

UNIVERSIDAD POLITECNICA DE VALENCIA

ESCUELA POLITECNICA SUPERIOR DE GANDIA

Grado en Ing. Sist. de Telecom., Sonido e Imagen



UNIVERSIDAD
POLITECNICA
DE VALENCIA



ESCUELA POLITECNICA
SUPERIOR DE GANDIA

“Diseño e implantación de una red inalámbrica unificada en el Colegio Nuestra Señora de Fátima de Valencia”

TRABAJO FINAL DE GRADO

Autor/a:

José María Murillo Safont

Tutor/a:

Fernando Boronat Seguí

GANDIA, 2015

Resumen

El objetivo del presente trabajo es mostrar como se ha diseñado, implantado y configurado, en el colegio Nuestra Señora de Fátima de Valencia, una red de comunicaciones inalámbrica unificada. Esta red permite dar cobertura a las seis plantas del edificio con zonas destinadas a fines académicos y con una velocidad adecuada a la demanda actual. Además, se puede gestionar de forma centralizada y casi automática, de ahí su nombre “unificada”.

El número de puntos de acceso inalámbricos necesarios se determina a partir del número de posibles usuarios potenciales y de las áreas a cubrir en las diferentes plantas del edificio. Un estudio detallado de la propagación radioeléctrica de la red, determina el número de los puntos de acceso necesarios definitivo y su óptima ubicación para cubrir todas las zonas requeridas.

Una vez emplazados los puntos de acceso, se diseña la arquitectura de la red cableada, que junto con todo el equipamiento necesario, permite la conexión a Internet y a la LAN existente. Finalmente se configuran los dispositivos (controladora, switch y servidor RADIUS) encargados de la gestión, la autenticación, la segmentación, la seguridad y del buen funcionamiento de la red.

Palabras clave: red inalámbrica, unificada, controladora, Wi-Fi, RADIUS.

Abstract

The aim of this work is to show as designed, installed and configured in the school Nuestra Señora de Fatima of Valencia, a unified wireless communications network. This network allows to cover all six floors of the building with areas intended for academic purposes and with adequate speed to the current demand. In addition, it can centrally manage and almost automatically, hence its name "unified".

The number of wireless access points required is determined from the number of potential users and possible areas to be covered in the different floors. A detailed study of radio propagation network, determines the definitive number of access points needed and the optimal location to cover all required areas.

Once deployed access points, the architecture of the wired network, with all the necessary equipment, allows connection to the Internet and the existing LAN is designed. Finally the devices (controller, switch and RADIUS server) responsible for the management, the authentication, the segmentation, the security and the proper functioning of the network are configured.

Key words: wireless network, unified, controller, Wi-Fi, RADIUS.

Índice de Contenido

1.INTRODUCCIÓN Y OBJETIVOS.....	5
1.1.INTRODUCCIÓN.....	5
1.2.DATOS DEL CENTRO.....	5
1.3.JUSTIFICACIÓN Y OBJETIVOS.....	5
2.ESTADO DEL ARTE.....	6
2.1.DISEÑO DE UNA RED INALÁMBRICA.....	6
2.2.ESTÁNDAR IEE 802.11.....	8
2.2.1.Norma 802.11b.....	8
2.2.2.Norma 802.11a.....	8
2.2.3.Norma 802.11g.....	8
2.2.4.Norma 802.11n.....	9
2.3.VENTAJAS E INCONVENIENTES ENTRE LA BANDA DE 2,4GHZ Y 5GHZ.....	9
3.DISEÑO Y CONFIGURACIÓN.....	10
3.1.ESTÁNDAR Y BANDA DE FRECUENCIA IDÓNEA PARA EL CENTRO.....	10
3.2.DIMENSIONADO Y PLANIFICACIÓN DEL SISTEMA.....	10
3.2.1.Cálculo del número de AP's basado en la capacidad.....	10
3.2.1.1.Quinta planta.....	11
3.2.1.2.Cuarta planta.....	11
3.2.1.3.Tercera planta.....	12
3.2.1.4.Segunda planta.....	12
3.2.1.5.Primera planta.....	12
3.2.1.6.Planta Baja.....	12
3.2.2.Cálculo del número de AP's basado en la cobertura.....	13
3.2.2.1.Estudio de cobertura previo.....	13
3.2.2.2.Estudio de cobertura posterior.....	13
3.2.3.Análisis de los cálculos.....	21
3.3.RED INALÁMBRICA UNIFICADA.....	22
3.3.1.Equipamiento utilizado.....	22
3.3.2.Eschema de la red cableada.....	24
3.3.3.Escenario.....	27
3.4.CONFIGURACIÓN DE LA RED UNIFICADA.....	29
3.4.1.Configuración de la Controladora Wireless DWC-1000.....	29
3.4.1.1.Configuración del Interface LAN.....	30
3.4.1.2.Configuración del Interface Option 1.....	31
3.4.1.3.Añadir nuevas VLANs.....	31
3.4.1.4.Configuración de las subredes VLAN.....	32
3.4.1.5.Asociar las VLANs al puerto.....	32
3.4.1.6.Crear un Perfil de Configuración para los Puntos de Acceso.....	33
3.4.1.7.Incluir los Puntos de Acceso al perfil de la Controladora.....	36
3.4.1.8.Configuración Manual de los Puntos de Acceso.....	37
3.4.1.9.Configuración del Servidor Externo RADIUS.....	38
3.4.1.10.Configuración del Portal Cautivo.....	39
3.4.2.Configuración del Switch DES-1210-28P.....	42
3.4.2.1.Configuración de las VLANs.....	43
3.4.3.Configuración del Router de Internet.....	45
3.4.4.Instalación y Configuración del Servidor RADIUS.....	46
3.4.4.1.Instalación de FreeRADIUS.....	46
3.4.4.2.Configuración de FreeRADIUS.....	47
4.CONCLUSIONES.....	49
5.BIBLIOGRAFÍA Y REFERENCIAS.....	50

Índice de Ilustraciones

Ilustración 1: Comparativa celdas norma 802.11g vs 802.11n.....	10
Ilustración 2: Nivel de Señal Quinta Planta.....	15
Ilustración 3: Nivel de Señal Cuarta Planta.....	16
Ilustración 4: Nivel de Señal Tercera Planta.....	17
Ilustración 5: Nivel de Señal Segunda Planta.....	18
Ilustración 6: Nivel de Señal Primera Planta.....	19
Ilustración 7: Nivel de Señal Planta Baja.....	20
Ilustración 8: Controladora de red Inalámbrica DWC-1000.....	22
Ilustración 9: Punto de Acceso Unificado DWL-2600AP.....	23
Ilustración 10: Switch DES-1210-28P.....	24
Ilustración 11: Esquema de Red Cableada.....	26
Ilustración 12: Armario Rack con Controlador WiFi y Switch PoE.....	27
Ilustración 13: Puntos de Acceso DWL-2600AP.....	27
Ilustración 14: Escenario Resumen del Sistema.....	28
Ilustración 15: Login Interface de Gestión Web.....	29
Ilustración 16: Disposición Menús del Interface de Gestión Web.....	30
Ilustración 17: LAN Setup del DWC-1000.....	30
Ilustración 18: Option 1 Setup.....	31
Ilustración 19: Lista de VLANs disponibles.....	31
Ilustración 20: Múltiple subredes VLANs.....	32
Ilustración 21: Configuración Subred VLAN 2 Profesores.....	32
Ilustración 22: Configuración del puerto como miembro VLAN1, 2 y 3.....	33
Ilustración 23: Creación de un nuevo Perfil.....	33
Ilustración 24: Configuración SSID "Profesores".....	34
Ilustración 25: Configuración SSID "Alumnos".....	34
Ilustración 26: Configuración Parámetros Radio de los AP (1/2).....	35
Ilustración 27: Configuración Parámetros Radio de los AP (2/2).....	35
Ilustración 28: Lista de APs detectadas y pendientes de gestionar.....	36
Ilustración 29: Configuración de nuevo Punto de Acceso al Perfil.....	36
Ilustración 30: Lista de todos los APs Gestionados.....	37
Ilustración 31: Configuración Manual de los APs.....	37
Ilustración 32: Configuración Manual del Canal y de la Potencia.....	38
Ilustración 33: Configuración del Servidor RADIUS.....	38
Ilustración 34: Chequeo de los Servidores RADIUS.....	39
Ilustración 35: Listado de los Grupos de Usuarios.....	39
Ilustración 36: Configuración de un nuevo Grupo.....	40
Ilustración 37: Importación de Usuarios mediante fichero CSV.....	40
Ilustración 38: Configuración de un Usuario del Portal Cautivo.....	41
Ilustración 39: Portal Cautivo Alumnos.....	41
Ilustración 40: Configurar Portal Cautivo en SSID.....	42
Ilustración 41: Opciones del Portal Cautivo en el SSID.....	42
Ilustración 42: Acceso Web al Switch.....	43
Ilustración 43: Configuración IP del Switch.....	43
Ilustración 44: Configuración VLANs Asimétricas.....	44
Ilustración 45: VLAN Profesores.....	44
Ilustración 46: VLAN Alumnos.....	45
Ilustración 47: Rutas Estáticas en el Router de Internet.....	45
Ilustración 48: Versión de Ubuntu utilizada y características del PC.....	46
Ilustración 49: Prueba exitosa a nivel local del FreeRADIUS.....	48

1. Introducción y Objetivos

1.1. Introducción

Desde hace ya algunos años atrás es evidente la irrupción de las nuevas tecnologías en prácticamente todos los ámbitos, en especial en la educación, que es el caso que nos atañe. El uso tan creciente de dichas tecnologías no se podría concebir sin un acceso a Internet, tanto para ordenadores como para otra inmensidad de dispositivos portátiles que tan necesarios son hoy en día en un entorno educativo.

En nuestra área, los profesores vemos en estos nuevos avances tecnológicos herramientas y posibilidades que mejoran la experiencia de la enseñanza. El termino movilidad se aplica, principalmente, a las ventajas que ofrecen los dispositivos móviles (smartphones o teléfonos móviles, notebooks y tabletas) permitiendo desde cualquier sitio poder interactuar con alumnos o familias, realizar trabajos, disponer de la información en soporte digital del centro o acceder a multitud de recursos didácticos gracias a Internet.

La enseñanza en el aula se ha modernizado con herramientas como ordenadores, pizarras electrónicas, proyectores, tablets, etc. Por ejemplo, el uso de tablets en el aula, tanto si se trata de un iPad o de una tableta Android, se pueden conectar por una red wifi a un ordenador que proyecte su contenido. Este sistema ofrece muchas opciones al profesor, entre las cuales están el tener la libertad de desplazarse por el aula mientras imparte la lección o mostrar recursos didácticos como ilustraciones, anotaciones, esquemas, gráficos, vídeos, etc.

1.2. Datos del centro

El Colegio Nuestra Señora de Fátima está situado en C/Jumilla nº6 de Valencia, muy cerca del Hospital General. El edificio consta de planta baja y cinco pisos con una superficie de 4.179 metros cuadrados. Además de las aulas, el Centro posee también laboratorios, biblioteca, salón de actos, diferentes despachos, talleres de tecnología y música, gimnasio, comedor y otras dependencias destinadas a Dirección, Jefatura de Estudios, Administración, Secretaría y Conserjería.

Referente al alumnado, el centro dispone de 12 unidades de Educación Primaria, con 300 puestos escolares, 8 unidades de Educación Secundaria Obligatoria, con 240 puestos, y 4 unidades de Bachillerato, con 130 puestos. Sumando a este alumnado un número aproximado de 70 docentes, hace un total de 740 personas que normalmente frecuentan las instalaciones.

1.3. Justificación y objetivos

La necesidad de dotar al centro de una red inalámbrica de calidad, viene por lo comentado en la introducción y por ofrecer a las familias y al alumnado de un valor añadido, entre los mas importantes, el uso del libro digital en las aulas y el de un sistema de gestión docente accesible vía web.

Durante en curso 2013-2014, la dirección y todo el claustro de profesores decidieron empezar a utilizar el libro digital en el mayor número de asignaturas posible, ya que las familias llevan varios años quejándose del alto precio que tienen que desembolsar al comienzo de cada curso. Además, el colegio llevaba utilizando desde hace mucho tiempo un sistema de gestión docente

y de comunicación con las familias muy precario y nada interactivo. Así que se decidió también empezar a utilizar para el curso 2014-2015 una nueva plataforma *online* (Clickedu) que permitiese centralizar todas las gestiones (académica, administrativa, interacción familias, base de datos, etc) de forma flexible y accesible desde cualquier dispositivo conectado a Internet.

El principal problema radicaba en que no se disponía de prácticamente nada de cobertura WiFi ni de una buena conexión a Internet en el centro. Solo existían tres o cuatro puntos de acceso, de nivel doméstico, que, simplemente, cubrían las salas de profesores, algunos despachos y el aula de informática. Además, la salida a Internet era mediante una conexión ADSL convencional, de 12 a 15 Mbps.

Se decidió pedir ayuda profesional de empresas del sector, pero los costes triplicaban o cuadruplicaban el presupuesto del que disponía el colegio para ello. Por lo tanto, dirección solicitó la colaboración del profesorado cualificado para que estudiaran una alternativa posible para dotar al centro de tal infraestructura.

De este modo, se estudiaron varias posibilidades con el fin de elegir una solución no tan costosa pero que cumpliera ciertas funcionalidades esenciales, como son las siguientes:

- Cobertura. Dar cobertura a toda aquella zona del centro utilizada por el alumnado, personal docente y de administración, con fines académicos y laborales, respectivamente.
- Velocidad. Ofrecer una velocidad de transmisión de calidad por usuario adecuada a la posible demanda actual.
- Escalabilidad. Poder ampliar el sistema en un futuro, tanto en velocidad como en un aumento de número de usuarios o accesos.
- Seguridad y Fiabilidad. Utilizar un sistema seguro y fiable.
- Gestión Centralizada. Gestionar de forma centralizada todos los puntos de acceso, usuarios, cortafuegos, niveles de acceso, filtros, etc.
- Adaptabilidad. Adaptar y conectar la nueva red a la red local ethernet existente.

2. Estado del arte

2.1. Diseño de una red inalámbrica

Antes de entrar de lleno en la descripción de la red inalámbrica, conviene tener una visión general de los aspectos que hay que tener en cuenta en un diseño e implantación de un proyecto y qué posibilidades y opciones nos podemos encontrar.

Un proyecto de red inalámbrica tiene dos partes bien diferenciadas. Por un lado, hay que abordar todo lo referente al aspecto de radiocomunicaciones y, por otro, todo lo que tiene que ver con la parte telemática. Una vez seleccionada la banda de frecuencias y el estándar utilizado, se tiene el número de canales disponibles y se pueden calcular el número de puntos de acceso que se necesiten para dar servicio. Este número dependerá del área a cubrir y del número de usuarios. Un estudio detallado de la propagación verificará si existen zonas de sombra y si las antenas utilizadas son las adecuadas. Habrá que pensar también si se desea tener *roaming* dentro de la red y asignar la velocidad de transmisión dentro de las posibilidades del estándar. Por otro lado, una vez emplazados los puntos de acceso, es necesario diseñar la

arquitectura de la red cableada (red de distribución) para dar conexión de salida a Internet o comunicación con la LAN existente. También hay que tener en cuenta aspectos tales como la segmentación, la autenticación, la seguridad de la transmisión y la elección de permisos a los posibles usuarios. Se pueden distinguir de forma resumida los siguientes aspectos:

Radiocomunicación:

- Número de canales y su planificación.
- Estimación de demanda de tráfico.
- Cálculo del número de puntos de acceso y radios de cobertura.
- Estudio de propagación.
- Necesidad de *roaming*.
- Asignación de velocidades de transmisión.

Telemática:

- Cableado y conexión al router principal.
- Segmentación mediante VLANs.
- Método de asignación de direcciones IP.
- Seguridad, autenticación, permisos, etc.

Es importante destacar que, en una red Wi-Fi, sin un adecuado diseño, sin una debida planificación de recursos, sin una cuidada instalación y sin unos protocolos de pruebas adecuados puede provocar [1]:

- Problemas de interferencias con otras redes que usen ese mismo estándar o con otros equipos y sistemas que trabajen en esas bandas de frecuencias.
- Al utilizar una banda de frecuencias de uso común, dificultades de protección frente a redes “concurrentes” u otras (incluyendo hornos de microondas) que empleen las mismas frecuencias.
- Falta de cobertura, o cobertura inadecuada, como consecuencia de un mal diseño de la red WiFi con respecto al entorno donde va a ser utilizada.
- Un aumento de las complejidades técnicas y del coste final de la red si se realiza una inadecuada elección en el número y posición de los puntos de acceso.
- Problemas de calidad del servicio como resultado de un inadecuado dimensionamiento de la capacidad de la red. Nominalmente, la velocidad de Wi-Fi es de 11 Mbps (de 4 a 7 Mbps en la práctica) en el caso del estándar 802.11b y, de 54 Mbps para 802.11a y 802.11g, pero esto disminuye según la distancia al punto de acceso (1 Mbps en las zonas límite de cobertura)
- Problemas o falta de seguridad en la red y, por tanto, posible intrusión de usuarios no autorizados que hacen uso de los recursos de red o acceden ilegalmente a la información.
- Falta de flexibilidad de la red para irse adecuando al número y perfil de usuarios que se incorporan al servicio en un futuro.
- Problemas de movilidad debido a una escasa o nula valoración de los procesos de itinerancia y traspaso.
- Problemas con el tránsito a nuevas aplicaciones y servicios por un inadecuado diseño de la red.

Tras este minucioso estudio y adaptándose siempre a las propias posibilidades, se podrá elaborar una memoria del proyecto incluyendo planos descriptivos, realizar un esquema o topología de la red y elegir el material y los dispositivos necesarios para tal fin. Después de esto, ya se podrán adquirir aquellos equipos (puntos de acceso, concentradores, controladora, etc) que se ajusten a las necesidades y solicitar uno o varios presupuestos referentes a la instalación del cableado estructurado.

Antes de adentrarse en el proyecto en sí, parece razonable dedicar unos apartados al aspecto de radiocomunicaciones y del estándar IEEE 802.11, ya que la elección de una norma u otra conlleva el uso de una banda de frecuencia saturada en el espectro u otra más libre pero con otra serie de inconvenientes a tener en cuenta.

2.2. Estándar IEE 802.11

IEEE 802.11 es un estándar para redes inalámbricas definido por el Institute of Electrical and Electronics Engineers (IEEE). Se trata de un instituto de investigación y desarrollo, de gran reconocimiento y prestigio, cuyos miembros pertenecen a decenas de países entre profesores y profesionales de las nuevas tecnologías [2].

