del archivo .wns se muestra en la interfaz grafica de usuario.	
Descripción El usuario puede abrir un archivo .wns creado en el RF-004 para visualizar la información asociada a este.		
Curso de eventos 1. El usuario hace clic sobre el botón “Abrir archivo”. 2. Se selecciona la ubicación del archivo. 3. Se hace clic en el botón “Abrir”. 4. El archivo se muestra en la interfaz grafica de usuario.		
Precondiciones Existe un archivo .wns para abrir.		
Pos condiciones El sistema muestra la información del archivo seleccionado.		
Manejo de situaciones anormales (Casos de excepción) Si el archivo .wns se encuentra corrupto se muestra al usuario un mensaje de error.		
Criterios de aceptación La interfaz grafica de usuario muestra toda la información del archivo seleccionado.		

6.1.6.7 Requerimiento funcional 007

Identificador RF-007	**Nombre** Detener escaneo.	**Sistema** Sistema de escaneo.
Categoría Visible	**Tipo** Necesario.	**Prioridad** Alta.
Requerimiento que lo utiliza RF-002	**Critico** Si	
Actor o Rol Usuario del sistema.		
Entradas Evento de clic sobre el botón “Detener escaneo”.	**Salidas**	
Descripción El usuario puede detener un escaneo que se está ejecutando con frecuencia periódica.		
Curso de eventos 1. El usuario hace clic sobre el botón “Detener escaneo”. 2. El escaneo se detiene.		
Precondiciones Se inicio un escaneo con frecuencia periódica.		
Pos condiciones El escaneo se detuvo.		
Manejo de situaciones anormales (Casos de excepción)		
Criterios de aceptación El escaneo se detuvo.		

6.1.6.8 Requerimiento funcional 008

Identificador RF-008	**Nombre** Abrir archivo wns.	**Sistema** Sistema de representación grafica.
Categoría Visible	**Tipo** Necesario.	**Prioridad** Alta.
Requerimiento que lo utiliza RF-009 RF-010	**Critico** Si	
Actor o Rol Usuario del sistema.		
Entradas Evento de clic sobre el botón “Abrir archivo”.	**Salidas** Mensaje de confirmación de la operación.	
Descripción Se debe abrir el archivo .wns generado en el sistema de escaneo para representar la información de este en un mapa.		
Curso de eventos 1. El usuario hace clic sobre el botón “Abrir archivo”. 2. Se selecciona la ubicación del archivo. 3. Se muestra un mensaje de confirmación de la operación.		
Precondiciones Existe un archivo .wns para abrir.		
Pos condiciones Se muestra un mensaje de confirmación de la operación.		
Manejo de situaciones anormales (Casos de excepción) Si no se tiene conexión a internet el usuario debe iniciar de nuevo el proceso de escaneo.		
Criterios de aceptación Se muestra un mensaje de éxito que indica que el archivo se abrió correctamente.		

6.1.6.9 Requerimiento funcional 009

Identificador RF-009	**Nombre** Ubicar red en mapa.	**Sistema** Sistema de representación grafica.
Categoría Visible	**Tipo** Necesario.	**Prioridad** Alta.
Requerimiento que lo utiliza RF-010	**Critico** Si	
Actor o Rol Usuario del sistema.		
Entradas RF-008 termino correctamente.	**Salidas** Un mapa que muestra la ubicación geográfica de las redes contenidas en el archivo .wns.	
Descripción Al terminar el requerimiento RF-008 de forma correcta, el sistema automáticamente crea un mapa con la ubicación geográfica de las redes contenidas en el archivo .wns.		
Curso de eventos 1. RF-008 termina exitosamente. 2. El sistema crea un mapa con la ubicación geográfica de las redes contenidas en el archivo .wns.		
Precondiciones RF-008 termina exitosamente.		
Pos condiciones Se muestra un mapa con la ubicación geográfica de las redes contenidas en el archivo wns.		
Manejo de situaciones anormales (Casos de excepción) Si no se tiene conexión a internet el usuario debe iniciar de nuevo el proceso de escaneo.		
Criterios de aceptación Se muestra un mapa con la ubicación geográfica de las redes contenidas en el archivo .wns.		

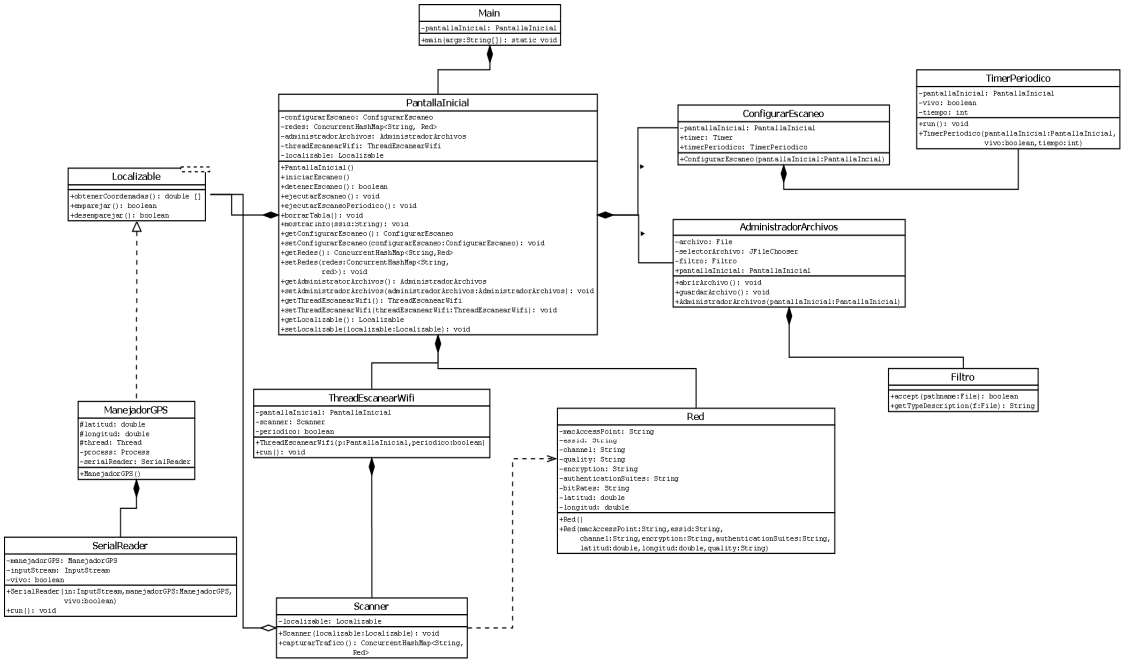
6.1.7 Requerimientos No funcionales

ID	Requerimiento	Prioridad	Casos de uso afectados
Sistema de representación grafica			
RNF-001	El sistema debe visualizarse de forma correcta en los principales navegadores como internet explorer, mozilla firefox y apple safari.	ALTA	Caso de uso 7 Caso de uso 8
RNF-002	La interfaz grafica de usuario debe ser intuitiva.	ALTA	Caso de uso 7 Caso de uso 8
RNF-003	La combinación de colores usada en los mapas debe permitir distinguir visualmente la información presentada.	ALTA	Caso de uso 8
RNF-004	El tiempo de respuesta a una petición hecha a la aplicación debe ser máximo 7 segundos.	ALTA	Caso de uso 7 Caso de uso 8
Sistema de escaneo			
RNF-005	La interfaz grafica de usuario debe ser intuitiva para facilitar el uso de la aplicación	ALTA	Caso de uso 1 Caso de uso 2 Caso de uso 3 Caso de uso 4 Caso de uso 5 Caso de uso 6
RNF-006	La información de coordenadas geográficas se mantendrá con la misma precisión desde el momento en el que se obtiene del	ALTA	TODOS

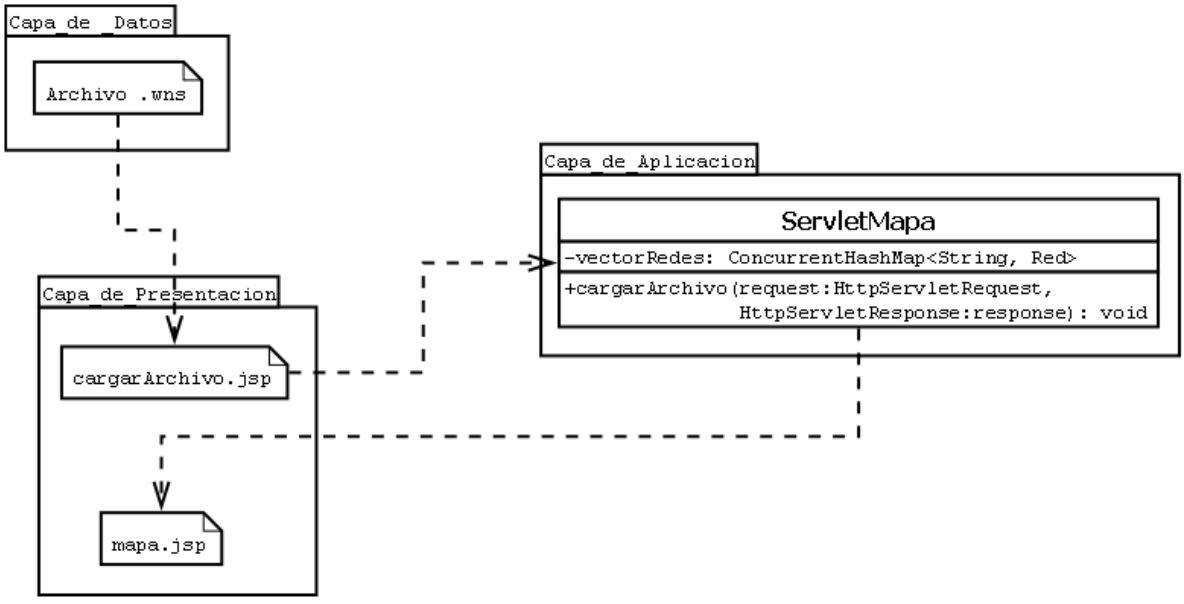
	receptor GPS hasta que se guarda en el archivo WNS.		
RNF-007	La aplicación será usada por personas que realicen trabajos de wardriving, campañas de sensibilización e investigaciones sobre los comportamientos de los usuarios respecto al manejo y la seguridad que se tiene con las redes inalámbricas.	ALTA	TODOS
RNF-008	Para que la aplicación funcione correctamente el usuario deberá contar el Java Runtime Environment versión 6 o superior	ALTA	TODOS

