Universidad Técnica de Cotopaxi

Unidad Académica de Ciencias de la Ingeniería y Aplicadas

Ingeniería en Informática y Sistemas Computacionales

Tesis previa a la optención del Título de Ingeniero en informática y sistemas computacionales.

TEMA:

Propuesta de diseño de una red inalámbrica 802.11b/g en la Universidad de Pinar del Río con análisis de cobertura y de seguridad.

AUTORES:

Edgar Mauricio Bastidas Garzón
Luis Rodrigo Ordoñez Villacis

DIRECTOR DE TESIS:

MSc. Alexei Blanco Ortiz

Latacunga - Ecuador

Septiembre - 2010

DECLARACIÓN DE AUTORIDAD

Declaramos que somos autores de este Trabajo de Diploma y autorizamos a la Universidad Técnica de Cotopaxi, a hacer uso del mismo, con la finalidad que estime conveniente.

Firma: _____

Firma: _____

Edgar Mauricio Bastidas Garzón
Luis Rodrigo Ordoñez Villacis

maurisystem@hotmail.com
llogo27@hotmail.com

AGRADECIMIENTOS

A nuestros padres, por el esfuerzo inmenso que han realizado para nuestra formación, tanto en la vida como profesional.

A nuestras familias, que siempre nos han brindado su mano para encaminar nuestras vidas.

A nuestros compañeros de grupo, quienes compartieron estos cinco meses universitarios y nos ofrecieron lo mejor de ellos, en todo momento. Especialmente a David, Miguel, Darwin por habernos ayudado siempre y más en estos últimos días en el desarrollo de la Tesis.

A nuestro tutor Alexei Blanco Ortiz, el cual nos encaminó en el saber profesional, y gracias a él se pudo terminar este proyecto de diploma, al que estamos eternamente agradecidos.

Al conjunto de profesores brillantes, que supieron inculcarnos sus más grandes experiencias para una formación integral.

A todos los que de una manera u otra contribuyeron al desarrollo de este trabajo.

A todos “Muchas Gracias”

DEDICATORIA

A nuestros padres y nuestros hermanos quienes los consideramos lo más grande en nuestras vidas.

A nuestros abuelos por su inmenso apoyo incondicional.

A nuestros tíos por el gran apoyo y en general a toda nuestras familias, que supieron guiarnos por este camino.

A todos ellos, por ser la fuente de inspiración y amor.

PENSAMIENTO

“Añade el hombre conocimientos a conocimientos: nunca el saber es bastante. Si tanto es uno más hombre cuanto más sabe, el más noble empleo será aprender”.

(Padre Baltasar Gracián y Morales)

INDICE

TABLA DE CONTENIDO **Página**

RESUMEN

Este trabajo está centrado en la propuesta de diseño de una red inalámbrica en la UPR (Universidad de Pinar del Río) superpuesta a la red cableada ya existente, persiguiendo la idea de minimizar al máximo las zonas de sombra, constituyendo una alternativa para que los estudiantes y profesores del centro, así como invitados o asistentes a eventos y demás actividades organizadas por el centro, puedan acceder a los diferentes servicios que brinda la red cableada, a través de dispositivos computacionales móviles, garantizando la necesaria seguridad para la protección de la información transmitida. La propuesta se limita al edificio docente y la residencia estudiantil quedando el edificio de rectoría para un trabajo posterior.

Se hizo necesario realizar primeramente un estudio del estándar de redes inalámbricas 802.11 original y sus actualizaciones 802.11b y g sobre los que se basa la propuesta y que operan en la misma banda de 2.4 GHz.

El diseño presentado está avalado por una serie de mediciones reales realizadas en el edificio docente y en la residencia estudiantil en las que se utilizaron los puntos de acceso WRT54G de Linksys, marca registrada de Cisco Systems, el DIR 600 de DLink y el CWR-854V de CNet siendo el CommView for Wifi el software usado para determinar los niveles de señal en cada punto de análisis.

Palabras Claves: Redes inalámbricas, punto de acceso, encriptar.

SUMMARY

This work is centered in the proposal of design of a wireless network in the University of Pinar del Río (UPR) superimposed to the wired network already existent, pursuing the idea of minimizing to the maximum the shade areas, constituting an alternative so that the students and professors of the center, as well as companies or assistants to events and other activities organized by the center, they can consent to the different services that it offers the wired network, through mobile devices, guaranteeing the necessary security for the protection of the transmitted information. The proposal is limited to the educational building and the student residence being the parsonage building for a later work.

It became necessary to carry out a study of the standard of nets wireless 802.11 original and their upgrades firstly 802.11b and g on those that the proposal is based and that they operate in the same band of 2.4 GHz.

The presented design is endorsed by a series of real mensurations carried out in the educational building and in the student residence in those that the access points WRT54G of Linksys was used, it marks registered of Cisco Systems, the DIR 600 of DLink and the CWR-854V of CNet being the CommView for Wifi the software used to determine the sign levels in each analysis point.

Key words: Wireless networks, access point, encrypt.

INTRODUCCION

En los últimos años se ha producido un crecimiento en lo referente al desarrollo y aceptación de las comunicaciones móviles y en concreto de las redes de área local inalámbricas (Wireless LANs, WLAN). El momento decisivo para la consolidación de estos sistemas fue la conclusión del estándar IEEE 802.11 en el mes de junio de 1997, el cuál rige todo lo referente a velocidades de transmisión, control de acceso al medio y seguridad.

El origen de las WLAN se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativos que superaban la velocidad de 1 Mbps, el mínimo establecido por el comité IEEE 802 para que la red sea considerada realmente una LAN, lo que se tradujo en una mayor actividad en la industria y la investigación enfocada al mercado.

Inicialmente, la aceptación de estas redes no era buena debido a ideas erróneas como la creencia de que eran redes inseguras ya que se pensaba que al utilizar el espectro como medio de transmisión, un intruso podía escuchar lo que se transmitía. A esto se le unía la falta de estándares, la baja velocidad de transmisión y el elevado costo de los equipos por lo que era imposible su expansión en el mercado.

La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria: ese respaldo hizo que las WLAN empezaran a dejar ya el laboratorio para iniciar el camino hacia el mercado. Otro de los factores que supuso un gran empuje al desarrollo de este tipo de red fue el asentamiento de Laptops y PDA en el mercado, ya que este tipo de producto portátil reclamaba más la necesidad de una red sin ataduras, sin cables.

Una WLAN utiliza ondas electromagnéticas (radio e infrarrojo) para comunicar, mediante un adaptador, los equipos conectados a la red, en lugar de utilizar cables coaxiales, pares trenzados o de fibra óptica que se utilizan en las LAN convencionales cableadas.

Partiendo del estándar original se han desarrollado otros estándares como son el IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11c, IEEE 802.11h, IEEE 802.11i e IEEE 802.11e entre otros. Igualmente, se encuentran disponibles en el mercado infinidad de productos inalámbricos procedentes de múltiples fabricantes entre los cuáles se destacan Atheros, Airlink 101, Clipsal, D-Link, Intelbras, Netgear, Nortel Networks, Linksys, Planex, CNet, SMC, Sony, TRENDnet, SparkLAN, Toshiba, ZyXEL, entre otros, los cuáles responden a los estándares antes mencionados.

La finalidad de todas las redes inalámbricas es la misma que la de las redes cableadas: permitir la conectividad en red a sus empleados, intercambiar información, acceder a internet, etc. Pero hay algo que diferencia las redes inalámbricas de las redes cableadas y que ha impulsado la tecnología inalámbrica a superar toda reticencia por parte de sus detractores: su sencillez y comodidad para el trabajo, con la seguridad de que sus datos sean siempre seguros y confiables en la mayoría de los casos.

La seguridad en una red WLAN es un aspecto del cual se debe tener una especial relevancia para poder tener la información libre de intrusos y es el mayor problema a resolver en una WLAN.

Debido al hecho de que el SSID se está difundiendo cada pocos segundos es muy simple para un atacante descubrir una red, solo bastaría que estuviese en un lugar próximo donde le llegase la señal y escuchar el medio por unos instantes para detectar en qué canales está operando una WLAN y el nombre de la misma. Es más, en el caso de un ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten una identificación posterior.

Es por ello que una de las primeras medidas tomadas por un fabricante para mejorar la seguridad de la red, fue por parte de Lucent en sus equipos Orinoco WaveLAN, y

consistió en lo que vinieron a llamar Red Cerrada (*Closed Network*). Esta red cerrada consistía simplemente en no anunciar la red mediante la trama de baliza (beacon), o sea, no hacer difusión del SSID.

Hoy en día esta medida es simplemente una dificultad añadida para el atacante, que debe tomar algún esfuerzo adicional para descubrir la red. Existen sniffers en la actualidad como AirSnort o AirTraf que pueden descubrir estas redes sin la menor dificultad.

Conscientes de este problema, el IEEE publicó un mecanismo opcional de seguridad, denominado WEP (*Wired Equivalent Privacy*, privacidad equivalente al cable).

Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN pero rápidamente se volvió vulnerable ya que utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso siendo, desde hace algunos años, relativamente fácil de obtener.

Viendo estos inconvenientes de WEP y para eliminar sus debilidades, el comité 802.11 trabajó intensamente en un nuevo estándar de seguridad, el 802.11i, que fue ratificado en el año 2004. Se centra en cubrir aspectos de seguridad en redes WLAN basadas en los estándares IEEE 802.11 a, b y g. Proporciona una alternativa al mecanismo WEP original disponible para ofrecer seguridad en este tipo de redes, ofreciendo nuevos métodos de cifrado y procedimientos de autenticación. El estándar abarca los protocolos 802.1x (autentificación basada en puertos), TKIP (Protocolo de Claves Integra – Seguras – Temporales), y AES (*Advanced Encryption Standard,* Estándar de Cifrado Avanzado).

La alianza Wifi, acepta a 802.11i y lo implementa en parte en su especificación WPA (*Wi-Fi Protected Access*, acceso protegido Wi-Fi) y totalmente en WPA2.

WPA constituye la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar. Por otro lado, no requiere de actualizaciones de hardware en los equipos.

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación utilizando códigos MIC (Message Integrity Code, código de integridad del mensaje)..

El sistema WPA soluciona la debilidad del vector de inicialización de WEP mediante la inclusión de vectores del doble de longitud y especificando reglas de secuencia que los fabricantes deben implementar.

Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

Para el completamiento de la seguridad de WPA, se incorporó el sistema WPA2, que incluye todas las características definidas en 802.11i como por ejemplo, el nuevo algoritmo de cifrado AES.

Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (*Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol*) en lugar de los códigos MIC.

Ya en el contexto en que se desenvuelve esta investigación, o sea, en la Universidad Pinar de Río, es importante señalar algunas características del campus universitario. En la **Figura 1** se muestra un acercamiento del mismo.

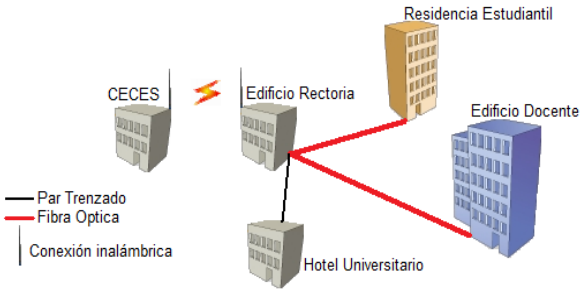


Figura 1: Campus universitario de la UPR.

Como se observa, existe un total de 5 edificaciones, de ellas, 3 son las fundamentales: edificio de rectoría, residencia estudiantil y el edificio docente, conectados entre sí por medio de fibra óptica multimodo a 100Mbps estando el nodo central en el edificio de rectoría. Estas edificaciones son grandes y de una estructura medianamente compleja separados a una distancia entre 100 y 400 metros. El CECES y el Hotel Universitario son instalaciones de menor relevancia que se encuentran conectados, el primero, a través de un enlace inalámbrico direccional y el segundo, por medio de cable UTP cat5.

Con anterioridad a esta investigación se planteó una propuesta de red inalámbrica en cada una de las 3 edificaciones principales que incluye dos AP (Access Point, *Punto de acceso*) en el edificio docente, uno en la residencia estudiantil y uno en en el edificio de rectoría. Esta propuesta no da cobertura a toda el área de la UPR y no se realizaron mediciones de la señal efectivas que permitieran delimitar las áreas en las que se brindaría el mejor servicio y aquellas en que se brindaría un servicio aceptable.

En la actualidad, el 90% de todas las áreas de la UPR forma parte de la red cableada existiendo redes inalámbricas en pequeñas dimensiones allí donde no se ha podido cubrir con ésta, siendo ínfima la cobertura de esta red.

Lo relatado anteriormente, permite identificar el **problema** en cuestión que dio origen a la presente investigación y que queda definido así: No existe en la UPR una red inalámbrica a la que se tenga acceso desde cualquier punto del campus universitario que facilite el acceso a los servicios brindados sobre la red cableada a usuarios móviles autorizados.

El **objeto de estudio** son los sistemas de redes de computadoras y el **campo de acción** los sistemas de redes inalámbricas 802.11.

El **objetivo general** que se persigue es:

Definir una propuesta de red inalámbrica para el edificio docente y la residencia estudiantil de la UPR basada en dos premisas: cobertura total y alta seguridad.

El hecho de limitarse a dos de las principales edificaciones existentes radica en la gran extensión del campus universitario que imposibilita realizar un diseño total en el tiempo requerido para este tipo de investigación pero dejaría las bases creadas para el completamiento del diseño que se persigue.

Los **objetivos específicos** son:

1. Analizar las características, elementos principales y la seguridad del estándar de red inalámbrica 802.11.
2. Realizar los diseños de planta del edificio docente y la residencia estudiantil.
3. Determinar la cobertura de un AP ubicado en puntos específicos mediante la medición de la señal emitida en los puntos que le circundan.
4. Configurar el AP para emplear un esquema de seguridad idóneo según las características de la red de la UPR.

Definiendo la siguiente **hipótesis:** La propuesta planteada permitirá un acceso inalámbrico seguro y de alta velocidad a los servicios de la red UPR, a usuarios autorizados desde cualquier punto del edificio docente y la residencia estudiantil.

El documento se ha dividido en 3 capítulos. El primero aborda los elementos de la tecnología 802.11 enfatizando en los estándares 802.11 b y g, con velocidades máximas de 11 y 54 Mbps respectivamente, por ser estos los de mayor despliegue en la actualidad. En el segundo capítulo se tratan los mecanismos de seguridad empleados en las WLAN 802.11 realizando comparaciones entre ellos. Y por último, en el capítulo 3, se presenta la propuesta de red inalámbrica junto con las mediciones efectuadas.

Capítulo I

ELEMENTOS DE LA TECNOLOGÍA 802.11

CAPITULO I: ELEMENTOS DE LA TECNOLOGÍA 802.11

1.1 Características generales del estándar 802.11.

La versión original del estándar *IEEE 802.11* publicada en 1997 especifica dos velocidades de transmisión teóricas de 1 y 2 Mbps por medio de señales de RF (Radio Frecuencias) en la banda de 2,4 GHz e infrarrojo; esta última sigue siendo parte del estándar, pero no hay implementaciones disponibles.

Utiliza técnicas de modulación de espectro ensanchado (Spread Spectrum) empleando un radiocanal de 5 MHz de ancho de banda antes del proceso de ensanchamiento y de 22 MHz con posterioridad.

Dichas técnicas emplean una baja densidad de potencia, por lo que la señal no interfiere con otros receptores y a su vez incorporan redundancia proporcionando a estos canales resistencia a interferencias y al ruido.

El estándar original también define el protocolo *CSMA/CA* (Carrier Sense Multiple Access with Collision Avoidance, *Acceso múltiple con detección de portadora y evitación de colisiones*) como método de acceso al medio. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en las variantes del estándar definidas posteriormente.

1.2 Evolución de la tecnología IEEE 802.11.

Existen varios estándares que han evolucionado dentro de la tecnología 802.11 como son:

- **Estándar IEEE 802.11a:** Opera en la banda de 5 GHz y utiliza 52 subportadoras OFDM (Orthogonal frequency-division multiplexing,

Multiplexación por división de frecuencias ortogonales) con una velocidad máxima de 54 Mbps, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbps.

- **Estándar IEEE 802.11b:** Tiene una velocidad máxima de transmisión de 11 Mbps y utiliza el mismo método de acceso *CSMA/CA* definido en el estándar original. Este estándar funciona en la banda de 2.4 GHz.
- **Estándar IEEE 802.11c:** Define las características que necesitan los *Access Points (APs)* para actuar como puentes *(bridges).* Actualmente está aprobado y se implementa en algunos productos.
- **Estándar IEEE 802.11d:** Es un complemento del estándar *IEEE 802.11* pensado para permitir el uso internacional de las redes *IEEE 802.11* locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.
- **Estándar IEEE 802.11e:** El objetivo de este estándar es introducir nuevos mecanismos a nivel MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo, *IEEE 802.11e* introduce un nuevo elemento llamado *Hybrid Coordination Function (HCF, Función de coordinación híbrida).*
- **Estándar IEEE 802.11f:** Surgida con el objetivo de lograr la interoperabilidad de puntos de acceso *IEEE 802.11 b/g* dentro de una *WLAN* con puntos de acceso de diferentes fabricantes dentro de la misma red.
- **Estándar IEEE 802.11g:** Es la evolución del estándar *IEEE 802.11b*. El mismo utiliza la banda de 2.4 GHz (al igual que el estándar *IEEE 802.11b*) pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22.0 Mbit/s de velocidad real de transferencia similar a la del estándar *IEEE 802.11a.* Es compatible 802.11b y utiliza las mismas frecuencias.
- **Estándar IEEE 802.11h:** Intenta resolver problemas derivados de la coexistencia de las redes *IEEE 802.11* con sistemas de radares y satélites.
- **Estándar IEEE 802.11i:** Se centra en cubrir aspectos de seguridad en *WLAN* basadas en algunos de los estándares *IEEE 802.11 a, b y g.* Proporciona una alternativa al mecanismo *WEP* original disponible para ofrecer seguridad en

este tipo de redes, ofreciendo nuevos métodos de cifrado y procedimientos de autenticación.

