UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

"Diseño de una red WLAN para cobertura total en el campus de la Universidad Católica de Santiago de Guayaquil empleando tecnología Cisco**"**

Previo a la obtención del título

INGENIERO EN TELECOMUNICACIONES CON

MENCIÓN EN GESTIÓN EMPRESARIAL EN TELECOMUNICACIONES

Elaborado por:

Christian Xavier Ferigra Orellana

Carlos Darío Ojeda Flores

Guayaquil, Enero de 2013

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

CERTIFICACIÓN

Certifico que el presente fue realizado en su totalidad por los Señores Christian Xavier Ferigra Orellana y Carlos Darío Ojeda Flores como requerimiento parcial para la obtención del título de INGENIERO EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL EN TELECOMUNICACIONES

Guayaquil, enero de 2013

ING. MARIA LUZMILA RUILOVA AGUIRRE
DIRECTOR

_____
ING. CARLOS ZAMBRANO MONTES

_____
ING.DANIELBOHORQUEZ HERAS
REVISADO POR

ING. ARMANDO HERAS
RESPONSABLE ACADÉMICO

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

DECLARACIÓN DE RESPONSABILIDAD

CHRISTIAN XAVIER FERIGRA ORELLANA
CARLOS DARIO OJEDA FLORES
DECLARAMOS QUE:

El proyecto de grado denominado "Diseño de una red WLAN para cobertura total en el campus de la Universidad Católica de Santiago de Guayaquil empleando tecnología Cisco", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de tercero conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente es de nuestra autoría.
En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del proyecto de grado en mención.

Guayaquil, Enero de 2013

LOS AUTORES

CHRISTIAN XAVIER FERIGRA ORELLANA

CARLOS DARIO OJEDA FLORES

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Nosotros, Christian Xavier Ferigra Orellana y Carlos Darío Ojeda Flores

Autorizamos a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del proyecto titulado "Diseño de una red WLAN para cobertura total en el campus de la Universidad Católica de Santiago de Guayaquil empleando tecnología Cisco", cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Guayaquil, Enero de 2013

LOS AUTORES

CHRISTIAN XAVIER FERIGRA ORELLANA

CARLOS DARIO OJEDA FLORES

AGRADECIMIENTO

A Dios por habernos dado la Sabiduría y la Fe para concluir esta tesis. A las familias Ojeda Flores y Ferigra Orellana por su apoyo moral y espiritual. Nuestros sinceros agradecimientos a nuestro amigo y profesor guía el Ing. Manuel Romero P. por su esfuerzo, dedicación, sus conocimientos compartidos y su orientación. Agradecemos a centro de cómputo por la ayuda brindada y a todos los que hicieron posible la realización de esta Tesis.

Christian Ferigra O. Carlos Ojeda F

PRÓLOGO

La necesidad de mantener un acceso permanente a la información de forma versátil y rápida ha llevado a que las redes *wireless* sean indispensables en las universidades. Este trabajo tiene el análisis de la red *wireless* actual del campus de la Universidad Católica de Santiago de Guayaquil en cada una de las facultades exceptuando la Facultad de Economía por tener una administración del internet independiente de centro de cómputo y el Edificio Principal por ser administrativo y a la vez tiene *wireless* con acceso restringido, se manifiestan las diversas deficiencias que presenta la red y se propone un nuevo diseño con equipos cisco que garantiza la eficiencia y eficacia de esta nueva red.

RESUMEN

Este proyecto de Tesis consiste en el diseño de una red WLAN (*Wireless Local Area Network,* Red de Área Local Inalámbrica) para optimizar el servicio entregado en el campus de la Universidad Católica de Santiago de Guayaquil. Se exponen los estándares actuales de redes WLAN y la metodología para diseños exitosos que Cisco utiliza, obteniendo de ésta manera resultados óptimos al momento de implementar un proyecto.

Se evaluó la red *wireless* actual del campus de la Universidad Católica de Santiago de Guayaquil mediante las herramienta de monitoreo *Solarwinds Network Performance Monitor, Observer y Visiwave.* Las cuales permitieron definir las deficiencias de la red de una manera gráfica como se lo presenta en el capítulo IV y en base a ello poder proponer un nuevo diseño con equipos de marca Cisco para que de esta manera se cumplan las expectativas de los estudiantes. Basados en el diseño que se propone se establecieron dos opciones de presupuesto.

ÍNDICE

ÍNDICE DE FIGURAS

INDICE DE TABLAS

CAPÍTULO I

MARCO CONTEXTUAL

En este capítulo se desarrolla la introducción a este trabajo de investigación, presentando los antecedentes que llevaron a proponer el mismo, la definición del problema de investigación, los objetivos planteados, la justificación y la hipótesis con la posible solución del problema planteado.

1.1. Introducción

Actualmente la Universidad Católica de Santiago de Guayaquil (UCSG) posee una infraestructura inalámbrica deficiente con redes independientes, es decir, hay equipos instalados para acceso inalámbrico en cada una de las nueve facultades y demás dependencias de la universidad, los cuales presentan problemas de conectividad. Debido a la gran importancia de tener una red inalámbrica óptima hoy en día, fue necesario hacer un análisis de la red actual y rediseñarla con tecnología de punta y mayor robustez.

En esta tesis se presentan los resultados obtenidos del análisis realizado para determinar el estado actual de la red *wireless* del campus de la UCSG, posterior al análisis se diseñó una red con tecnología Cisco que cumpla las expectativas de la comunidad universitaria.

La ejecución de dicho análisis y el diseño se lo realizó utilizando los planos originales del campus y de la cada una de las facultades otorgadas por la administración general de la universidad, con las siguientes herramientas de monitoreo:

- *Solawinds Network Performance Monitor*
- *Visiwave Site Survey*

- *Observer National Instrument*

Solarwinds Network Performance Monitor es un *software* integral de gestión del rendimiento de redes en tiempo real capaz de registrar latencias, paquetes perdidos, tráfico y ancho de banda utilizado, estado de nodos e interfaces y otros puntos críticos.

El *software* ofrece dos diferentes niveles de monitoreo:

- Dispositivos que soportan SNMP (*Simple Network Management Protocol*, Protocolo Simple de Administración de Red), permite ver estadísticas históricas y la disponibilidad de redes con cualquier navegador *web*, latencia, paquetes perdidos y ofrece información detallada del estado de una red.
- Dispositivos que no soportan SNMP, pueden ser monitoreados en la red con información de latencia de la red y paquetes perdidos.

El *set* de herramientas *Network Performance Monitor* ofrece una solución ideal para las siguientes necesidades:

1.1. Monitorear la utilización del ancho de banda de circuitos WAN (*Wide Area Network*, Red de Área Amplia).
1.2. Aislar el tráfico cuello de botella de la red
1.3. Graficar resultados en tiempo real
1.4. Identificar nodos con alto trafico
1.5. Construir reportes personalizados

VisiWave es una herramienta de *software* que muestra gráficamente áreas de cobertura de una red *wireless*, permite visualizar de manera grafica las ondas de radio y demostrar la eficacia de la cobertura de la red. Recoge información detallada sobre la red principal, las redes vecinas y luego visualiza los datos. Cada vista está diseñada para revelar detalles importantes acerca de la red de una forma intuitiva e

informativa. Con *VisiWave*, podrá: revelar los vacíos de cobertura, cualquier fuga de señal, descubrir la existencia y ubicación de los *routers* y puntos de acceso no autorizados, lista de los canales de uso, determinar los efectos de los puntos de acceso vecinos, visualizar superposición de cobertura del punto de acceso, y mucho más.

Observer *software* desarrollado por la *National Instrument* es una herramienta de análisis y monitoreo de protocolos para Ethernet, redes inalámbricas, etc. Permite al ordenador capturar diversas tramas de red en tiempo real para analizarlas, ayuda a resolver problemas de las redes. *Observer* incluye un decodificador de más de 500 protocolos que se ejecuta en el ambiente *windows*.

Con la ayuda de estas herramientas de monitoreo se pudo obtener la ubicación de los *routers* principales y APs (*Access Point*, Punto de Acceso) en cada una de las facultades, también un análisis grafico de las zonas en las que existe mayor cobertura y donde no la hay, los canales que se utilizan, las páginas de internet a la que más acceden los usuarios de la red *wireless*, las horas picos del tráfico, los números de usuarios que se conectan por facultades. Datos que permitieron ver las deficiencias de la red actual.

La red de la Universidad Católica se encuentra diseñada utilizando el modelo jerárquico de tres capas, en la capa de Núcleo o *Core* está el *Router* y *Switch* principal que se conectan al proveedor de internet, en la capa de distribución los *Switches* en cada una de las facultades y en la capa de acceso se tiene un *Router* central que brinda la conexión a los dispositivos de los usuario y además a APs que sirven para ampliar la cobertura de la red, como se observa en la Figura 1.1.

Dentro de este esquema existe una VLAN (**Virtual Local Area Network,** Red de área local virtual) asignada para el consumo de Internet a través de la red inalámbrica del campus UCSG que la separa de la parte administrada. Una de las mayores ventajas de adoptar esta modalidad es reducir y segmentar los problemas que pudiera

existir dentro de esta red para no afectar los otros servicios que operan en la red general del campus.

Hay que considerar que el diseño de la nueva red es a base de tecnología Cisco, lo cual asegura una alta disponibilidad, confiabilidad, seguridad del servicio y gestión de la infraestructura propuesta en el presente proyecto.

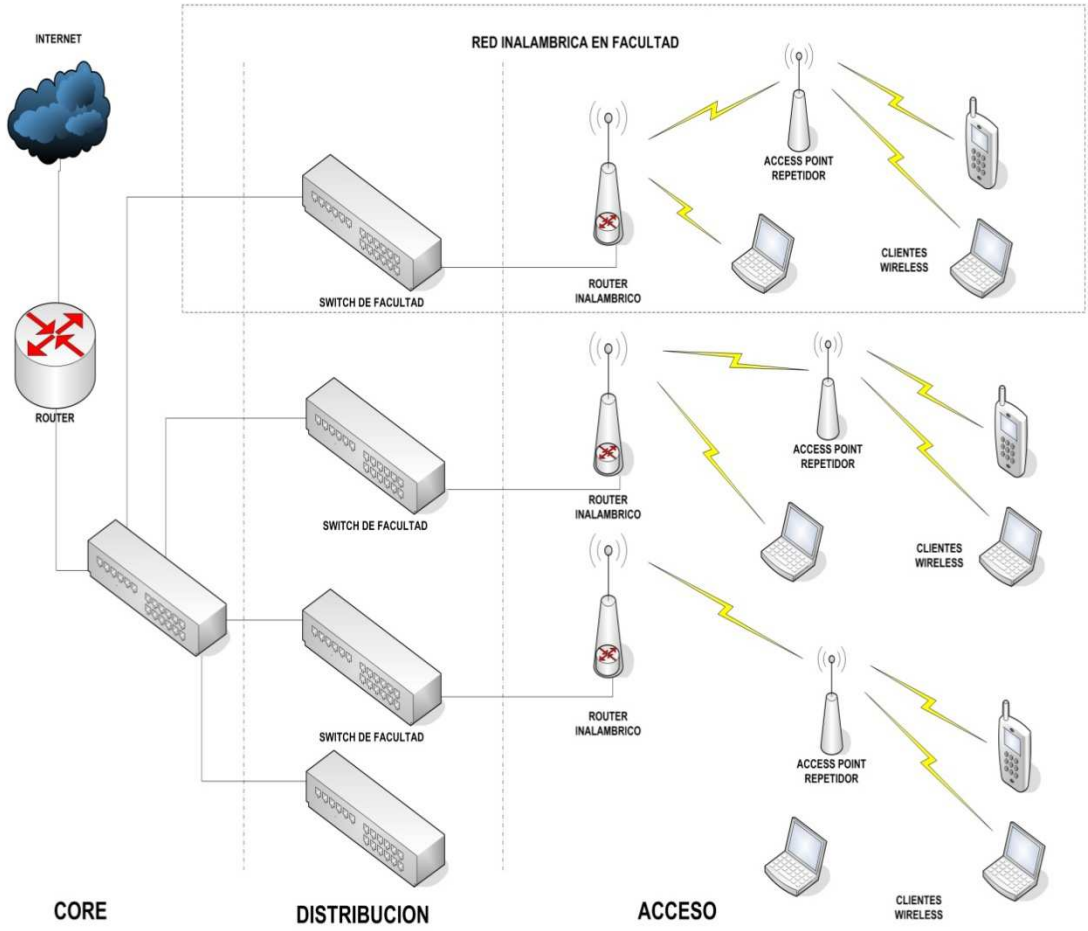


Figura 1.1 Esquema de red inalámbrica en la UCSG

Fuente: Autores

1.2. Antecedentes

En los inicios de las redes informáticas, estas eran fijas o estáticas. En 1969, cuando se creó la primera de esas redes de la historia (ARPANET), las redes se basaban en un enlace punto a punto fijo. Pero hubo visionarios que ya hablaban de la importancia de la movilidad en la red para el futuro.

La movilidad trae consigo el concepto de *wireless*, un concepto que no fue hasta 1971 cuando un grupo de investigadores bajo la dirección de Norman Abramson, en la Universidad de Hawái, crearon el primer sistema de conmutación de paquetes mediante una red de comunicación por radio, dicha red se llamó ALOHA. Ésta es la primera red de área local inalámbrica, estaba formada por siete computadoras situadas en distintas islas que se podían comunicar con un ordenador central al cual pedían que realizara cálculos. (Informática, 2010)

Uno de los primeros problemas que tuvieron y que tiene todo nuevo tipo de red inventada fue la MAC (*Medium Access Control*, Control de Acceso al Medio), es decir, el protocolo a seguir para evitar que las distintas estaciones solapen sus mensajes entre sí. En un principio se solucionó haciendo que la estación central emitiera una señal intermitente en una frecuencia distinta a la del resto de computadoras mientras estuviera libre, de tal forma que cuando una de las otras estaciones se disponía a transmitir, antes "escuchaba" y se cercioraba de que la central estaba emitiendo dicha señal para entonces enviar su mensaje, esto se conoce como CSMA (*Carrier Sense Multiple Access*, Acceso Múltiple por Detección de Portadora). (Informática, 2010)

A finales de la década de los setenta se publicaron los resultados de un experimento consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica llevada a cabo por IBM en Suiza. (Informática, 2010)

En 1999 Nokia y Symbol Technologies crearon WECA (*Wireless Ethernet Compatibility Alliance*, Alianza de Compatibilidad Ethernet Inalámbrica) que en 2003 fue renombrada a WI-FI *Alliance*, el objetivo de ésta fue crear una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurar la compatibilidad de equipos. Hoy en día las redes inalámbricas son indispensables convirtiéndose en el soporte de los campus universitarios ya a que ayudan a su mejor desarrollo de actividades y servicios. (Informática, 2010)

En la ciudad de Guayaquil, se encuentra la Universidad Católica de Santiago de Guayaquil, ésta institución de Educación Superior fue creada el 17 de mayo de 1962. El Campus Universitario de la UCSG, consta de 9 facultades cada una con bloques de aulas y oficinas o áreas administrativas, un Aula Magna, una Capilla, Biblioteca General, edificio de la Federación de Estudiantes, Asociación de Profesores, un coliseo, bares, restaurantes, zonas de parqueo y descanso.

Los inicios del Wi-Fi en la universidad fueron en sectores específicos como en la Biblioteca General y en la Asociación de Profesores que fueron los primeros en contar con esta tecnología. La red *wireless* de campus universitario fue implementada en el 2009 y se inició con un ancho banda de 2 Mbps, el siguiente año pasó a 3 Mbps y actualmente es de 5 Mbps, hasta la fecha se han implementado redes inalámbricas en todas las facultades.

El internet que recibe la UCSG por parte de la empresa TELCONET es de dos tipos, el internet total para la universidad de orden comercial para la navegación del cual solo 5 Mbps son asignados a la red inalámbrica mediante un *software* manejador de ancho de banda y el otro tipo de internet es la conexión hacia la red Académica Avanzada del Ecuador (RED CEDIA).

La red *wireless* del campus, actualmente consta de redes independientes en cada una de las facultades e incluso dentro de cada una de ellas existen varias redes. La Facultad de Ciencias Económicas y Administrativas y la Biblioteca General son las

únicas unidades académicas de la universidad que no están bajo la administración del Centro de Cómputo y por lo tanto tiene una infraestructura de internet independiente y el WI-FI no está dentro de los 5 Mbps que se indicó anteriormente, mientras que la Facultad de Especialidades Empresariales es la única que posee en su infraestructura con equipos Cisco.

1.3. Definición del problema

Por la deficiente infraestructura con que cuenta la UCSG no se tiene una cobertura total con las redes WLAN existentes provocando la falta de conectividad en varios sectores del campus universitario.

1.4. Objetivos

Los objetivos planteados para este proyecto son los siguientes:

1.4.1 Objetivos General

Diseñar una red WLAN para ampliar la cobertura dentro del campus de la UCSG con equipos marca Cisco, para mejorar el acceso inalámbrico que es de gran utilidad para docentes y estudiantes.

1.4.2 Objetivos Específicos

- Conocer la arquitectura en general, los componentes de *hardware* y *software*.
- Diagnosticar la situación de la infraestructura inalámbrica en el campus de la UCSG.
- Diseñar una nueva red WLAN que mejore la situación actual del acceso inalámbrico.
- Evaluar la red mediante las herramienta de monitoreo *Solarwinds Network Performance Monitor, Observer y Visiwave.*

- Determinar un presupuesto para una futura implementación.
- Realizar un estudio económico de la mejor propuesta presentada en el presupuesto de implementación de la solución.

1.5. Justificación

La propuesta que se plantea en este proyecto es una alternativa viable para brindar un mejor servicio de conexión WI-FI a la comunidad de la UCSG que le permita acceder a información y a todos los recursos de internet de los cuales hacen uso frecuentemente por diversos motivos desde un equipo portátil, teniendo la opción de desplazarse por las diferentes ubicaciones de la institución.

Son claras las necesidades actuales, tales como expandir el área de cobertura, mejorar la intensidad de la señal, administrar los equipos por medio de una plataforma de gestión centralizada y optimizar el consumo de ancho de banda, por lo que se toma la iniciativa de proponer un diseño de red moderno, con la más alta tecnología del mercado para la universidad y con el respectivo análisis económico.