6.2 DIAGRAMA DE CLASES

6.2.6 Diagrama de clases aplicación Escaneo de redes inalámbricas



6.2.7 Diagrama de clases del sistema de representación grafica



6.3 CASOS DE USO

6.3.6 *Caso de uso 1*

Caso de Uso 1	Conectar GPS con la aplicación	
Objetivo	Emparejar el receptor GPS con la aplicación para que esta pueda obtener las coordenadas aproximadas de las redes inalámbricas que se detecten.	
Precondiciones	El receptor GPS se encuentra emparejado con el equipo en el que corre la aplicación vía Bluetooth.	
Condiciones de éxito	El sistema debe mostrar el receptor GPS como conectado y debe mostrar las coordenadas asociadas a una red inalámbrica cuando se realice el escaneo.	
Condiciones de fracaso	No se puede abrir un puerto COM para transferir los datos del receptor GPS al equipo que corre la aplicación.	
Actor Principal	Aplicación	
Actores Secundarios	No Aplica	
Disparador	Se inicia la aplicación.	
Descripción	**Paso**	**Acción**
	1	El usuario inicia la aplicación (Se deben tener permisos de superusuario para ejecutarla).
	2	La aplicación inicia el proceso de emparejamiento con el receptor GPS, intentando abrir un puerto COM.
	3	La aplicación muestra un mensaje confirmando que se ha detectado el receptor GPS.
Extensiones	**Paso**	**Acción**
	1a	No se tienen permisos del superusuario. 1a1. La aplicación inicia correctamente pero no se pueden escanear redes inalámbricas.
	2a	La aplicación no se puede emparejar con el dispositivo bluetooth. 2a1. La aplicación muestra un mensaje de error informando la situación.

6.3.7 *Caso de uso 2*

Caso de Uso 2	Escanear redes inalámbricas	
Objetivo	Detectar las redes inalámbricas que se encuentran cercanas a la posición del usuario.	
Precondiciones	La aplicación está corriendo. Un receptor GPS se encuentra emparejado con la aplicación.	
Condiciones de éxito	Se muestra un listado con las redes inalámbricas detectadas.	
Condiciones de fracaso	El sistema no encuentra ninguna red inalámbrica.	
Actor Principal	Usuario de la aplicación	
Actores Secundarios	No Aplica	
Disparador	Se hace clic en el botón “Escanear” y se seleccionan los parámetros del escaneo.	
Descripción	**Paso**	**Acción**
	1	El usuario hace clic en el botón “Escanear”.
	2	El programa muestra un cuadro para seleccionar si se desea escanear una vez o hacer un escaneo periódico.
	3	El usuario hace clic en el botón “Iniciar Escaneo”.
	4	El sistema busca las redes inalámbricas cercanas.
Extensiones	**Paso**	**Acción**
	4a	No se pudo realizar el escaneo. 4a1. Si no se pudo realizar el escaneo es porque la aplicación se ejecuto sin permisos de superusuario.

6.3.8 *Caso de uso 3*

Caso de Uso 3	Listar redes inalámbricas.	
Objetivo	Con este requerimiento se busca mostrar al usuario los resultados de la búsqueda realizada en el caso de uso 2.	
Precondiciones	La aplicación está abierta. Se realizo un escaneo de redes inalámbricas.	
Condiciones de éxito	Los nombres de todas las redes inalámbricas detectadas se muestran en una lista.	
Condiciones de fracaso	Si el caso de uso 2 no termino correctamente, no se muestra ningún tipo de información.	
Actor Principal	Aplicación	
Actores Secundarios	No Aplica	
Disparador	El caso de uso numero 2 termina correctamente.	
Descripción	**Paso**	**Acción**
	1	Al terminar el caso de uso numero 2 se cargan los nombres de las redes en una lista.

6.3.9 *Caso de uso 4*

Caso de Uso 4	Mostrar información de una red inalámbrica.	
Objetivo	Con este requerimiento se busca mostrar la información de una red en el momento en el que el usuario de la aplicación haga clic sobre el nombre que se encuentra en la lista generada en el caso de uso numero tres.	
Precondiciones	Existe por lo menos una red inalámbrica en el listado resultante del caso de uso numero tres.	
Condiciones de éxito	Al hacer clic sobre un nombre de la lista, en la parte inferior de la pantalla se muestra toda la información asociada a esta red.	
Condiciones de fracaso		
Actor Principal	Usuario del sistema.	
Actores Secundarios	No Aplica	
Disparador	El usuario hace clic sobre un nombre de red.	
Descripción	**Paso**	**Acción**
	1	El usuario hace clic sobre un nombre de red.
	2	El sistema muestra la información asociada a esta red.

6.3.10 *Caso de uso 5*

Caso de Uso 5	Guardar resultados del escaneo.
Objetivo	Este requerimiento sirve para exportar a un archivo los resultados del escaneo con el fin de usarlos en el programa que pinta las redes en un mapa.
Precondiciones	El escaneo encontró al menos una red inalámbrica.

Condiciones de éxito	El sistema genera un archivo de extensión wns con la información de las redes encontradas al momento de guardar la información.
	
	El formato del archivo WNS es el siguiente:
	• Por cada red inalámbrica encontrada se empieza con el texto ***Red.***
	• Luego en líneas aparte se incluyen los campos SSID, Latitud, Longitud, Dirección MAC, Canal, Protocolo de cifrado, Suite de autenticación y Calidad de la señal.
	
	A continuación se muestra un ejemplo de un archivo WNS que contiene dos redes inalámbricas:
	
	`Red`
	`SEGAFREDO`
	`4.6671366691589355`
	`-74.05359649658203`
	`00:24:D2:AE:6A:E6`
	`2.412 GHz (Channel 1)`
	`WPA Version 1`
	`PSK`
	`Quality=38/100`
	`Red`
	`Ivoice`
	`4.667553424835205`
	`-74.05390930175781`
	`00:19:AA:15:20:90`
	`2.412 GHz (Channel 1)`
	`IEEE 802.11i/WPA`
	`PSK`
	`Quality=42/100`

Condiciones de fracaso	El sistema no puede guardar el archivo con la información de las redes encontradas.

Actor Principal	Usuario de la aplicación.	
Actores Secundarios	No Aplica	
Disparador	El usuario hace clic en el botón guardar.	
Descripción	**Paso**	**Acción**
	1	El usuario hace clic en el botón de guardar.
	2	El sistema muestra un cuadro de dialogo en el que el usuario busca el directorio donde quiere guardar el archivo y le da un nombre a este.
	3	El sistema guarda el archivo en la ruta especificada.

6.3.11 *Caso de uso 6*

Caso de Uso 6	Abrir archivo .wns	
Objetivo	Si el usuario desea ver en la aplicación la información capturada previamente, puede abrir el archivo guardado.	
Precondiciones	Se tiene un archivo .wns para abrir con la aplicación.	
Condiciones de éxito	El archivo .wns se carga y se muestra la información contenida en este.	
Condiciones de fracaso	El archivo esta corrupto y no se puede mostrar.	
Actor Principal	Usuario de la aplicación	
Actores Secundarios	No Aplica	
Disparador	El usuario hace clic en el botón “Abrir Archivo”	
Descripción	**Paso**	**Acción**
	1	El usuario hace clic en el botón “Abrir archivo”.
	2	Se muestra un cuadro de dialogo en el que el usuario puede seleccionar el archivo .wns a abrir.
	3	El sistema muestra la información del archivo en la aplicación.
Extensiones	**Paso**	**Acción**
	4a	El archivo esta corrupto y no se puede abrir. 4a1. Si el archivo está dañado se muestra al usuario un mensaje de error.