- **Estándar IEEE 802.11j:** Permite adaptarse a la regulación de Japón sobre el modo de operación, la velocidad de transmisión, la potencia radiada y la escucha del medio inalámbrico.
- **Estándar IEEE 802.11k:** Permite a los conmutadores y puntos de acceso inalámbricos calcular y valorar los recursos de radiofrecuencia de los clientes de una red *WLAN*, mejorando así su gestión. Está diseñado para ser implementado en *software*, y para soportarlo, el equipamiento *WLAN* sólo requiere ser actualizado.
- **Estándar IEEE 802.11m:** Constituye un complemento de mantenimiento del estándar *IEEE 802.11* para llevar a cabo correcciones técnicas y aclaraciones sobre los distintos estándares.
- **Estándar IEEE 802.11n:** Puede trabajar en dos bandas de frecuencias: 2.4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Gracias a ello, IEEE 802.11n es compatible con dispositivos basados en todas las ediciones anteriores. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y permite alcanzar un mayor rendimiento.
- **Estándar IEEE 802.11p:** Es una modificación de la capa *MAC* del estándar *IEEE 802.11* para permitir comunicaciones en la banda de 5GHz a velocidades vehiculares en un radio de 300m.
- **Estándar IEEE 802.11r:** Constituye una modificación de la capa *MAC* del estándar *IEEE 802.11* para permitir traspaso rápido de usuarios entre puntos de acceso. El objetivo del estándar es reducir al mínimo el tiempo de traspaso de usuarios evitando fallos en la conexión y pérdidas de paquetes.
- **Estándar IEEE 802.11s:** Es el estándar en desarrollo para redes *Wi-Fi* malladas, también conocidas como redes *Mesh.* El estándar *IEEE 802.11s* pretende responder a la fuerte demanda de infraestructuras *WLAN* móviles con un protocolo para la autoconfiguración de rutas entre puntos de acceso mediante topologías multisalto.

Hasta aquí se han detallado brevemente las distintas especificaciones y modificaciones realizadas al estándar original *IEEE 802.11*, de los cuáles se estudiará dos variantes principales más usadas en las redes WiFi como son el estándar IEEE 802.11b y el IEEE 802.11g en los que se detallará posteriormente.

1.3 Espectro ensanchado.

El espectro ensanchado (también llamado espectro esparcido, espectro disperso, o SS según sus siglas en inglés) es una técnica de modulación empleada en telecomunicaciones para la transmisión de datos, por lo común digitales y por radiofrecuencia.

Se dice que todos los sistemas de espectro ensanchado satisfacen dos criterios:

- El ancho de banda de la señal que se va a transmitir es mucho mayor que el ancho de banda de la señal original.

- El ancho de banda transmitido se determina mediante alguna función independiente del mensaje y conocida por el receptor.

Las técnicas de espectro ensanchado más empleadas son:

- **Espectro ensanchado por secuencia directa (DSSS):**
  La secuencia directa es quizás uno de los sistemas de espectro ensanchado más ampliamente conocido, utilizado y relativamente sencillo de implementar. Una portadora en banda estrecha se modula mediante una secuencia pseudoaleatoria (es decir, una señal periódica que parece ruido pero que no lo es) también llamada secuencia de baker. Para la secuencia directa, el incremento de ensanchado depende de la tasa de bits de la secuencia pseudoaleatoria por bit de información. En el receptor, la información se recupera al multiplicar la señal con una réplica generada localmente de la secuencia de código.

Cuanto mayor sea el patrón de bits (denominados chips, para diferenciarlos de los bits de información) de la secuencia de código, mayor será la resistencia de la señal a las interferencias. El estándar IEEE 802.11 recomienda un tamaño de 11 chips, pero el óptimo es de 100, diseñada para que aparezca aproximadamente la misma cantidad de 1 que de 0. Un ejemplo de esta secuencia es el siguiente. {+1-1+1+1-1+1+1+1-1-1-1} (el valor -1 se corresponde con 0) que es la usada por 802.11. Al sustituir cada bit de datos a transmitir, por una secuencia de 11 bits equivalente, aunque parte de la señal de transmisión se vea afectada por interferencias, el receptor aún puede reconstruir fácilmente la información a partir de la señal recibida. DSSS es usado en el estándar 802.11 y 802.11b.

- **Espectro ensanchado por salto de frecuencia (FHSS):**
  En los sistemas de salto de frecuencia, la frecuencia portadora del transmisor cambia (o salta) abruptamente de acuerdo con una secuencia pseudoaleatoria. El orden de las frecuencias seleccionadas por el transmisor viene dictado por la secuencia de código. El receptor rastrea estos cambios y produce una señal de frecuencia intermedia constante. Fue definida solamente en el estándar 802.11 original.

En la **Figura 1.1** se muestra la forma de onda ensanchada de una señal transmitida.

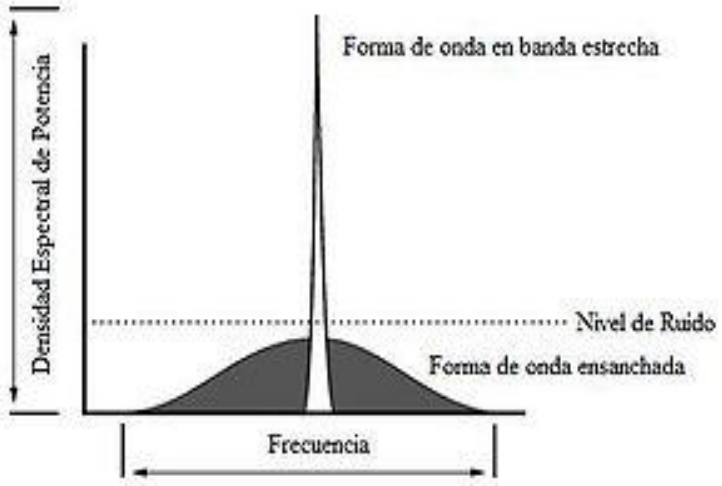


Figura 1.1 Forma de onda ensanchada.

1.3.1 Ventajas y desventajas.

El espectro ensanchado tiene muchas propiedades únicas y diferentes que no se pueden encontrar en ninguna otra técnica de modulación. Para verlo mejor, se listan debajo algunas ventajas y desventajas que existen en los sistemas típicos de espectro ensanchado.

Ventajas:

- Resiste todo tipo de interferencias, tanto las no intencionadas como las malintencionadas (más conocidas con el nombre de jamming), siendo más efectivo con las de banda estrecha.
- Tiene la habilidad de eliminar o aliviar el efecto de las interferencias multitrayecto.
- Se puede compartir la misma banda de frecuencia con otros usuarios.
- Confidencialidad de la información transmitida gracias a los códigos pseudoaleatorios (multiplexación por división de código).

Desventajas.

- Ineficiencia del ancho de banda.
- La implementación de los circuitos es en algunos casos muy compleja.

1.4 El espectro de frecuencias en la banda de 2.4 GHz.

Elegir el espectro de frecuencia inalámbrica ideal es realmente importante cuando tenga que diseñar sus enlaces inalámbricos. Una mala elección puede alterar los atributos y capacidades de su red. Cada espectro posee ventajas y desventajas, pero al ir conociéndolas se podrá determinar mejor donde implementar determinado equipamiento en una solución inalámbrica.

1.4.1 Características de las frecuencias utilizadas en redes inalámbricas.

Las señales de RF pueden verse afectadas por elementos externos, ya sea paredes, árboles, lluvia, etc., en mayor o menos medida de acuerdo al valor de la frecuencia

portadora. Así, cuando la frecuencia se incrementa, la señal se vuelve más fácil de atenuar (no puede viajar tan fácil a través de obstáculos como copas de árboles, muros, etc.) pero es capaz de transmitir mayor ancho de banda. En caso contrario, cuando la frecuencia disminuye, se hace más efectiva la transmisión en presencia de obstáculos pero disminuye el ancho de banda.

Las bandas de frecuencias más bajas (900 MHz, 2.4GHz), están mucho más congestionadas, con más "tráfico" inalámbrico que las de frecuencia alta como la banda de 5GHz.

En la siguiente tabla se muestra un esquema de comparación de las bandas de frecuencias usadas en enlaces inalámbricos.

	900 MHz	2.4 GHz	5 GHz
Popularidad	No usadas ampliamente en redes	Ampliamente Usadas	Volviéndose ampliamente usadas
Velocidad	Bajo Throughput	Alto Throughput	Alto Throughput
Costo	No caro	No caro	No caro
Frecuencia	Abarrotado, Buen uso Nlos (Non line of sigth)	Abarrotado	No abarrotado
Alcance	Alcance débil	Alcance promedio	Alcance promedio
Aplicación	Mesh (Malla), ptmp (punto multipunto) cortos con muchos obstáculos	Mesh, ptp (punto a punto), ptmp	ptp, ptmp

Tabla 1.1 Esquema de comparación de las bandas de frecuencias de 900 MHz, 2.4GHz y 5 GHz.

Como se ha relatado con anterioridad, 802.11, 802.11b y 802.11g utilizan la banda de 2.4 GHz y 802.11a la banda de 5 GHz.

1.4.2 Distribución del espectro en la banda de 2.4 GHz.

El espectro en la banda de 2.4 GHz utilizado por las WLAN 802.11 se extiende desde 2.412 a 2.472 GHz y es dividido en un total de 13 canales con un ancho de banda de

5 MHz cada uno. El número de canales puede variar según la legislación de cada país. En la **Tabla 1.2** se muestran estos canales y sus frecuencias centrales.

Para cada canal es necesario un ancho de banda de unos 22 MHz para poder transmitir la información debido al proceso de ensanchamiento del espectro, por lo que se produce un inevitable solapamiento de los canales próximos haciéndose necesario una planificación de frecuencia efectiva en aras de disminuir la interferencia entre canales.

No. de canal	Frecuencia	No. de canal	Frecuencia
1	2.412 GHz	8	2.447 GHz
2	2.417 GHz	9	2.452 GHz
3	2.422 GHz	10	2.457 GHz
4	2.427 GHz	11	2.462 GHz
5	2.432 GHz	12	2.467 GHz
6	2.437 GHz	13	2.472 GHz
7	2.442 GHz		

Tabla 1.2 Subdivisión del espectro en canales de 5 MHz en la banda de 2.4 GHz.

1.4.3 Planificación de frecuencia en la banda de 2.4 GHz.

La planificación de frecuencias es la parte del diseño de WLANs 802.11 encargada de determinar el canal que usará cada AP de la red. Para ello se debe tener en cuenta primero, los canales usados por redes vecinas, y segundo, la separación óptima que deben tener los canales de APs adyacentes para evitar la interferencia por solapamiento; esta separación debe ser de al menos 5 canales (25 MHz) mayor que el ancho de banda de 22 MHz de cada canal después del proceso de ensanchamiento.

En una red 802.11 de un único AP o de hasta dos AP la selección de los canales no representa un problema, pero en una red de 3 o más AP la selección podría tornarse

difícil dependiendo de la estructura en concreto; son típicas las configuraciones utilizando los canales 1-6-11, 2-7-12 y por último, 3-8-13.

La **Figura 1.2** y **1.3** dan una idea gráfica de esto último, para el caso de solo 11 canales disponibles. Se muestra cómo no hay solapamiento entre los canales 1, 6 y 11.

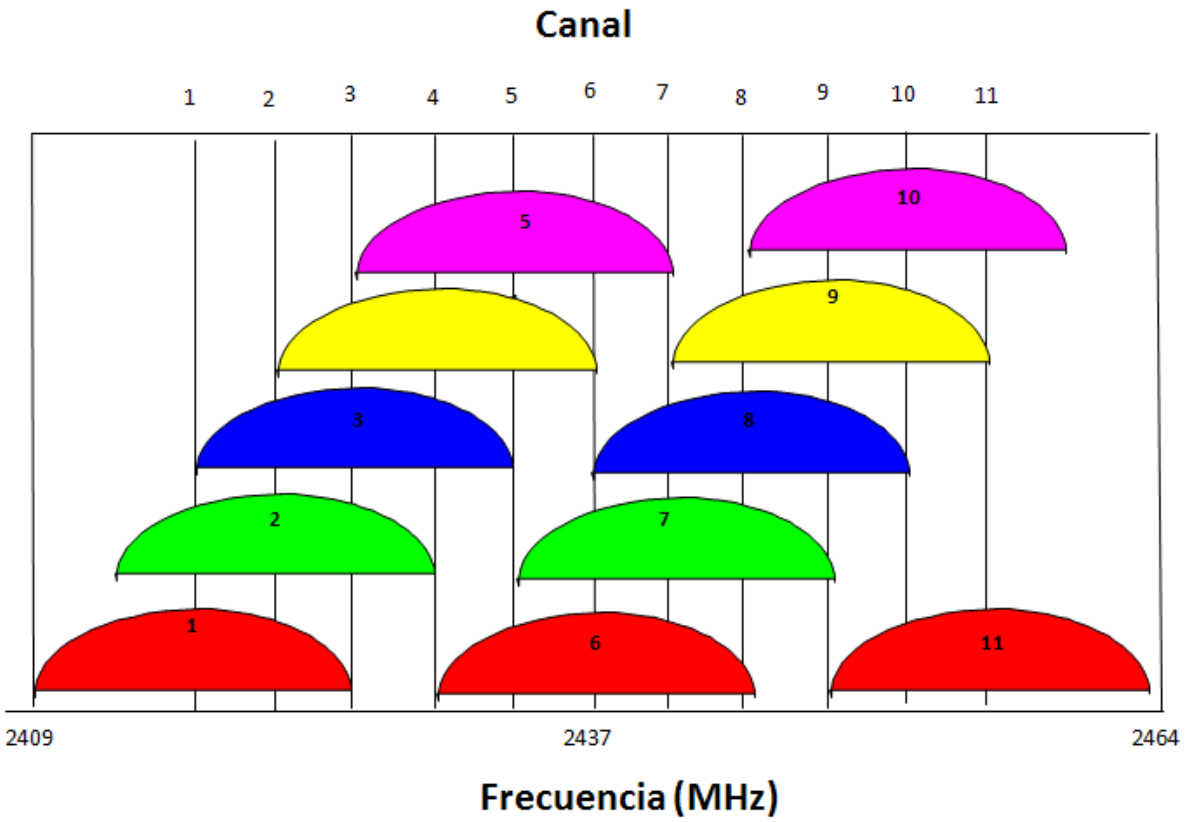


Figura 1.2 Canales 802.11 después del proceso de ensanchamiento.

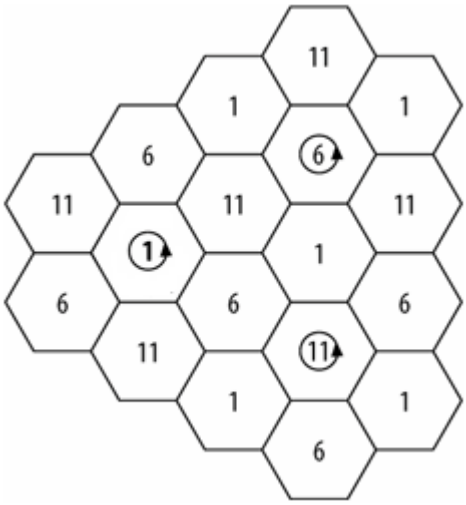


Figura 1.3 Planificación de frecuencia usando los canales 1, 6 y 11.

1.5 Multiplexación por División de Frecuencias Ortogonales OFDM.

La Multiplexación por División de Frecuencias Ortogonales, es una multiplexación que consiste en enviar un conjunto de ondas portadoras de diferentes frecuencias, donde cada una transporta información, la cual es modulada en QAM o en PSK.

Normalmente se realiza la multiplexación **OFDM** tras pasar la señal por un codificador de canal con el objetivo de corregir los errores producidos en la transmisión, entonces esta multiplexación se denomina **COFDM**, del inglés *Coded OFDM*.

Debido al problema técnico que supone la generación y la detección en tiempo continuo de los cientos, o incluso miles, de portadoras equiespaciadas que forma OFDM, los procesos de multiplexación y demultiplexación se realizan en tiempo discreto mediante la IDFT (Tranformada Discreta de Fourier Inversa) y la DFT (Tranformada Discreta de Fourier) respectivamente. OFDM es usada en el estándar 802.11g sobre la banda de 2.4 GHz.

1.5.1 Características de la modulación OFDM.

La multiplexación de portadoras OFDM es muy robusta frente al multitrayecto que es muy habitual en los canales de RF, frente a las atenuaciones selectivas en frecuencia y frente a las interferencias de RF.

