UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERIA EN SISTEMAS ELECTRONICA E INDUSTRIAL / DIRECCIÓN DE POSGRADO

MAESTRÍA EN INFORMÁTICA

Resolución del Problema Profesional

Tema: DISEÑO DE UNA RED WIFI PARA BRINDAR SERVICIOS DE INTERNET INALÁMBRICO A LA FACULTAD DE INGENIERIA EN CIENCIA APLICADAS

Resolución del Problema Profesional, previo a la obtención del Grado Académico de Magister en Informática a través del Examen Complexivo

Autor: EDGAR DANIEL JARAMILLO VINUEZA

Ambato - Ecuador

2016

La Unidad de Titulación/ Unidad Académica de Titulación de la Facultad de Ingeniería en Sistemas Electrónica e Industrial

El Tribunal receptor de la Resolución del Problema Profesional integrado por el Presidente y Miembros del Tribunal, designados por la Unidad Académica de Titulación de la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato, para receptar la Resolución del Problema Profesional con el tema: "DISEÑO DE UNA RED WIFI PARA BRINDAR SERVICIOS DE INTERNET INALÁMBRICO A LA FACULTAD DE INGENIERIA EN CIENCIA APLICADAS ", elaborado y presentado por el (la) señor (ita) Ing. Edgar Daniel Jaramillo Vinueza, para optar por el Grado Académico de Magister en Informática a través del Examen Complexivo; una vez escuchada la defensa oral el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. ……..,Mg.

Presidente y Miembro del Tribunal

Miembro del Tribunal

c.c…….

Miembro del Tribunal

c.c……..

AUTORÍA DE LA RESOLUCIÓN DEL PROBLEMA PROFESIONAL

La responsabilidad de las opiniones, comentarios y críticas emitidas en la Resolución del Problema Profesional presentado con el tema: DISEÑO DE UNA RED WIFI PARA BRINDAR SERVICIOS DE INTERNET INALÁMBRICO A LA FACULTAD DE INGENIERIA EN CIENCIA APLICADAS, me corresponde exclusivamente a ingeniero Edgar Daniel Jaramillo Vinueza.

Ing. Edgar Daniel Jaramillo Vinueza
c.c. 1001545142

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que la Resolución del Problema Profesional, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.

Ing. Edgar Daniel Jaramillo Vinueza
c.c. 1001545142

INDICE

Contenido

1. TEMA

DISEÑO DE UNA RED WIFI PARA BRINDAR SERVICIOS DE INTERNET INALÁMBRICO A LA FACULTAD DE INGENIERIA EN CIENCIA APLICADAS.

2. CONTEXTUALIZACION

Las soluciones inalámbricas presentes en la actualidad, son un producto de la sociedad occidental industrial, que fueron desarrolladas para la comunicación móvil en la sociedad urbana.

El concepto de redes inalámbricas se asocia a redes surgidas en el ámbito de transmisión de datos, en las que tradicionalmente se utilizaban redes basadas en cables eléctricos o en fibra óptica.

En los últimos años con gran éxito se han desarrollado diversos estándares de redes inalámbricas, en áreas en las que anteriormente solo existían algunos sistemas propietarios con baja implantación.

Las redes inalámbricas, están diseñadas para operar en bandas de frecuencia para las que no se necesita licencia de uso, son de carácter libre. Como es el caso de la banda de 2.4 GHz y de 5GHz. Esto ha favorecido la implantación de la tecnología inalámbrica, ya que da lugar a unos costos de uso mucho menores que las redes basadas en sistemas celulares. A pesar de esto, no se está exento de problemas ya que estas bandas de frecuencias son utilizadas por distintas tecnologías (WiFi, Bluetooth, etc) pudiendo aparecer problemas de interferencias. [5]

Además, permiten crear redes en áreas complicadas donde se pueden conectar gran cantidad de dispositivos, en lugares donde resulta dificultoso o muy cara la conexión de cables.

Gracias a la aparición y al éxito de los protocolos de comunicación inalámbrica se ha producido una gran difusión en la utilización de dichas redes, debido fundamentalmente a la interoperabilidad del equipamiento producido por distintos fabricantes. Esto ha promovido que se desarrollen productos de manera veloz, haciendo que los precios se hayan visto disminuidos gracias al volumen de producción.

Las redes inalámbricas de área local o WLAN (Wireless Local Area Network) cubren distancias de unos cientos de metros. Estas redes están pensadas para crear un entorno de red local entre ordenadores o terminales situados en un mismo edificio o grupo de edificios. En el mercado existen distintas tecnologías que dan respuesta a esta necesidad, aunque la más frecuente es la tecnología WiFi, existen otras como HomeRF, HiperLAN, OpenAir.

Las redes inalámbricas pueden clasificarse de distintas formas dependiendo del criterio al que se atienda. En este caso, vamos a clasificar los sistemas de comunicaciones inalámbricas de acuerdo con su alcance, definido como la distancia máxima a la que pueden situarse las dos partes de la comunicación inalámbrica. Las redes inalámbricas de área personal o WPAN (Wireless Personal Area Network) son aquellas que tienen un área de cobertura de unos pocos metros. La finalidad de estas redes es la comunicación entre cualquier dispositivo personal (por ejemplo, el ordenador con la impresora) con sus periféricos, así como permitir una comunicación directa a corta distancia entre estos dispositivos. Algunas tecnologías que se utilizan en este tipo de redes son Bluetooth, DECT y los infrarrojos. [5]

Las redes inalámbricas de área metropolitana o WMAN (Wireless Metropolitan Area Network) pretenden cubrir el área de una ciudad o entorno metropolitano. Tienen una cobertura desde cientos de metros hasta varios Kilómetros. Los protocolos WiMax (Worldwide Interoperability for Microwave Access) o LMDS (Local Multipoint Distribution Service) ofrecen soluciones de este tipo [5].

Las redes inalámbricas de área global o WWAN (Wireless Wide Area Network) son los sistemas basados en la tecnología celular y tienen la posibilidad de cubrir un país entero o un grupo de países. Se trata de un sistema para mantener la comunicación independientemente del lugar donde nos encontremos. Las

tecnologías WWAN se conocen también como sistemas de segunda generación (2G), de tercera generación (3G) o los actuales sistemas (4G) definidos como un estándar de la norma 3GPP.

Como hemos visto, existen tecnologías distintas de comunicaciones inalámbricas. Muchas de ellas son complementarias, otras dan respuesta a una misma necesidad y por ello compiten entre ellas por ser las preferidas en el mercado.

A continuación, se muestra una tabla comparativa de las principales tecnologías de las comunicaciones inalámbricas.

Tipo de red	WWAN (Wireless Wide Area Network)	WMAN (Wireless Metropolitan Area Network)	WLAN (Wireless Local Area Network)	WPAN (Wireless Personal Area Network)
Estándar	GSM/GPRS/UMTS	IEEE 802.16	IEEE 802.11	IEEE 802.15
Denominación/ Certificación	2G/3G	WiMAX	WiFi	Bluetooth, ZigBee
Velocidad	9.6/170/2000 Kb/s	15 - 134 Mb/s	1-2-11-54-300-600 Mb/s - 1Gb/s	721 Kb/s
Frecuencia	0,9/1,8/2,1 GHz	2-66 GHz	2,4 y 5 GHz, Infrarrojos	2,4 GHz
Rango	Limitado por células (máx. 35 Km por célula)	1.6 - 50 Km	30 - 150 m	10 m
Técnica radio	Varias	Varias	FHSS, DSSS, OFDM	FHSS
Itinerancia (roaming)	Sí	Sí, (802.16e)	Sí	No
Equivalente a:	Conex. telef. (módem)	ADSL, CATV	LAN	Cables de conexión

Tabla 1. Comparativa de tecnologías inalámbricas

Tecnología inalámbrica WIFI

Como se ha comentó, una de las tecnologías más utilizadas en la actualidad para la creación de redes inalámbricas de área local es WiFi.

Al inicio era habitual que las redes inalámbricas se llevasen a cabo utilizando soluciones particulares de cada fabricante, ya que los diferentes dispositivos que

existían en el mercado eran incompatibles entre sí. Esto suponía estar sometido siempre a las limitadas soluciones que un solo fabricante puede ofrecer. Para normalizar la situación, se desarrolló un sistema que fuese aceptado por todos los fabricantes como sistema común. [5]

De esta forma, se creó la asociación WECA (Wireless Ethernet Compatibility Alliance), actualmente conocida como WiFi Alliance, cuyo objetivo fue designar una marca que permitiese fomentar la tecnología inalámbrica y asegurar la compatibilidad de equipos. Además, WECA certifica la interoperabilidad de equipos según la norma IEEE 802.11. Esto quiere decir que el usuario tiene la garantía de que todos los equipos que tengan el sello WiFi pueden trabajar juntos sin problemas, independientemente del fabricante de cada uno de ellos.[5]

OFTELSAT diseña, desarrolla y adapta, los sistemas de hardware (hard ware hardening) de radios, equipos de comunicación y de computación, para su uso en ambientes, menos favorables y más exigentes, que trabajan en el Ecuador, conjuntamente con el IICD (Instituto Internacional de Conectividad y Desarrollos) y MCCH (Maquita Cushunchic), los cuales están dedicados a encontrar soluciones de conectividad para el desarrollo social y económico en ambientes rurales [2].

3. ANALISIS CRITICO

Para la elección del tema se tomó en cuenta las siguientes razones:

Sociales:

- Las tecnologías inalámbricas en particular, permiten un rápido desarrollo y despliegue de infraestructuras de comunicaciones, reduciendo el costo de la inversión.

Teóricas:

- Las TIC tienen un gran potencial para reducir la brecha de acceso a los servicios de salud (telemedicina), educación y comunicaciones.

- Las redes inalámbricas basadas en la tecnología Wi-Fi pueden ser diseñadas, instaladas y mantenidas por las propias comunidades interesadas en usarlas, pues no necesitan de grandes inversiones ni de personal técnico altamente especializado [5].

Personales:

- Utilización intensiva de servicios IP para reducción de costos. Voz sobre IP como alternativa ideal para la conectividad telefónica.
- Acceso a portales de transacciones y procedimientos de entidades del estado. Aprovechamiento de sinergias con otros proyectos del estado.
- Se desea aportar con el tema planteado, en el entrenamiento de las personas que estén motivadas para suministrarles los conocimientos necesarios, para que puedan realizar una instalación de una red inalámbrica exitosa, a través del empleo de métodos que permitan a Wi-Fi incrementar las áreas de cobertura.

La FICA tiene una red inalámbrica WiFi la cual brinda una mala experiencia de navegación para los usuarios ya sea para el uso correo electrónico, investigaciones académicas, videos en línea, descarga de archivos y cualquier otro uso que se le pueda dar a Internet.

En base a una evaluación técnica de la red WiFi de la FICA, se pudo determinar que la baja calidad de esta red tiene dos principales causas, las cuáles son cobertura y desempeño. Hay muchas locaciones de la Facultad que no tienen cobertura suficiente para establecer una conexión entre los dispositivos electrónicos de los usuarios (laptops, tabletas o smartphones) con los puntos de acceso instalados alrededor del campus, lo cual ocasiona que los usuarios se tengan que trasladar a zonas donde si hay buena cobertura WiFi para establecer una conexión congestionando la red en esa locación haciendo que el desempeño de esta sea deficiente.

Un ejemplo de esto son los pisos 1 y planta baja, los cuales tienen los niveles óptimos para establecer una conexión WiFi entre los usuarios y los puntos de acceso, los usuarios se dirigen a estas locaciones para hacer uso de la red lo cual

hace que se congestione causando que el usuario que a pesar de que tenga una conexión estable no cuente con los recursos para tener una buena experiencia de navegación.

La demanda de datos al igual que las exigencias de los usuarios tiende a un alto crecimiento, lo que está causando que la red sea cada vez menos eficiente. Si no hacen expansiones y mejoras de la red, aplicación de nuevas tecnologías y optimización de los puntos de acceso WiFi, esta red se convertirá en una red obsoleta con poca capacidad y mucha deficiencia en poco tiempo. De no ser tomadas medidas de optimización, luego se tendrá que hacer una completa sustitución de la red, lo cual será mucho más costoso para la Universidad y será mucho más engorroso.

Por las razones anteriormente mencionadas se avizora la necesidad y la importancia de realizar la investigación propuesta, ya que con las redes inalámbricas en la facultad se puede crear centros de comunicación que van a dar aporte y contenido de forma interactivo, y dar conectividad de datos a estudiantes, profesores, y personal administrativo.

