UNIVERSIDAD MAYOR DE SAN ANDRES

FACULTAD DE TECNOLOGIA

CARRERA DE ELECTRONICA Y TELECOMUNICACIONES

NIVEL LICENCIATURA

EXAMEN DE GRADO

(TRABAJO DE APLICACION)

“SISTEMA DE DETECCION, PREVENCION DE INTRUSIONES Y MONITOREO EN UNA RED INALAMBRICA DE AREA LOCAL”

Postulante: Walter Felipe Duran Huayta

La Paz- Bolivia

2016

DEDICATORIA

Con mucho cariño a mi familia que me ha apoyado en tantos momentos, principalmente a mi madre que me dio la vida y ha estado conmigo en todo momento. Gracias a mi familia por todo, por creer en mí, aunque hemos pasado momentos difíciles siempre han estado apoyándome y brindándome todo su amor, por todo esto les agradezco de todo corazón el que esten a mi lado

AGRADECIMIENTO

Quiero agradecer sinceramente a aquellas personas que compartieron sus conocimientos conmigo, ayudándome a ser cada día un mejor profesional.

Especialmente agradezco a los docentes de la Carrera de Electrónica y Telecomunicaciones por su guía y orientación siempre dispuesta.

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

1. INTRODUCCION

Wi-Fi es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica, con él se pueden crear redes de área local inalámbricas de alta velocidad siempre y cuando el equipo que se vaya a conectar no esté muy alejado del punto de acceso. En la práctica, Wi-Fi admite ordenadores portátiles, equipos de escritorio, celulares, tablets o cualquier otro tipo de dispositivo de alta velocidad con propiedades de conexión también de alta velocidad (11 Mbps o superior). Los equipos al conectarse a internet se encuentran expuestos a diferentes tipos de códigos maliciosos y son vulnerables si estos no tienen una correcta configuración de seguridad o un antivirus que pueda mitigar el número de infecciones posibles.

Debido a lo expuesto el proyecto se enfoca a realizar un sistema que monitoree el uso de datos, provea detección y prevención de intrusiones a partir de un punto de acceso en una red inalámbrica de datos,

1.1. PLANTEAMIENTO DEL PROBLEMA

- Un problema muy común es que la instalación de servicio de internet mediante cables es relativamente de alto costo.

- El uso de los cables representa además dificultades en su construcción, instalación, puesta del servicio y deterioro de la infraestructura.

- Para oficinas pequeñas u hogares es alto el costo de adquisición de equipos y software que provean seguridad como ser: firewalls, antivirus y otros.

- Es habitual que el uso del internet se vea saturada por unos cuantos usuarios, privando o malogrando el servicio para otros sin poder identificar al final del día o una fecha determinada quien ha realizado más uso del internet.

- La formación del usuario final es limitada como para poder administrar o configurar varios equipos o software de seguridad.

- El usuario final desea ver los resultados obtenidos por los diferentes sistemas desde una aplicación ya siendo desde su celular o Tablet.

- Se desea filtrar el contenido web que puedan visualizar los usuarios que se conecten a la red inalámbrica.

1.2. OBJETIVOS

1.2.1. OBJETIVO GENERAL:

Implementar un sistema para redes inalámbricas de pequeñas oficinas u hogares, que sea capaz de reaccionar ante incidentes de seguridad que tengan lugar en la red o en los equipos informáticos.

1.2.2. OBJETIVOS ESPECIFICOS:

- ✓ Implementar un sistema de red inalámbrica local mediante WIFI que permita realizar la transmisión de datos TCP/IP (formato de Internet) de manera que se hace innecesaria la utilización de cableado.
- ✓ Filtrar el tipo de contenido web al que los usuarios puedan acceder.
- ✓ Monitorear el uso de ancho de banda de la red inalámbrica por protocolo de cada usuario.
- ✓ Detectar de forma automatizada los incidentes de seguridad que se produzcan.
- ✓ Bloquear determinados tipos de ataques antes que estos tengan éxito.
- ✓ Realizar un filtrado de los servicios permitidos a los que el usuario podrá acceder del internet.

1.3. JUSTIFICACION

1.3.1. Justificación Académica:

Es importante el aumentar los conocimientos referentes a la tecnología, así como el uso de sistemas operativos Linux, software de código de libre (Open Source), programación de páginas web y el uso de minicomputadores. Es una oportunidad para integrar varios sistemas con la finalidad de obtener más conocimientos sobre seguridad de datos.

1.3.2. Justificación Tecnológica:

El uso de minicomputadores en pequeños proyectos, en la actualidad es usual, su uso en la seguridad de datos e integración de sistemas debe ser explotado, el presente proyecto intenta aportar que es posible implementar proyectos basados en software y hardware libre.

1.3.3. Justificación Social:

Muchas oficinas, pequeñas empresas y hogares, optan por servicio de internet de diferentes proveedores, ya sea internet adsl, modem 3G|4G, routers inalámbricos con recepción 3G|4G, sin considerar a las amenazas a las que sus equipos electrónicos se exponen o al contenido inapropiado o prohibido a la que los usuarios podrían acceder. Se pretende proporcionar una manera sencilla y más económica que las soluciones que se encuentran en el mercado, para gestionar el uso de la red inalámbrica y la seguridad de datos en la misma.

1.4. DELIMITACIONES

1.4.1. Delimitación Temática:

Se trataran temas como software de código libre, programación de páginas web con lenguajes como html y php, el uso de minicomputadores, programación de aplicaciones en android, la transmisión de datos en un medio inalámbrico, también intervienen aspectos de la transmisión de datos como el filtrado que se puede realizar en las capas del modelo OSI como: capa de red, capa de transporte y la capa de aplicación.

1.4.2. Delimitación Temporal:

La implementación de un sistema que sea capaz de proveer las medidas de seguridad de datos correctamente, realice un monitoreo del uso del ancho de banda usado y que estos servicios sean de fácil acceso para los usuarios que estén autorizados para su revisión tendrá una duración de aproximadamente de 2 semanas considerando los diseños, las configuraciones, la programación y las pruebas necesarias para su correcto funcionamiento.

1.4.3. Delimitación Espacial:

El proyecto a realizarse está orientado a aquellas oficinas pequeñas u hogares, donde el número de dispositivos a conectarse no supere las 10 unidades, la distancia de cada dispositivo al punto de acceso no sea mayor de los 10 metros.

1.5. METODOLOGIA

Para el proyecto a realizarse se adecua mejor el método experimental.

El método experimental es un proceso sistemático y una aproximación científica a la investigación en la cual el investigador manipula una o más variables y controla y mide cualquier cambio en otras variables.

Es decir, el método experimental se base en un verdadero experimento.

El proyecto describirá la forma de utilizar un miniordenador en la práctica como un punto de acceso de red inalámbrica de una red de área local que posea la capacidad de filtrar y rechazar paquetes ya sea a nivel de la capa de transporte o en la capa de aplicación. Ademas de monitorear a nivel de capa de aplicación.

2. MARCO TEORICO

2.1. Modelos de referencia.

2.1.1. Modelo OSI

El modelo OI (Open System Interconection = Interconexión de sistemas abiertos). Es usado para describir el uso de datos entre la conexión física de la red y la aplicación del usuario final. Este modelo es el mejor conocido y el más usado para describir los entornos de red. Este modelo OSI el propósito de cada capa es proveer lo servicios para la siguiente capa superior, resguardando la capa de los detalles de cómo los servicios son implementados realmente. Las capas son abstraídas de tal manera que cada capa cree que se está comunicando con la capa asociada en la otra computadora, cuando realmente cada capa se comunica solo con las capas adyacentes de la misma computadora. La información que envía una computadora debe de pasar por todas las capas inferiores. La información que envía una computadora debe de pasar por las capas inferiores. La información entonces se mueve a través del cable de red hacia la computadora que recibe y hacia arriba a través de las capas de esta misma computadora hasta que llegue al mismo nivel de la capa que envió la información.

La serie de las reglas que se usan para la comunicación entre las capas se llama protocolo.

El modelo OSI define 7 capas:

- La capa física
- La capa de enlace
- La capa de red
- La capa de transporte
- La capa de sesión
- La capa de presentación
- La capa de aplicación

Las primeras son conocidas como capas de medios y estas controlas la entrega física de mensaje a través de la red. El resto son conocidas como capas de host y proporcionan una entrega precisa de los datos entre los computadores.

2.1.1.1. La capa física

Este nivel dirige la transmisión de flujos de bits sobre un medio de conexión. Se encuentra relacionado con condiciones eléctricas-ópticas, mecánicas y funcionales del interfaz al medio de transmisión. A su vez está encargado de aportar la señal empleada para la transmisión de los datos generados por los niveles superiores.

2.1.1.2. La capa de enlace

Este nivel se encarga, en el computador de origen de alojar en una estructura lógica de agrupación de bits, llamada Trama (FRAME), los datos proveniente de los nivele superiores. En el computador de destino, se encarga de agrupar los bits provenientes del nivel físico en tramas de datos (frames) que serán entregadas al nivel de red. Este nivel es responsable de garantizar la transferencia de tramas libres de errores de un computador a otro a través de nivel físico.

2.1.1.3. La capa de red

Es responsable del direccionamiento de mensajes y de la conversión de las direcciones lógicas y nombres, en direcciones físicas. Esta encargado también de determinar la ruta adecuada ara el trayecto de los datos, basándose en condicione de la red, prioridad de servicio, etc. El nivel de red agrupa pequeños fragmentos de mensajes para ser enviados juntos a través de la red.

2.1.1.4. La capa de transporte

Se encarga de la recuperación y detección de errores. Garantiza también, la entrega de los mensajes del computador originados en el nivel de aplicación. Es el nivel encargado de informar a los niveles superiores del estatus de la red.

2.1.1.5. La capa de sesión

Permite que dos aplicaciones residentes en computadoras diferentes establezcan, usen y terminen una conexión llamada sesión. Este nivel realiza

reconocimientos de nombre y las funciones necesarias para que dos aplicaciones se comuniquen a través de la red, como en el caso de funciones de seguridad.

2.1.1.6. La capa de presentación

Determina el formato a usar para el intercambio de datos en la red. Puede ser llamado el traductor de la red. Este nivel también maneja la seguridad de emisión pues, provee a la red de servicios como el de encriptación de datos.

2.1.1.7. La capa de aplicación

Sirve como ventana para los procesos que requieren acceder a los servicios de red. La capa de aplicación comprende los servicios que el usuario final está acostumbrado a utilizar en una red.

2.1.1.8. Transmisión de datos en el modelo OSI

La transmisión de datos en el modelo OSI se realiza de forma análoga a lo ya descrito para el modelo de capas. La capa de aplicación recibe los datos del usuario y le añade una cabecera (que denominamos cabecera de aplicación). Constituyendo así la PDU (Protocol Data Unit) de la capa de aplicación. La cabecera contiene información de control propia del protocolo en cuestión. La PDU es transferida a la capa de aplicación en el nodo de destino, la cual recibe la PDU y elimina la cabecera entregando los datos al usuario. En realidad la PDU no es entregada directamente a la capa de aplicación en el nodo de destino, sino que es transferida a la capa de presentación en el nodo local a través de la interfaz; esto es una cuestión secundaria para la capa de aplicación, que ve a la capa de presentación como el instruméntenlo que le permite hablar con su homóloga en el otro lado.

A su vez la capa de presentación recibe la PDU de la capa de aplicación y le añade una cabecera propia (cabecera de presentación), creando la PDU de la capa de presentación. Esta PDU es transferida a la capa de presentación en el nodo remoto usando a la capa de sesión como instrumento para la comunicación, de manera análoga a lo ya descrito para la capa de aplicación.

En el caso más general cada capa añade una cabecera propia a los datos recibidos de la capa superior, y construye así su PDU. La capa homologa del nodo de destino se ocupara de extraer dicha cabera, interpretarla, y entregar la PDU correspondiente a la capa superior. En algunos casos la cabecera puede no existir. En el caso particular de la capa de enlace además de la cabecera añade una cola al construir la PDU (trama) que entrega a la capa física.

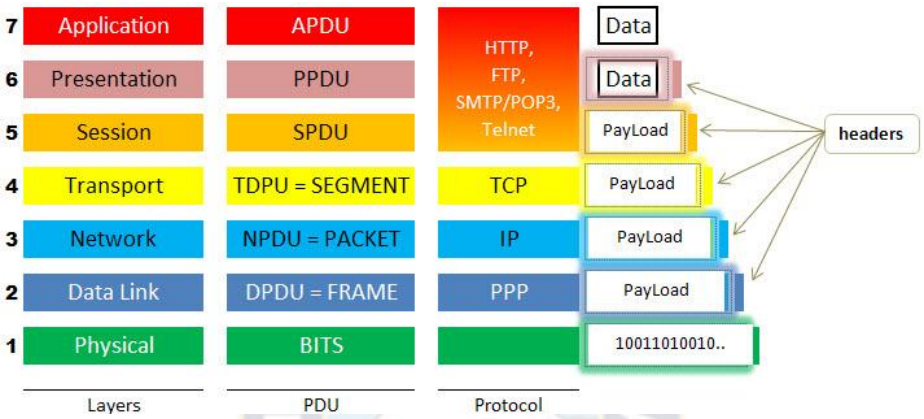

Figura 1 Capas del modelo OSI y sus respectivos PDU
Fuente: http://www.telecomhall.com Las capas del modelo OSI

2.1.2. El modelo TCP/IP

El segundo modelo de mayor estratificación por capas no se origina de un comité de estándares, sino que proviene de las investigaciones que se realizan respecto al conjunto de protocolos de TCP/IP. Con un poco de esfuerzo, el modelo OSI puede ampliarse y describir el esquema de estratificación por capas del TCP/IP, pero los presupuestos subyacentes son lo suficientemente distintos para distinguirlos como dos diferentes. En términos generales, TCP/IP está organizado en cuatro capas conceptuales que se construyen sobre una quinta capa de hardware. El hardware siguiente esquema muestra las capas conceptuales así como la forma en que los datos pasan entre ellas.

2.1.2.1. Capa de acceso a la red

Consta de una capa de interfaz de red responsable de aceptar los datagramas IP y transmitirlos hacia una red especifica. Una interfaz de red puede consistir en un dispositivo controlador (por ejemplo, cuando la red es una red de área local a la que

las máquinas están conectadas directamente) o un complejo subsistema que utiliza un protocolo de enlace de datos propios (por ejemplo, cuando la red consiste de conmutadores de paquetes que se comunican con anfitriones utilizando HDLC).

2.1.2.2. Capa de Internet

La capa de Internet maneja la comunicación de una maquina a otra. Esta acepta una solicitud para enviar un paquete desde la capa de transporte, junto con una identificación de la máquina, hacia la que se debe enviar el paquete. La capa de Internet también maneja la entrada de datagramas, verifica su validez y utiliza un algoritmo de ruteo para decidir si el datagrama debe procesarse de manera local o debe ser transmitido. Para el caso de los datagramas direccionados hacia la maquina local, el software de la capa de red de redes borra el encabezado del datagrama y selecciona, de entre varios protocolos de transporte, un protocolo con el que maneja el paquete. Por último la capa de internet envía los mensajes ICMP de error y control necesarios y maneja todos los mensajes ICMP entrantes.

2.1.2.3. Capa de Transporte

La principal tarea de la capa de transporte es proporcionar la comunicación entre un programa de aplicación y otro. Este tipo de comunicación se conoce frecuentemente como comunicación punto a punto. La capa de transporte regula el flujo de información. Puede también proporcionar un transporte confiable, asegurando que los datos lleguen sin errores y en secuencia. Para hacer esto, el software de protocolo de transporte tiene el lado de recepción enviando acuses de recibo de retorno y la parte de envió retransmitiendo los paquetes perdidos. El software de transporte divide el flujo de dato que se está enviando en pequeño fragmentos (por lo general conocidos como paquetes) y pasa cada paquete, con una dirección de destino, hacia la siguiente capa de transmisión. Aun cuando en el esquema anterior se utiliza un solo bloque para representar la capa de aplicación, una computadora de propósito general puede tener varios programas de aplicación accesando a la red de redes al mismo tiempo. La capa de transporte debe aceptar datos desde varios programas de usuario y enviarlos a la capa del siguiente nivel. Para hacer esto, se añade información adicional a cada paquete, incluyendo

códigos que identifican que programa de aplicación envía y que programa debe recibir, así como una suma de verificación para verificar que el paquete ha llegado intacto y utiliza el código de destino para identificar el programa de aplicación en el que se debe entregar.

2.1.2.4. Capa de Aplicación

Es el nivel más alto, los usuarios llaman a una aplicación que acceda servicios disponibles a través de la red de redes TCP/IP. Una aplicación interactúa con uno de los protocolos de nivel de transporte para enviar o recibir datos. Cada programa de aplicación selecciona el tipo de transporte necesario, el cual puede ser una consecuencia de mensajes individuales o un flujo continuo de octetos. El programa de aplicación selecciona el tipo de transporte necesario, el cual puede ser una secuencia de mensajes individuales o un flujo continuo de octetos. El programa de aplicación pasa por los datos en la forma requerida hacia el nivel de transporte para su entrega.

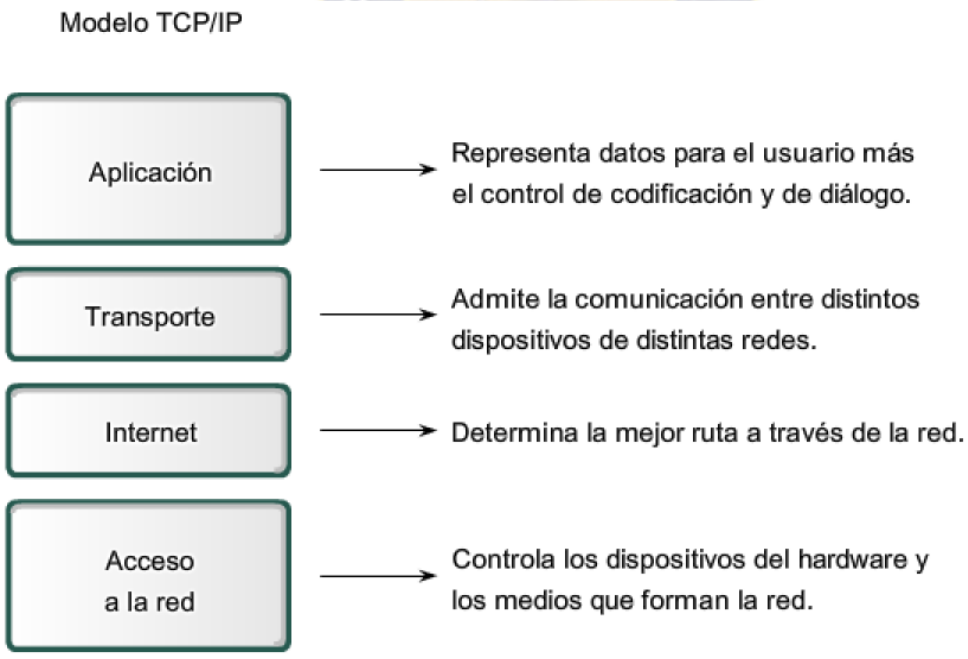

Figura 2 Modelo TCP/IP
Fuente: Modelo TCP/IP http://modelotcp18.blogspot.com/

2.1.3. Comparación de los modelos TCP/IP

Como ya hemos mencionado, la génesis del modelo OSI y TCP/IP fue muy diferente. En el caso de OSI primero fu el modelo y después los protocolos, mientras que en TCP/IP el orden fue inverso. Como consecuencia de esto el modelo OSI es más elegante y esta menos condicionado por ningún protocolo en particular, y se utiliza profusamente como modelo de referencia para todo tipo de redes. El modelo OSI hace una distinción muy clara entre servicios, interfaces y protocolos, conceptos que a menudo se confunden en el modelo TCP/IP. Podremos decir que la arquitectura (o el modelo) OSI es más modular y académico que el TCP/IP.

Pero este mayor nivel de abstracción también tiene sus inconvenientes. Los diseñadores del modelo OSI no tenían experiencia práctica aplicando su modelo para desarrollar protocolos y olvidaron algunas funcionalidades importantes. Por ejemplo, las redes broadcast no fueron previstas inicialmente en la capa de enlace, por lo que se tuvo que insertar a la fuerza la subcapa MAC para incluirlas. Otro problema era que no se había previsto la interconexión de redes diferentes, cosa que fue como ya hemos visto el alma mater del modelo TCP/IP.

El modelo OSI tiene siete capas, mientras que el modelo TCP/IP solo tiene 4. Aunque es desafortunado la fusión de la capa física y la de enlace en una oscura capa de acceso de red, la fusión de las capas de sesión, presentación y aplicación en una ola en el modelo TCP/IP es claramente más lógica que la del modelo OSI.