Los usuarios utilizarían al máximo esta solución ya que las redes inalámbricas de área local han tomado un papel muy importante en la sociedad en lo que se refiere a la transferencia y acceso a la información, en la actualidad el acceso a internet es tan necesario como un libro para expandir sus conocimientos y complementar lo recibido en los salones de clases. Hoy en día el desarrollo de la sociedad está enmarcada en un nivel tecnológico “la tecnología no se puede distinguir fácilmente de lo humano… pues se tiene dentro, cerca, fuera lo habitamos y nos habita”. (Fernández, 1996)

A nivel administrativo la solución planteada ofrecerá una plataforma de gestión propietaria para la configuración, administración, monitoreo, detección y corrección de fallas, optimizando de esta manera el manejo de los recursos y personal técnico de la universidad.

Se escogió la marca Cisco para el diseño ya que ofrece una innovación constante que le permitirá a la universidad obtener una ventaja tecnológica y los equipos Cisco trabajan mejor en conjunto en una autentica arquitectura de red.

1.6. Hipótesis

El diseño de una red WI-FI para su posterior implementación con tecnología de punta que permita una mayor y más amplia cobertura, como la propuesta en el presente proyecto brindará las facilidades necesarias de cobertura y acceso para la comunidad estudiantil y docente del campus de la UCSG.

Como ya se indicó en este capítulo, la propuesta a presentarse para la UCSG es de tecnología CISCO, por esta razón en el siguiente capítulo se hará un análisis de ella, incluyendo los equipos que utiliza.

1.7. Metodología

La metodología es el conjunto de procedimientos (métodos y técnicas) que se aplican apara responder al problema de la investigación.

Para el desarrollo de la presente tesis de grado, se utiliza el método de análisis en las que se identifican las causas y efectos del mal servicio de WIFI que posee la UCSG y el método exploratorio en la que nuestro propósito es analizar la red existente del campus que es un tema que no ha sido abordado antes, no posee antecedentes por lo que era necesario recolectar información realizando una evaluación detallada, identificando problemas para luego establecer soluciones.

CAPITULO II

CISCO: SU HISTORIA, METODOLOGÍA Y TECNOLOGÍA

2.1. La historia de Cisco

Leonard Bosack y Sandra Lerner, un matrimonio de científicos que trabajaban en el departamento de computación de la Universidad de Stanford en los años 80, decidieron crear Cisco en diciembre de 1984. (Rodríguez, 2007)

El nombre es fruto de una sencilla casualidad, desde la ventana solían ver un cartel en el que decía San Francisco, ciudad en la que empezaría su internacionalización. Un árbol tapaba parcialmente la vista del cartel de manera que se leía **cisco** separado del resto del nombre de la ciudad. (Rodríguez, 2007)

Pero el nombre vino después del "descubrimiento", aun en *Stanford* diseñaron un sistema para que computadores con diferente red se pudieran comunicar. Este fue un trabajo conjunto con otro compañero: William Yeager. A raíz de esta idea siguieron trabajando en Cisco hasta convertirla en lo que es hoy. (Rodríguez, 2007)

En 1986, Cisco lanzó su primer *multiprotocol router*, el *Advanced Gateway Server* o AGS. Este equipo operaba con solo dos protocolos de red al inicio, IP (*Internet Protocol*, Protocolo de Internet) y Xerox PARC (*Palo Alto Research Center*, Centro de Investigaciones Palo Alto) *Universal Protocol*. Tenía tres tipos de interfaces *Ethernet*, ARPANET y Serial de baja velocidad. Inicialmente, la red Ethernet de la Universidad de Stanford era el único lugar donde el AGS podía realizar tareas de enrutamiento entre protocolos soportando computadores con protocolo IP y PUP.

Alrededor de toda la nación, programadores e ingenieros en laboratorios empezaron a comunicarse utilizando el protocolo IP sobre la NSFNet (*National Science*

Foundation Net, Red desarrollada por la Fundación Nacional de Ciencia), la precursora del Internet. Tener una red diferente para la comunicación utilizando varios proveedores era muy costoso. La innovación de Cisco fue el *multiprotocol router* que permitía la operación de diferentes sistemas a través de la misma infraestructura.

En 1988, la mayoría de compañías aún confiaban en los *bridges* para unificar sus redes. Mientras una red puenteada podía soportar todos los protocolos, era extremadamente vulnerable a lo que se conoce como tormenta de *broadcast*. En casos de fallas de *software*, una tormenta de *broadcast* llenaría toda la red con una enorme cantidad de paquetes, dejando al final la red fuera de servicio.

Los *routers* eliminaban las tormentas de *broadcast* porque creaban subredes o redes individuales, que eran parte de la red física pero a su vez separadas lógicamente. El uso de *bridges* era permitido en zonas reducidas de la red que utilizaban el mismo protocolo.

Para 1989 la NSFnet crecía rápidamente, pero este crecimiento estaba causando problemas debido a que el protocolo de enrutamiento externo utilizado en el *backbone* fue diseñado para una red pequeña. Miembros de la IETF (*Internet Engineering Task Force*, Grupo Especial sobre Ingeniería de Internet) pudieron notar que cientos de redes habían ingresado a las tablas de enrutamiento. Kirk Lougheedy Yakov Richter desarrollaron el formato de los paquetes para un nuevo protocolo de enrutamiento que años más tarde se convertiría en BGP (*Border Gateway Protocol*,), una pieza de tecnología muy importante que ha sido adoptada por la gran mayoría de proveedores de servicio.

En 1990 Cisco lanza el primer Simposio llamado *Networkers*, un evento anual que ayudaría a brindar información sobre los avances tecnológicos a la creciente comunidad. Cisco, como sus clientes, comenzó a utilizar el Internet como una herramienta de negocios al final de los 80’s. En este año Cisco lanza su AGS+ con

un nuevo puerto llamado cBus, El cBus aceleró el desempeño del enrutamiento hasta 20.000 paquetes por segundo.

Conforme las compañías conectaron sus redes entre sí se tuvieron que enfrentar a un nuevo desafío: asegurar la compatibilidad entre múltiples tipos de dispositivos de red. El Cisco IOS era el sistema operativo mayormente seleccionado para diseñar redes de empresas y asegurar la compatibilidad de dispositivos.

En 1993 el Internet dio un gran paso con el diseño de la interfaz gráfica para los usuarios, el uso del Internet se incrementó rápidamente en cuanto los usuarios pudieron observar gráficamente a través de la información disponible en línea. Los negocios y los proveedores de servicio demandaban *routers* de alta calidad para lograr manejar la creciente cantidad de información. Fue en este año que se lanzó al mercado el Cisco 7000, el cual sería nombrado como el producto más influyente de los años 90's por la revista *Network Computing*.

Contando con una variedad de *switches* de compañías adquiridas por Cisco, se introdujo la idea de los *multilayer switches*. El mensaje fue "los switches no son únicamente para almacenarlos en el cuarto de cableado, estos equipos también pueden mejorar las capas de agregación y núcleo".

En 1995, el lanzamiento del Cisco 7500 que incluía un procesador independiente para enrutar/switchear y un VIP (*Versatile Interface Processor*, Procesador de Interfaz Versátil) que lograba eliminar los conocidos cuellos de botella en el traspaso de información. Este dispositivo logró alcanzar 1 millón de paquetes procesados por segundo y rápidamente se convirtió en un *router* principal en el *BackBone* de Internet.

En 1996, Cisco dejó de vender únicamente productos y empezó a ofrecer soluciones de negocios *end-to-end*. Para esta fecha Cisco poseía el hardware y además el software que lograba unificarlos, el Cisco IOS (*Internetworking Operating System,*

Sistema Operativo de Interconexión de Redes). Este año además marcó la historia de los proveedores de servicio revolucionando la forma en la que se diseñaban sus redes, debido al lanzamiento de la tecnología MPLS (*Multiprotocol Label Switching*, Conmutación Multiprotocolo por Etiquetas), la cual combinaba la inteligencia y la escalabilidad del enrutamiento con la confiabilidad de redes de transporte tradicionales. Actualmente la mayoría de redes de los grandes proveedores de servicio están diseñadas utilizando MPLS.

En 1997, se introdujo el programa de Academias de Redes Cisco, este programa inició como un proyecto e-*learning* para brindar a los estudiantes las habilidades esenciales sobre la tecnología de Internet en la economía global. Cisco realizó una inversión de 18 millones de dólares en pensum, equipamiento y recursos para 57 colegios, universidades y escuelas técnicas en los Estados Unidos de Norteamérica. Luego de 7 años existen más de 400 mil estudiantes en más de 149 países que se encuentran activos en este programa y alrededor de 10 mil academias operando.

En 1999, la visión de Cisco del Internet que soportaría varios medios de información como audio y video llevó a presentar la AVVD (*Architecture for Voice, Video and Integrated Data*, Arquitectura para Voz, Video y Datos Integrados), la cual contenía el diseño para la convergencia de voz, video y datos a través de una red IP. Actualmente más de 150 mil organizaciones utilizan el Cisco AVVD para implementar comunicaciones IP que incluyen telefonía, mensajes, *contact centers*, *web* y conferencias de audio o video. Cisco adquirió la compañía *Aironet Wireless Communications* marcando su entrada al mercado inalámbrico permitiendo a sus clientes ganar capacidades inalámbricas que extenderían sus redes locales.

Para el año 2000 la mayoría de los negocios adoptaron el modelo *e-business*, utilizando el Internet, las empresas conformaban relaciones más fuertes con sus clientes, proveedores, asociados y empleados. Con este nuevo esquema, la seguridad fue la nueva prioridad para mantener asegurado el modelo *e-business*. En este año se lanzó el diseño SAFE (*Security Architecture for Enterprise*, Arquitectura de

Seguridad para Empresas) con un enfoque modular que aplica seguridad a diferentes secciones de la red según sea necesario, incluyendo la capa de núcleo, distribución, granja de servidores y los sistemas de administración. En conjunto a este diseño, Cisco ofreció varios productos de seguridad para lograr tener un red que se pueda defender por sí misma. El diseño SAFE sería luego aplicado a los proveedores de servicio, colocando a Cisco como líder en la protección de las redes en SP's (*Service Provider*, Proveedor de Servicio) contra los crecientes ataques cibernéticos.

El crecimiento de Cisco en los mercados empresariales durante los años 90 nunca disminuyó su alta ubicación en la comunidad tecnológica, técnicos de Cisco continuaron colaborando en importantes estándares al IETF. Cisco anunció su participación en el desarrollo del estándar para soportar IPv6 de la IETF en el año 2001.

Un gran giro en la forma que las compañías utilizan la tecnología para comunicarse de varias maneras (audio, video, voz e inalámbrica) se presentó con la posibilidad de migrar a una infraestructura IP. Utilizando telefonía IP se lograba ahorrar el costo de llamadas de larga distancia debido a que la información era enviada a través de la red IP.

En el corto periodo de 20 años, Cisco ha pasado de una ilusión de alguien a una compañía multimillonaria con una presencia y alcance global. A través de su tecnología, su gente y su visión esta empresa ha impactado la manera en la que el mundo vive, trabaja, juega y aprende. En Cisco en lugar de descansar para tomar aliento, el movimiento que dará forma al futuro ya se ha puesto en marcha.

2.2. El Enfoque *Ppdioo Life-Cycle* para redes

El PPDIOO de Cisco define la metodología del ciclo de vida de los servicios requeridos por una red. Las siglas de ésta metodología significan Preparar, Planear, Diseñar, Implementar, Operar y Optimizar. (Cisco Press, 2012)

Preparar: Envuelve el establecer los requerimientos organizacionales, desarrollar la estrategia de la red y proponer una arquitectura conceptual de alto nivel identificando las tecnologías que brindarán el mejor soporte. (Cisco Press, 2012)

Planear: Identifica los requerimientos iniciales de la red basado en metas, necesidades de usuario y demás. Determinar si la infraestructura existente soportará la tecnología propuesta. Es muy útil para administrar las tareas, responsabilidades, puntos clave y recursos requeridos para los cambios que se realizarán a la red. (Cisco Press, 2012)

Diseñar: Los requerimientos establecidos en la fase anterior sirven de guía a los especialistas en diseño. Las especificaciones del diseño de una red es un diseño detallado y comprensivo que debe cumplir con los actuales requerimientos de negocios y técnicos e incorpora las especificaciones de soporte, disponibilidad, confiabilidad, seguridad, escalabilidad y desempeño. La fase de diseño es la base para la implementación. (Cisco Press, 2012)

Implementar: La red es construida de acuerdo a las especificaciones de diseño con el objetivo de integrar dispositivos sin interrumpir las funciones de la red existente o creando puntos de vulnerabilidad. (Cisco Press, 2012)

Operar: Es la fase final de pruebas de un diseño para determinar lo adecuado del mismo. Involucra el mantenimiento de la integridad de la red a través de las operaciones del día a día, incluyendo alta disponibilidad y reduciendo gastos. La corrección y monitoreo de desempeño y fallas que ocurren a diario brindan la información necesaria para la fase de optimización. (Cisco Press, 2012)

Optimizar: Implica la administración proactiva de la red. El objetivo de ésta tarea es identificar y resolver problemas antes de que afecten a la organización. Los problemas en una red se presentan cuando se carece de una administración proactiva

por lo que no se puede predecir y mitigar las fallas. La fase de optimización puede denotar la necesidad de un rediseño si se llegan a presentar muchos errores dentro de la red, el desempeño no cumple las expectativas o nuevas aplicaciones son necesarias para soportar los requerimientos organizacionales y técnicos. (Cisco Press, 2012)

2.3. Metodología del diseño de ppdioo

La metodología del diseño de una red bajo este esquema está compuesta por tres pasos muy importantes:

- Identificar los requerimientos del cliente.
- Descripción o análisis de la red existente y sus nodos.
- Diseño de la topología de red y soluciones a implementar.

2.3.1 Identificando los requerimientos del cliente

El diseñador tiene 5 metas que alcanzar durante la recolección de información que definen los requerimientos del cliente. Son necesarias varias sesiones con los miembros del *staff* del cliente para obtener información y documentación necesarias para el proceso de diseño.

Es importante indicar que los 5 pasos a seguir no son unidireccionales, es decir, en cualquier momento durante el proceso el diseñador puede verse obligado a retroceder y plantear nuevos requerimientos. Los pasos necesarios para este proceso son los siguientes:

- **Paso 1.** Identificar las aplicaciones y servicios de red planeados a utilizar.
- **Paso 2.** Definición de las metas organizacionales.
- **Paso 3.** Definir y revisar las posibles restricciones organizacionales.
- **Paso 4.** Definir las metas de carácter técnico.

- **Paso 5.** Definir y revisar las posibles restricciones técnicas.

Luego de completar la recolección de información, el diseñador estará listo para interpretar y analizar la información para elaborar la propuesta de diseño.

Identificando las aplicaciones y servicios

Dentro del proceso de recolección de información es muy importante determinar las aplicaciones que se utilizarán y que tan importantes son. La persona encargada del diseño hace uso de muchas tablas para mantener la organización dentro del proceso.

La tabla para este proceso capta la siguiente información:

- Tipo de aplicaciones planeadas a usar, por ejemplo: e-*mail*, voz sobre IP, navegación, video sobre demanda, bases de datos, transferencia de archivos, etc.
- Aplicaciones que serán usadas, por ejemplo: *Microsoft Outlook*, Cisco *Unified Meeting Place*, etc.
- Importancia de ciertas aplicaciones denotadas con palabras clave como: crítico, importante, no importante.
- Comentarios adicionales.

En la tabla 2.1 se muestra las aplicaciones y servicios.

Tabla 2.1 Identificación de aplicaciones y servicios.

Fuente: (*Systems, Designing Cisco Network Service Architectures*, 2010)

Tipo de Aplicación	Aplicación	Importancia	Comentarios
Colaboración	Cisco *Unified Meeting Place*	Importante	Compartición de presentaciones durante reuniones

Navegación	Internet Explorer, Opera, Firefox	Importante	-
Video sobre demanda	IP/TV	Crítico	-
Base de Datos	Oracle	Crítico	-
Soporte	Aplicaciones del cliente	Crítico	-

La planeación de la infraestructura para servicios también es realizada para tener las consideraciones respectivas durante el proceso de diseño. Aquí se podrá incluir las siguientes opciones: seguridad, calidad de servicio, telefonía IP, *multicast*, servicios AAA (*Authentication Autorization and Accounting*, Autenticación Autorización y Contabilización).

Definición de las metas organizacionales

Una solución de red efectiva debe ser capaz de soportar los procesos de la organización. Las metas de esta deben ser consideradas durante el diseño para brindar la mejor solución de red.

Anteriormente los diseñadores daban inicio al proceso con los requerimientos técnicos, en la actualidad se prefiere empezar con los requerimientos de la organización para obtener una red bien diseñada enfocada en satisfacer las necesidades del cliente. Con esto se obtiene que el usuario vea a la solución planteada como un arma estratégica para mejorar su productividad, dando de esta manera éxitos al proyecto.

Para lograr identificar las metas organizacionales se debe cumplir con lo siguiente:

- Identificar y conversar con el cliente sobre sus requerimientos, las metas que desean cumplir y finalmente el propósito de la red.
- Determinar los criterios de éxito.
- Entender las consecuencias en caso de fallas.

Hay algunas preguntas básicas que ayudan a los diseñadores en esta etapa:

- ¿Qué está tratando de lograr?
- ¿Cuáles son los retos en negocios que está afrontando actualmente?
- ¿Cuáles son las consecuencias de no resolver estos problemas?
- ¿Cuáles son las aplicaciones críticas?
- ¿Cuál es el objetivo principal de este proyecto?
- ¿Cuáles son las preocupaciones principales de ejecutar este proyecto?

Definir las restricciones organizacionales

Al analizar las metas organizacionales no debemos descuidar las posibles restricciones que posea el cliente que pudieran afectar el desarrollo del diseño. A continuación se analizan algunas de las restricciones más frecuentes:

- **Presupuesto:** Recursos limitados regularmente obligan a los diseñadores a desarrollar un proyecto que pueda ser adquirido que incluya compromisos de disponibilidad, operabilidad, desempeño y escalabilidad. Dentro del presupuesto se incluye la compra de *hardware*, *software*, licencias, entrenamiento, etc. Se debe conocer hasta cuanto podría invertir la organización para proponer el diseño adecuado.
- **Personal:** La disponibilidad de personal con entrenamiento adecuado dentro de la organización puede llegar a ser una consideración del diseño, más aun cuando el cliente contrata el soporte y administración de su red en forma de *outsorcing*.