La red inalámbrica debe quedar integrada en la LAN de datos actual de UTN aprovechando la infraestructura existente en la medida de lo posible.

Se desea cobertura en el 100% de la totalidad del centro, con un umbral de señal suficiente como para establecer comunicaciones a una velocidad aceptable.

Los puntos de acceso serán resultado del análisis previsto y estarán convenientemente distribuidos a lo largo del edificio para dotar de cobertura radioeléctrica de calidad a los usuarios independientemente de cuál sea su posición dentro del edificio. Se realizarán una serie de actuaciones previas orientadas a la obtención del lugar óptimo donde situar los APs y el número de ellos.

Se considera que la investigación del tema es factible porque se cuenta con los conocimientos, recursos técnicos, materiales, metodología, y las herramientas de software para la evaluación de la red.

4. OBJETIVOS

4.1 Objetivo General

Diseñar una red WiFi que permita dar un servicio de acceso a internet confiable y oportuno a estudiantes y profesores de la Facultad de Ingeniería en Ciencias Aplicadas de la UTN.

4.2 Objetivos Específicos

1. Analizar las diferentes tecnologías inalámbricas para interconectar los diferentes pisos del edificio de la FICA con la finalidad de permitir un despliegue adecuado de la Red, de manera de ofrecer un servicio apropiado en toda la zona de cobertura WiFi.
2. Realizar el levantamiento de la información necesaria para establecer las características con las que debe contar la red WiFi en la FICA.
3. Dimensionar la red inalámbrica con tecnología WiFi, en base a los planos arquitectónicos, con la finalidad de cubrir el 100% de las áreas, optimizando la cantidad de puntos de acceso de tal manera de cubrir la totalidad del edificio.
4. Estudiar la factibilidad técnica y económica de implementar la red inalámbrica diseñada.

5. MARCO TEORICO

Estándares IEEE 802.11 [5]

La familia de estándares de redes WLAN IEEE 802.11 ha sido la causa de la incorporación y el desarrollo rápido de las redes WLAN en el mercado. Dentro del grupo de trabajo IEEE 802.11 se pueden encontrar diferentes estándares:

- IEEE 802.11b

Publicado en 1999, ganó una amplia aceptación en la industria. Tiene una velocidad máxima de transmisión de 11 Mbps y utiliza el método de acceso definido en el estándar original CSMA/CA. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, la velocidad real de transmisión se reduce a 5.9 Mbps sobre TCP y 7.1 Mbps sobre UDP.

El estándar 802.11b funciona en la banda de frecuencia de 2.4 GHz, la cual, al no necesitar licencia de uso, puede ser utilizada por cualquier tecnología inalámbrica y producir interferencias.

- IEEE 802.11a

Estandarizado por el IEEE en julio de 1999 aunque no llega a comercializarse hasta 2002. Se consiguen velocidades de 54 Mbps e incluso es posible alcanzar los 72 y 108 Mbps con versiones propietarias de esta tecnología. Esto hace que sea un estándar con velocidades reales de hasta 20 Mbps.

Trabaja en la banda de 5GHz, y utiliza la técnica OFDM (Orthogonal Frequency-Division Multiplexing) con 52 subportadoras. El estándar 802.11 tiene doce canales sin solapa, 8 para red inalámbrica y 4 para conexiones punto a punto.

El hecho de que no pudiera interoperar con equipos del estándar 802.11b, salvo si se dispone de equipos que implementen ambos estándares y la limitación del radio de alcance debido a un mayor índice de absorción de sus ondas, supuso una desventaja que limitó su aceptación en la industria.

- IEEE 802.11g

En junio de 2003 aparece el estándar 802.11g con la idea de aumentar la velocidad sin renunciar a las ventajas de la banda de los 2.4 GHz. Esta norma, permite transmitir datos a 54 Mbps que en promedio es de 22 Mbps de velocidad real de transferencia.

Es compatible con el protocolo 802.11b y puede trabajar con el protocolo 802.11a cambiando la configuración de los equipos. Esto es debido a que 802.11g, puede operar con las tecnologías OFDM y DSSS.

Pese a la compatibilidad, en redes bajo el estándar b, la presencia de nodos g reduce notablemente la velocidad de transmisión, debido a que los clientes 802.11b no comprenden los mecanismos de envío de OFDM.

- IEEE 802.11n

El estándar 802.11n fue ratificado en septiembre de 2009 por la organización IEEE. La base de su funcionamiento es la incorporación de varias antenas, que permiten utilizar varios canales para enviar y recibir datos simultáneamente, mejorando de forma sustancial la señal recibida por el receptor y multiplicándose de esta forma el ancho de banda utilizado. Esto es lo que se conoce como la tecnología MIMO (Multiple Input Multiple Output).

El 802.11n incluye grandes mejoras en el uso del entorno radio con el fin de mejorar el caudal neto de la WLAN. Algunos de los cambios más relevantes son:

Incremento del canal de transmisión: A diferencia de los estándares 802.11a/b/g que utilizan un canal con un ancho de banda de 20 MHz, el 802.11n usa canales con un ancho de banda de 20 MHz y 40 MHz. Un canal de 40 MHz está formado por una combinación de dos canales de 20 MHz adyacentes. La unión de canales aumenta la velocidad de transmisión de datos debido a que la velocidad de transmisión de datos es directamente proporcional al ancho de banda. La idea de este solapamiento es aprovechar el ancho de banda de las cabeceras de inicio del canal y las cabeceras de la cola del canal para enviar datos. Al unir dos canales adyacentes la cola del primer canal que se usa para reducir la interferencia entre canales adyacentes y la cabecera del segundo canal ya no tienen ninguna utilidad y el ancho de banda que ocupan pasa a ser usado para la transmisión de datos.

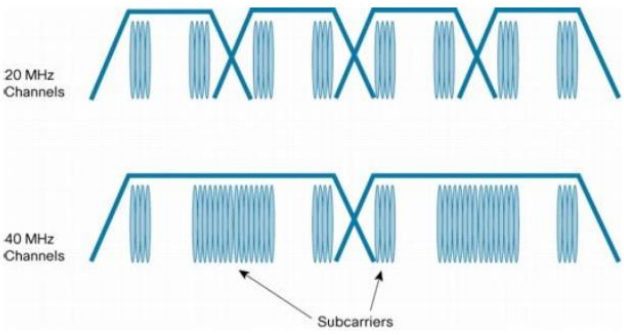


Figura 1. Canales de 20 MHz y 40 MHz de ancho de banda

Fuente: Yaagoubi, M. Universidad Carlos III

- Alta tasa de modulación: El estándar 802.11n usa la modulación OFDM (Ortogonal Frequency Division Multiplexing) que divide un canal de transmisión en varios subcanales, teniendo cada subcanal su propia subportadora que transporta información independientemente de las otras portadoras. El aumento de ancho de banda de los canales de 802.11n a 40 MHz proporciona más portadoras, traduciéndose en un aumento de la velocidad de transmisión de hasta 600 Mbps.

- Reducción de cabeceras (Intervalo de guarda): El intervalo de guarda se utiliza para asegurarse de que no interfieren las diferentes transmisiones entre ellas. El 802.11a/g utilizan un intervalo de guarda de 0.8 microsegundos al igual que el estándar 802.11n en su modo por defecto, pero para aumentar la velocidad de los datos, dicha norma añadió un soporte opcional para un intervalo de guarda de 0.4 microsegundos que proporciona un aumento de 11% en la velocidad de transferencia de datos.

Además, la versión 802.11n introduce cambios en la trama MAC. Se añade lo que se llama Frame Aggregation que consiste en el envío de dos o más fragmentos en una sola transmisión.

A diferencia de las otras versiones de WiFi, 802.11n puede trabajar tanto en la banda de frecuencia de 2.4 GHz como en la de 5 GHz, lo que hace que sea compatible con las tres tecnologías anteriores (a, b y g).

Es muy útil que pueda trabajar en la banda de frecuencias de 5GHz, ya que esta menos congestionada y permite un mejor rendimiento de dicho estándar.

- IEEE 802.11ac

Es una mejora de la norma 802.11n que se ha desarrollado entre 2012 y 2013. La industria ya trabaja en nuevos protocolos y dispositivos basados en el protocolo 802.11ac. El sistema permite unas tasas de transferencia de 1Gbps en la banda de 5GHz, un ancho de banda hasta 160 MHz, hasta ocho flujos MIMO y modulación de alta densidad.

Otra de las ventajas con respecto a las versiones anteriores, es el alcance de cobertura, que llega hasta un máximo de 90-100 metros mediante el uso de tres antenas internas.

Es necesario aclarar la diferencia entre velocidad de transmisión en el aire y velocidad real (comúnmente conocida como throughput). Cuando se habla de velocidad de transmisión en el aire se incluye la información de usuario, así como toda aquella información adicional para asegurar el intercambio fiable de información (protocolos, verificación errores, etc.), mientras que cuando hablamos de velocidad real es la velocidad en cuanto a transferencia de datos que observa el usuario. Una manera de medir este último es monitorizando la velocidad de transmisión en el puerto Ethernet de los equipos mientras se está usando alguna aplicación que consuma todo el ancho de banda (como puede ser una transferencia de archivos mediante FTP). Es importante realizar todo el diseño, en cuanto a ancho de banda se refiere, basándose siempre en la velocidad real.

Otro parámetro a tener en cuenta a la hora de diseñar una red WiFi es el alcance de su cobertura inalámbrica. Algunos de los motivos por los que puede variar el alcance de la señal son los siguientes:

- Las obstrucciones en el trayecto que recorre la señal como pueden ser árboles, edificios, paredes, accidentes geográficos, etc.
- Tipo de material con que está construida la locación donde se desea recibir la señal WiFi
- Potencia de emisión de la estación base o Punto de Acceso
- Posición y ubicación de la antena receptora
- Ganancia de la antena receptora
- Interferencias que puedan provenir de otros sistemas radioeléctricos
- Longitud del cable que une la antena receptora con la placa WiFi

Bandas de frecuencias de las redes WIFI

Se ha hablado de que las redes WiFi funcionan en dos bandas de frecuencias:

- Banda de 2.4 GHz

- Banda de 5GHz

Ninguna de las dos bandas requiere licencia para su utilización, pero se encuentran sujetas a la regulación fijada por la Secretaria de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI) en el Cuadro Nacional de Frecuencias (CNAF). Ambas bandas están designadas para aplicaciones ISM (Industry, Science and Medical) ó ICM (Industrial, Científica y Médica).

Elementos básicos de una red

A la hora de diseñar una red es importante conocer los elementos básicos que la componen, es cierto, que no existe un diseño de red modelo, si no que cada red está formada por un equipamiento y una topología diferente. Sin embargo, en las redes inalámbricas existen una serie de elementos básicos que son indispensables.

El punto de acceso (Access Point, 'AP') Es el centro de las comunicaciones de la mayoría de las redes inalámbricas. Por medio de ondas de radio frecuencia (RF) recibe información de diferentes dispositivos y la transmite a través del cable al servidor de la red cableada o viceversa. El punto de acceso no sólo es el medio de intercomunicación de todos los terminales inalámbricos, sino que también es el puente de interconexión con la red fija e Internet. Desde este punto de vista, es importante tener en cuenta aspectos como:

- Comprobar las características del router del punto de acceso. DHCP, NAT
- propiedades firewall son facilidades que ayudan en la configuración y manejo de las comunicaciones con Internet o con otras redes.
- Conviene comprobar que el AP que se va a comprar sea compatible con el protocolo de red cableada con el que se va a conectar.
- Los puntos de acceso WiFi funcionan sin problema con los adaptadores de red de cualquier fabricante. No obstante, existe cierta incompatibilidad cuando se desea crear una red con varios puntos de acceso de distintos fabricantes. El estándar 802.11 es bastante ambiguo y no define con claridad todas las funciones que debería realizar un Punto de Acceso. Esto dio lugar

a que cada fabricante los diseñara según su criterio y, por lo tanto, existen en el mercado decenas de Puntos de Acceso con características y funcionalidades muy dispares.

La falta de entendimiento aparece a la hora de mantener en servicio una comunicación cuando un usuario pasa del área de cobertura de un punto de acceso a otro (a esto se le llama itinerancia o roaming). Es recomendable que los puntos de acceso vecinos sean del mismo fabricante para evitar cortes de comunicación al pasar de un AP a otro.