6.3.12 *Caso de uso 7*

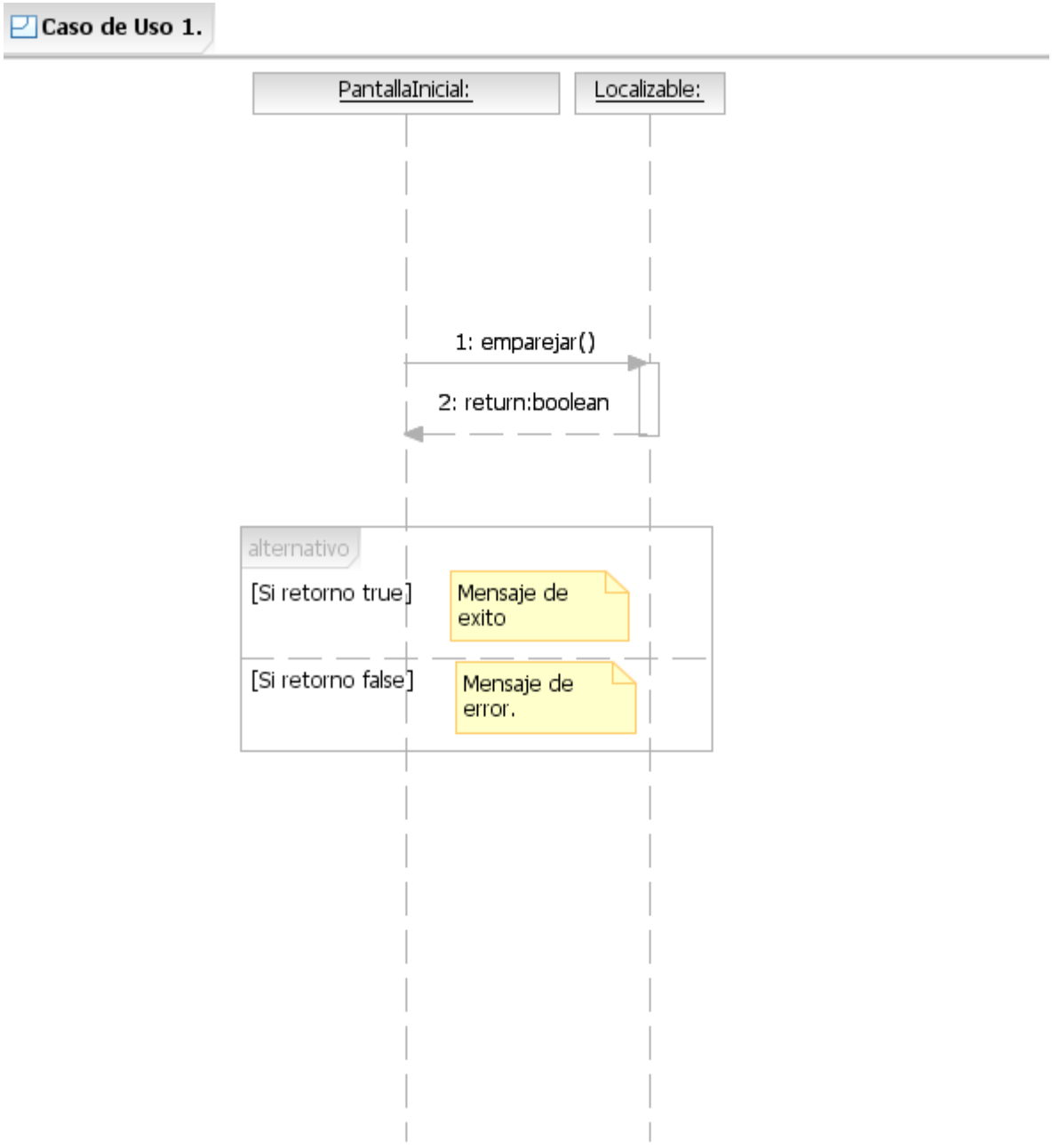
Caso de Uso 7	Abrir archivo .wns	
Objetivo	El usuario carga en sistema de representación grafica el archivo wns generado en el sistema de escaneo.	
Precondiciones	Se tiene un archivo .wns para abrir con la aplicación.	
Condiciones de éxito	El archivo .wns se carga correctamente	
Condiciones de fracaso	Se pierde conectividad con el servidor.	
Actor Principal	Usuario de la aplicación	
Actores Secundarios	No Aplica	
Disparador	El usuario hace clic en el botón “Subir Archivo”	
Descripción	**Paso**	**Acción**
	1	El usuario hace clic en el botón “Subir archivo”.
	2	Se muestra un cuadro de dialogo en el que el usuario puede seleccionar el archivo .wns a cargar.
	3	El archivo se carga en el sistema.
Extensiones	**Paso**	**Acción**
	2a	Se pierde la conexión con el servidor. 2a1. El usuario debe iniciar el proceso de nuevo tan pronto que recupere la conectividad con el servidor

6.3.13 *Caso de uso 8*

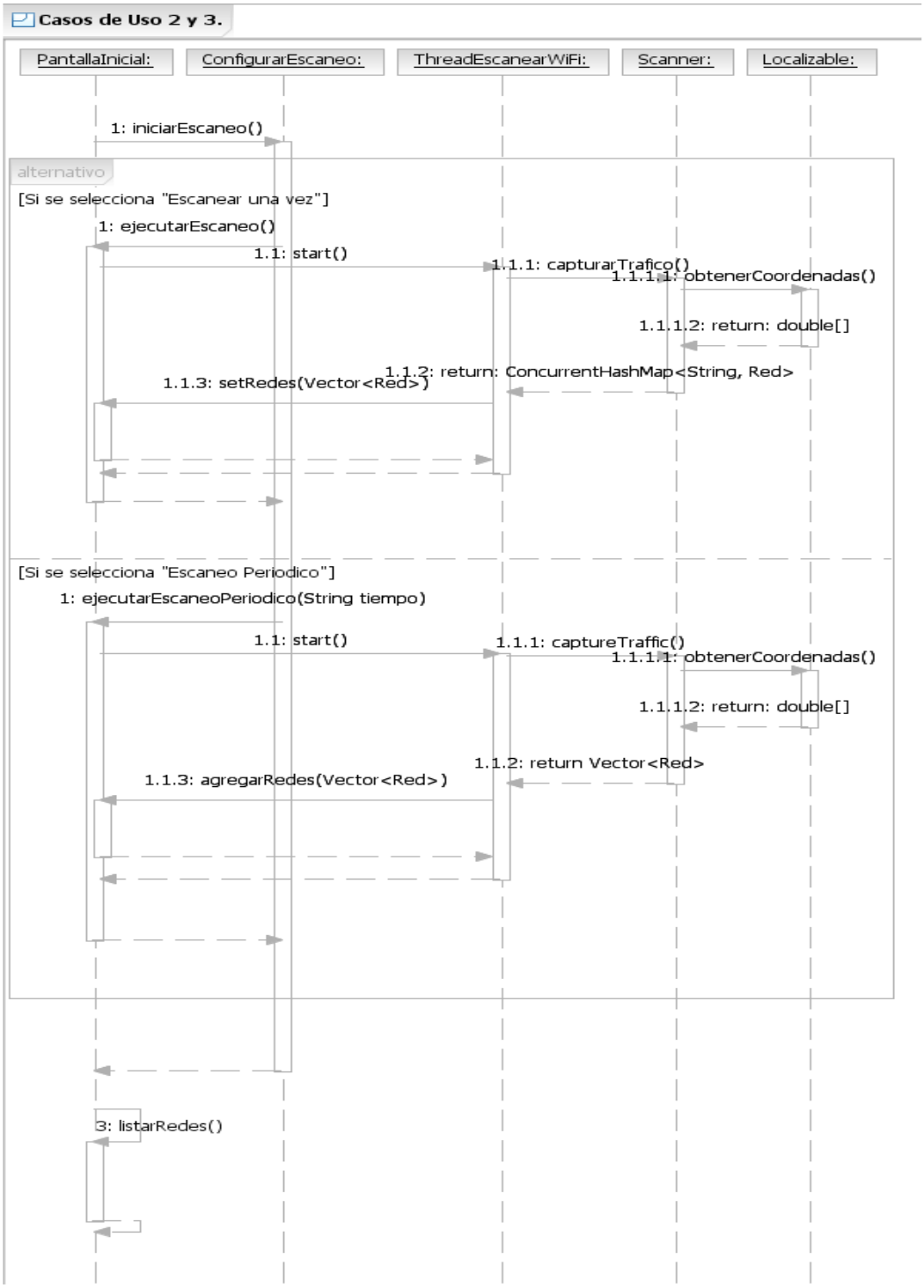
Caso de Uso 8	Ubicar red en mapa	
Objetivo	Al terminar el caso de Uso 7 de forma correcta, el sistema automáticamente crea un mapa con la ubicación geográfica de las redes contenidas en el archivo wns.	
Precondiciones	Se ha cargado de forma correcta un archivo .wns en el sistema.	
Condiciones de éxito	Se muestra un mapa con la ubicación geográfica de las redes contenidas en el archivo.	
Condiciones de fracaso	Se pierde conectividad con el servidor	
Actor Principal	Usuario de la aplicación	
Actores Secundarios	No Aplica	
Disparador	El caso de Uso 7 finaliza correctamente.	
Descripción	**Paso**	**Acción**
	1	El caso de Uso 7 finaliza correctamente.
	2	El sistema crea un mapa con la ubicación geográfica de las redes contenidas en el archivo wns.
Extensiones	**Paso**	**Acción**
	2a	Se pierde la conexión con el servidor. 2a1. El usuario debe iniciar el proceso de nuevo tan pronto que recupere la conectividad con el servidor