- **Políticas:** Ninguna organización es igual a la anterior porque ciertos factores cambian dependiendo de sus políticas, protocolos, estándares, aplicaciones y marcas. Éstas políticas deben ser entendidas para desarrollar la solución de manera correcta.
- **Programación de tareas:** El diseño de red incluye tareas programadas que se encuentran regularmente relacionadas. Los tiempos de cada tarea deben ser presentados al administrador del proyecto dentro de la organización para que sean aprobados.

Definir las metas de carácter técnico

Es una realidad que conforme crece una red dentro de una empresa, mayormente dependiente de esa red es la organización que la utiliza. La información y las aplicaciones que están disponibles dentro de la red dependen de la disponibilidad de la misma. Algunas metas son las siguientes:

- **Mejorar la capacidad de tráfico:** Ésta característica de una red regularmente se reduce conforme la cantidad de usuarios y aplicaciones son utilizadas. La primera tarea del diseñador es mejorar esta función e incrementar el desempeño realizando un *upgrade* a las velocidades de los *links*, segmentando la red o ambos a la vez.
- **Reducir el *downtime* y costos relacionados:** Cuando se presenta un problema en la red, el tiempo que se encuentre fuera de funcionamiento debe ser mínimo. La red debe responder lo suficientemente rápido para minimizar los costos relacionados.
- **Simplificar la administración de la red:** Ésta tarea debe ser considerada para facilitar el entendimiento y uso de la red.
- **Mejorar la seguridad y confiabilidad:** Debido a las actuales amenazas (internas y externas) que pueden afectar a una red, las seguridades deben ser actualizadas para asegurar las aplicaciones e información.

- **Modernizar las tecnologías utilizadas:** Conforme se adquieren nuevas tecnologías y aplicaciones se debe considerar la modernización del equipamiento de la red.
- **Mejorar la escalabilidad:** La red debe permitir actualizaciones y crecimiento a futuro.

Definir las restricciones técnicas

Identificar las posibles restricciones que existen en la red actual previos al diseño es necesario para poder determinar los cambios que son requeridos. Entre las principales restricciones se puede mencionar:

- Disponibilidad de ancho de banda.
- Equipamiento existente.
- Compatibilidad de aplicaciones.

2.3.2 Descripción de la red existente y sus nodos

Lo primero que se debe hacer es obtener la mayor cantidad de información posible sobre la red existente. La documentación existente, auditorías de red, análisis de tráfico, etc. pueden proveer información importante que el diseñador podría utilizar. Algunos pasos a seguir son los siguientes:

- **Paso 1.** Obtener la documentación existente de la red y solicitar detalles al cliente para lograr descubrir datos adicionales. Se debe tener en cuenta que la información que se encuentre documentada puede tener errores o imprecisiones.
- **Paso 2.** Realizar una auditoría de la red para tener una visión más detallada de la misma. De ser posible se debe utilizar la información recopilada para describir al cliente las aplicaciones y protocolos utilizados en la red. Realizar una auditoría de la red puede resultar muy

costoso en términos de tiempo y esfuerzo, por lo que regularmente es enfocada a áreas específicas con información vital para el proceso de diseño.

- **Paso 3.** Emitir un reporte a partir de la información obtenida en los pasos anteriores para describir el estado actual de la red. A partir de este informe se pueden plantear requerimientos de *hardware* y *software* que soporten la solución propuesta.

2.3.3 Diseñar la topología de red y soluciones

Debido a que el diseño de una red no es una tarea sencilla, existen varias recomendaciones para hacerlo y una de ellas es utilizar el método *top-down*, el cual clarifica los objetivos del diseño y da inicio al mismo desde la perspectiva de las aplicaciones requeridas y soluciones a implementar. Su principal objetivo es dividir el proceso de diseño en mini procesos que simplifiquen el trabajo.

Antes de empezar el diseño se debe definir el enfoque del trabajo, es decir, determinar si el diseño es para una nueva red, modificaciones de una red, un segmento o módulo, varias LAN's, una WAN o una red de acceso remoto.

Las prácticas recomendadas de un modelo estructurado para diseño de redes consisten en dividir las tares en procesos relacionados entre sí, reduciendo su complejidad, de la siguiente manera:

- **Paso 1.** Identificar la aplicación que necesita el cliente.
- **Paso 2.** Identificar los requerimientos de conectividad lógica de la aplicación basado en los requerimientos de servicios y soluciones necesarios.
- **Paso 3.** Dividir la funcionalidad de la red para el desarrollo de los requerimientos de infraestructura y de la estructura jerárquica.

- **Paso 4.** Diseñar cada elemento de la red por separado y guardando relación con los demás. La infraestructura y el diseño de los servicios están muy conectados ya que ambos operan sobre la misma estructura física y lógica.

Luego de concluir la etapa de diseño dentro del esquema PPDIOO, el siguiente paso es desarrollar los planes de migración e implementación de manera detallada. Mientras más detallada se entregue la información de implementación, menos conocimiento sobre el diseño se requiere del ingeniero encargado de implementar.

2.4. Beneficios del enfoque de *life-cycle*

Este enfoque provee varios beneficios además de un diseño organizado en procesos de la red. Las principales razones para aplicar este enfoque son las siguientes:

- Reducción del costo total de una red.
- Incremento de la disponibilidad.
- Mejora la agilidad del negocio.
- Acelera el acceso a servicios y aplicaciones. (Cisco Press, 2012)

El costo total de una red es especialmente importante en la actualidad. Los precios más bajos asociados con los gastos de IT *(Information Technlogy*, Tecnología de la Información) están siendo buscados agresivamente por las empresas. Esto se lo consigue por medio de las siguientes acciones:

- Identificación y validación de los requerimientos tecnológicos.
- Planeación de requerimientos para cambios de infraestructura y recursos.
- Desarrollo de un diseño de red sólido que se alinea con los requerimientos técnicos y del negocio al mismo tiempo.
- Acelerando una implementación exitosa.
- Mejorando la eficiencia de su red y del *staff* que la administra.

- Reducción de gastos operativos por medio de la mejora en la eficiencia de los procesos operativos y herramientas. (Cisco Press, 2012)

La alta disponibilidad siempre ha sido un factor de gran prioridad pues la caída de la operación de una red puede significar grandes pérdidas para las empresas. El incremento de esta propiedad al utilizar este enfoque se logra por las siguientes acciones:

- Identificar el estado de la seguridad de la red y la capacidad de soportar el diseño propuesto.
- Especificación del *hardware* correcto y las versiones de *software* adecuadas.
- Desarrollo de un diseño de red sólido y validación de la operación adecuada de la red.
- Implementación por fases y pruebas respectivas del diseño propuesto antes de la puesta en marcha.
- Mejora de las capacidades del *staff* de la empresa.
- Monitoreo proactivo del sistema y reconocer las amenazas de disponibilidad y alertas.
- Monitoreo proactivo de fallas de seguridad y definición de las soluciones. (Cisco Press, 2012)

En la actualidad las empresas necesitan reaccionar lo más rápido posible a los cambios en la economía. Aquellas empresas que actúan inmediatamente ganan ventajas competitivas. Se mejora la agilidad de la empresa por medio de las siguientes acciones:

- Definición de estrategias tecnológicas.
- Preparación de los sitios necesarios que soporten la solución que se requiere implementar.

- Integración de los requerimientos técnicos y las metas del negocio en un diseño detallado que demuestra la funcionalidad de la red.
- Instalando, configurando e integrando los componentes del sistema de una manera eficiente y experta.
- Incrementando el desempeño constantemente. (Cisco Press, 2012)

El acceso rápido a las aplicaciones de red y servicios es crítico para la producción y se obtiene por medio de las siguientes acciones:

- Identificar y mejorar la capacidad de aceptar el esquema actual y el diseño propuesto de servicios y tecnología.
- Mejorar la efectividad de la entrega de servicios incrementando la disponibilidad, capacidad de recursos y desempeño.
- Optimizar la confiabilidad, disponibilidad y estabilidad de la red y las aplicaciones que operan sobre ella.
- Manejo y resolución de problemas que afecten el sistema y mantener el *software* de aplicaciones actualizado. (Cisco Press, 2012)

2.5. Modelo jerárquico

Este modelo, cuya estructura se muestra en la figura 2.1, es utilizado para tener una visón de la red de manera modular lo cual facilita las tareas de diseño e implementación de una red escalable. Está conformado por las capas Núcleo, Distribución y Acceso. Provee flexibilidad durante el diseño y facilita la implementación y resolución de problemas.

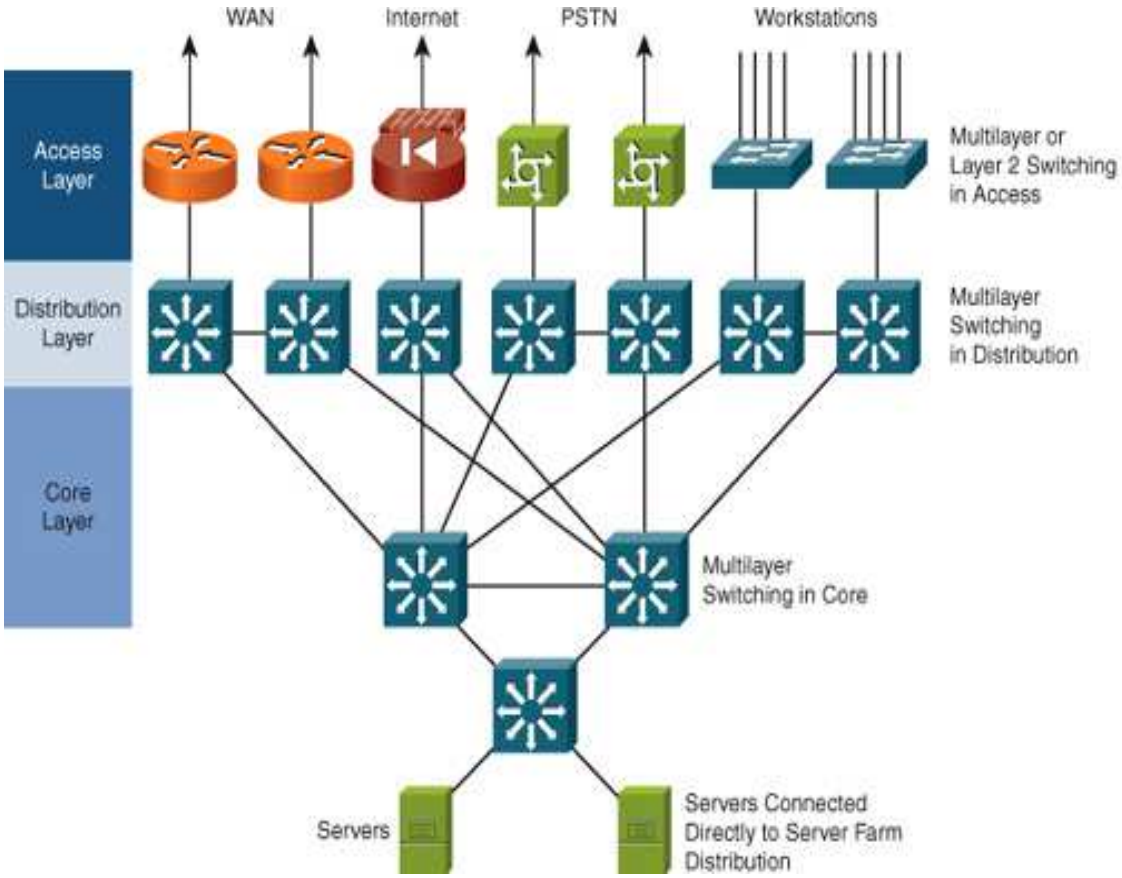


Figura 2.1 – Modelo Jerárquico

Fuentes: http://jampad.net/Library/arch/

2.5.1 Capa de núcleo

Conocida también como *backbone* es la capa que está diseñada para transportar paquetes con alta velocidad y lo más rápido posible, brindando servicios que optimizan la comunicación dentro de la red. Debido a su gran importancia esta capa debe tener alta disponibilidad y poder adaptarse rápidamente a los cambios, es decir, debe poder mantener conectividad incluso si los enlaces que los conectan fallan. Mostrándose como una capa que ofrece servicio sin detenerse.

Un diseño desarrollado para alta tolerancia a las fallas asegura que los problemas que se presenten no tendrán un mayor impacto en la conectividad de la red. Asimismo se

debe evitar la implementación de servicios complejos y no puede permitir conexión a usuarios directamente.

2.5.2 Capa de distribución

Al contrario de las otras, la capa de distribución es multifuncional ya que concentra las conexiones a lo largo la infraestructura, se utilizan *switches* para segmentar los grupos de trabajo con el propósito de aislar problemas que se puedan presentar en la red. Controla el acceso a los recursos que se encuentran disponibles en el núcleo y por esto debe contar con un efectivo manejo del ancho de banda. Se incorporan servicios de QoS (*Quality of Service*, Calidad de Servicio) para diferentes protocolos, control de tráfico basado en políticas separando las capas de núcleo y acceso apropiadamente, funciones de seguridad para permitir o negar el paso de paquetes por medio del uso de ACL *(Access Control List*, Lista de Control de Acceso). Similarmente en esta capa se concentran las conexiones WAN que sirven de borde y brindan conectividad al exterior de la red. Posee una tarea única, la de establecer control sobre los servicios brindados a las capas de acceso y núcleo.

2.5.1 Capa de acceso

Es la capa donde se conectan a la red los dispositivos finales (computadoras, impresoras, cámaras, etc.). También se puede encontrar aquí aquellos dispositivos que extienden la red como los teléfonos IP y los AP. Una de sus características principales es la alta cantidad de puertos que se puede llegar a tener dependiendo de la magnitud de la red empresarial o del campus.

Es la capa con mayor variedad de características técnicas debido a la gran cantidad de equipos que se pueden conectar y los diferentes servicios que se brindan. Los dispositivos ubicados en esta capa deben proporcionar conectividad sin comprometer la integridad de la red. Por ejemplo, deben ser capaces de reconocer un *host* que trata de enviar información que perjudicará el estado actual de la red.

2.6. Diseño *Wireless*

El primer paso para el diseño e implementación de una solución *wireless* es realizar un análisis de RF (Radio Frecuencia) en el sitio para asegurar la operación deseada. Por medio de este proceso el diseñador estudia las instalaciones físicas para entender el comportamiento y características RF en el ambiente, detección de interferencias, áreas de cobertura y la ubicación de la infraestructura inalámbrica.

En este tipo de redes pueden existir varios problemas que impidan que la señal RF tenga la cobertura deseada, es por esto que la tarea del diseñador será encontrar estas limitaciones para superarlas. Es necesario el uso de herramientas que puedan captar principalmente las interferencias a la señal RF,

Durante esta fase se podrá identificar las posiciones y cantidad de equipos necesarios para dar el acceso inalámbrico a los usuarios. Los requerimientos del cliente sobre la red inalámbrica deben ser definidos para que sean tomados en cuenta durante el proceso de diseño.

2.6.1 Análisis del sitio

Las tareas que se deben realizar durante el análisis de sitio incluyen las siguientes:

1. **Definir los requerimientos del cliente:** Se obtiene lo que el cliente espera recibir de la solución inalámbrica como niveles de servicio, ubicación de equipos, etc.
2. **Diagrama del sitio:** Con el fin de ubicar los posibles obstáculos de RF y determinar las zonas de cobertura esperada.
3. **Inspección visual del sitio:** Identificando las posibles barreras para la señal RF como: escaleras, rejas metálicas, etc.
4. **Detección de sitios de usuarios:** Determinar los sectores con mayor cantidad de usuarios y los que raramente son usados.

5. Ubicación preliminar de los AP: Además de las ubicaciones es necesario incluir los puntos eléctricos y de red, cobertura de celdas y *overlap*, selección de canales y antenas.

6. Análisis del sitio: Asegurarse de utilizar en el análisis el modelo de AP que será usado en producción. Si es necesario, durante el análisis se podrá reubicar los AP que sea necesario.

7. Documentación de resultados: Información sobre ubicación y lecturas de señal de cobertura de la red inalámbrica.

Requerimientos del cliente: Es necesario obtener toda la información necesaria por parte del cliente para el proceso de diseño. Hay preguntas que el diseñador utiliza para lograr definir estos requerimientos de manera más rápida.

- ¿Qué tipos de dispositivos necesitan conectarse a la red inalámbrica?
- ¿Existen equipos inalámbricos o RF trabajando actualmente? ¿Estos equipos deben integrarse a la red diseñada?
- ¿Cuál será el uso de la red inalámbrica? ¿Habrá tráfico de voz?
- ¿Existen picos de servicio que deben ser tomados en cuenta?
- ¿Los usuarios inalámbricos serán estáticos o móviles?
- ¿Cuál es la cobertura esperada?
- ¿Qué nivel de disponibilidad es necesario?

Con la información recibida luego de esta serie de consultas, el diseñador será capaz de tener en cuenta ciertas consideraciones durante el diseño para cumplir las expectativas del cliente.

Identificar áreas de cobertura: Dentro del reporte del análisis se debe incluir un diagrama de cobertura, en el cual se muestren las zonas con servicio y las que fueron definidas como áreas sin cobertura por el cliente. Esto le brinda al cliente, equipo de implementación y al departamento técnico la información necesaria sobre la cobertura de cada AP ubicado.

Es necesario tratar de definir la densidad de dispositivos inalámbricos que se conectarán a la red, cada AP puede llegar a brindar conexión aproximadamente a 8 teléfonos IP o 20 dispositivos de datos únicamente.

Se debe identificar durante la inspección las áreas con posibles problemas, por ejemplo: escaleras, elevadores y lugares con equipos de microondas.

Ubicación preliminar de APs. : En esta tarea el diseñador hará uso de las herramientas que estén a su alcance para simular el ambiente en el cual será instalada la red inalámbrica. Haciendo uso de los planos del sector estas herramientas podrán estimar la cantidad de AP's necesarios para cada una de las zonas y las posibles ubicaciones que brindarán un punto de partida para el proceso de diseño.

Análisis del sitio: Para determinar las características de cobertura del sitio, es necesario realizar las siguientes mediciones durante el análisis:

- Medir el radio de cobertura.
- Fuerza de señal detrás de escaleras, oficinas, cubículos y demás.
- Desarrollar la cobertura deseada con los AP que sean necesarios.
- Establecer los canales sin tener *overlap* para disminuir interferencias.
- Repetir este procedimiento hasta que todas las zonas que requieren cobertura hayan sido analizadas.