En cualquier caso, un Punto de Acceso está compuesto por un equipo radio, antenas exteriores o interiores, un software de gestión de comunicaciones y puertos para conectar el punto de acceso a Internet o a la red cableada.

Los adaptadores inalámbricos de red son fundamentalmente unas estaciones de radio que se encargan de comunicarse con otros adaptadores (modo ad hoc) o con un punto de acceso (modo infraestructura) para mantener a los dispositivos que están conectados dentro de la red inalámbrica a la que se asocie.

Estos equipos pueden recibir el nombre de tarjetas de red, interfaces de red o NIC (Network Interface Cards) y cumplen con el estándar 802.11 que permite a un equipo conectarse a una red inalámbrica. Hay diversos tipos de adaptadores en función del tipo de cableado o arquitectura que se utilice en la red.

En la actualidad, la mayoría de los dispositivos y ordenadores tienen integrado el adaptador de red inalámbrico. Es importante que el adaptador WiFi sea compatible con el router. La elección de un adaptador u otro dependerá de nuestras necesidades y de las características de nuestro equipo.

También existen amplificadores y antenas que se pueden agregar, según las necesidades, a instalaciones WiFi y sirven para direccionar y mejorar las señales de RF (Radio Frecuencia) transmitidas.

Configuraciones de red [5]

Las redes inalámbricas WiFi admiten dos tipos de configuraciones desde el punto de vista del tipo de equipamiento:

- **Modo Ad hoc**. Se trata de una configuración en la cual sólo se necesita disponer de tarjetas o dispositivos inalámbricos WiFi en cualquier equipo susceptible de ser conectado a la red. La red es ad hoc porque no depende de una infraestructura pre-existente, como routers (en redes cableadas) o de puntos de accesos en redes inalámbricas administradas. En lugar de ello, cada nodo participa en el encaminamiento mediante el reenvío de datos hacia otros nodos, de modo que la determinación de estos nodos hacia la información se hace dinámicamente sobre la base de conectividad de la red.

  Este tipo de red permite la adhesión de nuevos dispositivos, con el solo hecho de estar en el rango de alcance de un nodo ya perteneciente a la red establecida. El principal inconveniente de este tipo de redes radica en el número de saltos que debe recorrer la información antes de llegar a su destino. Cada nodo que retransmite la información implica un salto, cuantos más saltos, mayor es el tiempo que tarda en llegar la información a su destino y aumenta la probabilidad de que la información se corrompa con cada salto.

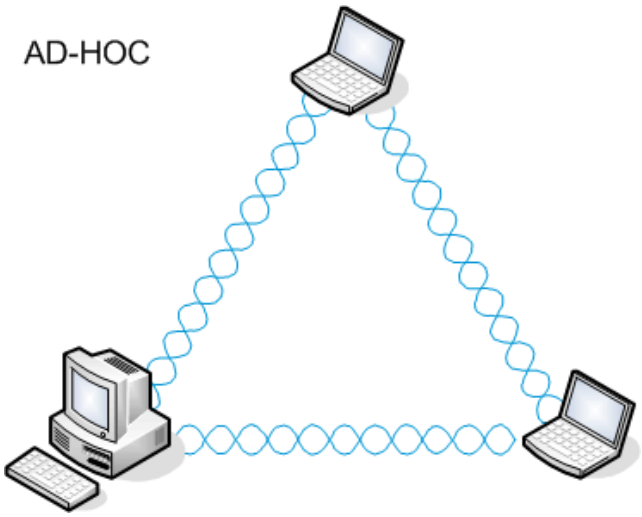


Figura 2. Configuración de red modo AD-HOC

Fuente: José Barrachina

- **Modo infraestructura.** En esta configuración, además de las tarjetas WiFi se necesita disponer de un equipo conocido como Punto de

Acceso (AP). Cada estación informática (EST) se conecta a un punto de acceso a través de un enlace inalámbrico. La configuración formada por el punto de acceso y las estaciones ubicadas dentro del área de cobertura se llama conjunto de servicio básico o BSS. Estos forman una célula. Cada BSS se identifica a través de un BSSID que en modo infraestructura corresponde al punto de acceso de la dirección MAC

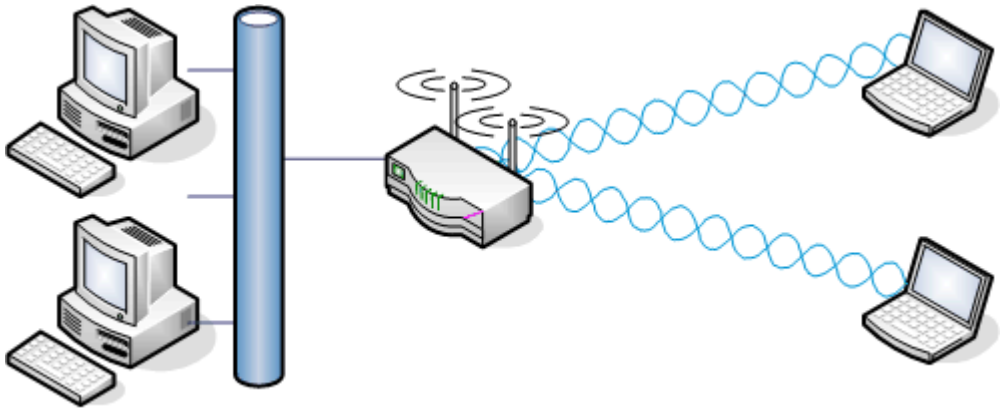
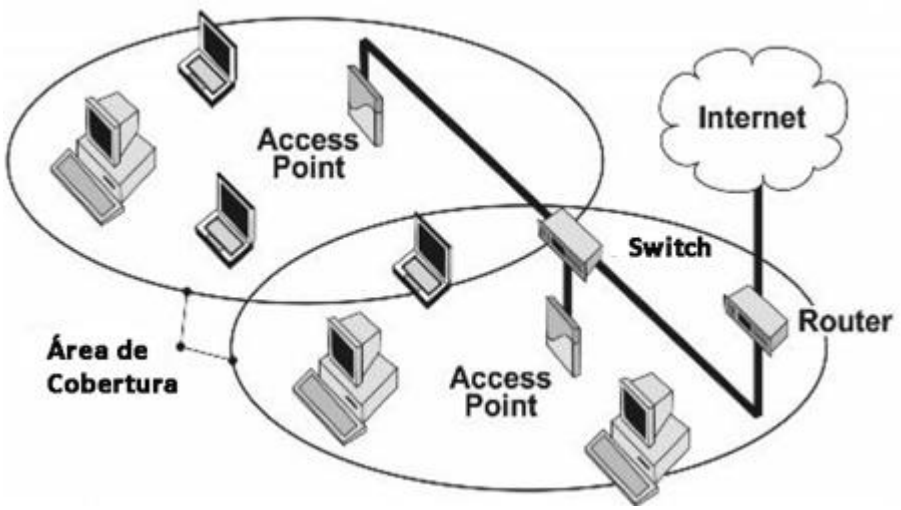


Figura 3. Configuración de red modo Infraestructura

Fuente: José Barrachina

Con una conexión llamada sistema de distribución (SD), es posible relacionar varios puntos de acceso juntos (o con más exactitud, varios BSS) para formar un conjunto de servicio extendido o ESS.



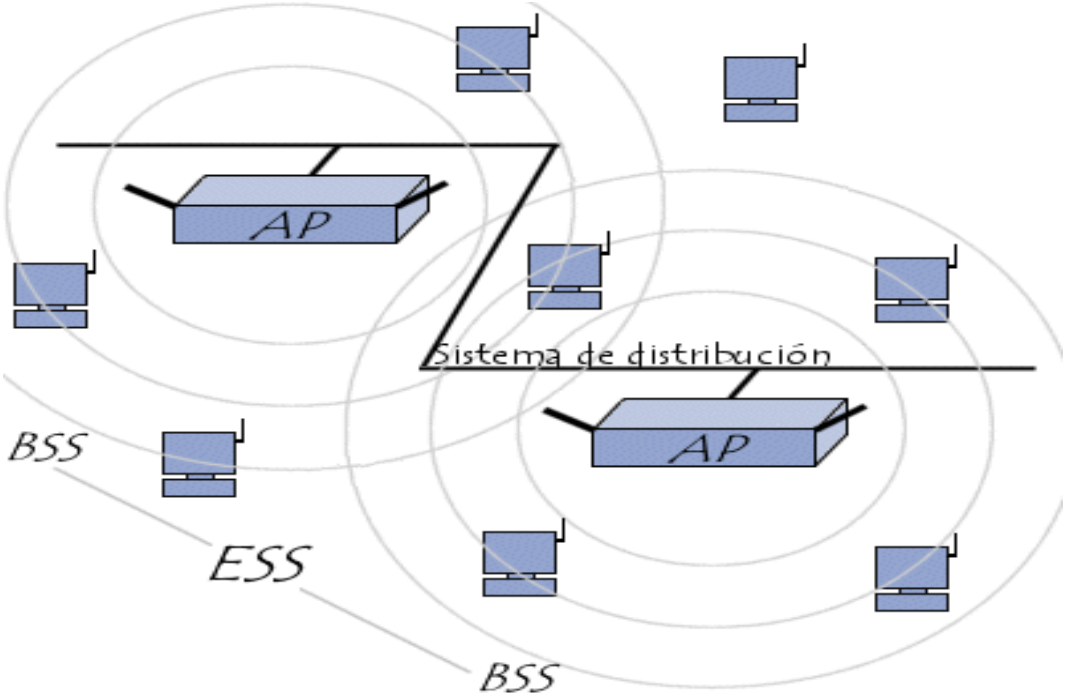


Figura 4. Configuración de red llamada sistema de distribución

Fuente: Cristian Jimenez –SENA CAUCA

Un servicio ESS se identifica a través de un ESSID (identificador del conjunto de servicio extendido), a menudo abreviado como SSID, que muestra el nombre de la red y de alguna manera representa una medida de seguridad de primer nivel ya que una estación debe saber el SSID para conectarse a la red extendida.

Las comunicaciones ad hoc son muy fáciles de configurar y resultan muy interesantes cuando se necesita establecer una comunicación temporal entre dos equipos. Por otro lado, el modo infraestructura es el más adecuado para crear redes permanentes. Las razones que nos llevan a esta conclusión son varias: [5]

- El modo infraestructura ofrece un mayor alcance que la modalidad ad hoc. Los terminales no tienen por qué estar dentro del área de cobertura el uno del otro; al tener un punto de acceso intermedio pueden, al menos, duplicar su distancia.

- El punto de acceso permite compartir el acceso a Internet entre todos sus terminales. Esto permite compartir un acceso de banda ancha (ADSL o cable) entre todos los terminales que forman la red, sean dos o cientos de ellos.
- El punto de acceso permite crear redes con un mayor número de terminales.
- El punto de acceso ofrece características de gestión de la comunicación que no ofrece el modo ad hoc.
- El punto de acceso, al igual que cualquier red local, permite compartir los recursos de los terminales que forman la red (archivos, impresoras, etc.

Seguridad de las redes WiFi [5]

La seguridad de una red, incluidas las redes WiFi, puede ser comprometida en dos aspectos: autenticación y cifrado.

Los mecanismos de autenticación se emplean para identificar un usuario inalámbrico ante un punto de acceso y viceversa, mientras que los mecanismos de cifrado aseguran que no sea posible decodificar el tráfico de usuario.