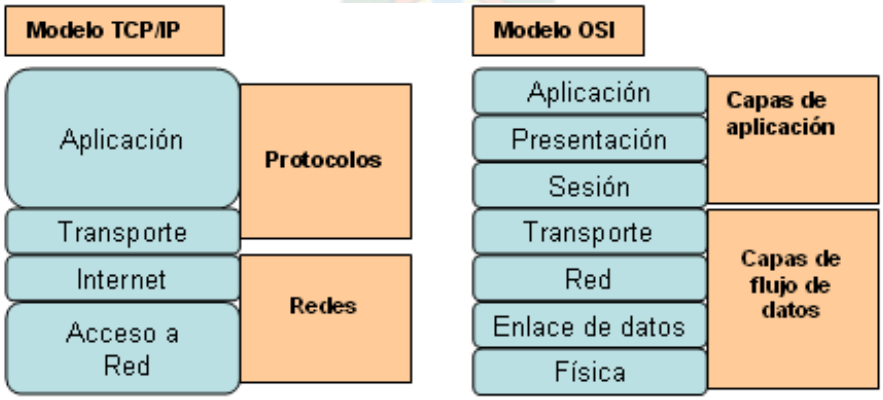

Figura 3 Comparación del modelo OSI y el modelo TCP/IP
Fuente: 4.6 Comparación entre el modelo OSI y el modelo TCP/IP
http://www.adrformacion.com

2.1.4. Ancho de banda

El ancho de banda es el rango de frecuencias en el que una señal determinada existe donde se concentra la mayor potencia de la señal.

El termino ancho de banda es a menudo utilizado por algo que deberíamos denominar tasa de transferencia de datos, en computación de redes (el ancho de banda o ancho de banda digital o ancho de banda de red) es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un periodo dado, es expresado en bits/s (bits por segundo) o en su defecto en múltiplos.

Ancho de banda puede referirse a la capacidad de ancho de banda o ancho de banda disponible en bit/s, lo cual típicamente significa el rango neto de bits o la máxima salida de una huella de comunicación lógico o físico en un sistema de comunicación digital.

A pesar de que las capacidades de transmisión o tasa de transmisión (ancho de banda digital) se mide en (bps = bits por segundo), el tamaño de paquetes se mide en bytes (1 byte=1024 bits).

2.2. Red Informática.

2.2.1. Que son las redes?

Una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de equipos informáticos conectados entre si por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información y recursos, y ofrecer servicios.

La finalidad principal para la creación de una red de computadoras es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo general de estas acciones.

2.2.2. Clasificación de las redes.

RED DE AREA PERSONAL o PAN (personal área network) es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora cerca de una persona.

REDES DE AREA LOCAL o LAN (local área network) Es un sistema de comunicación entre computadoras que permite compartir información, con la característica de que la distancia entre las computadoras debe ser pequeña. Estas redes son usadas para la interconexión de computadoras personales y estaciones de trabajo. Se caracterizan por tamaño restringido, tecnología de transmisión por lo general broadcast, alta velocidad y topología. Son redes con velocidades entre 10 y 100 Mbps, tiene baja latencia y baja tasa de errores. Cuando se utiliza un medio compartido es necesario un mecanismo de arbitraje para resolver conflictos. Dentro de este tipo de red podemos nombrar a intranet, una red privada que utiliza herramientas tipo internet, pero disponible solo dentro de la organización.

REDES DE AREA METROPOLITANA o MAN (metropolitan área network) Es una versión de mayor tamaño de la red local. Puede ser pública o privada. Una MAN pude soportar tanto voz como datos. La razón principal para distinguirla de otro tipo de rede, es que para las MAN's se a adoptado un estándar llamado DQDB (Distibuted-Queue Dual Bus) o IEEE 802.6. Utiliza medios de difusión al igual que las Rede de Area Local.

RED DE AREA DE CAMPUS o CAN (campus área network) es una red de computadoras que conecta rede de área local a través de una área geográfica limitada, como un campus universitario, o una base militar.

REDES DE AMPLIA COBERTURA o WAN (wide área network) Son rede que cubren una amplia región geográfica, a menudo un país o un continente. Este tipo de rede contiene maquinas que ejecutan programas de usuario llamada host o sistemas finales (endsystem). Los sistemas finales están conectados a una subred de comunicaciones. La función de la subred e transportar los mensajes de un host a otro.

En la mayoría de las redes de amplia cobertura se pueden distinguir dos componentes. Las líneas transmisión y los elementos de intercambio o conmutación. Las líneas de transmisión se conocen como circuitos, canales o troncales. Los elementos de intercambio son computadores especializados utilizados para conectar dos o más líneas de transmisión.

Las rede de área local son diseñadas de tal forma que tienen topologías simétricas, mientras que las redes de amplia cobertura tienen topología irregular. Otra forma de lograr de una red de amplia cobertura es a través de satélite o sistemas de radio.

DIFERENCIAS ENTRE UNA LAN Y UNA WAN

LAN:

- Canales de difusión
- Pocos kilómetros
- Velocidad de varios Mbps a Gbps
- Una sola organización
- Libertad de elegir el medio físico de comunicación
- Canal confiable (tasa de error 1000 menor que en WAN)
- Estructura imple para el manejo de errores.
- Protocolos más sencillos, sin importar mucho el rendimiento

WAN:

- Canales punto a punto (excepto satélites)
- Incluye países enteros
- Varias organizaciones
- Obligación de utilizar servicios públicos
- Canal poco confiable
- Estructura compleja para el manejo de errores

2.2.3. Tipo de Conexión

MEDIO GUIADOS

- El cable coaxial se utiliza para transportar señales eléctricas eléctrica de alta frecuencia que posee dos conductores concéntricos, uno central llamado vivo, encargado de llevar información, y uno exterior, de aspecto tubular, llamado malla o blindaje, que sirve como referencia de tierra y retorno de las corrientes.
- El cable de par trenzado es una forma de conexión en la que dos conductores eléctricos aislados son entrelazados para tener una menor interferencia y aumentar la potencia y disminuir la diafonía de los cables adyacentes.
- La fibra óptica es un medio de transmisión empleado habitualmente en redes de datos: un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

MEDIOS NO GUIADOS

- Red por radio es aquella que emplea la radiofrecuencia como medio de unión de las diversas estaciones de la red. Es un tipo de red muy actual, usada en distintas empresas dedicadas al soporte de redes en situaciones difíciles para el establecimiento de cableado, como es el caso de edificios antiguos no pensados para la ubicación de los diversos equipos componentes de una red de ordenadores.
- Red por infrarrojos. Las redes por infrarrojos no permitan la comunicación entre dos nodos, usando una serie de leds infrarrojos para ello. Se trata de emisores/receptores de las ondas infrarrojas entre ambos dispositivos, cada dispositivo necesita al otro para realizar la comunicación por ello es escasa su utilización a gran escala.
- Red por microondas es un tipo de red inalámbrica que utiliza microondas como medio de transmisión. El protocolo más frecuente es el IEEE 802.11b y transmite a 2.4 GHz, alcanzando velocidades de 11 Mbps (megabits por

segundo). Otras redes utilizan rango de 5.4 a 5.7 GHz para el protocolo IEEE 802.11ª.

2.2.4. Topologías de red.

La topología de una red es el arreglo físico o lógico en el cual los dispositivos o nodos de una red (en computadoras, impresoras, servidores, hubs, switches, enrutadores, etc.) se interconectan entre si sobre un medio de comunicación.

a) Topología Física: Se refiere al diseño actual del medio de transmisión de la red.
b) Topología lógica: Se refiere a la trayectoria lógica que una señal a su paso por los nodos de la red.

Existen varias topológicas de red básicas (BUS, estrella, anillo y malla), pero también existen redes hibridas que combinan una más de las topologías anteriores en una misma red.

Por el contexto del proyecto no se abordara en detalle de las topologías.

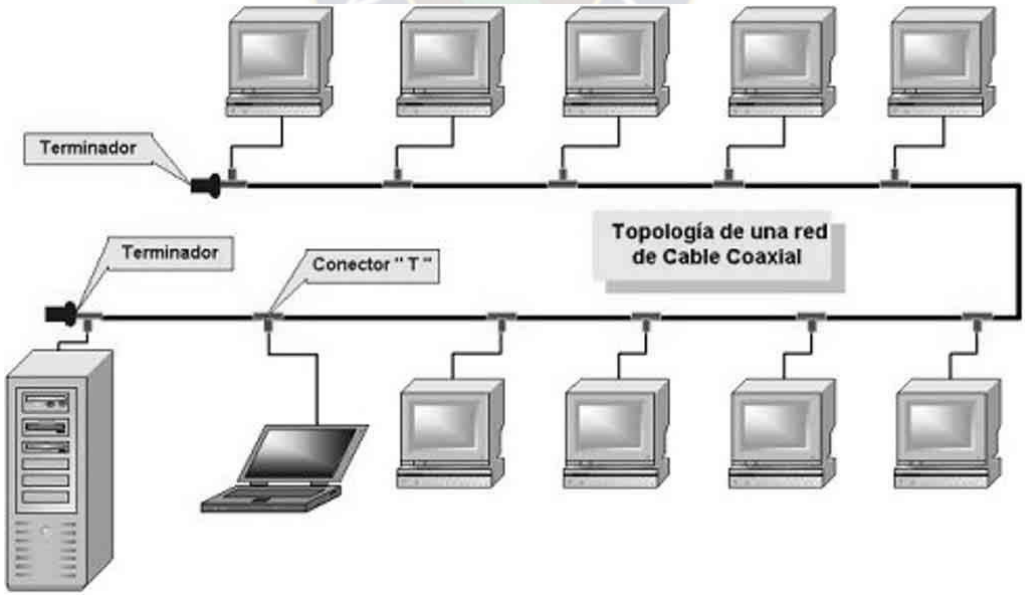

Figura 4 Topología BUS
Fuente: Redes por su teología http://gaboalex.blogspot.com

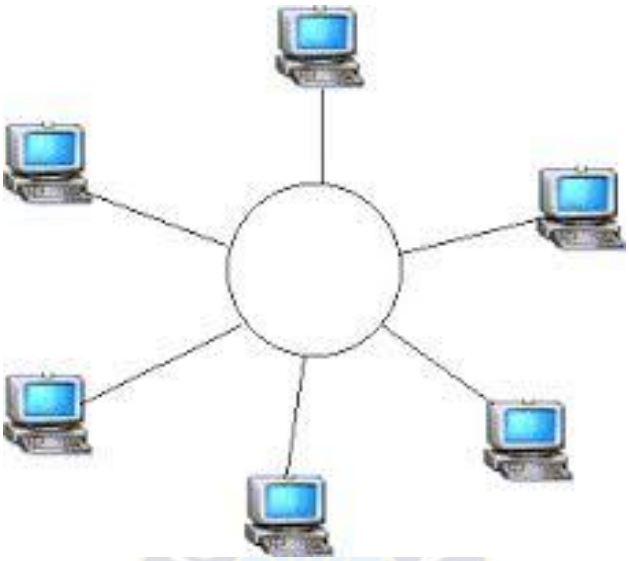

Figura 5 Topología Estrella
Fuente: Introducción a las Redes http://www1.frm.utn.edu.ar

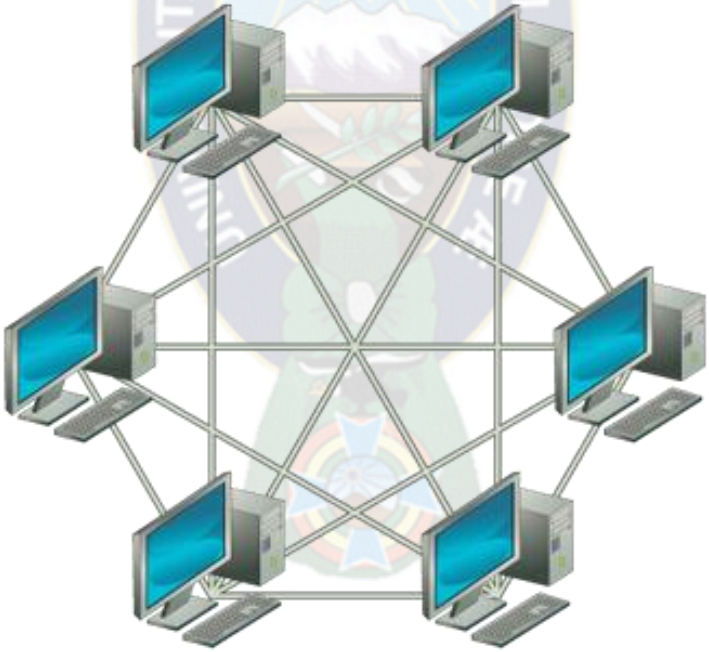

Figura 6 Topología Malla
Fuente: Tipos de redes https://www.emaze.com

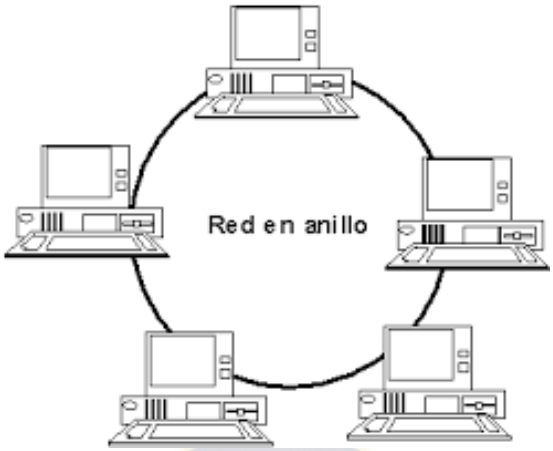

Figura 7 Topología Anillo
Fuente: Topología para redes http://topologializ.blogspot.com/

2.3. Redes Inalámbricas de área local (WLAN).

Es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes de área local cableadas o como extensión de estas. Utiliza tecnologías de radio frecuencia para transmitir y recibir datos a través de ondas electromagnéticas. Permite mayor movilidad a los usuarios al minimizar las conexiones cableadas, estableciendo conexión a los usuarios situados dentro de la misma zona de cobertura, tales como oficinas, campus, hogares, edificios o espacios públicos.

En la actualidad ya existen una multitud de dispositivos que permiten este tipo de conexión, tales como televisores, teléfonos, videoconsolas, ordenadores, impresoras, neveras, etc.

Figura 8 Dispositivos en redes inalámbricas de área local
Fuente: Importancia de las redes WIFI https://leidiyana.wordpress.com

2.3.1. Tipos de redes inalámbricas

Actualmente existen varios tipos de redes inalámbricas. Podemos clasificarlas en función del rango de frecuencia utilizado por cada una y en función de su rango de cobertura.

- *Clasificación en función del rango de frecuencia utilizado:*

Ya se ha mencionado en medios no guiados a las ondas de radio (propagación de 3Hz hasta los 3GHz, infrarrojos (propagación desde 300GHz hasta los 384 THz).

Microondas terrestres: se utilizan antenas parabólicas en enlaces punto a punto para transmitir. Las antenas tienen que estar perfectamente alineadas y a distancias no muy grandes. Su rango de frecuencias va desde 1GHz hasta los 300 GHz. Sufren atenuación con las inclemencias meteorológicas.

Microondas satelitales: se utilizan antenas parabólicas que envían la señal a un satélite, este la amplifica y la reenvía al receptor. Opera en el mismo rango de frecuencias que las microondas terrestres. La ventaja respecto a las terrestres es que en este caso los dispositivos pueden estar en cualquier posición.

- *Clasificación en función del rango de cobertura*:

WPAN (Wireless Personal Area Network-Red inalámbrica de área personal). Son redes inalámbricas de corto alcance. Dentro de este tipo de redes podemos encontrar la tecnología de infrarrojos (hasta 10m de distancia y velocidades de hasta 115 kbps). Bluetooth (hasta 100m de distancia y velocidades de hasta 24Mbps), Zigbee (velocidades de hasta 250kbps) y la más reciente la tecnología NFC (dispositivos casi pegados y velocidades de hasta 848kbps). Su uso se limita básicamente a periféricos para transmitir información entre ellos (móviles, impresoras, ratones, teclado, altavoces, electrodomésticos, etc.).

WLAN (Wireless Local Area Network-Red Inalámbrica de área local). Este tipo de redes son en las que se basa este proyecto. Son redes de medio alcance, como puede ser una casa, o un edificio de oficinas. Más adelante profundizaremos en ella.

WMAN (Wireless Metropolitan Area Network-Red inalámbrica de are metropolitana). Son redes inalámbricas de largo alcance. Pueden abarcar kilómetros de distancia, como por ejemplo una población o una ciudad. Dentro de este tipo de redes podemos encontrar las tecnologías como WIMAX o LMDS.

WWAN (Wireless Wide Area Network-Red Inalambrica de áreas extensas). Son redes inalambricas de muy largo alcance. Pueden abarcar hasta miles de kilometros. Dentro de este tipo de redes podemos encontrar tecnologías como la CDMA, GSM, HSPA, GPRS, UMTS utilizadas en telefonía móvil.

2.3.2. Topología.

Los elementos que intervienen principalmente en las comunicaciones inalámbricas son los puntos de acceso (equipos que dan acceso a la red de forma centralizada) y los clientes (dispositivos inalámbricos).

Existen dos tipos de topologías:

- Los clientes que se conectan directamente entre ellos para comunicarse (modo Ad-Hoc).
- Los clientes se conectan a un punto de acceso para comunicarse con el exterior o entre ellos mismos (modo infraestructura).

2.3.2.1. Modo Ad-Hoc

En este modo los equipos inalámbricos se conectan entre si para formar una red de punto a punto, es decir, los clientes intercambian la información entre ellos directamente sin pasar por ningún equipo intermedio.

Las opciones de configuración de seguridad nombre de red y canal de comunicación se configuran en el propio cliente.

Una vez que los clientes pertenecen a la misma red, se transmiten los datos al aire y los otros dispositivos reciben y reenvían la información.

La configuración que forman los clientes se llama conjunto de ervicio básico independiente o IBSS (Independent Basic Service Set).

Figura 9 Diagrama de una red Ad-Hoc
Fuente: Conventional and wireless ad hoc network http://www.conceptdraw.com

2.3.2.2. Modo Infraestructura.

En este modo los clientes deben comunicarse con el punto de acceso para poder utilizar la red, ya que el punto de acceso es el encargado de gestionar la autorización.

Al grupo formado por el punto de acceso y los clientes que se encuentran dentro de la misma zona de cobertura se le llama conjunto de servicio básico o BSS (Basic Service Set).

En este tipo de redes el nombre de la red e define en el punto de acceso con el parámetro ESSID (Extended Service Set ID). Esto nos permite diferenciar una red de otra.

En este modo de infraestructura se basa el presente proyecto.

Figura 10 Ejemplo de una red inalámbrica en modo infraestructura
Fuente: Modos de funcionamientos de las redes WI-FI http://redestelematicas.com

2.3.3. Estándares WLAN

Actualmente existen cuatro organizaciones que tienen mucho que ver con los estándares que se utilizan para las WLAN. Estas cuatro organizaciones son:

- ITU-R normalización a nivel mundial de las comunicaciones que utilizan la energía radiada, en concreto la asignación de frecuencias.
- IEEE: normalización de las WLAN (802.11)
- Alianza Wi-Fi consorcio industrial que impulsa la interoperabilidad de los productos que implementan estándares WLAN a través de su programa certificado Wi-Fi.
- FCC: agencia del gobierno de USA que regula el uso de distintas frecuencias de comunicaciones.

De las organizaciones mencionadas anteriormente, el IEEE desarrolla los estándares específicos para los distintos tipos de WLAN que se utilizan actualmente. Estos estándares deben tener en cuenta las elecciones de frecuencia efectuadas por las diferentes agencias regulatoria mundiales, como la FCC en USA y la ITU-R.

2.3.4. Estándares IEEE 802.11

El estándar IEEE 802.11 fue definido por el IEEE (instituto de Ingenieros Eléctricos y Electrónicos) en el año 1997 como nuevo estándar para las redes de área local inalámbrica. Inicialmente proporcionaba una velocidad de transferencia máxima de 2Mbps pero, como veremos a continuación, esta ha ido aumentando con las nuevas tecnologías hasta proporcionar velocidades de 300Mbps (802.11n), esta última es la más usada actualmente aunque en los últimos años se ha adoptado 802.11ac que proporciona velocidades de 1Gbps. Continua en desarrollo 802.11ad que alcanzaría una velocidades arriba de 7Gbps.