Debido a las características de esta multiplexación, es capaz de recuperar la información de entre las distintas señales con distintos retardos y amplitudes (*fading*) que llegan al receptor, por lo que existe la posibilidad de crear redes de frecuencia única sin que existan problemas de interferencia.

Si se compara con las técnicas de banda ancha como CDMA, OFDM genera una alta tasa de transmisión al dividir el flujo de datos en muchos canales paralelos o subportadoras que se transmiten en igual número de portadoras de banda estrecha y con tiempos de símbolo (uno o varios bits) mayores al caso de usar banda ancha donde para lograr la misma tasa de transmisión los tiempos de símbolo son más cortos.

Los canales de banda estrecha de OFDM son ortogonales entre sí, lo que evita el uso de bandas de guardas y así proporciona un uso eficiente del espectro. Ya que los desvanecimientos (fading) afectan selectivamente a uno o un grupo de canales, es relativamente simple ecualizarlos en forma individual lo que también se contrapone a la ecualización de un sistema de banda ancha.

En la **Figura 1.4** se muestra un ejemplo de modulación OFDM.

OFDM además es una tecnología de modulación digital, una forma especial de modulación multi-carrier considerada la piedra angular de la próxima generación de productos y servicios de radio frecuencia de alta velocidad para uso tanto personal como corporativo. La técnica de espectro disperso de OFDM distribuye los datos en un gran número de portadoras que están espaciados entre sí en distintas frecuencias precisas. Ese espaciado evita que los demoduladores vean frecuencias distintas a las suyas propias.

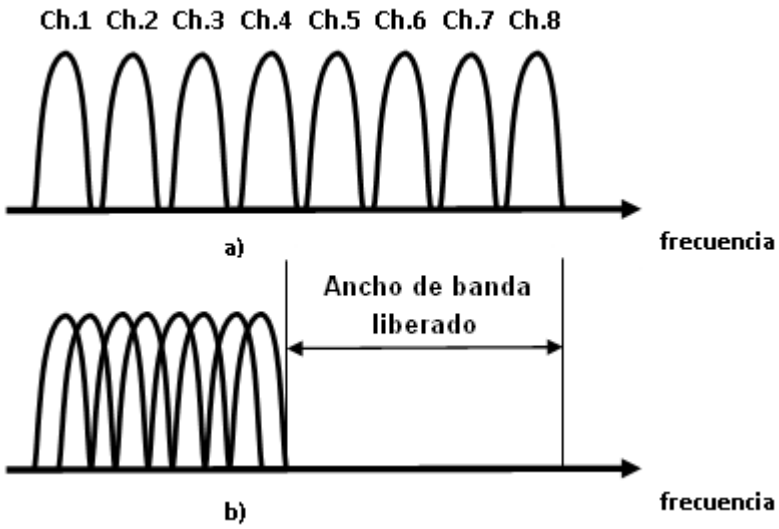


Figura 1.4 Modulación OFDM. a) Técnica multiportadora convencional. b) Modulación con portadoras ortogonales.

1.6 Descripción del estándar 802.11.

La versión inicial del estándar 802.11 en 1997 describe 2 capas físicas diferentes definidas como DSSS PHY, FHSS PHY en la banda sin licencia de 2.4 GHz. Las velocidades alcanzadas son de 1 y 2 Mbps para las dos técnicas de modulación por espectro ensanchado utilizadas pero los fabricantes prefirieron optar por DSSS por su potencial de alcanzar velocidades superiores.

Emplear una banda sin regulación como la de 2.4 GHz presupone la ocurrencia de interferencias con otros dispositivos o utensilios como hornos microondas, teléfonos móviles y otros aparatos que funcionen en la misma frecuencia. Sin embargo, si las instalaciones 802.11b están a una distancia razonable de otros elementos, estas interferencias son fácilmente evitables. Además, los fabricantes prefieren bajar el costo de sus productos, aunque esto suponga utilizar una banda sin regulación.

A continuación se resumen las ventajas y desventajas de 802.11.

- ✓ **Ventajas:** Bajo costo, rango de señal muy bueno y difícil de obstruir.

- ✓ **Desventajas:** Baja velocidad máxima, soporte de un número bajo de usuarios a la vez y produce interferencias en la banda de 2.4 GHz.

La modulación utilizada para la transmisión de los chips correspondientes a cada palabra de código es DBPSK (Differential Binary Phase Shift Keying, *modulación por cambio de fase binaria diferencial*) para el caso de 1 Mbps y DQPSK (Differential Quadrature Phase Shift Keying, *modulación por cambio de fase diferencial en cuadratura*) para 2 Mbps.

A continuación se dan los detalles de cómo es que se obtienen las distintas velocidades de datos:

1. Primeramente hay que saber que la velocidad de transmisión de los símbolos (codifican a los chips según la utilización de DBPSK o DQPSK) es común en todas las variantes y tiene un valor de 11 MBaud.
2. Con DBPSK se tienen solamente dos símbolos (0 y 1) por lo que cada uno representa a un chip de la palabra de código a transmitir y la velocidad de chips sería 11 Mcps.
3. Como la palabra (word) de código contiene 11 chips entonces la velocidad de transmisión de palabras sería de 1 Mwps.
4. Por último, y teniendo en cuenta que siempre la palabra de código codifica a un bit de información, se obtiene la velocidad de transmisión de datos de 1 Mbps.
5. Para el caso de DQPSK se tienen 4 símbolos (00, 01, 10 y 11) representando cada uno a dos chips. En tal caso la velocidad de chips sería 22 Mcps y la velocidad de palabras de 2 Mwps que es equivalente a la velocidad de bits de información resultante de 2 Mbps.

La **Tabla 1.3** muestra un resumen de las características de 802.11.

802.11	
Banda de Frecuencia	2.4GHz
Velocidad de datos	1Mbps, 2Mbps
Medidas de seguridad	WEP, WPA, WPA2 en combinación con DSSS.
Rango de Operación óptima	50 metros en interior, 100 metros en exterior.
Modulación empleada	DSSS con DBPSK y DQPSK

Tabla 1.3 Características del estándar 802.11.

1.7 Descripción del estándar 802.11b

Inmediatamente después de aprobarse el estándar 802.11, el comité 802.11 se puso en función de aumentar la velocidad de transmisión pues 2 Mbps como velocidad máxima no resultaba nada llamativo y en julio de 1999, la IEEE expande el 802.11 creando la especificación 802.11b, la cual soporta velocidades de 5,5 y 11 Mbps, comparable a la Ethernet de 10 Mbps, manteniendo la compatibilidad con 802.11 al utilizar la misma banda de frecuencia de 2.4 GHz y DSSS.

DQPSK requiere que el receptor distinga entre 4 diferencias de fases. Aumentar estas diferencias de fases entre símbolos para lograr mayores velocidades no es una solución viable puesto que la detección de fases menores es más difícil en presencia de interferencia por multitrayecto y requiere una electrónica más compleja.

En su lugar, el comité 802.11 optó por un método de codificación alternativo denominado CCK (Complementary Code Keying) manteniendo la modulación DQPSK. CCK divide el flujo de chips en una serie de símbolos de código de 8 chips, que usando métodos matemáticos complejos pueden codificar 4 u 8 bits de datos para lograr

velocidades de 5.5 u 11 Mbps respectivamente.

A diferencia de 802.11, la palabra de código de 11 chips no es estática siendo derivada parcialmente de los datos.

Para diferenciar la técnica DSSS de su predecesora se determinó llamarla HR/DSSS (High Rate DSSS) por la mayor velocidad alcanzada.

En la **Tabla 1.4** se muestra un resumen de las características de 802.11b.

802.11b	
Banda de Frecuencia	2.4GHz
Velocidad de datos	1Mbps, 2Mbps, 5,5Mbps y 11Mbps
Medidas de seguridad	WEP, WPA, WPA2 en combinación con HR/DSSS.
Rango de Operación óptima	50 metros en interior, 100 metros en exterior.
Modulación empleada	HR/DSSS, CCK (Complementary code keying), DQPSK.

Tabla 1.4 Características del estándar 802.11b.

1.8 Descripción del estándar 802.11g.

El 2002 y 2003 ha aparecido un nuevo estándar denominado 802.11g. Este nuevo estándar intenta aprovechar lo bueno de cada uno de los anteriores 802.11a y 802.11b. La 802.11g permite velocidades de hasta 54 Mbit/s y utiliza la banda de frecuencia de 2.4 GHz. Además, al trabajar en la misma banda de frecuencia, la 802.11g es compatible con la 802.11b, por lo que puntos de acceso 802.11g pueden trabajar en redes 802.11b y viceversa.

Algunas ventajas y desventajas se pueden resumir a continuación:

- ✓ **Ventajas:** Velocidad máxima alta, soporte de muchos usuarios a la vez, rango de señal muy bueno y difícil de obstruir.
- ✓ **Desventajas:** Alto costo y produce interferencias en la banda de 2.4 GHz.

La capa física en 802.11g pasó a llamarse **ERP** (Extended Rate PHY, *Capa* física de velocidad extendida) aunque en realidad 802.11g se compone de varias especificaciones de capa física en una. Pero hay una de ellas que es la más extendida, ERP-OFDM que soporta las velocidades de 6, 9, 12, 18, 24, 36, 48, y 54 Mbps.

En la **Tabla 1.5** se muestra un resumen de las características de 802.11g.

802.11g	
Banda de Frecuencia	2.4GHz
Velocidad de datos	6, 9, 12, 18, 24, 36, 48, y 54 Mbps
Medidas de seguridad	WEP, WPA, WPA2
Rango de Operación óptima	50 metros dentro, 100 metros afuera
Modulación empleada	ERP-OFDM

Tabla 1.5 Características del estándar 802.11g

1.9 Acceso al medio en 802.11, CSMA/CA.

Las redes 802.11, ya sean bajo el estándar original o sus sucesores, utilizan CSMA/CA como protocolo de acceso al medio en el nivel de enlace. Es un protocolo de control de redes de bajo nivel que permite que múltiples estaciones utilicen un mismo medio de transmisión. Cada equipo anuncia opcionalmente su intención de transmitir antes de hacerlo para evitar colisiones entre los paquetes de datos (comúnmente en redes inalámbricas, ya que estas no cuentan con un modo práctico

para transmitir y recibir simultáneamente). De esta forma, el resto de equipos de la red sabrán cuando hay colisiones y en lugar de transmitir la trama en cuanto el medio está libre, se espera un tiempo aleatorio adicional corto y solamente si, tras ese corto intervalo el medio sigue libre, se procede a la transmisión reduciendo la probabilidad de colisiones en el canal. CSMA/CA es utilizada en canales en los que por su naturaleza no se puede usar CSMA/CD.

Aunque CSMA/CD y CSMA/CA aseguren que un nodo va a obtener un acceso al medio no se asegura que el nodo destino esté en contacto con el nodo origen. Para solucionar este problema se ha añadido un procedimiento de saludo adicional al protocolo de la capa MAC. Este procedimiento se ha denominado protocolo de MAC inalámbrico de fundamento distribuido (DFW MAC) con el fin de que sirva para los diferentes métodos de la capa MAC.

Para enviar una trama, el equipo origen primero envía una trama corta de control de solicitud de transmisión RTS (Request To Send) mediante el método CSMA/CA. Este mensaje de control RTS contiene las direcciones de MAC del equipo origen y destino. Si el equipo destino recibe esta trama significa que está preparado para recibir una trama. Este equipo devolverá una trama de contestación: preparado para transmitir CTS (Clear To Send) o receptor ocupado (RxBUSY). Si la respuesta es afirmativa el equipo origen transmite la trama en espera (DATA). Si el equipo destino recibe correctamente el mensaje contesta con la trama de confirmación positiva ACK (ACKnowledged) y si no la recibe correctamente contesta con la trama de confirmación negativa NAK (NAKnowledged) y el equipo origen tratará de volver a enviarlo. Este procedimiento se repite un número predefinido de veces hasta conseguirse una transmisión correcta de la trama DATA.

A continuación se muestra un esquema general de este procedimiento (**Figura 1.5**).

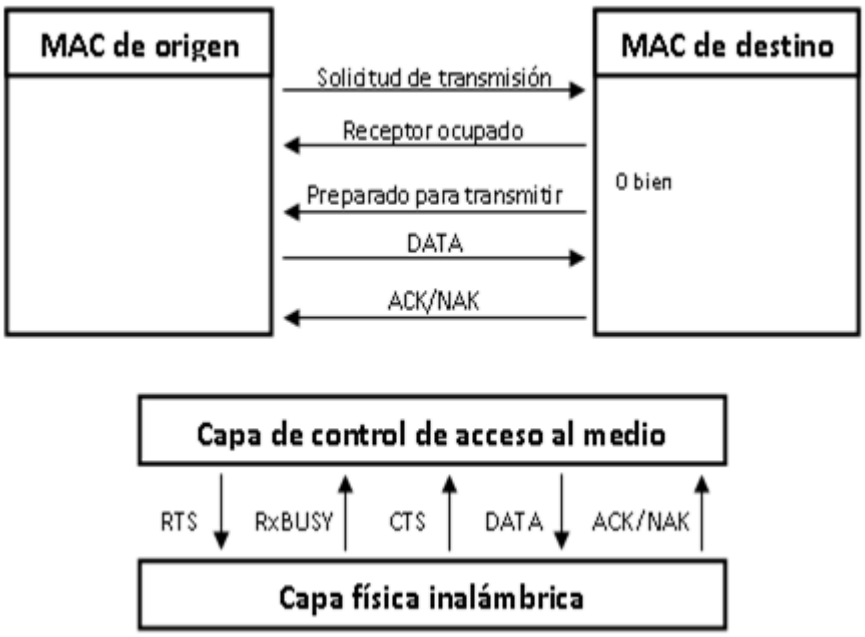


Figura 1.5 Esquema general del mecanismo CSMA/CA.

1.10 Topologías posibles en una red Wifi.

La topología de red es la disposición física en la que se conecta una red de ordenadores. Si una red tiene diversas topologías se le llama mixta.

En las redes *WLAN,* las topologías más usadas son el Modo *Ad-Hoc*, y el Modo Infraestructura.

El modo *ad-hoc* se utiliza para conectar clientes inalámbricos directamente entre sí, sin necesidad de un punto de acceso inalámbrico o una conexión a una red con cables existente. Una red *ad-hoc* consta de un máximo de 9 clientes inalámbricos, que se envían los datos directamente entre sí, y de esta manera el área de cobertura está limitada por el alcance de cada estación individual. En la figura siguiente se muestra una red inalámbrica en modo *ad-hoc* (**Figura 1.6**).

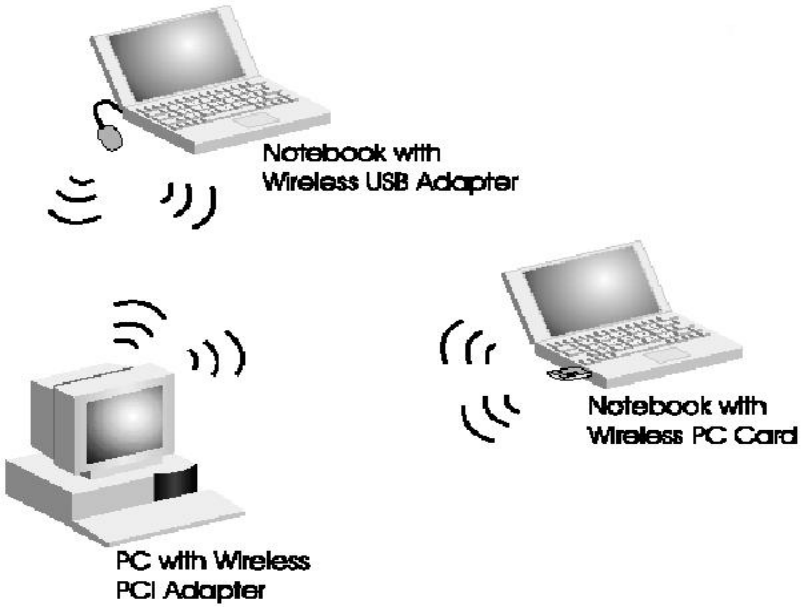


Figura 1.6 Topología ad-hoc.

En el modo infraestructura (**Figura 1.7**), los ordenadores provistos de una tarjeta de red inalámbrica se comunican con el AP que conecta entre sí una red inalámbrica y una red cableada. Además, el *AP* controla el tráfico ya que dirige los datos de la red y aumenta el alcance de la red inalámbrica puesto que ahora la distancia máxima no es entre estaciones sino entre cada estación y el punto de acceso.

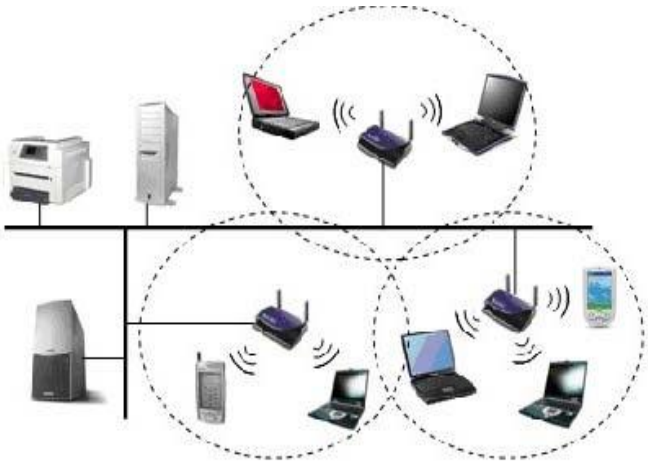


Figura 1.7 Topología en modo infraestructura.