Los protocolos de seguridad para redes Wifi, deben, por lo tanto, proteger estos dos puntos vulnerables ante posibles ataques. Con ese objetivo, desde la aparición de dichas redes los protocolos del nivel de enlace desarrollados específicamente para dotarlas de seguridad han sido WEP, WPA, WPA2. [5]

La evolución de la seguridad en el estándar IEEE 802.11 y la WiFi Alliance, se muestra en la siguiente figura:

Fecha	Hitos
Septiembre 1997	Estándar IEEE 802.11 ratificado, incluyendo WEP.
Abril 2000	Lanzamiento del programa de certificación (WiFi CERTIFIED), con soporte para WEP.
Mayo 2001	Se crea el grupo de trabajo IEEE 802.11i
Abril 2003	Se introduce WPA con: • Autenticación IEEE 802.11X • Encriptación *Temporal Key Integrity Protocol* (TKIP) • Compatible con *EAP-Transport Layer Security* (EAP-TLS)
Septiembre 2003	Obligatorio WPA para todos los equipos WiFi CERTIFIED
Junio 2004	Rectificación IEEE 802.11i ratificada
Septiembre 2004	Se introduce WPA2 con: • Autenticación IEEE 802.11X • Encriptación AES • Compatible con EAP-TLS
Abril 2005	Apoyo a cuatro tipos EAP adicionales: • *EAP Tunneled TLS Microsoft Challenge Handshake Authentication Protocol Version 2* (EAP-TTLS/MSCHAPv2) • *Protected EAP Version 0* (PEAPv0)/EAP-MSCHAPv2 • *Protected EAP Version 1* (PEAPv1)/EAP *Generic Token Card* (EAP-GTC) • *EAP-Subscriber Identity Module* (EAP-SIM)
Marzo 2006	Obligatorio WPA2 para todos los equipos WiFi CERTIFIED
Enero 2007	Lanzamiento *WiFi Protected Setup* (WP S)
Noviembre 2007	Se crea el grupo de trabajo IEEE 802.11w
Mayo 2009	Apoyo para EAP-AKA y EAP-FAST añadido

Por otro lado, los mecanismos de seguridad del nivel de enlace utilizables en este tipo de redes son PPTP y P2TP. Por lo que, estos mecanismos de seguridad no son específicos de redes WiFi, sino que son aplicables también en otro tipo de redes, estas tecnologías tienen la capacidad de crear una Red Privada Virtual o VPN.

-WEP: (Wired Equivalency Protocol, 'Protocolo de equivalencia con red cableada') es el sistema de cifrado incluido en el estándar 802.11 como protocolo que permite cifrar la información que se transmite entre los usuarios y el punto de acceso utilizando el algoritmo de cifrado RC4.

RC4 fue diseñado en 1987 por Ron Rivest. Este algoritmo se basa en generar claves de cifrado arbitrarias empleando la función lógica XOR. La longitud de RC4 no es fija, puede ser de 64 bits (40 bits de clave con un vector de inicialización (IV) de 24 bits), o de 128 (104 bits con un vector de inicialización de 24 bits). El vector de

inicialización es una parte variable de la clave para impedir que un posible atacante recopile suficiente información cifrada con una misma clave. Además, se utiliza un checksum basado en CRC32 para prevenir que se inyecten paquetes en el flujo de datos.

Como primera solución de seguridad, WEP resultó vulnerable debido a las limitaciones en el tamaño de las claves, a la facilidad para obtenerlas espiando el tráfico y a la falta de detección de réplicas maliciosas. A pesar de las múltiples vulnerabilidades, los usuarios solían completar la seguridad WEP generalmente de forma conjunta con otras soluciones de seguridad como por ejemplo soluciones VPN, facilidades IEEE 802.11X y soluciones propietarias de los fabricantes.

En cualquier caso, para neutralizar los problemas se ofrecieron alternativas con mayores niveles de seguridad como WPA, WPA2.

En 2003 la Alianza WiFi promovió la seguridad WPA con un subconjunto de las facilidades que se estaban diseñando en el 802.11i.

-WPA: WiFi Protected Access fue creado para corregir las deficiencias del sistema previo, WEP, incorporando un método de autenticación y mejoras en el nivel de codificación existente. Cuando IEEE se puso a trabajar en su nueva recomendación 802.11i, buscaba una solución rápida a los inconvenientes WEP y además una solución que fuese compatible con el hardware existente. Por este motivo, se decidió desarrollar dos soluciones. Una rápida y temporal que se denominó WPA y otra más definitiva para aplicar en nuevos puntos de acceso, no siendo compatible con el hardware anterior, que se denominó WPA2.

WPA es un estándar que opera a nivel MAC y está basado en un borrador del estándar IEEE 802.11i. Aunque WPA tiene algunas carencias que el definitivo IEEE 802.11i no tiene.

WPA consigue paliar las debilidades conocidas de WEP introduciendo una extensión del vector de inicialización que pasa a ser de 24 a 48 bits, minimizando así la reutilización de claves. Se proponen mecanismos nuevos de derivación y distribución de claves y un nuevo protocolo conocido como TKIP (Temporal Key

Integrity Protocol) para la generación de claves por paquete. Este protocolo emplea el algoritmo de cifrado RC4, al igual que WEP, pero elimina el problema de las claves estáticas compartidas. Se encarga de cambiar dicha clave cada cierto tiempo, ampliando la longitud de la clave de 40 a 128 bits, y pasa de ser única y estática a ser generada de forma dinámica para cada usuario y para cada paquete.

TKIP cifra el vector de inicialización, que suponía un problema de privacidad en WEP ya que el IV se enviaba por el aire sin cifrado alguno, para evitar ataques que permitan revelar la clave.

Además, se incluye el Control de la Integridad del Mensaje (Message Integrity Check, MIC), llamado Michael, que verifica la integridad de los datos de las tramas diseñado para prevenir que intrusos capturen paquetes, los alteren y los reenvíen. La función MIC, reemplaza el Checksum CRC32 utilizado en WEP. Michael provee una función matemática de alta fortaleza en la cual el transmisor y el receptor deben computar y comparar si coinciden o no los datos; Si no coinciden los datos se consideran corruptos y se desecha el paquete. De este modo, TKIP impide que un atacante pueda alterar los datos que se transmiten dentro de un paquete.

En cuanto a la autenticación, el mecanismo usado emplea 802.X y EAP. En función del entorno de aplicación, en WPA es posible operar en dos modalidades:

- Modalidad de red doméstica o WPA-PSK (Pre-Shared Key): En estos entornos no es posible contar con un servidor de autenticación centralizado o un marco EAP. Se requiere introducir una contraseña compartida en el punto de acceso o modem ADSL, así como en cada uno de los dispositivos que desean conectarse a la red WiFi. Solamente podrán acceder al punto de acceso los dispositivos cuya contraseña coincida con la del punto de acceso. Esto evita ataques basados en escuchas, así como acceso de usuarios no autorizados. La contraseña provee una relación de acuerdo único para generar el cifrado TKIP en la red. Por lo tanto, aunque la contraseña inicial es compartida por todos los dispositivos de la red, no lo son las claves de cifrado que son diferentes para cada dispositivo.

- Modalidad de entorno empresarial: En este entorno WPA utiliza el estándar IEEE 802.11x y EAP. EAP se emplea como transporte extremo a extremo para los métodos de autenticación entre el dispositivo de usuario y los puntos de acceso. Mientras que IEEE 802.1x se emplea como marco para encapsular los mensajes EAP en el enlace radio. El conjunto de estos dos mecanismos, junto con el esquema de cifrado forman una fuerte estructura de autenticación que utiliza un servidor de autenticación centralizado, por ejemplo, un servidor RADIUS. [9]

-WPA2: Es la versión certificada interoperable de la especificación completa del estándar IEEE 802.11i. La seguridad es mucho más robusta que la que ofrece WPA. WPA2 refuerza el algoritmo de cifrado utilizando como protocolos de cifrado CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) basado en el algoritmo de encriptación AES (Advanced Encryptation Standard) de 128 bits. Este brinda un alto nivel en la autenticación de usuarios, pero tiene como desventaja que no es compatible con versiones anteriores de software.

El elemento estándar que negocia dinámicamente los algoritmos de autentificación y de cifrado que se utilizarán para las comunicaciones entre los puntos de acceso y los usuarios inalámbricos es conocido como RSN (Robust Security Network). RSN utiliza AES, junto con IEEE 802.1x y EAP. El protocolo de seguridad que RSN construye sobre AES es el CCMP.

Otra mejora respecto a WPA es que incluye soporte no sólo para el modo infraestructura BSS sino también para redes ad-hoc y permite la de-autenticación y disociación segura de la red.

-Autenticación y gestión de claves WPA, WPA2: EAP e IEEE 802.1X

- IEEE 802.1X: Es un estándar para el control de acceso a red de nivel 2 que contempla un marco para la autenticación y la distribución de claves. El estándar traduce las tramas enviadas por un algoritmo de autenticación en el formato necesario para que estas sean entendidas por el sistema de autenticación que utilice la red. Por lo tanto, IEEE 802.1x, no es por sí mismo un método de autenticación y debe emplearse de forma conjunta con protocolos de autenticación para llevar a

cabo la verificación de las credenciales de usuario, así como la generación de las claves de cifrado.

802.1x involucra la existencia de tres actores:

- Solicitante: Usuario inalámbrico que desea acceder a la red
- Autenticador: Generalmente es un punto de acceso que recibe la conexión del solicitante, su función es forzar el proceso de autenticación y enrutar el tráfico a las entidades adecuadas de la red.
- Servidor de autenticación: Se trata del servidor que verifica las credenciales del solicitante. Generalmente se suele emplear como servidor de autenticación remota de usuarios servidores RADIUS (Remote Authentication Dial In User Service)

Cuando el equipo del usuario va a acceder a la red, el punto de acceso le envía una petición de identificación. El usuario le envía su identificación, que el punto de acceso reenvía al servidor. Tras comprobar el derecho de acceso del usuario, el servidor envía su autorización para permitir su acceso a la red.

La autenticación del cliente se lleva a cabo mediante el protocolo EAP y generalmente un servidor RADIUS; Existen algunas variantes del protocolo EAP, según la modalidad de autenticación que se emplee.

-EAP: Un punto de acceso 802.1x sólo se comunica con los usuarios autentificados. Antes de su autenticación sólo admite las comunicaciones con el protocolo EAP (Extensible Authentication Protocol) para verificar su identidad.

EAP es un protocolo de autenticación definido para llevar a cabo tareas de AAA y fue diseñado originalmente como una extensión del protocolo PPP (Point to Point Protocol). Cuando una red inalámbrica utiliza EAP, el usuario solicita conectividad a la red WiFi a través de un punto de acceso. El punto de acceso solicita al dispositivo que se identifique y envía los datos de identificación que éste le envía a un servidor de autenticación. Una vez el servidor ha comprobado la veracidad del nuevo dispositivo, envía su respuesta al punto de acceso, y este concluye la autenticación del nuevo dispositivo si la respuesta por parte del servidor de autenticación ha sido satisfactoria.

Existen diferentes versiones de EAP, siendo las más comunes: EAP-MD5 (Message Digest 5): Para la autenticación emplea un nombre de usuario y contraseña. La contraseña se cifra mediante el algoritmo MD5, mientras que el nombre de usuario se envía sin ningún tipo de protección. Este sistema es vulnerable a los ataques del tipo Man-In-TheMiddle y ataques diccionario. Además, no utiliza ningún mecanismo de seguridad para autenticar el servidor y la estrategia para autenticar al usuario es por medio de contraseñas. Proporciona un nivel de seguridad muy bajo por lo que no es recomendable utilizarlo como protocolo en redes inalámbricas.

- EAP-LEAP (Lightweight EAP): Protocolo propietario de Cisco en el que se utilizan las contraseñas como método de autenticación del servidor. Las credenciales de usuario se envían sin cifrar. LEAP no soporta la utilización de One Time Password (OTP) y requiere de infraestructura CISCO para poder ser utilizado. Esta autenticación, aunque ligera, previene de ataques Man-in The-middle y de secuestro de la sesión, pero sigue manteniendo el riesgo de exposición de la identidad y de ataques diccionario.
- EAP-TLS (Transport Layer Security): Está considerado como el protocolo más seguro. Ofrece una autenticación mutua entre el cliente y el servidor. Utiliza certificados digitales para garantizar la identidad del cliente y del servido. Esto obliga a disponer de una infraestructura de clave pública para gestionar estos certificados, lo que lo hace aconsejable sólo cuando se necesitan altos niveles de seguridad.
- EAP-TTLS (Tunnelled TLS): Está orientado a trabajar con servidores RADIUS. Está integrado con una gran variedad de formatos de almacenamiento de contraseñas y sistemas de autenticación basados en contraseñas así como con múltiples bases de datos de seguridad. TTLS ofrece autenticación fuerte mutua y sólo requiere certificados en el servidor. Con EAPTTLS se elimina la necesidad de configurar certificados para cada usuario de la red inalámbrica. Se autentica al usuario en el sistema con las credenciales basadas en nombre de usuario y contraseñas, y se cifran las

credenciales de usuario para garantizar la protección de la comunicación inalámbrica.