La definición del estándar 802.11 fue diseñada para sustituir a las capas físicas y de enlace del modelo OSI para redes cableadas (IEEE 802.3) especificando su funcionamiento en redes WLAN, haciendo que ambas redes sean identificas excepto en la forma en la que los terminales acceden a la red. Esto hace que ambas redes sean compatibles.

La capa física PHY (Physical Layer) de la especificación IEEE 802.11 se ocupa de definir los métodos por lo que se difunde la señal. Ofrece 4 tipos de técnicas de transmisión:

- Infrarrojos: usa transmisión difusa con una velocidad de 1Mbps o 2Mbps.
- FHSS (Frequency Hopping Spread Spectrum): espectro disperso por salto de frecuencia. Se transmiten los datos saltando de canal a canal, de acuerdo a una secuencia pseudo aleatoria particular que distribuye uniformemente la señal a través de la banda de frecuencia operativa (79 canales en Europa). Una vez que la secuencia de saltos se configura en un AP (Punto de Acceso), las estaciones se sincronizarán automáticamente según la secuencia de salto correcta. Se consiguen velocidades de transmisión de 1Mbps a 2Mbps. Opera en la banda de los 2,4GHz.
- DSSS (Direct Sequence Spread Spectrum): espectro disperso de secuencia directa. Utiliza un rango de frecuencia amplio de 22 MHz todo el tiempo. La señal se expande a través de diferentes frecuencias. Cada bit de datos se

convierte en una secuencia de chipping que se transmiten en paralelo a través del rango de frecuencia. Se consiguen velocidades de transmisión de 1Mbps a 2Mbps en la versión normal, y hasta 11 Mbps en la versión HR/DSSS. Opera en la banda de los 2,4GHz.

- OFDM (Orthogonal Frequency Division Multiplexing): multiplicación por división de frecuencia ortogonal. Divide una portadora de datos de alta velocidad en varias subportadoras de más baja velocidad, que luego se transmiten en paralelo. OFDM utiliza el espectro de manera mucho más eficiente, espaciando los canales a una distancia mucho menor. El espectro es más eficiente porque todas las portadoras son ortogonales entre sí, evitando de esa forma la interferencia entre portadoras muy cercanas. Se consiguen velocidades de transmisión de hasta 54Mbps. Opera en la banda de los 5GHz.

La capa de enlace de la especificación 802.11 está compuesta por dos subcapas:

- LLC (Logical Link Control). Capa que se ocupa del control del enlace lógico. Define cómo pueden acceder múltiples usuarios a la capa MAC.
- MAC (Medium Acces Control). Conjunto de protocolos que controlan cómo los distintos dispositivos comparten el uso del espectro radioeléctrico. Es más compleja que las de otras especificaciones (802.3, 802.5, etc.). En WLAN se utiliza CSMA/CA (acceso múltiple con detección de portadora y colisión evitable).

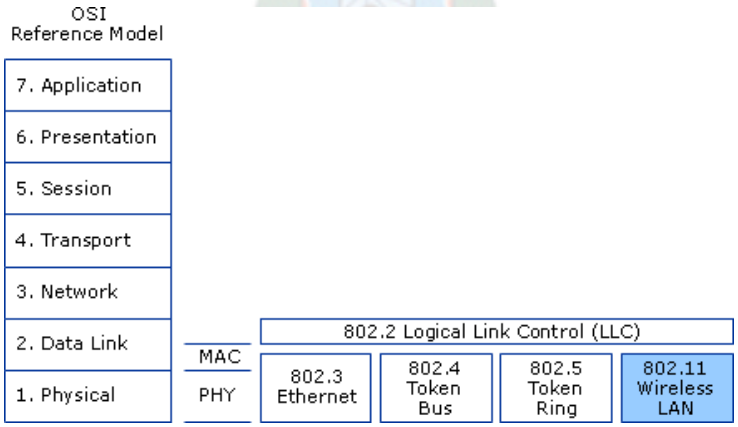

Figura 11 Capa LLC y capa MAC
Fuente: How 802.11 Wireless Works https://technet.microsoft.com

802.11 Wireless Standards					
IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

Figura 12 Estándares aprobados por IEEE
Fuente: Catch the wave 802.11ac http://www.l-com.com/

2.3.4.1. IEEE 802.11a

La revisión 802.11a fue aprobada en 1999. Utiliza la banda de frecuencias de 5GHz con una velocidad máxima de transmisión de 54 Mbps.

Utiliza la tecnología de transmisión OFDM que permite transmitir grandes cantidades de datos digitales sobre una onda de radio, dividiendo la señal y transportándola mediante 52 subportadoras a diferentes frecuencias que son transmitidas simultáneamente hacia el receptor.

La utilización de la banda de 5GHz representa la ventaja de recibir menos interferencias, pero también el inconveniente de que el rango de cobertura que ofrece es menor ya que penaliza mucho la potencia de la señal en función de la distancia.

2.3.4.2. IEEE 802.11b

La revisión 802.11b, al igual que la 802.11, fue aprobada en 1999. Utiliza la banda de frecuencias de 2,4GHz con una velocidad máxima de transmisión de 11Mbps.

Los productos de este estándar aparecieron en el mercado muy rápido debido a que es una extensión directa de la técnica de modulación DSSS definida en el estándar original. Por lo tanto los chips y productos fueron fácilmente actualizados para soportar las mejoras del 802.11b.

El rápido incremento en el uso del 802.11b junto con sustanciales reducciones de precios causó una rápida aceptación del 802.11b como la tecnología WLAN definitiva.

2.3.4.3. IEEE 802.11g

La revisión 802.11g fue aprobada en 2003. Utiliza la banda de frecuencias de 2,4GHz con una velocidad máxima de transmisión de 54Mbps. Es compatible con el estándar 802.11b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión. . El rango máximo de los dispositivos 802.11g es ligeramente mayor al de los 802.11b, pero el rango en el que el cliente puede alcanzar 54Mbps es mucho más corto que en el que puede alcanzar 11Mbps en 802.11b.

2.3.4.4. IEEE 802.11n

El estándar 802.11n fue ratificado por el IEEE en el año 2009. Mejora significativamente el rendimiento de la red con un incremento significativo de la velocidad máxima de transmisión de hasta 600Mbps en capa física. Puede trabajar en las bandas de frecuencia 2,4GHZ y 5GHz, lo que lo hace compatible con los dispositivos basados en estándares anteriores.

La incorporación también de la tecnología MIMO (Multiple Input – Multiple Output) que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de 3 antenas, hace que el alcance del radio de las redes sea mucho mayor.

2.3.4.5. IEEE 802.11ac

El estándar 802.11ac fue aprobado en enero de 2014. El estándar consiste en mejorar las tasas de transferencia hasta 443Mbits por flujo de datos, consiguiendo teóricamente tasas de 1.3Gbps empleando 3 antenas. Opera dentro de la banda de 5GHz, amplia el ancho de banda hasta 160MHz (40MHz en las redes 802.11n), utiliza hasta 8 flujos MIMO e incluye modulación de alta densidad (256 QAM).

2.3.5. Canales y frecuencias

El estándar 802.11a utiliza la banda de 5GHz. En esta banda se definen 23 canales utilizables por los equipos inalámbricos, que se pueden configurar de acuerdo a necesidades. Sin embargo, los 23 canales no son completamente independientes. Los canales contiguos se superponen y se producen interferencias, así que en la práctica es aconsejable usar 12 (canales no superpuestos) de forma simultánea. Esto también es válido para 802.11n si opera en esta banda.

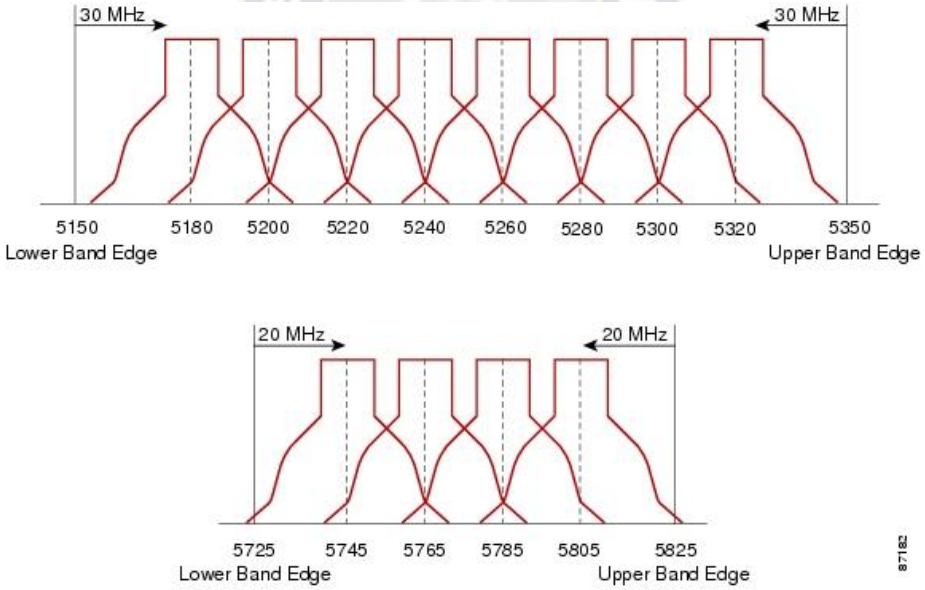

Figura 13 Canales y frecuencias de 802.11a/n
Fuente: Enlace entre Tplink y Tplink http://www.peruhardware.net

Los estándares 802.11b y 802.11g utilizan la banda de 2,4GHz. En esta banda se definen 11 canales utilizables (13 en Europa). Estos canales no son completamente independientes ya que los contiguos se superponen y se producen

interferencias, así que en la práctica es aconsejable utilizar 3 de forma simultánea como máximo. Esto también es válido para 802.11n si opera en esta banda.

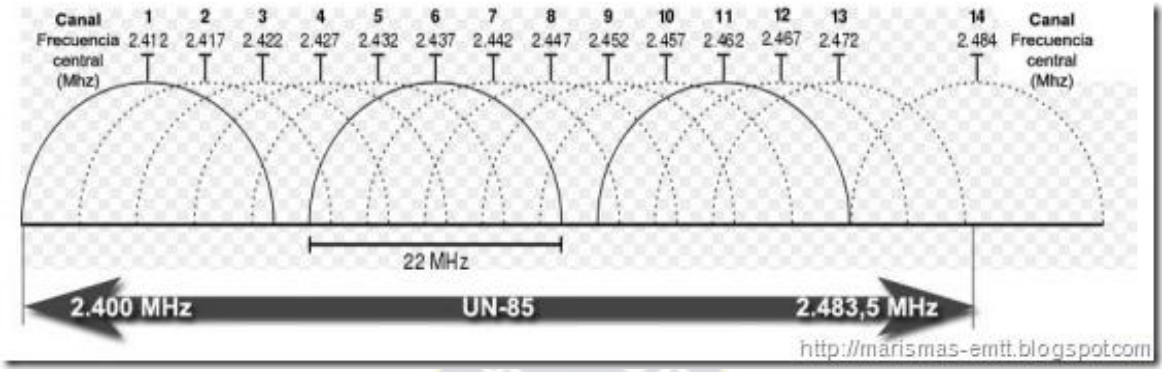

Figura 14 Canales y frecuencias de 802.11b/g/n
Fuente: Canales 802.11 http://marismas-emtt.blogspot.com

La utilización de 12 canales no superpuestos en un caso, y 3 en el otro, no significa que no puedan coexistir, sino que existen mayores interferencias entre dos puntos de acceso configurado con dos canales contiguos, lo que significa que el rendimiento de nuestra WLAN con mucho tráfico podría verse disminuido.

2.3.6. Wi-Fi

Wi-Fi (Wireless Fidelity) es un certificado proporcionado por el consorcio industrial sin ánimo de lucro Alianza Wi-Fi, que asegura la interoperabilidad de los productos que implementan estándares WLAN.

La alianza Wi-Fi, que se estableció originalmente como WECA (Wireless Ethernet Compatibility Alliance) en agosto de 1999, está formada por varias compañías líderes del sector de la tecnología de redes inalámbricas. Desde 1999, el número de miembros de la alianza Wi-Fi se ha incrementado considerablemente dado que cada vez más compañías de productos electrónicos de consumo, proveedores de servicios de red y fabricantes de ordenadores se han dado cuenta de la necesidad de ofrecer a sus clientes compatibilidad inalámbrica entre sus productos.

Figura 15 Logo de la alianza WIFI
Fuente: http://www.wi-fi.org/

Para que un equipo reciba el logotipo Wi-Fi es necesario que sea probado y verificado en los laboratorios de pruebas de esta asociación, asegurando que los productos con el logotipo Wi-Fi trabajan perfectamente unos con otros. Una vez que el producto inalámbrico pasa el proceso de pruebas, la compañía obtiene el sello Wi-Fi para dicho producto y puede utilizarlo con él.

Es importante resaltar que el certificado lo recibe un producto en concreto, y no una familia de productos. Cada vez que el fabricante modifique alguno de sus componentes, el producto debe pasar por todo el programa de pruebas antes de obtener de nuevo el certificado Wi-Fi.

Figura 16 Logo de la certificado WIFI
Fuente: http://www.wi-fi.org/

2.3.7. Ventajas y desventajas de las WLAN

Vamos a empezar hablando de las ventajas que supone el uso de las redes inalámbricas:

En primer lugar tenemos la movilidad que nos ofrece una red sin cables. Nos permite conectarnos desde nuestro terminal en cualquier lugar donde tengamos cobertura (dentro de nuestra casa, oficina, etc.). En segundo lugar tenemos la facilidad de instalación que supone respecto a una LAN cableada. Nos evita la difícil

tarea que supone el tirar cable por nuestra casa u oficina, con las obras que ello conlleva, o si tenemos que unir LANs separadas geográficamente. Otras ventajas que supone el uso de las WLAN es la flexibilidad que aportan (permite dotar de conexión a puntos en los que era imposible hacer llegar cableado) y la adaptabilidad (permite realizar fácilmente cambios en la topología de nuestra red y garantizar escalabilidad).

Por último, una de las ventajas más importantes que supone el uso de las WLAN en los tiempos actuales, es la reducción de costes que supone su implementación. Todo y que los dispositivos electrónicos inalámbricos puedan tener un coste superior a los de cable, el no tener que hacer grandes obras para cablear todo el lugar donde se quiera implementar una red hace que sea mucho más económico

Para acabar mencionaremos de las desventajas principales de las WLAN:

En primer lugar tenemos las interferencias que ocasionan los dispositivos cercanos entre sí que operan en la misma banda de frecuencias y que hacen que el rendimiento de la WLAN decaiga. En segundo lugar tenemos la limitación de cobertura existente que depende de la potencia máxima de radiación de los dispositivos, que viene delimitada por la legislación vigente. Estos dos inconvenientes, se puede reducir su impacto en nuestra WLAN cambiando los canales en los que operan los dispositivos en el primero, e instalando más puntos de acceso o repetidores de señal en el segundo. También podemos considerar un inconveniente la limitación del rango de frecuencias del espectro libre utilizables en este tipo de redes.

Una desventaja importante de este tipo de redes es sin duda la baja velocidad de transferencia de datos en comparación con las redes con cables, que alcanzan velocidades mucho mayores. En la actualidad una LAN cableada puede llegar a transferir 1000Mbps (Gigabit Ethernet) mientras que una inalámbrica puede transferir unos 600Mbps teóricos (802.11n).

Por último, la desventaja más importante que supone el uso de este tipo de redes es el tema de la seguridad. Al ser el aire el medio de propagación empleado por las

ondas, hace que la información esté expuesta a sufrir ataques. En la actualidad el tema de la seguridad inalámbrica es en el que más hincapié se está haciendo. El nivel de seguridad actual de estas redes está a años luz del de sus comienzos.

2.3.8. Seguridad en WLAN

Es importante hacer una pequeña introducción de cómo se realiza una conexión a una red inalámbrica por parte de un cliente:

a) Por un lado tenemos un punto de acceso en el que hemos configurado nuestra WLAN que emite en su zona de cobertura tramas llamadas “Beacon Frames” con las que comunica su presencia. Estos “Beacon Frames” contienen por ejemplo el SSID, la velocidad que admite, el tipo de seguridad de la red, etc.
b) Por otro lado tenemos al cliente que primero de todo ha de descubrir la existencia de una WLAN e identificarla. Tiene dos formas de hacerlo:
    - mediante un escaneo pasivo: el dispositivo espera recibir los “Beacon Frames” que envía un AP y a través de ellos identifica la WLAN.
    - mediante un escaneo activo: el cliente lanza tramas llamadas “Sondas” a un AP determinado y espera una respuesta.
c) Una vez el cliente detecta un AP ha de autenticarse. Para ello el estándar 802.11 define dos tipos de autenticación:
    - Sistema de autenticación abierta: se limita a autenticar a cualquier cliente que lo solicite y la comunicación se realiza sin cifrar. Este sistema de autenticación se limita a una solicitud de autenticación por parte del cliente y a una respuesta por parte del punto de acceso, indicando el resultado de la autenticación.
    - Sistema de autenticación por clave compartida: consta de dos partes: autenticación del cliente y autenticación del punto de acceso. La autenticación del cliente, manda una trama de solicitud de autenticación en la que solicita utilizar una clave compartida al punto de acceso. El punto de acceso responde con una trama de desafío (Authentication Challenge), creada con la clave compartida .El cliente responde a la

trama de desafío (Authentication Response) con el contenido cifrado. El punto de acceso procesará esta trama descifrando su contenido y verificando que el texto de desafío sea correcto.

d) Una vez autenticado el cliente, se procede a realizar la asociación donde AP y cliente intercambian sus MAC, el identificador ESS y el identificador de asociación AID. Ahora el cliente ya está conectado a la WLAN y puede enviar y recibir datos a través de ella

Esta es la parte de la seguridad de las WLAN que se encarga de quién debe tener acceso a la red. La otra parte es la que se encarga que nuestros datos vayan protegidos, es decir, que alguien no autorizado que haya conseguido captar paquetes de datos pueda descifrar su contenido. Aquí entra en juego la seguridad a nivel de protocolo, que explicaremos a continuación.

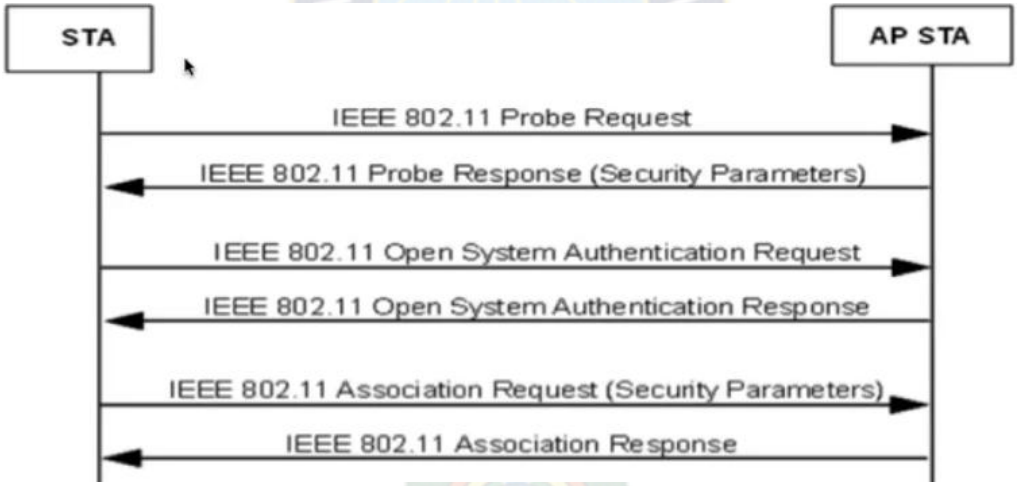

Figura 17 Conexión del cliente al AP
Fuente: Hacking WiFi http://highsec.es

2.3.8.1. Seguridad a nivel de protocolo

Como hemos comentado anteriormente, la seguridad a nivel de protocolo es la encargada de que los datos transmitidos por una WLAN no puedan ser descifrados por alguien ajeno a nuestra red. Para ello nuestra red ha de tener un algoritmo de codificación y gestión de claves.

En primer lugar, el IEEE publicó un algoritmo de seguridad opcional en el estándar 802.11 llamado WEP, el cual no tardó mucho en ser roto. Mientras el IEEE

trabajaba en otro algoritmo más potente, la Alianza Wi-Fi lanzó un algoritmo alternativo y más potente que WEP, llamado WPA.

Posteriormente el IEEE publicó el estándar 802.11i, también conocido como WPA2, que actualmente es el más seguro de los tres.