El estándar IEEE 802.11 es un estándar en continua evolución, debido a que existen muchos grupos de investigación, trabajando en paralelo para mejorar el estándar, a partir de las especificaciones originales. Dentro del estándar hay definidos una serie de variantes que se resumen a continuación [3]:

2.2.1. Norma 802.11b

La norma 802.11b trabaja en la banda de 2,4 GHz y permite obtener una velocidad de hasta 11 Mbps. Surgió como una evolución de la 802.11 en el año 1999, con el objetivo de solventar el problema de velocidad que esta presentaba. Con la adopción de esta nueva norma se popularizaron las redes Wi-Fi pues la velocidad que ofrece, aun estando lejos de la red cableada, la hace apta para los usos más comunes. Añadido a esto, los costes de fabricación disminuyeron y los equipos fueron asequibles para un gran número de empresas y particulares.

2.2.2. Norma 802.11a

La norma 802.11a define el funcionamiento de equipos en la banda de 5 GHz, permitiendo velocidades de hasta 54 Mbps. Fue aprobada el mismo año que la norma 802.11b pero, a pesar de las ventajas de la tecnología debido a la banda de frecuencia utilizada, su adopción ha sido muy lenta, y en nuestro país casi nula debido a varios problemas. En un principio la calidad de lo sistemas 802.11a presentó problemas en cuanto a fiabilidad, lo cual junto a un precio elevado debido al mayor coste y dificultad de fabricación de los elementos necesarios para construir estos sistemas, retrasó su implantación en un primer momento.

2.2.3. Norma 802.11g

La norma 802.11g fue aprobada en el año 2003. Se trata de una tecnología que opera en la banda de los 2,4 GHz y proporciona una velocidad máxima de 54 Mbps. La principal ventaja de esta tecnología reside en la mayor velocidad aportada y la compatibilidad con la base de equipos Wi-Fi conformes a la norma 802.11b ya instalados.

Es de mencionar, que si la red Wi-Fi se compone de varias celdas, aunque tan solo una de ellas tenga clientes 802.11b, todos los puntos de acceso funcionarán en modo compatible b/g pues los clientes pueden tener movilidad y pasar de la zona de cobertura de un punto de acceso al adyacente, lo cual provocara un menor rendimiento en toda la red, no solo en la celda con clientes 802.11b. Es por estas razones por lo que resulta recomendable evitar en la medida de lo posible el modo de compatibilidad b/g y fijar el modo puro 802.11g si en la red no se ha de dar servicio a clientes 802.11b.

2.2.4. Norma 802.11n

La norma 802.11n fue publicada en el año 2007, con el objeto de dar mayor velocidad que las existentes hasta el momento, pasando de 54 Mbps a unos teóricos 600 Mbps. Ofrece la posibilidad de funcionar en ambas bandas, tanto en 2,4 GHz como en 5 GHz. Una de las grandes ventajas de la nueva norma es la compatibilidad con las normas anteriores lo cual posibilita la integración de sistemas nuevos en redes ya existentes y una migración sencilla y económica.

Actualmente hay una gran oferta de sistemas con posibilidades de conexión Wi-Fi 802.11n en 2,4 GHz, pero pocos que soporten la banda de 5 GHz o proporcione conexión dual. El menor coste y la compatibilidad con los sistemas Wi-Fi anteriores que funcionan en la banda de 2,4 GHz causo esta tendencia del mercado. Para conseguir esta mayor velocidad, los equipos 802.11n siguen dos estrategias: un mayor ancho de banda del canal y uso de la tecnología MIMO con división por multiplexación espacial (SDM).

El ancho de banda que ocupa un canal en 802.11n pasa de los 20 MHz que ocupaban los sistemas anteriores, a 40 MHz. Esto no es un problema en 5GHz, donde los canales no se solapaban, pero en 2,4 GHz, un canal de 40 MHz ocupa el 82% de la banda disponible. Esto implica que no podrán coexistir dos canales 802.11n sin solapamiento en 2,4 GHz y que este solapamiento abarcará además la mayoría del canal. Incluso con sistemas Wi-Fi de otras normas o equipos no Wi-Fi que emitan en esta frecuencia (como Bluetooth, teléfonos inalámbricos,...) el espectro libre será mínimo, quedando casi asegurada la interferencia con el resto de sistemas.

2.3. Ventajas e inconvenientes entre la banda de 2,4GHz y 5GHz

Vista la diferencia entre las diferentes normas del estándar IEEE 802.11, se puede decir que a pesar de que las redes de 5GHz ya llevan bastantes años usando la norma 802.11a, son las redes de 2.4GHz con estándar 802.11b/g las que gozan de mayor popularidad entre los usuarios, en parte porque los equipos de 5GHz siempre han sido más caros de implantar [4].

Esta es la razón por la que durante años la gran mayoría de redes inalámbricas se han ido creando bajo la frecuencia de 2.4GHz. Pero, es a partir del crecimiento exponencial de antenas Wi-Fi en áreas urbanas con elevada densidad de población cuando empiezan a surgir problemas de conflictos e interferencias en la red inalámbrica. Si se tiene en cuenta que otras tecnologías como teléfonos móviles, ratones inalámbricos, bluetooth o microondas comparten también el mismo espectro, la situación se complica con la irremediable reducción de la velocidad y la saturación de la red inalámbrica.

Por el contrario, las redes de 5GHz operan en un espectro mucho más amplio, con mayor número de canales no compartidos con ninguna otra red y que pueden ser combinados a mayor

velocidad. Mientras que la banda completa de las Wi-Fi de 2.4GHz solo tiene 80MHz de ancho de banda, en las de 5GHz cada canal tiene 20MHz, lo que garantiza mayor velocidad. Estas ventajas han hecho que poco a poco se incremente su popularidad entre los usuarios, frente a los continuos problemas de saturación de las redes de 2.4GHz.

Sin embargo, el paso hacia la frecuencia 5 GHz tiene también algunas desventajas que conviene saber. La principal desventaja afecta al rango, es decir, cuanto más alta es la frecuencia de la señal Wi-Fi menor es el rango que cubre. Justo lo contrario a lo que ocurre con la frecuencia 2.4GHz. Otro aspecto importante a tener en cuenta son los problemas de las redes 5GHz a traspasar objetos sólidos, lo que limita el uso de estas redes en el interior de domicilios donde la señal tenga que atravesar varios tabiques. Además la cobertura de un punto de acceso 802.11n es más irregular que la cobertura de los puntos de acceso basados en 802.11 a/b/g. Esto puede dar lugar a agujeros de cobertura más alto y, posiblemente, interferencias en el mismo canal [5].



Ilustración 1: Comparativa celdas norma 802.11g vs 802.11n.

3. Diseño y Configuración

3.1. Estándar y banda de frecuencia idónea para el centro

Se puede sacar como conclusión, que el colegio Nuestra Señora de Fátima está ubicado en una zona rodeada de viviendas, por lo que es fácil presuponer que el espectro de la banda de los 2,4GHz estará saturada. Pero también es verdad que los inconvenientes que se acaban de describir de las redes de 5GHz no es favorable, ya que justamente el edificio tiene un elevado número de gruesos tabiques (antiguos) destinados a dividir todas las aulas y despachos del centro. Interesa, económicamente hablando, utilizar el menor número de puntos de acceso posible, por lo que habría que ubicarlos en una zona común para que ofrezca cobertura a varias aulas a la vez. Pero también habría que pensar en un sistema flexible y compatible con la banda de los 5GHz ya que en un futuro se podría plantear el instalar un punto de acceso dentro de cada estancia.

3.2. Dimensionado y planificación del sistema

Una vez justificado que la banda de frecuencia que se va a utilizar del estándar IEEE 802.11, es el 802.11g, el cual ofrece una velocidad máxima de 54 Mbps; se procede a determinar el número total de puntos de acceso (AP's) necesarios para satisfacer las propias necesidades. Como ya se ha comentado, este número dependerá del número de usuarios y del área a cubrir.

3.2.1. Cálculo del número de AP's basado en la capacidad

Hay que pensar que si se quiere ofrecer un valor añadido, la capacidad del sistema debería ofrecer a cada usuario potencial, una tasa de transferencia mínima de 1 Mbps. Es por ello, que

para determinar la capacidad total necesaria en la red, será necesario estimar el número de posibles usuarios existentes, conectados a la vez, en cada una de las plantas del edificio.

El número de puntos de acceso que aquí se determinan, no sería en principio el número de puntos de acceso definitivo, ya que podría ser necesaria una cantidad superior de puntos de acceso para cubrir posibles zonas sin cobertura. En este caso, el número de puntos de acceso vendrían impuestos por el estudio de cobertura.

Para llevar a cabo dicho análisis se debe tener en cuenta los siguientes parámetros de partida [1]:

- **Ce:** Capacidad efectiva de un punto de acceso. De los 54 Mbps totales 22 Mbps son los efectivos para la transmisión y recepción de datos. Esto es debido a que la comunicación es half-dúplex y que difícilmente tendremos un nivel de potencia superior a -30 dBm [6].
- **N:** Número máximo de usuarios potenciales por cada planta.
- **Fs:** Factor de simultaneidad. Número máximo de usuarios que están usando la red inalámbrica simultáneamente. Se utilizará un factor de simultaneidad del 30%, para las zonas concretas en las que un alto número de usuarios, necesitan acceder a la red en el mismo instante y un factor de simultaneidad del 20% para el resto de usuarios.
- **Cg:** Capacidad garantizada por usuario. Tasa de transferencia mínima que se le garantiza a un usuario en el caso de que F sea máximo. En nuestro caso tomaremos 1 Mbps.
- **Fe:** Factor de escalabilidad. Debido a un previsible aumento de la demanda de usuarios conectados a la red, se utilizará un factor de escalabilidad del 10%.
- **C:** Capacidad necesaria por cada planta.

A continuación se calcula el número de puntos de acceso necesarios en cada planta:

3.2.1.1. Quinta planta

- 4 Aulas de Bachillerato con una media de 30 alumnos por aula
- Aula de Música y taller de tecnología (dependiendo del horario) unos 30 alumnos.
 - $N = 30 + (4 \cdot 30) = 150$ usuarios
- Se supone un factor de simultaneidad alto ya que los alumnos de Bachillerato son los que más utilizarán la red.
 - $C = N \cdot F_s \cdot C_g = 150 \cdot 0,3 \cdot 1 = 45$ Mbps
- Por tanto, asumiendo el factor de escalabilidad y que el reparto de carga entre puntos de acceso es equilibrado, son necesarios:
 - $C \cdot F_e / C_e = 45 \cdot 1,1 / 22 = 2,25$ (3 PUNTOS DE ACCESO)

3.2.1.2. Cuarta planta

- 1 Aula de Bachillerato y 3 de 4º de ESO con una media de 25 alumnos por aula
- Salón de actos, Sala de Profesores y Despachos hacen un total de posibles 20 usuarios.
 - $N = 20 + (4 \cdot 25) = 130$ usuarios
- Se supone un factor de simultaneidad alto ya que los Profesores y alumnos de Bachillerato y 4º de ESO son de los que más utilizarán la red.
 - $C = N \cdot F \cdot C_g = 130 \cdot 0,3 \cdot 1 = 39$ Mbps
- Por tanto, asumiendo el factor de escalabilidad y que el reparto de carga entre puntos de acceso es equilibrado, son necesarios:
 - $C \cdot F_e / C_e = 39 \cdot 1,1 / 22 = 1,95$ (2 PUNTOS DE ACCESO)

3.2.1.3. Tercera planta

- 6 Aulas de 1º, 2º y 3º de ESO con una media de 25 alumnos por aula
- Aula de Informática con sólo 20 puestos, pero ya tienen red LAN y no suelen utilizar la WiFi, pero se tiene en cuenta para un futuro.
 - $N = 20 + (6 \cdot 25) = 170$ usuarios
- Se supone un factor de simultaneidad bajo ya que los alumnos de primer ciclo de ESO aun no demandan un uso de la red inalámbrica.
 - $C = N \cdot F \cdot C_g = 170 \cdot 0,2 \cdot 1 = 34$ Mbps
- Por tanto, asumiendo el factor de escalabilidad y que el reparto de carga entre puntos de acceso es equilibrado, son necesarios:
 - $C \cdot Fe / Ce = 34 \cdot 1,1 / 22 = 1,70$ (2 PUNTOS DE ACCESO)

3.2.1.4. Segunda planta

- 6 Aulas de Primaria donde solo están utilizando Internet los profesores, así que se contabiliza un total de 12 posibles usuarios.
 - $N = 12$ usuarios
- Se supone un factor de simultaneidad alto ya que los profesores necesitan estar siempre conectados.
 - $C = N \cdot F \cdot C_g = 12 \cdot 0,3 \cdot 1 = 3,6$ Mbps
- Por tanto, asumiendo el factor de escalabilidad y que el reparto de carga entre puntos de acceso es equilibrado, son necesarios:
 - $C \cdot Fe / Ce = 3,6 \cdot 1,1 / 22 = 0,18$ (1 PUNTO DE ACCESO)

3.2.1.5. Primera planta

- 6 Aulas de Primaria donde solo están utilizando Internet los profesores, así que se contabiliza un total de 12 posibles usuarios.
- Sala de Profesores de Primaria, Despachos, Gabinete y Escuela de Música pueden llegar a 20 usuarios más
 - $N = 12 + 20 = 32$ usuarios
- Se supone un factor de simultaneidad alto ya que los profesores necesitan estar siempre conectados tanto en el aula como en despachos y sala.
 - $C = N \cdot F \cdot C_g = 32 \cdot 0,3 \cdot 1 = 9,6$ Mbps
- Por tanto, asumiendo el factor de escalabilidad y que el reparto de carga entre puntos de acceso es equilibrado, son necesarios:
 - $C \cdot Fe / Ce = 9,6 \cdot 1,1 / 22 = 0,48$ (1 PUNTO DE ACCESO)

3.2.1.6. Planta Baja

- Aulas de Infantil, Biblioteca, Gimnasio, Comedor, Secretaría y Conserjería podrían hacer un total de 60 usuarios en determinados momentos.
 - $N = 60$ usuarios
- Suponiendo un factor de simultaneidad alto:
 - $C = N \cdot F \cdot C_g = 60 \cdot 0,3 \cdot 1 = 18$ Mbps
- Por tanto, asumiendo el factor de escalabilidad y que el reparto de carga entre puntos de acceso es equilibrado, son necesarios:
 - $C \cdot Fe / Ce = 18 \cdot 1,1 / 22 = 0,90$ (1 PUNTO DE ACCESO)

3.2.2. Cálculo del número de AP's basado en la cobertura

3.2.2.1. Estudio de cobertura previo

Tras realizar in-situ un análisis del edificio y de sus planos, se aprecia que en determinadas plantas, las áreas a cubrir con respecto al número de puntos de acceso anteriormente calculado no son suficientes. Es por ello, que para ofrecer un nivel de potencia mínimo (establecido en unos -75dBm) y dotar a la red de *roaming* (solapamiento mínimo entre puntos de acceso adyacentes), se prevé el aumentar el número de puntos de acceso en algunas zonas para evitar pérdidas de señal o desconexiones de la red a aquellos usuarios que deseen desplazarse por el edificio.

Teniendo en cuenta estas consideraciones y con la intención de determinar la ubicación óptima de los puntos de acceso, es aconsejable evaluar la idoneidad de dichas ubicaciones mediante la utilización de alguna de las numerosas herramientas software profesionales que existen en el mercado. Estas ofrecen, además de la parametrización de los equipos empleados, la importación de planos para determinar así dicha ubicación mediante una simulación del entorno. Sin embargo, dichas herramientas tienen un alto coste, tanto software como hardware, y muchas veces, sus resultados no son del todo fehacientes, ya que los datos que se introducen para su simulación y cálculo (diagrama de radiación de las antenas, grosor y tipo de material de paredes, ventanas y puertas, etc.) difícilmente son conocidos con exactitud, y por lo tanto, el resultado obtenido del mismo puede ser inexacto.

Por tanto, según lo comentado y con la intención de minimizar costes al centro, se decide en este caso seguir un proceso iterativo, mediante el cual se ubican los puntos de acceso temporalmente y se verifica si se cumplen todos los requisitos (nivel de señal, ancho de banda, etc.), en caso negativo, se realiza un cambio de ubicación hasta que el resultado es totalmente satisfactorio. No obstante, el número y ubicación definitiva de los puntos de acceso viene determinada por un estudio posterior más exhaustivo.

3.2.2.2. Estudio de cobertura posterior

Por último, para determinar el número de Puntos de Acceso (AP's) definitivo, que por cobertura, cubrirá todas las zonas requeridas por el centro, es necesario un estudio más minucioso de la red inalámbrica al completo, es decir, un estudio de todos los AP's emitiendo a la vez. De esta manera se podrá asegurar, además del rendimiento de la red, la existencia de solapamiento entre AP's adyacentes suficiente para que se produzca *roaming*, la localización de zonas de baja cobertura o la existencia de áreas de una planta cubiertas por AP's de plantas vecinas con el fin de ver reducido el número total de AP's definitivo.

Para realizar dicho estudio, se decide utilizar un aplicación gratuita pero muy potente para la recogida y visualización de datos Wi-Fi, denominado *TamoGraph Site Survey* en modo evaluación. Dicha versión de prueba permite utilizar el software durante 30 días pero con algunas limitaciones como: inclusión de marcas de agua en las visualizaciones, restricción en el guardado de proyectos o la limitación en la recogida de datos en los estudios de cobertura de más de diez minutos.

Para realizar el estudio se utiliza un equipo portátil con las siguientes características:

- Portátil: Sony Vaio PCG-4T1M
- Sistema Operativo: Windows XP

- Tarjeta de red inalámbrica: Atheros AR9285 (compatible con la versión del software)
- Software: TamoGraph Site Survey, versión 4.0

Una vez instalada y configurada la aplicación, el modo utilizado para la recogida de los datos, es el de estudio pasivo. Durante este estudio, la aplicación recoge los datos más completos sobre el entorno de radiofrecuencia de los puntos de acceso y sus características, intensidad de la señal, el nivel de ruido, interferencias, etc. Se llama pasivo porque durante este tipo de estudio, la aplicación escucha pasivamente a los paquetes y no intenta conectarse a las redes inalámbricas detectadas.

Después de cargar y calibrar el plano de la planta a estudiar, portátil en mano y con la batería cargada, se procede a la recopilación de datos, de forma que una vez iniciado el estudio, se le indica a la aplicación periódicamente nuestra ubicación en el plano mientras nos desplazamos por la planta. Dicho recorrido debe de estar previamente planificado para perder el menor tiempo posible y para evitar encontrarnos con estancias cerradas.

Los resultados por plantas obtenidos de dicho estudio muestran el nivel de potencia de la señal en dBm mediante un mapa de calor superpuesto al plano de la planta. Los colores representados fuera del edificio o de los lugares no barridos durante la recopilación de datos, son extrapolados por la aplicación teniendo en cuenta la distancia y las características de los obstáculos (paredes y ventanas) introducidos en la aplicación para tal fin.

Señalar también, que los Puntos de Acceso son localizados por la propia aplicación automáticamente al indicar que se quiere analizar la señal procedente de solamente esta red. En la tabla siguiente se pueden ver los nombres utilizados de los AP's analizados. Estos aparecen en las ilustraciones de la propia planta y de la inmediatamente inferior, ya que en muchos casos son determinantes para cubrir las áreas requeridas en dicha planta.