Durante este proceso de análisis es necesario obtener la siguiente información de cada uno de los AP:

- Fuerza de señal.
- Niveles de ruido.
- Relación Señal/Ruido.
- Interferencia de canales.
- Tasa de datos.
- Tasa de pérdidas.

Documentación de resultados: La documentación del análisis realizado sirve como guía para el proceso de diseño, implementación y verificación de la infraestructura inalámbrica instalada. Un análisis detallado correctamente provee información sobre los requerimientos del cliente, cobertura, fuentes de interferencia, ubicación de equipos, consideraciones eléctricas, requerimientos de cableado. Además debe incluirse la siguiente información:

- Número total de AP's que se necesitarán.
- Número y tipos de antenas necesarias.
- Componentes de red propuestos.

Además se incluye los diagramas de cobertura y ubicación de AP dentro del informe del análisis. En lo posible se adjunta fotografías de referencia sobre los equipos y antenas que serán instalados para que se tenga una referencia de la correcta ubicación.

2.6.2 Consideraciones de diseño

Dentro de las interrogantes planteadas al cliente para poder obtener los requerimientos iniciales, existen consideraciones que el diseñador debe tomar en cuenta como:

- **¿Dónde se deben colocar los AP?** Los equipos deben ser colocados en las zonas donde existirán clientes. Operan mejor estando en ubicaciones céntricas que permiten maximizar la cobertura, son más efectivos cuando están ubicados cerca de los clientes.
- **¿Cómo recibirán energía eléctrica los equipos?** La tecnología PoE (*Power over Ethernet*, Energía sobre Ethernet) es la solución típica que nos permite reducir costos de cableado eléctrico para los equipos AP.
- **¿Cuántos WLC (*Wireless LAN Controller*, Controlador de LAN inalámbrica) son necesarios?** El número de AP's que un WLC puede soportar varía dependiendo del dispositivo seleccionado. Se deben considerar los suficientes equipos WLC para proveer redundancia y soportar la cantidad de AP's instalados.
- **¿Dónde se deben colocar los WLC?** Es recomendado que la ubicación de los WLC sea en un lugar seguro como los armarios de cableado o en el *data center*. Teniendo en consideración las debidas consideraciones de redundancia en caso de cortes eléctricos.

2.6.3 Ubicación de controladores

Es recomendable que los controladores sean colocados de tal manera que se logre evitar en lo posible el *roaming* entre controladores y latencia en el tráfico que es transmitido por la red. Existen dos formas de ubicar los controladores: distribuida y centralizada.

La recomendación general es utilizar el diseño centralizado para disminuir la complejidad durante la operación y soporte de los controladores. Se debe ubicar los controladores de manera centralizada en aquellas zonas en las que existirá *roaming* de dispositivos inalámbricos, esto es que los controladores deben encontrarse físicamente en el mismo sector.

La figura 2.2 muestra el esquema de diseño de controladores distribuidos donde se colocan los AP en la capa de acceso y el WLC en la capa de distribución.

En la figura 2.3 se muestra el diseño centralizado de controladores en el cual los AP se encuentran en la capa de acceso y el WLC se encuentra en un bloque de servicio de la capa de núcleo.

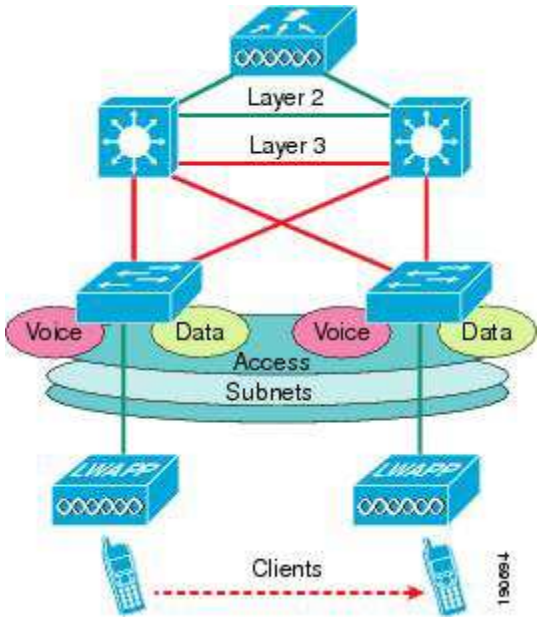


Figura 2.2 – Diseño Distribuido de WLC

Fuente:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch2_Arch.html

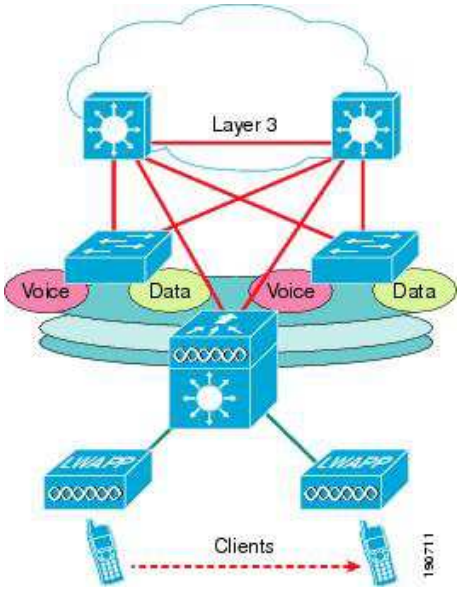


Figura 2.3 – Diseño Centralizado de WLC

Fuentes: (Systems, Enterprise Mobility 4.1 Design Guide)

En el capítulo 3 se analizarán las características fundamentales de una red WLAN a fin de poder realizar el diagnóstico de la red de la UCSG y posteriormente el diseño de la nueva red con tecnología CISCO.

CAPÍTULO III

REDES WLAN

3.1. Introducción a las Redes WLAN

Las redes WLAN representan hoy en día una solución tecnológica de gran utilidad en el sector de las comunicaciones inalámbricas, son redes que generalmente cubren distancias de los 10 a 100 metros. Estos sistemas se caracterizan por trabajar en bandas de frecuencia exentas de licencia de operación, lo cual dota a la tecnología de un gran potencial de mercado y le permite competir con otro tipo de tecnologías de acceso inalámbrico de última generación como la integración de las WLAN en entornos de redes móviles de 3G UMTS (*Universal Mobile Telecommunications System*, Sistema Universal de Telecomunicaciones Móviles) para cubrir las zonas de alta concentración de usuarios (los denominados *hotspots*), como solución de acceso público a la red de comunicaciones móviles y otras tecnologías como HyperLAN apoyada por el ETSI (*European Telecommunications Standards Institute*, Instituto Europeo de Normas de Telecomunicaciones), y el nuevo estándar HomeRF para el hogar, también pretenden acercarnos a un mundo sin cables y en algunos casos, son capaces de operar en conjunto y sin interferirse entre sí.

Las WLANs son un sistema de comunicación que transmite y recibe datos utilizando ondas electromagnéticas (aunque también es posible con luz infrarroja), en lugar del par trenzado, coaxial o fibra óptica utilizados en las LAN convencionales, Ahora bien, ello también obliga al desarrollo de un marco regulatorio adecuado que permita un uso eficiente y compartido del espectro radioeléctrico de dominio público disponible.

La productividad ya no se limita a un lugar de trabajo fijo, ahora se puede estar conectado en cualquier momento y lugar ya que originalmente las redes WLAN fueron diseñadas para el ámbito empresarial. Sin embargo, en la actualidad han

encontrado una gran variedad de escenarios de aplicación, tanto públicos como privados: entorno residencial y del hogar, grandes redes corporativas, PYMES (Pequeñas y Medianas Empresas), zonas industriales, campus universitarios, entornos hospitalarios, hoteles, aeropuertos, medios públicos de transporte, entornos rurales, etc. Incluso son ya varias las ciudades en donde se han instalado redes inalámbricas libres para acceso a Internet. Básicamente, una red WLAN permite a los usuarios movilidad en las zonas de cobertura alrededor de cada uno de los puntos de acceso, los cuales se encuentran interconectados entre sí y con otros dispositivos o servidores de la red cableada. Entre los componentes que permiten configurar una WLAN se pueden mencionar los siguientes: terminales de usuario o clientes (dotados de una tarjeta interfaz de red que integra un transceptor de radiofrecuencia y una antena), puntos de acceso y controladores de puntos de acceso, que incorporan funciones de seguridad, como autorización y autenticación de usuarios, *firewall*, etc.

La seguridad e interoperabilidad son determinantes para el futuro de la tecnología WLAN, es donde se centran actualmente la mayor parte de los esfuerzos. Sin embargo, desde el punto de vista de los usuarios, también es importante reducir la actual confusión motivada por la gran variedad de estándares existentes.

3.2. Ventajas de WLANs sobre las Redes Alámbricas

Muchos de los fabricantes de computadoras y equipos de comunicaciones como PDAs (*Personal Digital Assistants*, Asistente Digital Personal), módems, microprocesadores inalámbricos, lectores de punto de venta y otros dispositivos están introduciendo aplicaciones en soporte a las comunicaciones inalámbricas. Las nuevas posibilidades que ofrecen las WLANs son permitir una fácil incorporación de nuevos usuarios a la red, ofrecen una alternativa de bajo costo a los sistemas cableados, además de la posibilidad universal para acceder a cualquier base de datos o cualquier aplicación localizada dentro de la red. A continuación se resumen

algunas de estas ventajas de las WLANs, concernientes a productividad, conveniencia y costo, en comparación con las redes alámbricas.

- **Movilidad:** Los usuarios de redes inalámbricas tienen acceso a la información en tiempo real en cualquier lugar dentro de la organización. Esta movilidad incluye oportunidades de productividad y servicio que no es posible con una red alámbrica. (Villacrés Ortiz, 2006)
- **Simplicidad y rapidez en la instalación:** La instalación de una red inalámbrica puede ser rápida y fácil, además que se evitan obras para instalar cables por muros y techos, ya que no los necesita, mejorando así el aspecto de los lugares donde se lo implemente, y reduciendo el tiempo de instalación. También permite el acceso instantáneo a usuarios temporales de la red. (Villacrés Ortiz, 2006)
- **Flexibilidad en la instalación:** La tecnología inalámbrica permite llegar a lugares donde el cable no puede, superando mayor número de obstáculos, llegando a atravesar paredes. Así, es útil en zonas donde el cableado no es posible o es muy costoso: parques naturales, reservas o zonas escarpadas. (Villacrés Ortiz, 2006)
- **Costo de propiedad reducido:** Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una LAN alámbrica, la inversión de toda la instalación y el costo del ciclo de vida puede ser significativamente inferior. Los beneficios y costos a largo plazo son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes. (Villacrés Ortiz, 2006)
- **Escalabilidad:** Los sistemas de WLANs pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además es muy fácil la incorporación de nuevos usuarios a la red. (Villacrés Ortiz, 2006)

Otra atracción importante de los productos WLAN es la interoperatibilidad. Gracias al desarrollo de estándares, pueden mezclarse dispositivos inalámbricos de diversos fabricantes haciendo un acceso más directo y transparente con la tecnología.

3.3. Desventajas de las Redes Inalámbricas

La principal desventaja es la pérdida de velocidad de transmisión en comparación con los cables y las posibles interferencias. Otra desventaja es que al ser una red abierta puede ocasionar problemas de seguridad, aunque actualmente existen mecanismos de protección como es la contraseña.

3.4. Las organizaciones que definen las redes WLAN

Varias organizaciones han dado un paso adelante para establecer redes LAN inalámbricas (WLAN), las normas y certificaciones.

Las organizaciones que definen estándares WLAN:

ITU-R:

- International Telecommunicacion Union- Radiocommunication Sector, Unión internacional de Telecomunicaciones -Sector Radiocomunicaciones
- Regulaciones de RF usados en Wireless

IEEE:

- *Institute of Electrical and Electronic Engineers*, Instituto de Ingenieros Eléctricos y

Electrónicos

- 802.11 documentos wireless

de estándares técnicos

ETSI:

- *European Telecommunications Standards Institute*, Instituto Europeo de Normas de Telecomunicaciones

Wi-Fi Alliance:

- Asociación internacional sin fin

De lucro que prueba y certifica que los Equipos cumplan con los estándares Wi-Fi

La UIT Sector de Radiocomunicaciones (UIT-R) desempeña un papel fundamental en la gestión global del espectro de frecuencias radioeléctricas y de las órbitas de satélite para servicios como telefonía fija y móvil, radiodifusión, de aficionados, la investigación espacial, las telecomunicaciones de emergencia, la meteorología, los sistemas de posicionamiento global, la vigilancia del medio ambiente y servicios de comunicación, etc.

Tiene como misión velar por la utilización racional, equitativa, eficaz y económica del espectro de frecuencias radioeléctricas por todos los servicios de radiocomunicaciones, incluidos los que utilizan los satélites, y llevar a cabo estudios y aprobar recomendaciones sobre radiocomunicaciones.

En cumplimiento de esta misión, el UIT-R tiene como objetivo crear las condiciones para el desarrollo armónico y el funcionamiento eficiente de los sistemas de radiocomunicaciones existentes y nuevas, teniendo debidamente en cuenta todas las partes interesadas.

UIT-R gestiona la coordinación detallada y los procedimientos de registro de los sistemas espaciales y estaciones terrenas. Su función principal es procesar y publicar datos y llevar a cabo el examen de las notificaciones de asignación de frecuencias presentadas por las administraciones para su inclusión en los procedimientos de coordinación formales o registros en el Registro Internacional de Frecuencias.

El Instituto de Ingenieros Eléctricos y Electrónicos define los estándares. IEEE es la asociación más grande del mundo profesional dedicada al avance de la innovación tecnológica y excelencia en beneficio de la humanidad. IEEE y sus miembros tienen como misión inspirar a la comunidad global a través de publicaciones muy citadas, conferencias, estándares de tecnología y las actividades profesionales y educativas. IEEE 802.11 es parte del proceso de creación de redes de normalización 802.

ETSI produce normas de aplicación mundial para las tecnologías de la información y la comunicación (TIC), incluyendo telefonía fija, móvil, radio, convergente, de difusión y las tecnologías de internet. Oficialmente reconocida por la Unión Europea como un organismo europeo de normalización. ETSI es una organización sin fines de lucro con más de 700 organizaciones miembros procedentes de 62 países de todo el mundo.

Wi-Fi Alliance anteriormente WECA es una organización internacional, sin ánimo de lucro, formada en 1999 para certificar la interoperabilidad de productos inalámbricos de redes de área local basados en la especificación del IEEE 802.11. Actualmente la Wi-Fi Alliance tiene más de 200 miembros alrededor del mundo, que representan a un nutrido grupo de relevantes empresas y más de 1.000 productos han recibido la certificación Wi-Fi® desde que este proceso empezase en Marzo de 2000. El objetivo de los miembros de la Wi-Fi Alliance es enriquecer la experiencia de los usuarios a través de la interoperabilidad de sus productos.

Organizaciones de este tipo son totalmente imprescindibles para promover una determinada tecnología y lograr que los productos tengan la calidad requerida y la interoperabilidad necesaria (Wi-Fi Alliance)

3.5. Bandas de frecuencia

Las WLANs se manejan principalmente en las bandas: 900 MHz, 2,4 GHz y 5,7 GHz. Las bandas 900-MHz y 2,4 GHz se conocen como ISM (*Industrial Scientific and Medical*, Industrial Científica y Médica), y la 5-GHz banda que comúnmente se conoce como UNII (*Unlicensed National Information Infrastructure*, Infraestructura de Información Nacional Sin Licencia).

Las frecuencias de estas bandas son las siguientes:

- 900-MHz banda: 902 MHz a 928 MHz.
- 2,4 GHz banda: 2,400 MHz a 2,483 GHz (en Japón, esta banda se extiende a 2,495 GHz).
- 5-GHz banda: 5,150 MHz a 5,350 MHz, 5.725 MHz a 5.825 MHz.

Este tipo de bandas son de uso común y no requieren de licencia para utilizarlas. Esto quiere decir que no están protegidas frente a interferencias y que no es posible obstaculizar en aplicaciones con licencia.

3.6. Aplicaciones de la tecnología WIFI

En la actualidad, las redes WLAN han encontrado una gran variedad de nuevos escenarios de aplicación, tanto en el ámbito residencial como en entornos públicos.

Escenario Residencial: Una línea telefónica terminada en un *router* ADSL (*Asymmetric Digital Subscriber Line*, Línea de Abonado Digital Asimétrica) al cual

se conecta un AP para formar una red WLAN que ofrece cobertura a varios ordenadores en el hogar. (COIT, 2008)

Redes Corporativas: Una serie de puntos de acceso distribuidos en varias áreas de la empresa conforman una red WLAN autónoma o complementan a una LAN cableada. Son aplicaciones de alta densidad de tráfico con altas exigencias de seguridad. (COIT, 2008)

Usos industriales: Dentro del uso corporativo, existen diversas aplicaciones especialmente potenciadas por los sistemas Wi-Fi, utilizados en régimen de autoprestación: gestión de almacenes, telecontrol y seguimiento, comunicaciones vocales internas, aplicaciones de video. (COIT, 2008)

Acceso público a Internet desde cafeterías, bares, etc. En estos establecimientos se ofrece a los clientes acceso a Internet desde sus propios portátiles o dispositivos. Es un escenario de acceso, involucrando un bajo número de puntos de acceso, parecido al residencial, pero que necesita mayores funcionalidades en el núcleo de red. (COIT, 2008)

Acceso público de banda ancha en pequeños pueblos, hoteles, campus universitarios, En general, este escenario necesita múltiples puntos de acceso para garantizar la cobertura del área considerada. El acceso se construye, mayoritariamente, a través de nodos 802.11b/g estructurados jerárquicamente y mediante una cuidadosa planificación de frecuencias de forma que exista el menor solapamiento entre ellas y, por tanto, la menor pérdida de ancho de banda. En el caso de grandes coberturas y/o altas densidades de usuarios, sería preciso establecer redes de distribución, bien mediante conexión de las propias celdas, bien mediante enlaces dedicados 802.11 a/b/g. (COIT, 2008)

WLAN para cobertura de "*Hot-spots*" (escenario público). Estas redes cubren áreas donde se concentra un gran número de usuarios de alto tráfico como son

aeropuertos, estaciones, centros de congresos, etc. La red a instalar requiere un elevado número de puntos de acceso, así como importantes exigencias de seguridad, gestión de red y facilidades de facturación. Representan el mayor número tanto por cantidad de puntos de acceso, como de usuarios como de volumen de negocio generado. (COIT, 2008)

3.7. Los Estándares de WLAN

El gran éxito de las WLANs es que utilizan frecuencias de uso libre, es decir no es necesario pedir autorización o algún permiso para utilizarlas. Aunque hay que tener en mente, que la normatividad acerca de la administración del espectro varía de país a país.