	WEP	WPA	WPA2
Cipher	RC4	RC4	AES
Key Size	40 bits	128 bits encryption 64 bits authentication	128 bits
Key Life	24 bit IV	48 bit IV	48 bit IV
Packet Key	Concatenated	Mixing Function	Not needed
Data Integrity	CRC-32	Michael Algorithm	CCM
Header Integrity	None	Michael Algorithm	CCM
Replay Attack	None	IV Sequence	IV Sequence
Key Management	None	EAP Based	EAP Based

Figura 18 Protocolos WEP, WPA y WPA2
Fuente: Hacking Wireless Network http://slideplayer.com/

2.3.8.1.1. WEP

El protocolo WEP (Wired Equivalent Privacy) es el mecanismo de cifrado básico opcional definido en el estándar IEEE 802.11. Su objetivo es proporcionar confidencialidad, autentificación y control de acceso en redes inalámbricas.

Utiliza el algoritmo de cifrado RC4 (Rivest Cipher 4), diseñado en 1987 por Ron Rivest de la empresa RSA Security, para cifrar todos los datos que se intercambian entre los clientes y el punto de acceso.RC4 consiste en generar una clave de forma pseudo-aleatoria que tiene la misma longitud que el texto original. A esta clave y al texto original se le aplica la operación lógica XOR (O exclusiva), obteniendo como resultado un texto cifrado. La clave pseudo-aleatoria se genera utilizando una clave secreta que define el propio usuario con una longitud de 40 o 104 bits y un vector de inicialización (IV) de 24 bits que lo genera aleatoriamente el sistema para cada trama. La clave secreta se concatena con el vector de inicialización creado, lo que se conoce como semilla (Seed), obteniendo la clave pseudo aleatoria de 64 o 128 bits utilizando el algoritmo PRNG (Pseudorandom

Number Generation). El IV viaja en cada trama que se envía por lo cual hace que sea fácil de interceptar por un atacante.

Para garantizar la integridad, el texto original se envía como ICV (Integrity Check Value), que se trata de 32 bits de comprobación de integridad que se calculan con el algoritmo CRC-32 (Código de redundancia cíclica).

2.3.8.1.2. WPA

WPA (Wifi Protect Access) es el protocolo de seguridad que lanzó la Alianza Wi-Fi para solucionar los problemas de seguridad del protocolo WEP, mientras el IEEE trabajaba en el estándar 802.11i. Básicamente la Alianza Wi-Fi decidió, en colaboración con el IEEE, tomar aquellas partes del nuevo estándar que ya estaban suficientemente avanzadas y publicar WPA.

Este protocolo implementa las siguientes mejoras:

- Autenticación del usuario mediante el IEEE 802.1x (control de acceso a red basada en puertos).
- Soluciona la debilidad del vector inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia. Los 48 bits permiten generar 2 elevado a 48 combinaciones de claves diferentes, lo cual es un número suficientemente elevado como para tener duplicados.
- Utiliza el intercambio dinámico de claves medianteel protocolo TKIP (Temporal Key Integrity Protocol).
- El algoritmo de cifrado utilizado por WPA sigue siendo RC4 como en WEP, pero para comprobar la integridad de los mensajes ICV, se cambió el código de detección de errores CRC-32 por uno nuevo llamado MIC (Message Integrity Code).

WPA puede funcionar en dos modos:

- WPA-Enterprise: este modo requiere de una infraestructura de autenticación 802.1x con un servidor de autenticación, generalmente un servidor RADIUS.

Requiere una implementación compleja, pero da una seguridad extra. Más adelante profundizaremos más en este tema, hablando de los servidores RADIUS y del Protocolo de Autenticación Extensible (EAP).

- WPA-Personal: este modo permite la implementación de una infraestructura segura basada en WPA sin tener que utilizar un servidor de autenticación. Se basa en el uso de una clave compartida (PSK) en el AP y el cliente. Esta clave solo se utiliza como punto de inicio de la autenticación, pero no para el cifrado de los datos.

2.3.8.1.3. WPA2

En Junio de 2004 se ratificó el nuevo estándar IEEE 802.11i. Se creó para corregir las vulnerabilidades detectadas en el protocolo WEP.

Aunque tiene el inconveniente de no ser compatible con el hardware anterior, tiene la ventaja de ser mucho más seguro.

La Alianza Wi-Fi, debido al éxito del estándar WPA y a la popularidad del término, decidió rebautizar el estándar 802.11i con el nombre WPA2, que es como se conoce actualmente.

Al igual que el protocolo WPA, WPA2 incluye el intercambio dinámico de la clave, un cifrado mucho más fuerte, y la autenticación de usuario, pero añade las mejoras siguientes:

- Nuevo algoritmo de cifrado AES (Advanced Encryption Standard). Se trata de un algoritmo de cifrado de bloque simétrico. Utiliza la misma clave para cifrar y descifrar, y el texto en claro se divide en bloques más pequeños que se cifran por separado de manera iterativa.
- Utiliza el protocolo CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) para asegurar la integridad y la autenticidad de los mensajes. Este protocolo utiliza el cifrado AES en lugar

de los códigos MIC (Message Integrity Code), y utiliza llaves de 128 bits con vectores de inicialización de 48 bits.

Igual que WPA, WPA2 puede funcionar en los modos WPA2-Enterprise y WPA2-Personal, ambos descritos anteriormente.

2.3.9. Elementos básicos de una red WLAN

2.3.9.1. Punto de Acceso

Es un dispositivo inalámbrico central de una red inalámbrica WiFi que por medio de ondas de radio frecuencia (RF) recibe información de diferentes dispositivos móviles y la transmite a través de cable al servidor de la red cableada o viceversa.

El estándar 802.11 es bastante ambiguo y no define con claridad todas las funciones que debería realizar un Punto de Acceso y sólo lo describe de una manera muy superficial. Esto dio lugar a que cada fabricante lo diseñara según su criterio y, por lo tanto existen en el mercado decenas de Puntos de Acceso con características y funcionalidades muy dispares.

Es aconsejable mantener el punto de acceso en un lugar alto para poder disponer de una buena emisión/recepción. Es posible que si no disponemos de la velocidad de emisión/recepción esperada sea por mala ubicación del punto de acceso, o de obstáculos que se interpongan entre el punto de acceso y el dispositivo WiFi (paredes, puertas...).

Figura 19 Ejemplo de un punto de acceso comercial
Fuente: TP-LINK TL-WA801ND http://www.pcworld.co.uk/

2.3.9.2. Adaptadores de red inalámbricos

Los hay de muy diversos tipos como ordenadores portátiles, PDA, teléfonos móviles... Estos pueden tener instaladas diferentes clases de tarjetas, mayoritariamente:

- Las tarjetas PCI para WiFi se agregan a los ordenadores de sobremesa, permiten un acceso muy eficiente, la única desventaja de este tipo de tarjeta es que requiere abrir el ordenador.

Figura 20 Ejemplo de un PCI WiFi
Fuente: Elegir antena PCI o USB http://www.chw.net

- Las tarjetas PCMCIA son un modelo muy utilizado en ordenadores portátiles; aunque en un principio la mayor parte de estas tarjetas solo eran capaces de llegar hasta la tecnología del 802.11b, actualmente ya existen tarjetas PCMCIA con tecnología 802.11g e incluso 802.11n (adelantándose a la aprobación final).

Figura 21 Ejemplo de PCMCIA
Fuente: Tarjeta red tarjeta Pcmcia http://www.pcexpansion.es

- Las tarjetas USB para WiFi son el tipo de tarjeta más moderno que existe y más sencillo de conectar a un PC, ya sea de sobremesa o portátil, haciendo uso de todas las ventajas que tiene la tecnología USB, además la mayor parte de las tarjetas USB actuales permiten utilizar la tecnología g de WiFi, incluso algunas ya ofrecen la posibilidad de utilizar la llamada tecnología 802.11n, que aún no está estandarizada.

Figura 22 Ejemplo de dongle USB a WiFi
Fuente: Tipos de dongle USB:Wifi http://www.informatica-hoy.com.ar

2.4. Proxy

Un servidor proxy es un equipo que actúa de intermediario entre los equipos de la red local y otras redes externas a la organización, encargándose de realizar las peticiones a los servidores de Internet en nombre de los equipos de la red interna. Los equipos y servidores de las redes externas no pueden conocer la identidad de los equipos por lo que actúa el servidor proxy.

De este modo todas las conexiones pasan a través de un único equipo, que se encarga de la supervisión y control, además proporciona mayor seguridad a la red local frente a intentos de acceso desde otras redes.

A partir de este dispositivo el administrador de la red puede negar o permitir el acceso a internet y a los servicios de la organización de forma selectiva.

Al conectarse todos los equipos al servidor proxy, estos pueden compartir una única línea de comunicaciones (línea ADSL, cable de fibra óptica, otros) y una única dirección IP. También lo usuarios se verán obligados a cumplir con la restricciones configuradas en el proxy.

Es necesario implantar una serie de restricciones y emplear algunas de las funciones del servidor proxy que permiten llevar a cabo un control y registro de las conexiones a internet, con la posibilidad de contemplar franjas horarias, distintas prioridades en el ancho de banda disponible y la implementación de filtros de acceso a contenidos.

Figura 23 Red WLAN con servidor Proxy
Fuente: Redes http://rpc.yoreparo.com

El servidor proxy es capaz de realizar las siguientes funciones:

- Definición de los permisos de acceso a los servicios de Internet, controlando que equipos y que usuarios pueden utilizarlos. Posibilidad de contemplar franjas horarias y filtros de acceso a contenidos
- Compartición de un número limitado de direcciones publicas externas entre varios equipos de la red local. Traducción de direcciones privadas a direcciones publicas mediante el protocolo NAT.
- Bloqueo del acceso a determinadas direcciones IP y dominios de Internet.
- Auditoria de la utilización de los servicios de internet y del consumo de ancho de banda.
- Memoria cache de páginas más visitadas (optimización del ancho de banda).
- Filtrado de paquetes e instalación de filtro de aplicación y de filtros de detección de intrusiones.
- Instalación de un antivirus perimetral.

2.5. Firewall.

Un firewall (cortafuegos) es un sistema que realiza un filtrado de paquetes de datos a partir de unas reglas definidas por el administrador de la red, teniendo en cuenta las direcciones IP de origen o de destino (es decir de que ordenador provienen y a que ordenador van dirigidos los paquetes de datos) y el servicio de red al que se corresponden.

Un cortafuego está constituido por un dispositivo hardware, es decir, por una maquina específicamente diseñada y construida para esta función, aunque también podría utilizarse un software que se instala en un ordenador conectado a la red de la organización.

No obstante, a diferencia con un servidor proxy, en este caso los equipos de la red interna sí podrían establecer una conexión directa con otras máquinas y servidores remotos ubicados en internet, siempre y cuando esta conexión sea autorizada por el cortafuego.

De este modo el cortafuego permite establecer dos zonas de trabajo independientes: la zona segura o de confianza, correspondiente a los equipos de la red local de la organización, en contraposición con la zona no segura (inside), en la que se ubicaran los demás equipos de redes externas (outside).

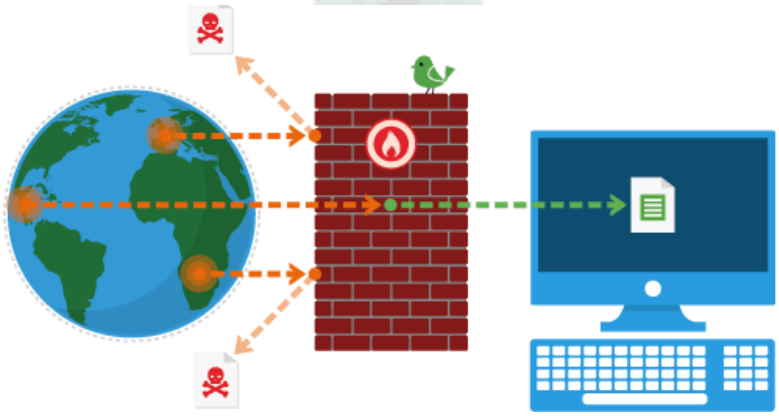

Figura 24 Firewall y su función en una red de datos
Fuente: Como configurar un firewall Cisco Pix https://alteageek.com

2.5.1. Servicios de protección que ofrece un firewall

- *Bloqueo del tráfico no autorizado por la organización:* servicios de internet que se deseen restringir (ftp, telnet, ssh, etc.), bloqueo de determinadas direcciones de equipos que se deseen restringir o de ciertas páginas web, etc.
- *Ocultación de los equipos de la red local de la organización*, de forma que estos puedan resultar "invisibles" ante posibles ataques provenientes del exterior. Asimismo, los cortafuegos pueden ocultar información sobre la topología de la red local, los nombres de los equipos (protocolo smb), los dispositivos de red utilizado (ataque de reconocimiento), etc.
- *Registro de todo el tráfico* entrante y saliente de la red corporativa.
- *Redirección del trafico entrante hacia determinadas zonas restringidas o especialmente vigiladas* (zona DMZ= zona desmilitarizada, no se tomara esta zona en el presente proyecto debido a que es una zona que es más usada para servidores de infraestructuras más grandes de las que se está considerando).

2.5.2. Tipos de Firewalls

- *Firewall que actúan a nivel de paquetes de datos:* se encargan del filtrado de los paquetes IP teniendo en cuenta las direcciones de origen y destino, asi mismo como los puertos utilizados. Son los más sencillos y los que ofrecen mejores prestaciones, ya que consumen menos recursos computacionales y de ancho de banda.
- *Firewall que actúa a nivel de circuito:* en este caso, además de la información sobre las direcciones de origen y destino y de los puertos utilizados, también tiene en cuenta los estados de la sesión ("stateful inspection"). De este modo, las reglas de filtrado tienen en cuenta la información de la cabecera de los paquetes IP ("flags") relativa al estado de la sesión y los números de la secuencia de los paquetes. Por este motivo, al tener conocimiento del paquete que se espera en cada caso, estos cortafuegos pueden detectar y

evitar cierto tipo de ataques, como los que pueden intentar llevar a cabo un secuestro de sesion (“sesión hijacking”).

- *Firewall que funciona como “pasarela de aplicación”:* se encargan de analizar todos los paquetes de datos correspondientes a un determinado servicio o aplicación, teniendo en cuenta las reglas del protocolo en cuestión y los estados de la sesión, y no solo los datos de los paquetes individuales. Por este motivo, solo se pueden utilizar para el servicio o aplicación para el que han sido diseñados, por lo que se requiere un Gateway o pasarela de aplicación por cada servicio, utilizando un protocolo como SOCKS para la comunicación con los equipos internos.

2.6. IDS/IPS

2.6.1. IDS, Sistema detector de intrusiones.

Los sistemas de detección de intrusiones (Intrusion Detection Systems, IDS) son los sistemas encargados de detectar y reaccionar de forma automatizada ante los incidentes de seguridad que tienen lugar en las redes y equipos informáticos.

Para ellos estos sistemas se encargan de monitorear el funcionamiento de los equipos y de las redes en busca de indicios posibles incidentes o intentos de intrusión, avisando a los administradores del sistema informático ante la detección de cualquier actividad sospechosa mediante una serie de alarmas e informes.

En la arquitectura de un IDS podemos distinguir los siguientes elementos funcionales básicos:

- Una fuente de información que proporcionara eventos del sistema o red informática.
- Una base de datos de patrones de comportamiento considerados como normales, así como los perfiles de los diferentes tipos de ataques.
- Un motor de análisis encargado de detectar evidencias de intentos de intrusión.
- Un módulo de respuesta capaz de llevar a cabo determinadas actuaciones a partir de las indicaciones del motor de análisis.

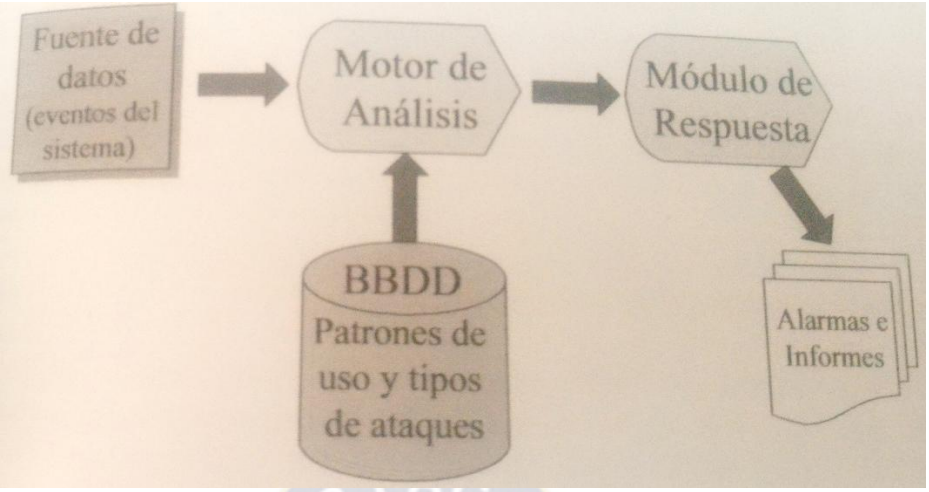

Figura 25 Arquitectura de un Sistema de Detección de Intrusiones
Fuente: Cap. 16 Herramientas de seguridad, libro Enciclopedia de la seguridad informática

Por otra parte, un IDS puede utilizar dos modelos de detección:

- *Detección de un mal uso*: tipos ilegales de trafico secuencia utilizadas para realizar ataques contra los equipos ("exploits"), escaneo de puertos, etcétera.
- *Detección de un uso anómalo*: análisis estadístico del tráfico en la red, monitorización de procesos y del comportamiento de los usuarios, con el fin de poder detectar aquellos comportamientos que se pueden considerar anómalos según los patrones de uso registrados hasta el momento, franjas horarias, utilización de puertos y servicios.

2.6.2. Tipos de IDS

- *HIDS (Host IDS):* pueden detectar las intrusiones a nivel de "host", es decir, a nivel de equipo informático, observando para ellos si se han producido alteraciones significativas de los archivos del sistema operativo o analizando los "logs" del equipo en busca de actividades sospechosas.
- *MHIDS (Multihost IDS):* este tipo de IDS permite detectar actividades sospechosas en base a los registros de actividad de diferentes equipos informáticos. Por este motivo también se los conoce como sistemas "IDS distribuidos".
- *NIDS (Network IDS):* se instalan en una red de ordenadores para monitorizar el tráfico de red en busca de cualquier actividad sospechosa, escaneo de

puertos, intentos de explotación de agujeros de seguridad en los servicios instalados en los equipos de red, ataques conocidos contra determinados protocolos, intentos de ejecución de scripts CGI vulnerable en los servidores, etc.

- *IPS ("Intrusion Prevention Systems):* es un sistema que permite prevenir las intrusiones. Se trata, por lo tanto, de un tipo de sistema que pretende ir un poco más allá de los IDS convencionales, ya que puede bloquear determinados tipos de ataques antes de que estos tengan éxito.

2.6.3. Raspberry Pi

Raspberry Pi es el nombre que recibe un modelo de ordenador de placa reducida (SBC, Single Board Computer) lanzado en 2011. El proyecto Raspberry Pi surge en 2006 de la mano de Eben Upton, Rob Mullins, Jack Lang y Alan Mycroft, a partir de la idea de crear un ordenador de bajo costo orientado a la enseñanza de conocimientos informático a los alumnos más jóvenes. Asi en 2009 surge la organización Raspberry Pi Fundation.

En agosto 2011, un primer modelo Alpha del Raspberry Pi es lanzado, mostrando algunas de las características que posteriormente serían las que integre el prototipo final.

En febrero de 2012 empieza la comercialización del Raspberry Pi en dos modelos A y B, a partir de los cuales en los últimos anos serian liberado dos versiones más.

2.6.4. Comparación entre versiones

	Raspberry Pi	Raspberry Pi 2	Raspberry Pi 3
Fecha de lanzamiento	Febrero de 2012	Febrero de 2015	Febrero de 2016
CPU	ARM1176JZF-S	ARM Cortex-A7	ARM Cortex-A53
Velocidad del CPU	700 MHz	900 MHz	1200 MHZ

RAM	512 MB (256 MB rev 1)	1 GB	1GB
GPU	Broadcom Videocore IV	Broadcom Videocore IV	Broadcom Videocore IV
Almacenamiento	Ranura SDHC y ranura MicroSDHC	Ranura MicroSDHC	Ranura MicroSDHC
Puertos USB	Dos en el modelo B	4	4
WiFi	Sin WiFi	Sin WiFi	802.11n y Bluetooth 4.1

Tabla 1 Tabla de comparación de versiones de Raspberry Pi
Fuente: The Raspberry Pi 1, 2 and 3 compared https://www.stewright.me

2.6.5. Accesorios Necesarios

Para poder interactuar y desarrollar el Sistema necesario para el controlador central se necesita contar con algunos periféricos aparte del propio Raspberry PI. Entre los dispositivos necesarios son los siguientes.