Capítulo II

MECANISMOS DE SEGURIDAD EN REDES WIFI

CAPÍTULO II: MECANISMOS DE SEGURIDAD EN REDES WIFI.

La seguridad es un aspecto que cobra especial relevancia cuando hablamos de redes inalámbricas. Las ondas de radio se propagan por todas partes, es por esto, que es vital comprender la importancia de la encriptación de datos para así poder traficar información de forma segura.

La seguridad en las redes *IEEE 802.11* consta básicamente de cifrado y autenticación. El cifrado se utiliza para cifrar o codificar los datos de las tramas inalámbricas antes de que se envíen a la red inalámbrica. Con la autenticación se requiere que los clientes inalámbricos se identifiquen antes de que se les permita unirse a la red inalámbrica. A continuación se explica cómo funcionan los algoritmos WEP, WPA y WPA2 (IEEE 802.11i) y cuáles son sus fortalezas y debilidades.

2.1 Cifrado WEP.

WEP es un sistema que forma parte del estándar 802.11 desde sus orígenes. Es el sistema más simple de cifrado y lo admiten la totalidad de los adaptadores inalámbricos. El cifrado WEP se realiza en la capa MAC del adaptador de red inalámbrico o en el punto de acceso, utilizando claves compartidas de 64 ó 128 bits. Cada clave consta de dos partes, una de las cuales la tiene que configurar el usuario/administrador en cada uno de los adaptadores o puntos de acceso de la red. La otra parte se genera automáticamente y se denomina vector de inicialización (IV). El objetivo del vector de inicialización es obtener claves distintas para cada trama. Ahora se describirá el funcionamiento del cifrado WEP.

Cuando se tiene activo el cifrado WEP en cualquier dispositivo inalámbrico, bien sea una adaptador de red o un punto de acceso, se está forzando a que el emisor cifre los datos y el CRC de la trama 802.11 que el receptor recogerá y descifrará. El cifrado se lleva a cabo partiendo de la clave compartida entre dispositivos que, como

fue indicado con anterioridad, previamente se ha tenido que configurar en cada una de las estaciones. En realidad un sistema WEP almacena cuatro contraseñas y mediante un índice se indica cual de ellas será utilizada en las comunicaciones.

El proceso de cifrado WEP agrega un vector de inicialización (IV) aleatorio de 24 bits concatenándolo con la clave compartida para generar la llave de cifrado. Observamos cómo al configurar WEP hay que introducir un valor de 40 bits (cinco dígitos hexadecimales), que junto con los 24 bits del IV obtenemos la clave de 64 bits. El vector de inicialización podría cambiar en cada trama trasmitida. WEP usa la llave de cifrado para generar la salida de datos que serán, los datos cifrados más 32 bits para la comprobación de la integridad, denominada ICV (integrity check value). El valor ICV se utiliza en la estación receptora donde se recalcula y se compara con el del emisor para comprobar si ha habido alguna modificación y tomar una decisión, que puede ser rechazar el paquete.

Para cifrar los datos WEP utiliza el algoritmo RC4, que básicamente consiste en generar un flujo de bits a partir de la clave generada, que utiliza como semilla, y realizar una operación XOR entre este flujo de bits y los datos que tiene que cifrar. El valor IV garantiza que el flujo de bits no sea siempre el mismo. WEP incluye el IV en la parte no cifrada de la trama, lo que aumenta la inseguridad. La estación receptora utiliza este IV con la clave compartida para descifrar la parte cifrada de la trama.

Lo más habitual es utilizar IV diferentes para transmitir cada trama aunque esto no es un requisito de 801.11. El cambio del valor IV mejora la seguridad del cifrado WEP dificultando que se pueda averiguar la contraseña capturando tramas, aunque a pesar de todo sigue siendo inseguro.

2.1.1 Debilidades de WEP.

Las debilidades de WEP se basan en que, por un lado, las claves permanecen estáticas y por otro lado los 24 bits de IV son insuficientes y se transmiten sin cifrar. Aunque el algoritmo RC4 no esté considerado de los más seguros, en este caso la debilidad de WEP no es culpa de RC4, sino de su propio diseño.

Si se tiene un vector de inicialización de 24 bits existen 2^24 posibles IV distintos y no es difícil encontrar distintos paquetes generados con el mismo IV. Si la red tiene bastante tráfico estas repeticiones se dan con cierta frecuencia. Un atacante puede recopilar suficientes paquetes similares cifrados con el mismo IV y utilizarlos para determinar el valor del flujo de bits y de la clave compartida. El valor del IV se transmite sin cifrar por lo que es público. Esto puede parecer muy complicado, pero hay programas que lo hacen automáticamente y en horas o días averiguan la contraseña compartida. No olvidar que aunque la red tenga poco tráfico el atacante puede generarlo mediante ciertas aplicaciones.

Una vez que alguien ha conseguido descifrar la contraseña WEP tiene el mismo acceso a la red que si pudiera conectarse a ella mediante cable.

Vista la debilidad real de WEP lo ideal es que se utilizaran claves WEP dinámicas, que cambiaran cada cierto tiempo lo que haría materialmente imposible utilizar este sistema para asaltar una red inalámbrica, pero 802.11 no establece ningún mecanismo que admita el intercambio de claves entre estaciones. En una red puede ser tedioso, simplemente inviable, ir estación por estación cambiando la contraseña y en consecuencia es habitual que no se modifiquen, lo que facilita su descifrado.

Algunos adaptadores sólo admiten cifrado WEP por lo que a pesar de su inseguridad puede ser mejor que nada.

2.2 Cifrado WPA.

La alianza Wi-Fi decidió, en colaboración con el IEEE, tomar aquellas partes del futuro estándar que ya estaba suficientemente maduro y publicar así WPA, hecho que ocurrió en el 2003. WPA es, por tanto, un subconjunto de IEEE 802.11i que se ofrece en los dispositivos actuales.

WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan WPA no vean necesidad de cambiar a IEEE 802.11i, materializado en WPA2.

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

WPA incluye las siguientes tecnologías:

- **IEEE 802.1x:** Estándar del IEEE de 2001 para proporcionar un control de acceso en redes basadas en puertos. El concepto de puerto, en un principio pensado para las tramas de un switch, también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP (*Extensible Authentication Protocol*, protocolo de autenticación extensible) y un servidor AAA (*Authentication Authorization Accounting,* contabilidad de autorización y autenticación) como puede ser RADIUS (Remote Authentication Dial-In User Service). Si la autorización es positiva, entonces el punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros).
- **EAP:** definido en la RFC 2284, es el protocolo de autentificación extensible para llevar a cabo las tareas de autentificación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (*Point-to-Point Protocol*, protocolo de punto a punto), aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1x bajo el nombre de EAPOL (EAP over LAN).
- **TKIP** (Temporal Key Integrity Protocol). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama.
- **MIC** (Message Integrity Code). Código que verifica la integridad de los datos de las tramas.

2.2.1 Mejoras de WPA respecto a WEP.

WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2^48 combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados. El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (replay).

Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC.

Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

Para la autentificación, se sustituye el mecanismo de autentificación de secreto compartido de WEP así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad.

2.2.2 Modos de funcionamiento de WPA.

WPA puede funcionar en dos modos:

- **Con servidor AAA, RADIUS normalmente.** Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.
- **Con clave inicial compartida** (PSK, Pre-Shared Key). Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y

punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

2.3 Cifrado WPA2.

WPA2 es una certificación de producto que otorga Wi-Fi Alliance y certifica que los equipos inalámbricos son compatibles con el estándar IEEE 802.11i. WPA2 admite las características de seguridad obligatorias adicionales del estándar 802.11i que no están incluidos para productos que admitan WPA.

WPA2 incluye el nuevo algoritmo de cifrado AES (Advanced Encryption Standard), desarrollado por el NIS (Network Information Service**)**. Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requerirá un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.

Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol) en lugar de los códigos MIC.

Capítulo III

PROPUESTA DE RED INALÁMBRICA

CAPITULO III: PROPUESTA DE RED INALÁMBRICA

El diseño de una red inalámbrica presupone ante todo conocimiento de la tecnología para posteriormente centrarse en los aspectos prácticos de la misma como la ubicación efectiva de un AP y cantidad de estos para cubrir el área deseada. Obviamente, el diseñador tiene que tener a mano las herramientas y dispositivos que le permitan llegar a un diseño veraz que cumpla con las expectativas de los clientes y de él mismo.

3.1 Dispositivos y herramientas usadas.

Durante la investigación realizada se contó con 3 APs de diferentes marcas WRT54G de Linksys, marca registrada de Cisco Systems, el DIR 600 de D-Link y el CWR-854V de CNet. Los 3 APs tienen características similares siendo todos routers inalámbricos, lo que significa que el AP que los miembros de la red inalámbrica pueden pertenecer a una subred IP diferente a la de los miembros de la red cableada mejorando la gestión de la red en redes grandes. A pesar de esta potencialidad de los APs, el diseño que se propone no presupone el uso del AP como ruteador, primero, y como se verá más adelante, por la gran cantidad de APs necesarios, y segundo, para lograr la movilidad de los usuarios móviles en todo el recinto manteniendo las comunicaciones activas, hecho este que no ocurre si las distintas redes inalámbricas pertenecen a subredes IP diferentes.

En las **Figuras 3.1** y **3.2** se muestra una vista posterior y frontal del AP WRT54G de Linksys respectivamente.

Figura 3.1 Panel posterior del ruteador WRT54G.

Botón Reset (Reinicio): Para restablecer los parámetros predeterminados de fábrica del ruteador.

Internet: En el puerto Internet se conecta la conexión a Internet de banda ancha o simplemente se conecta a cualquier switch de la red Ethernet cuando se utilice como ruteador.

Puertos Ethernet 1, 2, 3, 4: Estos puertos (1, 2, 3, 4) conectan el ruteador a los PC en red y a otros dispositivos de la red Ethernet. Pertenecen a la misma subred IP que la red inalámbrica.

Figura 3.2 Panel frontal del ruteador WRT54G

En el panel frontal del ruteador aparecen los leds indicadores de encendido, WLAN habilitada y puertos ethernet 1, 2, 3 y 4 con dispositivos conectados.

La gestión de los puntos de acceso se realiza mediante un sitio web que incorporan. Para ello deberán tener una dirección IP accesible desde la red cableada que de forma predeterminada el fabricante la informa ya sea plasmándola al fondo del dispositivo o si no, anunciándola en el manual de usuario; en el caso del ruteador WRT54G es 192.168.1.1, y la máscara 255.255.255.0. En ese caso, se conecta una PC a un puerto ethernet del ruteador que deberá tener una IP que pertenezca a la misma subred del AP, por ejemplo, 192.168.1.1. De otro modo es imposible la conexión al AP para su gestión. Una vez que se acceda a la interfaz Web de configuración se puede cambiar la IP predeterminada del AP.

Para la realización de las mediciones efectuadas solo hay que configurar el AP para que trabaje en un canal RF sin uso, pudiendo quedar la red abierta (sin seguridad).

El otro dispositivo usado fue una PC portátil que con el uso del software CommView for Wifi permite medir el nivel de la señal emitida por el AP en toda el área cubierta por este.

CommView for Wifi está diseñado para capturar y analizar paquetes en redes inalámbricas 802.11a/b/g/n además de identificar las redes inalámbricas existentes en el área de cobertura de la PC en que se encuentra instalado.

En la **Figura 3.3** se muestra la ventana “Scanner” (búsqueda) de este software que permite hacer una búsqueda de todos los AP y dispositivos 802.11 presentes mostrando entre otros datos si es un AP, si usa WEP/WPA, el SSID, el nivel de señal, la dirección MAC y la dirección IP, agrupándolos en la parte izquierda de la ventana por el canal que usan.

Por otra parte, en la **Figura 3.4,** se observan las opciones de búsqueda de esta utilidad donde el usuario puede seleccionar, por ejemplo, los canales que se explorarán.

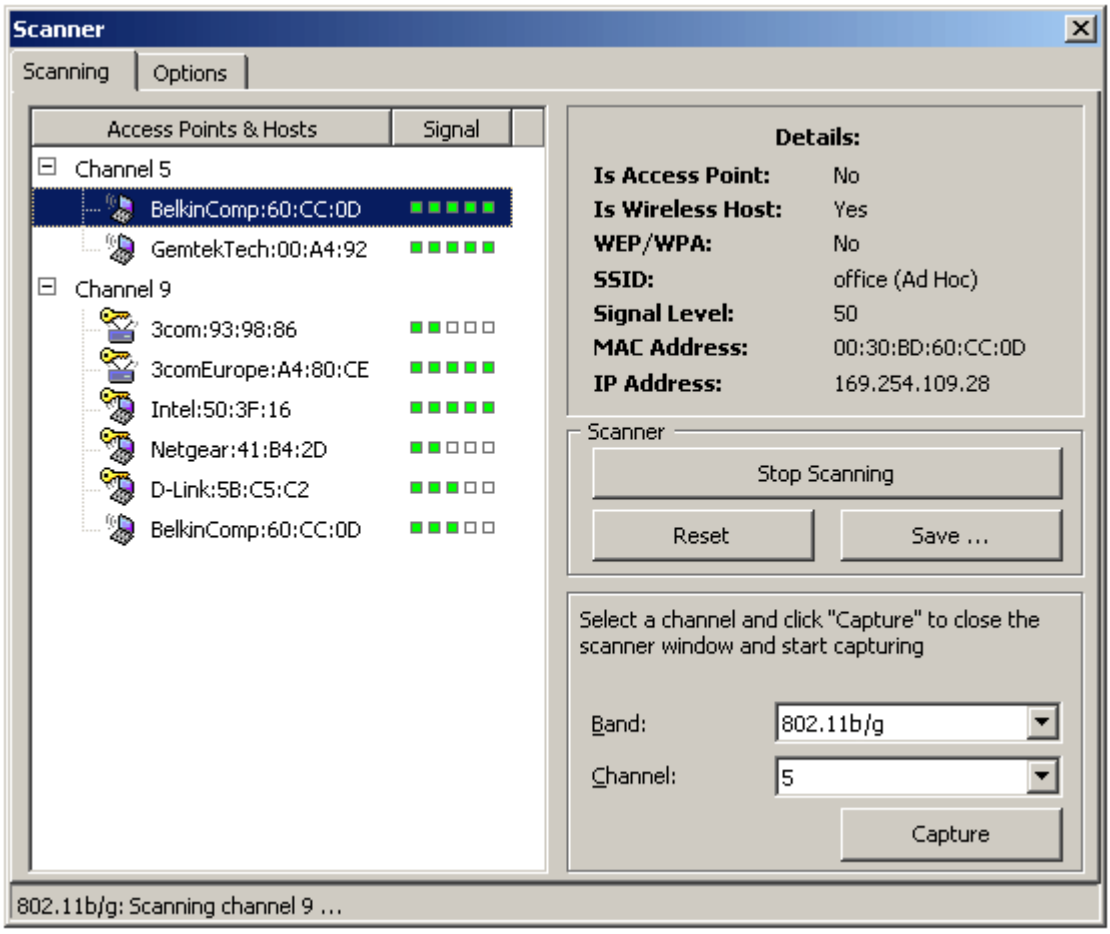


Figura 3.3 Vista de la ventana de búsqueda del CommView for Wifi.

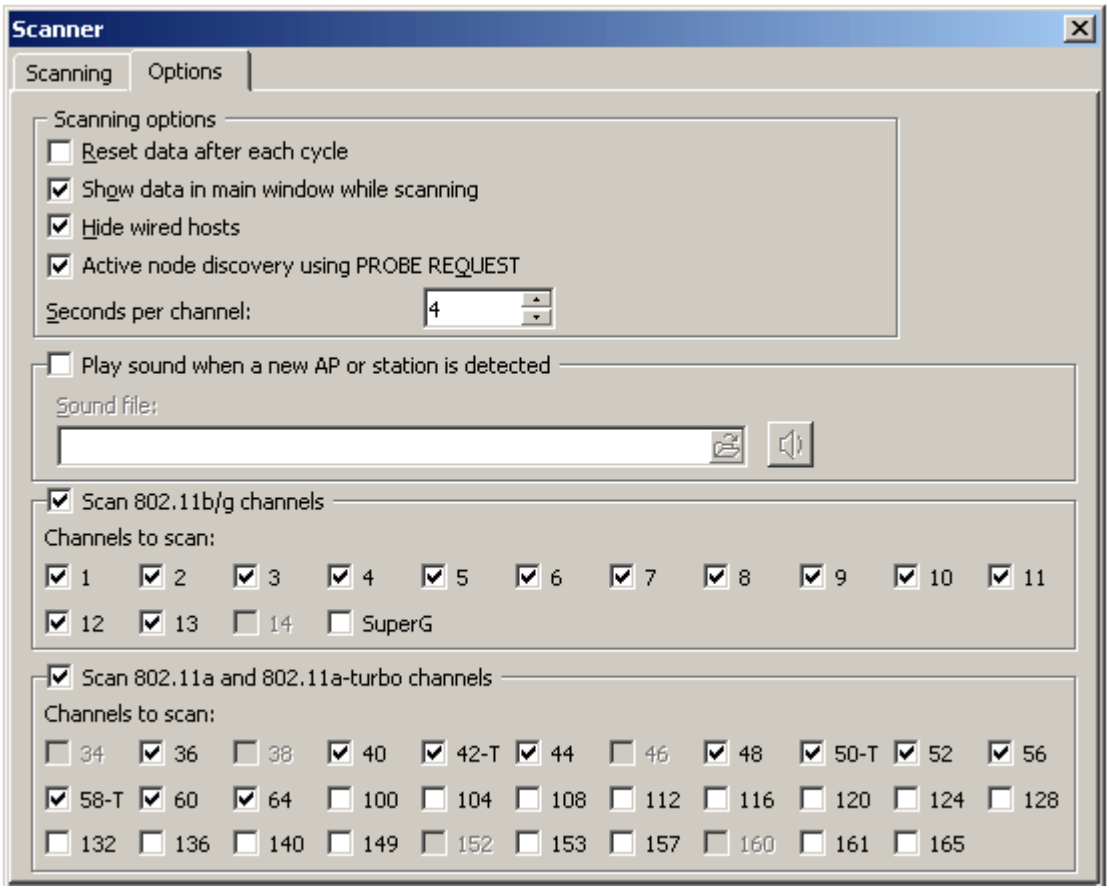


Figura 3.4 Ventana de opciones de búsqueda del CommView for Wifi.