6.4 DIAGRAMA DE SECUENCIA

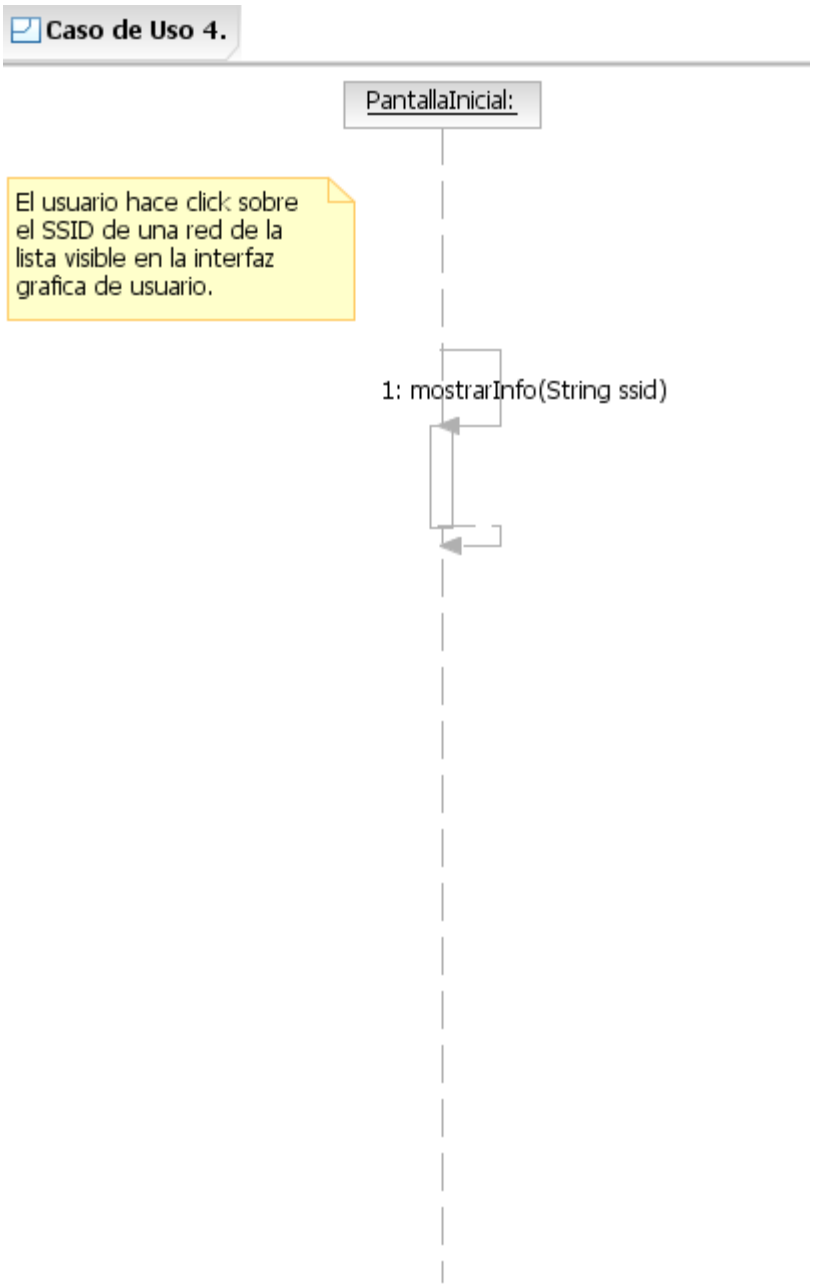
6.4.6 *Caso de uso 1*



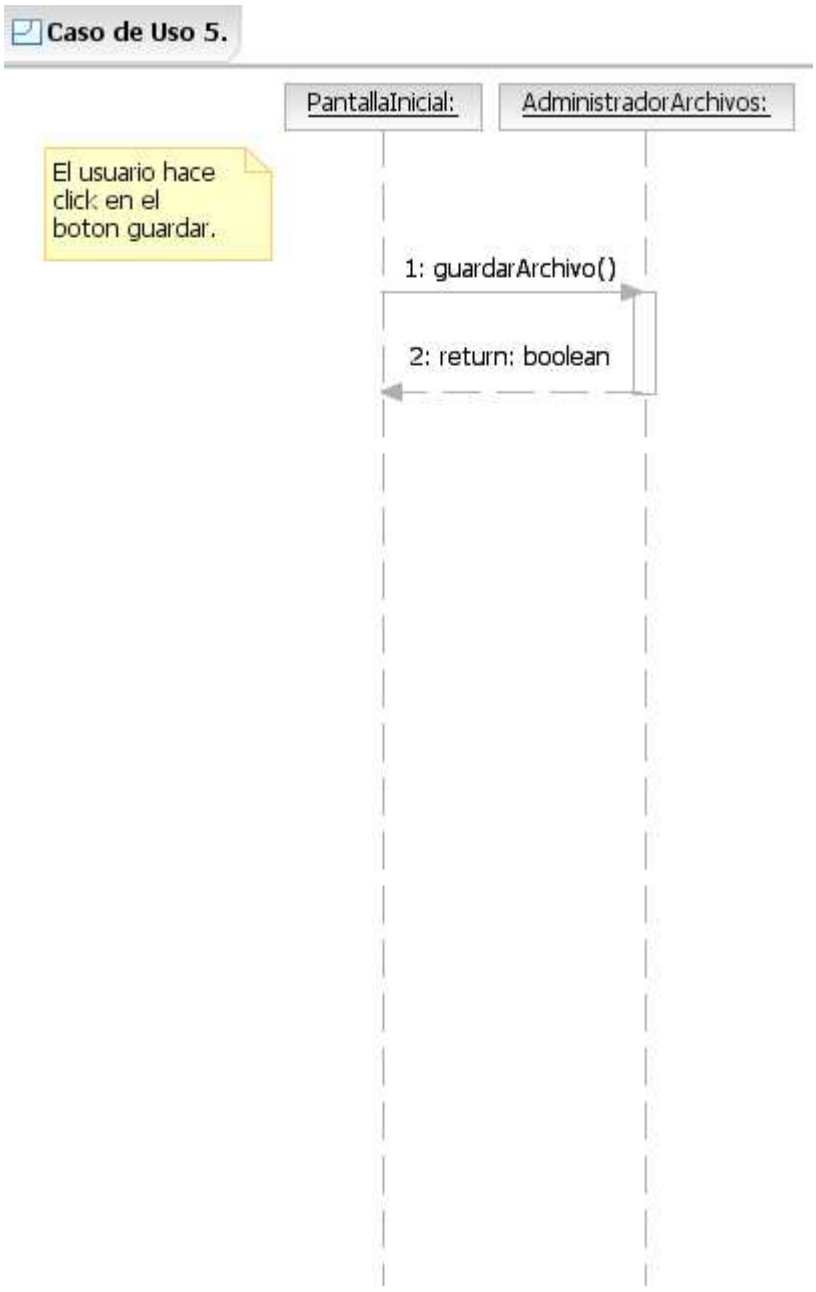
6.4.7 *Caso de uso 2-3*



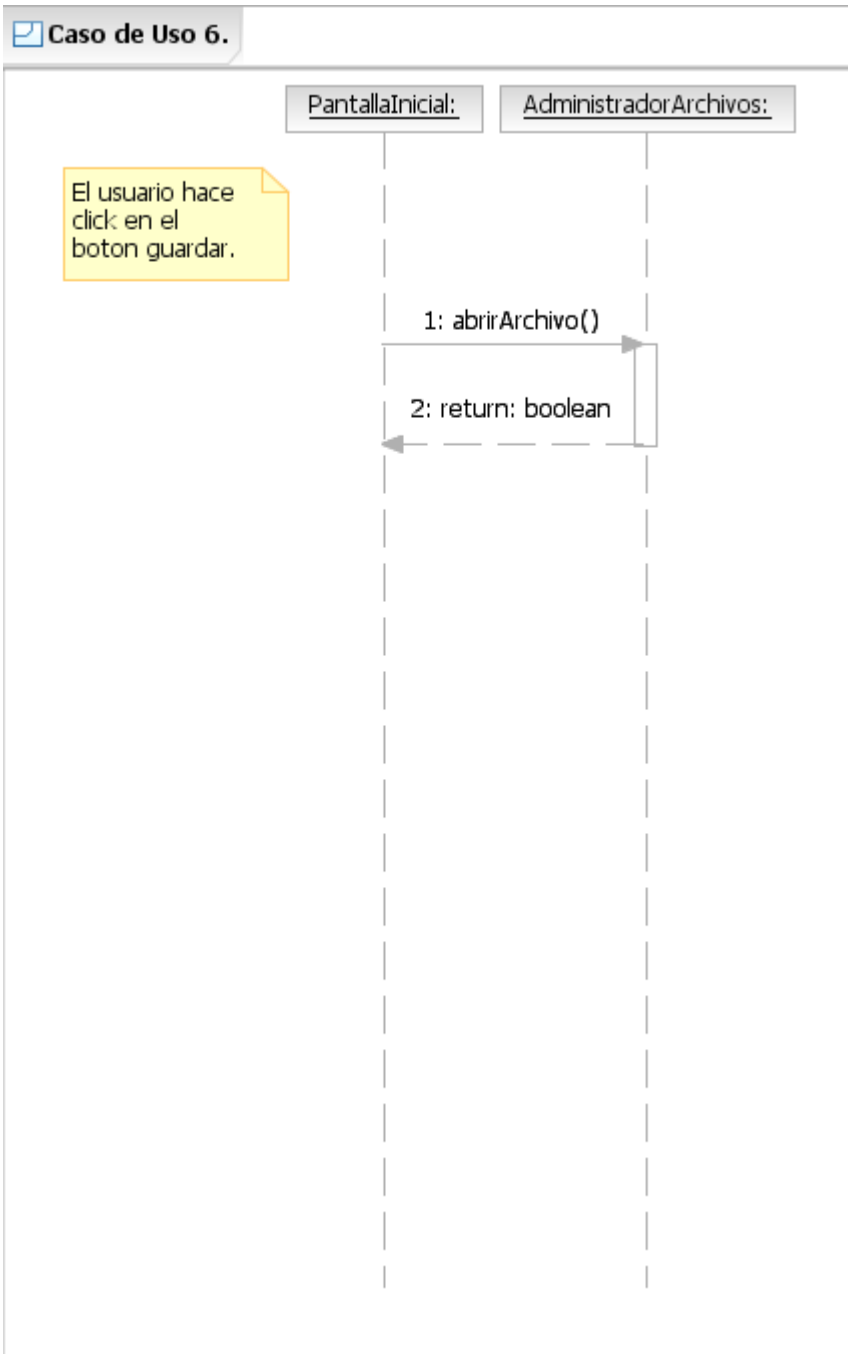
6.4.8 *Caso de uso 4*



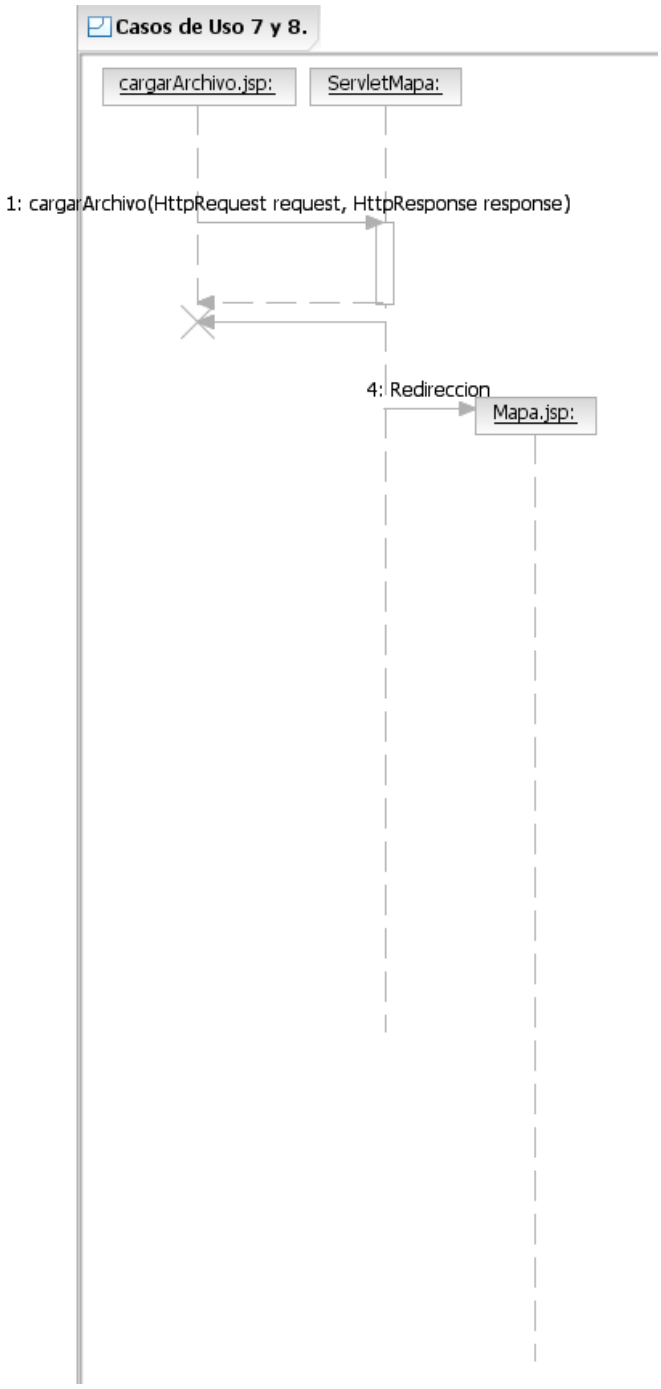
6.4.9 *Caso de uso 5*



6.4.10 *Caso de uso 6*



6.4.11 *Caso de uso 7-8*



7 SOLUCION AL PROBLEMA

Después de realizar un análisis sobre las redes inalámbricas 802.11 y los métodos existentes para obtener información sobre estas de forma efectiva, así como de los distintos APIS de Google Maps, se diseño la siguiente solución que permite cumplir con los objetivos del proyecto.

1. El levantamiento de información de redes inalámbricas en las tres zonas de Bogotá definidas en el alcance del presente documento, se hará en dos etapas, como se explica a continuación:

    a. **Etapa de reconocimiento:** Esta etapa consiste en recorrer las zonas residencial, comercial y de negocios usando la aplicación desarrollada para escanear en busca de redes inalámbricas.
    b. **Etapa de análisis:** en esta etapa se usara la aplicación que ubica geográficamente las redes en Google Maps para poder analizar la distribución de las redes en la ciudad así como la configuración de estas.

2. Las aplicaciones usadas para escanear y para ubicar geográficamente las redes serán desarrolladas de forma independiente, una como aplicación de escritorio (Sistema de escaneo) y la otra como aplicación Web (Sistema de representación grafica). Se decidió abordar el problema de esta forma para que los usuarios puedan graficar los resultados de sus búsquedas de redes inalámbricas desde cualquier lugar en el que tengan una conexión a internet. Además, el API Web de Google Maps provee una mayor flexibilidad (navegación por el mapa, mapas satelitales y de relieve, etc.) que el API de imágenes estáticas.

3. Para geolocalizar las redes inalámbricas escaneadas se usara un receptor GPS bluetooth, este dispositivo se conecta a los satélites del sistema GPS y transmite las coordenadas a un computador con el que se encuentre emparejado, esta transmisión de coordenadas se realiza una vez por segundo. Esto permite ubicar de forma rápida y precisa las redes que se van encontrando.

4. Con el fin de ubicar las redes con la mayor precisión posible se recorrerá la zona varias veces, midiendo la intensidad de la señal de estas en cada pasada. Se tomara como medición definitiva la muestra que tenga la señal más alta.