2.6.5.1. HUB USB.

Dependiendo de la versión de Raspberry Pi a usar, la cantidad de puertos usb del hub puede variar, con el fin de tener más capacidad de conectar otros dispositivos como memorias flash, dispositivos usb a bluetooth, etc.

Figura 26 Hub USB de 3 puertos
Fuente: http://www.peruhardware.net

2.6.5.2. Teclado y ratón

Para poder interactuar con el Raspberry Pi, se necesita un teclado y un ratón, ambos USB.

Otra alternativa son el teclado bluetooth, el ratón bluetooth o teclado touchpad (teclado con mouse pad), todos con sus respectivos dongle usb a bluetooth.

Figura 27 Mini teclado Mouse Pad
Fuente: Mini teclado mouse Pad http://articulo.mercadolibre.com.ar

1.6.5.4. Monitor

Se necesita un monitor con un puerto HDMI para poder visualizar la información generada por el Raspberry Pi.

Otra opción más económica y para reutilizar televisores analógico a colores con conectores rca (el cable necesitara algunas modificaciones).

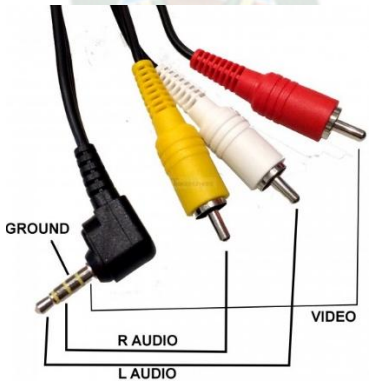

Figura 28 Configuración del cable adaptador de compuesto a RCA
Fuente: Composite to RCA adapter http://tinkersphere.com

1.6.5.5. Tarjetas MicroSD

Como parte de almacenamiento es necesario utilizar las tarjetas micro sd que se pueden encontrar en el mercado local.

Como mínimo debe ser una tarjeta microSD clase 4 de 4 GB a mas (dependiendo de la distribución a usarse en caso de ser sistema operativo Linux)

Lo habitual y recomendación de mejores prácticas para no sacrificar rendimiento, memoria microSD clase 10 de 16 GB. Lo máximo en el caso de ser la versión 3 se puede usar microSD de 32 GB.

1.6.5.6. Accesorios disponibles

Aunque estos dispositivos no son necesarios, es interesante incluir algunos de estos, según el uso que se le dará al miniordenador.

- Adaptador inalámbrico: como se vio en el cuadro 2, las primeras dos versiones no cuentan con bluetooth ni WiFi, pero la versión tres si, a lo cual es poco usual a esta última comprarle adaptadores comunes.
- Dispositivos para puertos GPIO (General Purposse Input/output o Entrada/Salida de propósito general): el puerto GPIO del Raspberry Pi permite la utilización de numerosos dispositivos digitales a partes de la integración de diferente pines de comunicación digital, y puertos de alimentación que funcionan 5 V. De esta forma, podemos diseñar dispositivos como cámaras o paneles de visualización, receptores de telefonía celular que añadan nuevas funcionalidades a nuestro sistema.

Figura 29 Modulo 4G y GPS para Raspberry Pi
Fuente: PiAnywhere 4G http://www.pianywhere.com/

1.6.5.7. Soporte Software

Desde su lanzamiento, existen números versiones de distribuciones (versiones del sistema operativo Linux) disponibles para su instalación en el Raspberry Pi.

Dentro de las distribuciones oficiales se encuentran los que pertenecen parte del proyecto:

- NOOBS
- Raspbian

Las distribuciones de terceras partes y en el último año también incursiono Windows

- Ubuntu MATE
- Snappy Ubuntu Core
- Windows 10 IOT Core
- OSMC
- Libreelec
- Pinet
- Risc OS
- Weather Station

En los últimos años varias otras distribuciones sacaron versiones para procesadores arm de manera no oficial (in coordinar con la gente del proyecto Raspberry Pi), entre los más importantes estarían:

- Centos
- Kali Linux

3. INGENIERIA DEL PROYECTO

3.1. Diagrama de bloques del sistema de detección, prevención de intrusiones, y monitoreo de una red inalámbrica de área local

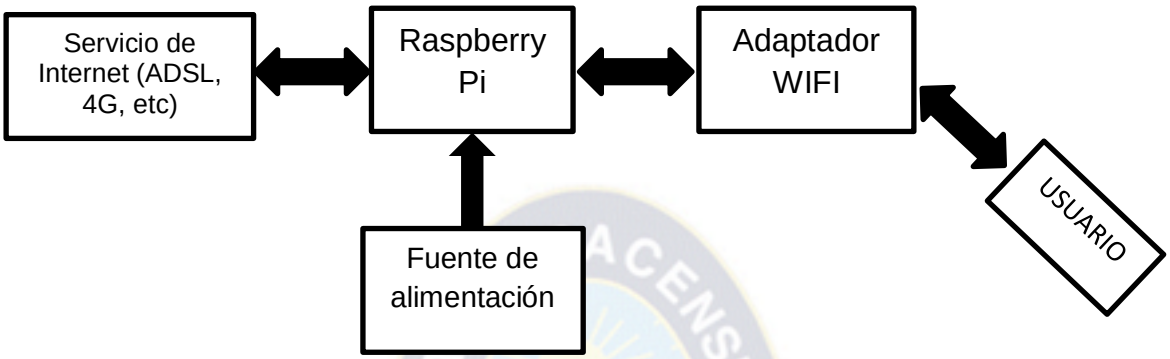

Figura 30 Diagrama de bloques del sistema principal de la red inalámbrica
Fuente: Diseño propio

3.1.1. Adaptador USB a WIFI

Debido a la elección del raspberry pi, se debe escoger una adaptador wifi que sea compatible con él, que encuentre certificado por la alianza WIFI y que pueda su chipset pueda trabajar en modo AP.

En la siguiente tabla se mostrara algunos de los adaptadores WiFi comerciales.

Fabricante	Nombre	Descripción del hardware	Debian	Raspbian	Otros	Modo AP	Ad-Hoc
Adafruit	Módulo WiFi miniatura	Realtek RTL8192cu	Wheezy	preinstalado	OpenLec	Si	-
ALFA Network	AWUS036NH	Ratlink RT3070	Wheezy	Instalar aircrack-ng	-	Si	-
ALFA Network	AWUS036NHA	Atheros AR9271	-	Instalar aircrack-ng	-	-	-
TP-LINK	TL-WN722N	Atheros ath9k_htc	-	Si	Archlinux	Si	Si
TP-LINK	TL-WN822N v1.1	Atheros AR-9170	-	SI	Archlinux	Si	Si
TP-LINK	TL-WN822N v2	Atheros AR-9287	-	SI	Archlinux	Si	Si

Tabla 2 Tabla de los adaptadores WiFi compatibles con Raspberry pi
Fuente: RPi USB Wi-Fi Adapters http://elinux.org

El adaptador elegido es el TP-LINK WN822N v2, por su disponibilidad en Bolivia. Sus características son:

CARACTERÍSTICAS DE HARDWARE	
Interfaz	Mini USB 2.0
Botón	botón QSS/Software
Dimensiones (W X D X H)	3.5 x 2.7 x 0.7 pulgadas. (90 x 68 x 16.8mm)
Tipo de Antena	Dual Omnidireccional
Ganancia de Antena	3dBi

CARACTERÍSTICAS INALÁMBRICAS	
Wireless Standards	IEEE 802.11n, IEEE 802.11g, IEEE 802.11b
Frequency	2.400-2.4835GHz
Signal Rate	11n: Hasta 300Mbps(dinámica) 11g: Hasta 54Mbps(dinámica) 11b: Hasta 11Mbps(dinámica)
Reception Sensitivity	270M: -68dBm@10% PER 130M: -68dBm@10% PER 108M: -68dBm@10% PER 54M: -68dBm@10% PER 11M: -85dBm@8% PER 6M: -88dBm@10% PER 1M: -90dBm@8% PER
Transmit Power	<20dBm(EIRP)
Wireless Modes	modo Ad-Hoc / Infraestructura
Wireless Security	Soporta 64/128 bit WEP, WPA-PSK/WPA2-PSK
Modulation Technology	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Advanced Functions	WMM

Figura 31 Características de Hardware de TP-LINK WN822N v2
Fuente: TP-LINK WN822N http://www.tp-link.com

Figura 32 Imagen del adaptador TP-LINK WN822N v2
Fuente: TP-LINK WN822N https://www.amazon.es

3.1.1.1. Diagrama circuital del adaptador

El adaptador escogido TL-WN822N está desarrollado a partir de la arquitectura de atheros AR9287+AR7010, el cual se procederá a describir a continuación.

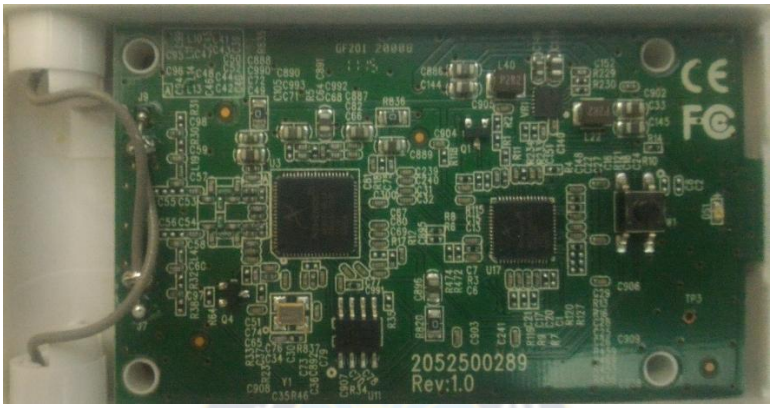

Figura 33 Circuito interno del adaptador TL-WN822N
Fuente: Foto del adaptador a usar

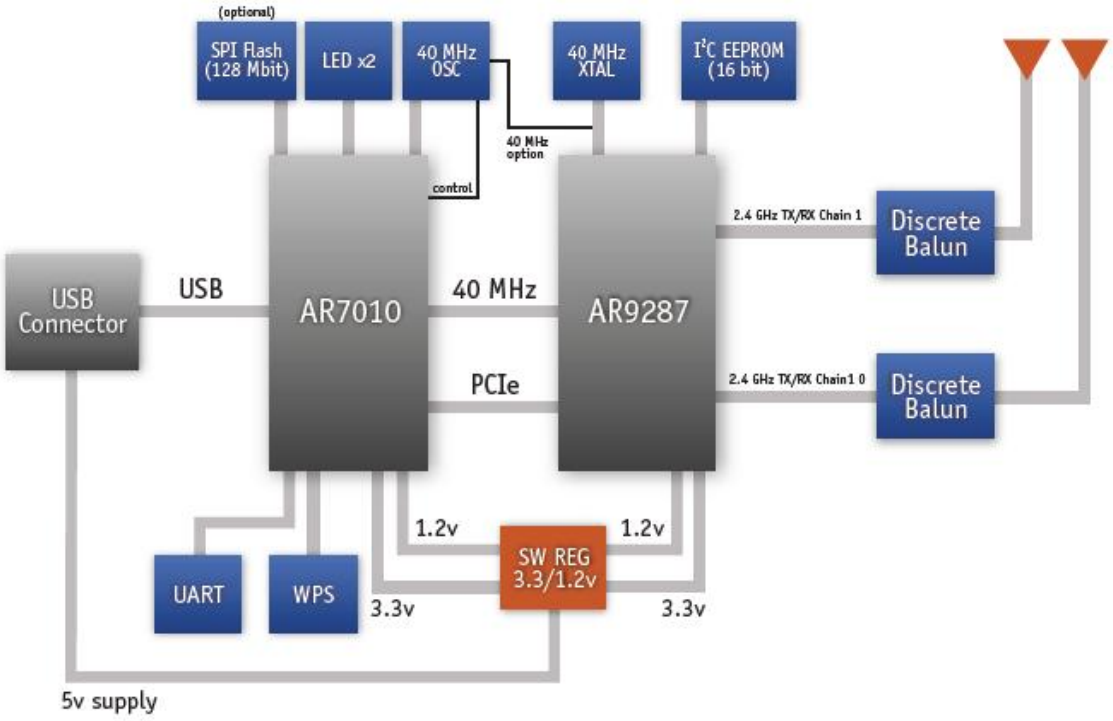

Figura 34 Diagrama circuital del adaptador usb wifi TL-WN822N
Fuente: https://wikidevi.com/files/Atheros/specsheets/AR7010+AR9287.pdf

- ❖ USB Conector: es la interfaz que transmite y recibe del chipset los datos hacia y desde el miniordenador. También recibe la alimentación del puerto USB del miniordenador
- ❖ Regulador de 5V a 3.3V/1.2: a partir del voltaje de 5V recibido por el conector usb lo regula a 3.3V y a 1.2V, para alimentar al chipset AR7010 y al chipset AR9287
- ❖ XTAL de 40MHz: es el reloj que sincroniza a ambos chipset
- ❖ AR9287: es el chipset de Atheros para redes inalámbricas que cumplan con el estandar 802.11n bajo la frecuencia de 2.4GHz. Este chip integra un multi protocolo MAC, procesador de banda base, conversor análogo digital y digital a análogo.
- ❖ AR7010: es el chipset de Atheros que proporciona un punto de acceso para redes inalámbricas bajo el estándar 802.11n, Posee las funcionalidades de encapsulación, desencapsulacion, agregación control de velocidad y baliza.

3.1.2. Raspberry Pi.

El raspberry pi elegido es el raspberry pi v3, este posee 1GB de memoria RAM, cuatro puertos USB, son los rasgos más destacables respecto a otras versiones.

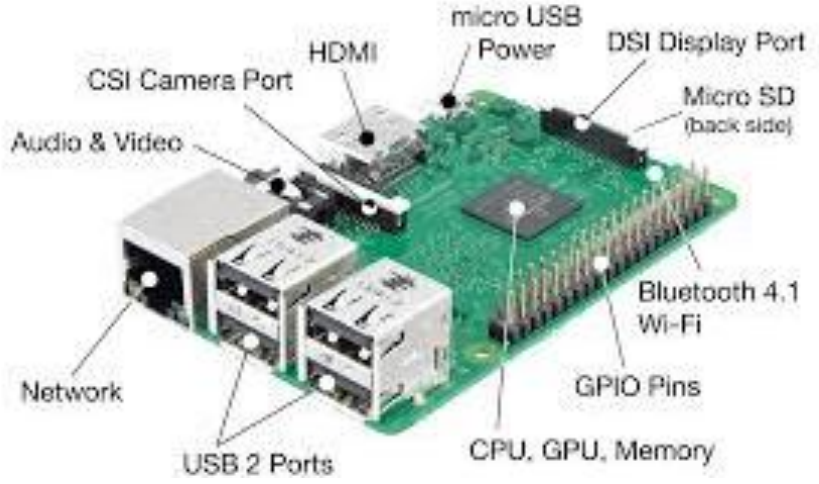

Figura 35 Raspberry Pi v3 modelo B
Fuente: Lab 4 Raspberry Pi Setup http://ocw.cs.pub.ro

3.1.2.1. Diagrama circuital del Raspberry PI 3

El raspberry pi es un proyecto del tipo hardaware libre. A continuación describiremos el funcionamiento de los circuitos que se encuentran en el raspberry y que haremos uso.

- Circuito regulador: es el encargado de recibir 5V de alimentación, estabilizar la alimentación y proteger a los demás componentes

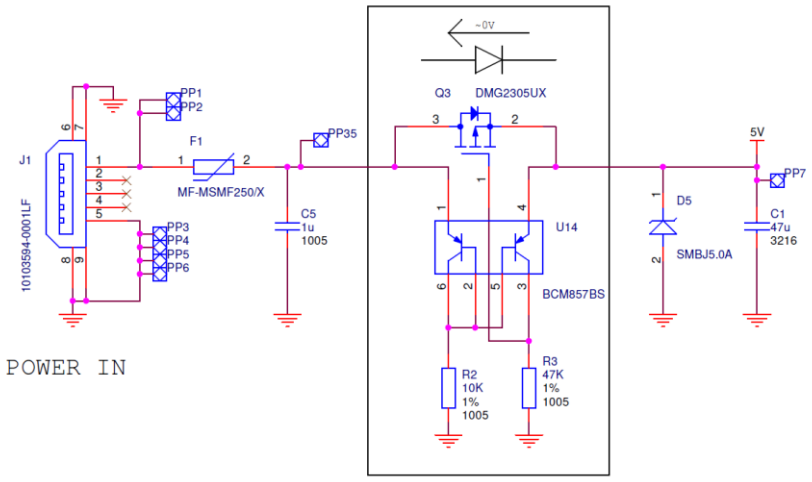

Figura 36 Circuito regulador de alimentación
Fuente: RPI-3B-V1_2-SCHEMATIC-REDUCED.pdf https://www.raspberrypi.org

- Leds de encendido y estado: son leds que nos avisan si el miniordenador esta encendido y si a cargado la distribucion a usar

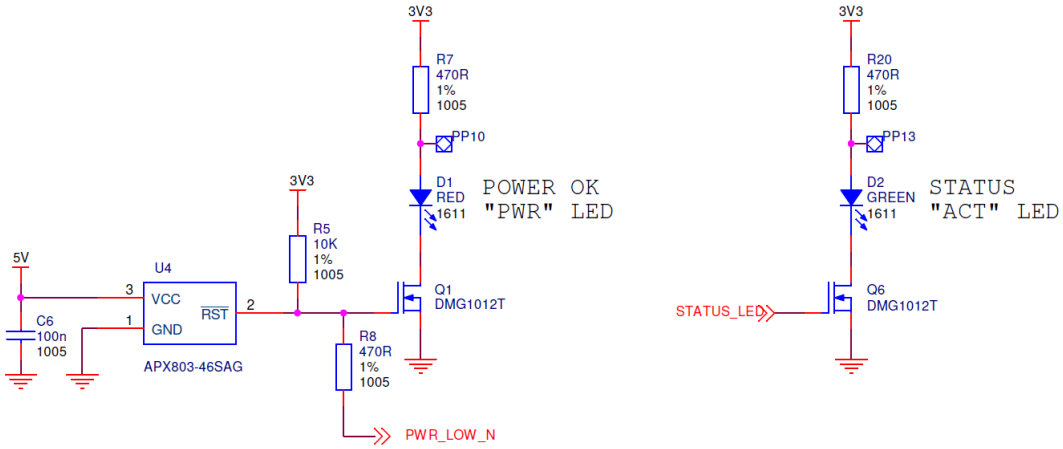

Figura 37 Circuito de leds de encendido y estado
Fuente: RPI-3B-V1_2-SCHEMATIC-REDUCED.pdf https://www.raspberrypi.org

- Circuito reloj: se encarga de sincronizar last areas realizadas por los diferentes components, pero todas estas a partir del CPU BCM2837

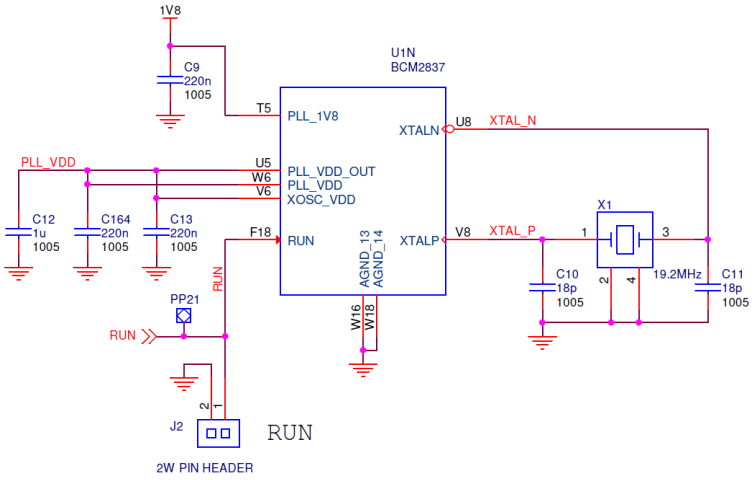

Figura 38 Circuito reloj del CPU BCM2837

Fuente: RPI-3B-V1_2-SCHEMATIC-REDUCED.pdf https://www.raspberrypi.org

- Lector de micro SD: es el encargado de leer el sistema operativo que se encuentre en la memoria micro SD y enviarlo al CPU BCM2837

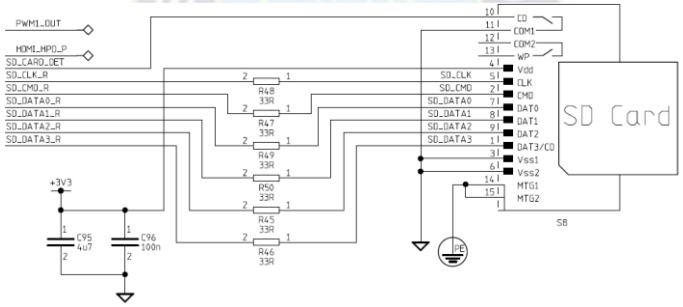

Figura 39 Lector de Micro SD

Fuente: https://cdn-shop.adafruit.com/datasheets/pi2schem.pdf

- Circuito de video compuesto: es el que se comunica con el CPU y genera la señal de video y audio compatible con las entradas RCA de un televisor analógico.