Fue usado también el Autocad 2008 como herramienta para diseñar la planta de cada edificación prevista, en este caso, el edificio docente y la residencia estudiantil.

3.2 Metodología empleada.

Se describirá a continuación, mediante pasos, la metodología que se empleó para llegar a un diseño óptimo, basado en las mediciones efectuadas.

Paso 1: Diseñar la planta de cada edificación. En el **Anexo 1** se encuentran los diseños de planta del edificio docente y de la residencia estudiantil. El diseño de planta de una localidad determinada aumenta la noción que desde el punto de vista espacial y estructural se tiene de una edificación. Ayuda a determinar fácilmente, por ejemplo, la distancia y la cantidad de paredes entre dos puntos determinados.

Paso 2: Realizar un scanning con el software CommView for Wifi en el área analizada para determinar si existe actividad en la banda de frecuencia a emplear, en este caso, la banda de 2.4 GHz. De existir algún AP o una red Ad-hoc operando en un canal determinado, no se podrá seleccionar este canal para realizar las mediciones de campo.

Con el scanning realizado se encontró la existencia de un AP en el edificio docente operando en el canal 6 (Dpto. de Inglés) y en la residencia estudiantil se encontraron dos operando en el canal 4 y 6 por lo que se determinó configurar el AP con el que se realizaron las pruebas, para operar en el canal 11, fuera de toda interferencia provocada por los APs presentes.

Paso 3: Ubicar el AP en un punto abierto, nunca dentro de un área cerrada pues se estaría limitando la potencia de la señal. Preferiblemente en alguna posición alta en los pasillos centrales.

Paso 4: Realizar las mediciones con el software CommView for Wifi en la mayor cantidad de puntos posibles que circundan el AP para poder determinar su cobertura real. Ahora, el CommView for Wifi se configura para escanear solamente el canal de operación del AP, o sea, el 11 y cada 3 segundos para tener en todo momento el valor instantáneo del nivel de señal en el punto de análisis.

Paso 5: Realizar el trazado del mapa de cobertura sobre el diseño de planta, en la horizontal y en la vertical, teniendo en cuenta, según la bibliografía estudiada, que un valor del nivel de la señal de hasta -35 dBm se considera como excelente, entre -45 y -75 dBm como bueno y por debajo de -85 dBm como pobre.

Si los mapas de cobertura obtenidos no son los adecuados para el tipo de servicio que se desea brindar se vuelve al paso 3 ubicando el punto de acceso en otro punto. Si el resultado es similar se está indicando que el área analizada tendrá que ser cubierta con 2 ó más APs, ejecutando el proceso desde el paso 3 todas las veces que sean necesarias hasta llegar al resultado esperado.

Al finalizar se tendrá la cantidad de APs necesarios en el diseño y su ubicación óptima.

Paso 6: Restaría entonces asignar un canal a cada AP según una planificación de frecuencia adecuada.

3.3 Mediciones efectuadas y propuesta de red inalámbrica.

En este punto se muestran los resultados de las mediciones efectuadas según la ubicación definitiva de los APs. Pero antes es menester señalar que las primeras mediciones efectuadas en el edificio docente se realizaron ubicando el AP en un punto central de cada planta y al evaluar los resultados se determinó que un AP no daba la suficiente cobertura en una planta para lograr un servicio aceptable en toda el área requerida; por ejemplo, ubicando el AP en el punto P1 (**Ver Anexo1**) de la planta 1, el nivel de la señal en el aula 101, en el laboratorio de circuitos y en el aula 107, oscilaba entre -75 y -85 dBm, existiendo momentos en que la conexión se establecía a 11 Mbps y otros que bajaba a 1Mbps respondiendo de forma esporádica el AP a una solicitud de respuesta de eco con el comando ping. En el resto de las plantas el resultado fue peor en los extremos del edificio. Esto fue razón más que suficiente para determinar que por cada planta se ubicarían dos APs. En la residencia estudiantil fue necesario también incorporar 2 AP por cada bloque con el objetivo igual de tener cobertura total con buena calidad de servicio.

Estos resultados preliminares hicieron ver que con un nivel de señal entre -25 y -55 dBm se lograban velocidades entre 36 y 54 Mbps (considerado por los autores de este trabajo como excelente) y con niveles de señal entre -60 y -75 dBm las velocidades obtenidas oscilaban entre 5.5 y 24 Mbps (considerado como bueno). Las siguientes tablas muestran las mediciones obtenidas para cada AP solo en aquellos puntos donde la señal al menos es buena.

AP1: En planta baja Edificio Docente		AP2: En planta baja Edificio Docente	
Punto	Nivel de Señal (dBm)	Punto	Nivel de Señal (dBm)
P1	-28	P1	-48
P2	-75	P2	-47
P3	-60	P3	-26
P4	-25	P4	-70
P5	-60	A1	-72
A9	-70	A2	-75
A10	-65	A3	-70
A11	-50	A4	-67
A12	-55	A5	-54
A13	-48	A6	-55
A14	-50	A7	-50
A15	-58	A8	-45
A16	-65	A9	-54
A17	-73	A10	-65
A18	-75	A11	-69
A19	-55	A12	-73
A20	-45	A22	-65
A21	-35	P2.B	-70
A22	-55	P3.B	-58
P1.B	-60	B2	-75
P4.B	-70	B3	-74
B6	-75	B4	-75
B10	-75	B12	-75

Tabla 3.1 Mediciones obtenidas para AP1 y AP2 ubicados en la planta baja del edificio docente.

AP3: En planta #1 Edificio Docente		**AP4: En planta #1 Edificio Docente**	
Punto	Nivel de Señal (dBm)	Punto	Nivel de Señal (dBm)
P1	-33	P1	-49
P2	-70	P2	-50
P3	-65	P3	-28
P4	-28	P4	-75
P5	-62	B1	-52
B4	-70	B2	-53
B5	-64	B3	-45
B6	-48	B4	-39
B7	-45	B5	-55
B8	-59	B6	-65
B9	-40	B11	-72
B10	-44	B12	-69
B11	-65	P1.A	-76
B12	-70	P2.A	-75
P1.A	-78	P3.A	-65
P4.A	-65	A7	-80
P5.A	-70	A8	-70
A14	-75	A9	-79
A15	-79	P1.C	-75
A19	-73	P2.C	-75
A20	-77	P3.C	-65
A21	-70	C4	-76
P1.C	-75	C5	-70
P4.C	-66	C6	-72
P5.C	-71		
C9	-77		
C10	-79		

Tabla 3.2 Mediciones obtenidas para AP3 y AP4 ubicados en la planta 1 del edificio docente.

AP5: En planta #2 Edificio Docente		**AP6: En planta #2 Edificio Docente**	
Punto	Nivel de Señal (dBm)	Punto	Nivel de Señal (dBm)
P1	-35	P1	-50
P3	-68	P2	-47
P4	-30	P3	-26
P5	-64	P4	-77
C6	-75	C1	-75
C7	-68	C2	-65
C8	-60	C3	-60
C9	-40	C4	-55
C10	-42	C5	-45
C11	-50	C6	-55
C12	-60	C7	-60
C13	-65	C8	-64
C14	-70	C9	-75
P1.B	-70	P1.B	-75
P4.B	-65	P2.B	-73
P5.B	-70	P3.B	-65
B6	-77	B2	-80
B7	-75	B3	-75
B9	-75	B4	-76
B10	-73	B12	-74
P1.D	-73	P1.D	-72
P4.D	-66	P2.D	-77
P5.D	-70	P3.D	-65
D10	-75	D4	-75
D11	-70	D5	-75
D12	-72	D6	-76

Tabla 3.3 Mediciones obtenidas para AP5 y AP6 ubicados en la planta 2 del edificio docente.

AP7: En planta # 3 Edificio Docente		AP8: En planta # 3 Edificio Docente	
Punto	Nivel de Señal (dBm)	Punto	Nivel de Señal (dBm)
P1	-35	P1	-55
P3	-50	P2	-35
P4	-28	P3	-28
P5	-44	P4	-70
D6	-74	D1	-65
D7	-70	D2	-60
D8	-65	D3	-48
D9	-55	D4	-35
D10	-40	D5	-30
D11	-35	D6	-35
D12	-39	D7	-45
D13	-50	D8	-60
D14	-57	D9	-70
D15	-72	P2.C	-69
P1.C	-50	P3.C	-55
P4.C	-45	C4	-65
C9	-60	C5	-56
C10	-70	C6	-60
C11	-75	P1.E	-60
C12	-70	P2.E	-65
P1.E	-60	P3.E	-55
P4.E	-45	E4	-75
P5.E	-60	E5	-60
E10	-75	E6	-75
E11	-70		
E12	-74		

Tabla 3.4 Mediciones obtenidas para AP7 y AP8 ubicados en la planta 3 del edificio docente.

AP9: En planta # 4 Edificio Docente		**AP10: En planta # 4 Edificio Docente**	
Punto	Nivel de Señal (dBm)	Punto	Nivel de Señal (dBm)
P1	-40	P1	-55
P3	-65	P2	-55
P4	-28	P3	-28
P5	-44	P4	-70
E7	-75	E1	-70
E8	-70	E2	-66
E9	-60	E3	-62
E10	-45	E4	-55
E11	-35	E5	-36
E12	-44	E6	-53
E13	-55	E7	-60
E14	-60	E8	-70
E15	-65	E9	-75
P1.D	-65	P1.D	-65
P4.D	-55	P2.D	-64
P5.D	-70	P3.D	-55
D10	-75	D4	-69
D11	-65	D5	-56
D12	-75	D6	-65

Tabla 3.5 Mediciones obtenidas para AP9 y AP10 ubicados en la planta 4 del edificio docente.

AP11: En planta #1 Residencia Estudiantil Bloque 1		AP12: En planta #3 Residencia Estudiantil Bloque 1	
Punto	Nivel de Señal (dBm)	Punto	Nivel de Señal (dBm)
P1. #B	-74	P1. #2	-73
P2. #B	-55	P2. #2	-51
P3. #B	-47	P3. #2	-48
P1. #1	-68	P1. #3	-65
P2. #1	-40	P2. #3	-38
P3. #1	-35	P3. #3	-33
P1. #2	-70	P1. #4	-72
P2. #2	-58	P2. #4	-55
P3. #2	-50	P3. #4	-48

Tabla 3.6 Mediciones obtenidas para AP11 y AP12 ubicados en el bloque 1 de la residencia estudiantil.

AP13: En planta #1 Residencia Estudiantil Bloque 2		AP14: En planta #3 Residencia Estudiantil Bloque 2	
Punto	Nivel de Señal (dBm)	Punto	Nivel de Señal (dBm)
P1. #B	-70	P1. #2	-76
P2. #B	-57	P2. #2	-54
P3. #B	-44	P3. #2	-50
P1. #1	-66	P1. #3	-68
P2. #1	-40	P2. #3	-40
P3. #1	-33	P3. #3	-36
P1. #2	-74	P1. #4	-72
P2. #2	-54	P2. #4	-53
P3. #2	-50	P3. #4	-46

Tabla 3.7 Mediciones obtenidas para AP13 y AP14 ubicados en el bloque 2 de la residencia estudiantil.

AP15: En planta #1 Residencia Estudiantil Bloque 3		**AP16: En planta #3 Residencia Estudiantil Bloque 3**	
Punto	Nivel de Señal (dBm)	Punto	Nivel de Señal (dBm)
P1. #B	-75	P1. #2	-77
P2. #B	-58	P2. #2	-56
P3. #B	-48	P3. #2	-53
P1. #1	-67	P1. #3	-67
P2. #1	-44	P2. #3	-44
P3. #1	-36	P3. #3	-37
P1. #2	-72	P1. #4	-74
P2. #2	-51	P2. #4	-57
P3. #2	-47	P3. #4	-50

Tabla 3.8 Mediciones obtenidas para AP15 y AP16 ubicados en el bloque 3 de la residencia estudiantil.

AP17: En planta #1 Residencia Estudiantil Bloque 4		**AP18: En planta #3 Residencia Estudiantil Bloque 4**	
Punto	Nivel de Señal (dBm)	Punto	Nivel de Señal (dBm)
P1. #B	-75	P1. #2	-71
P2. #B	-52	P2. #2	-53
P3. #B	-43	P3. #2	-45
P1. #1	-70	P1. #3	-68
P2. #1	-38	P2. #3	-35
P3. #1	-32	P3. #3	-31
P1. #2	-73	P1. #4	-72
P2. #2	-54	P2. #4	-55
P3. #2	-43	P3. #4	-46

Tabla 3.9 Mediciones obtenidas para AP17 y AP18 ubicados en el bloque 4 de la residencia estudiantil.

AP19: En planta #2 Residencia Estudiantil Bloque 5A (6A,AP21)		AP20: En planta #2 Residencia Estudiantil Bloque 5B (6B,AP22)	
Punto	Nivel de Señal (dBm)	Punto	Nivel de Señal (dBm)
P1. #B	-58	P1. #B	-55
P2. #B	-62	P2. #B	-60
P3. #B	-55	P3. #B	-53
P1. #1	-52	P1. #1	-55
P2. #1	-58	P2. #1	-53
P3. #1	-54	P3. #1	-57
P1. #2	-28	P1. #2	-26
P2. #2	-47	P2. #2	-45
P3. #2	-38	P3. #2	-40
P1. #3	-49	P1. #3	-50
P2. #3	-57	P2. #3	-55
P3. #3	-55	P3. #3	-53
P1. #4	-60	P1. #4	-59
P2. #4	-64	P2. #4	-74
P3. #4	-60	P3. #4	-68

Tabla 3.10 Mediciones obtenidas para AP19 y AP20 ubicados en el bloque 5 de la residencia estudiantil.

Con estos resultados se confeccionaron los mapas de cobertura que se muestran en el Anexo 2 que dan una idea gráfica de la propuesta de red planteada.

Como propuesta para la seguridad de la red, y para completar el diseño se propone el uso de WPA2 en su modalidad empresarial haciendo uso de un servidor Radius central; en las pruebas efectuadas se utilizó el servidor FreeRadius sobre Linux Debian.

3.3.1 Planificación de frecuencia para la propuesta de red inalámbrica.

En la Tabla 3.11 y 3.12 se muestra el canal que usará cada AP en la propuesta de red inalámbrica.

PUNTO DE ACCESO	CANAL RF
AP1	1
AP2	6
AP3	11
AP4	1
AP5	1
AP6	6
AP7	11
AP8	1
AP9	1
AP10	6

Tabla 3.11 Planificación de frecuencia para el edificio docente.

PUNTO DE ACCESO	CANAL RF
AP11	1
AP12	6
AP13	11
AP14	6
AP15	1
AP16	11
AP17	6
AP18	1
AP19	11
AP20	6
AP21	1
AP22	8

Tabla 3.12 Planificación de frecuencia para la residencia estudiantil.

.

VALORACIÓN ECONÓMICA

Esta propuesta surge en un momento donde es de vital importancia para Cuba la búsqueda de nuevos mecanismos para disminuir los costos de importación de tecnologías, y a la vez lograr contribuir al desarrollo y crecimiento económico.

A continuación se muestra la relación de costo para la inversión de la red inalámbrica que se propone.

Descripción	Cantidad	Precio Unitario	Total
Puntos de acceso	22	$ 90.00 CUC	$ 1980.00 CUC
Cable UTP Cat5e.	450 metros	0.35 CUC	157.50 CUC
Conector RJ 45	44	0.25 CUC	11.00 CUC
TOTAL			**$ 2148.50 CUC**

.

CONCLUSIONES

Como conclusiones del trabajo se pueden resumir las siguientes:

1. Para brindar una cobertura total y un servicio con una calidad aceptable, se tendrán que emplear un total de 10 APs en el edificio docente y 12 en la residencia estudiantil para un total de 22 APs bajo el estándar 802.11b/g.
2. La seguridad de la red es lograda con la utilización de WPA en su modalidad empresarial haciendo uso de un servidor RADIUS para toda la red.