Plantas	Nombre de los AP's
Quinta	AP5-1, AP5-2 y AP5-3
Cuarta	AP4-1 y AP4-2
Tercera	AP3-1 y AP3-2
Segunda	AP2
Primera	AP1-1, AP1-2 y AP1-3
Baja	APB

Tabla 1: Nombre de AP's por plantas

A continuación se muestran las ilustraciones de las seis plantas analizadas y unas observaciones sobre los resultados obtenidos:

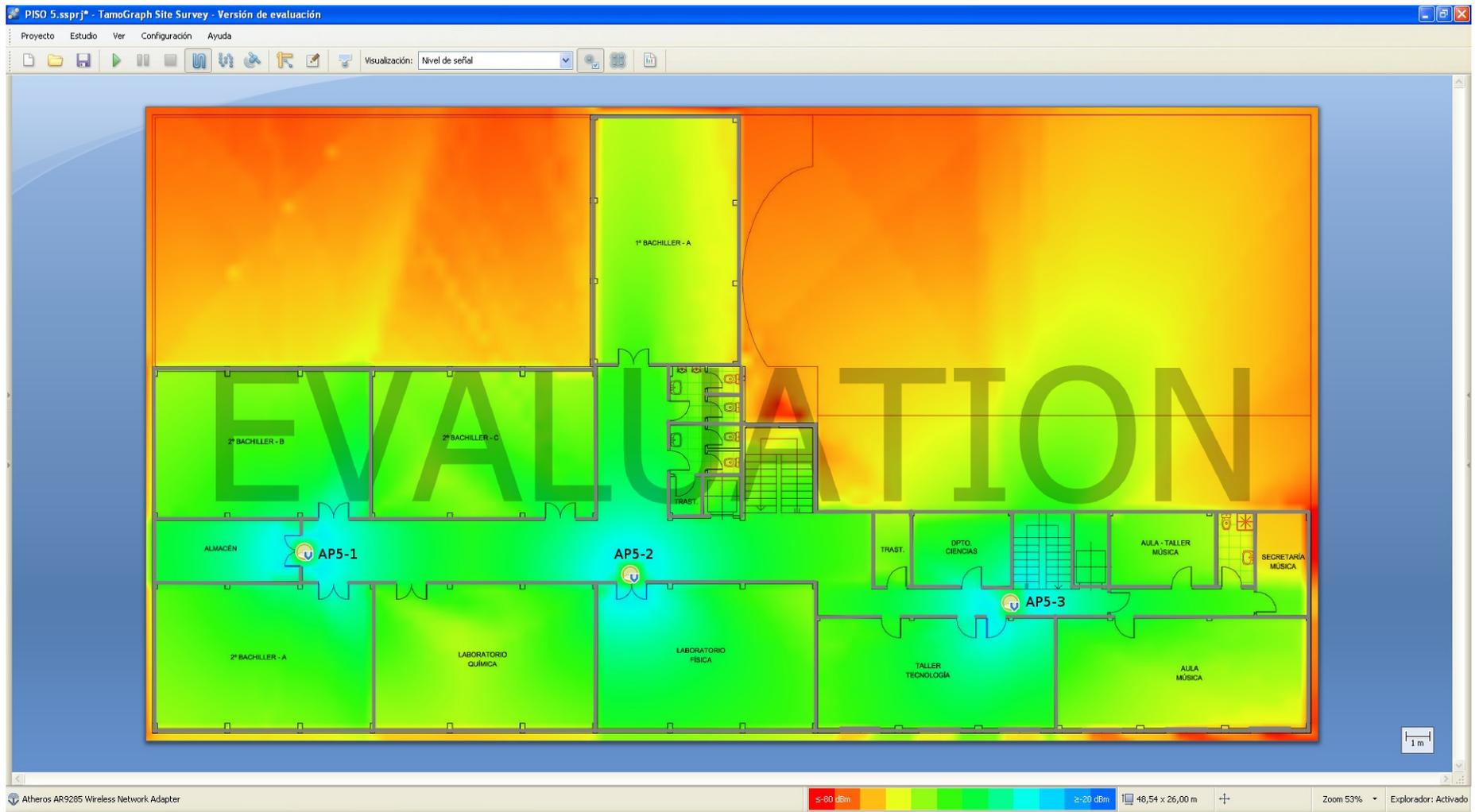


Ilustración 2: Nivel de Señal Quinta Planta

Observaciones: Todas las Aulas, Laboratorios, Talleres y Despachos reciben un buen nivel de señal de los tres AP's.

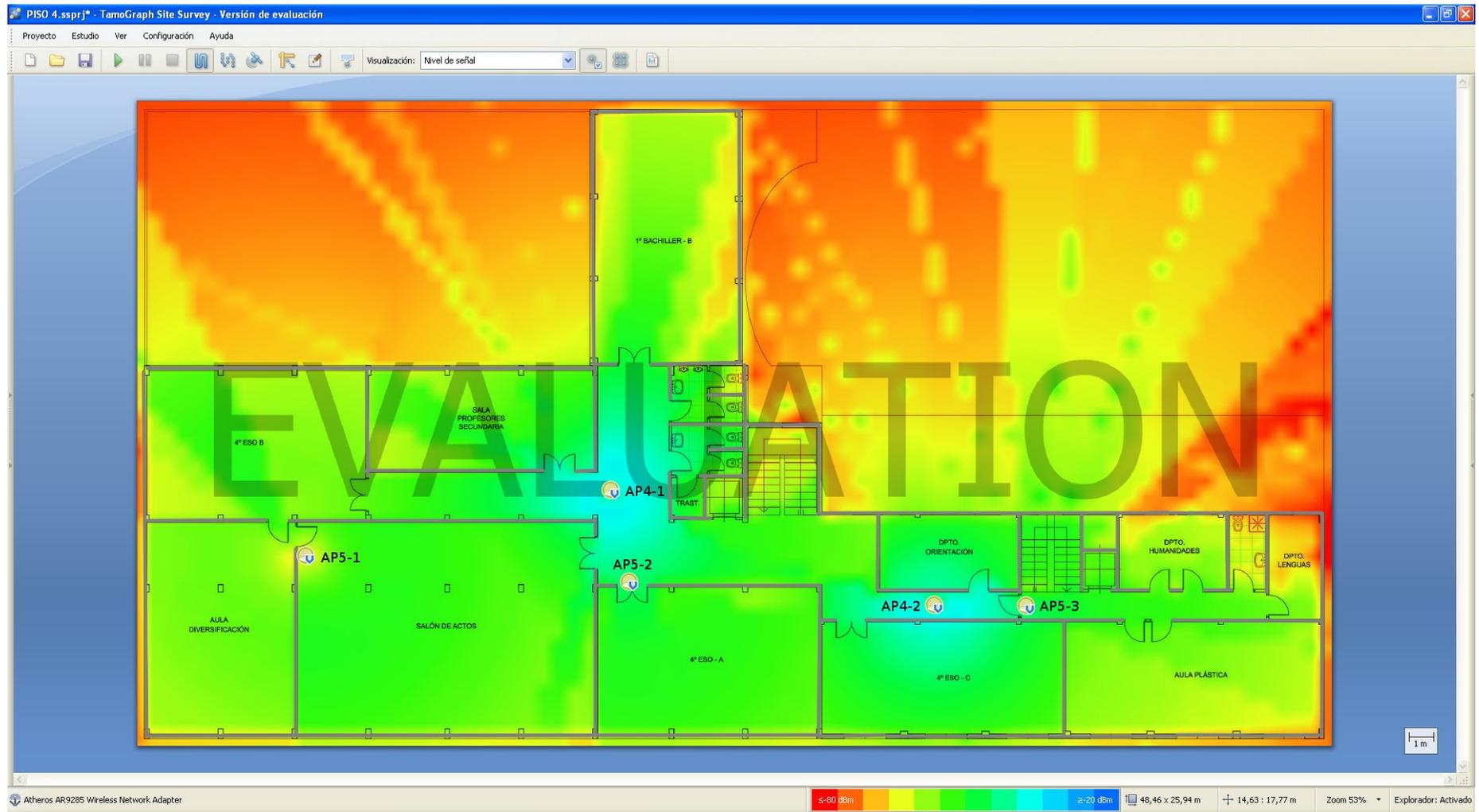


Ilustración 3: Nivel de Señal Cuarta Planta

Observaciones: En esta planta hay Aulas donde los usuarios se conectarían a los AP's de la planta superior. Se aprecian pequeñas zonas donde el nivel de cobertura está casi al mínimo.

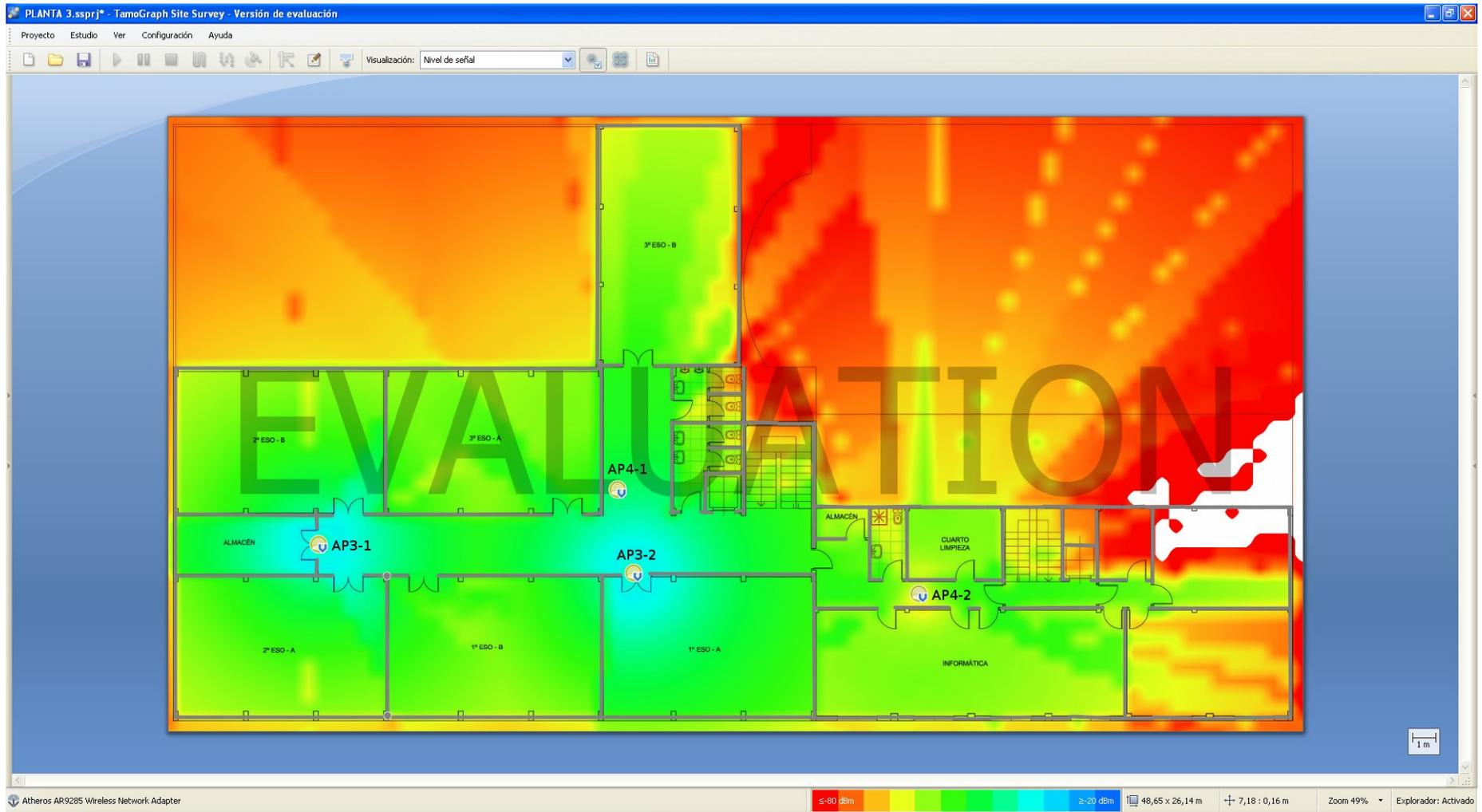


Ilustración 4: Nivel de Señal Tercera Planta

Observaciones: Todas las Aulas reciben una buena cobertura de los dos AP's ubicados en esta planta. El Aula de Informática recibe la señal del AP de la cuarta planta. Las estancias de más a la derecha no necesitan señal porque no se utilizan para fines docentes o educativos.

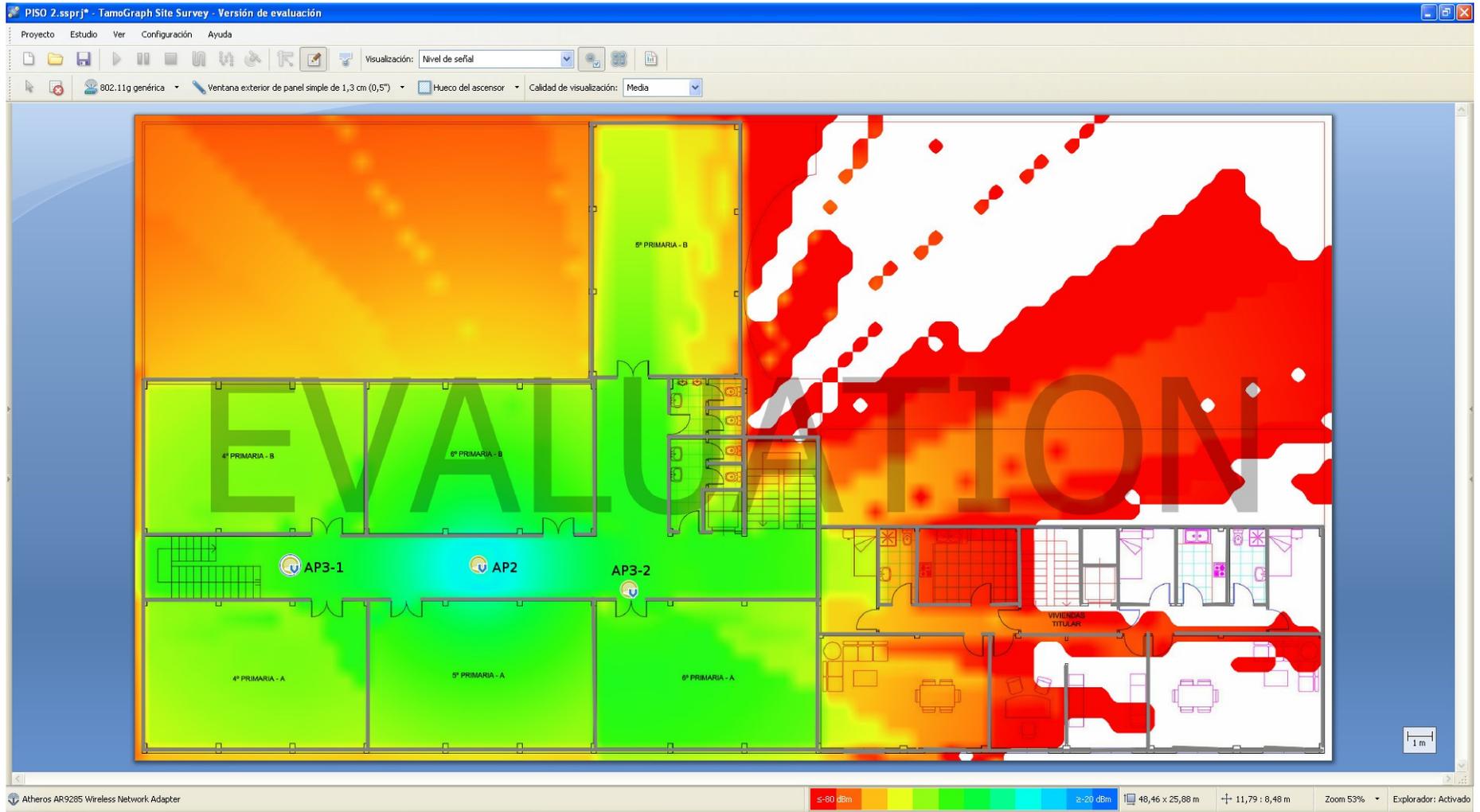
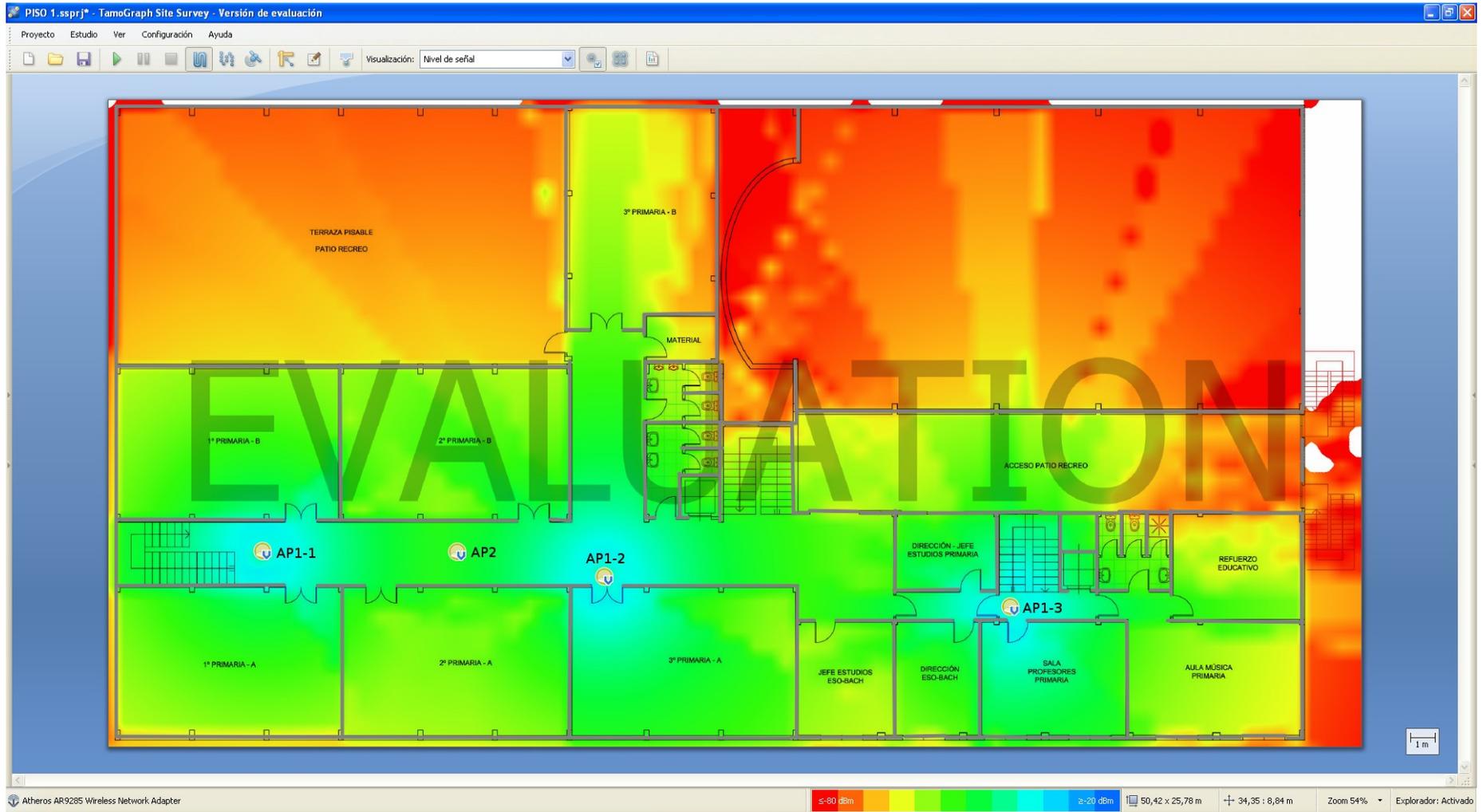


Ilustración 5: Nivel de Señal Segunda Planta

Observaciones: Se puede contemplar que las seis Aulas reciben una buena señal, en parte gracias a la señal recibida por los dos AP's de la planta superior. Las estancias de más a la derecha no necesitan señal porque no se utilizan para fines docentes o educativos.