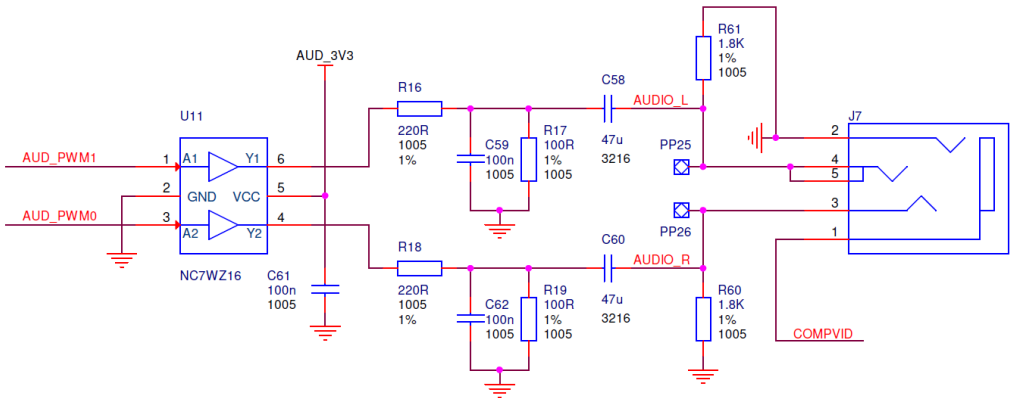

Figura 40 Circuito compuesto de video

Fuente: RPI-3B-V1_2-SCHEMATIC-REDUCED.pdf https://www.raspberrypi.org

- Circuito USB y Ethernet: A partir del integrado LAN9514 que tiene las características de estar compuesto por 4 puertos USB 2.0 y un puerto fastethernet, este circuito es un periférico del CPU BCM2837

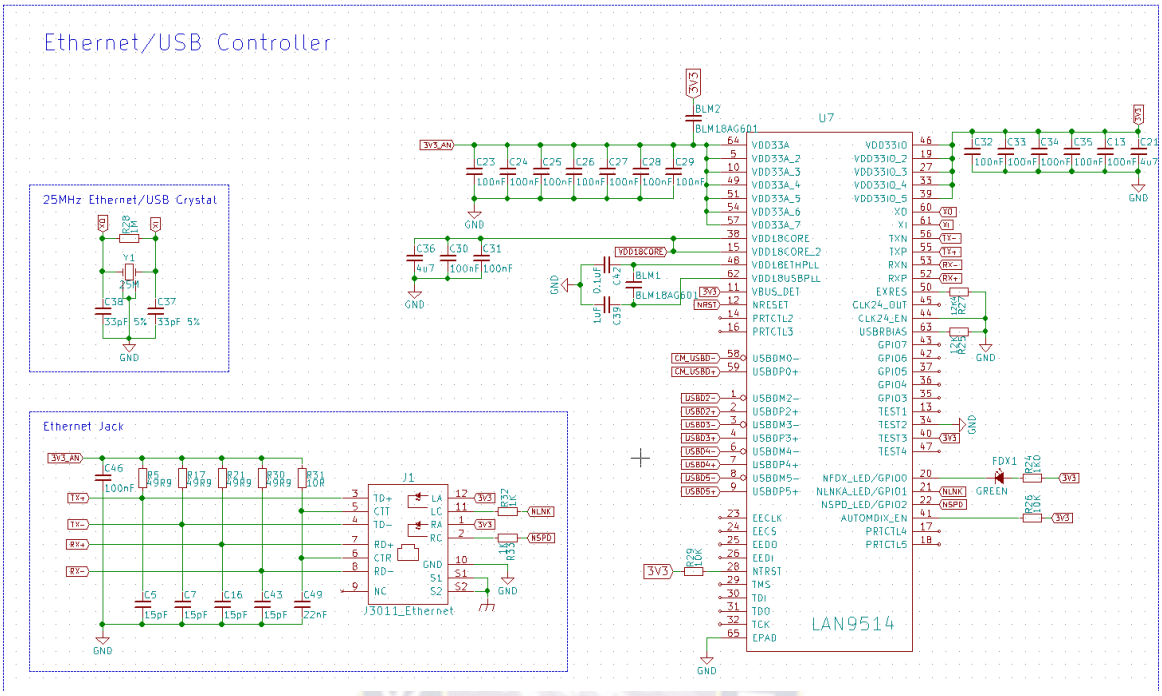

Figura 41 Circuito del integrado LAN9514
Fuente: https://www.raspberrypi.org/forums/viewtopic.php?f=98&t=141974

3.1.3. Criterios de funcionamiento del trabajo de aplicación

Anteriormente se expuso la operación que realizan los diferentes circuitos que componen el miniordenador elegido, como ser el raspberry pi. Ahora explicaremos el proceso de como se generara la red inalámbrica y se otorgaran los direntes servicios.

El adaptador de red inalámbrica al conectarse al puerto USB del Raspberry pi será reconocido sus 2 chipset (ar7010 y ar9287) por el CPU BCM2837, este apartir del software que posee mandara datos a través del integrado LAN9514 al adaptador de red inalámbrica, con la orden de actuar como un punto de acceso.

El adaptador usb de red inalámbrica a través de su chipset AR7010 generara la red inalámbrica, los parámetros de esta seran definidas desde el miniordenador.

De esta manera el adaptador de red WiFi solo será un transmisor y receptor, mientras que el raspberry pi será el elemento que realice todas las tareas de análisis, monitoreo y mande los parámetros de configuración de la red wifi.

3.1.4. Servicios del Raspberry Pi

Este dispositivo realizara todas las tareas del sistema planteado.

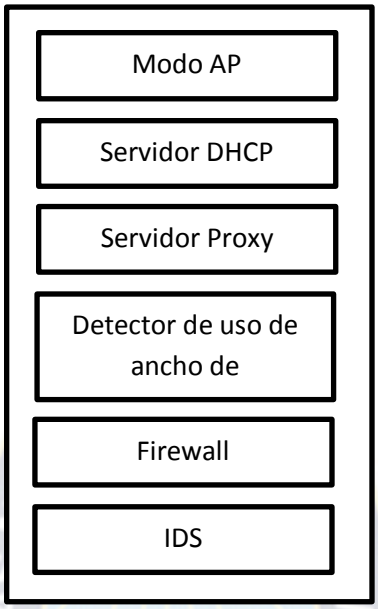

Figura 42 Diagrama de bloques de los sistemas que procesara el raspberry pi
Fuente: Diseño propio

3.1.4.1. Configuración básica

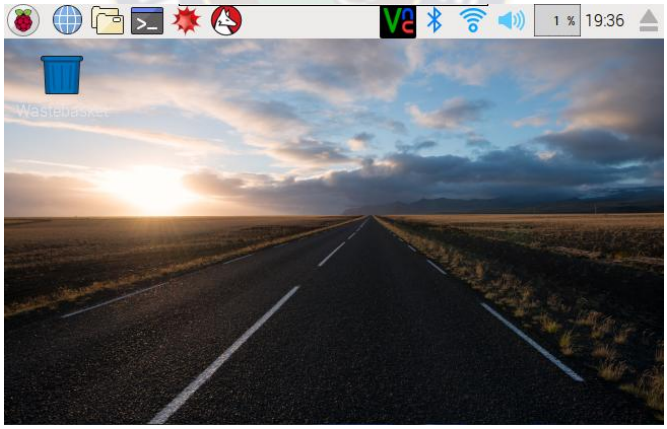

Figura 43 Escritorio del Raspbian
Fuente: Captura de pantalla.

En la consola:

##Preparar la Raspberry pi

#actualizar la distribución

sudo apt-get update && apt-get –y dist-upgrade

#actualizar el kernel

sudo rpi-update

#configurar interfaz wan o isp(eth0), la dirección gateway de la red inalámbrica(wlan1)

#sudo nano /etc/network/interfaces

```
auto eth0
allow-hotplug eth0
iface eth0 inet dhcp #de esta manera el isp tomara por dhcp(automáticamente)
#la dirección que provenga de equipo del proveedor de internet
allow-hotplug wlan1
iface wlan inet static
    address 192.168.21.1 #la dirección que del punto de acceso en la red
#inalámbrica, la cual será la dirección de gateway en las terminales
    netmask 255.255.255.0 #mascara de red de la red inalambrica
```

sudo service networking restart

#reiniciar

sudo reboot

3.1.4.2. Servidor DHCP

##instalar y configurar el servidor dhcp para la red inalámbrica

sudo apt-get install isc-dhcp-server

sudo nano /etc/dhcp/dhcpd.conf

```
#comentar las siguientes lineas:
#option domain-name “example.org”;
#option domain-name-servers ns1.example.org, ns2.example.org;
# añadir la configuración para el servicio dhcp
subnet 192.168.21.0 netmask 255.255.255.0 { #la red privada de la red inalámbrica
    range 192.168.21.10 192.168.21.50; #rango de las direcciones que se podrán
otorgar
option broadcast-address 192.168.21.255; #la dirección broadcast de la red inalámbrica
option routers 192.168.21.1;
default-lease-time 600;
max-lease-time 7200;
option domain-name “local”;
option domain-name-servers 8.8.8.8 8.8.4.4;
}
```

#asignar la interfaz que proveerá el servicio dhcp

sudo nano /etc/defaul/isc-dhcp-server

```
INTERFACES =”wlan1”
```

#realizar el arranque del servicio dhcp al arranque del sistema operativo

sudo service isc-dhcp-server start

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

3.1.4.3. Modo AP

##instalar hostapd

sudo apt-get install hostapd

##configurar los parámetros iniciales del Access point

sudo nano /etc/hostapd/hostapd.conf

```
interface=wlan1 # interface del adaptador wifi
logger_syslog=-1
logger_syslog_level=0
logger_stdout=-1
logger_stdout_level=2
ctrl_interface=/var/run/hostapd
ctrl_interface_group=0
ssid=Electronica #nombre de la red inalambrica
country_code=BO #Codigo del pais
ieee80211d=1
hw_mode=g
channel=3
beacon_int=100
dtim_period=2
max_num_sta=255
rts_threshold=2347
fragm_threshold=2346
macaddr_acl=0
auth_algs=3
ignore_broadcast_ssid=0
wmm_enabled=1
wmm_ac_bk_cwmin=4
wmm_ac_bk_cwmax=10
wmm_ac_bk_aifs=7
wmm_ac_bk_txop_limit=0
wmm_ac_bk_acm=0
wmm_ac_be_aifs=3
wmm_ac_be_cwmin=4
wmm_ac_be_cwmax=10
wmm_ac_be_txop_limit=0
wmm_ac_be_acm=0
wmm_ac_vi_aifs=2
wmm_ac_vi_cwmin=3
wmm_ac_vi_cwmax=4
wmm_ac_vi_txop_limit=94
wmm_ac_vi_acm=0
wmm_ac_vo_aifs=2
wmm_ac_vo_cwmin=2
wmm_ac_vo_cwmax=3
wmm_ac_vo_txop_limit=47
wmm_ac_vo_acm=0
```

```
ieee80211n=0
eapol_key_index_workaround=0
eap_server=0
own_ip_addr=192.168.1.1
wpa_pairwise=TKIP CCMP
rsn_pairwise=CCMP
ht_capab=
wpa=3
wpa_passphrase=proyecto #contraseña de la red inalámbrica
```

#configurar el demonio del servicio

sudo nano /etc/default/hostapd

```
DAEMON_CONF=”/etc/hostapd/hostapd.conf”
```

sudo nano /etc/init.d/hostapd

```
DAEMON_CONF=/etc/hostapd/hostapd.conf
```

#levantar la red inalámbrica (sin la regla del firewall no podrá salir a internet)

sudo /usr/sbin/hostapd /etc/hostapd/hostapd.conf

#realizar el arranque del servicio hostapd al arranque del sistema operativo

sudo hostapd start

sudo update-rc.d hostapd enable

3.1.4.4. Firewall o Cortafuegos

##Instalar WEBMIN

nano /etc/apt/sourcelist.conf

```
deb http://download.webmin.com/download/repository sarge contrib #añadir esta línea
```

cd /root

#Descargar e instalar la llave del repositorio añadido

wget http://www.webmin.com/jcameron-key.asc

apt-key add jcameron-key.asc

#Instalar webmin desde el repositorio añadido

apt-get update

apt-get install webmin

##Instalar el firewall shorewall

apt-get install shorewall

Ingresar a 127.0.0.1:10000 (pagina de webmin)

#Crear las zonas de red

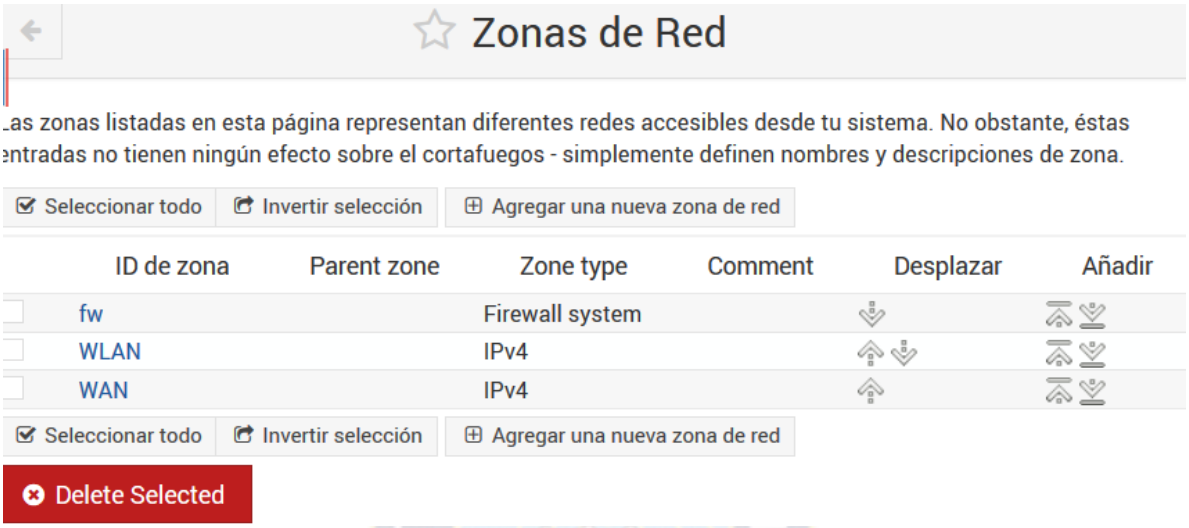

Figura 44 Zonas de red en el firewall
Fuente: Captura de pantalla

##Asignar las zonas a interfaces

Figura 45 Interfaces y zonas
Fuente: Captura de pantalla

##Creación política de firewall

Figura 46 Configuración de Políticas
Fuente: Captura de pantalla

##Creacion de la regla de NAT

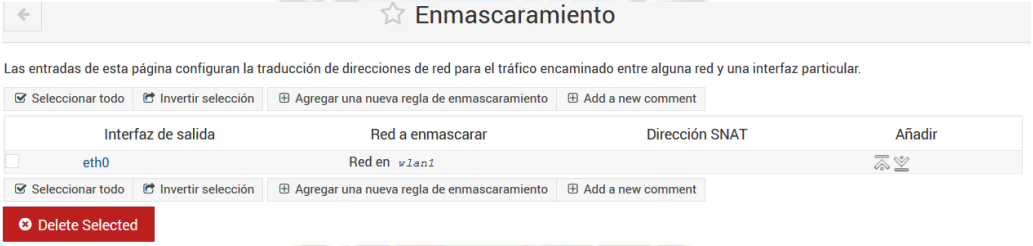

Figura 47 Configuración NAT
Fuente: Captura de pantalla

#habilitar el inicio de shorewall desde el arranque del sistema operativo

sudo nano ++4 /etc/default/shrewall
Startup=1

#si falla el arranque usar cron

Figura 48 Configuración de arranque de shorewall con cron
Fuente: Captura de pantalla

3.1.4.5. Servidor Proxy transparente

##Instalar el proxy squid, habilitar –enable -ssl

sudo apt-get install squid3

sudo apt-get build-dep squid3 openssh openssl

sudo apt-get install devscripts build-essential fakeroot libtool libssl-dev libcrypto++-dev devscripts ssl-cert squid-langpack libecap2-dev

cd /usr/src

sudo wget http://ftp.debian.org/debian/pool/main/squid3_3.4.8.orig.tar.bz2

sudo wget http://ftp.debian.org/debian/pool/main/squid3_3.4.8-6.debian.tar.xz

sudo tar –xvf squid3_3.4.8.orig.tar.bz2

sudo cd squid-3.4.8/

sudo tar –xvf ../squid3_3.4.8-6.debian.tar.xz

#anadir –enable-ssl \ y –enable-ssl-crtd \ en debían/rules

sudo nano debían/rules #despues de anadir las 2 lineas guardar y salir

./configure #empezaremos a compilar los nuevos paquetes de squid

debuild –us –uc –b –d

cd ..

dpkg –I squid3*.deb #instalaremos todos los archivos .deb que compilamos

squid3 –v #revisaremos la version de squid instalada y las opciones que este posee

/usr/libsquid3/ssl_crtd –c –s /var/lib/ssl_db/

chown –r proxy:proxy /var/lib/ssl_db/

mkdir /var/cache/squid

chown –r proxy:proxy /var/cache/squid/

chown –r proxy:proxy /var/spool/squid3

##Generar el certificado ssl

openssl genrsa –out squid.key 2048

openssl req –new –key squid.key –out squid.csr

openssl x509 –req –days 1825 –in squid.csr –signkey squid.key –out squid.crt

#configurar squid para que el Puerto 3128 escuche http y el Puerto 3130 https

Nano /etc/squid3/squid.conf

```
#Nombre del proxy
visible_hostname AccessPoint.localhost
#Almacenamiento de logs del proxy
access_log stdio:/var/log/squid3/access.log
cache_log /var/log/squid3/cache.log
coredump_dir /var/cache/squid
#Parametros SSL
ssl_bump none localhost
always_direct allow all
sslcrtd_program /usr/lib/squid3/ssl_crtd -s /var/lib/ssl_db/ -M 256MB
sslcrtd_children 50
sslproxy_cert_error allow all
sslproxy_flags DONT_VERIFY_PEER,NO_DEFAULT_CA
```

```
#Lista de acceso de la red WLAN
acl localnet src 192.168.21.0/24
#Ports allowed through Squid
acl SSL_ports port 443
acl Safe_ports port 80
acl Safe_ports port 21
acl Safe_ports port 443
acl CONNECT method CONNECT
#Acciones de permitir o denegar
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
http_access allow localnet
http_access allow localhost
http_access deny all
#Puertos del proxy
http_port 3128 intercept
https_port 3130 intercept ssl-bump generate-host-certificates=on
dynamic_cert_mem_cache_size=256MB cert=/etc/ssl/private/squid.crt
key=/etc/ssl/private/squid.key version=3
#Directorio de la memoria cache
cache_dir ufs /var/spool/squid3 500 16 256
cache_mem 512 MB
#Servidor DNS en el que se apoyara el squid
dns_nameservers 127.0.0.1
```

#reiniciar el servicio

Service squid3 restart

##Modificar políticas del firewall

Figura 49 Modificaciones de las políticas por defecto
Fuente: Captura de pantalla