Los estándares son desarrollados por organismos reconocidos internacionalmente, tal es el caso de la IEEE y la ETSI. Una vez desarrollados se convierten en la base de los fabricantes para desarrollar sus productos.

3.7.1. Estándares de las redes inalámbricas (IEEE 802.11)

El estándar IEEE 802.11 **s**e publicó en 1997, fue el primero de los estándares definidos por la IEEE para aplicaciones WLAN, y especifica dos velocidades de transmisión teóricas de 1 y 2 Mbps. Funciona sobre la banda ISM de 2.4 GHz (de 2.400 MHz a 2.483,5 MHz), usando tres tecnologías diferentes:

- FHSS (*Frequency Hopping Spread Spectrum,* Salto de Frecuencia de Espectro Ensanchado)
- DSSS (*Direct Sequence Spread Spectrum,* Espectro Ensanchado por Secuencia Directa)
- IR (*Infrared,* Infrarrojas).

El estándar original aseguraba la interoperabilidad entre equipos de comunicación dentro de cada una de estas tecnologías inalámbricas, pero no entre las tres tecnologías. El estándar original también define el protocolo CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance,* Múltiple Acceso por Detección de Portadora Evitando Colisiones) como método de acceso. 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. Debido a la aparición de una serie de variantes que mejoran no sólo la velocidad de transferencia, sino que además dan cobertura a funciones especiales de seguridad este estándar está prácticamente en desuso. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores. (IEEE, 2012)

IEEE 802.11a

Estándar de conexión inalámbrica que tiene una velocidad de transmisión de 54 Mbps con velocidades reales de aproximadamente 20 Mbps, en una banda de 5 GHz.

El estándar usa el método OFDM (*Orthogonal Frequency Division Multiplexing,* Multiplexación por División de Frecuencias Ortogonales) para la transmisión de datos, su mayor inconveniente es que no es compatible con el estándar 802.11b. (IEEE, 2012)

La revisión 802.11a al estándar original fue ratificada en 1999, es también conocido como “Wi- Fi5”. Las desventajas de la utilización de esta banda es que dado que sus ondas son más fácilmente absorbidas, los equipos 802.11a deben quedar en línea de vista y es necesario un mayor número de AP. Sus características se detallan en la Tabla 3.1. (IEEE, 2012)

Tabla 3.1 Resumen del estándar 802.11a

Fuente: Autores

802.11a	
Rango de frecuencias	De 5,15 a 5,25 GHz (50mW) De 5,25 a 5,35 GHz (250mW) De 5,725 a 5,825 GHz (1W)
Acceso	OFDM
Velocidad	Hasta 54 Mbps
Compatibilidad	No compatible con los sistemas 802.11b, 802.11, HiperLAN2, Infrarrojos (IR) ni con HomeRF.
Distancia	Depende de la instalación y de los obstáculos.
Aplicación	Todo tipo de red de dato Ethernet.

IEEE 802.11b

Estándar de conexión inalámbrica que tiene una velocidad de transmisión entre 5.5 y 11 Mbps, dependiendo de diferentes factores, en una banda de 2.4 GHz. Es la evolución natural del IEEE 802.11 y fue ratificada en 1999. No es compatible con el 802.11a pero es totalmente compatible con el estándar original de 1 y 2 Mbps (sólo con los sistemas DSSS, no con los FHSS o sistemas infrarrojos), incluye una nueva técnica de modulación CCK (*Complementary Code Keying*) que permite el incremento de velocidad. (IEEE, 2012)

En cuanto a las distancias a cubrir, dependerá de las velocidades aplicadas, del número de usuarios conectados y del tipo de antenas y amplificadores que se puedan utilizar. Aún así, se podrían dar unas cifras de alrededor de entre 120m (a 11 Mbps) y 460m (a 1 Mbps) en espacios abiertos, y entre 30m (a 11 Mbps) y 90m (a 1 Mbps) en interiores, dependiendo lógicamente del tipo de materiales que sea necesario atravesar. La tabla 3.2 muestra las características de este estándar. (IEEE, 2012)

Tabla 3.2 Resumen del estándar 802.11b

Fuente: Autores

802.11b	
Rango de frecuencias	De 2.4 a 2.4835 GHz
Acceso	DSSS usando CCK
Velocidad	Hasta 11Mbps
Compatibilidad	Compatible con sistemas 802.11 DSSS de 1 y 2 Mbps. No compatibles con los sistemas 802.11 FHSS, infrarrojos ni con *HomerRF*.
Distancia	Dependiendo de la instalación y los obstáculos en zona abierta un máximo de 460m y en interior un máximo de 90m.
Aplicación	Todo tipo de red de dato Ethernet.

IEEE 802.11e

Estándar en elaboración desde Junio de 2003 y publicado en el 2005, el objetivo del nuevo estándar IEEE 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de calidad de servicio. Para cumplir con su objetivo introduce un nuevo elemento llamado HCF (*Hybrid Coordination Function*, Función de Coordinación Híbrida) con dos tipos de acceso: (EDCA, *Enhanced Distributed Channel Access*, Función Mejorada de Distribución de Acceso al Canal) y HCCA (HCF *Controlled Channel Access*, Función HCF de Control de Acceso al Canal). (IEEE, 2012)

IEEE 802.11g

El estándar IEEE 802.11g ofrece 54Mbps en la banda de 2,4GHz. Dicho con otras palabras, asegura la compatibilidad con los equipos Wi-Fi preexistentes. Para aquellas personas que dispongan de dispositivos inalámbricos de tipo Wi-Fi, 802.11g

proporciona una forma sencilla de migración a alta velocidad. Una de sus ventajas es la compatibilidad con el estándar 802.11b. Cubre de 50 a 100m de distancia en interiores pero permite hacer comunicaciones de hasta 50Km con antenas parabólicas apropiadas. El estándar fue aprobado en Junio de 2003 pero se publicó como borrador en Noviembre de 2001 con los siguientes elementos obligatorios y opcionales: (IEEE, 2012)

- El método OFDM es obligatorio y es lo que permite velocidades superiores en la banda de los 2,4GHz. (IEEE, 2012)
- Los sistemas deben ser totalmente compatibles con las tecnologías anteriores de 2,4GHz Wi-Fi (802.11b). Por lo que el uso del método CCK también será obligatorio para asegurar dicha compatibilidad. (IEEE, 2012)

Un resumen de las características de este estándar se presenta en la tabla 3.3.

Tabla 3.3 Resumen del estándar 802.11g

Fuente: Autores

802.11g	
Rango de frecuencias	De 2.4 a 2.4835 GHz
Acceso	Obligatoriamente CCK y OFDM
Velocidad	Hasta 54 Mbps
Compatibilidad	Compatible con sistemas 802.11b de 11 y 5.5 también con los sistemas 802.11 DSSS de 1 y 2 Mbps Mbps. No compatibles con los sistemas 802.11 FHSS, infrarrojos ni con HomerRF
Distancia	Dependiendo de la instalación y los obstáculos en interior entre 50 a 100m
Aplicación	Todo tipo de red de dato Ethernet

Como estándares adicionales dentro del grupo 802.11, dignos de mención por su importancia en la mejora y evolución de las normas básicas o por cubrir aspectos no contemplados en esas normas se destacan los siguientes:

IEEE 802.11e

Se podría definir como la implementación de características de QoS (*Quality of Service*, Calidad de Servicio) y multimedia para las redes 802.11b. Esta especificación, que está haciendo el IEEE será aplicable tanto a 802.11b como a 802.11a. (IEEE, 2012)

IEEE 802.11f

Básicamente, es una especificación que funciona bajo el estándar 802.11g y que se aplica a la intercomunicación entre puntos de acceso de distintos fabricantes, permitiendo el *roaming* o itinerancia de clientes. (IEEE, 2012)

IEEE 802.11h

Una evolución del IEEE 802.11a que permite asignación dinámica de canales y control automático de potencia para minimizar los efectos de posibles interferencias. (IEEE, 2012)

IEEE 802.11i

Este estándar permite incorporar mecanismos de seguridad para redes inalámbricas, ofrece una solución interoperable y un patrón robusto para asegurar datos. (IEEE, 2012)

IEEE 802.11n

El borrador fue desarrollado en el 2007 y aprobado en 2009. La velocidad real estimada es de 600 Mbps (la velocidad teórica de transmisión es aún mayor), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. Mejor rendimiento en 5GHz, se puede usar en 2.4 GHz si las frecuencias están libres. (IEEE, 2012)

3.7.2. El Estándar HiperLAN2

Por otro lado el foro global HiperLAN2 definió una especificación que opera en la banda de 5 GHz y que permite la transferencia de datos de hasta 54 Mbps que utiliza la técnica de modulación OFDM para transmitir señales analógicas. OFDM es muy eficiente en ambientes dispersos en el tiempo, como oficinas, donde las señales de radio son reflejadas desde muchos puntos, donde la señal llega a diferentes tiempos de propagación antes de que llegue al receptor. Debido a que HiperLAN es orientado a conexión, posee características de Calidad de Servicio (QoS). El soporte de QoS en combinación con las altas velocidades de HiperLAN facilita la transmisión de diferentes tipos de ráfagas de datos como vídeo, voz y datos.

Ambas especificaciones, la 802.11a (IEEE) y la HiperLAN2 (ETSI) son para WLANs de alta velocidad que operan en el intervalo de frecuencias de 5.15 a 5.35 GHz. El radioespectro asignado para el 802.11a y el HiperLAN2 es dividido en 8 segmentos o canales de 20 MHz cada uno. Cada canal soporta un cierto número de dispositivos; dispositivos individuales pueden transitar a través de segmentos de red como si fueran teléfonos móviles de una estación a otra. Este espectro de 20 MHz para un segmento de red soporta 54 Mbps de caudal eficaz compartido entre los dispositivos en el segmento en un tiempo dado. Un resumen de este estándar se presenta en la tabla 3.4

Tabla 3.4 Resumen del estándar HiperLAN2

Fuente: Autores

HiperLAN2	
Rango de frecuencias	De 5,15 a 5,25 GHz (50mW) De 5,25 a 5,35 GHz (250mW) De 5,725 a 5,825 GHz (1W)
Acceso	OFDM
Velocidad	Hasta 54 Mbps
Compatibilidad	No compatible con los sistemas 802.11g, 802.11b, 802.11 ni con HomeRF
Distancia	Depende de la instalación y de los obstáculos máximo 150m
Aplicación	WAN/LAN, voz encapsulada, vídeo, datos

3.7.3. El Estándar HomeRF.

HomeRF es otra organización que ha desarrollado sus propios estándares para entrar de lleno al mundo de las redes inalámbricas. Ha sido desarrollada por el grupo de trabajo *Home Radio Frequency*, el cual está conformado por más de 50 compañías líderes en el ámbito mundial en las áreas de redes, periféricos, comunicaciones, software, semiconductores, etc. Este grupo fue fundado en marzo de 1988 para promover de manera masiva dispositivos de voz, datos y vídeo alrededor de los hogares de manera inalámbrica. Al inicio del 2001, se anunció la formación un grupo de trabajo europeo de HomeRF enfocado hacia el mercado europeo. HomeRF es la tecnología que compite directamente con los productos de la IEEE 802.11b y Bluetooth en la banda de 2.4 GHz. La velocidad máxima de HomeRF es 10 Mbps, ideal para las aplicaciones caseras, aunque se manejan otras velocidades de 5, 1.6 y 0.8 Mbps Según el grupo de trabajo, HomeRF ofrece más seguridad, los dispositivos consumen menos potencia que los productos de las tecnologías contrincantes, además de permitir aplicaciones para telefonía y vídeo. Sus principales características se muestran en la Tabla 3.5

Tabla 3.5 Resumen del estándar HomeRF

Fuente: Autores

HomeRF	
Rango de frecuencias	De a 2.4 a 2.4835 GHz.
Acceso	OFDM
Velocidad	10 Mbps
Compatibilidad	No compatible con ningún otro estándar inalámbrico
Aplicación	Se diseño para uso de los hogares

3.7.4. Bluetooth

Bluetooth es un enlace radio de corto alcance que aparece asociado a las WPAN (*Wireless Personal Area Network*, Red Inalámbrica de Área Personal). Este concepto hace referencia a una red sin cables que se extiende a un espacio de funcionamiento personal o POS (*Personal Operating Space*, Espacio de Trabajo Personal) con un radio de hasta 10 metros.

Las WPAN constituyen un esquema de red de bajo costo que permite conectar entre sí equipos informáticos y de comunicación portátil y móvil, como ordenadores, PDAs, impresoras, ratones, micrófonos, auriculares, lectores de código de barras, sensores, *displays*, localizadores, teléfonos móviles y otros dispositivos de electrónica de consumo. El objetivo es que todos estos equipos se puedan comunicar e interoperar entre sí sin interferencias.

Bluetooth trabaja en el rango de frecuencias de 2,402 GHz a 2,48 GHz. Se trata de una banda de uso común que se puede usar para aplicaciones ICM y que no necesita licencia. La primera versión de Bluetooth, la que implementan los circuitos disponibles actualmente, puede transferir datos de forma asimétrica a 721 Kbps y simétricamente a 432 Kbps. Se puede transmitir voz, datos e incluso vídeo. Para

transmitir voz son necesarios tres canales de 64 Kbps. Para transmitir vídeo es necesario comprimirlo en formato MPEG-4 y usar 340 Kbp. Están previstas dos potencias de emisión en función de la distancia que se desea cubrir, 10 metros con 1 miliwatio y 100 metros con 100 miliwatios. La tabla 3.6 presenta un resumen del estándar. (Bluetooth Technology , 2008)

Tabla 3.6 Resumen del estándar Bluetooth

Fuente: Autores

Bluetooth	
Rango de frecuencias	De a 2.4 a 2.4835 Ghz.
Acceso	FHSS
Velocidad	Versión 1.1 – 721Kbps Versión 1.2 – 10Mbps
Compatibilidad	No compatible con ningún otro estándar inalámbrico.
Distancia	10 metro máximo.
Aplicación	La aplicación más conocida es teléfonos móviles.

La tabla 3.7 permite comparar las características de los diferentes estándares.

Tabla 3.7 Resumen de los estándares de redes inalámbricas más comunes

Fuente: Autores

Estándar	**Origen**	**Velocidad máxima**	**Modulación**	**frecuencia**	**Ancho de banda**
802.11	IEEE	2 Mbps	FHSS/DSSS	2.4 GHz	25 MHz
802.11b	IEEE	11 Mbps	DSSS/CCK	2.4 GHZ	25 MHz
802.11a	IEEE	54 Mbps	OFDM	5.0 GHz	25 MHz
802.11g	IEEE	54 Mbps	OFDM/CCK	2.4 GHZ	25 MHz
HiperLAN2	ETSI	54 Mbps	OFDM	5.0 GHz	25 MHz

Bluetooth	Bluetooth	10 Mbps	DSSS/FHSS	2.4 GHZ	5 MHz
HomeRF	HomeRF	0.721/10 Mbps	OFDM	2.4 GHz	5 MHZ

3.8. Componentes de una WLAN

Entre los componentes que permiten configurar una WLAN se puede mencionar los siguientes:

- Terminales de Usuario o Clientes, dotados de una NIC, (*Network Interface Card*, Tarjeta de Interface de Red) que incluye un transceptor de radio y la antena.
- Puntos de Acceso o APs, que permiten enviar la información de la red cableada, por ejemplo Ethernet, hacia los Clientes.
- Controlador de puntos de acceso necesario para despliegues que requieren varios APs por razones de cobertura y/o tráfico. Este último suele incorporar funcionalidad de AP, de cliente VPN (*Virtual Private Networks*, Red Privada Virtual), de cliente RADIUS (*Remote Authentication Dial In User Service*) para labores de autentificar y autorizar con un servidor AAA apropiado de routing y de firewall.

La existencia en el mercado de dichos dispositivos capaces de interconectarse de forma barata y sencilla ha dado origen a una gran variedad de aplicaciones que sobrepasan ampliamente el ámbito de utilización en entornos empresariales para el que nacieron las WLAN.