Observaciones: Toda esta planta recibe una buena señal a excepción de unas pequeñas áreas que reciben un nivel de señal bajo probablemente debido a las paredes alicatas de los aseos.

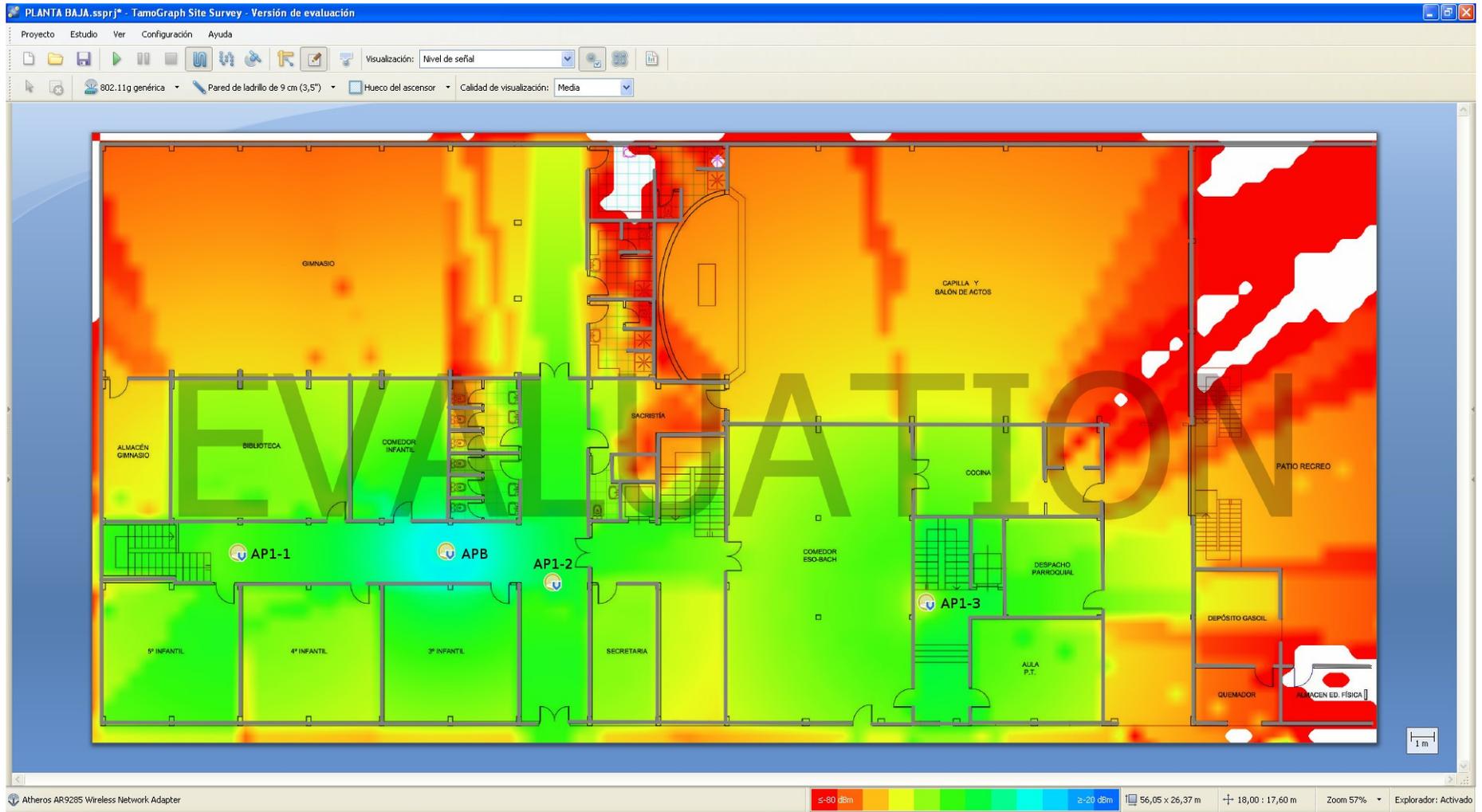


Ilustración 7: Nivel de Señal Planta Baja

Observaciones: En esta planta las zonas que interesan cubrir, reciben una buena señal, en parte gracias a los AP's de la planta superior. En el Gimnasio, la Capilla o en el Patio, no se necesita por ahora tener señal.

3.2.3. Análisis de los cálculos

A continuación se muestran los resultados finales obtenidos, comparando el número de puntos de acceso (APs) necesarios según la demanda estimada por los usuarios y el número de puntos de acceso necesarios para cubrir las zonas de servicio.

Planta	N.º de AP's por capacidad	N.º de AP's por cobertura	N.º usuarios estimado	N.º usuarios máximo
PB	1	1	18	22
P1	1	3	10	66
P2	1	1	4	22
P3	2	2	34	44
P4	2	2	39	44
P5	3	3	45	66
TOTAL	10	12	150	264

Tabla 2: Análisis de los cálculos

Como se puede apreciar en la tabla, tras el estudio de propagación radioeléctrica, es necesario aumentar la zona de cobertura en la P1 del edificio. El número total de puntos de acceso a utilizar será de 12, en vez de 10, por lo que el número de usuarios máximo que se podrán conectar a la vez en el sistema para la velocidad de 1Mbps ofrecida, podrá verse incrementado en más de 100, siempre y cuando el ancho de banda de conexión a Internet lo permita.

En la siguiente tabla se resumen los datos más relevantes teniendo en cuenta el ancho de banda de conexión a Internet contratado actualmente:

Datos	Estimado	Ofrecido
N.º máximo usuarios simultáneos	150	200
Velocidad por usuario	1Mbps	1Mbps
Velocidad máx por PA	22Mbps	22Mbps
N.º de PA requeridos	10	12
N.º medio usuarios por PA	15	16,6
Velocidad total	150Mbps	200Mbps

Tabla 3: Datos relevantes del análisis

Podemos observar en la tabla anterior, que debido a la actual demanda de 150 posibles usuarios conectados a la vez con una velocidad mínima de conexión ofrecida de 1Mbps, resulta un total de 150Mbps de ancho de banda total necesarios de salida a Internet. Por lo tanto, el centro se vio en la obligación de contratar una conexión de Internet de fibra óptica de 200Mbps simétricos garantizados. Es por ello, que en la actualidad la red esta capacitada en ofrecer una conexión simultánea garantizada de 1Mbps a 200 usuarios, aunque en un futuro podría ser de 264 usuarios simplemente contratando un servicio de ancho de banda superior al actual.

3.3. Red Inalámbrica Unificada

Tras buscar y comparar diferentes alternativas y posibilidades, se decide utilizar una solución Inalámbrica Unificada Profesional. Esta se basa en la filosofía de una estructura de Puntos de Acceso “ligeros” y un controlador que centralizan la gestión de la red [7].

Este diseño permite la centralización de un sistema de gestión casi automático de la red que facilita la visualización en tiempo real, y en todo momento, del estado de la misma, asignando éste de manera automática tanto las frecuencias como las potencias y las cargas de los puntos de acceso. Esto significa que el personal que gestione la red no necesita tener unos elevados conocimientos de radiofrecuencia.

Este sistema centralizado es capaz de gestionar diferentes Puntos de Acceso que operan en las bandas de 5Ghz y 2,4Ghz (802.11a, 802.11b, 802.11g y 802.11n), tanto en modo simple como en dual. También proporciona un escudo de seguridad integrado. Los Puntos de acceso, monitorizan constantemente el entorno Wireless y alertan de eventos tales como Puntos de Acceso Intrusos o Falsos, nivel excesivo de interferencia, actuaciones maliciosas, desconexión de Puntos de Acceso, etc.

El sistema es altamente flexible y escalable. La agregación de nuevos servicios es sencilla, y no interfiere en servicios ya implantados. Otra característica, consiste en permitir gestionar diferentes SSIDs emitidos por todos los Puntos de Acceso, pudiendo pertenecer cada una a una red totalmente independiente.

La ampliación de puntos de acceso para nuevas zonas de cobertura no requiere modificar configuraciones. Esta característica permite disponer de Puntos de Acceso adicionales de reserva para uso ocasional, o adquirir nuevos en un futuro para aumentar el dimensionado del sistema.

3.3.1. Equipamiento utilizado

Viendo que un sistema unificado se adapta totalmente a las exigencias del centro, se decidió buscar un equipamiento que estuviese dentro de las posibilidades económicas, pero que a la vez ofreciese todas las características profesionales mencionadas. A continuación, se muestra todo el equipamiento utilizado junto con sus especificaciones más relevantes de cara a nuestro proyecto:

- **Controladora de red Inalámbrica Unificada DWC-1000 de D-link**



Ilustración 8: Controladora de red Inalámbrica DWC-1000

Sus especificaciones más relevantes son:

- 4 puertos LAN Gigabit
- Capacidad de gestión de 6 puntos de acceso inicial (ampliable a 24)
- Autenticación por Portal Cautivo (red LAN/inalámbrico)
- Capaz de gestionar 6 modelos diferentes de Puntos de Acceso D-link
- Monitorización de Aps y de Clientes
- Ajuste automático de canales y potencia de señal RF.
- Seguridad inalámbrica WEP/WAP/WAP2 y Radius 802.1x.
- VLAN basado en puerto o en subred.
- Firewall y filtrado de contenido web (URL estática/ palabras clave)
- Balanceo de carga saliente
- Interfaz de usuario basado en web HTTP

Mas información en la página web del producto:

<http://www.dlink.com/es/es/support/product/dwc-1000-d-link-wireless-controller>

- **Punto de Acceso Inalámbrico Unificado DWL-2600AP de D-Link**



Ilustración 9: Punto de Acceso Unificado DWL-2600AP

Es un punto de acceso Wi-Fi de interior diseñado específicamente para su implementación en entornos empresariales. Es compatible con el estándar 802.11b/g/n en la banda de 2,4GHz. Muy manejable y veloz, el DWL-2600AP se integra perfectamente en la infraestructura de red existente y se puede escalar fácilmente para satisfacer futuras demandas. Puede ser gestionado de forma unificada por el DWC-1000. También incorpora PoE (alimentación mediante el cable ethernet) lo que hace aún más fácil su instalación.

Sus especificaciones más relevantes son:

- Interfaz de conexión Wi-Fi 802.11b/g/n 2.4 Ghz
- Antena interna MIMO 2x2
- Método de alimentación PoE (af) o 12 V / 1 A
- Seguridad SSID (hasta 16 SSID) y 802.1Q VLAN
- Seguridad WPA/WPA2 Personal / Empresa (Radius)
- Gestionable mediante Controladora Unificada DWC-1000

Mas información en la página web del producto:

<http://www.dlink.com/es/es/business-solutions/wireless/access-points/unified-access-points/dwl-2600ap-unified-wireless-n-poe-access-point>

- **Switch DES-1210-28P de D-Link**



Ilustración 10: Switch DES-1210-28P

El DES-1210-28P es la última generación de Smart Switches. Equipado con 24 puertos Fast Ethernet, 2 puertos Gigabit y 2 puertos combo Gigabit/SFP, este modelo ofrece todas las características necesarias en una pequeña y mediana empresa, sin una necesaria complejidad añadida. Integra una interfaz web basada en la utilidad SmartConsole que hacen a estos conmutadores fácil de implementar, configurar y solucionar problemas. Su completo conjunto de características permite una perfecta integración en cualquier entorno.

La opción PoE está disponible en sus 24 puertos Fast Ethernet. La integración de tecnologías tales como PoE basado en tiempo, permite poder programar el apagado a una hora predeterminada de los dispositivos conectados a él.

Otras especificaciones relevantes son:

- Soporte 802.1Q VLAN
- Soporte QoS y control de ancho de banda
- Características avanzadas de administración
- Listas de control de acceso ACL
- Características a nivel L2: Control de Flujo, IGMP Snooping, Spanning Tree Protocol, Detección de bucle invertido, Port Mirroring...
- Seguridad 802.1x Radius.

Mas información en la página web del producto:

http://www.dlink.com/es/es/business-solutions/switching/smart_switches/des-1210-series-fast-ethernet-smart-switches

3.3.2. Esquema de la red cableada

Una vez adquirido todo el equipamiento necesario, y seleccionados los emplazamientos de los puntos de acceso, se procede al diseño de la red cableada. Teniendo en cuenta que los puntos de acceso van a ser alimentados a través del cable ethernet mediante PoE, resulta mucho más fácil su instalación, además de ver reducidos los costes.

Como se puede apreciar en la siguiente ilustración (esquema red cableada), se decide situar el Controlador WiFi, el Switch y el Servidor Radius en el tercer piso. Esta decisión se toma por dos razones: una, porque en ese lugar se encuentra el Aula de Informática y el equipo puede mantenerse bajo llave; y otra, porque de este modo la máxima longitud del cable Ethernet, que también alimenta mediante PoE a los Puntos de Acceso, se ve reducida considerablemente.

El cableado vertical entre plantas se decide sacar mediante tubo por fachada externa, ya que la instalación eléctrica del edificio es muy antigua y puede producir interferencias. Por otro lado, el Router principal se deja en su antiguo emplazamiento porque a él le llegan otros cables procedentes de la antigua Red LAN existente.

El cable azul oscuro del esquema de red, corresponde al UpLink de 1Gbps del Switch que se conecta a la boca LAN-1 de la Controladora DWC-1000 de también de 1Gbps. Por este cable se empaquetan todos los datos procedentes de los 12 Puntos de Acceso.

El cable de color rojo, une la Controladora DWC-1000 con el Router principal (conexión troncal de 1Gbps) que proporciona acceso a Internet con un ancho de banda de 200Mbps simétricos, gracias al acceso de fibra óptica contratada.

El Servidor RADIUS se instalará en el PC que ya realizaba las funciones de Servidor del Aula de Informática, y que se conecta a la nueva red cableada a través de la antigua LAN (mostrado mediante el cable de color verde), y que sigue estando conectada al Router principal situado en la Planta Baja.

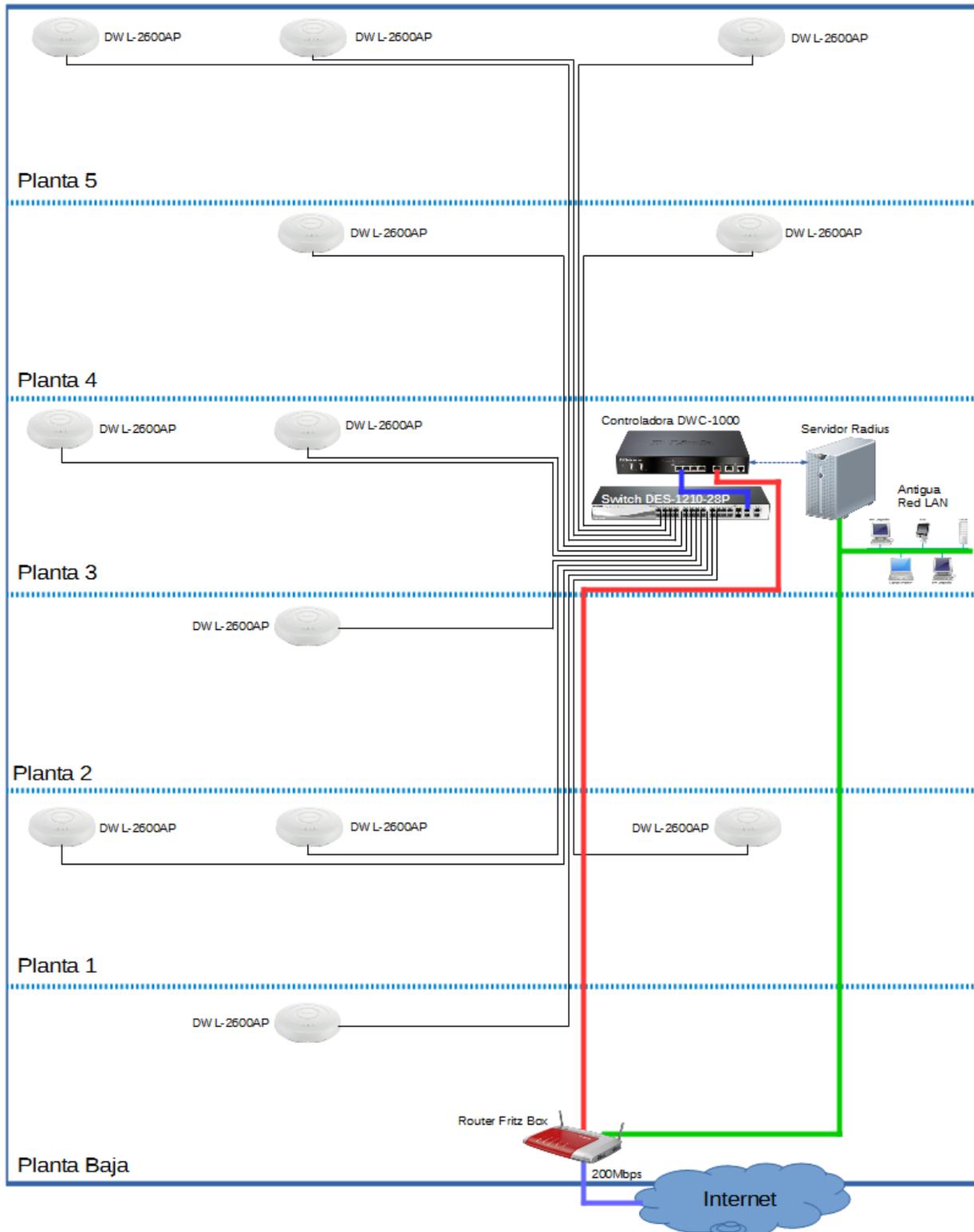


Ilustración 11: Esquema de Red Cableada

A continuación se muestran algunas fotografías correspondientes al equipo físicamente ya montado:

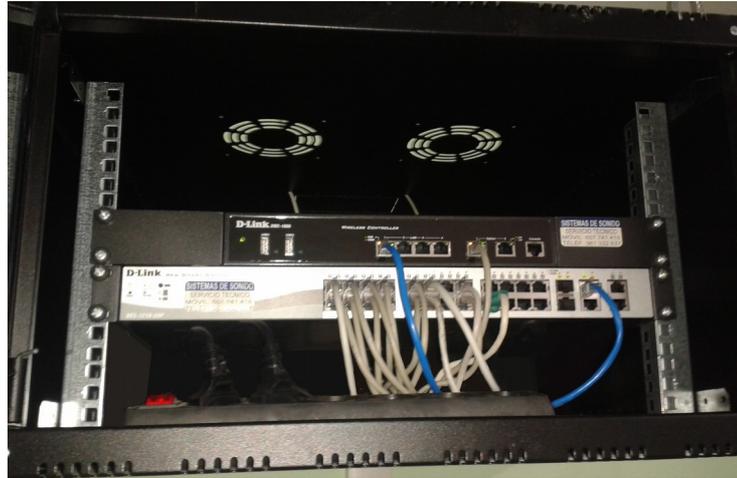


Ilustración 12: Armario Rack con Controlador WiFi y Switch PoE



Ilustración 13: Puntos de Acceso DWL-2600AP

3.3.3. Escenario

Una vez montado físicamente el sistema se procede a la configuración del mismo según las necesidades. Como ya se comentó en el apartado justificación, el centro quiere ofrecer a los alumnos acceso inalámbrico a Internet, pero también a los docentes y personal de administración. Esto obliga a tener que compartir la red inalámbrica, pero, a la vez, mantener separada, y de forma segura, la información entre estos. Por ejemplo, se quiere ofrecer a los docentes, además de Internet, la posibilidad de acceder a las impresoras y a los recursos de red ya existentes en la antigua LAN, pero en cambio, al alumnado solamente se le quiere brindar de la conexión a Internet y que esta sea limitada (filtrado de algunas webs).