#Modificaciones de las reglas del cortafuego

Acción	Origen	Destino	Protocolo	Puertos de origen	Puertos destino
ACCEPT	Host 192.168.1.0/24 de la zona WAN	Cortafuegos	TCP	Cualquiera	10000
ACCEPT	Host 192.168.1.0/24 de la zona WAN	Cortafuegos	TCP	Cualquiera	80
ACCEPT	Host 192.168.1.0/24 de la zona WAN	Cortafuegos	TCP	Cualquiera	443
ACCEPT	Host 192.168.1.0/24 de la zona WAN	Cortafuegos	TCP	Cualquiera	22
ACCEPT	Host 192.168.1.0/24 de la zona WAN	Cortafuegos	TCP	Cualquiera	5900
ACCEPT	Host 192.168.1.0/24 de la zona WAN	Cortafuegos	ICMP	Cualquiera	8
ACCEPT	Host 192.168.1.0/24 de la zona WAN	Cortafuegos	TCP	Cualquiera	3128
ACCEPT	Cortafuegos	Zona WAN	TCP	Cualquiera	22
ACCEPT	Cortafuegos	Zona WAN	TCP	Cualquiera	80
ACCEPT	Cortafuegos	Zona WAN	TCP	Cualquiera	443
ACCEPT	Cortafuegos	Zona WAN	TCP	Cualquiera	53
ACCEPT	Cortafuegos	Zona WAN	UDP	Cualquiera	53
ACCEPT	Cortafuegos	Zona WAN	UDP	Cualquiera	123
ACCEPT	Cortafuegos	Zona WAN	ICMP	Cualquiera	8
REDIRECT	Zona WLAN	Puerto 3128	TCP	Cualquiera	www
REDIRECT	Zona WLAN	Puerto 3130	TCP	Cualquiera	443
ACCEPT	Zona WLAN	Zona WAN	TCP	Cualquiera	80
ACCEPT	Zona WLAN	Zona WAN	TCP	Cualquiera	443
ACCEPT	Zona WLAN	Zona WAN	TCP	Cualquiera	22
ACCEPT	Zona WLAN	Zona WAN	TCP	Cualquiera	53
ACCEPT	Zona WLAN	Zona WAN	UDP	Cualquiera	53
ACCEPT	Zona WLAN	Zona WAN	TCP	Cualquiera	10000
ACCEPT	Zona WLAN	Zona WAN	TCP	Cualquiera	5900
ACCEPT	Zona WLAN	Zona WAN	UDP	Cualquiera	123
ACCEPT	Zona WLAN	Zona WAN	ICMP	Cualquiera	8

Figura 50 Reglas del firewall para el proxy transparente
Fuente: Captura de pantalla

##Configurar puertos y forma de trabajo del proxy

Figura 51 Configuración de puertos del proxy
Fuente: Captura de pantalla

Figura 52 Listas de Control de Acceso
Fuente: Captura de pantalla

Figura 53 Restricciones del proxy
Fuente: Captura de pantalla

```
visible_hostname AccessPoint.localhost
access_log stdio:/var/log/squid3/access.log
cache_log /var/log/squid3/cache.log
coredump_dir /var/cache/squid
ssl_bump none localhost
always_direct allow all
sslcrtd_program /usr/lib/squid3/ssl_crtd -s /var/lib/ssl_db/ -M 256MB
sslcrtd_children 50
sslproxy_cert_error allow all
sslproxy_flags DONT_VERIFY_PEER,NO_DEFAULT_CA
acl localnet src 192.168.21.0/24
acl SSL_ports port 443
acl Safe_ports port 80
acl Safe_ports port 21
acl Safe_ports port 443
acl CONNECT method CONNECT
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
http_access allow localnet
http_access allow localhost
http_access deny all
http_port 3128 intercept
https_port 3130 intercept ssl-bump generate-host-certificates=on dynamic_cert_mem_cache_size=256MB cert=/etc/ssl/private/squid.crt key=/etc/ssl/private/squid.key version=3
cache_dir ufs /var/spool/squid3 500 16 256
cache_mem 512 MB
dns_nameservers 127.0.0.1
shutdown_lifetime 3 seconds

```

Figura 54 Archivo de configuraciones
Fuente: Captura de pantalla

3.1.4.6. Control de Ancho de Banda

#Instalar SARG

Apt-get install sarg

#intalar fuentes de letra para el informe

sudo apt-get install fonts-dejavu and fonts-dejavu-core

sudo cp /usr/share/fonts/truetype/dejavu/DejaVuSansMono.ttf /usr/share/fonts/truetype/ttf-dejavu/DejaVuSansMono.ttf

sudo cp /usr/share/fonts/truetype/dejavu/DejaVuSans-Bold.ttf /usr/share/fonts/truetype/ttf-dejavu/DejaVuSans-Bold.ttf

sudo cp /usr/share/fonts/truetype/dejavu/DejaVuSans.ttf /usr/share/fonts/truetype/ttf-dejavu/DejaVuSans.ttf

sudo cp /usr/share/fonts/truetype/dejavu/DejaVuSansMono-Bold.ttf /usr/share/fonts/truetype/ttf-dejavu/DejaVuSansMono-Bold.ttf

sudo cp /usr/share/fonts/truetype/dejavu/DejaVuSerif-Bold.ttf /usr/share/fonts/truetype/ttf-dejavu/DejaVuSerif-Bold.ttf

cp /usr/share/fonts/truetype/dejavu/DejaVuSerif.ttf /usr/share/fonts/truetype/ttf-dejavu/DejaVuSerif.ttf

3.1.4.7. Detector de intrusiones

sudo apt-get install git python-pcapy

cd /home/pi

git clone https://github.com/stamparm/mailtrail.git

cd maltrail

sudo python sensor.py

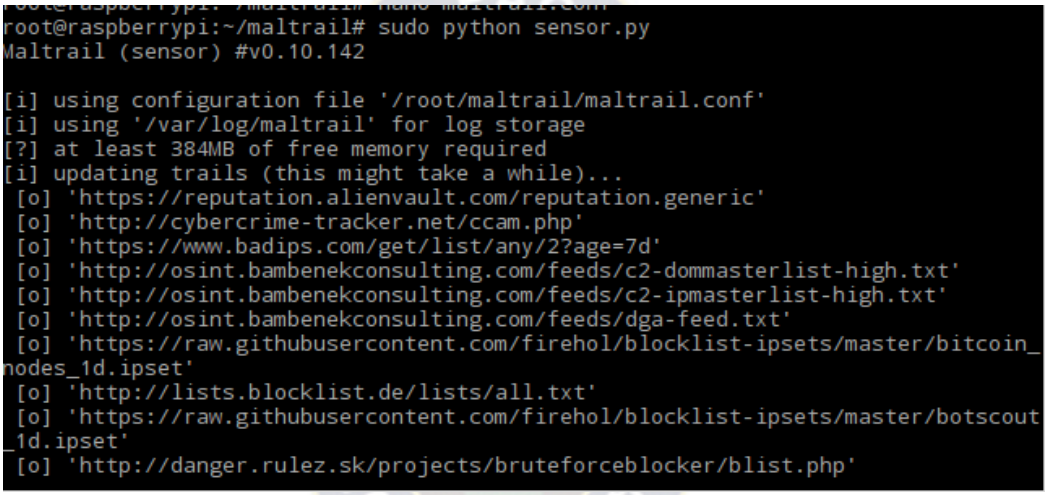

Figura 55 Descarga de Base de Datos
Fuente: Captura de pantalla

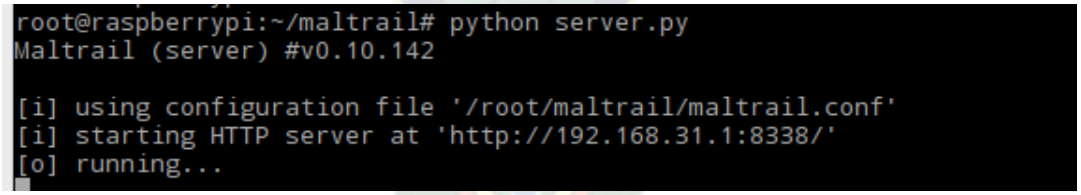

Figura 56 Arranque de la interfaz
Fuente: Captura de pantalla

#Configurar que se ejecuten desde el arranque sensor.py y server.py

nano /home/pi/launcher.sh

```
#!/bin/sh
# launcher.sh
cd /
cd home/pi/maltrail
sudo python server.py
cd /
```

nano /home/pi/launchsen.sh

```
#!/bin/sh
# launcher.sh
cd /
cd home/pi/maltrail
sudo python sensor.py
cd /
```

chmod 755 /home/pi/launcher.py

chmod 755 /home/pi/launchsen.py

root	Si	/etc/cron.monthly/sarg
root	Si	sh /home/pi/launchshor.sh
root	Si	sudo sh /home/pi/launcher.sh
root	Si	sudo sh /home/pi/launchsen.sh

Figura 57 Los scripts creados se ejecutaran al arrancar el sistema operativo
Fuente: Captura de pantalla

3.1.4.8. Página web de configuración

##instalar y configurar la página web de configuración de las características de la red inalámbrica

#instalar nginx con soporte de php

apt-get install –y nginx php5-fpm

#desahabilitar la pagina web por defecto de nginx

rm /etc/nginx/sites-enabled/default

crear la configuracion del sitio web para el punto de acceso

nano /etc/nginx/sites-available/RaspberryWifiRouter.Nginx.Siteconf

```
server {
        listen 80 default_server; # la página está disponible en http
        listen [::]:80 default_server;

        # SSL configuration
        # listen 443 ssl default_server;
        # listen [::]:443 ssl default_server;
        #
        # Self signed certs generated by the ssl-cert package
        # Don't use them in a production server!
        #
        # include snippets/snakeoil.conf;
        root /home/pi/Raspberry-Wifi-Router/www;
        # Add index.php to the list if you are using PHP
        index index.php login.php index.html index.htm index.nginx-debian.html;
        server_name RaspberryWifiRouter;
        location / {
                # First attempt to serve request as file, then
```

```
                # as directory, then fall back to displaying a 404.
                try_files $uri $uri/ =404;
        }
        # pass the PHP scripts to FastCGI server listening on 127.0.0.1:9000
        #
        location ~ \.php$ {
                include snippets/fastcgi-php.conf;
        #
        #       # With php5-cgi alone:
        #       fastcgi_pass 127.0.0.1:9000;
        #       # With php5-fpm:
                fastcgi_pass unix:/var/run/php5-fpm.sock;
                fastcgi_buffering off;
        }
        # deny access to .htaccess files, if Apache's document root
        # concurs with nginx's one
        #
        #location ~ /\.ht {
        #       deny all;
        #}
}
```

#enlazar el archive anterior en la carpeta de sitios habilitados

ln -s /etc/nginx/sites-available/RaspberryWifiRouter.Nginx.Siteconf /etc/nginx/sites-enabled/RaspberryWifiRouter.Nginx.Siteconf

#deshabilitar la salida de buffer de php

sed -i 's/output_buffering = 4096/;output_buffering = 4096/g' /etc/php5/fpm/php.ini

#establecer los permisos para el archivo de la configuración de la pagina web del Access point.

chgrp www-data /home/pi/Raspberry-Wifi-Router/www/routersettings.ini

chmod g+w /home/pi/Raspberry-Wifi-Router/www/routersettings.ini

#habilitar la carga de archivos en php

sed -i 's/;file_uploads = On/file_uploads = On/g' /etc/php5/fpm/php.ini

establecer permisos del archivo de configuración del router para que pueda ser modificado

chgrp www-data /etc/hostapd/hostapd.conf

chmod g+w /etc/hostapd/hostapd.conf

#configurar lo comandos de inicio

nano /etc/sudoers.d/wr_commands

```
www-data ALL = (root) NOPASSWD: /usr/sbin/dpkg-reconfigure -f noninteractive tzdata
www-data ALL = (root) NOPASSWD: /etc/init.d/networking restart
www-data ALL = (root) NOPASSWD: /sbin/ifconfig
www-data ALL = (root) NOPASSWD: /sbin/brctl
www-data ALL = (root) NOPASSWD: /usr/sbin/service
www-data ALL = (root) NOPASSWD: /sbin/ifdown wlan1
```

```
    www-data ALL = (root) NOPASSWD: /sbin/ifup wlan0
    www-data ALL = (root) NOPASSWD: /usr/bin/macchanger
    www-data ALL = (root) NOPASSWD: /sbin/sysctl -w net.ipv4.ip_forward=1
    www-data ALL = (root) NOPASSWD: /sbin/sysctl -w net.ipv4.ip_forward=0
    www-data ALL = (root) NOPASSWD: /sbin/iptables
    www-data ALL = (root) NOPASSWD: /sbin/iptables-save
    www-data ALL = (root) NOPASSWD: /usr/sbin/update-rc.d
    www-data ALL = (root) NOPASSWD: /bin/sed
    www-data ALL = (root) NOPASSWD: /usr/bin/tee
    www-data ALL = (root) NOPASSWD: /sbin/ip
    www-data ALL = (root) NOPASSWD: /bin/echo
    www-data ALL = (root) NOPASSWD: /usr/bin/tail
    www-data ALL = (root) NOPASSWD: /usr/bin/killall chilli
    www-data ALL = (root) NOPASSWD: /sbin/reboot
    www-data ALL = (root) NOPASSWD: /bin/cp
    www-data ALL = (root) NOPASSWD: /usr/bin/mysql
    www-data ALL = (root) NOPASSWD: /bin/mkdir
    www-data ALL = (root) NOPASSWD: /usr/bin/zip
    www-data ALL = (root) NOPASSWD: /bin/rm -fv /var/www/temp/*
    www-data ALL = (root) NOPASSWD: /bin/rm -fv /home/pi/Raspberry-Wifi-
    Router/www/temp/*
    www-data ALL = (root) NOPASSWD: /bin/rm -fv /tmp/*
    www-data ALL = (root) NOPASSWD: /bin/systemctl start ntp.service
    www-data ALL = (root) NOPASSWD: /bin/systemctl stop ntp.service
    www-data ALL = (root) NOPASSWD: /bin/systemctl enable ntp.service
    www-data ALL = (root) NOPASSWD: /bin/systemctl disable ntp.service
    www-data ALL = (root) NOPASSWD: /bin/systemctl start hostapd.service
    www-data ALL = (root) NOPASSWD: /bin/systemctl stop hostapd.service
    www-data ALL = (root) NOPASSWD: /bin/systemctl enable hostapd.service
    www-data ALL = (root) NOPASSWD: /bin/systemctl disable hostapd.service
    www-data ALL = (root) NOPASSWD: /bin/systemctl restart hostapd.service
    www-data ALL = (root) NOPASSWD: /bin/systemctl daemon-reload
    www-data ALL = (root) NOPASSWD: /bin/mount
    www-data ALL = (root) NOPASSWD: /bin/umount
    www-data ALL = (root) NOPASSWD: /sbin/resolvconf -u
    www-data ALL = (root) NOPASSWD: /usr/bin/mysqldump
    www-data ALL = (root) NOPASSWD: /usr/bin/pgrep
    www-data ALL = (root) NOPASSWD: /bin/tar
#configurar los permisos de wr_commands
chmod 644 /etc/sudoers.d/wr_commands
#Asignar los permisos de modificación al archivo de configuración ntp
chgrp www-data /etc/ntp.conf
```

```
chmod g+w /etc/ntp.conf
#configurar los permisos de timezone.conf
chgrp www-data /etc/timezone
chmod g+w /etc/timezone
#deshabilitar ntp por defecto
systemctl stop ntp
systemctl disable ntp
#asignar los permisos sobre /etc/rc.local
chgrp www-data /etc/rc.local
chmod g+w /etc/rc.local
#asignar permisos sobre la carpeta del router WiFi
chgrp -R www-data /home/pi/Raspberry-Wifi-Router/www/temp
chmod -R 775 /home/pi/Raspberry-Wifi-Router/www/temp
#levantar y configurar mysql
apt-get -y install debhelper
echo 'mysql-server mysql-server/root_password password raspberry' | debconf-set-selections
echo 'mysql-server mysql-server/root_password_again password raspberry' | debconf-set-selections
apt-get -y install mysql-server php5-mysql
#crear la base de datos para el logueo
echo 'create database login;' | mysql --host=localhost --user=root --password=raspberry
echo " \
    CREATE TABLE users ( \
    id int(11) NOT NULL auto_increment, \
    username varchar(64) NOT NULL default '', \
    password varchar(64) NOT NULL default '', \
    PRIMARY KEY  (id) \
  ) ;" | mysql --host=localhost --user=root --password=raspberry --database login
#crear dos usuarios usuarios
echo "INSERT INTO users (username,password) VALUES('admin','raspberry');" | mysql --host=localhost --user=root --password=raspberry --database login
echo "INSERT INTO users (username,password) VALUES('wduran','proyecto');" | mysql --host=localhost --user=root --password=raspberry --database login
```

3.1.5. Desarrollo Practico experimental

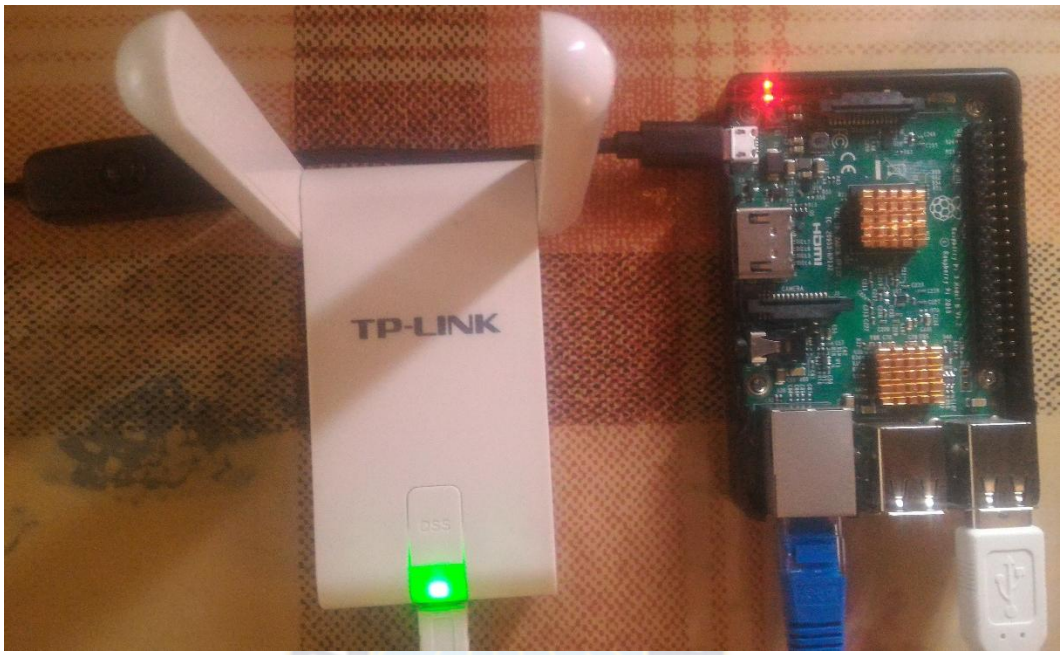

Figura 58 Raspberry Pi v3 y adaptador usb WiFi
Fuente: Fotografía

3.1.5.1. Evidencias de la Red Inalámbrica

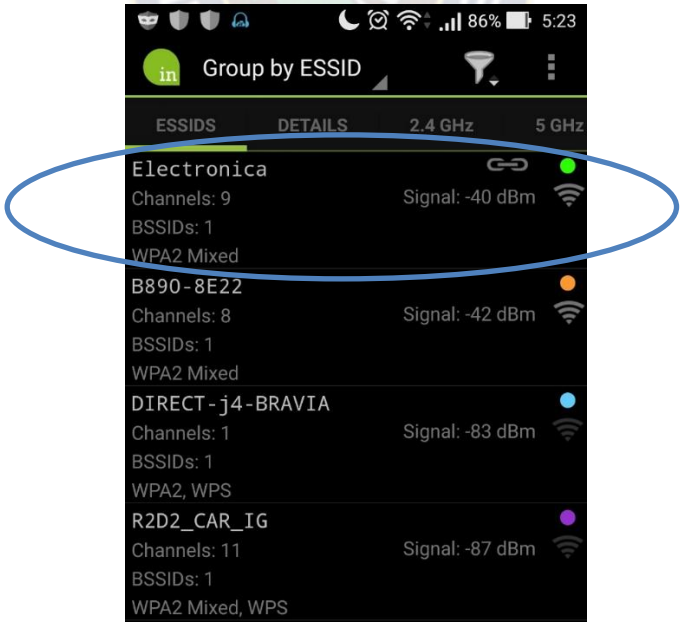

Figura 59 La red inalámbrica se encuentra activa
Fuente: Captura de pantalla

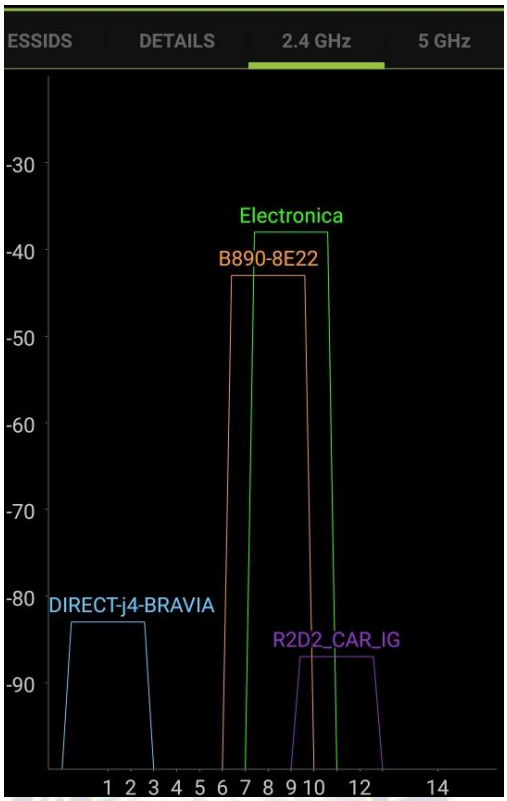

Figura 60 Análisis de canales
Fuente: Captura de pantalla

Figura 61 Logueo en la red inalámbrica
Fuente: Captura de pantalla

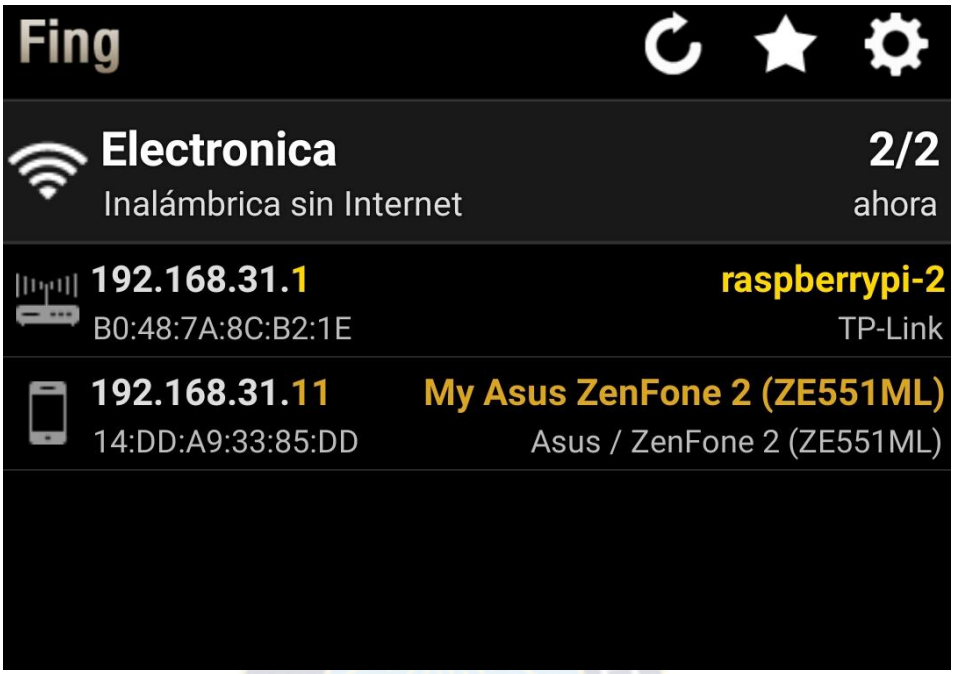

Figura 62 Escaneo de los dispositivos dentro la red inalámbrica
Fuente: Captura de Pantalla