5. Para obtener la información de las redes inalámbricas en la aplicación de escaneo se usara el comando de Linux iwlist, este muestra la información de los Access Points que están al alcance de la tarjeta de red inalámbrica del dispositivo desde el que se ejecuta el comando. Debido a que la información que muestra el comando es dependiente de la tarjeta de red del equipo, se decidió usar un equipo que tenga la tarjeta de red Intel ProWireless 3945abg.

En las pruebas hechas con distintas tarjetas inalámbricas se concluyo que esta es la que ofrece más información.

8 RESULTADOS PRUEBAS

8.1 OBJETIVOS

- Validar el funcionamiento de la aplicación (Sistema de escaneo)
- Recopilar información arrojada por la aplicación (Sistema de Escaneo)
- Realizar escaneo de redes inalámbricas en tres sectores de la ciudad
- Realizar un análisis de la información arrojada por la aplicación durante los escaneo.
- Brindar al usuario un panorama de la importancia y utilidad que tiene la información arrojada por el sistema de escaneo.

8.2 HARDWARE

Sistema Operativo	Ubuntu
Tarjeta de Red Inalámbrica	Tarjeta de Red Intel(R) PRO/ wireless 3945ABG Network Connection
GPS	HOLUX M-1200
Software de Escaneo	Sistema de Escaneo realizado en esta Tesis

Tabla 5. Hardware utilizado en las Pruebas

8.3 DESCRIPCION

La prueba consistió en realizar un escaneo de redes inalámbricas a través de la técnica Wardriving, este recorrido se realizo en tres lugares diferentes de la ciudad (Bogotá):

- Una zona residencial (Ciudad Salitre)
- Una zona Empresaria (calle 100 desde carrera 9 , hasta la carrera 7)
- Una zona comercial (Zona T y sus alrededores).

Durante la captura se obtuvieron los siguientes datos de las redes:

- ESSID
- Latitud
- Longitud

- MAC
- Channel
- Encription
- Authentication
- Quality

8.4 RESULTADOS SECTOR RESIDENCIAL

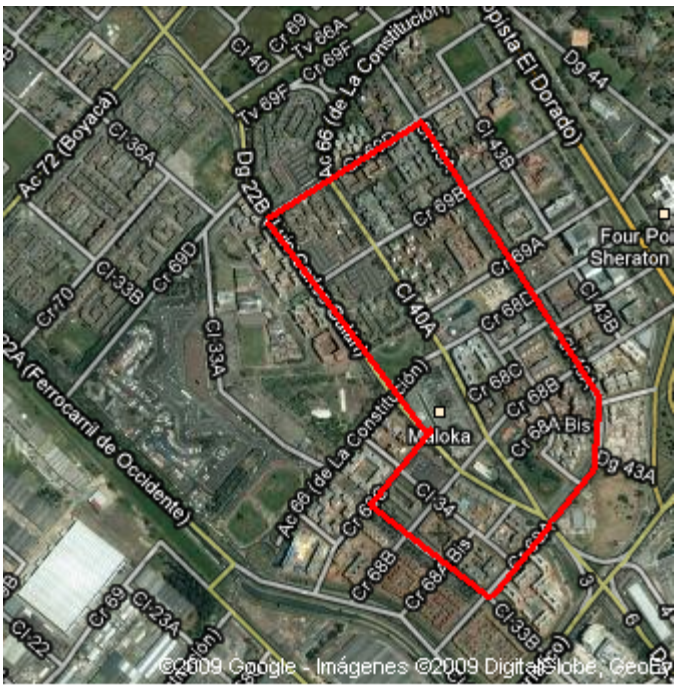


Ilustración 38. Sector residencial Ciudad Salitre

Control de Acceso

Con la información obtenida se puede identificar que el cifrado de datos en las redes inalámbricas de Salitre es Bueno. Se infiere por la cantidad de redes que utilizan el estándar WPA. WAP (Acceso Protegido de Fidelidad inalámbrica). *Ver Sección Seguridad y Autenticación.*

Encripción	Cantidad
D:"UNE_EPM_CAVIE	1
IEEE 802.11i/WPA	11
Unknown: 2D1A2C0	1
WPA Versión 1	58
Total general	**71**

Tabla 6. Resultado Control De Acceso Residencial

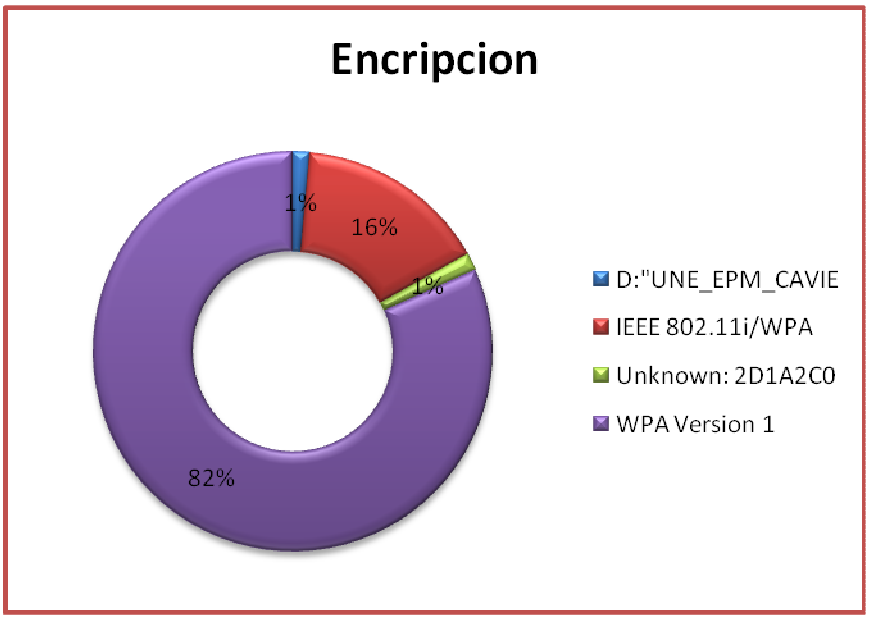


Ilustración 39. Resultados control de Acceso Residencial

Autenticación

Con esta información obtenida se observa que todas las redes capturadas con la herramienta en el sector de salitre utilizan la modalidad de red casera (PSK), quien exige contraseña para la autenticación.