A continuación, se muestra el escenario en el que se basará toda la configuración:

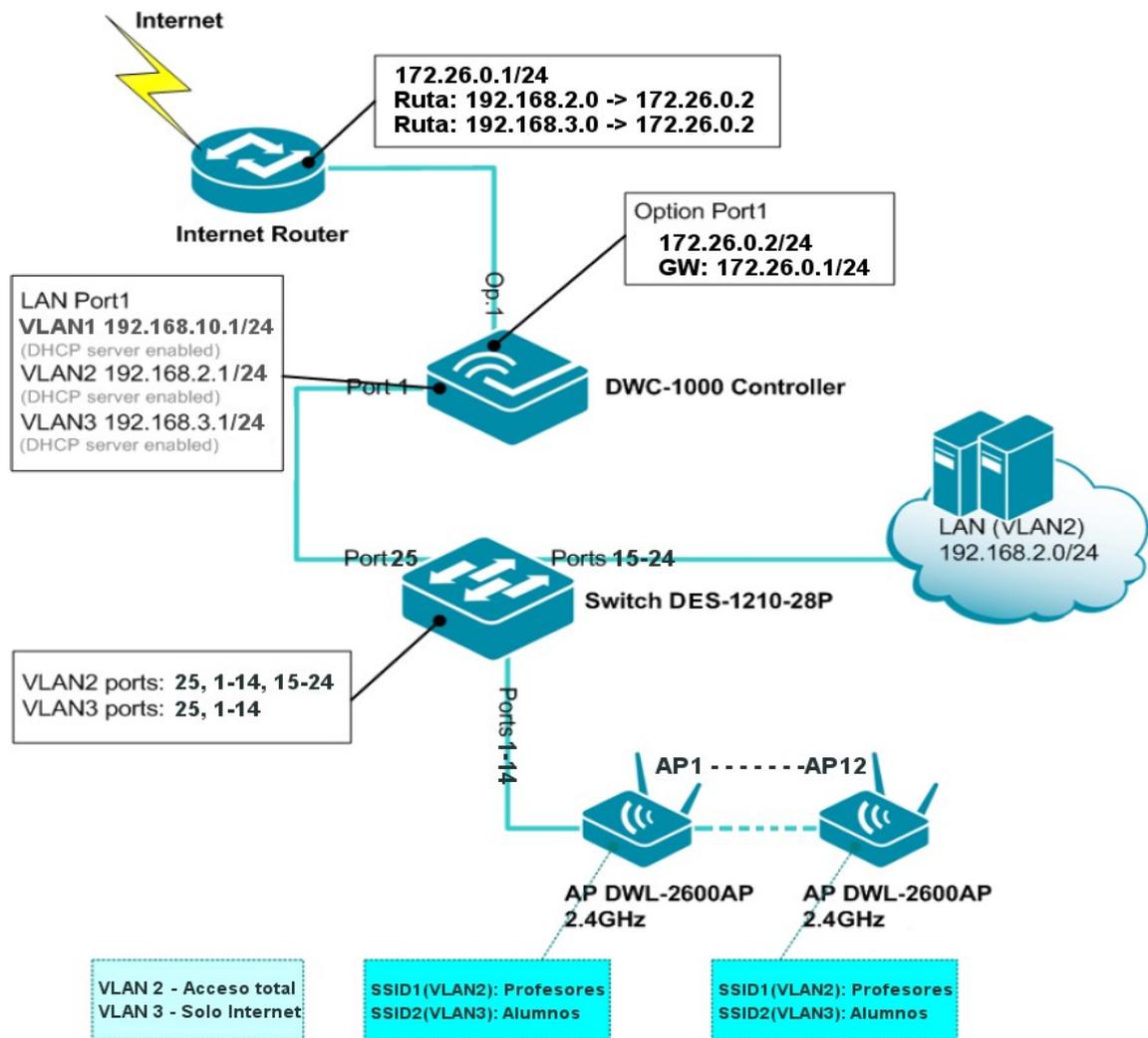


Ilustración 14: Escenario Resumen del Sistema

Los Puntos de Acceso emitirán dos SSID diferentes, una “Profesores” y otra “Alumnos” y se configurará tanto la Controladora como el Switch para que haya una distinción entre estas dos redes.

Esto se conseguirá mediante la configuración de dos redes inalámbricas WLAN diferentes pero utilizando físicamente la misma red, por lo tanto será necesario la utilización de VLANs de nivel 2 (pertenencia según su dirección de subred IP). Los usuarios que se conecten a la SSID “Profesores”, pertenecerán a la VLAN2 (subred 192.168.2.0/24) con un perfil de acceso total a la red y acceso a los recursos compartidos de la misma. Por otro lado, los usuarios que se conecten a “Alumnos” pertenecerán a la VLAN3 (subred 192.168.3.0/24) con sólo acceso a Internet y sin posibilidad de acceder a ningún dispositivo de la VLAN2.

La VLAN1 es la utilizada de forma nativa y por defecto por la Controladora Wireless para su configuración y conexión con los Puntos de Acceso que también pertenecerán a esa misma VLAN1 con una subred 192.168.10.0/24.

3.4. Configuración de la Red Unificada

Una vez aclarado el escenario que se quiere conseguir, se procede a la configuración paso a paso de todos los dispositivos implicados.

Primero se describe mediante apartados la configuración más fundamental de la Controladora Wireless, la configuración de VLANs en el Switch y la creación de rutas estáticas en el router de acceso a Internet.

Para terminar, se explica la instalación y configuración del Servidor RADIUS

3.4.1. Configuración de la Controladora Wireless DWC-1000

Para poder acceder vía configuración web a la Controladora, es necesario estar conectado físicamente a unas de sus 4 bocas LAN (o conectado al switch como en la Ilustración 6) y tener configurado el PC con alguna dirección de su misma subred 192.168.10.0/24, ya que por defecto la Controladora viene con el DHCP deshabilitado.

Una vez conectados, desde el navegador se puede acceder al Interface de Gestión Web introduciendo la dirección <http://192.168.10.1> con el *Username* y *Password* por defecto de administración.



Ilustración 15: Login Interface de Gestión Web

Antes de seguir con la configuración, será necesario conocer la disposición que muestra el Interface de Gestión Web para poderse mover correctamente por los menús.

Como se puede apreciar en la siguiente Ilustración, el Interface Web incluye los siguientes componentes:

- **1^{er} Nivel: Menú de Navegación Principal.** Esta barra, situada en la parte superior, permanece mostrada constantemente en pantalla. Está compuesta por las opciones SETUP, ADVANCED, TOOLS , STATUS y HELP proporcionan acceso a toda la configuración del 2^o Nivel.
- **2^o Nivel: Menú de Configuración.** Este menú aparece en el lado izquierdo del Interface Web y va cambiando conforme a lo seleccionado en el 1^{er} Nivel. Algunos menús tienen implícito un submenú con más opciones.
- **3^{er} Nivel: Espacio de Trabajo.** Muestra los parámetros asociados con la selección realizada por el menú o submenú del 2^o Nivel.

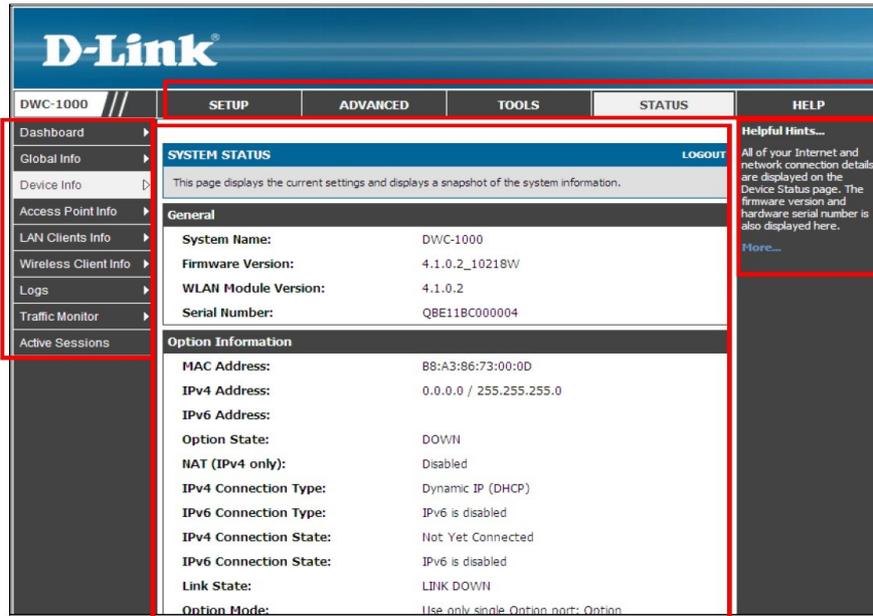


Ilustración 16: Disposición Menús del Interface de Gestión Web

- **Consejos útiles.** En el lado derecho aparece, de forma resumida, una pequeña ayuda de la ventana que se está mostrando.

3.4.1.1. Configuración del Interface LAN

Dentro del menú principal SETUP se elige del menú de configuración Network Settings > LAN Setup. Aquí se especifica la dirección de la Interface LAN de la Controladora y su Máscara de Subred.

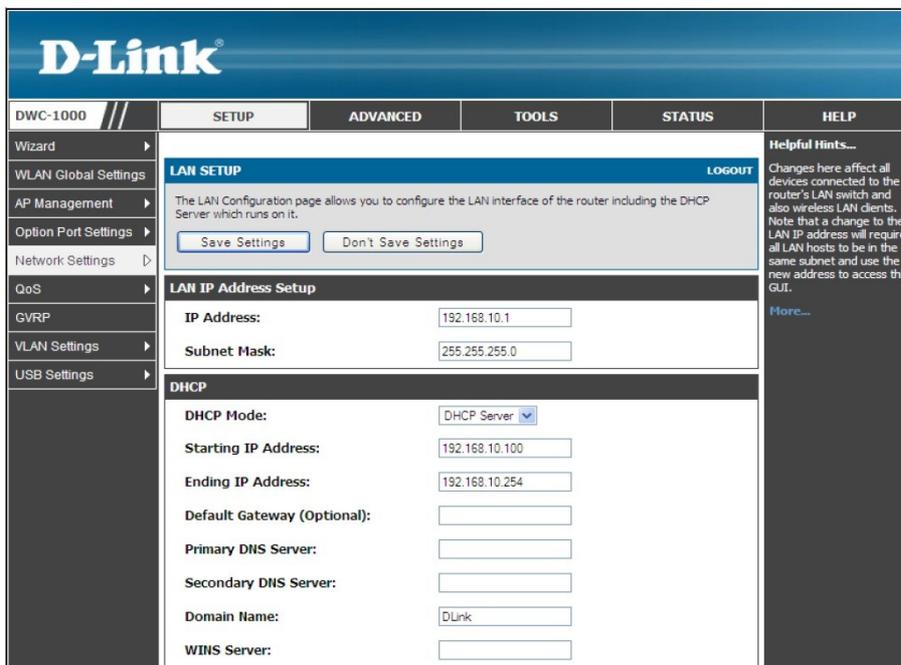


Ilustración 17: LAN Setup del DWC-1000

Seleccionar también en DHCP el Modo DHCP Server para que los Puntos de Acceso obtengan una dirección automáticamente de esta red. También se introduce el rango de IPs que podrá asignar el Servidor DHCP de dicha red.

Finalmente, se seleccionará “Save Settings” para guardar los datos introducidos. En posteriores apartados no se mencionará este paso por evitar repetir, y porque resulta obvio.

3.4.1.2. Configuración del Interface Option 1

En el menú SETUP, entrando en Internet Settings > Option 1 Settings > Option 1 Setup y se elige como Tipo de Conexión “Static IP”. Se introduce la dirección de la Interface Option 1 que en este caso es la 172.26.0.2 con Mascara de Subred 255.255.255.0. La dirección IP del Gateway será la del Router de Internet 172.26.0.1. Será necesario también introducir los DNS del proveedor de acceso a servicios de Internet para que funcione correctamente.

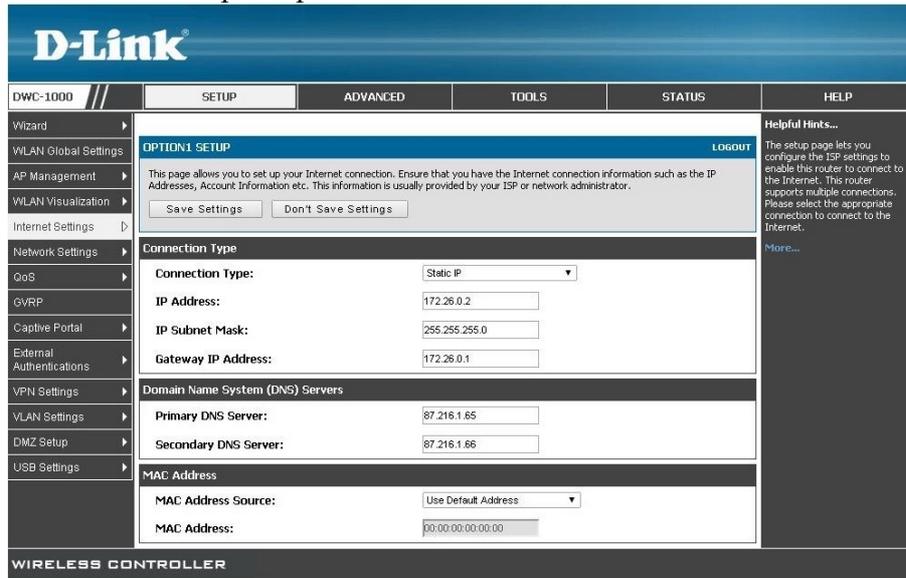


Ilustración 18: Option 1 Setup

3.4.1.3. Añadir nuevas VLANs

El soporte de VLAN está deshabilitado por defecto en la Controladora, por lo que antes de nada en SETUP > VLAN Settings > VLAN Configuration, se deberá habilitar.

Después en VLAN Settings > Available VLANs, se puede añadir las VLANs necesarias. En este caso se añade la VLAN “Profesores” con un ID = 2 y “Alumnos” con un ID = 3. Este ID es el número identificativo de la VLAN. La VLAN con ID = 1 se reserva para la VLAN por defecto, la cual es utilizada por los paquetes no etiquetados (untagged) recibidos en el Interface.

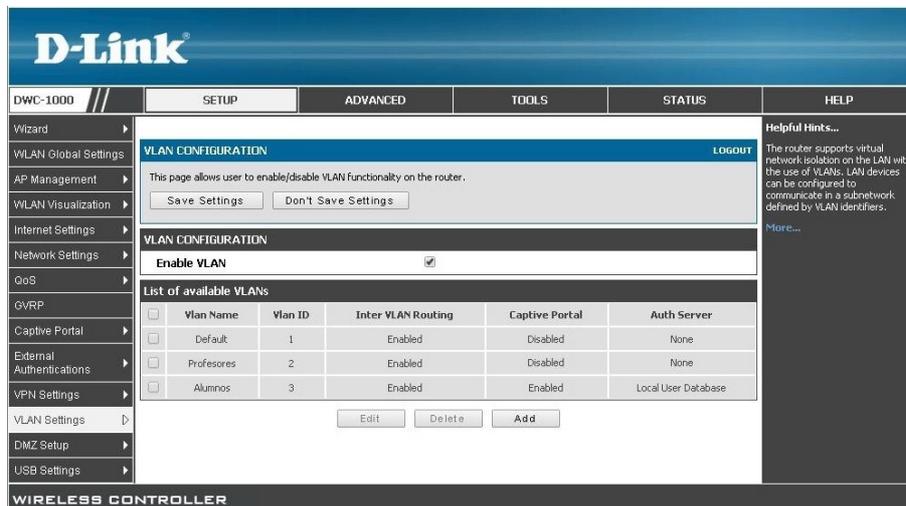


Ilustración 19: Lista de VLANs disponibles

3.4.1.4. Configuración de las subredes VLAN

Ir a SETUP > VLAN Settings > Multiple VLAN Subnets. Aquí se selecciona la VLAN a configurar.



Ilustración 20: Múltiple subredes VLANs

En la VLAN “Profesores” se introduce la dirección de subred 192.168.2.1/24 y en el Modo de DHCP se elige DHCP Server con un rango de direcciones suficientemente amplio para que la Controladora asigne las direcciones IPs de esta subred a los usuarios que se conecten a la SSID “Profesores”.