- PEAP (Protected EAP): Desarrollado por Microsoft, Cisco y RSA Security, es muy similar a EAP-TTLS, en el sentido de que solamente requiere certificado de seguridad en el servidor. Provee protección a métodos más antiguos de EAP mediante el establecimiento de un túnel seguro TLS entre cliente y el autenticador.
- EAP-FAST (Flexible Authentication via Secure Tunnelling): Protocolo creado por Cisco para reemplazar a LEAP. Ofrece una autenticación mutua tunelada y no es imprescindible que el servidor se identifique con un certificado digital. En su lugar ofrece utilizar una clave secreta compartida conocida como PAC (Protected Access Credential, 'Credencial de acceso protegido').
- EAP-SIM (Subscriber Identity Module): Ofrece una autenticación mutua mediante la utilización de tarjetas SIM insertadas en el propio dispositivo inalámbrico o conectada a través del puerto USB. [14]

6. METODOLOGIA DE LA INVESTIGACION

6.1 Enfoque

Este apartado del proyecto de investigación, presenta las actividades y los medios a través de los que se pretende cumplir con los objetivos formulados y por ende, dar respuesta a la pregunta de la problemática de investigación. En este sentido, se utiliza un enfoque cuantitativo y cualitativo.

Cuantitativo en vista que se pretende medir los niveles de señal electromagnéticos que permitan garantizar una cobertura adecuada para las zonas requeridas dentro de la FICA.

Y un enfoque Cualitativo, toda vez que se quiere evidenciar el grado de satisfacción respecto a la conectividad hacia el Internet a través de la red Wifi planteada.

6.2 Modalidad básica de la investigación

Algunas de las áreas de la práctica científica son:

* Investigación Documental: Este tipo de investigación es la que se realiza apoyándose en fuentes de carácter documental, esto es, en documentos de cualquier especie. Como subtipos de esta investigación están la investigación bibliográfica, la hemerográfica y la archivística; la primera se basa en la consulta de libros, la segunda en artículos o ensayos de revistas y periódicos, y la tercera en documentos que se encuentran en los archivos, como cartas, oficios, circulares, expedientes.

* Investigación de Campo: Este tipo de investigación se apoya en informaciones que provienen entre otras, de entrevistas, cuestionarios, encuestas y observaciones. En esta se obtiene la información directamente en la realidad en que se encuentra, por lo tanto, implica observación directa por parte del investigador.

* Investigación Experimental: Es la investigación en la que se obtiene la información por medio de la observación de los hechos, y que se encuentra dirigida a modificar la realidad con el propósito de estudiarla en circunstancias en las que normalmente no se encuentran, con el fin de describir y analizar lo que ocurriría en determinadas condiciones.

* Investigación Exploratoria: Es la que se realiza con el propósito de destacar los aspectos fundamentales de una problemática determinada y encontrar los procedimientos adecuados para elaborar una investigación posterior. Es útil desarrollar este tipo de investigación porque, al contar con sus resultados, se simplifica el abrir líneas de investigación y proceder a su comprobación.

* Investigación Descriptiva: Mediante este tipo de investigación, que utiliza el método de análisis, se logra caracterizar un objeto de estudio o una situación concreta, señalar sus características y propiedades. Combinada con ciertos criterios

de clasificación sirve para ordenar, agrupar o sistematizar los objetos involucrados en el trabajo indagatorio.

* Investigación Explicativa: Mediante este tipo de investigación, que requiere la combinación de los métodos analítico y sintético, en conjugación con el deductivo y el inductivo, se trata de responder o dar cuenta de los porqués del objeto que se investiga

En este sentido, en el presente proyecto se utiliza una modalidad que comprende la investigación documental, descriptiva y de campo.

Se pretende desarrollar todos los aspectos relacionados con el marco teórico de referencia; recolectando toda la información necesaria de fuentes primarias y secundarias, para construir un estado del arte lo suficientemente fuerte como para analizar y caracterizar de manera crítica un objeto de estudio, señalando sus características y propiedades con respecto al campo de conocimiento de redes inalámbricas de área local (WLAN) utilizando tecnología WiFi.

Para llevar a cabo la investigación se acudirá a la realización de una revisión exhaustiva de la bibliografía relacionada con los temas de interés respecto al proyecto.

A continuación, se pretende alcanzar a través de la revisión de documentos, artículos, libros, foros, páginas web, congresos, actividades académicas, etc., que tengan relación con el problema de investigación. Además, se utilizará las herramientas apropiadas como encuestas y entrevistas para determinar las características y propiedades de la red a diseñar, todo esto requiere la observación directa del investigador.

6.3 Nivel o Tipo de Investigación

Para el cumplir con los objetivo propuesto se llegará a desarrollar y describir los diseños, soluciones principales y alternas, recomendaciones, mejores prácticas través de lo cual se pueda obtener finalmente un modelo para la implementación de la infraestructura tecnológica WiFi para la FICA.

6.4 Población y Muestra

El presente análisis se basa en un universo de estudio conformado por 2000 estudiantes y profesores de la Facultad que constituyen posibles usuarios del sistema de Internet inalámbrica. La muestra utilizada para realizar la encuesta del estudio de mercado se basa en un muestreo probabilístico aleatorio simple en el cual se calculó la muestra tomando la fórmula de poblaciones finitas, de la siguiente manera:

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

En donde:

σ = 1.96 para α = 0.05. Para un 95% de seguridad de la muestra

N = tamaño conocido de la población

p = Prevalencia esperada del parámetro a evaluar, si se desconoce utilizar 0.5

que hace mayor el tamaño de la muestra.

q = 1 – p

e = error que se prevé cometer, para este caso 0.1 que equivale al 10%.

Entonces:

$$n = \frac{1.96^2 \text{ x } 2000 \text{ x } 0.5 \text{ x } 0.5}{0.1^2 \text{ x } 1999 + 1.96^2 \text{ x } 0.5 \text{ x } 0.5} = 92$$

Para realizar esta etapa se utilizaron las siguientes herramientas.

a. Entrevista a funcionarios. Se llevaron a cabo 25 entrevistas a profundidad en distintos profesionales de la FICA, pertenecientes a las distintas carreras.

b. Encuestas. La muestra necesaria para este proyecto pue de 92, sin embargo se realizaron 180 encuestas a distintos estudiantes y profesores perteneciente a la FICA.

Como resultado de esta fase se obtuvieron datos que permitieron desarrollar la siguiente fase de este estudio.

En esta etapa se pretende realizar un análisis estadístico cuantitativo que permite establecer el estado y avance de despliegues de redes WiFi en el FICA.

6.5 Recolección de Información

Respecto a las técnicas de recolección se utilizarán las que se mencionan a continuación:

- Investigación Bibliográfica.
- Investigación en la Web.
- Charlas y conversatorios con expertos en el tema a fin de sustentar en forma justificada las soluciones a plantearse.
- Observación.
- Entrevistas
- Encuestas.
- Análisis.

7. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Para el análisis e Interpretación de Resultados de la investigación propuesto, se utilizó la Estadística Descriptiva, la cual permitirá recoger, organizar y analizar los datos.

Estos datos se representarán en gráficas de pastel con su respectivo análisis donde se interpretarán los resultados de las encuestas realizadas, nivel y calidad de señal de cobertura en las áreas a implementarse la red WiFi, asi como también posteriormente evaluar el nivel de satisfacción de los usuarios respectos a los servicios ofrecidos en la red WiFi a implementarse. Con lo cual, para luego proyectarse a las conclusiones.

8. PROPUESTA DE SOLUCION

8.1 Detalle de acciones

Para alcanzar el objetivo principal propuesto en el proyecto se planteó las siguientes fases:

- Documentación: Se elaborará el estudio del arte, tomando como base la bibliografía, de las tecnologías inalámbricas existentes. Se llevará a cabo un análisis minucioso de las tecnologías WiFi que es la que se diseñará y se implementará en la facultad.
- Toma de requisitos: Se ajustará los requerimientos que transmitan las autoridades de la Facultad, y se irá implementando paulatinamente la red en base a estos requerimientos. Se analizará estos requerimientos de manera que permitan alcanzar el objetivo propuesto de la forma más eficiente.
- Análisis y diseño: En esta fase se planteará el caso de estudio de nuestra red inalámbrica. Así como también la arquitectura de red general del sistema que se implementará en la FICA. Cómo se conectarán los puntos de acceso entre sí y con las plataformas centrales. Donde se ubicarán las líneas de comunicación.
- Ejecución: En esta fase se explicarán los pasos a seguir y la metodología que habría que emplear si se llevase a cabo el proyecto.
    1. Adquisición del equipamiento necesario para la implementar la red inalámbrica.
    2. Configuración de los puntos de acceso.
    3. Configuración de las controladoras principales.
- Certificación y mantenimiento: En esta fase se garantiza la calidad del estudio:
    1. Verificación en el sitio de la red diseñada en la facultad.

2. Estudio de la monitorización de los puntos de acceso y su funcionamiento.
3. Mantenimiento mediante programa apropiados para el efecto.

- Documentación y seguimiento:
    1. Para garantizar la correcta ejecución durante la vida del proyecto, se realiza una labor de seguimiento permanente, para que en cualquier momento solucionar cualquier problema que se presente.
    2. Elaboración de la memoria técnica de todo el proyecto.

8.2 Criterios de diseño para políticas de uso de red WIFI

Perfiles y Subredes

Tipo de Usuario (Perfil)	**FICA_ID01** **Invitados VIP**	**FICA_ID02** **Invitados**	**FICA_ID03** **Proveedores**	**FICA_ID04** **Autoridades**	**FICA_ID05** **Soporte TI**	**FICA_ID06** **Usuarios FICA**
Permisos **Para portátiles FICA y equipos Fijos.**				Navegación VIP, acceso a servicios de red (correo institucional, impresión). Autenticación LDAP.	Navegación TI con descargas, acceso a servicios de red (correo institucional, impresión) Autenticación LDAP.	Navegación básica sin descargas, acceso a servicios de red (correo institucional, impresión) Autenticación LDAP
Permisos **Otros dispositivos** **(portátiles adicionales, dispositivos móviles)**	Navegación VIP por tiempo.	Navegación básica sin descargas por tiempo	Navegación TI con descargas, acceso a servicios de red soportado por tiempos.			

Tipo de Usuario (Perfil)	**FICA_ID01** **Invitados VIP**	**FICA_ID02** **Invitados**	**FICA_ID03** **Proveedores**	**FICA_ID04** **Autoridades**	**FICA_ID05** **Soporte TI**	**FICA_ID06** **Usuarios FICA**
Rango de direcciones (Pueden ser el mismo o diferentes, especificar)	172.22.61.4 - 172.22.61.255	172.22.62.4 - 172.22.62.255	172.22.63.4 - 172.22.63.255	172.22.64.4 - 172.22.64.255	172.22.65.4 - 172.22.65.255	172.22.66.4 - 172.22.67.255
Máscara (Pueden ser el mismo o diferentes)	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.254.0
Gateway (Pueden ser el mismo o diferentes, especificar)	172.22.61.3	172.22.62.3	172.22.63.3	172.22.64.3	172.22.65.3	172.22.66.3
DNS1 (Pueden ser el mismo o diferentes, especificar)	172.20.40.215	172.20.40.215	172.20.40.215	172.20.40.215	172.20.40.215	172.20.40.215
DNS2 (Pueden ser el mismo o diferentes, especificar)	172.21.21.13	172.21.21.13	172.21.21.13	172.21.21.13	172.21.21.13	172.21.21.13

Tipo de Usuario (Perfil)	**FICA_ID01** **Invitados VIP**	**FICA_ID02** **Invitados**	**FICA_ID03** **Proveedores**	**FICA_ID04** **Autoridades**	**FICA_ID05** **Soporte TI**	**FICA_ID06** **Usuarios FICA**
Sufijo DNS (Pueden ser el mismo o diferentes, especificar)	FICA.ec	FICA.ec	FICA.ec	FICA.ec	FICA.ec	FICA.ec
Si se va a utilizar LDAP, nombre completo de la unidad	o=FICA, ou=uio	o=FICA, ou=uio	o=FICA, ou=uio	o=FICA, ou=uio	o=FICA, ou=uio	o=FICA, ou=uio
Si se va a utilizar RADIUS, nombre del grupo	No se usará RADIUS en primera fase.	No se usará RADIUS en primera fase.	No se usará RADIUS en primera fase.	No se usará RADIUS en primera fase.	No se usará RADIUS en primera fase.	No se usará RADIUS en primera fase.