3.9. Arquitectura interna de las redes Wi-Fi

El elemento fundamental de la arquitectura de las redes 802.11 es la celda, la cual se puede definir como el área geográfica en que una serie de dispositivos se interconectan entre sí por un medio aéreo. En general, esta celda estará compuesta

por estaciones y un único punto de acceso. Las estaciones son adaptadores que permiten la conversión de información, generalmente encapsulada bajo el protocolo Ethernet, existente en terminales o equipos clientes, y su envío y recepción dentro de la celda. El punto de acceso es el elemento que tiene la capacidad de gestionar todo el tráfico de las estaciones y que puede comunicarse con otras celdas o redes. Es a todos los efectos un puente que comunica a nivel 2 (enlace) los equipos, tanto de su celda de cobertura, como a otras redes a las cuales estuviese conectado. A esta configuración se le denomina BSS (*Basic Service Set*, Grupo de Servicio Básico). (COIT, 2008)

El BSS es, por tanto, una entidad independiente que puede tener su vinculación con otros BSS a través del punto de acceso mediante un DS (*Distribution System*, Sistema de Distribución). El DS puede ser interrogado (comunica el BSS con una red externa), cableado (con otros BSS a través de cable como por ejemplo una red Ethernet fija convencional), o también inalámbrico, en cuyo caso se denomina Sistema de Distribución Inalámbrica. (COIT, 2008)

Sobre este concepto básico surgen una serie de alternativas:

- **IBSS** (*Independent Basic Service Set*, Grupo de Servicio Básico Independiente). Es una celda inalámbrica en la cual no hay sistema de distribución y, por tanto, no tiene conexión con otras redes, como se observa en la figura 3.1. (COIT, 2008)

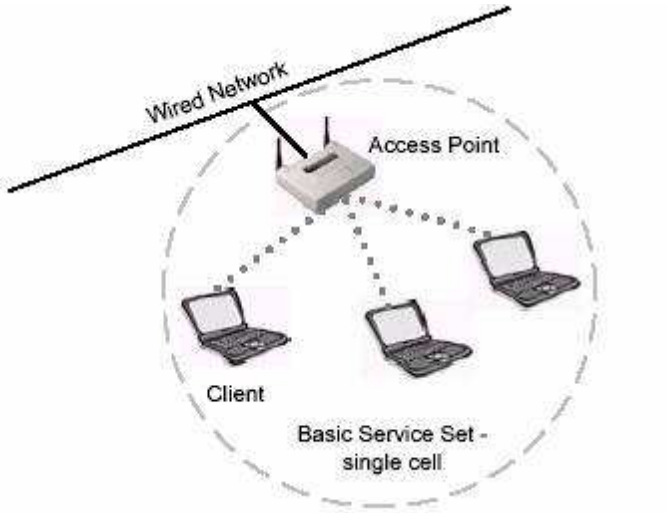


Figura 3.1 Basic Service Set

Fuente: http://www.netsite.gigfa.com/index.php/wireless/139-wireless.html

- **Modo Ad-hoc**. Es una variante del IBSS en el cual no hay punto de acceso. Las funciones de coordinación son asumidas de forma aleatoria por una de las estaciones presentes. El tráfico de información se lleva a cabo directamente entre los dos equipos implicados, sin tener que recurrir a una jerarquía superior centralizadora, obteniéndose un aprovechamiento máximo del canal de comunicaciones. La cobertura se determina por la distancia máxima entre dos equipos, la cual suele ser apreciablemente inferior a los modos en que hay un punto de acceso. Es un modo de empleo infrecuente por las connotaciones de aislamiento que conlleva aunque puede ser muy útil cuando el tráfico existente se reparte entre todos los equipos presentes (Figura 3.2). (COIT, 2008)

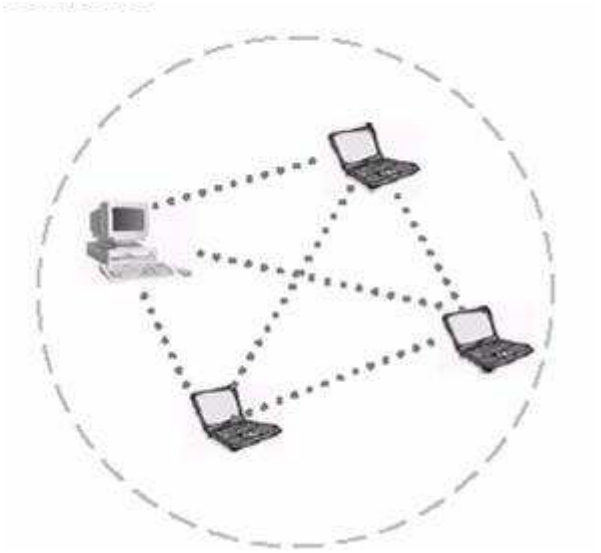


Figura 3.2 Modo Ad-hoc

Fuente: http://www.netsite.gigfa.com/index.php/wireless/139-wireless.html

- **Modo infraestructura.** El punto de acceso realiza las funciones de coordinación. Todo el tráfico tiene que atravesarlo, por lo que hay una clara pérdida de eficiencia cuando dos estaciones dentro de un mismo BSS desean comunicarse entre sí (los paquetes de información son enviados una vez al punto de acceso y otra vez al destino). Es una arquitectura apropiada cuando la mayor parte del tráfico se origina o finaliza en las redes exteriores a las cuales está conectado el punto de acceso. La cobertura alcanza una distancia cercana al doble de la distancia máxima entre el punto de acceso y estación. Es el modo que se emplea habitualmente para conectar una red inalámbrica con redes de acceso a Internet (ADSL, RDSI –Red Digital de Servicio Integrados-, etc.) y redes locales de empresas. (COIT, 2008)
- **BSS extendido** Es un caso específico del modo infraestructura, representado por un conjunto de BSS asociados mediante un sistema de distribución. Esto permite una serie de prestaciones avanzadas opcionales como el *roaming* entre celdas. Su aplicación se muestra en la figura 3.3. (COIT, 2008)

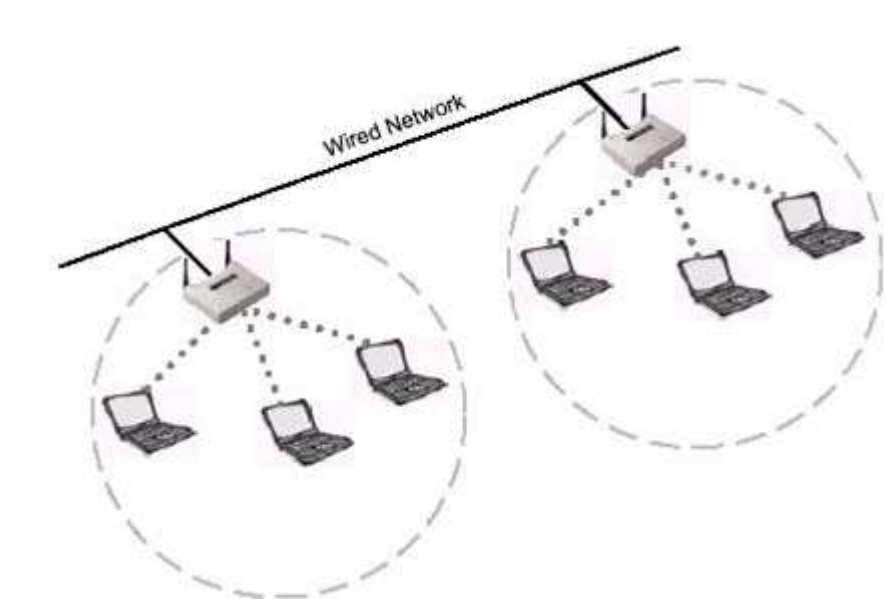


Figura 3.3 Extended Service Set

Fuente: http://www.netsite.gigfa.com/index.php/wireless/139-wireless.html

3.10. Seguridades de WLANs

Una de las debilidades normalmente atribuidas a las tecnologías inalámbricas, y más en concreto a la tecnología Wi-Fi, es la falta de seguridad.

No se refiere tanto a la seguridad física sino, a la seguridad de la información, su integridad y a la no accesibilidad a terceros.

- La seguridad es un requisito esencial para la aceptación de las WLAN por los usuarios empresariales o en aplicaciones públicas.
- La posible carencia de medidas de seguridad adecuadas puede ocasionar que un "*hacker*" se introduzca en la red, acceda a la información o la manipule a su antojo. No obstante, existen herramientas, funciones y protocolos de seguridad que ofrecen protección adecuada para redes WLAN.
- Las redes WLAN no deben ser más vulnerables que las redes de cable.
- El nivel de seguridad será dependiente del tipo y funcionalidad de la red.

- Mayor nivel de seguridad exige más costo y más capacidad de proceso.

Actualmente existen vías efectivas para garantizar una transmisión segura de los datos y, a pesar de que ninguna medida de seguridad es infalible, la clave está en que las empresas pueden aplicar ahora múltiples niveles de seguridad inalámbrica según sus necesidades.

3.10.1. Las soluciones

A continuación se presentan algunas soluciones para la seguridad de estos sistemas:

SSID (Service Set Identifier,* Identificador de conjunto de servicios*)

Como uno de los primeros niveles de seguridad que se pueden definir en una red inalámbrica se puede citar al SSID (*Service Set Identifier*, Identificador del Servicio).

Es un código que está incluido en todos los paquetes de una red inalámbrica y consiste en un máximo de 32 caracteres alfanuméricos. Sirve para identificarlos como parte de esa red y para determinar el área cubierta por uno o más APs. En un modo comúnmente usado, el AP periódicamente transmite su SSID. Una estación inalámbrica que desee asociarse con un AP puede escuchar estas transmisiones y puede escoger un AP al que desee asociarse basándose en su SSID. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID. (COIT, 2008)

Cuando se activa la WLAN en el *router*, se debe configurar parámetros y uno de ellos es el nombre de la red inalámbrica para que identifiquen los dispositivos. Las redes inalámbricas pueden verse desde el exterior, sólo buscando los SSID existentes en el aire, se puede conectar un ordenador con la propia red inalámbrica, o con otras redes vecinas cercanas a la red LAN. (COIT, 2008)

Para garantizar la no conexión de otros dispositivos externos en las redes inalámbricas, existe la autentificación y aceptación de dichos dispositivos a la red LAN y WLAN del *router*.

Si no se está bien autentificado, la red inalámbrica rechazará dicho dispositivo y no lo dejará entrar a la red. (COIT, 2008)

Filtrado de direcciones MAC: Subiendo un escalón en estos sistemas de protección, está la posibilidad de definir ACL (Access Control List, Listas de Control de Acceso) en los puntos de acceso.

Cada uno de estos puntos puede contar con una relación de las direcciones MAC de cada uno de los clientes que se quiere que se conecten a la red inalámbrica. Cada adaptador cuenta con una dirección que la identifica de forma inequívoca, y si el punto de acceso no la tiene identificada, simplemente no recibirá contestación por su parte. (COIT, 2008)

Hay que tener en cuenta que éste no es el método más seguro para proteger la entrada a la red inalámbrica. Para empezar habrá que actualizar esta ACL cada vez que se identifique un nuevo adaptador inalámbrico, eliminando aquellos que se quieren dejar de utilizar. (COIT, 2008)

Sistemas de cifrado y autenticación: Aparte de observar una serie de medidas para controlar el acceso a la red, poco a poco se han ido desarrollando una serie de tecnologías que permitirán hacer a la WLAN tan segura como una LAN cableada. (COIT, 2008).

WEP *(Wired Equivalent Privacy,* Privacidad Equivalente a Cableado): El cifrado de la información es una de las técnicas más utilizadas, y para ello ya se lleva un tiempo empleando sistemas como WEP. Se puede definir este sistema como la generación de una clave que se comparte entre el cliente y el punto de acceso, y que permite o deniega la comunicación entre ambos dispositivos. WEP utiliza un sistema con una clave de 64 ó 128 bits, que pueden ser hexadecimales o ASCII, mediante la que se autentifica el acceso y se encripta la información que se transmite entre ambos dispositivos. (COIT, 2008)

Aunque en teoría este sistema debería ser suficiente, lo cierto es que existen métodos para averiguar esta clave utilizando determinadas herramientas software, además del problema que se deriva de utilizar una misma clave para todos los usuarios. (COIT, 2008)

DSL *(Dynamic Security Link,* Enlace de Seguridad Dinámico): La gestión de estas claves puede convertirse en un auténtico problema en empresas con un gran número de usuarios. Para evitar esto, existen herramientas como la que 3Com incluye en sus puntos de acceso, que soporta un mecanismo adicional de autentificación a través de la asignación dinámica de claves. Este mecanismo denominado DSL, permite realizar una gestión automática y dinámica de las claves a través del propio punto de acceso. Al contrario que el sistema WEP, estándar en el que se utiliza una misma clave para todos lo usuarios y cuya modificación debe hacerse de forma manual, DSL se basa en proteger la red inalámbrica de posibles intrusiones externas mediante la generación automática, al comienzo de cada sesión, de una única clave cifrada de 128 bits para cada usuario de la red. (COIT, 2008)

Además de esto, DSL también proporciona autentificación de usuario, obligándolo a introducir el correspondiente nombre de usuario y contraseña para cada sesión que se abra. (COIT, 2008)

RADIUS: Cuando aumentan las necesidades en cuanto a niveles de seguridad y número de usuarios que es necesario administrar, además de la encriptación, es necesario añadir por otro mecanismo de seguridad como es la autentificación. La autenticación es el proceso por el cual se controla el acceso de los usuarios a la red. Para este propósito, el IEEE creó el grupo 802.1x con objeto de obtener un estándar de autenticación para redes (cableadas o no). RADIUS es la infraestructura recomendada por la WiFi Alliance como sistema de gestión centralizada que da una solución de autenticación para entornos con un elevado número de usuarios. (COIT, 2008)

Teniendo en cuenta que este tipo de entornos utilizará normalmente estructuras mixtas (cable tradicional y WLAN), la utilización de este protocolo permitirá mejorar la capacidad de autentificación del usuario inalámbrico, proporcionando un nivel de seguridad superior, escalable y una gestión centralizada. (COIT, 2008)

A través de este sistema se podrá obtener un Certificado de Cliente Universal para permitir la autentificación mutua (autentificación del cliente al AP y del AP al cliente), gestión de clave protegida a través del soporte para RADIUS-EAP-TLS, así como la integración en entornos RADIUS existentes que soporten el protocolo MD-5 con sistemas de autenticación múltiples con protocolo EAP (*Extensible Authentication Protocol*, Protocolo de Autenticación Extensible). (COIT, 2008)

VPNs inalámbricas: Sin embargo, para conseguir que el nivel de confianza en las WLAN se equipare a las redes cableadas, algunos usuarios han optado por otra alternativa para reforzar la seguridad, implementando soluciones de seguridad de red convencionales adaptadas al entorno *wireless*. (COIT, 2008)

En este modelo, es donde entran en juego el establecimiento de túneles IPSec (*Internet Protocol Security*, Protocolo de Seguridad de Internet). Este mecanismo, que asegura el tráfico de datos por una VPN utiliza algoritmos para la encriptación de datos, otros algoritmos para la autentificación de paquetes y certificados digitales

para la validación de los usuarios. Debido a ello, se empieza a recomendar como solución idónea para responder a las necesidades actuales de seguridad en las redes inalámbricas, la combinación de la VPNs (IPSec) con el estándar 802.1x. (COIT, 2008)

WPA: Además, Wi-Fi Alliance ha anunciado la adopción de nuevas medidas de seguridad cuyo objeto es facilitar a los propietarios de redes inalámbricas un control mayor sobre quién accede a las mismas y mayor protección de las comunicaciones *wireless*. Actualmente WEP está siendo sustituido por un nuevo protocolo: WPA (WI -FI *Protected Access*). WPA mejora la forma de codificar los datos respecto a WEP, utilizando TKIP (*Temporal Key Integrity Protocol*, Protocolo de Integridad de Clave Temporal), al mismo tiempo que proporciona autenticación de usuarios mediante 802.1x y EAP. (COIT, 2008)

Wi-Fi *Protected Access* será compatible con las especificaciones de seguridad 802.11i que actualmente está desarrollando el IEEE. De hecho, WPA está formada por los componentes ya aprobados del estándar 802.11i. Dichas funciones pueden habilitarse en la mayoría de productos certificados Wi-Fi existentes con una sencilla actualización de software. (COIT, 2008)

El estándar 802.11i aún no se ha desarrollado completamente, aunque WPA irá asumiendo completamente dicho estándar conforme vaya cerrando especificaciones que supondrán incluso modificaciones de hardware. Wi-Fi Alliance ha certificado más de 175 productos con WPA desde septiembre de 2003. La organización ha empezado a requerir WPA para todos los productos certificados y ya no considera WEP como un mecanismo seguro. (COIT, 2008)

RSN (Robust Network Security, Red Segura Robusta)

RSN corresponde con la segunda parte (versión definitiva) del estándar 802.11i, de ahí que también sea conocido como WPA2. Este estándar añadirá a las redes inalámbricas seguridad más que suficiente y será totalmente compatible con WPA.

Como inconveniente, necesitará actualización de hardware tanto de puntos de acceso como de estaciones. (COIT, 2008)

DHCP (Dynamic Host Configuration Protocol, Protocolo de Configuración Dinámica de Servidor): Es un protocolo que facilita la administración de la red, ya que permite automatizar y gestionar de una manera centralizada la asignación de direcciones IP en una red de una organización o de un Proveedor de Servicios de Internet (ISP). Cuando se usan los Protocolos de Internet (TCP/IP), cada ordenador que puede conectarse necesita una dirección IP exclusiva.

Sin DHCP, la dirección IP debe ser configurada manualmente en cada ordenador, y si los estos cambian de sitio a otro lugar de la red, hay que introducir una nueva dirección IP.

DHCP usa el concepto de alquiler o préstamo de dirección IP, cuyo significado es que esta será válida para un ordenador durante un cierto período de tiempo. La duración del préstamo puede variar dependiendo de cuánto tiempo esté conectado a Internet el usuario de una ubicación determinada. Utilizando préstamos muy cortos, DHCP puede reconfigurar dinámicamente las redes en las cuales hay más ordenadores que direcciones IP.

Este es un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado posteriormente.

3.11. Asignación de direcciones IP

El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

- **Asignación manual o estática:** Asigna una dirección IP a una máquina determinada. Se suele utilizar cuando se quiere controlar la asignación de dirección IP a cada cliente y evitar que se conecten clientes no identificados.
- **Asignación automática:** Asigna una dirección IP de forma permanente a una máquina cliente la primera vez que hace la solicitud al servidor DHCP y hasta que el cliente la libera. Se suele utilizar cuando el número de clientes no varía demasiado.
- **Asignación dinámica**: El administrador de la red determina un rango de direcciones IP y cada computadora conectada a la red está configurada para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable, esto facilita la instalación de nuevas máquinas clientes a la red. Es el único método que permite la reutilización dinámica de las direcciones IP.