Autenticación	Cantidad
PSK	71
Total general	**71**

Tabla 7. Resultados de autenticación residencial

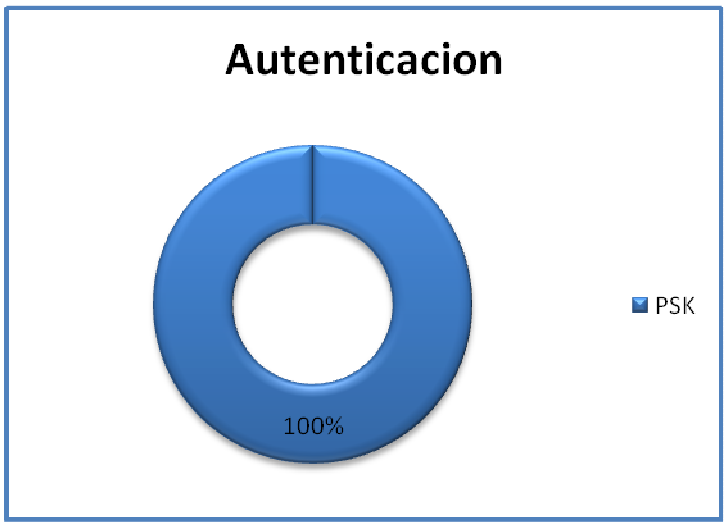


Ilustración 40. Resultados autenticación residencial

8.5 RESULTADO SECTOR COMERCIAL

Ilustración 41. Sector comercial (zona T)

Control de Acceso

Con la información obtenida se puede identificar que el cifrado de datos en las redes inalámbricas de Andino y Atlantis es Bueno. Se infiere por la cantidad de redes que utilizan el estándar WPA, pero adicionalmente se puede observar por la cantidad aceptable de redes con el protocolo de acceso 802.11X. *Ver Sección Seguridad y Autenticación.*

Tipo Encripción	Cantidad
IEEE 802.11i/WPA	6
Unknown: 2D1A4E1	1
Unknown: 2D1AEC0	3
WPA Version 1	25
Total general	**35**

Tabla 8. Sector comercial (zona T)

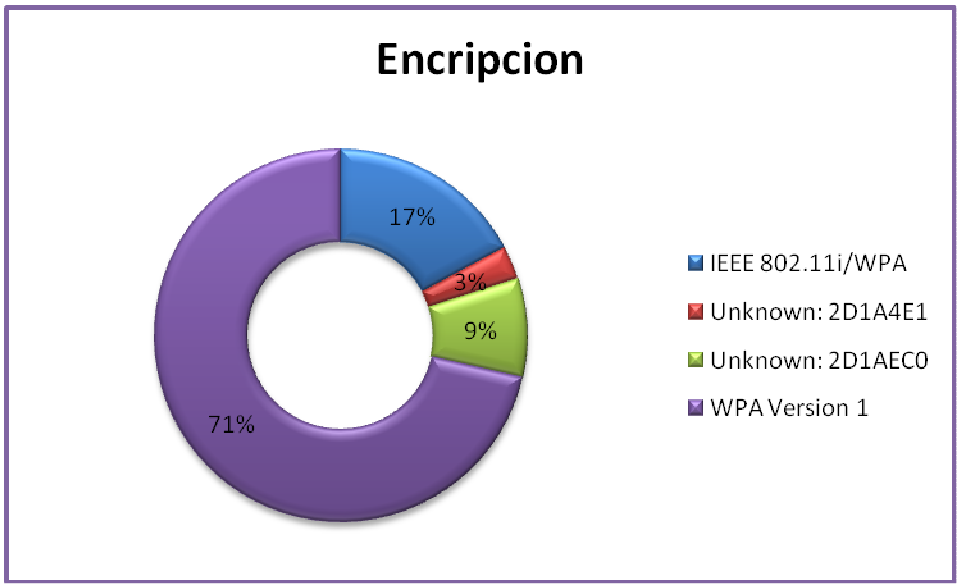


Ilustración 42. Sector comercial (zona T)

Autenticación

Con esta información obtenida se observa que todas las redes capturadas con la herramienta en el sector de Andino y Atlantis utilizan la modalidad de red casera (PSK), quien exige contraseña para la autenticación.

Rótulos de fila	Cuenta de Autenticación
PSK	35
Total general	**35**

Tabla 9 Resultados Autenticación Comercial

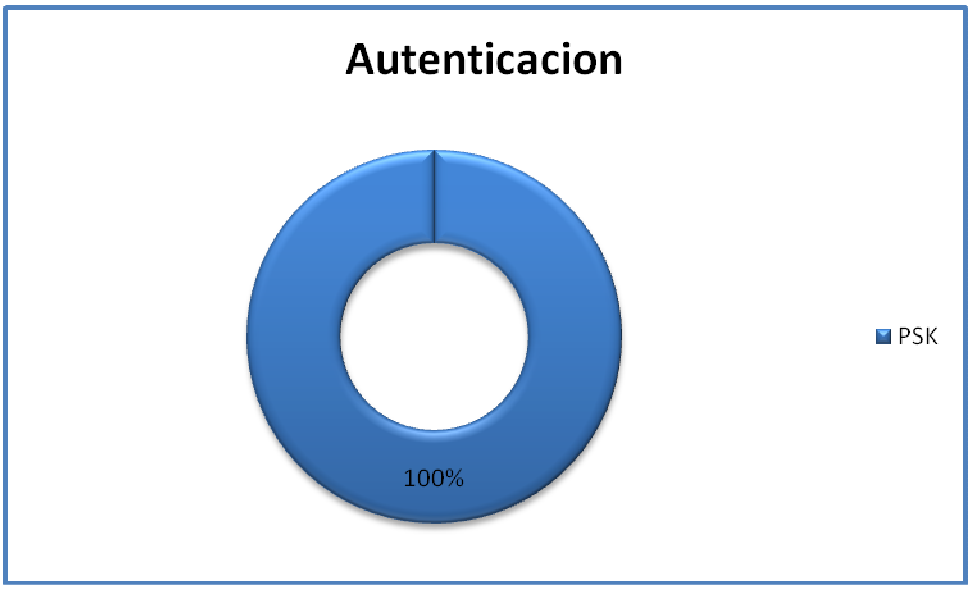


Ilustración 43. Resultados Autenticación comercial

8.6 RESULTADOS SECTOR EMPRESARIAL

Ilustración 44. Sector Empresarial Calle 100

Control de Acceso

Con la información obtenida se puede identificar que el cifrado de datos en las redes inalámbricas del sector empresarial es Muy Bueno. Se infiere por la cantidad de redes que utilizan el estándar WPA, pero adicionalmente se puede observar por la cantidad buena de redes con el protocolo de acceso 802.11X. *Ver Sección Seguridad y Autenticación.*

Encripción	Cantidad
D:"ANDINA BIENES	2
D:"ATELIER GOURM	1
D:"FENIX INGENIE	1
D:"MEIERS"	1
D:"OCHA-CHARLIE-	1
D:"P5_ORIENTE"	1
IEEE 802.11i/WPA	154
Unknown: 2D1A0C1	2
Unknown: 2D1A1C1	6
Unknown: 2D1A1E1	1
Unknown: 2D1A2C0	4
Unknown: 2D1A4C1	12
Unknown: 2D1A4E1	4
Unknown: 2D1A6C1	5
Unknown: 2D1A6E1	3
Unknown: 2D1A7C1	3
Unknown: 2D1A7E1	2
Unknown: 2D1AEC0	1
Unknown: 2D1AEE1	7
WPA Version 1	490
Total general	**701**