POLITICAS DE BYOD: CAPA 2/3/4 “NO AUTORIZADOS”

Son los permisos que se aplican a los dispositivos conectados antes de que sean autenticados y autorizados

Tipo de Usuario (perfil)	**FICA_ID01 Invitados VIP**	**FICA_ID02 Invitados**	**FICA_ID03 Proveedores**	**FICA_ID04 Autoridades**	**FICA_ID05 Soporte TI**	**FICA_ID06 Usuarios FICA**
Cliente DHCP Int 0.0.0.0/0:67(WC puede dar direccionamiento inicial)	No	No	No	No	No	No
Acceso DNS1 Interno IP/32:53	No	No	No	No	No	No
Acceso DNS2 Interno 2 IP/32:53	No	No	No	No	No	No
Acceso a Portal NAC IP NAC/32:80	Validar	Validar	Validar	Validar	Validar	Validar
Oculto	Sí	Sí	Sí	Si	Sí	Sí

POLITICAS DE BYOD: CAPA 2/3/4 “AUTORIZADOS”

Son los permisos que se aplican a los dispositivos conectados una vez que han sido autenticados y autorizados

SSID Name	**FICA_ID01** **Invitados VIP**	**FICA_ID02** **Invitados**	**FICA_ID03** **Proveedores**	**FICA_ID04** **Autoridades**	**FICA_ID05** **Soporte TI**	**FICA_ID06** **Usuarios FICA**
Subred a Utilizar para registro	**172.22.60.0-172.22.60.255**	**172.22.60.0-172.22.60.255**	**172.22.60.0-172.22.60.255**	**172.22.60.0-172.22.60.255**	**172.22.60.0-172.22.60.255**	**172.22.60.0--172.22.60.255**
Subred a Utilizar Usuario registrado	172.22.61.4 - 172.22.61.255	172.22.62.4 - 172.22.62.255	172.22.63.4 - 172.22.63.255	172.22.64.4 - 172.22.64.255	172.22.65.4 - 172.22.65.255	172.22.66.4 - 172.22.67.255
TAG VLAN ID	61	62	63	64	65	66
Cliente DHCP 0.0.0.0/0:67	172.20.40.215	172.20.40.215	172.20.40.215	172.20.40.215	172.20.40.215	172.20.40.215
Cliente DNS	8.8.8.8	8.8.8.8	8.8.8.8	172.20.40.215	172.20.40.215	172.20.40.215
Acceso puerto http	Si	Si	Si	Si	Si	Si
Acceso puerto https	Si	Si	Si	Si	Si	Si

Acceso a Red Servers (172.20.40.0)	No *Acceso solo a 172.20.40.215 (DHCP)	No *Acceso solo a 172.20.40.215 (DHCP)	No *Acceso solo a 172.20.40.215 (DHCP)	Si	Si	Si
Acceso a Red Administración 1 (10.20.1.0/24)	No	No	Si	No	Si	No
Acceso a Red Administración 2 (10.20.2.0/24)	No	No	Si	No	Si	No
Acceso a Red de Pisos (172.22.4X.0/24) X corresponde al Piso	No	No	No	Si	Si	Si
Permitir todo lo demás	No	No	No	No	Si	No
QoS	Si	Si	Si	Si	Si	Si
QoS (802.1p / Rate Limit)	Si	Si	Si	Si	Si	Si
Difusión	24 h	07:00 am – 22:00 pm	24 h	24 h	24 h	07:00 am – 22:00 pm

METODO DE AUTENTICACION

SSID	FICA_ID01 Invitados VIP	FICA_ID02 Invitados	FICA_ID03 Proveedores	FICA_ID04 Autoridades	FICA_ID05 Soporte TI	FICA_ID06 Usuarios FICA
802.1x						
LDAP				**X**	**X**	**X**
Captive Portal		**X**	**X**			
Guest (MAC) Registration	**X**			**X**		

Definiciones:

- SSID: Invitados VIP – SSID no oculto, PSK, activación bajo demanda en PB (Auditorio).
- SSID: Invitados – SSID oculto, SIN SPONSOR, PSK, helpdesk
- SSID: Proveedores – Oculto, Correo a helpdesk, SPONSOR OBLIGATORIO.

8.3 Criterios de diseño para ubicación de los access point en la FICA

8.3.1 Antecedentes

El edificio de la Facultad de Ingeniería en Ciencias Aplicadas (FICA) tiene una longitud de 36 metros por esto se ha dispuesto la colocación del Access Point en base a la calidad de señal de recepción mediante las pruebas de campo realizadas con Access Point ubicados en los pisos y midiendo el nivel de recepción mediante un cliente tanto en el piso donde se ubica el Access point como en los pisos contiguos, por lo tanto, se considera la distribución de equipos Access point de acuerdo al diagrama unifilar siguiente:

8.3.2 Diagrama unifilar

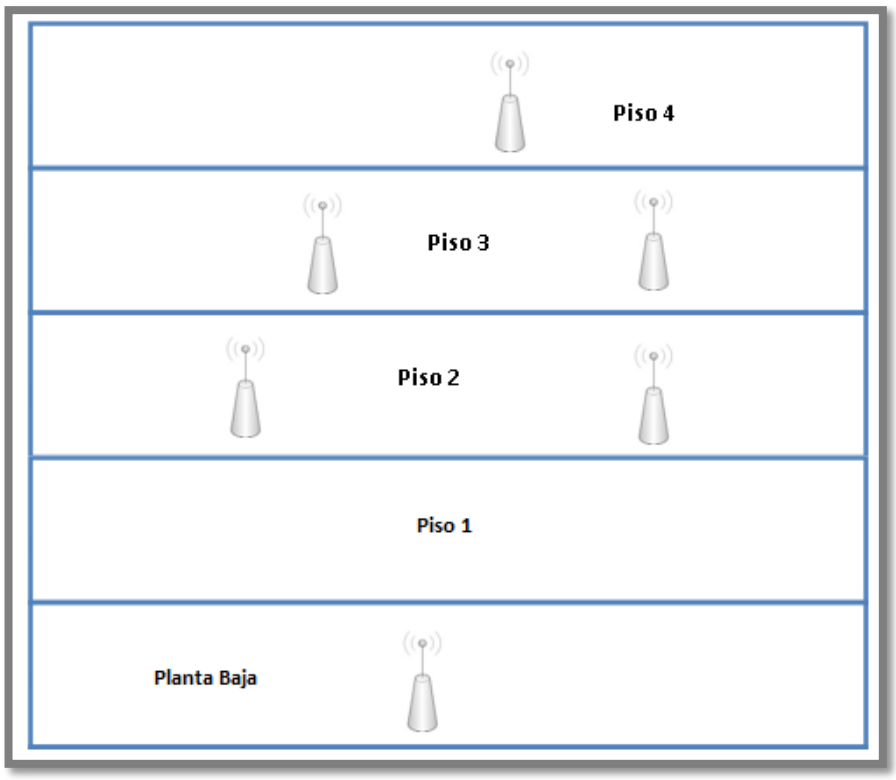


Figura 1 Diagrama Unifilar General

Para la solución técnica de este planteamiento se propone intercalar seis Access Point, uno en la planta baja, dos en el segundo piso, dos en el tercer piso y un último en el cuarto piso. La cobertura de esta manera estará bien dimensionada y equilibrada para todos los usuarios, de esta manera se tendrá la conexión hacia un LAN Controller por la ubicación intercalada de los seis AP´s.

Se pretende colocar de este modo los Access Point por las siguientes razones:

PLANTA BAJA

En la planta baja se colocará un Access Point en el centro del piso, con la finalidad de proveer cobertura en la parte exterior de la facultad y una parte de los laboratorios, además para que puedan acceder al servicio los docentes que lleven sus computadores.

PRIMER PISO

En el primer piso no se colocará ningún Access Point puesto que los laboratorios están conectados a la red cableada de la facultad, además la cobertura del Access Point de la planta baja y de los dos que se instalarán en el segundo piso va a cubrir los requerimientos de las personas que deseen conectarse en este piso.

SEGUNDO Y TERCER PISO

En estos dos pisos se encuentran ubicadas todas las aulas de la facultad, es por eso que aquí se tendrá la mayor concentración de estudiantes y lógicamente la demanda de conexión será más alta, es por estos motivos que se ha pensado colocar dos Access Point por piso, para así poder satisfacer la demanda requerida.

CUARTO PISO

En el cuarto piso se colocará un solo Access Point el mismo que dará cobertura a los laboratorios ubicados allí y que conjuntamente con los dos Access Point colocados en el piso de abajo puedan satisfacer la necesidad de cobertura.

Además se debe tener en cuenta esta solución los seis AP's tendrían que conectar a la energía eléctrica, por lo que necesitaremos encontrar los tomas de corriente cercanos al centro de cada piso que cumpla con las normas del estándar *TIA/EIA – 607* que se refiere a la Protección de Puesta a Tierra.

En los seis casos el planteamiento de la ubicación, el Access Point será colocado sobre una base metálica para de esta manera asegurar su estabilidad y seguridad. A este dispositivo solo tendrá acceso el personal encargado de dirigir la administración de la red, para evitar el uso indebido y la mala manipulación causando daños físicos e internos a los equipos.

Todo el sistema del cableado estará debidamente etiquetado de acuerdo al estándar *ANSI/TIA/EIA-606*, con una numeración local que identifique la nueva red inalámbrica, además para la verificación del cableado nos basaremos en el estándar *TIA/EIA – TSB67*.

Según lo establecido por el Instituto Nacional de Estándares Americanos (ANSI) la vida útil de los documentos reconocidos es de 5 años, es por eso que el estándar *ANSI/TIA/EIA-568-B* es ahora reemplazado por el estándar *ANSI/TIA/EIA-568-C* (en el cual nos basaremos*)* compilando en un solo documento las adendas del estándar anterior.

Se utiliza cable UTP categoría 6 para la realización del cableado. Las mediciones respectivas para este planteamiento se muestran a continuación.

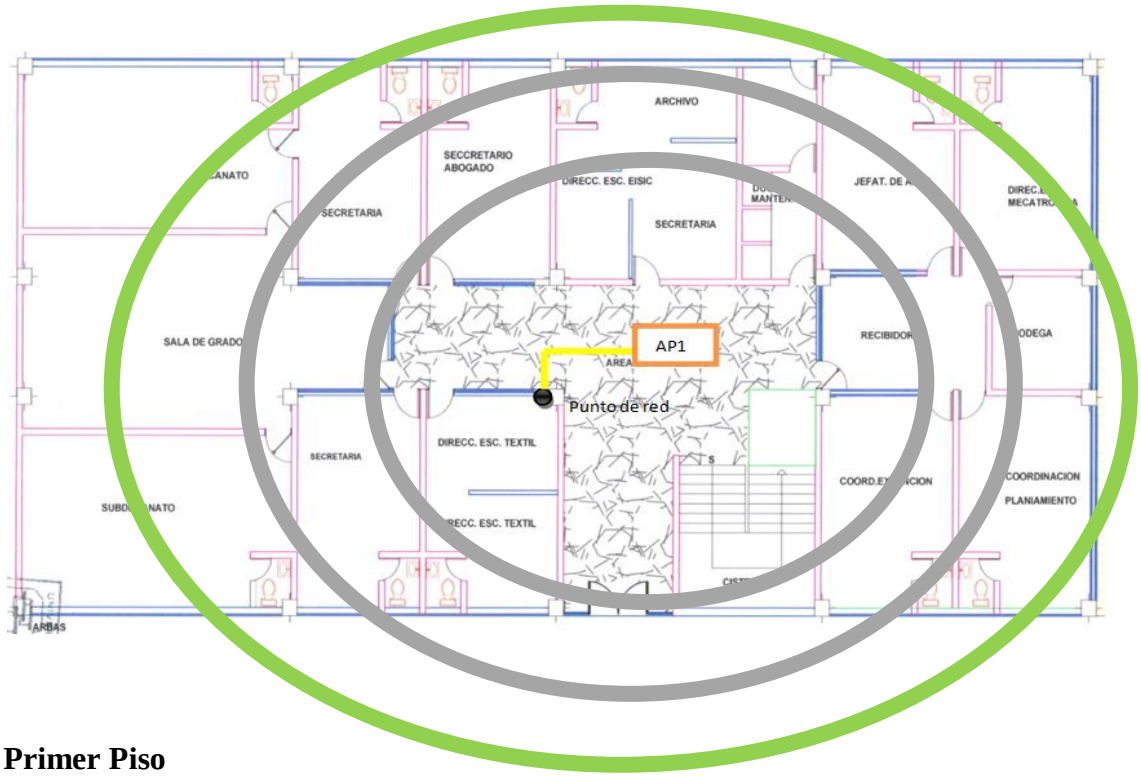
8.3.3 Disposición de los puntos de red y ubicación el rack