RECOMENDACIONES

1. Realizar el diseño de la red inalámbrica para el edificio de rectoría siguiendo la metodología presentada en este trabajo.
2. Realizar una simulación de la red propuesta haciendo uso de algún software profesional de simulación de redes 802.11b/g.
3. Someter a análisis esta propuesta por parte de los directivos de la UPR con el objetivo de su implementación en un futuro cercano.

BIBLIOGRAFÍA

1. Matthew Gast. 802.11 Wireless Networks The Definitive Guide. 2nd edition. OReilly, 2005.
2. Historia de las redes inalámbricas
   http://cecy150.tripod.com/pag2.html
3. Evolución de las redes inalámbricas
   http://www.maestrosdelweb.com/principiantes/evolucion-de-las-redes-inalambricas/
4. Cobertura de redes inalámbricas 802.11
   http://www.34t.com/box-docs.asp?doc=638
5. Seguridades de la red inalámbrica
   http://foro.elhacker.net/index.php/topic,62799.msg287872.html#msg287872
6. Accediendo al Router
   http://www.phenoelit.de/dpl/dpl.html
7. Descripción de la tecnología 802.11
   http://www.content4reprint.com/view/spanish-27045.htm
8. Descripción del estándar 802.11 b
   http://www.laserwifi.com/estander802b.11.htm
9. Descripción de la estándar 802.11 g
   http://www.interwifisa.com/estander802g.11.htm
10. Protocolo CSMA/CA
    http://cursos.die.udec.cl/~redes/apuntes/myapuntes/node72.html
11. Redes inalámbricas, estándares y mecanismos de seguridad
    http://www.enterate.unam.mx/Articulos/2004/agosto/redes.htm
12. Protectec Access Overview
    http://www.weca.net/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf
13. Estándares de redes inalámbricas
    http://www.unincca.edu.co/boletin/indice.htm
14. Estrategias de una Wlan
    http://www.intel.com/ebusiness/strategies/wireless/wlan/standards.htm

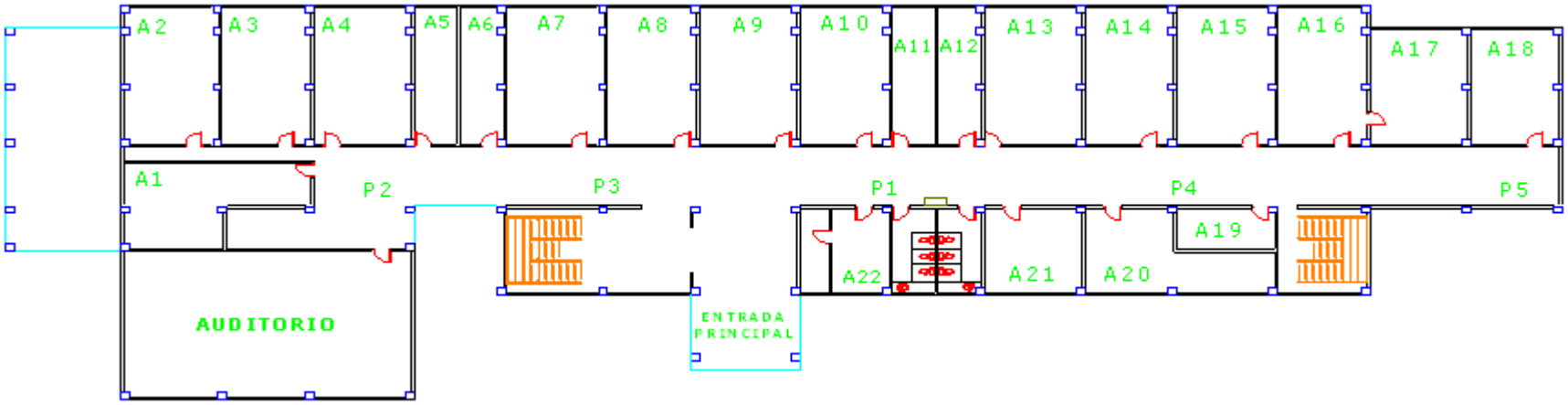
15. Monografías
http://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml
16. Configuring Wired Equivalent Privacy (WEP).
http:// www.cisco.com
17. Wikipedia, WPA
http://es.wikipedia.org/wiki/Wi-Fi_Protected_Access.
18. Wikipedia, WPA2
http://es.wikipedia.org/wiki/WPA2.
19. Wikipedia TKIP
http://es.wikipedia.org/wiki/TKIP.
20. Seguridad en redes inalámbricas
http://documentos.shellsec.net/otros/SeguridadWireless.pdf
21. Wired Equivalent Privacy.
http://lasecwww.epfl.ch/securityprotocols/wep/WEP.pdf
22. Protocolos de seguridad en redes inalámbricas.
http://www.saulo.net/pub/inv/SegWiFi-art.htm
23. Wi-Fi Protected Access:
http://www.wi-fi.org/

ANEXOS

ANEXO 1: Diseños de planta.

Se presentan aquí los diseños de planta de cada piso del edificio docente y una vista frontal del mismo. Respecto a la residencia estudiantil se presenta solo una vista superior de cada bloque ya que todas los pisos tienen la misma estructura y finalmente una vista frontal.

VISTA SUPERIOR PLANTA BAJA DEL EDIFICIO DOCENTE



A1: Dpto. Dirección De Extensión Universitaria.

A2: Dpto. 1

A3: Dpto. 2

A4: Dpto. Comité Del Partido.

A5: Dpto. Turismo.

A6: Dpto. Defensa.

A7: Aula 006

A8: Dpto. Matemática.

A9: Decanato Informática y Tele.

A10: Dpto. Contabilidad y Finanzas.

A11: Administración Informática y Tele.

A12: Admon. Facultad de Ciencia Económica.

A13: Dpto. Informática.

A14: Cedecon.

A15: Aula 001

A16: Decanato de Facultad de Economía.

A17: Área de Facultad de Economía.

A18: Dpto. Ingeniería Industrial.

A19: Oficina de Servicio General.

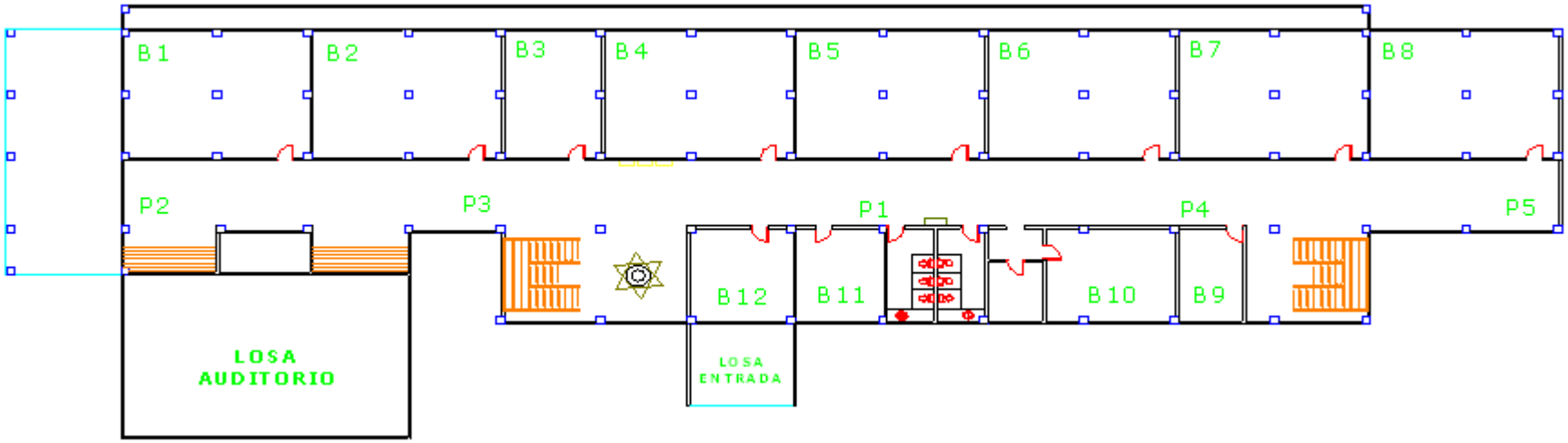
A20: Imprenta.

A21: Secretaria Informática y Tele.

A22: Gedeltur.

P: Puntos de Medición.

VISTA SUPERIOR PLANTA 1 DEL EDIFICIO DOCENTE



B1: Laboratorio Circuitos.

B2: Aula 101.

B3: Aula 102.

B4: Aula 103.

B5: Aula 104

B6: Aula 105.

B7: Aula 106.

B8: Aula 107.

B9: Aplicación de SW.

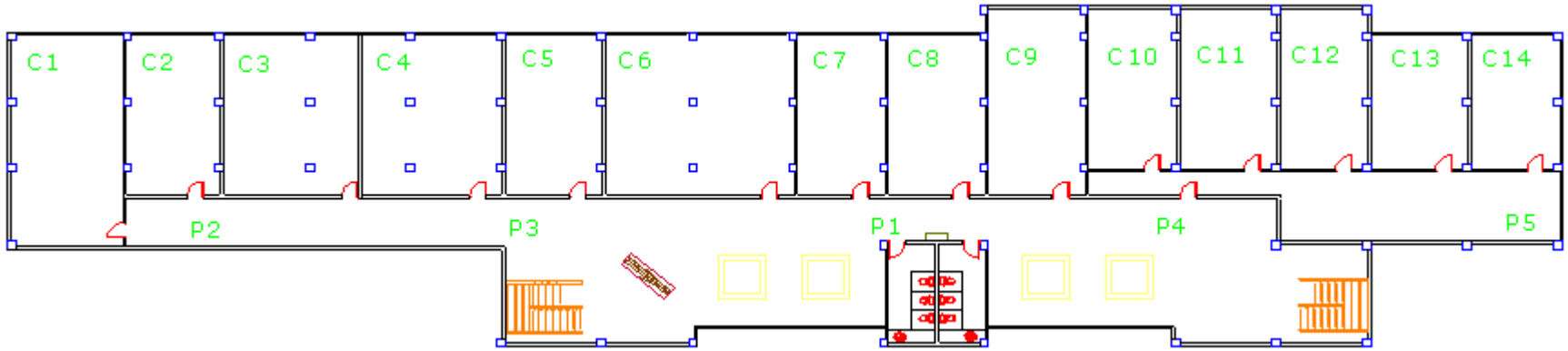
B10: Depto. Electrónica.

B11: Aula 110.

B12: Aula Circuitos.

P: Puntos de Medición.

VISTA SUPERIOR PLANTA 2 DEL EDIFICIO DOCENTE



C1: Aula 201.

C2: Laboratorio 1.

C3: Laboratorio 2.

C4: Laboratorio 3.

C5: Dpto. Marxismo.

C6: Aula Dibujo.

C7: Laboratorio de computación

C8: Laboratorio de la FFA.

C9: Sindicato.

C10: Aula 209.

C11: Aula 210.

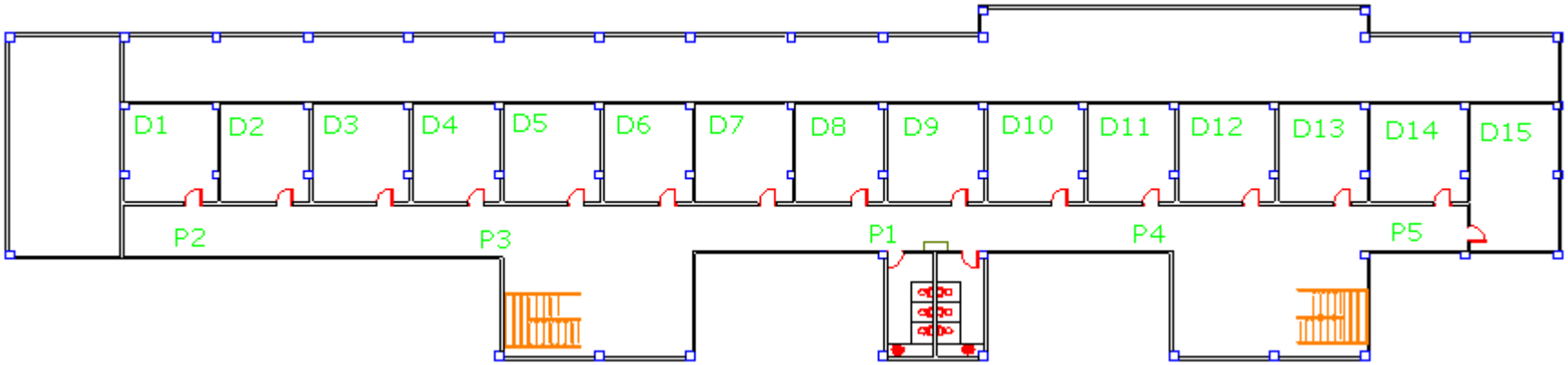
C12: Aula 211.

C13: Aula 212.

C14: Oficina y Laboratorio.

P: Puntos de Medición.

VISTA SUPERIOR PLANTA 3 DEL EDIFICIO DOCENTE



D1: Cemarna.

D2: Aula 302.

D3: Aula 303.

D4: Dpto. Economía Global.

D5: Laboratorio Idiomas.

D6: UPRedes.

D7: Dpto. Idiomas.

D8: Dpto. Telecomunicaciones.

D9: Dpto. Química.

D10: Forestal.

D11: Agronomía.

D12: Secretaria Forestal – Agronomía.

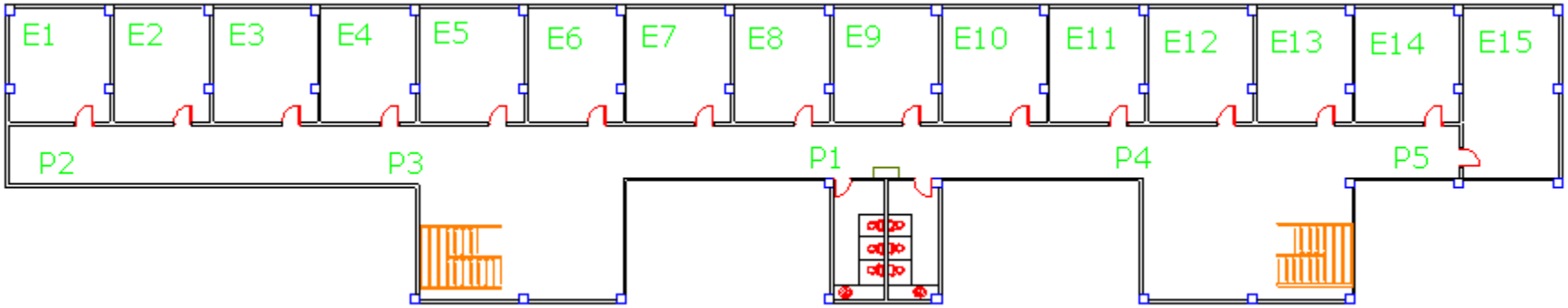
D13: Centro de Estudios Forestales.

D14: Admon. Forestal y Agronomía.

D15: Decanato Forestal y Agronomía.

P: Puntos de Medición.

VISTA SUPERIOR PLANTA 4 DEL EDIFICIO DOCENTE



E1: Aula 401.

E2: Aula 402.

E3: Aula 403.

E4: Aula 404.

E5: Aula 405.

E6: Aula 406.

E7: Aula 407.

E8: Aula 408.

E9: Aula 409.

E10: Aula 410.

E11: Aula 411.

E12: Aula 412.

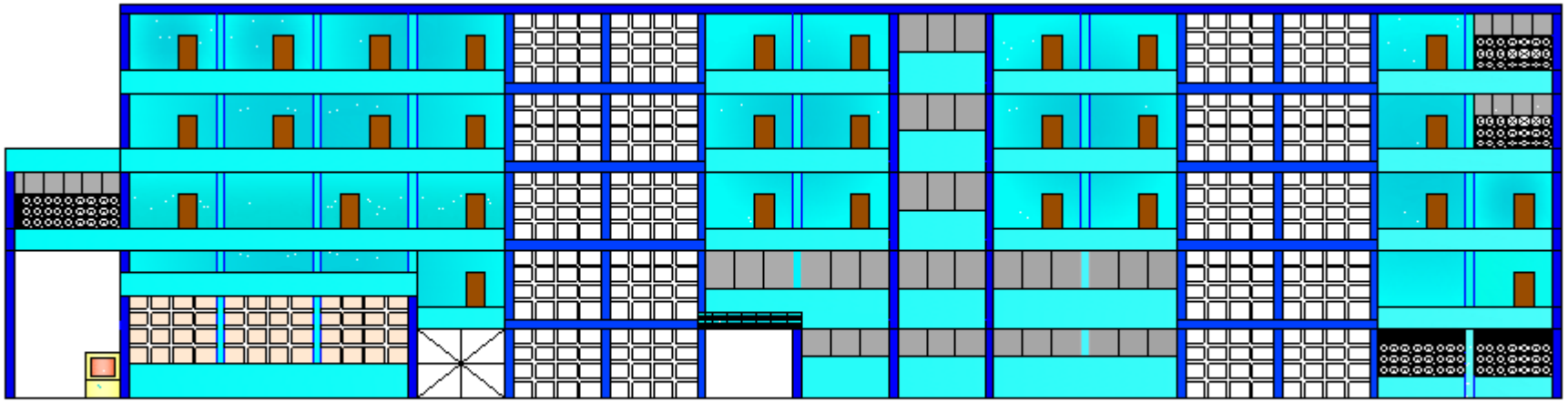
E13: Aula 413.