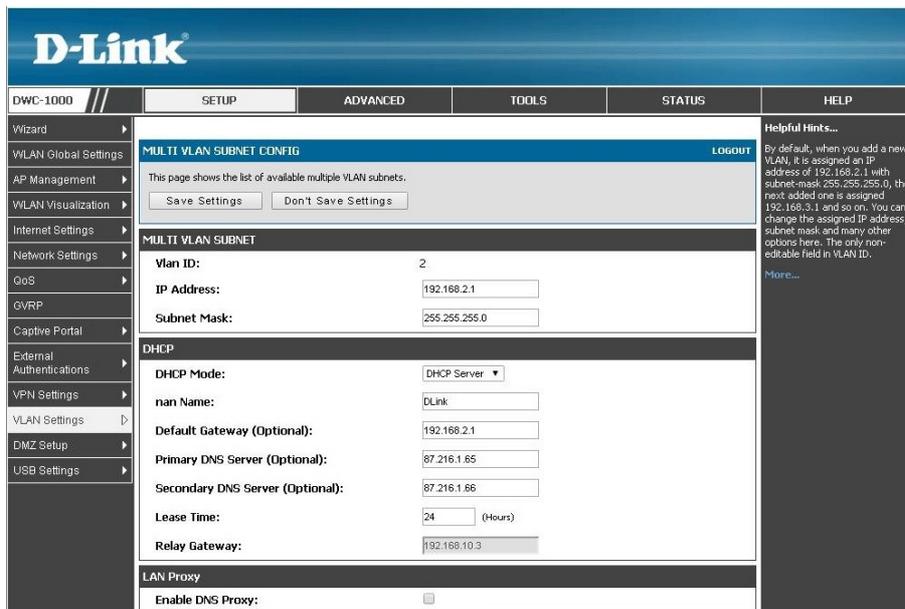


Ilustración 21: Configuración Subred VLAN 2 Profesores

En la VLAN “Alumnos” se procede igual, pero en este caso la dirección de subred será la 192.168.3.1/24.

3.4.1.5. Asociar las VLANs al puerto

Como ya se mostró en el Escenario del Sistema, la Controladora se conectará a través del Port 1 al Port 25 del Switch. Por este enlace se van a tener que gestionar los datos de ambas VLAN procedentes de los Puntos de Acceso con usuarios conectados a los SSID “Profesores” y “Alumnos”. Por ello es necesario indicarle a la Controladora que asocie las VLAN 1, 2 y 3 al puerto en cuestión.

En este caso se deberá ir a SETUP > VLAN Settings > Port VLAN y seleccionar Port 1. El Modo se seleccionará “General” para poder trabajar con varias VLANs y finalmente se añaden la VLAN 2 y VLAN 3 como asociados al puerto.

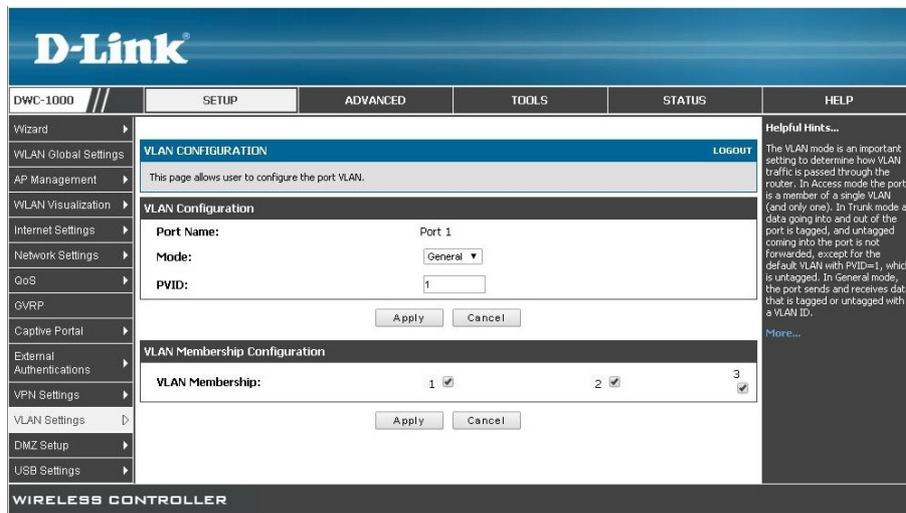


Ilustración 22: Configuración del puerto como miembro VLAN1, 2 y 3

3.4.1.6. Crear un Perfil de Configuración para los Puntos de Acceso

Esta vez se irá al menú ADVANCED > AP Profile. Aquí se añade un nuevo perfil de configuración donde se guardará toda la configuración que se aplicará de forma unificada a todos los Puntos de Acceso de la WLAN. Se podrán crear tantos Perfiles como diferentes escenarios posibles se deseen para la red configurada. En este caso el Perfil creado según el escenario planteado se denomina con el nombre del colegio “FATIMA”.



Ilustración 23: Creación de un nuevo Perfil

Lo primero que deberá hacerse, es crear las SSIDs. Por lo tanto se selecciona la opción “Configure SSID” para crear la SSID “Profesores” y posteriormente la de “Alumnos”. Es importante recalcar que para la SSID “Profesores” se introducirá la opción VLAN = 2 y para la SSID Alumnos la VLAN = 3. De esta forma, por ejemplo, los paquetes que se transmitan a través de la SSID “Profesores” serán etiquetados con el ID = 2 para su correcta clasificación, gestión o análisis de los demás dispositivos de nuestra red.

Client	SSID	PROFESORES
WDS Configuration ▶	Hide SSID	<input type="checkbox"/>
Application Rules ▶	Ignore Broadcast	<input type="checkbox"/>
Website Filter ▶	VLAN	2 (1 to 4093)
Firewall Settings ▶	MAC Authentication	<input type="radio"/> Local <input type="radio"/> RADIUS <input checked="" type="radio"/> Disable
IPv6 ▶	Redirect	<input checked="" type="radio"/> None <input type="radio"/> HTTP
Advanced Network ▶	Redirect URL	
Routing ▶	Wireless ARP Suppression Mode	Disable ▼
Certificates	L2 Distributed Tunneling Mode	Enable ▼
Users ▶	RADIUS Authentication Server Name	Default-RADIUS-Server
IP/MAC Binding	RADIUS Authentication Server Status	Configured
Switch Settings	RADIUS Accounting Server Name	Default-RADIUS-Server
Intel® AMT	RADIUS Accounting Server Status	Configured
	RADIUS Use Network Configuration	Enable ▼
	RADIUS Accounting	<input type="checkbox"/>
	Security	<input type="radio"/> None <input type="radio"/> WEP <input checked="" type="radio"/> WPA/WPA2 <input type="radio"/> WPA Personal <input checked="" type="radio"/> WPA Enterprise
	WPA Versions	<input checked="" type="checkbox"/> WPA <input checked="" type="checkbox"/> WPA2
	WPA Ciphers	<input checked="" type="checkbox"/> TKIP <input checked="" type="checkbox"/> CCMP(AES)
	Pre-Authentication	<input checked="" type="checkbox"/>
	Pre-Authentication Limit	0 (0 to 192)
	Key Caching Hold Time	10 (1 to 1440)

Ilustración 24: Configuración SSID "Profesores"

Client	SSID	ALUMNOS
WDS Configuration ▶	Hide SSID	<input type="checkbox"/>
Application Rules ▶	Ignore Broadcast	<input type="checkbox"/>
Website Filter ▶	VLAN	3 (1 to 4093)
Firewall Settings ▶	MAC Authentication	<input type="radio"/> Local <input type="radio"/> RADIUS <input checked="" type="radio"/> Disable
IPv6 ▶	Redirect	<input checked="" type="radio"/> None <input type="radio"/> HTTP
Advanced Network ▶	Redirect URL	
Routing ▶	Wireless ARP Suppression Mode	Disable ▼
Certificates	L2 Distributed Tunneling Mode	Disable ▼
Users ▶	RADIUS Authentication Server Name	Default-RADIUS-Server
IP/MAC Binding	RADIUS Authentication Server Status	Configured
Switch Settings	RADIUS Accounting Server Name	Default-RADIUS-Server
Intel® AMT	RADIUS Accounting Server Status	Configured
	RADIUS Use Network Configuration	Disable ▼
	RADIUS Accounting	<input type="checkbox"/>
	Security	<input type="radio"/> None <input type="radio"/> WEP <input checked="" type="radio"/> WPA/WPA2 <input checked="" type="radio"/> WPA Personal <input type="radio"/> WPA Enterprise
	WPA Versions	<input checked="" type="checkbox"/> WPA <input checked="" type="checkbox"/> WPA2
	WPA Ciphers	<input checked="" type="checkbox"/> TKIP <input checked="" type="checkbox"/> CCMP(AES)
	WPA Key Type	ASCII
	WPA Key	*****
	Bcast Key Refresh Rate(seconds)	300 (0 to 86400)

Ilustración 25: Configuración SSID "Alumnos"

Respecto a la Seguridad, se decide otorgar la máxima a la SSID "Profesores" mediante WPA Enterprise. Se debe especificar que se va a utilizar el Servidor RADIUS para gestionar las credenciales de los usuarios. Respecto a la SSID "Alumnos" se elige una Seguridad WPA Personal mediante una contraseña (WPA Key) que se dará a conocer al alumnado. Posteriormente, para tener acceso a Internet, los alumnos deberán establecer sesión a través de Portal Cautivo con un usuario dado de alta localmente en la Controladora.

Más adelante, se describirá la configuración de la conexión con un Servidor externo RADIUS para la autenticación de los profesores, así como la habilitación del Portal Cautivo y el alta de usuarios para el acceso a Internet de los alumnos.

Otra opción a tener en cuenta en el Perfil creado es "Configure Radio". En esta página se pueden configurar todos los Puntos de Acceso con aspectos tan importantes como el Balanceo

de Carga, Número Máximo de Clientes por AP, el Modo IEEE 802.11 más idóneo para nuestro entorno, el Ancho de Banda o el Ajuste Automático de Canal y Potencia de Transmisión de Radio. A continuación, se muestra la configuración elegida:

The screenshot shows the 'Radio Configuration' section of the AP configuration interface. The left sidebar contains various configuration categories like Global, Peer Controllers, AP Profile, SSIDs, WIDS Security, Client, WIDS Configuration, Application Rules, Website Filter, Firewall Settings, IPv6, Advanced Network, Routing, Certificates, Users, IP/MAC Binding, Switch Settings, and Intel® AMT. The main area is titled 'AP PROFILE SUMMARY' and 'AP Profile Radio Configuration'. The 'Radio Configuration' section includes the following settings:

- State: On
- Radio Scheduler: Scheduler Off
- RTS Threshold: 2347 (0 to 2347) (Bytes)
- Load Balancing:
- Load Utilization: 70 (1 to 100) (%)
- Maximum Clients: 100 (0 to 200)
- RF Scan Other Channels:
- RF Scan Sentry:
- Mode: IEEE 802.11b/g/n
- DTIM Period: 10 (1 to 255) (# Beacons)
- Beacon Interval: 100 (20 to 2000) (Msecs)
- Automatic Channel:
- Automatic Power:

Ilustración 26: Configuración Parámetros Radio de los AP (1/2)

Como se puede apreciar en la figura, se elige la opción de “Load Balancing” para indicar al sistema que si un Punto de Acceso (AP) se satura, cederá usuarios al AP vecino, siempre y cuando dichos usuarios se encuentren en la zona de solapamiento de cobertura de ambos. El número máximo de usuarios por AP se establece en 100 aunque el máximo calculado no debería superar los 22 como ya se vio en el apartado Dimensionado del Sistema.

Otras opciones muy interesantes son “Automatic Channel” y “Automatic Power”. Al mantenerlas activas, la Controladora se encarga de asignar a cada AP el canal y la potencia de radiación idónea según la situación del entorno, interferencias, demanda de usuarios, etc.

The screenshot shows the advanced radio parameters section of the AP configuration interface. The settings are as follows:

- Automatic Power:
- Initial Power: 100 (1 to 100) (%)
- Minimum Power: 100 (1 to 100) (%)
- APSD Mode: Enable
- RF Scan Interval (secs): 60 (30 to 120)
- Frag Threshold (bytes): 2346 (256 to 2346)
- RF Scan Sentry Channels: 802.11a 802.11b/g
- Short Retries: 7
- RF Scan Duration (msecs): 10 (10 to 2000)
- Long Retries: 4
- Rate Limiting:
- Transmit Lifetime (msecs): 512
- Rate Limit (pkts/sec): 60 (1 to 50)
- Receive Lifetime (msecs): 512
- Rate Limit Burst (pkts/sec): 75 (1 to 75)
- Station Isolation:
- Channel Bandwidth: 20 MHz
- Primary Channel: Lower
- Protection: Auto
- Short Guard Interval: Enable
- Space Time Block Code: Enable
- Radio Resource Management: Enable
- No ACK: Disable
- Multicast Tx Rate (Mbps): Auto

Ilustración 27: Configuración Parámetros Radio de los AP (2/2)

En esta segunda parte de la configuración, merece la pena comentar la opción “Channel Bandwidth”. Es recomendable dejarlo en 20MHz ya que a 40MHz, como ya se vio en la descripción del Estándar 802.11, ocuparía gran parte del espectro disponible y sería imposible compartirlo entre los 12 Puntos de Acceso sin sufrir interferencias.

3.4.1.7. Incluir los Puntos de Acceso al perfil de la Controladora

Al conectar por primera vez los Puntos de Acceso al Sistema, estos deben de ser añadidos manualmente para que puedan ser gestionados por el Perfil creado.

Si se va al menú STATUS > Acces Point Info > Authentication Failure Status, aparecerán en un listado, los Puntos de Acceso reconocidos. Para incluirlos en la lista de Gestionados, se tendrán que ir seleccionando uno a uno mediante la opción “Manage” e incluirlos en el Perfil FATIMA creado con anterioridad.

MAC Address	IP Address	Last Failure Type	Age
<input checked="" type="checkbox"/> fc:75:16:75:c9:00	192.168.1.242	No Database Entry	0d:00:00:24

Ilustración 28: Lista de APs detectadas y pendientes de gestionar

Ilustración 29: Configuración de nuevo Punto de Acceso al Perfil

Después de haber incluido todos los Puntos de Acceso con éxito, se podrán listar y ver toda su configuración y estado en STATUS > Acces Point Info > Managed AP Status:

MAC Address (*)	Peer Managed	IP Address	Age	Status	Profile	Radio Interface	Scheduler Global Status	Scheduler Global Reason
70:62:b8:13:42:e0		192.168.10.225	0d:00:00:04	Managed	1-FATIMA	2-802.11b/g/n	Disabled	-
70:62:b8:13:42:a0		192.168.10.247	0d:00:00:03	Managed	1-FATIMA	2-802.11b/g/n	Disabled	-
70:62:b8:13:42:c0		192.168.10.103	0d:00:00:04	Managed	1-FATIMA	2-802.11b/g/n	Disabled	-
70:62:b8:13:42:e0		192.168.10.114	0d:00:00:04	Managed	1-FATIMA	2-802.11b/g/n	Disabled	-
70:62:b8:13:43:00		192.168.10.110	0d:00:00:04	Managed	1-FATIMA	2-802.11b/g/n	Disabled	-
70:62:b8:13:4d:20		192.168.10.231	0d:00:00:00	Managed	1-FATIMA	2-802.11b/g/n	Disabled	-
70:62:b8:13:4e:80		192.168.10.182	0d:00:00:04	Managed	1-FATIMA	2-802.11b/g/n	Disabled	-
70:62:b8:13:53:a0		192.168.10.248	0d:00:00:00	Managed	1-FATIMA	2-802.11b/g/n	Disabled	-
70:62:b8:13:54:00		192.168.10.111	0d:00:00:05	Managed	1-FATIMA	2-802.11b/g/n	Disabled	-

Ilustración 30: Lista de todos los APs Gestionados

3.4.1.8. Configuración Manual de los Puntos de Acceso

En algunos casos resulta interesante poder configurar manualmente algunas opciones que el Perfil de la Controladora maneja automáticamente, como puede ser el Canal o la Potencia de los Puntos de Acceso.

Para acceder a esta configuración debemos de ir a SETUP > AP Management > Manual management, que listará los Puntos de Acceso incluidos en el Sistema además de informar del Canal y de la Potencia utilizada por cada uno en ese momento.

MAC Address	Location	Debug	Radio Interface	Channel	Power (%)
70:62:b8:13:42:e0	PISO 5 AULAS	Disabled	2-802.11b/g/n	3	100
70:62:b8:13:42:a0	PLANTA BAJA	Disabled	2-802.11b/g/n	1	100
70:62:b8:13:42:c0	PISO 4 DESPACHOS	Disabled	2-802.11b/g/n	1	100
70:62:b8:13:42:e0	PISO 5 DESPACHOS	Disabled	2-802.11b/g/n	8	100
70:62:b8:13:43:00	PISO 3 AULAS	Disabled	2-802.11b/g/n	6	100
70:62:b8:13:4d:20	PISO 1 AULAS	Disabled	2-802.11b/g/n	12	100
70:62:b8:13:4e:80	PISO 2	Disabled	2-802.11b/g/n	1	100
70:62:b8:13:53:a0	PISO 4 AULAS	Disabled	2-802.11b/g/n	12	100
70:62:b8:13:54:00	PISO 1 DESPACHOS	Disabled	2-802.11b/g/n	6	100

Ilustración 31: Configuración Manual de los APs

La opción “Edit Channel/Power” permite cambiar manualmente estos valores, los cuales anularían la configuración establecida por el Perfil en funcionamiento referente a la selección del Canal y Potencia automática. En la siguiente figura podemos ver un ejemplo:

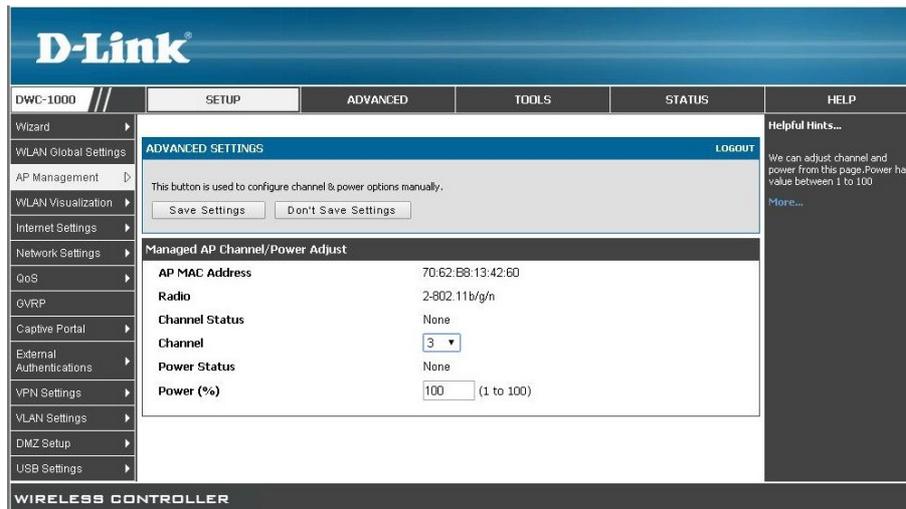


Ilustración 32: Configuración Manual del Canal y de la Potencia

3.4.1.9. Configuración del Servidor Externo RADIUS

Como se ha comentado con anterioridad, los usuarios que se conecten a la SSID “Profesores” se autenticarán mediante RADIUS. Para ello, en la Controladora se deberá ir al menú SETUP > External Authentications > RADIUS Settings.