PUNTO DE ACCESO	LUGAR	PUNTO	SWITCH	PUERTO	FILA EN EL RACK
AP 1	PLANTA BAJA	PPC 23	Switch 5	Puerto 23	Segunda fila
AP 2	SEGUNDO PISO AULA 201	PPE10	Switch 4	Puerto 10	Segunda fila
AP 3	SEGUNDO PISO AULA 202	PPE14	Switch 4	Puerto 14	Segunda fila
AP 4	TERCER PISO ARCHIVO PUNTO 1	PPF9	Switch 4	Puerto 38	Primera Fila
AP 5	TERCER PISO ARCHIVO PUNTO 2	PPF10	Switch 4	Puerto 40	Primera Fila
AP 6	TERCER PISO ARCHIVO	PPF7	Switch 4	Puerto 37	Segunda Fila

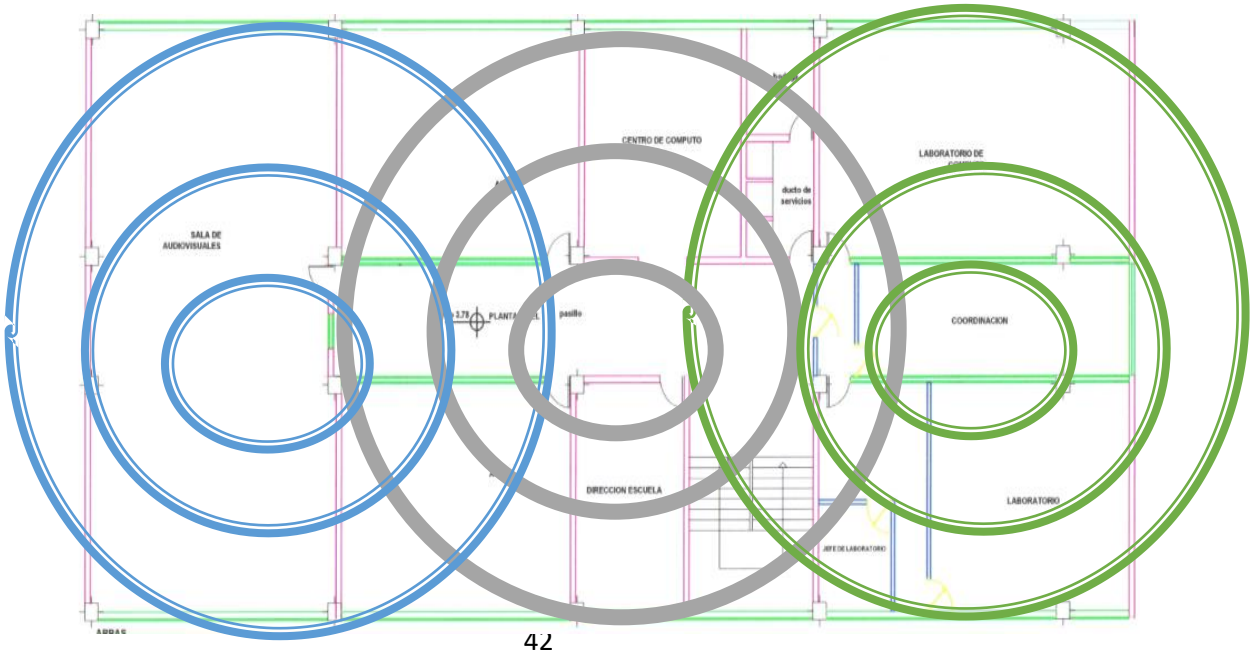
8.3.4 Criterios de área de cobertura

- Se considera que el AP1 cubrirá, toda la planta baja por estar posicionado en el medio, y partes del primer piso.

Planta Baja

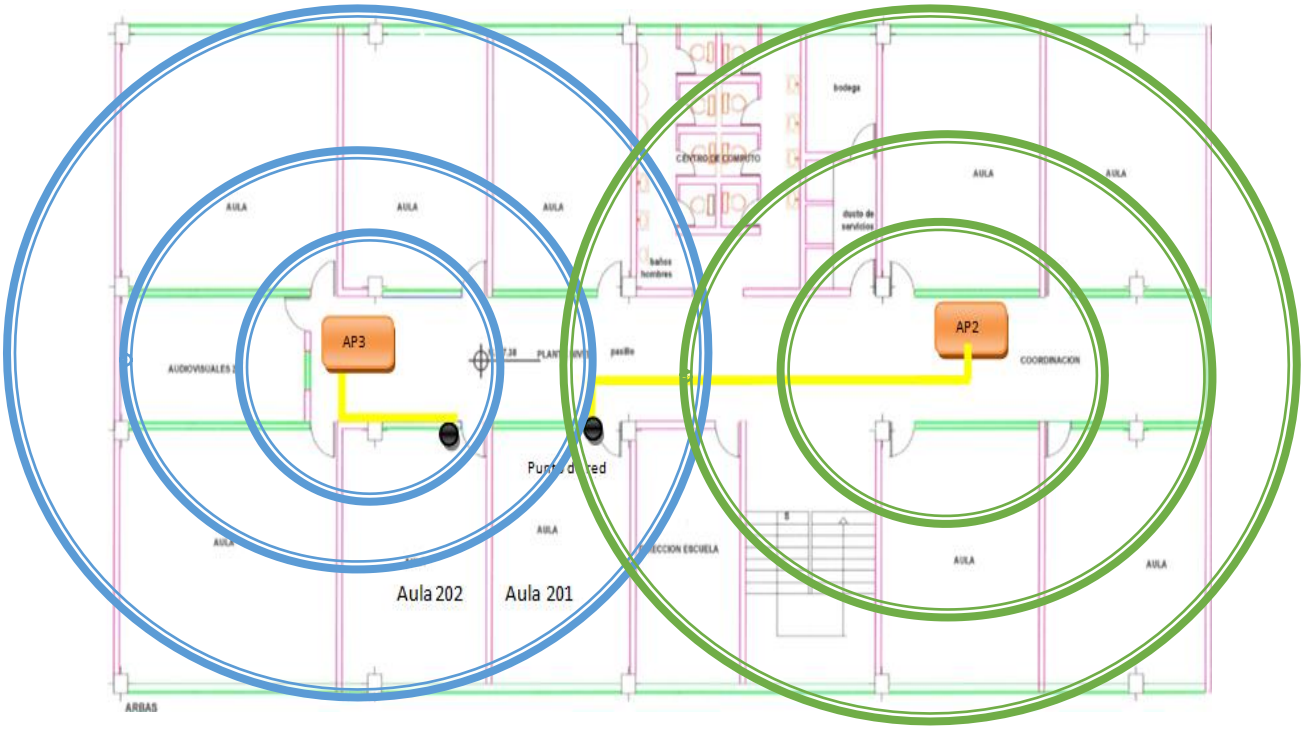


Primer Piso



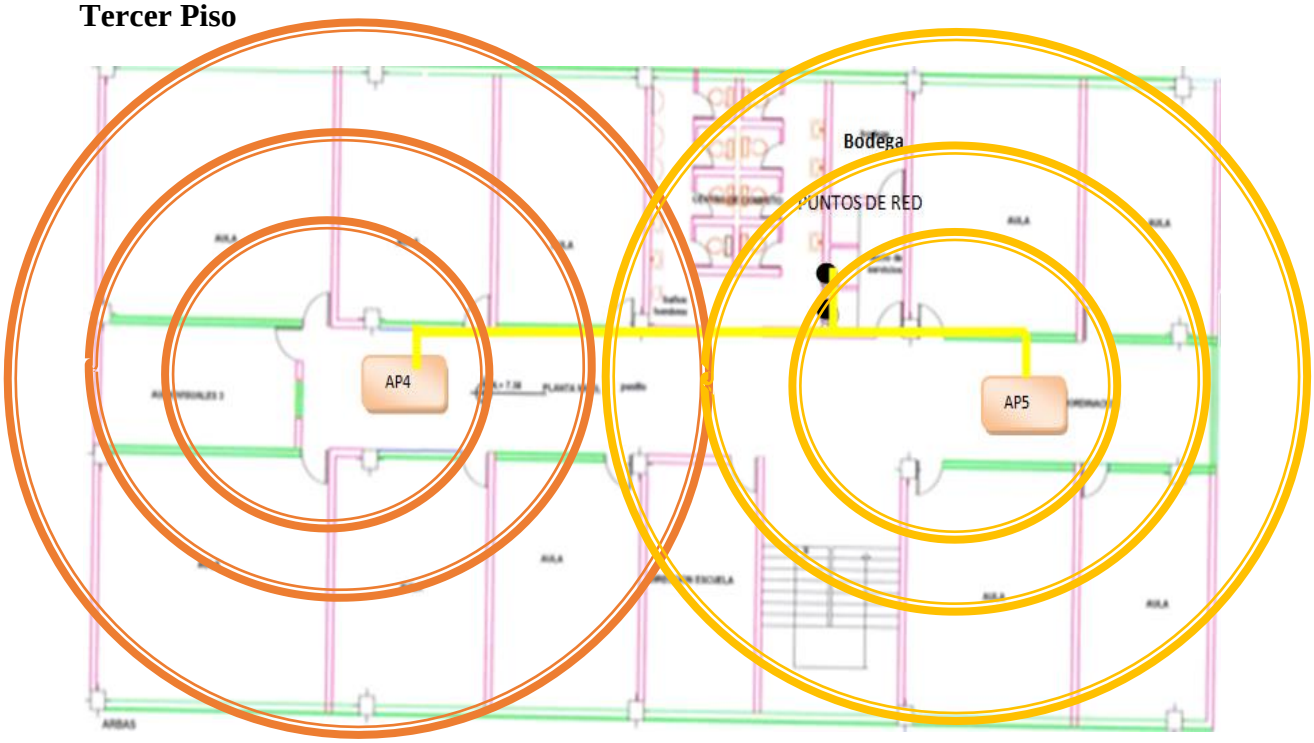
- Se considera que los AP2 y AP3 cubrirán todo el segundo piso y partes que no cubre el AP1 del Primer Piso.

Segundo Piso



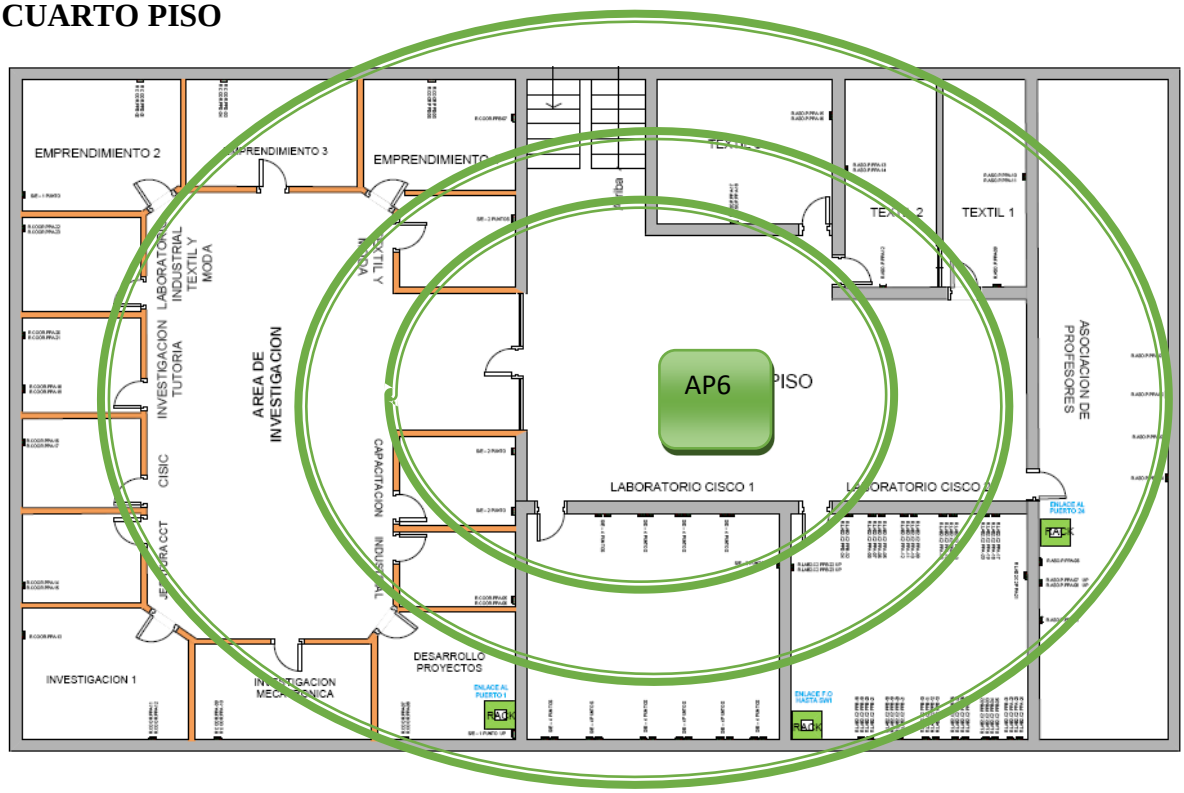
- Los AP4 y AP5 cubrirán todo el Tercer piso y partes del cuarto Piso.