E14: Aula 414.

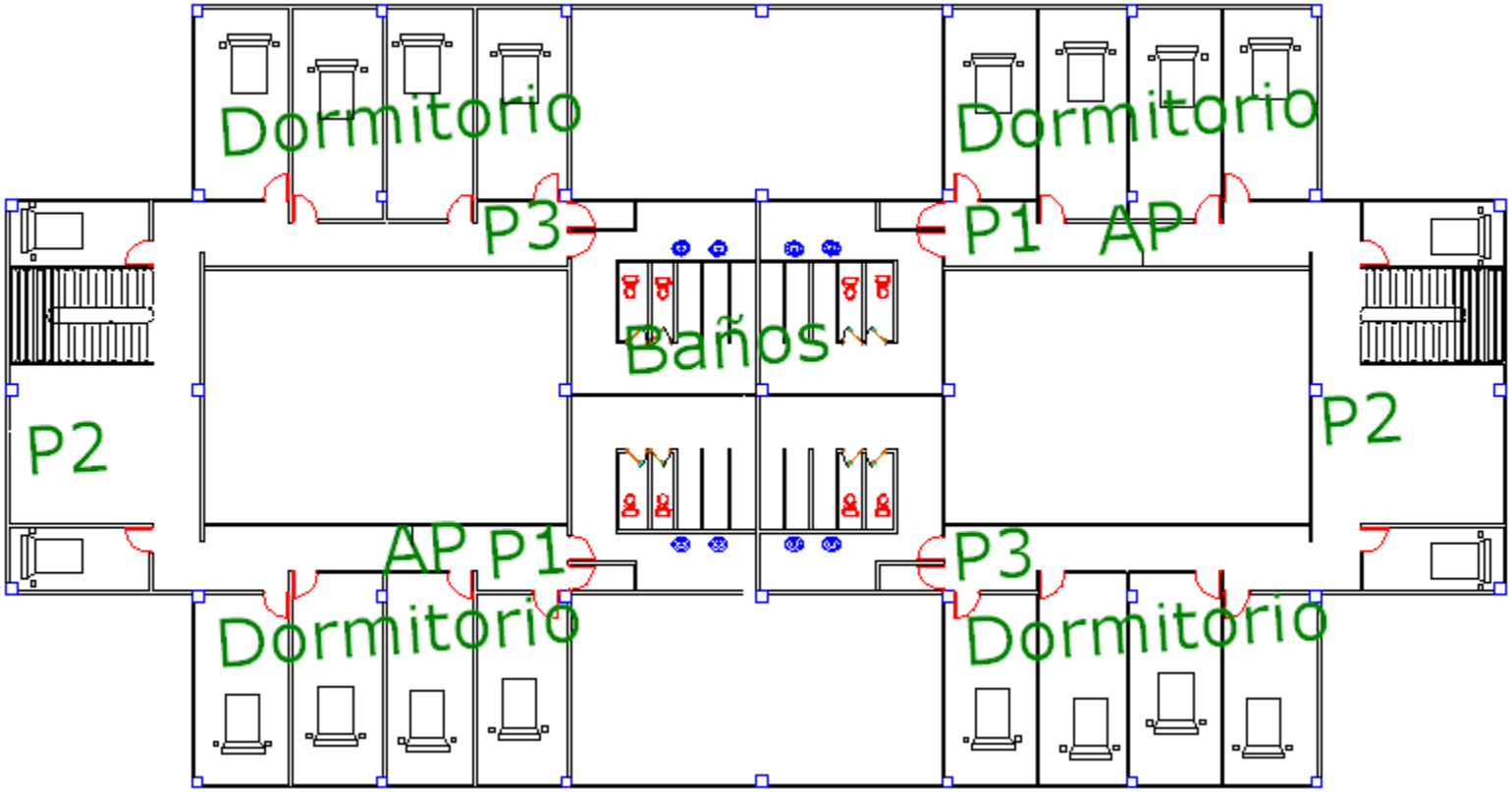
E15: Aula 415.

P: Puntos de Medición.

VISTA FRONTAL DEL EDIFICIO DOCENTE



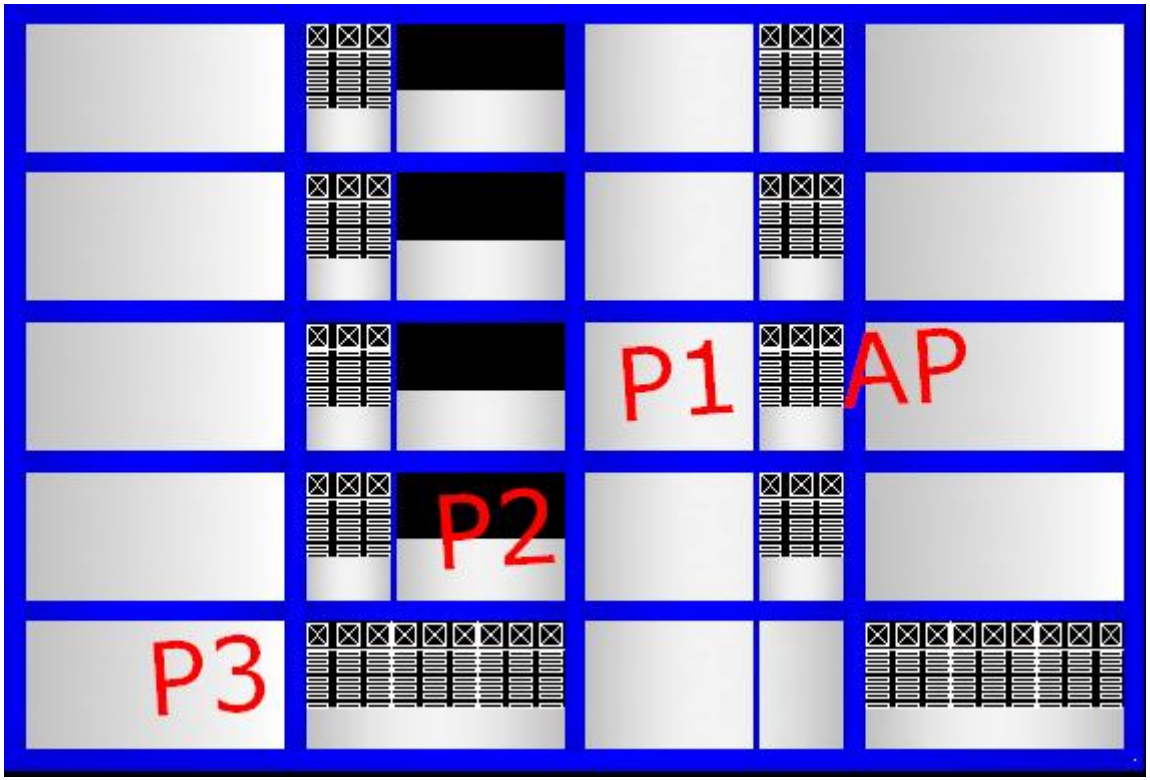
VISTA SUPERIOR DEL BLOQUE 6 DE LA RESIDENCIA ESTUDIANTIL (IGUAL AL BLOQUE 5)



P: Puntos de Medición.

AP: Punto de Acceso.

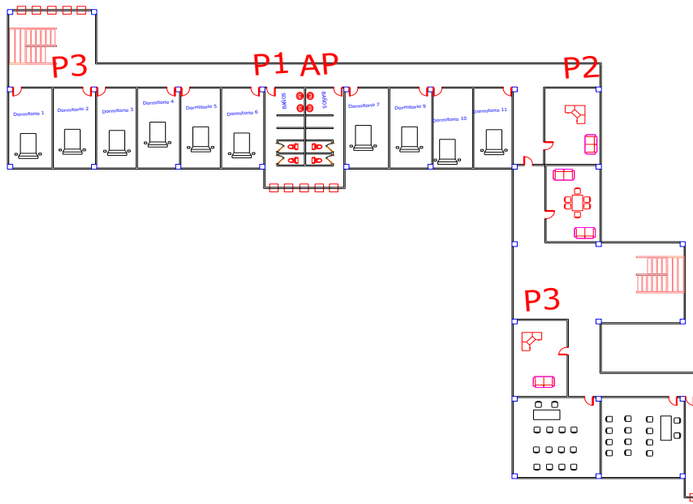
VISTA LATERAL (ALA IZQUIERDA) DEL BLOQUE 6 DE LA RESIDENCIA ESTUDIANTIL (IGUAL AL BLOQUE 5)

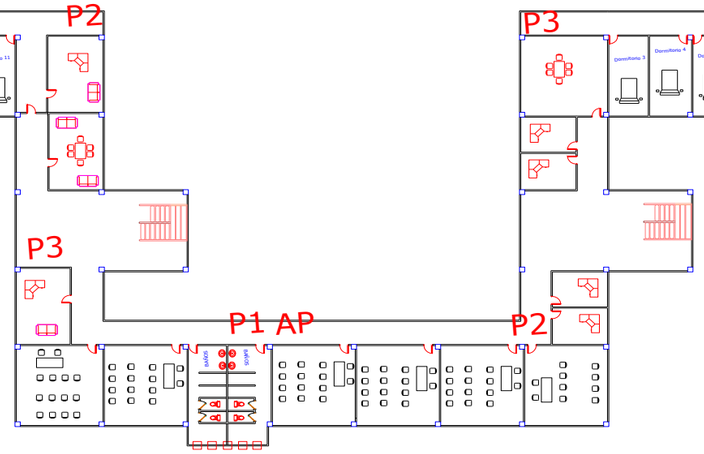


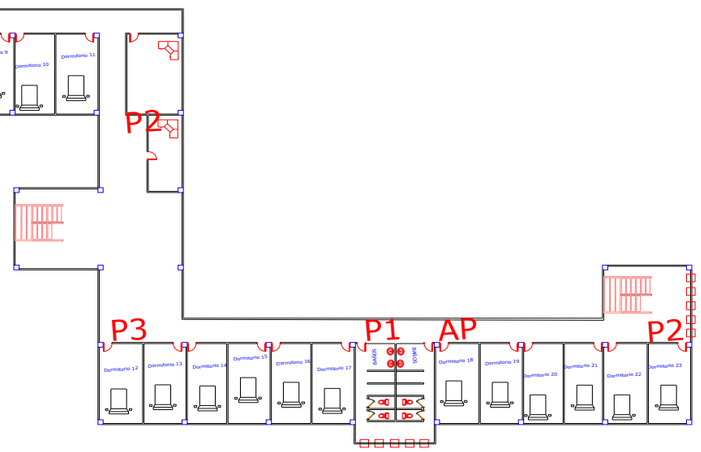
P: Puntos de Medición.

AP: Punto de Acceso.

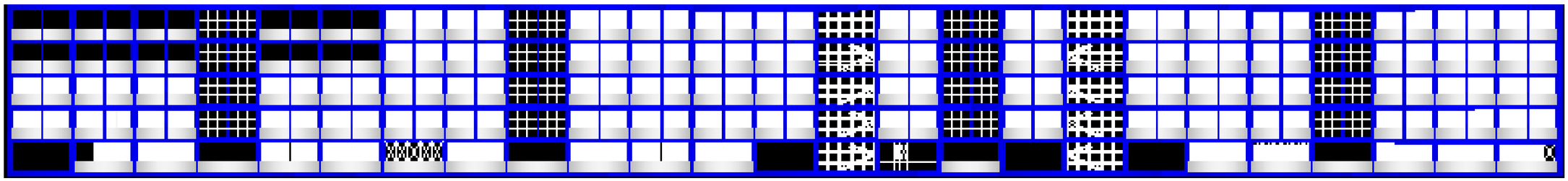
VISTA SUPERIOR DE LOS BLOQUES 1, 2, 3 Y 4 DE LA RESIDENCIA ESTUDIANTIL







VISTA FRONTAL DE LOS BLOQUES 1, 2, 3 Y 4 DE LA RESIDENCIA ESTUDIANTIL

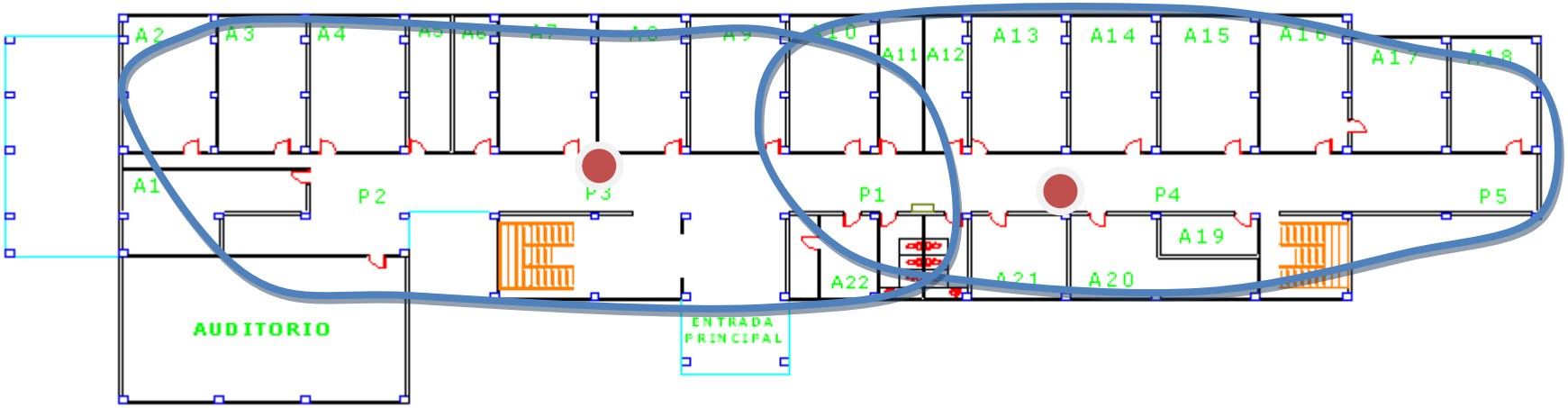


ANEXO 2: Mapas de cobertura de los puntos de acceso.

Se presentan aquí la ubicación final de los APs y sus mapas de cobertura constituyendo lo que sería la propuesta definitiva de este trabajo de investigación.

MAPA DE COBERTURA

VISTA SUPERIOR PLANTA BAJA DEL EDIFICIO DOCENTE



A1: Dpto. Dirección De Extensión Universitaria.

A2: Dpto. 1

A3: Dpto. 2

A4: Dpto. Comité Del Partido.

A5: Dpto. Turismo.

A6: Dpto. Defensa.

A7: Aula 006

A8: Dpto. Matemática.

A9: Decanato Informática y Tele.

A10: Dpto. Contabilidad y Finanzas.

A11: Administración Informática y Tele.

A12: Admon. Facultad de Ciencia Económica.

A13: Dpto. Informática.

A14: Cedecon.

A15: Aula 001

A16: Decanato de Facultad de Economía.

A17: Área de Facultad de Economía.

A18: Dpto. Ingeniería Industrial.

A19: Oficina de Servicio General.

A20: Imprenta.

A21: Secretaria Informática y Tele.

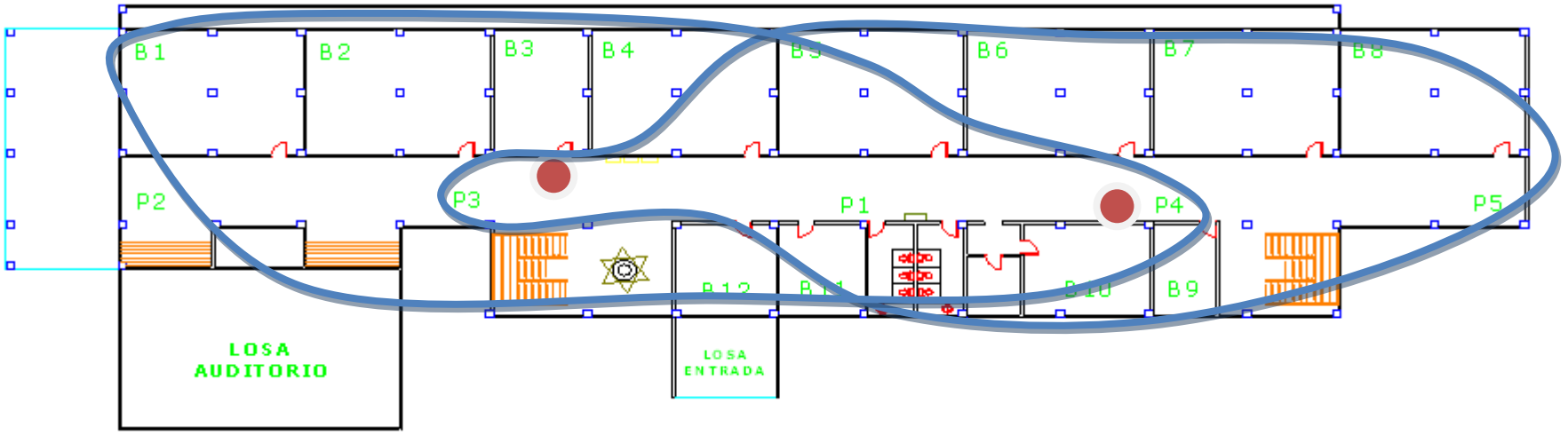
A22: Gedeltur.