3.12. EVOLUCIÓN DE LAS TECNOLOGÍAS INALÁMBRICAS

Dentro de la consideración genérica de redes inalámbricas se puede encontrar distintas categorías en función del rango o alcance en que una tecnología presta un servicio:

- **PAN** (*Personal Area Network,* Redes de Area Personal): Redes para interconexión de dispositivos personales (PDA's, portátiles, etc.) a muy corto alcance (<10 metros), baja velocidad (<1 Mbps) y con necesidad de visión sin obstáculos. (COIT, 2008)
- **LAN** (*Local Area Network*): Redes para interconexión corporativa (oficinas, escuelas, etc.) con cobertura de entorno a 100 metros y velocidad entre 2 y 54 Mbps. (COIT, 2008)
- **MAN** (*Metropolitan Area Network,* Red de Area Metropolitana): Redes usadas típicamente para interconexión de distintas oficinas de una

misma empresa en el radio de una ciudad (aproximadamente 20 metros), cubriendo unas velocidades de hasta 150 Mbps. (COIT, 2008)

- **WAN**: Colección de redes conectadas a través de una subred con un área de cobertura que puede oscilar entre los 100 y los 1000 Kilómetros y unas velocidades entre 10 y 384 Kbps. (COIT, 2008)
- **MBWA** (*Mobile Broadband Wireless Access*, Banda Ancha Inalambrica): Redes inalámbricas para acceso de Banda Ancha. (COIT, 2008)

Esta clasificación, junto con la figura 3.4, ayudará a ver cuál es el posicionamiento y evolución de las tecnologías inalámbricas para los próximos años:

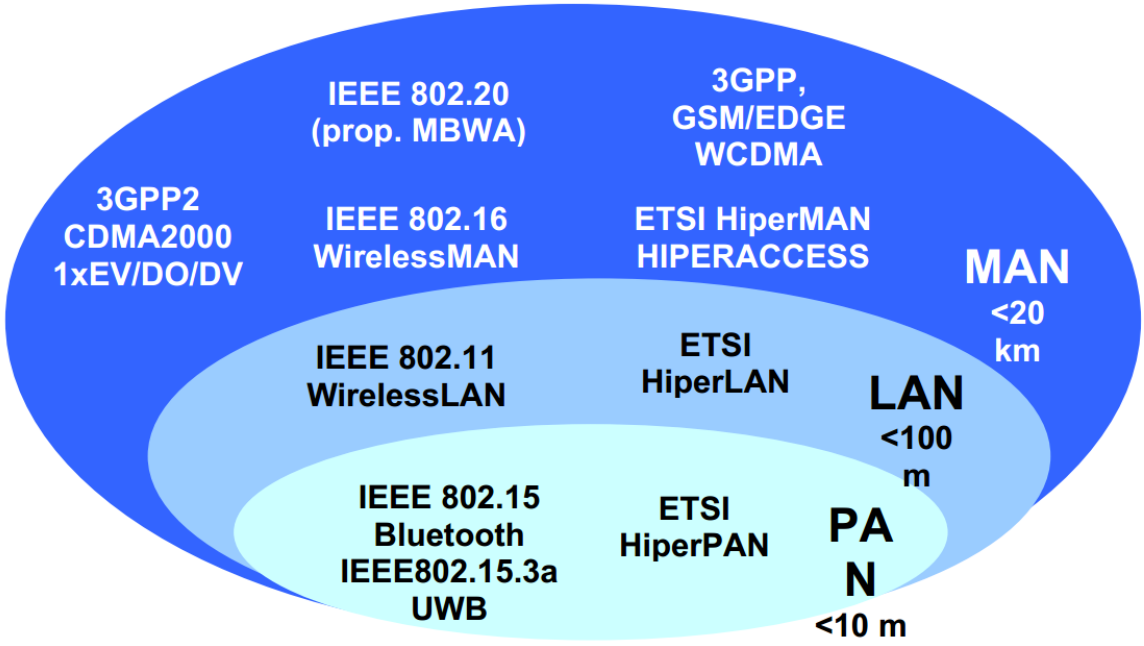


Figura 3.4 Tecnologías inalámbricas por área cubierta

Fuente: Colegio Oficial de Ingenieros de Telecomunicaciones

Con los datos y conocimientos alcanzados en los tres primeros capítulos, se procederá a realizar el análisis de la red *wireless* existente y posteriormente a diseñar la nueva red.

CAPÍTULO IV

ANÁLISIS DE LA RED *WIRELESS* ACTUAL Y DISEÑO DE LA NUEVA SOLUCIÓN PARA EL CAMPUS UCSG

4.1. Requerimientos del cliente.

Para definir los requerimientos que deben ser cumplidos por el diseño propuesto se mantuvo varias reuniones con el personal encargado del centro de cómputo de la UCSG. Durante estas sesiones fueron planteadas las siguientes necesidades:

- Analizar la situación actual de la red *wireless* del campus UCSG.
- Analizar el consumo de ancho de banda de la VLAN de Internet para la red *wireless.*
- Determinar las áreas sin cobertura inalámbrica dentro del campus UCSG.
- Elaborar un diseño con tecnología Cisco para la red *wireless* con cobertura total del campus UCSG.

En la actualidad el ancho de banda disponible para el acceso a Internet por la red *wireless* es de 5 Mbps. Esta capacidad es entregada sin ninguna regla de *QoS* por lo que se pueden presentar problemas de lentitud en sectores, lo recomendado es establecer prioridades a los diferentes tipos de tráfico dentro de la red.

4.1.1. Metas organizacionales

Lo esperado es ofrecer un servicio de alta calidad para los usuarios dentro del campus UCSG que utilizan el acceso inalámbrico y expandir el área de cobertura actual para facilitar el acceso desde cualquier ubicación dentro del campus.

4.1.2. Restricciones organizacionales

Durante las etapas de análisis y diseño es muy importante la comunicación con el personal encargado de la UCSG para programar las tareas necesarias. Esta relación de colaboración debe ser continua para lograr cumplir los requerimientos del cliente en los tiempos establecidos.

Se debe establecer un presupuesto aproximado para poder tomar las decisiones adecuadas referentes a los modelos de equipos que se tomarán en cuenta en el diseño de la nueva infraestructura para el campus.

Evaluar el conocimiento actual del personal que estará a cargo de la operación de la red para definir las capacitaciones que sean necesarias. Es muy importante tomar esta consideración ya que de ellos dependerá el éxito de la solución planteada conforme la red siga creciendo.

4.1.3. Metas de carácter técnico.

Con el diseño de esta solución se espera obtener mayor estabilidad y escalabilidad en la red *wireless* del campus UCSG brindando a los usuarios la herramienta más importante en el mundo estudiantil, el Internet.

Conocer el estado actual de la red *wireless* es importante para determinar la calidad de servicio que se está entregando a lo largo del campus UCSG. Asimismo conocer si el ancho de banda de 5 Mbps otorgado es suficiente para satisfacer los requerimientos de los usuarios.

Establecer un esquema de red *wireless* adecuado que permita la rápida gestión y resolución de problemas dentro de la infraestructura instalada y obtener una visión clara del estado y operación de los equipos que permita evaluar de manera constante su funcionamiento.

4.1.4. Restricciones técnicas.

Evaluar la posible compatibilidad de la infraestructura existente con la que está siendo planteada en el diseño para asegurar el correcto funcionamiento de la red cuando sea puesta en operación.

Realizar un análisis de consumo de ancho de banda para medir la cantidad de tráfico y los protocolos más utilizados por los usuarios actuales de la red *wireless* del campus UCSG.

4.2. Descripción de la red existente.

Se ha elaborado un procedimiento para evaluar y analizar la red *wireless* actual con la que cuenta el campus de la UCSG en el cual se incluye a las facultades que comparten el ancho de banda otorgado por el centro de cómputo para brindar Internet a los usuarios. A continuación se enumera las actividades relacionadas:

- Obtener documentación existente.
- Auditoría de la red actual.
- Informe de resultados, observaciones y sugerencias.

4.2.1. Obtener documentación existente.

La red inalámbrica implementada en el campus UCSG, está conformada de equipos que brindan conexión *wireless* de las marcas TPLINK y LINKSYS. Estos equipos se encuentran ubicados en las diversas Facultades y distribuidos de acuerdo a la necesidad que existía a la fecha de la implementación. La instalación de los AP está realizada dentro de cajas plásticas utilizadas comúnmente para albergar dispositivos en instalaciones de equipos de radio en ambiente intemperie.

El recurso de Internet se entrega por parte del ISP en un *router* público el cual se conecta a un *switch* que administra las VLAN que operan dentro de la red del campus UCSG. En este equipo son asignados los puertos a la VLAN creada para la red inalámbrica, del mismo se distribuye el servicio a cada uno de los *switches* ubicados en las facultades por medio de conexiones de fibra óptica tipo Monomodo.

Al *switch* de cada facultad se conecta el *router* inalámbrico que asigna el direccionamiento privado a cada uno de los clientes inalámbricos y brinda el servicio de Internet tal como lo muestra la figura 4.1.

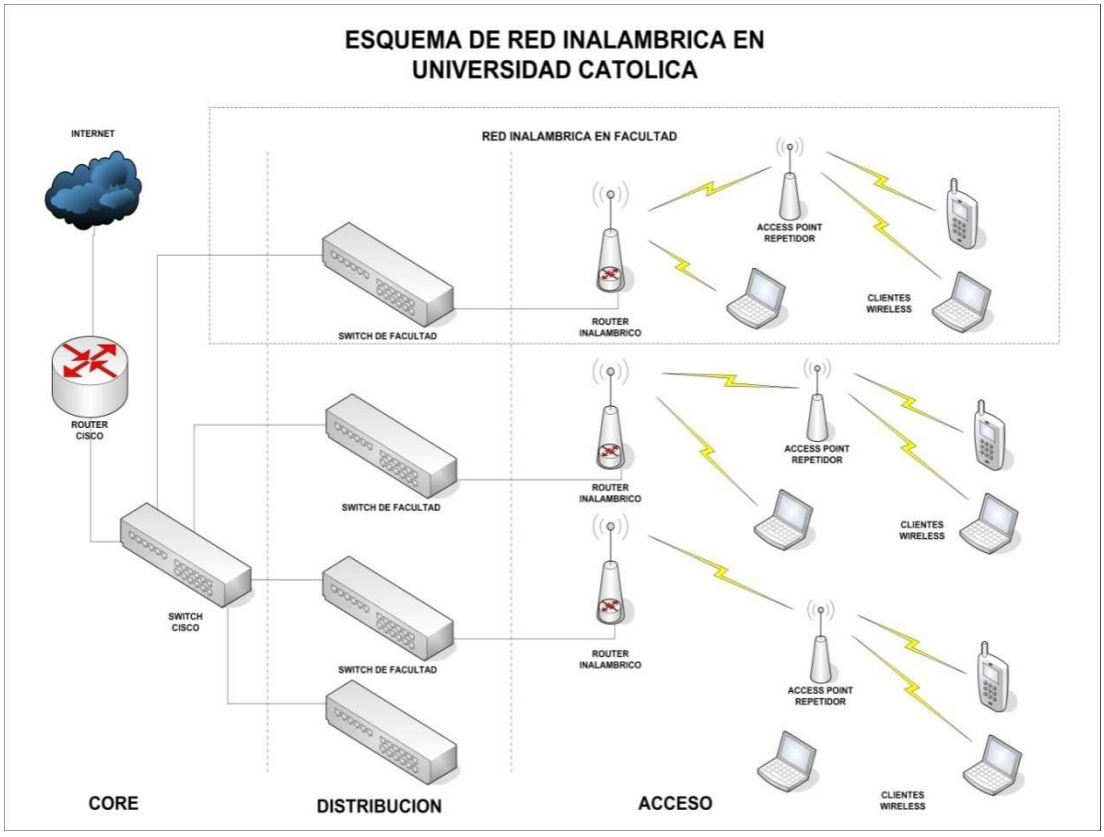


Figura 4.1 – Diagrama de Red *Wireless* del campus UCSG.

Fuente: Autores

4.2.2. Auditoría de la red actual.

Existen varias herramientas para poder llevar a cabo esta tarea que ayudará a tener la visión del estado general de la red *wireless* del campus UCSG. Se utilizará el software *VisiWave Site Survey* y a continuación se detalla el procedimiento que se efectuará por cada facultad para obtener los datos necesarios para iniciar el diseño de la nueva solución.

Para el proceso de análisis utilizando este programa es necesario previamente tener la foto digital o plano del área que se analizará. Se pueden utilizar los formatos de imagen jpg, jpeg,bmp, gif, png. En este software existen tres métodos de captura de datos para el análisis de la red inalámbrica:

- Paso a Paso
- Continuo
- GPS (*Global Positioning System*, Sistema de Posicionamiento Global)

Cuando se utiliza el método GPS se confirma que existen valores erróneos en el posicionamiento, debido a que los dispositivos GPS tienen un margen de error de algunos metros y en este caso en el que los dispositivos inalámbricos no están muy alejados unos de otros, unos metros son críticos.

Elegimos dos métodos inicialmente el Paso a Paso, el cual consiste en ir definiendo algunos puntos de captura en el área de análisis de tal forma que el programa pueda dibujar el patrón de radiación de los APs.

El método continuo es parecido al Paso a Paso con la diferencia que la captura de información es más exacta y por ende la grafica resultante es más fiel al ambiente de radiación.

Se conoce que los clientes AP o tarjetas de red inalámbricas de los dispositivos móviles pueden conectarse a un *Access Point* cuando en la ubicación en la que se encuentra dicho cliente inalámbrico existe un nivel de señal de 70 dB, con esto se garantiza la conectividad. A medida que los niveles de señal toman valores que tienden a cero, significa que la potencia de la señal aumenta.

Procedimiento: Configuración del ambiente para análisis. En este punto inicial se realiza lo siguiente:

1. Se elige correctamente el gráfico a utilizar, en el caso de la Facultad Técnica se eligió un plano en el que se muestra una vista de planta, fue la más adecuado ya que la disposición de los equipos inalámbricos están en los alrededores de los edificios que conforman dicha facultad. Se define la escala a utilizarse, mediante una herramienta del mismo programa en el que conociendo la distancia entre dos puntos físicos en el plano se coloca el valor en metros. Se selecciona en las opciones del programa la tarjeta de red que se utilizará en la captura de señal WIFI y se indica el método de captura a realizarse, inicialmente se utiliza el paso a paso.
2. El personal a cargo de esta tarea se ubica físicamente en el primer punto de recolección de datos que concuerde con el gráfico y se empieza la grabación de información. A medida que se van moviendo físicamente deben confirmar la ubicación que se tiene en el gráfico para hacer la captura de datos correspondiente a cada punto. En el caso de las Facultades ubicadas en edificios de más de un piso tales como la Facultad de Jurisprudencia, se utilizaron los planos por piso de dichos edificios.
3. Luego de realizada la captura de datos de las redes inalámbricas de cada Facultad se identifican los AP que dan cobertura a dicha área y se generan los gráficos de cobertura para el respectivo análisis.

En los gráficos se podrá observar la cobertura de los equipos inalámbricos segmentada por colores que representan la fuerza de la señal en el área analizada. El

área en color azul, mientras más oscuro sea el nivel de señal será mayor. La parte color naranja representa el área en la que existe menos cobertura con lo mínimo necesario para una conexión inalámbrica de un cliente o AP.

El nivel de señal depende de algunos factores, tales como:

- Densidad de las paredes de los edificios.
- Potencia de radiación de los equipos.
- Disposición de las antenas de los equipos.
- Ganancia de los equipos AP.

Análisis gráfico por Facultades: A continuación se muestran los gráficos del análisis de cobertura de los diferentes *Access Point* en las Facultades de la Universidad Católica de Santiago de Guayaquil.

Facultad de Ciencias Médicas

Planta Baja: En la figura 4.2 se observa una cobertura aproximada del 90% del área total con intensidad óptima para una conexión inalámbrica. El área de color azul intenso representa la cobertura de mayor intensidad, aproximadamente -45dB. El área en color naranja tiene intensidad de -70dB lo cual es lo mínimo para una conexión inalámbrica.

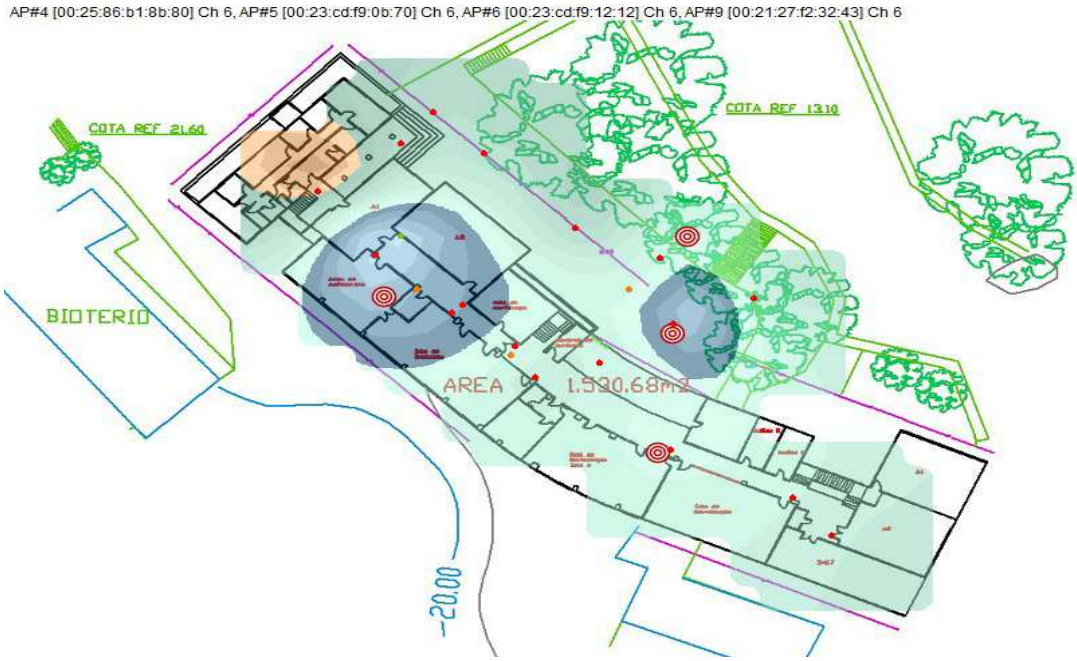


Figura 4.2 Planta baja, Facultad Ciencias Médicas UCSG

Fuente: Autores

Primera Planta: En la figura 4.3 se muestra una cobertura aproximada del 80% del área total.

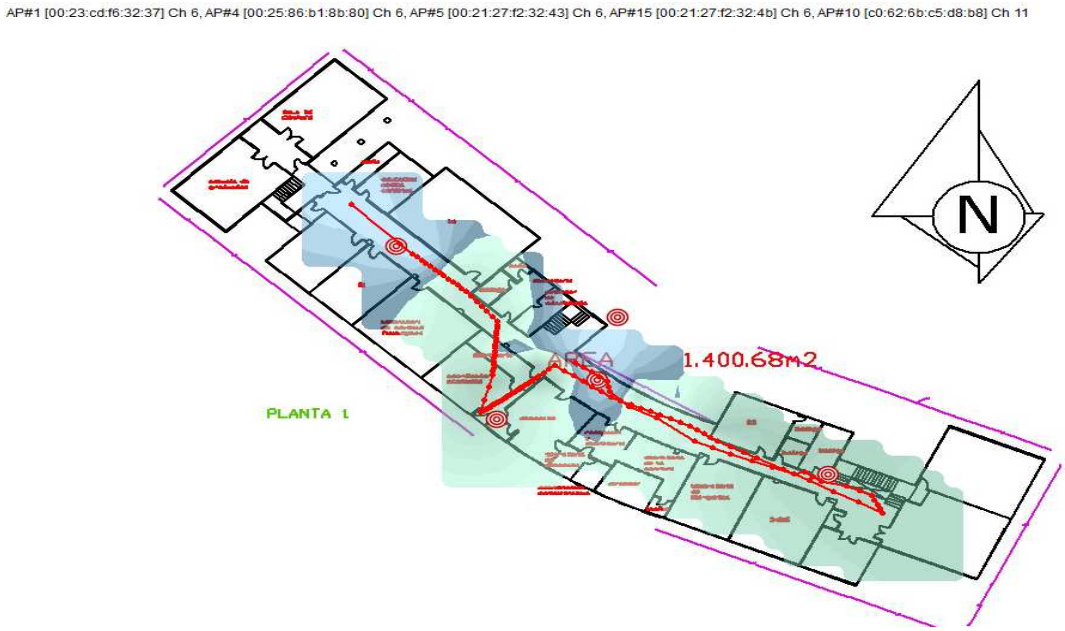


Figura 4.3 Primera planta, Facultad Ciencias Médicas UCSG

Fuente: Autores

Segunda planta: En la figura 4.4 se muestra una cobertura aproximada del 80% del área total.