Desde esta página se pueden añadir hasta 3 Servidores RADIUS, configurar sus opciones y ver su información de estado. En este caso, se añade como Servidor Primario el 172.26.0.14 con el puerto 1812 (por defecto) y la clave secreta, que deberá ser la misma que se introduzca en el Servidor.

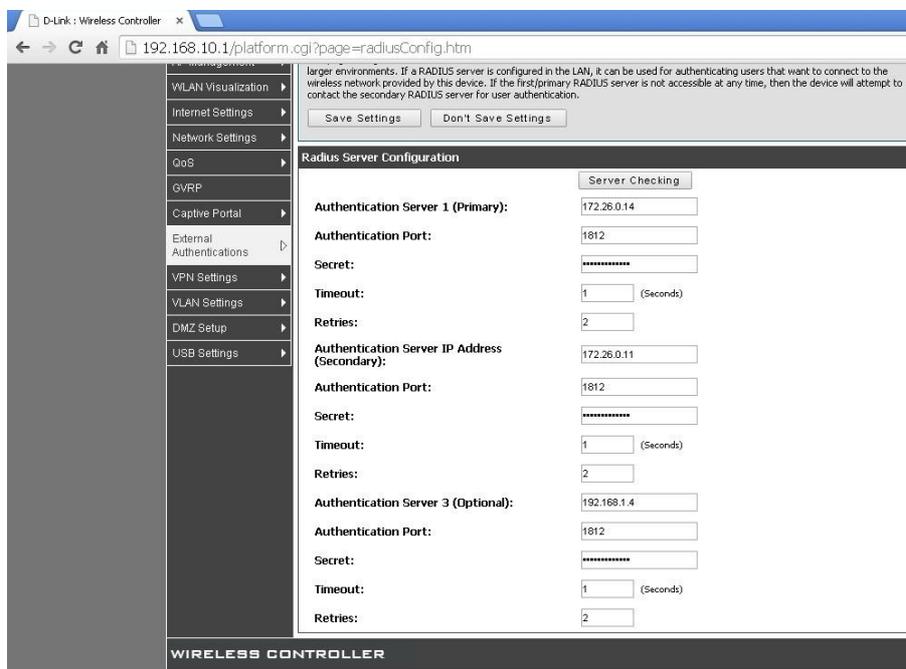


Ilustración 33: Configuración del Servidor RADIUS

Si se pulsa en el botón “Server Checking”, se comprueba si la conexión y la configuración introducida es correcta.

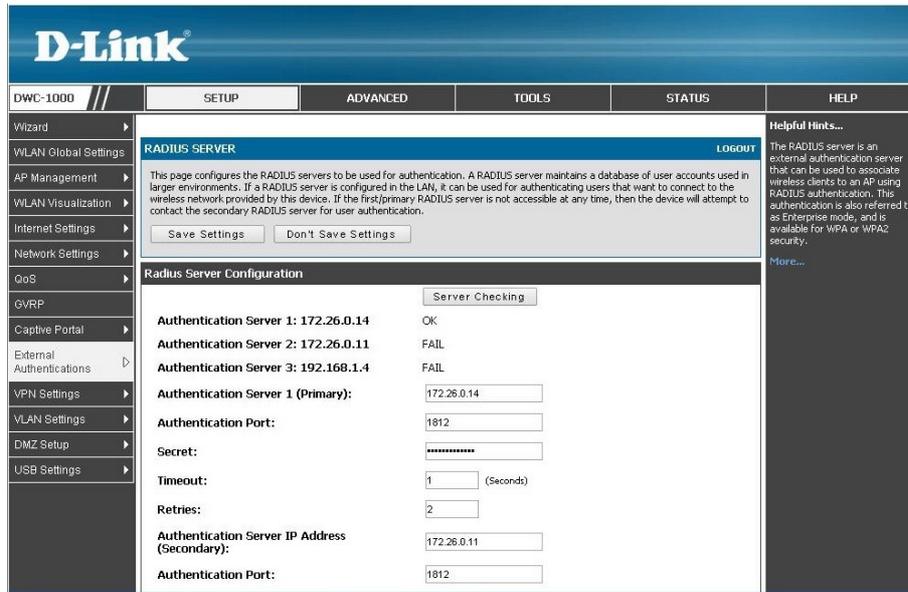


Ilustración 34: Chequeo de los Servidores RADIUS

3.4.1.10. Configuración del Portal Cautivo

La técnica del Portal Cautivo fuerza al usuario que se conecte a abrir un navegador web para poder iniciar sesión y tener acceso a Internet. En este caso en concreto, esta opción es la elegida para dar acceso a los usuarios que se conecten a la SSID “Alumnos” y cuyas credenciales deberán ser previamente introducidas en la base de datos de usuarios autorizados de la Controladora.

Paso 1 – Crear los grupos de usuarios

Antes de configurar el Portal Cautivo en sí, habrá que introducir los usuarios dentro de la base de datos local. Esto se hace creando primero un Grupo al cual pertenecerán posteriormente los usuarios. En ADVANCED > Users > Groups, se puede añadir un nuevo Grupo o editar alguno existente. En este caso, para dar de alta a los alumnos, se han creado 3 Grupos denominados BACH, ESO1 y ESO2 según el nivel de estudios que están cursando y para poder tener un mayor control sobre ellos.



Ilustración 35: Listado de los Grupos de Usuarios

Cuando se da de alta un nuevo Grupo, hay que especificar, además del Nombre y una breve Descripción, que tipo de usuarios va ha contener. En este caso serán todos “Captive Portal User”. El Idle Timeout será el tiempo en minutos que se les ofrece a los usuarios seguir con la sesión activa en el Sistema después de no recibir actividad alguna. Después de este tiempo se les echa y se les volvería a pedir un Inicio de Sesión.

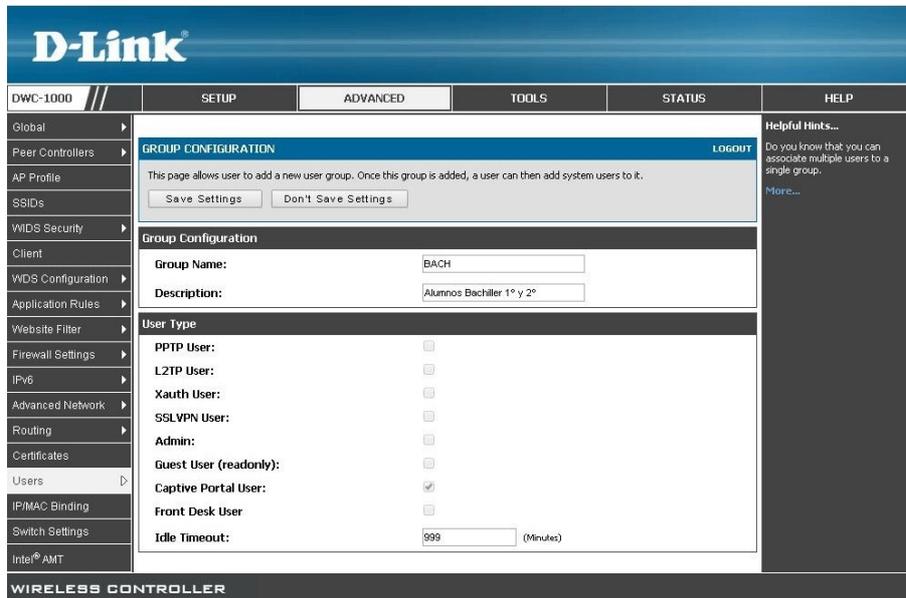


Ilustración 36: Configuración de un nuevo Grupo

Paso 2 – Crear los Usuarios

Una vez creado el Grupo, ya se pueden configurar nuevos usuarios asociándolos a sus respectivos Grupos. Se pueden configurar uno a uno, pero en este caso, como son tantos los alumnos en dar de alta, se elige la opción de Importar Usuarios de un fichero. Esto se consigue desde ADVANCED > Users > Get Users DB.

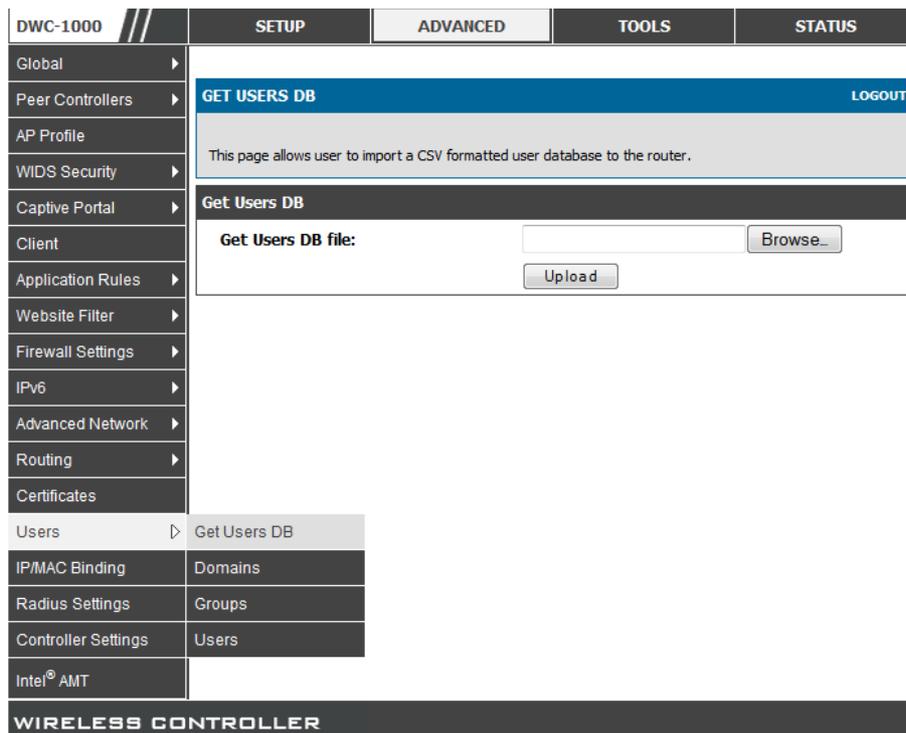


Ilustración 37: Importación de Usuarios mediante fichero CSV

El fichero CSV importado deberá contener el siguiente formato:

"UserName","FirstName","LastName","GroupName","MultiLogin","Enable password change","Password"

En este caso, a los alumnos se les da la opción de cambiar la contraseña pero no la de "MultiLogin", de esta forma sólo se les permite poder tener un dispositivo conectado a la vez.

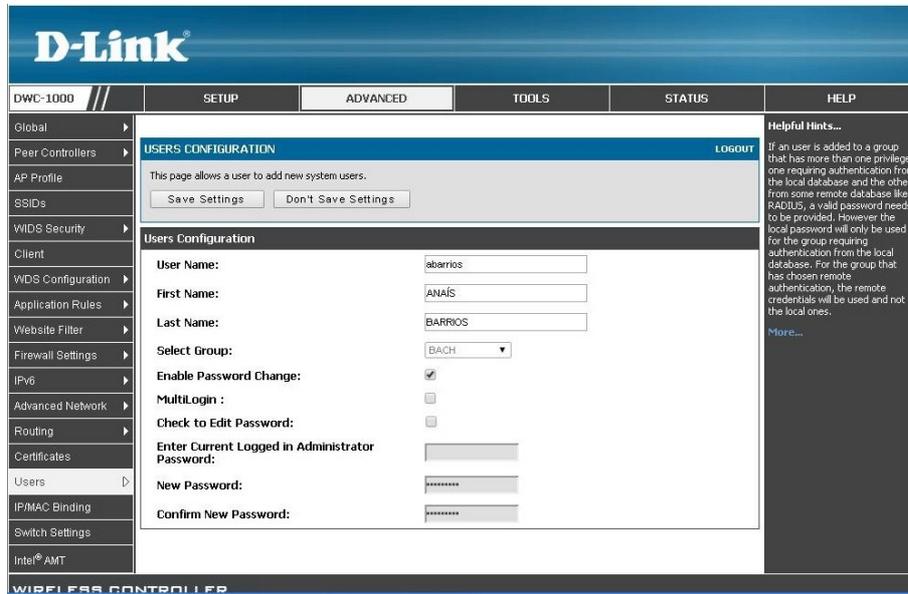


Ilustración 38: Configuración de un Usuario del Portal Cautivo

Paso 3 – Crear la página del Portal Cautivo mediante un perfil

Para crear la página del portal cautivo hay que dirigirse a SETUP > Captive Portal > Captive Portal Setup. Se puede crear un perfil nuevo presionando el botón "Add" o editar uno de los perfiles existentes. En este caso, el Portal queda configurado de la siguiente manera:



Ilustración 39: Portal Cautivo Alumnos

Paso 4 – Asociar el Portal Cautivo a la red inalámbrica (SSID)

Finalmente, para asociar el portal cautivo a un SSID, es necesario dirigirse a SETUP > Captive Portal > Captive Portal SSID Setup. En esta página se selecciona el SSID "Alumnos" y se presiona el botón "Edit".

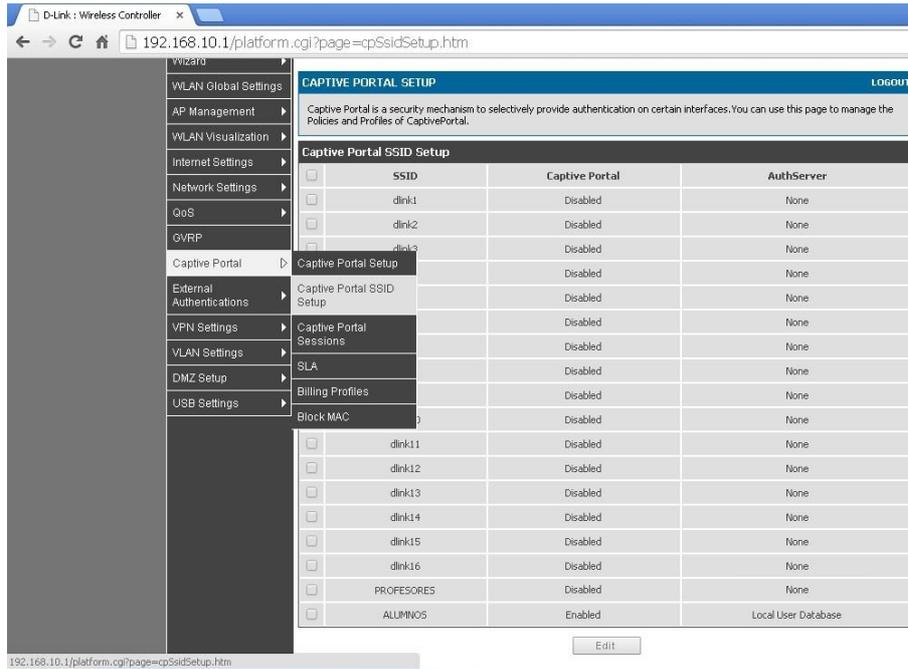


Ilustración 40: Configurar Portal Cautivo en SSID

Dentro de la configuración del SSID, se selecciona “Permanent User” para indicar después con “Local User Database” que serán los usuarios introducidos en la Base de Datos Local los que accederán mediante esta vía. Luego se selecciona el perfil creado especialmente para los alumnos en “Captive Portal Profile”.

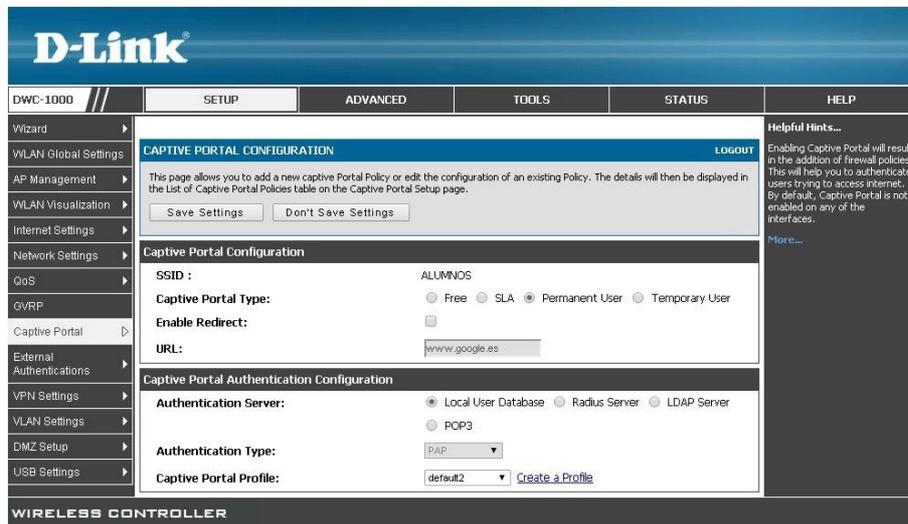


Ilustración 41: Opciones del Portal Cautivo en el SSID

Finalmente, para guardar y que se aplique la configuración, se pulsa como siempre el botón “Save Settings”.

3.4.2. Configuración del Switch DES-1210-28P

Para poder entrar vía control Web por primera vez al switch, es necesario conectarse mediante Ethernet con un PC configurado con la misma subred que el switch. Por ejemplo, este modelo de switch tiene una dirección IP 10.90.90.90, entonces el PC deberá tener una dirección 10.x.y.z con una máscara 255.0.0.0.

Abriendo un navegador web e introduciendo la dirección por defecto comentada 10.90.90.90, el switch abrirá una ventana solicitando una contraseña.

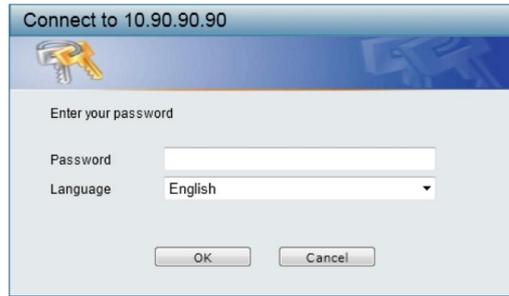


Ilustración 42: Acceso Web al Switch

Al entrar por primera vez, se abrirá un asistente solicitando cambiar la dirección IP estática y la contraseña de acceso. En este caso se cambia la IP por una de la misma subred de la Controladora y los Puntos de Acceso, exactamente la 192.168.10.2.