Tabla 10. Sector Empresarial

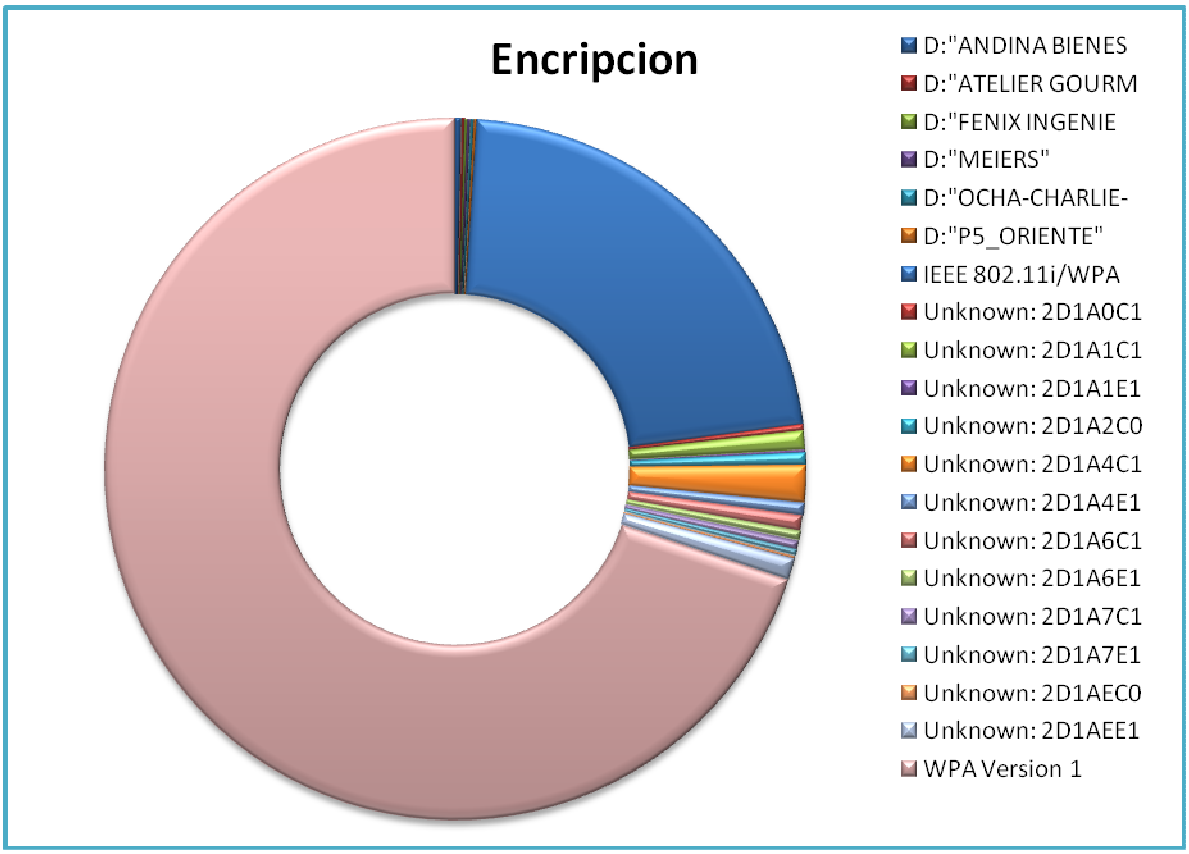


Ilustración 45. Resultados control de acceso empresarial

Nota: Como anotación especial, se puede observar que al parecer existen protocolos o estándares de autenticación personalizados. El dato "Unknown: 2D1A4C1" se repitió 12 veces.

Autenticación

Con esta información obtenida se observa que la mayoría de las redes capturadas con la herramienta en el sector empresarial utilizan la modalidad de red casera (PSK) y un porcentaje pequeño utiliza modalidad red Empresarial (con servidor RADIUS).

Autenticación	Cantidad
802.1	42
PSK	658
Total general	**700**

Tabla 11. Resultados Autenticación Total

Ilustración 46. Resultado Autenticación total

En general se puede concluir que la gran mayoría de las redes inalámbricas, sin importar sector, utilizan el estándar WPA para el control de acceso.

Encripción	Cantidad
D:"ANDINA BIENES	2
D:"ATELIER GOURM	1
D:"FENIX INGENIE	1
D:"MEIERS"	1
D:"OCHA-CHARLIE-	1
D:"P5_ORIENTE"	1
D:"UNE_EPM_CAVIE	1
IEEE 802.11i/WPA	171
Unknown: 2D1A0C1	2
Unknown: 2D1A1C1	6
Unknown: 2D1A1E1	1
Unknown: 2D1A2C0	5
Unknown: 2D1A4C1	12
Unknown: 2D1A4E1	5
Unknown: 2D1A6C1	5
Unknown: 2D1A6E1	3
Unknown: 2D1A7C1	3
Unknown: 2D1A7E1	2
Unknown: 2D1AEC0	4
Unknown: 2D1AEE1	7
WPA Version 1	573
(en blanco)	
Total general	**807**

Tabla 12. Resultado Control de Acceso Total

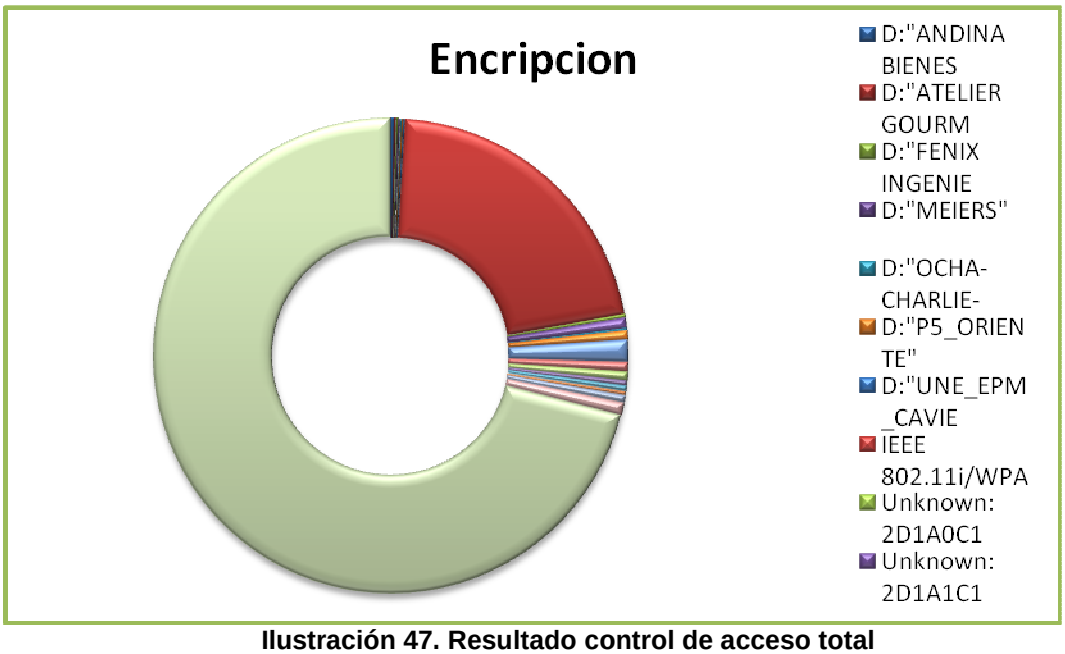


Ilustración 47. Resultado control de acceso total

Adicionalmente se puede observar que en el 95% de las redes inalámbricas de la cuidad se utiliza el estándar de autenticación en modalidad Casera, es decir con contraseña

Autenticación	Cantidad
802.1	42
PSK	764
Total general	**806**

Tabla 13. Resultados Autenticación Empresarial

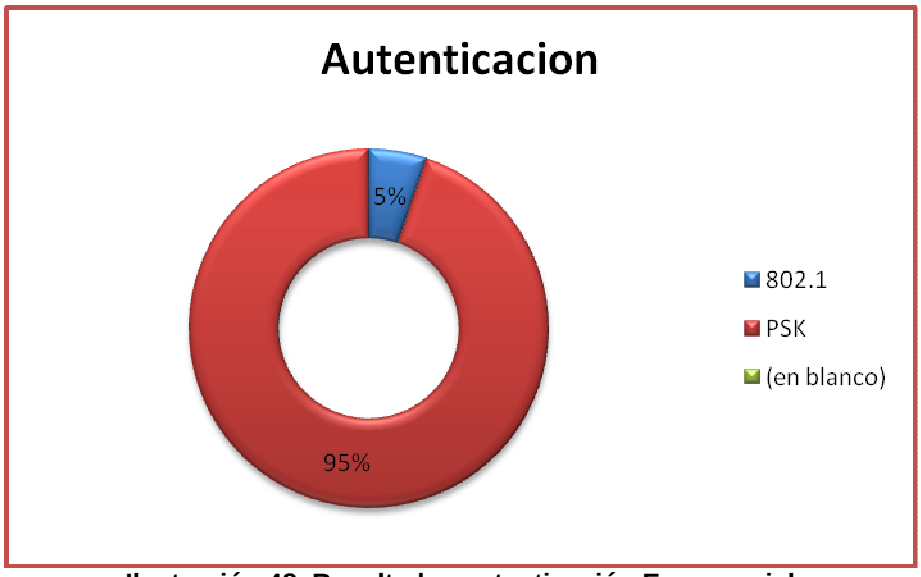


Ilustración 48. Resultados autenticación Empresarial

9 CONCLUSIONES

El diseño de un sistema de escaneo brinda la posibilidad de identificar las redes inalámbricas con sus respectivos detalles y configuraciones. Herramienta útil para quienes hacen uso de este tipo de tecnologías inalámbricas, manipulan la información brindada en técnicas como wardriving, campañas de sensibilización e investigaciones sobre los comportamientos de los usuarios respecto al manejo y la seguridad que se tiene con las redes inalámbricas. La posibilidad de visualizar las redes inalámbricas de forma grafica es una ventaja frente los diferentes sistemas de escaneo que ofrece el mercado actualmente, el gran auge de las tecnologías ha forzado a los fabricantes de computadores y dispositivos a crear sistemas de escaneo básicos que ofrecen la información necesaria para ubicar redes, sin embargo la principal ventaja de este sistema es el manejo de la información capturada y la integración de esta con aplicaciones de terceros (Google maps).

Obtener información geo-referenciada es muy útil ya que permite establecer tendencias que pueden, de ser necesario, indicar la configuración de seguridad de las redes inalámbricas de acuerdo a la zona de la ciudad, el número de redes identificadas en un barrio, localidad, calle o ciudad, entre otras.

Los sistemas de escaneo y representación grafica diseñados en esta investigación brindan la información útil que permite identificar y graficar de forma puntual las redes inalámbricas escaneadas, sin embargo nació la idea de diseñar una herramienta que además brinde la gran ventaja de identificar restaurantes y centros comerciales, basado en el contenido de los SSID de las redes inalámbricas.

10 BIBLIOGRAFIA

Redes inalámbricas IEEE 802.11,[Paper] Enrique de Miguel Ponce, Enrique Molina Tortosa, Vicente Mompó Maicas.

Tutorial Redes inalámbricas.(Paper)

IEEE, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. [Paper] 2007, IEEE computer Society.

Redes inalámbricas,[Paper] Carlos Varela, Luis Domínguez, escuela técnica superior de ingeniería informática .2002.