3.1.5.2. Firewall y Proxy

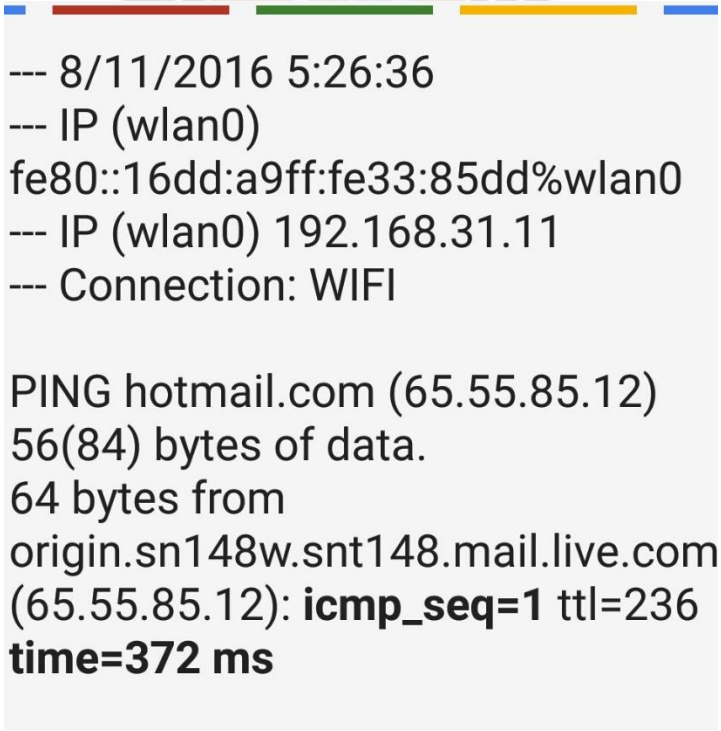

Figura 63 Protocolo ICMP permitido
Fuente: Captura de pantalla

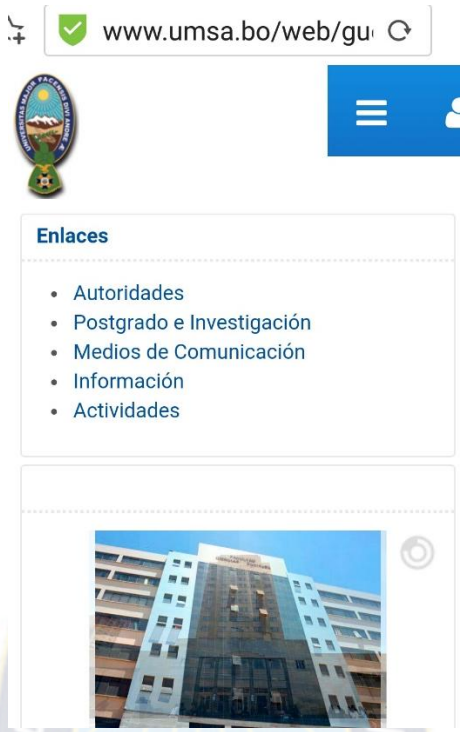

Figura 64 Se navega a páginas de protocolo https
Fuente: Captura de pantalla

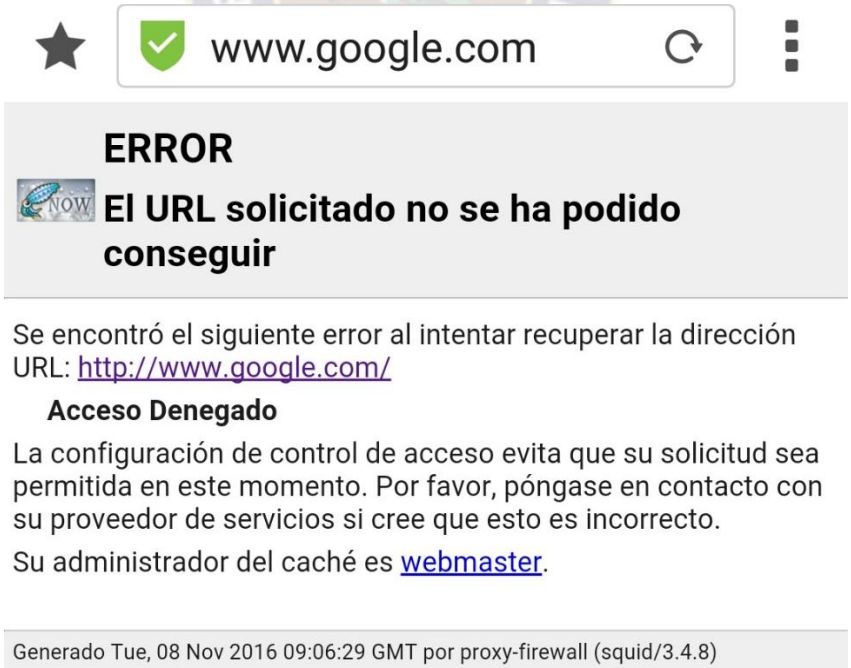

Figura 65 Acceso denegado a google.com
Fuente: Captura de pantalla

3.1.5.3. Administración WEB

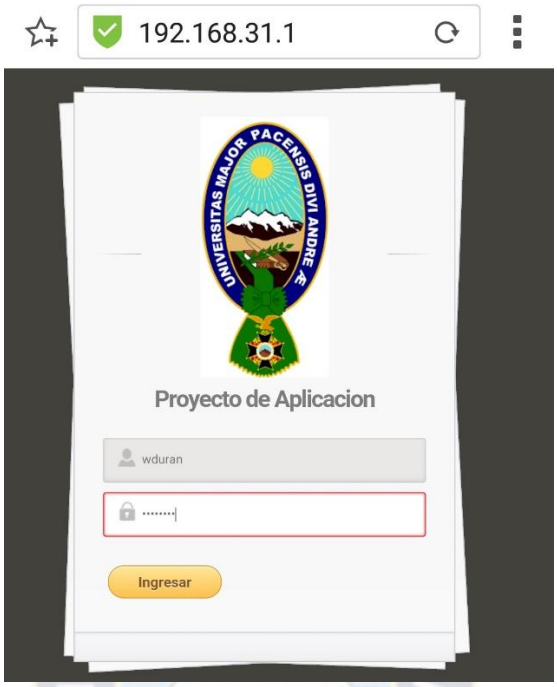

Figura 66 Acceso a la página de administración
Fuente: Captura de pantalla

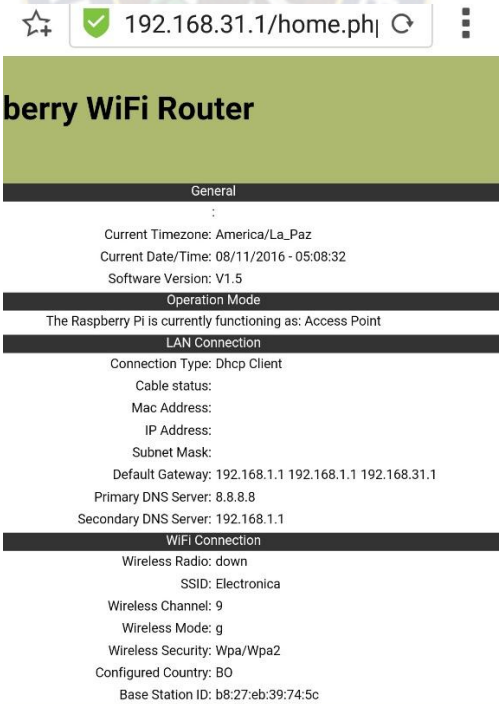

Figura 67 Parámetros de la red inalámbrica
Fuente: Captura de pantalla

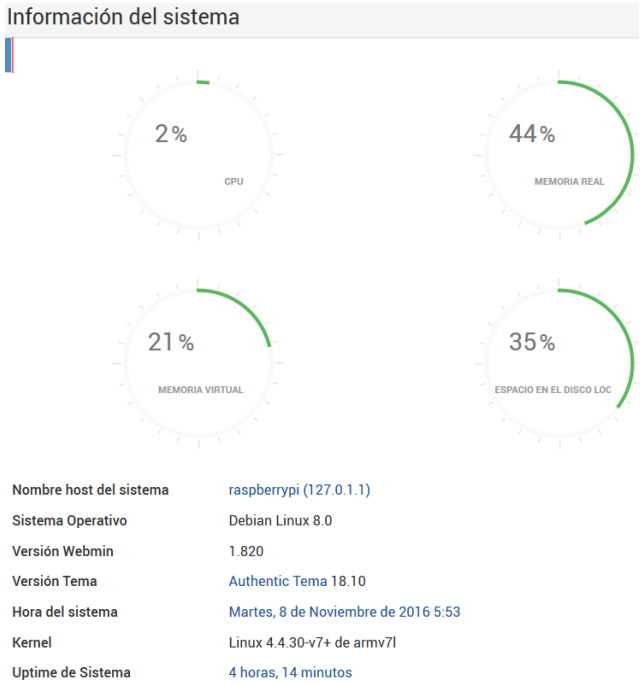

Figura 68 Información del sistema
Fuente: Captura de pantalla

3.1.5.4. Informe de uso de ancho de Banda

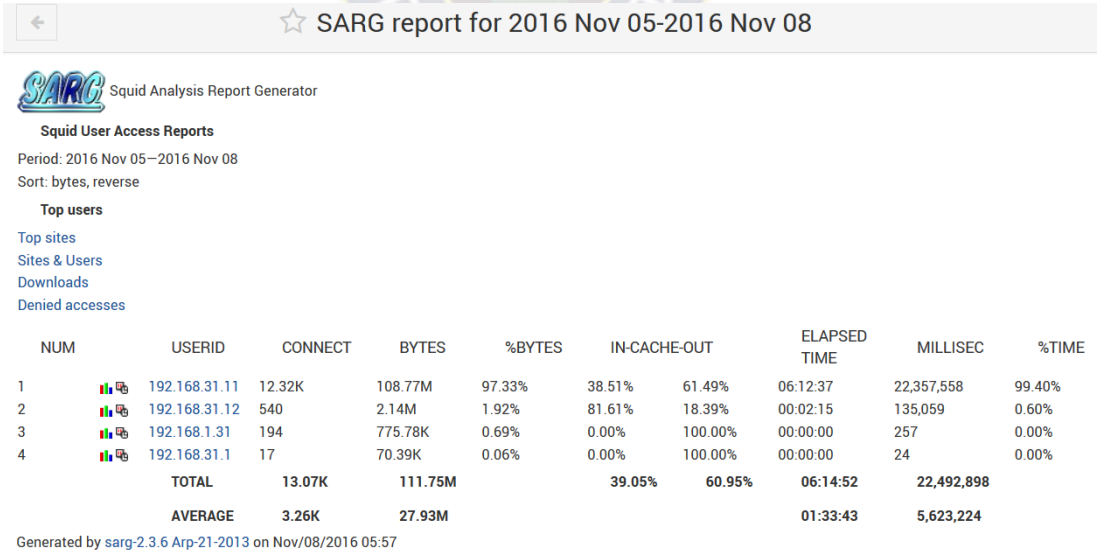

Figura 69 Uso de ancho de banda
Fuente: Captura de pantalla

3.1.5.5. Detector de intrusiones

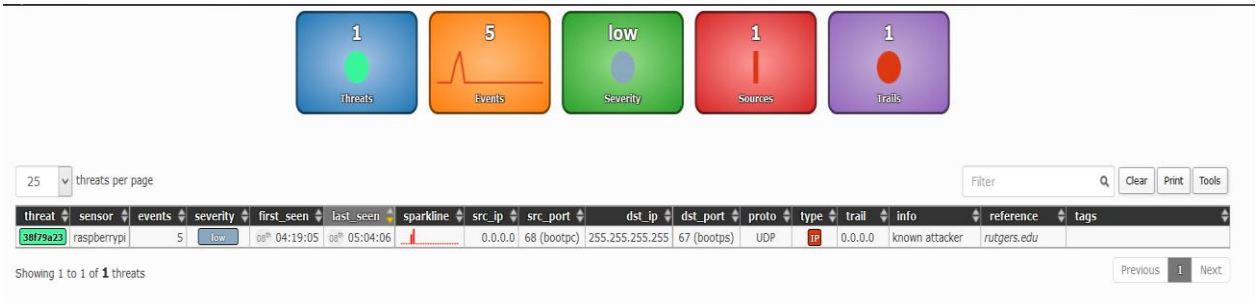

Figura 70 Detección de malware (código malicioso)
Fuente: Captura de pantalla

4. Costos

A continuación se detalla un presupuesto aproximado para la completa implantación de la solución propuesta.

Equipos

El proyecto no requiere una gran cantidad de hardware

Adaptador USB a WiFi: modelo TL-WN822N, posee una ganancia de 3dbi, compatible con la norma 802.11n

En bolivianos

Costo = 140 Bs

Raspberry Pi v3 B se encargara de realizar todos los procesos tanto de control, direccionamiento, monitoreo y bloqueo para todos los usuarios de la red inalámbrica.

Costo= 450 Bs

Bateria y su cable para el miniordenador que suministrara energía al Raspberry Pi.

Costo=100 Bs

Gastos Generales

Costo=110 Bs

Total de Aproximación

COSTO TOTAL= 800 Bolivianos

5. Conclusiones

De este estudio se destacaría lo siguiente:

- La característica más destacada de WiFi trabajando como punto de acceso a redes de área local es la ausencia de cableado, lo que permite movilidad dentro de la zona de cobertura.

- Las frecuencias en las que trabajamos son sin licencia, lo que supone ahorro económico.

- El inconveniente de usar bandas sin licencia es que tenemos una limitación en la potencia de emisión para no interferir con otros sistemas que estén usando la misma parte del espectro.

- Los estándares WiFi están evolucionando mucho, de hecho las expectativas del nuevo estándar 802.11n son muy altas, 300 Mbps teóricos y 70 metros de alcance indoor.

- El uso de los miniordenadores como servidores de baja carga, accesibles al público en general para el desarrollo e implementación de proyectos.

- Finalmente, el uso de las tecnologías inalámbricas está regulado y hay establecidas normas que definen las pautas de seguridad radioeléctrica que deben de cumplir los fabricantes.

6. Bibliografía

Debido a que se está utilizando tecnología inalámbrica existen pocos libros que hablen acerca del tema así que la información fue extraída de diferentes páginas web aquí mencionadas

- https://cdn-learn.adafruit.com/downloads/pdf/setting-up-a-raspberry-pi-as-a-wifi-access-point.pdf
- http://www.google.com.bo/url?sa=t&rct=j&q=justificacion%20de%20proyecto%20wifi&source=web&cd=5&ved=0CD4QFjAE&url=http%3A%2F%2Ftelemetria.wikispaces.com%2Ffile%2Fview%2FPRESENTACIONLYX.pdf&ei=UueWT6y0H87lggfi-KDtDQ&usg=AFQjCNHjWrfHjAO2mp0XAw7HTtg762xxhw
- http://www.google.com.bo/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=7&sqi=2&ved=0CHAQFjAG&url=http%3A%2F%2Fwww.ansel.com.mx%2Fsoporte%2Fwireless_networking%2F2412%2Fguia-bridge.ppt&ei=cKvzT9HoKsry0gGQwInyBg&usg=AFQjCNEAet-twyJ7cNndOJChUDNGUCMjvA&sig2=erCbs4q86PD5lk9C2rwv3w
- http://www.google.com.bo/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=18&ved=0CGIQFjAHOAo&url=http%3A%2F%2Fwww.ansel.com.mx%2Fsoporte%2Fwireless_networking%2F2412%2F2412-54.ppt&ei=pqzzT5O4D4uy0QH5_5z1Bg&usg=AFQjCNEjqy7nMp-tA0wd-ugY5RBgNKgbXA&sig2=_KixFFKPaevKTcyC7Uagxw
- http://es.wikipedia.org/wiki/Red_de_área_local_inalámbrica.html.
- http://dns.bdat.net/seguridad_en_redes_inalambricas/x187.html
- www_34t_com .html.
- http://www.ceditec.etsit.upm.es/dmdocuments/wifi.pdf
- http://www.x-net.es/tecnologia/wireless.pdf
- http://en.wikipedia.org
- http://www.telecomhall.com
- http://modelotcp18.blogspot.com/
- http://www.adrformacion.com
- http://gaboalex.blogspot.com
- http://gaboalex.blogspot.com
- http://www1.frm.utn.edu.ar
- https://www.emaze.com
- http://topologializ.blogspot.com/
- https://leidiyana.wordpress.com
- http://www.conceptdraw.com
- http://redestelematicas.com
- https://technet.microsoft.com

- http://www.l-com.com/
- http://www.peruhardware.net
- http://www.wi-fi.org/
- http://slideplayer.com/
- http://www.pcworld.co.uk/
- http://www.chw.net
- http://www.pcexpansion.es
- http://www.informatica-hoy.com.ar
- http://rpc.yoreparo.com
- https://alteageek.com
- https://www.stewright.me
- http://www.peruhardware.net
- http://articulo.mercadolibre.com.ar
- http://tinkersphere.com
- http://www.pianywhere.com/
- http://www.tp-link.com
- https://www.amazon.es
- http://ocw.cs.pub.ro
- https://wikidevi.com/files/Atheros/specsheets/AR7010+AR9287.pdf
- https://www.raspberrypi.org
- https://www.faix.cz/2015/03/squid-transparent-proxy/

ALGUNOS LIBROS

- INTERNET Y REDES INALAMBRICAS ARIAS ARAGUEZ 510
- REDES INALAMBRICAS
  EN PAISES E DESARROLLO
- REDES DE COMUNICACIONES
- ENCICLOPEDIA DE LA SEGURIDAD INFORMATICA