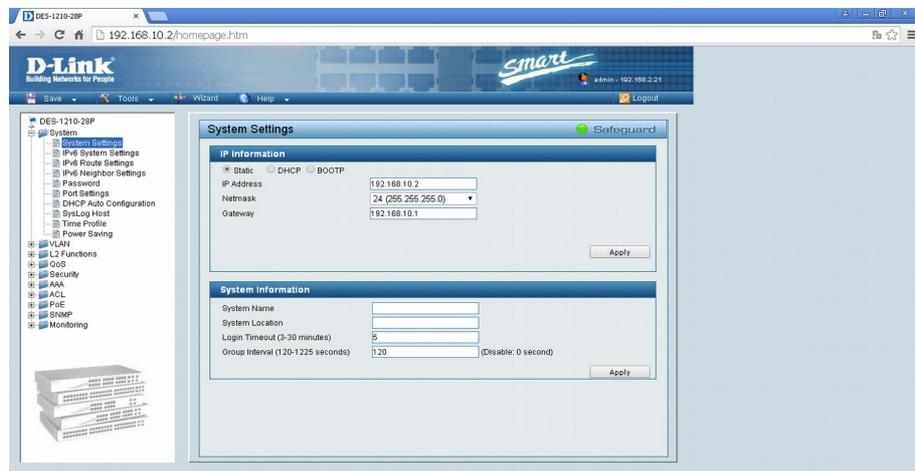


Ilustración 43: Configuración IP del Switch

3.4.2.1. Configuración de las VLANs

Debido a que la Red Unificada va a utilizar un escenario de múltiples SSIDs (SSID “Profesores” y “Alumnos”) los Puntos de Acceso necesitarán estar conectados al switch con soporte de VLANs.

En este escenario planteado, se utiliza el Switch DES-1210-28P con el puerto 25 (con soporte Gigabit) conectado a la Controladora DWC-1000. Los puertos 1-14 se reservan para conectarse con los Puntos de Acceso. Los demás puertos (del 15 al 28 menos el 25) se dejan configurados para poder ser utilizados por equipos destinados a pertenecer a la subred VLAN2 de Profesores.

Para proceder a dicha configuración, se debe entrar en VLAN > 802.1Q VLAN. Allí se deberá tener marcada la opción “Asymmetric VLAN” en “Enabled” ya que esta opción está pensada para redes como el planteado, donde se permiten tener dispositivos conectados al switch sin soporte de etiquetado VLAN, como puede ser el caso de una impresora que se desee compartir a usuarios pertenecientes a otra VLAN.

Una vez habilitada la VLAN Asimétrica se puede añadir una nueva VLAN al sistema pulsando el botón “Add”.

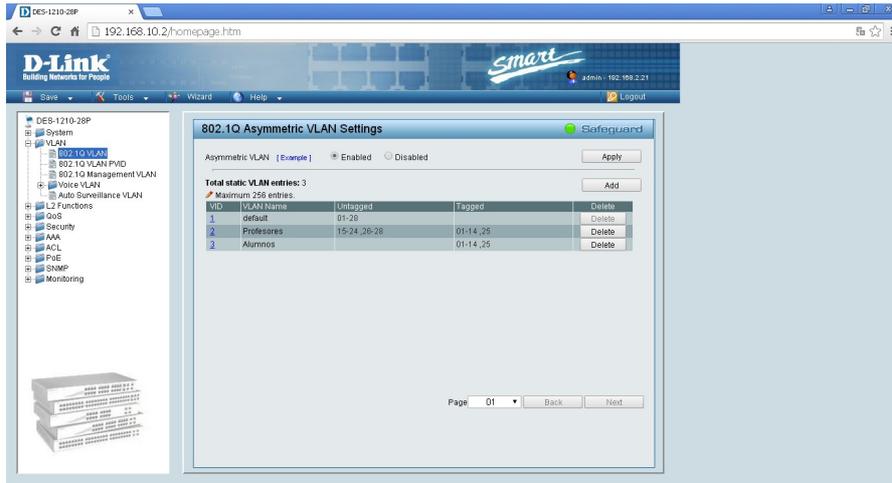


Ilustración 44: Configuración VLANs Asimétricas

En el caso que nos atañe, se crea primero la VLAN con ID = 2 denominada “Profesores”.

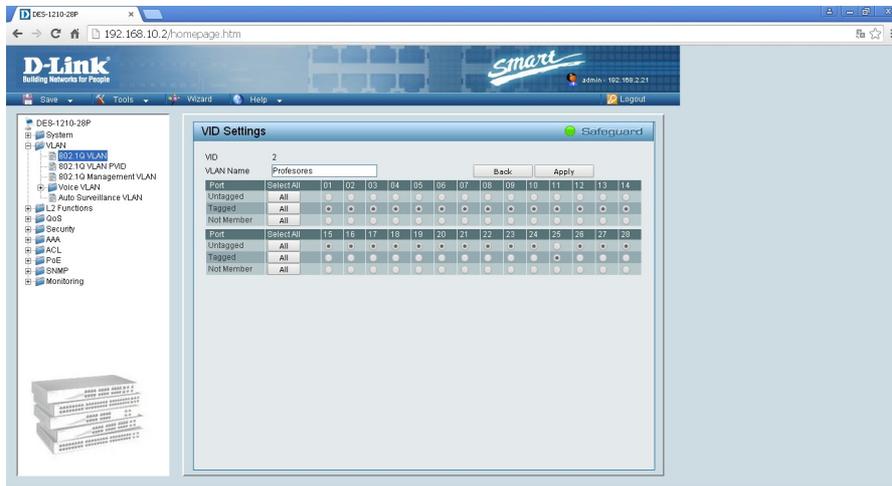


Ilustración 45: VLAN Profesores

Como se puede apreciar en la anterior Ilustración, tenemos tres opciones diferentes para cada puerto correspondiente a esta VLAN. Su significado es el siguiente:

"Not Member": Este puerto no es miembro de la VLAN.

"Tagged": Los paquetes ya tienen un etiquetado VLAN, es decir, ya han sido etiquetados por el dispositivo de red conectado a este puerto.

"Untagged": Los paquetes en este puerto no tienen etiquetas VLAN, por lo que los paquetes entrantes serán etiquetados por el switch, mientras que los paquetes salientes se enviarán sin etiquetado.

Ahora se puede comprender mejor, que como los Puntos de Acceso ya etiquetan los paquetes procedentes de la VLAN con ID = 2 de la SSID “Profesores”, en el switch se configurarán sus puertos (del 1 al 14) como “Tagged”. También se configura como “Tagged” el puerto 25, ya que la Controladora también etiquetará sus paquetes con destino a esta VLAN o SSID.

Los demás puertos (15-24 y 26-28) se configuran como “Untagged” para que sea el switch el encargado de etiquetar los paquetes que tengan como destino algún equipo o PC conectado a esta misma VLAN con ID = 2.

Finalmente se crea la VLAN con ID = 3 denominada "Alumnos".

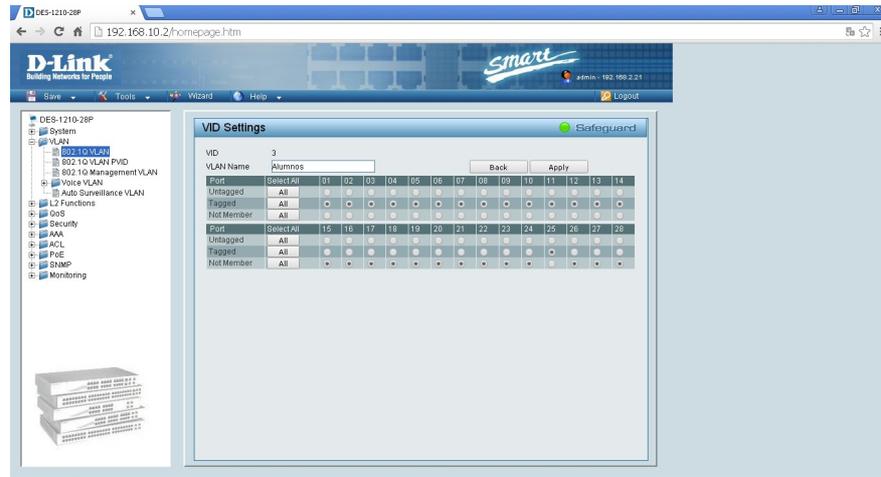


Ilustración 46: VLAN Alumnos

En este caso, al igual que en la VLAN Profesores, los Puntos de Acceso que se conectan a los puertos (del 1 al 14) se configuran como "Tagged" porque estos ya se encargarán de etiquetar con ID = 2 los paquetes procedentes de la SSID "Alumnos". Se procede igual con el puerto 25 que se conecta a la Controladora.

Los demás puertos (15-24 y 26-28) se configuran como "Not Member" con la intención de que ningún usuario conectado al SSID "Alumnos" tenga posibilidad de acceder a algún equipo o recurso compartido de estos puertos del switch reservados para la otra VLAN.

3.4.3. Configuración del Router de Internet

Para que el router principal tenga noción de las nuevas subredes creadas y pueda enrutar correctamente los paquetes con destino a estas, será necesario añadir unas rutas estáticas. La puerta de enlace para estas dos subredes, será evidentemente la dirección IP del puerto "Option 1" de la Controladora (172.26.0.2).

El router de este centro, modelo Fritz Box 7490, las rutas estáticas quedan de la siguiente manera:



Ilustración 47: Rutas Estáticas en el Router de Internet

3.4.4. Instalación y Configuración del Servidor RADIUS

Para no extenderse demasiado, se va a explicar simplemente como se instala y configura un Servidor RADIUS sin entrar en detalles de qué es, cómo funciona o qué protocolos utiliza para autenticar usuarios.

Con la intención de minimizar costes, se ha elegido el popular Servidor de código abierto FreeRADIUS instalado en una máquina ya empleada por el Colegio como Servidor del Aula de Informática.

En la página oficial de FreeRADIUS (<http://freeradius.org/>) se puede encontrar documentación y manuales referente al propio protocolo RADIUS, descargarse la última versión del software, guiarse paso a paso en la instalación y configuración del mismo o incluso consultar una amplia FAQ pensada para resolver posibles dudas.

En este caso, se va a explicar de manera sencilla cómo instalar y configurar un FreeRADIUS en una máquina con el Sistema Operativo también de código abierto UBUNTU.

Antes de empezar, hay que dejar constancia de la versión utilizada por el equipo en cuestión, ya que lo explicado a continuación podría variar para otras versiones.

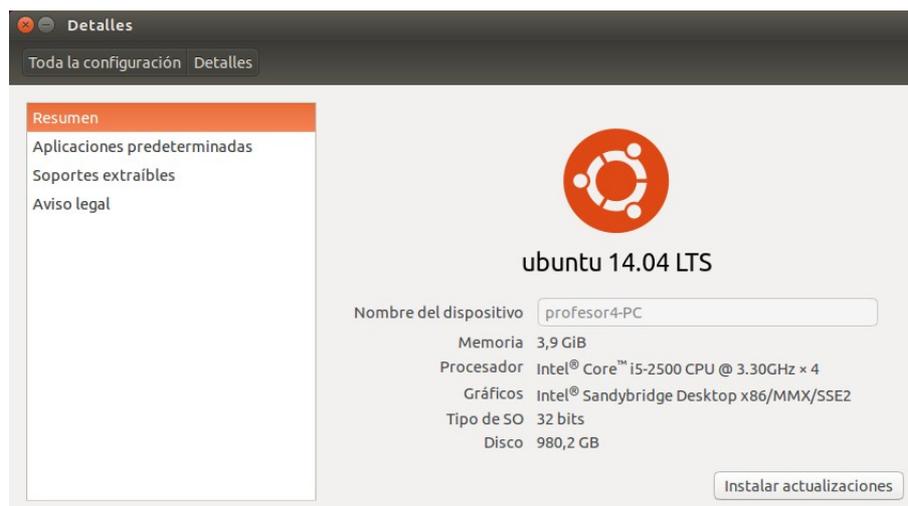


Ilustración 48: Versión de Ubuntu utilizada y características del PC

3.4.4.1. Instalación de FreeRADIUS

Existe la opción de descargar de la página web de FreeRADIUS la última versión y seguir las instrucciones que allí se dan, pero resulta muy tedioso. Las instrucciones que se dan a continuación son mucho más fáciles y además se instalan paquetes del repositorio oficial, testados por Ubuntu.

Primero se debe abrir un terminal (se puede abrir con las teclas CTRL+ALT+T). Una vez dentro del terminal, se deberá de loguearse como super-usuario mediante el comando:

```
> sudo -i
```

Se solicitará la contraseña, y una vez aceptada, se conseguirá ser usuario "root" para poder ejecutar los comandos necesarios.

Ahora ya se puede proceder a la instalación de la herramienta FreeRADIUS con el comando:

```
> apt-get install freeeadius
```

Si todo funciona correctamente, después de un breve intervalo de tiempo, en el mismo terminal, deberá aparecer el siguiente mensaje:

```
> * Starting FreeRADIUS daemon freeradius [OK]
```

Esto significa que ya está instalado y con el servicio iniciado. Si se accede a la carpeta del programa, se pueden listar los archivos de configuración que contiene.

```
> cd /etc/freeradius/  
> ls
```

3.4.4.2. Configuración de FreeRADIUS

Para configurarlo a las necesidades comentadas, necesitaremos editar un par de archivos.

Primero se edita el archivo “**users**”, el cual contiene la configuración de los usuarios que se van a poder conectar al sistema. Para comprobar el funcionamiento del FreeRADIUS, se da de alta un usuario de prueba en dicho archivo. Para editarlo se puede ejecutar:

```
> gedit users
```

Se introduce, por ejemplo, al final del archivo la siguiente línea:

```
prueba Cleartext-Password := "abc123"
```

Con esta línea tan simple, se está informando al Servidor que el usuario se denomina “prueba” y que su contraseña para acceder es “abc123”.

Ahora para ejecutar la prueba de autenticación a nivel local con el FreeRADIUS se ejecuta:

```
radtest prueba abc123 localhost 0 testing123
```

Si funciona correctamente, el programa tiene que contestar “Access-Accept paquet” como se puede ver en la siguiente Ilustración.

```

root@profesor4-PC: /etc/freeradius
root@profesor4-PC:/etc/freeradius# radtest prueba abc123 localhost 0 testing123
Sending Access-Request of id 195 to 127.0.0.1 port 1812
  User-Name = "prueba"
  User-Password = "abc123"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 0
  Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=195, length=35
  Tunnel-Type:0 = VLAN
  Tunnel-Medium-Type:0 = IEEE-802
  Tunnel-Private-Group-Id:0 = "2"
root@profesor4-PC:/etc/freeradius#

```

Ilustración 49: Prueba exitosa a nivel local del FreeRADIUS

Ahora, para que el Servidor FreeRADIUS puede aceptar peticiones de autenticación de la Controladora Wireless DWC-1000, será necesario editar el archivo “clients.conf”.

Al igual que con el archivo “users”, al final del archivo “clients.conf” se incluyen las siguientes líneas:

```

client 172.26.0.2 {
  secret = *****
  shortname = DWC-1000
}

```

Como se puede apreciar, después de la instrucción “client”, se introduce la dirección IP de la Controladora. El comando “secret” contendrá la misma clave secreta introducida en la configuración RADIUS de la Controladora (ver Ilustración 27). Y por último, “shortname” se corresponde con el nombre del host.

Para que FreeRADIUS tenga en cuenta la nueva configuración introducida, habrá que reiniciar el servicio mediante el comando:

```

> freeradius restart
* Stopping FreeRADIUS daemon freeradius      [OK]
* Starting FreeRADIUS daemon freeradius      [OK]

```

Llegados a este punto, ya se puede incluir a todos los usuarios autorizados, editando el archivo “users” (y con el mismo formato que el usuario prueba), para conectarse a la red inalámbrica con SSID “Profesores”.

4. Conclusiones

Una vez vistos los resultados y teniendo en cuenta los pocos recursos, tanto económicos como técnicos, puedo decir orgullosamente que se han alcanzado todas las premisas previstas desde un principio.

Gracias a este proyecto se consigue dar cobertura WiFi a gran parte del centro, utilizada en su mayor medida por alumnado, personal docente y de administración. Se garantiza una velocidad de conexión de calidad y lo que es más importante, ofrece una alta seguridad y fiabilidad.

El sistema es muy flexible y escalable, por lo que se podrá ampliar, si así se necesita, en un futuro tanto en velocidad como en cobertura o en un aumento de número de usuarios o accesos.

No hay que olvidar que se puede gestionar de forma centralizada todos los puntos de acceso, usuarios, cortafuegos, perfiles de usuarios, filtros, etc., por lo que supone un ahorro considerable de tiempo para las personas encargadas en esas tareas de administración de la red o de solución de incidencias técnicas.

En este documento, no se comenta, pero han sido numerosos los problemas encontrados durante la puesta en marcha y configuración del Sistema. Por ejemplo, ha sido muy difícil situar los Puntos de Acceso en los lugares idóneos para alcanzar una mayor cobertura, o una vez puestos en marcha, había que reubicarlos o cambiarlos de orientación porque aparecían zonas de sombra donde teóricamente sí que iba a llegar bastante señal.

Respecto a la Controladora, me he encontrado con muchas dificultades a nivel de configuración y de funcionamiento en sí. En los primeros días de su puesta en marcha, sufría repentinos “cuelgues” sin ninguna explicación. Por ejemplo, el servidor DHCP muchas veces no asignaba IPs, por lo que solo podían tener acceso los que ya tenían asignada una. Pero después de estar en contacto con el equipo de soporte de D-Link se dio con la solución de actualizar el “Firmware” a una versión que tan solo estaba disponible en EEUU. Desde entonces la Controladora funciona perfectamente.

Como conclusión final, espero que de alguna forma este proyecto sirva de ejemplo a otros muchos Centros o Colegios que se ven en la necesidad de adaptarse a los nuevos cambios y no tengan los suficientes recursos económicos para afrontarlo.

5. Bibliografía y Referencias

- [1] Carballar Falcón, José Antonio, "Wi-Fi. Cómo construir una red inalámbrica", Ra-Ma, 2003
- [2] Pablo Iñiguez Villarroya, "Redes Inalámbricas: IEEE 802.11, seguridad y otros aspectos", , 2002
- [3] Tomás Simal, "MONOGRÁFICO: Redes Wifi - Tecnologías", 2011, Disponible en: <http://recursostic.educacion.es/observatorio/web/gl/cajon-de-sastre/38-cajon-de-sastre/961-monografico-redes-wifi>
- [4] Miguel A. Perez, "¿Cuáles son las ventajas de un router de doble banda?", 2014, Disponible en: <http://blogthinkbig.com/wifi-de-doble-banda/>
- [5] Alfonso Moresco, "Estándar Redes Locales Inalámbricas IEEE 802.11n", 2012, Disponible en: <http://ticylamejorasocial.blogspot.com.es/2012/04/estandar-redes-locales-inalambricas.html>
- [6] Manuel Santos González, "¿Cuál es la velocidad real de las conexiones Wi-Fi (IEEE 802.11g)?", 2012, Disponible en: <http://redestelematicas.com/cual-es-la-velocidad-real-de-las-conexiones-wi-fi-ieee-802-11g/>
- [7] SPCnet Soluciones de Negocio Electrónico, "Cisco: Red Inalámbrica Unificada Profesional", 2014, Disponible en: <http://www.spcnet.es/SPCnet-Ingenieria-wireless-cisco>