DISEÑO E IMPLEMENTACIÓN DE UNA RED INALÁMBRICA IEEE802.11b PARA APLICACIONES DE VOZ Y DATOS EN LA CUENCA DEL RÍO NAPO – PERÚ, [tesis de grado telecomunicaciones] , Marc Baños Aixalá. 2007

Redes inalámbricas [paper], Abaco instituto superior tecnológico privado.

Integración de Protocolos de Acceso Avanzados de Redes WLAN IEEE 802.11, Cristian Crespo Cintas, [trabajo de fin de carrera], 2008.

El Estándar IEEE 802.11, Wireless LAN [Paper], Francisco López Ortiz.

Tecnología Wi-Fi, Ing. Ricardo Alberto Andrade, Ing. Pablo Hernan Salas, Ing. Daniel Santos Paredes .2008.

Introducción de las tecnologías inalámbricas IEEE 802.11 y acceso de última milla.

Introducción a las redes inalámbricas 802.11 [Paper], Javier Cañas R. 2003.

Estándar IEEE para redes inalámbricas, José Félix Lucia Embid, José Ramón Manau Peirón.

GPS Fácil, uso del sistema de posicionamiento global, autor: Lawrence Letham, editorial: Paidotribo ,2001.

Hacking GPS, autores: Kingsley-Hughes, Kathie, Editorial: Hungry Minds, 2005. Volumen 1.

Calculo: Trascendentes tempranas, autor: James Stewart , Editorial : Thomson, Cuarta Edición, 2002.

Geometría Analítica, autor: Charles Lehmann , editorial : Limusa,1994.

Vectores y Matrices, autor: Ricardo Figueroa, Editorial: San Marcos, 1992.

Así funciona el GPS[En línea], autor: José Antonio E. García Álvarez. Disponible en: http://www.asifunciona.com/electronica/af_gps/af_gps_10.htm ,

Introduction to GPS, The global position System, Ahmed El- Rabbany, 2002.

Funcionamiento del GPS [En línea], Disponible en: http://www.gps-auto.org/navegador-gps/funcionamiento-gps.html .

Estándares IEEE 802.11 Wireless LAN [En línea], autor: Diego Alejandro Villegas Oliveros. Disponible en: http://www.scribd.com/doc/13842125/ESTANDAR-IEEE-80211,

WLAN Red Inalámbrica de Área Local [En línea]. Disponible en: http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/valle_i_lf/capitulo1.pdf,

Protocolo WEP (Wired Equivalent Privacy)[En línea]. Disponible en: http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/de_l_j/capitulo3.pdf

Ataque practico al algoritmo de cifrado RC4 [En línea]. Disponible en: http://tlapixqui.izt.uam.mx/septcol/pags/resumenes/Contrib2_Cripto_S-Estrella.pdf

Análisis de WPA/WPA2 Vs WEP [En línea], autor: Jhonatan Revelo, Edison Pazmiño, 2008. Disponible en: http://www.cybsec.com/upload/ESPE_Analisis_WPA_WEP.pdf

Protocolos de seguridad en redes inalámbricas [Paper], autor: Saulo Barajas. Disponible en: http://www.saulo.net/pub/inv/SegWiFi-art.htm

Inseguridad en redes 802.11b [En línea], autor: Oliva Fora. Disponible en: http://www.matarowireless.net/

Seguridad Wi-Fi – WEP, WPA y WPA2 [En línea], autor: Lehembre, Guillaume. Disponible en: http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf

Seguridad en redes inalámbricas. Universidad de Valencia [En línea], autor: Alapont Miquel, Vicent. Disponible en: http://www.uv.es/montanan/ampliacion/trabajos/SeguridadWireless.pdf

Redes Inalámbricas [En línea]. Disponible en: http://www.fain.uade.edu.ar/simposio/images/archivos/14.pdf.

Conceptos básicos de los mapas (API)[En línea]. Disponible en: http://code.google.com/intl/es/apis/maps/documentation/introduction.html#GMap2,

Estudio de Google Earth y Google maps[En linea], autor: Valeria Araya, Marzo 11 del 2009.Disponible en: http://alumnos.elo.utfsm.cl/~varaya/practica/reportes/kml/kml.pdf.

¿Qué es un GPS?[En linea], autor: Ingesur (ingeniería, geotécnica y servicios). Disponible en: http://www.ingesur.com/descargas/gps.pdf

Cómo Funciona el sistema GPS en cinco pasos lógicos [En línea], autor: Pedro Gutovnok, 1999. Disponible en: http://paginas.fe.up.pt/~ee95080/GPS.pdf

Arboles multicriterio, Árbol-r. X-tree [En línea]. Disponible en: http://www.webdelprofesor.ula.ve/ingenieria/ibc/ayda/c14Rtree.pdf.

Sistemas de información Geográfica. [En línea]. Disponible en: http://catarina.udlap.mx/u_dl_a/tales/documentos/msp/aragon_p_sm/capitulo1.pdf

Geographic Data Structures. [En línea], Autor: Maria Antonia Brovelli. Disponible en: http://geomatica.como.polimi.it/corsi/geog_info_system/l10_geographicdatastructures.pdf

[RFC3580] Congdon, P., “IEEE 802.1X Remote Authentication Dial In User Service (RADIUS), September 2003.

[RFC2284] Blunk, L. and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

[RFC2869] Rigney, C., “RADIUS Extensions", RFC 2866, June 2000.

[RFC2284] Aboba, B.,” Extensible Authentication Protocol (EAP)”, June 2000

ANEXOS

ANEXO A. Código Manejo de GPS[13]

```
/*
 * ManejadorGPS.java
 * German Ulloa
 *
 */
package capturarRedesWireless.Logic;

import capturarRedesWireless.Interfaces.Localizable;
import java.io.IOException;
import java.io.InputStream;
import java.util.regex.Pattern;

public class ManejadorGPS implements Localizable {

    protected double latitud;
    protected double longitud;
    protected Thread thread;
    private Process process;
    private SerialReader serialReader;

    public ManejadorGPS() {
    }

    public double[] obtenerCoordenadas() {
        double result[] = new double[2];
        result[0] = getLatitud();
        result[1] = getLongitud();
        return result;
    }

    public boolean emparejar() {
        Runtime r = Runtime.getRuntime();
        try {
            setP(r.exec("cat /dev/rfcomm10"));
            InputStream in = getP().getInputStream();
            serialReader=new SerialReader(in, this, true);
            thread = new Thread(serialReader);
            thread.start();
        } catch (IOException e) {
            return false;
        }
        return true;
    }

    public boolean desemparejar() {
        serialReader.setVivo(false);
        process.destroy();
        return true;
    }

    /**
     * @return the latitud
```

```
 */
public double getLatitud() {
    return latitud;
}

/**
 * @param latitud the latitud to set
 */
public void setLatitud(double latitud) {
    this.latitud = latitud;
}

/**
 * @return the longitud
 */
public double getLongitud() {
    return longitud;
}

/**
 * @param longitud the longitud to set
 */
public void setLongitud(double longitud) {
    this.longitud = longitud;
}

/**
 * @return the p
 */
public Process getP() {
    return process;
}

/**
 * @param p the p to set
 */
public void setP(Process p) {
    this.process = p;
}


public class SerialReader implements Runnable {

    private ManejadorGPS manejadorGPS;
    private InputStream inputStream;
    private boolean vivo;

    public SerialReader(InputStream in, ManejadorGPS manejadorGPS, boolean vivo) {
        this.inputStream = in;
        this.manejadorGPS = manejadorGPS;
        this.vivo=vivo;
    }

    public void run() {
        while (vivo) {
```

```
            byte[] buffer = new byte[1024];
            int len = -1;
            try {
               Pattern pattern = Pattern.compile(".*\\$GPRMC(,.*){12}",
                     Pattern.DOTALL);
               StringBuilder sb = new StringBuilder();
               while ((len = this.getIn().read(buffer)) > -1) {
                  try {
                     sb.append(new String(buffer, 0, len));
                     if (pattern.matcher(sb.toString()).matches()) {
                        String rmc[] = sb.toString().substring(
                              sb.indexOf("GPRMC"),
                              sb.indexOf("$", sb.indexOf("GPRMC"))).split(",");
                        String lat = rmc[3].replaceAll("\\.", "");
                        String lon = rmc[5].replaceAll("\\.", "");
                        int latitudeInt = Integer.parseInt(lat);
                        int longitudeInt = Integer.parseInt(lon);

                        float latitude = (latitudeInt / 1000000 * 60 + (latitudeInt % 1000000) /
10000f) / 60;
                        float longitude = (longitudeInt / 1000000 * 60 + (longitudeInt % 1000000) /
10000f) / 60;
                        manejadorGPS.latitud = latitude;
                        manejadorGPS.longitud = (-1)*longitude;
                        //System.out.println(manejadorGPS.latitud + " -" + manejadorGPS.longitud);
                        sb = new StringBuilder();
                     }
                  } catch (Exception e) {
                  }
               }
            } catch (IOException e) {
            }
         }
      }

      /**
       * @return the manejadorGPS
       */
      public ManejadorGPS getManejadorGPS() {
         return manejadorGPS;
      }

      /**
       * @param manejadorGPS the manejadorGPS to set
       */
      public void setManejadorGPS(ManejadorGPS manejadorGPS) {
         this.manejadorGPS = manejadorGPS;
      }

      /**
       * @return the in
       */
      public InputStream getIn() {
         return inputStream;
      }
```

```
        /**
         * @param in the in to set
         */
        public void setIn(InputStream in) {
            this.inputStream = in;
        }

        /**
         * @return the vivo
         */
        public boolean isVivo() {
            return vivo;
        }

        /**
         * @param vivo the vivo to set
         */
        public void setVivo(boolean vivo) {
            this.vivo = vivo;
        }
    }
}
```

[13] Código Realizado por Germán Ulloa, quien autoriza su uso y aplicación en el proyecto Herramienta de localización de redes inalámbricas para Google maps.