P: Puntos de Medición.

Punto de Acceso.

MAPA DE COBERTURA

VISTA SUPERIOR PLANTA 1 DEL EDIFICIO DOCENTE



B1: Laboratorio Circuitos.

B2: Aula 101.

B3: Aula 102.

B4: Aula 103.

B5: Aula 104

B6: Aula 105.

B7: Aula 106.

B8: Aula 107.

B9: Aplicación de SW.

B10: Depto. Electrónica.

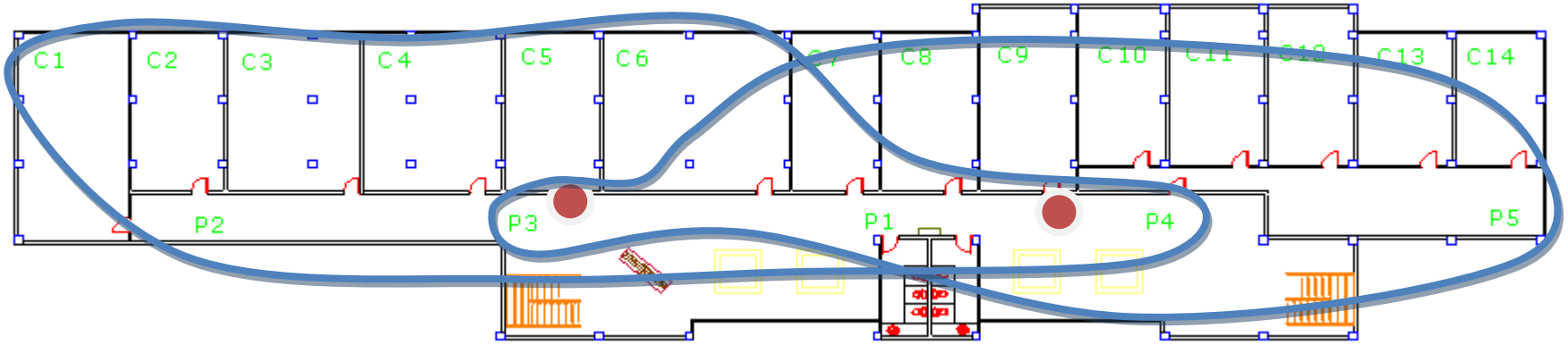
B11: Aula 110.

B12: Aula Circuitos.

P: Puntos de Medición.

MAPA DE COBERTURA

VISTA SUPERIOR PLANTA 2 DEL EDIFICIO DOCENTE



C1: Aula 201.

C2: Laboratorio 1.

C3: Laboratorio 2.

C4: Laboratorio 3.

C5: Dpto. Marxismo.

C6: Aula Dibujo.

C7: Laboratorio de computación

C8: Laboratorio de la FFA.

C9: Sindicato.

C10: Aula 209.

C11: Aula 210.

C12: Aula 211.

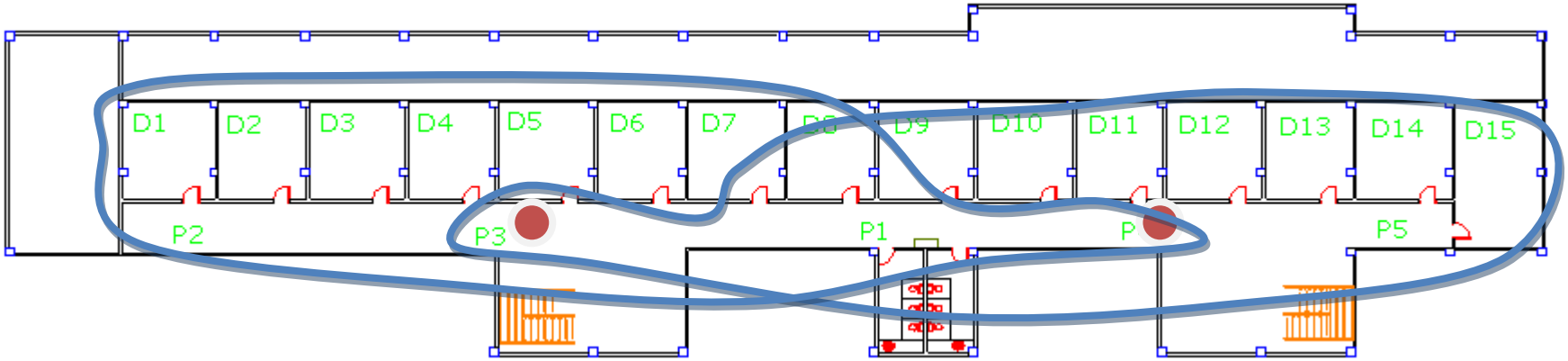
C13: Aula 212.

C14: Oficina y Laboratorio.

P: Puntos de Medición.

MAPA DE COBERTURA

VISTA SUPERIOR PLANTA 3 DEL EDIFICIO DOCENTE



D1: Cemarna.

D2: Aula 302.

D3: Aula 303.

D4: Dpto. Economía Global.

D5: Laboratorio Idiomas.

D6: UPRedes.

D7: Dpto. Idiomas.

D8: Dpto. Telecomunicaciones.

D9: Dpto. Química.

D10: Forestal.

D11: Agronomía.

D12: Secretaria Forestal – Agronomía.

D13: Centro de Estudios Forestales.

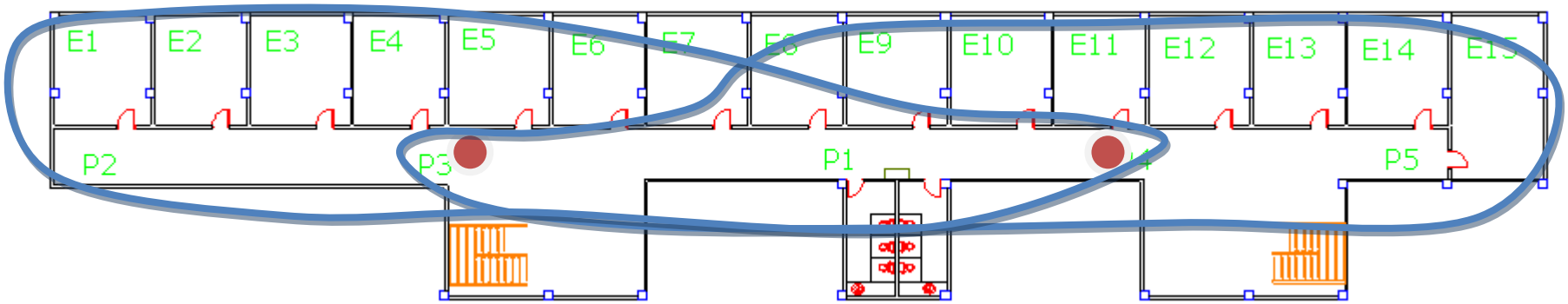
D14: Admon. Forestal y Agronomía.

D15: Decanato Forestal y Agronomía.

P: Puntos de Medición.

MAPA DE COBERTURA

VISTA SUPERIOR PLANTA 4 DEL EDIFICIO DOCENTE



E1: Aula 401.

E2: Aula 402.

E3: Aula 403.

E4: Aula 404.

E5: Aula 405.

E6: Aula 406.

E7: Aula 407.

E8: Aula 408.

E9: Aula 409.

E10: Aula 410.

E11: Aula 411.

E12: Aula 412.

E13: Aula 413.

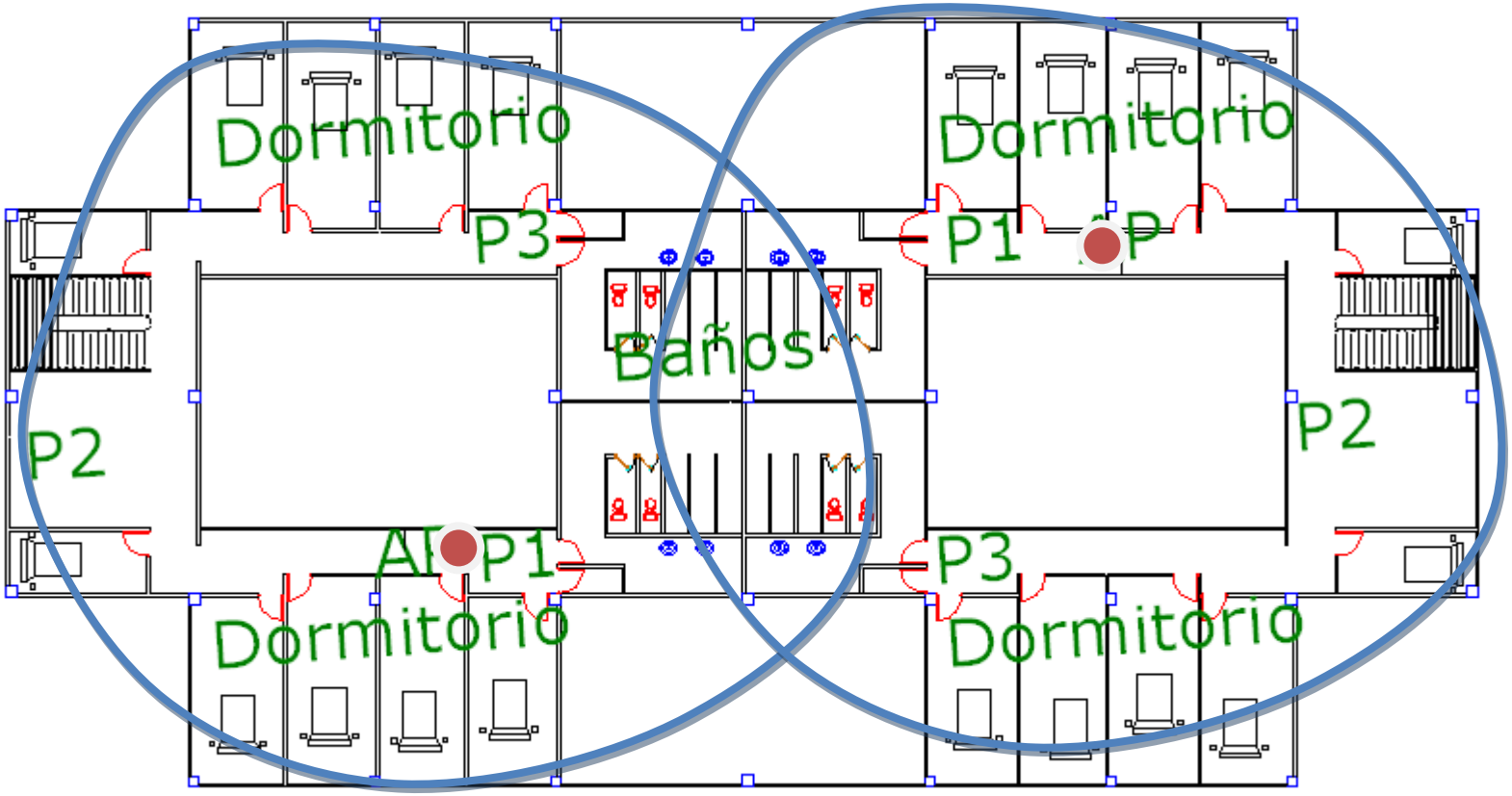
E14: Aula 414.

E15: Aula 415.

P: Puntos de Medición.

MAPA DE COBERTURA

VISTA SUPERIOR DEL BLOQUE 6 DE LA RESIDENCIA ESTUDIANTIL (IGUAL AL BLOQUE 5)

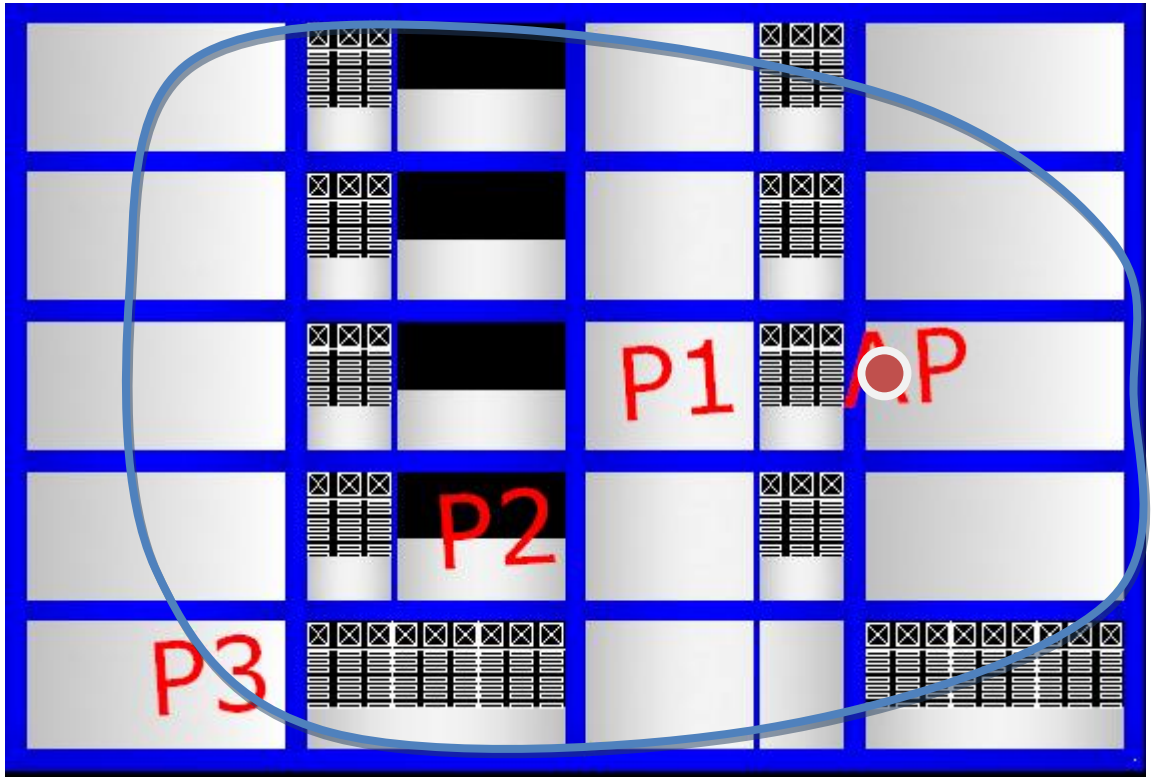


P: Puntos de Medición.

AP: Punto de Acceso.

MAPA DE COBERTURA

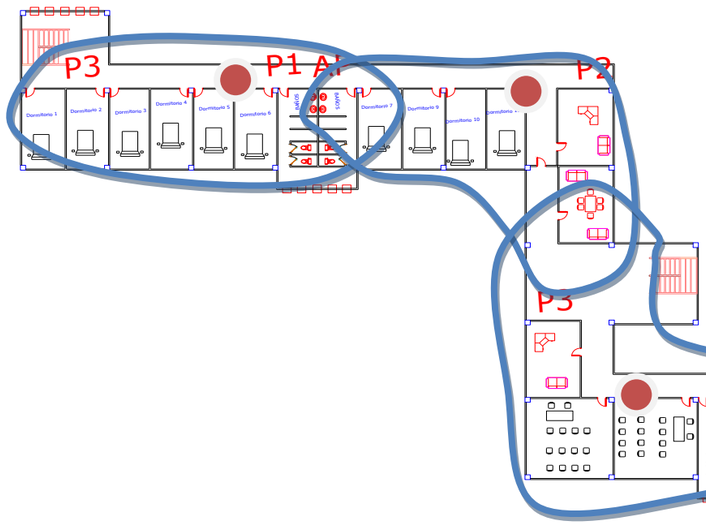
VISTA LATERAL (ALA IZQUIERDA) DEL BLOQUE 6 DE LA RESIDENCIA ESTUDIANTIL (IGUAL AL BLOQUE 5)

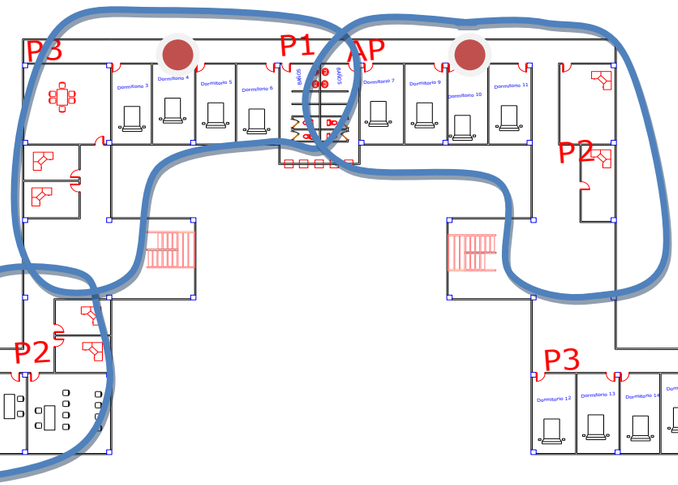


P: Puntos de Medición.

AP: Punto de Acceso.

MAPA DE COBERTURA VISTA SUPERIOR DE LOS BLOQUES 1, 2, 3 Y 4 DE LA RESIDENCIA ESTUDIANTIL





MAPA DE COBERTURA

VISTA FRONTAL DE LOS BLOQUES 1, 2, 3 Y 4 DE LA RESIDENCIA ESTUDIANTIL