Tercer Piso



- El AP6 cubrirá todo el cuarto piso.

CUARTO PISO



NOTA IMPORTANTE

8.3.5 Descripción de instalación del cableado de red

Después que realizamos todo el estudio para la ubicación de los Access Point, el estudio de los puntos de red en cada piso y las zonas de cobertura de cada AP, se realizará la inspección del cableado antiguo en la facultad y lo que podíamos rescatar para nuestra nueva instalación, es por este motivo que se retiraron los cables de red que estaban pasados por las canaletas y no tenían ninguna utilidad y así estas serán parte de la instalación desde los puntos de red hacia el punto de acceso en el piso que se encuentren.

Se tomará las medidas del cable que se utilizará en cada punto de red de los cuales se realizará la canalización para:

- AP 1 ubicado en la planta baja se utiliza un recorrido de cable de 4.5 metros y 2 metros de holgura 1 metro por cada extremo.
- AP 2 ubicado en el segundo piso se utiliza un recorrido de cable de 5 metros y 2 metros de holgura 1 metro por cada extremo.
- AP 3 ubicado en el segundo piso se utiliza un recorrido de cable de 15.50 metros y 2 metros de holgura 1 metro por cada extremo.
- AP 4 ubicado en el tercer piso se utiliza un recorrido de cable de 34.50 metros y 2 metros de holgura 1 metro por cada extremo.
- AP 5 ubicado en el segundo piso se utiliza un recorrido de cable de 16.50 metros y 2 metros de holgura 1 metro por cada extremo.
- AP 6 ubicado en el cuarto piso se utiliza un recorrido de cable de 30.00 metros y 2 metros de holgura 1 metro por cada extremo.

Se instalará una canaleta 3 tornillos y tacos en el corredor para el AP 5 y el resto de recorrido se reutilizaron las canaletas ya instaladas.

PUNTO DE ACCESO	**UBICACIÓN**	**PUNTO**	**RECORRIDO DE CABLE (m)**	**HOLGURA (m)**	**TOTAL DE CABLE (m)**
AP 1	PLANTA BAJA	PPC 23	4.50 m	2.00 m	6.50 m
AP 2	SEGUNDO PISO AULA 201	PPE10	5.00 m	2.00 m	7.00 m
AP 3	SEGUNDO PISO AULA 202	PPE14	15.50 m	2.00 m	17.50 m
AP 4	TERCER PISO ARCHIVO PUNTO 1	PPF9	34.50 m	2.00 m	36.50 m
AP 5	TERCER PISO ARCHIVO PUNTO 2	PPF10	16.50 m	2.00 m	18.50 m
AP6	CUARTO PISO ARCHIVO PUNTO 3	PPF	28.00 m	2.00 m	30.00 m

8.3.6 Descripción de instalación del cableado eléctrico

Se realizará la instalación de la fuente de alimentación para cada uno de los Access Point, se tomará la medida del recorrido desde el punto donde se conecta la fuente de alimentación hasta el punto de energía eléctrica elegido:

AP 1 ubicado en la Planta Baja se utilizará un recorrido de 1.20 metros hasta el cajetín que contiene la fuente de alimentación 2.00 metros hasta el primer toma de corriente. El recorrido del cable eléctrico tiene una medida de 0.20 metros.

AP 2 ubicado en el segundo piso en la Asociación de CIME se utilizará un recorrido de 1.00 metros hasta el cajetín que contiene la fuente de alimentación 0.50 metros hasta el primer toma de corriente. El recorrido del cable eléctrico tiene una medida de 4.00 metros. Se utilizará 2 canaletas y 8 tacos y tornillos para su instalación.

AP 3 ubicado en el segundo piso se utilizará un recorrido de 1.20 metros hasta el cajetín que contiene la fuente de alimentación 0.50 metros hasta el primer toma de corriente. El recorrido del cable eléctrico tiene una medida de 6.70 metros. Se utilizará 1 canaleta y 5 tacos y tornillos para su instalación.

AP 4 ubicado en el tercer piso se utiliza un recorrido de 1.20 metros hasta el cajetín que contiene la fuente de alimentación 2.00 metros hasta el primer toma de corriente. El recorrido del cable eléctrico tiene una medida de 12 metros.

AP 5 ubicado en el tercer piso se utilizará un recorrido de 1.20 metros hasta el cajetín que contiene la fuente de alimentación 2.00 metros hasta el primer toma de corriente. El recorrido del cable eléctrico tiene una medida de 11.90 metros.

AP 6 ubicado en el cuarto piso se utiliza un recorrido de 0.40 metros hasta el cajetín que contiene la fuente de alimentación 0.70 metros hasta la primera toma de corriente. El recorrido del cable eléctrico tiene una medida de 3 metros.

Se tomará las medidas exactas del cable que se utilizará en cada toma de corriente eléctrico tomando en cuenta el montaje de la fuente de alimentación de cada punto de acceso:

PUNTO DE ACCESO	**UBICACIÓN**	**FUENTE DE PODER(m)**	**RECORRIDO DE CABLE (m)**
AP 1	PLANTA BAJA	3.20 m	0.20 m
AP 2	ASOCIACION CIME	1.00 m	4.00 m
AP 3	SEGUNDO PISO AULA 203	1.70 m	6.70 m
AP 4	TERCER PISO AULA 303	3.20 m	11.80 m
AP 5	TERCER PISO AULA 311	3.20 m	11.90 m
AP6	CUARTO PISO CORREDOR	1.00 m	3.00 m

Se necesita un total de 37.60 metro de cable calibre 12 AWG para la instalación del cableado eléctrico.

Después de instalar el cableado tanto de red como eléctrico se instalará los tomacorrientes para los Access Point que necesitaran de alimentación eléctrica. Además de la instalación de cajetines de paso para el adaptador de energía que tiene cada Access Point.

CONCLUSIONES

- Los estudiantes y profesores de la Facultad de Ingeniería en Ciencias Aplicadas de la UTN, en aproximadamente un 80% están dispuestos y tienen los equipos necesarios para utilizar un servicio de Internet inalámbrica propuesto.
- Las redes inalámbricas pueden interactuar perfectamente con las redes Ethernet, permitiendo de esta manera aprovechar las ventajas de las redes cableadas junto con la funcionalidad y movilidad de las redes sin cables.
- Se recabó información y se analizó la situación real existente de la red de Facultad, así como las exigencias impuestas por los potenciales usuarios.
- Se propuso una solución inicial, con un plan de etapas o de actuación para la elaboración y ejecución de ésta.
- Mediante la implementación de red Wifi centralizada se facilita la gestión de equipamiento activo de la red, así como también la gestión y autenticación del acceso de los usuarios a la misma de una forma controlada.
- La utilización de tecnología inalámbrica en las redes de datos de área local, facilita y optimiza el despliegue de la red de acceso para usuarios móviles, los cuales en la actualidad tienden a un crecimiento de utilización en todas las empresas e instituciones.
- Al momento del dimensionamiento se consideró la sobreposición de celdas, con lo cual permite el roaming transparente para los usuarios y así brindar una fácil movilidad por el edificio.
- Es de mucha utilidad el uso de frecuencias diferentes para cada Punto de Acceso, ya que permite disminuir la interferencia electromagnética entre los diferentes Puntos de Acceso que forman parte de la red inalámbrica basada en WIFI.
- El diseño la red inalámbrica de la facultad se basó en los siguientes puntos:
    - Se definió el modelo de referencia adoptado y la arquitectura lógica de la red. La topología se basa en la integración de la WLAN en la

LAN de datos y el estándar de funcionamiento escogido es el IEEE 802.11g.

  - Se pensó en la arquitectura física adecuada. Se adquirió el equipamiento necesario según las condiciones de la facultad (puntos de acceso).
  - Se aplicó un etiquetado para los equipos.
  - Se pensó en una localización para éstos y definimos su conexionado mediante tablas y esquemas.
  - Se aplicó las medidas de seguridad pertinentes.
- Se configuró todos los puntos de acceso, y se los instaló en los lugares habilitados para ello.
- Se puso en funcionamiento la red y se inició las pruebas de verificación del estado de la misma

BIBLIOGRAFIA

1. WIFI, "Nada es imposible: Conexion WiFi de más de 500 Km", http://wifiw.com/2010/03/nada-es-imposible-conexion-wifi-de-mas-de-500-km/, 29 de marzo delo 2010
2. OFTELSAT A.C.P., "Tecnologías de Información y Comunicación para el Desarrollo", http://www.oftelsat.com/WEBlogs/weblogs.html, 6 de noviembre del 2010
3. WIKIPEDIA, "Wi-Fi de largo alcance", http://translate.google.com.ec/translate?hl=es&sl=en&u=http://en.wikipedia.org/wiki/Long-range_Wi-Fi&ei=Wzm_TJupJ8OB8gaewaG9Bg&sa=X&oi=translate&ct=result&resnum=1&ved=0CBwQ7gEwAA&prev=/search%3Fq%3Dwifi%2Blong%2Bdistance%26hl%3Des%26sa%3DG%26biw%3D780%26bih%3D454, Septiembre 2008
4. WIKIPEDIA, "La enciclopedia libre", http://es.wikipedia.org/wiki/Wikipedia:Portada, 6 de noviembre del 2010

5. arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20150123MartaMorenoMartin.pdf
6. http://docplayer.es/10155460-Diseno-de-un-sistema-de-red-inalambrico-basado-en-wimax-para-su-aplicacion-en-las-instalaciones-de-la-universidad-catolica-andres-bello.html
7. FRIENDLY, Hacker LLC, "Redes Inalámbricas en los Países en Desarrollo", Editorial Creative Commons, Tercera Edición, 2008
8. SIMÓ REIGADAS, Francisco Javier, Tesis Doctoral, "Modelado y optimización de IEEE 802.11 para su aplicación en el despliegue de redes extensas en zonas rurales aisladas de países en desarrollo", MADRID, ESPAÑA, Enero de 2007
9. Libros, papers, tutoriales publicados en Internet
10. Azadeh Kushki, Konstantinos N. Plataniotis,Anastasios N. Venetsanopoulos. (2012). WLAN Positioning Systems: Principles and Applications in Location-Based Services. Cambridge: Cambridge University.
11. David Roldán Martínez, José Huidrobo Moya. (2005). Comunicaciones en redes WLAN. Madrid: Creaciones Copyright.
12. Izaskun Pellejero, Fernando Andreu, Amaia Lesta. (2006). Fundamentos y aplicaciones de seguridad en redes WLAN. Barcelona: Marcombo S.A.
13. Arelys E. Ramos Fleites, Jesús García, Cesilio García Cruz. (2014). Procedimientos teóricos para el diseño de una Red WLAN. ilustrada.
14. Byron W. Putman. (2005). 802.11wlan Hands-on Analysis. AuthorHouse.
15. Carlos Valdivia Miranda. (2014). Sistemas informáticos y redes locales. Madrid: Paraninfo S.A.
16. Krishna Sankar. (2005). Cisco Wireless LAN Security. Indianapolis: Cisco Press.
17. Leonhard Korowajczuk. (2011). LTE, WiMAX and WLAN Network Design, Optimization and Performance Analysis. Chennain: John Wiley.
18. Neeli Prasad, Anand Prasad. (2002). WLAN Systems and Wireless IP for Next Generation Communications.
19. Pejman Roshan, Jonathan Leary. (2004). 802.11 Wireless LAN Fundamentals. Indianapolis: Cisco Press.