Figura 4.4 Segunda planta, Facultad Ciencias Médicas UCSG

Fuente: Autores

Primera planta del Edificio Nuevo: En la figura 4.5 se muestra una cobertura aproximada del 60% del área total.

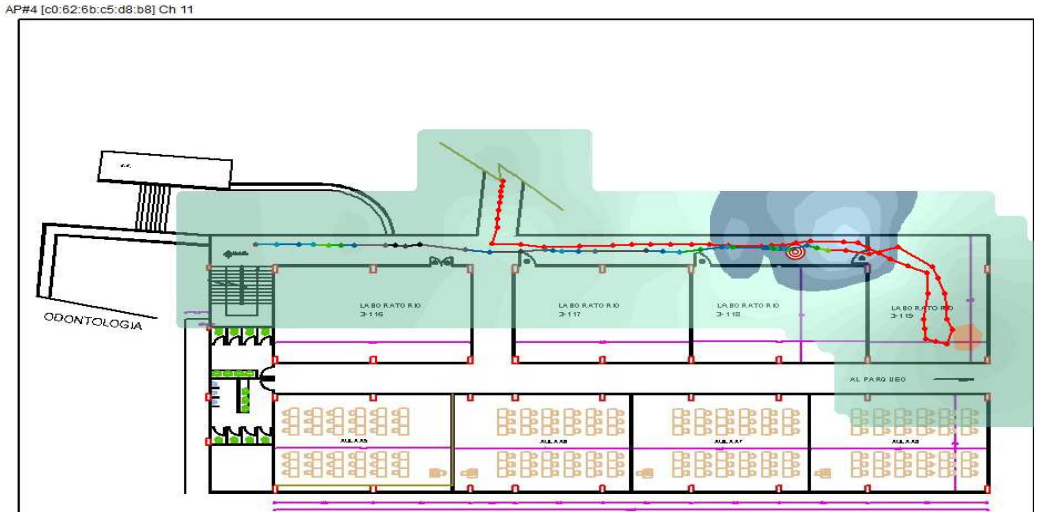


Figura 4.5 Primera planta de Edificio Nuevo, Facultad Ciencias Médicas UCSG

Fuente: Autores

Segunda planta del Edificio Nuevo: En la figura 4.6 se muestra una cobertura aproximada del 90% del área total.

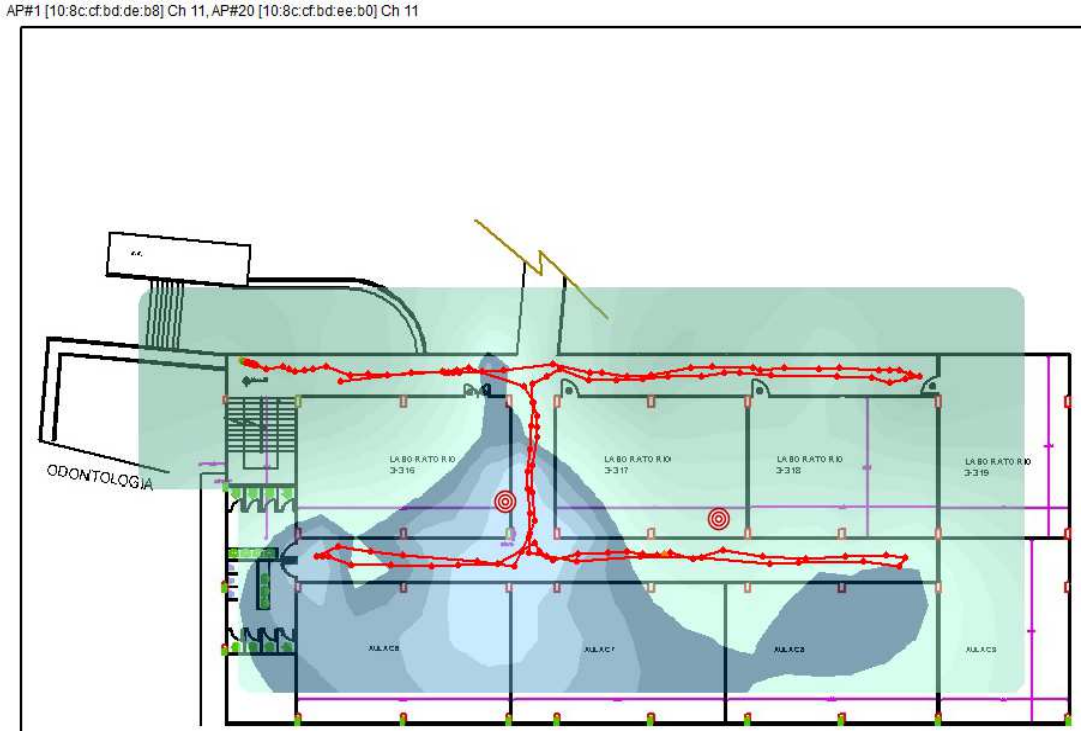


Figura 4.6 Segunda planta de Edificio Nuevo, Facultad Ciencias Médicas UCSG

Fuente: Autores

En el análisis realizado en la Facultad de Medicina se nota que existen varios AP que se encuentran configurados en el mismo canal de frecuencias, esto ocasiona interferencia e impide una transmisión y recepción óptima de señal. En los casos que se necesite ubicar equipos en los que pueda existir *overlap* de señales, estos deben estar configurados en diferentes canales de frecuencia.

A continuación se muestra el detalle de los equipos AP operativos en la Facultad de Medicina, en la figura 4.7 se observa que los equipos ubicados en las aulas están configurados para operar en el canal 11 y los 10 equipos que se encuentran en las diferentes áreas están configurados para operar en el canal 6.

SSID	AP#	Name	MAC	Ch	Security	Mode	Ave SNR	Max SNR	Min SNR	# Assoc Points	# Non-Assoc Points
Medicina	AP #1		00:23:cd:f6:32:37	Ch 6	Clear	Infra	23	68	11	0	228
Medicina	AP #3		00:21:27:f2:2d:41	Ch 6	Clear	Infra	21	39	13	0	33
Medicina	AP #4		00:25:86:b1:8b:80	Ch 6	Clear	Infra	42	72	12	0	742
Medicina	AP #5		00:21:27:f2:32:43	Ch 6	Clear	Infra	63	80	11	442	195
Medicina	AP #6		00:23:cd:f9:12:12	Ch 6	Clear	Infra	24	33	12	0	519
Medicina	AP #9		00:21:27:f2:33:5d	Ch 6	Clear	Infra	19	46	12	0	196
Medicina	AP #14		00:23:cd:f9:0d:93	Ch 6	Clear	Infra	46	54	12	0	639
Medicina	AP #15		00:21:27:f2:32:4b	Ch 6	Clear	Infra	27	45	12	0	42
Medicina	AP #17		00:21:27:f2:32:8d	Ch 6	Clear	Infra	27	47	11	0	555
Medicina	AP #27		00:23:cd:f9:0b:70	Ch 6	Clear	Infra	48	55	12	0	636
medicina_aulas	AP #10		c0:62:6b:c5:d8:b8	Ch 11	Clear	Infra	18	51	11	0	661
medicina_aulas	AP #16		10:8c:cf:bd:de:b8	Ch 11	Clear	Infra	31	43	13	0	69
medicina_aulas	AP #19		e8:40:40:80:ca:a8	Ch 11	Clear	Infra	20	30	12	0	80
medicina_aulas	AP #20		10:8c:cf:bd:ee:b0	Ch 11	Clear	Infra	18	24	11	0	49
medicina_aulas	AP #21		1c:aa:07:ec:d6:18	Ch 11	Clear	Infra	18	32	12	0	58

Figura 4.7 Access Point encontrado, Facultad Ciencias Médicas UCSG

Fuente: Autores

El equipo r*outer* inalámbrico ubicado en la Facultad de Medicina tiene las siguientes características:

Marca: TPLINK

Firmware Version: 3.4.6 Build 090226 Rel.63282n

Hardware Version: WR941N/WR941ND v2 00000000

En la tabla 4.1 se muestra el listado de los dispositivos conectados a la red inalámbrica con su respectiva dirección MAC, el puerto IP asignado por el *router* y el tiempo asignado a la IP antes de su renovación. En esta configuración de red de equipos inalámbricos, el *router* tiene conectado varios AP formando una red de transporte *wireless*.

Tabla 4.1 Listado de dispositivos Conectados Facultad Ciencias Médicas

Fuente: Autores

ID	ClientName	MAC Address	Assigned IP	Lease Time
1	BLACKBERRY-CE6D	A0-6C-EC-83-0F-2E	192.168.0.100	00:21:28

2	BLACKBERRY-8DD7	2C-A8-35-C1-84-77	192.168.0.141	00:45:10
3	Unknown	00-23-B4-E8-6B-6F	192.168.0.102	01:04:43
4	LiliPhone	CC-08-E0-58-6A-21	192.168.0.101	00:03:04
5	Unknown	00-25-47-7F-D6-33	192.168.0.111	00:32:22
6	BLACKBERRY-C6AD	E8-3E-B6-8A-A9-96	192.168.0.106	00:41:17
7	BLACKBERRY-5F20	40-5F-BE-1E-3D-5C	192.168.0.107	01:35:31
8	Christians-iPad	28-6A-BA-69-73-BA	192.168.0.108	01:09:49
9	BLACKBERRY-8CF1	80-60-07-EB-1D-DA	192.168.0.109	01:59:28
10	BLACKBERRY-9345	40-6A-AB-8B-DD-6E	192.168.0.110	01:42:35
11	BLACKBERRY-C2BD	F4-0B-93-69-09-1E	192.168.0.112	01:55:27
12	android-d28abd281249b0fa	5C-0A-5B-BC-AD-0A	192.168.0.115	00:33:26
13	BLACKBERRY-325B	A8-6A-6F-E7-5B-1F	192.168.0.116	00:48:52
14	BLACKBERRY-E0AE	A8-6A-6F-DE-08-72	192.168.0.135	01:31:25
15	BLACKBERRY-8509	40-6A-AB-F1-8F-A4	192.168.0.118	01:48:11
16	BLACKBERRY-0F56	68-ED-43-2B-96-05	192.168.0.119	01:48:58
17	Unknown	C8-19-F7-B1-A2-4C	192.168.0.172	01:51:56
18	BLACKBERRY-AFD8	CC-55-AD-23-38-CC	192.168.0.121	00:08:17
19	kevin	64-20-0C-8F-5E-CA	192.168.0.122	00:02:00
20	BLACKBERRY-CB38	70-D4-F2-24-85-9F	192.168.0.123	00:47:14
21	Unknown	F0-E7-7E-29-56-F5	192.168.0.198	01:05:45
22	Stefy	70-73-CB-36-E3-99	192.168.0.168	00:02:40
23	Unknown	60-FA-CD-6B-BE-93	192.168.0.124	00:13:37
24	BLACKBERRY-782D	68-ED-43-46-71-9D	192.168.0.127	00:43:00
25	BELEN	F0-DC-E2-68-5C-9E	192.168.0.125	00:05:03
26	MacFernando	68-A8-6D-2B-D8-0E	192.168.0.126	00:04:20
27	Esther	14-8F-C6-94-06-58	192.168.0.129	00:16:01
28	BLACKBERRY-8A1C	F4-0B-93-CF-E3-48	192.168.0.130	00:16:24

29	Unknown	28-D1-AF-4F-81-E5	192.168.0.176	01:21:35
30	Unknown	7C-61-93-9D-75-09	192.168.0.161	01:46:46
31	android-3b532cd6722e704f	28-98-7B-C7-4F-98	192.168.0.114	01:14:14
32	Unknown	14-5A-05-24-88-F6	192.168.0.104	00:15:48
33	Unknown	D0-C1-B1-C9-2C-85	192.168.0.128	01:14:08
34	Unknown	E0-A6-70-FD-7B-14	192.168.0.117	00:27:31
35	BLACKBERRY-10D9	80-60-07-E0-F4-6E	192.168.0.173	00:38:22
36	BLACKBERRY-D6AC	14-74-11-0B-7A-C2	192.168.0.193	01:58:02
37	BLACKBERRY-78D1	40-5F-BE-85-04-5B	192.168.0.140	01:05:07
38	Romina-Paredes	E0-C9-7A-D2-E1-6F	192.168.0.139	00:49:18
39	BLACKBERRY-9617	68-ED-43-2C-B0-2E	192.168.0.142	01:57:17
40	BLACKBERRY-A9A6	14-74-11-78-85-98	192.168.0.185	01:42:15
41	Totos-Iphone	E0-C9-7A-C9-9F-69	192.168.0.147	01:06:12
42	Carlos-Quezada	54-26-96-78-06-41	192.168.0.148	00:57:16
43	BLACKBERRY-91B2	E8-3E-B6-BA-AA-AA	192.168.0.143	01:49:22
44	BLACKBERRY-E1F3	A0-6C-EC-E4-12-F5	192.168.0.149	01:44:46
45	BLACKBERRY-16D2	70-D4-F2-73-34-73	192.168.0.145	01:00:57
46	Unknown	F8-D0-BD-66-1A-30	192.168.0.150	01:10:15
47	BLACKBERRY-C472	40-5F-BE-BB-1C-AF	192.168.0.181	00:37:18
48	Nicole	E0-C9-7A-ED-14-6E	192.168.0.153	00:57:01
49	Unknown	EC-85-2F-25-B2-8E	192.168.0.138	00:15:54
50	LuQuiroz	D8-A2-5E-AB-15-44	192.168.0.151	01:11:02
51	iPhone	78-A3-E4-E0-AC-7D	192.168.0.154	01:11:57
52	Unknown	00-F4-B9-28-EE-33	192.168.0.155	01:37:51
53	android_9774d56d682e549c	74-A7-22-99-C6-08	192.168.0.159	01:05:43
54	BLACKBERRY-2D87	E8-3E-B6-F3-CF-6E	192.168.0.157	00:34:01
55	BLACKBERRY-459D	14-74-11-36-8B-7B	192.168.0.156	01:35:29

56	android-a44ef09697e2f879	BC-20-A4-53-99-5B	192.168.0.189	01:29:49
57	Unknown	CC-F9-E8-9E-79-60	192.168.0.166	01:13:03
58	BLACKBERRY-EBC7	CC-55-AD-04-7C-0E	192.168.0.175	01:37:01
59	Unknown	1C-66-AA-25-16-FF	192.168.0.164	01:26:29
60	BLACKBERRY-A9DF	2C-A8-35-DD-3B-EC	192.168.0.182	01:48:21
61	Unknown	78-2E-EF-F9-02-74	192.168.0.158	01:08:07
62	BLACKBERRY-C38A	A8-6A-6F-16-02-A6	192.168.0.167	01:39:46
63	android_252199ad30ce0fa0	8C-77-12-AD-A2-61	192.168.0.133	00:28:18
64	BLACKBERRY-A5F8	CC-55-AD-9D-4B-CF	192.168.0.195	01:58:34
65	BLACKBERRY-A5A5	F4-0B-93-9F-49-27	192.168.0.170	01:45:16
66	Unknown	98-0C-82-CC-5D-56	192.168.0.152	00:49:04
67	BLACKBERRY-3FC2	30-7C-30-CB-C1-68	192.168.0.186	01:48:21
68	iPad-de-Carla	8C-2D-AA-C0-95-52	192.168.0.134	01:05:03
69	ANTHONY	18-E7-F4-7A-63-7ª	192.168.0.174	00:10:45
70	Unknown	98-03-D8-DB-98-A3	192.168.0.163	01:12:59
71	BLACKBERRY-79E2	E8-3E-B6-04-D9-7B	192.168.0.160	01:17:31
72	Unknown	00-07-AB-D3-4A-52	192.168.0.177	00:47:04
73	Unknown	60-33-4B-B8-13-DB	192.168.0.178	01:00:46
74	Liss-Silva	F0-CB-A1-1E-AD-47	192.168.0.179	00:23:23
75	android_9fc8ff40ad2afc9	90-C1-15-72-CD-9F	192.168.0.131	01:27:04
76	BLACKBERRY-EE04	14-74-11-42-A9-01	192.168.0.137	01:35:31
77	Joel	00-26-B0-0F-12-6C	192.168.0.180	01:33:10
78	BLACKBERRY-4399	3C-74-37-3B-2E-F9	192.168.0.146	01:35:29
79	android_eda807e693bf0c19	5C-DA-D4-FE-87-FB	192.168.0.183	01:50:54
80	BLACKBERRY-C34B	F4-0B-93-DA-83-E9	192.168.0.184	00:49:04
81	android-d4c9c8dce24ead1a	98-0C-82-16-E4-81	192.168.0.165	01:39:57
82	BLACKBERRY-AEB6	CC-55-AD-97-42-4B	192.168.0.144	01:53:02

83	BLACKBERRY-AB62	14-74-11-10-F8-5F	192.168.0.187	01:40:59
84	BLACKBERRY-D07B	30-7C-30-C6-0E-18	192.168.0.188	01:51:22
85	BLACKBERRY-00EF	70-D4-F2-24-BA-07	192.168.0.120	01:55:39
86	BLACKBERRY-5350	30-7C-30-9A-9A-C1	192.168.0.190	01:55:27
87	BLACKBERRY-3317	30-7C-30-C5-D7-23	192.168.0.191	01:59:55

Facultad de Jurisprudencia

Se encontró que en esta Facultad el *router* Inalámbrico está ubicado con las antenas omnidireccionales en dirección vertical, de tal forma que se pueda conseguir mayor cobertura entre los pisos, además esta configuración permite que los AP ubicados en los diferentes pisos trabajen como repetidores del *router* principal que se encuentra ubicado en el primer piso.

Primera Planta: En la figura 4.8 se muestra una cobertura aproximada del 80% del área total.

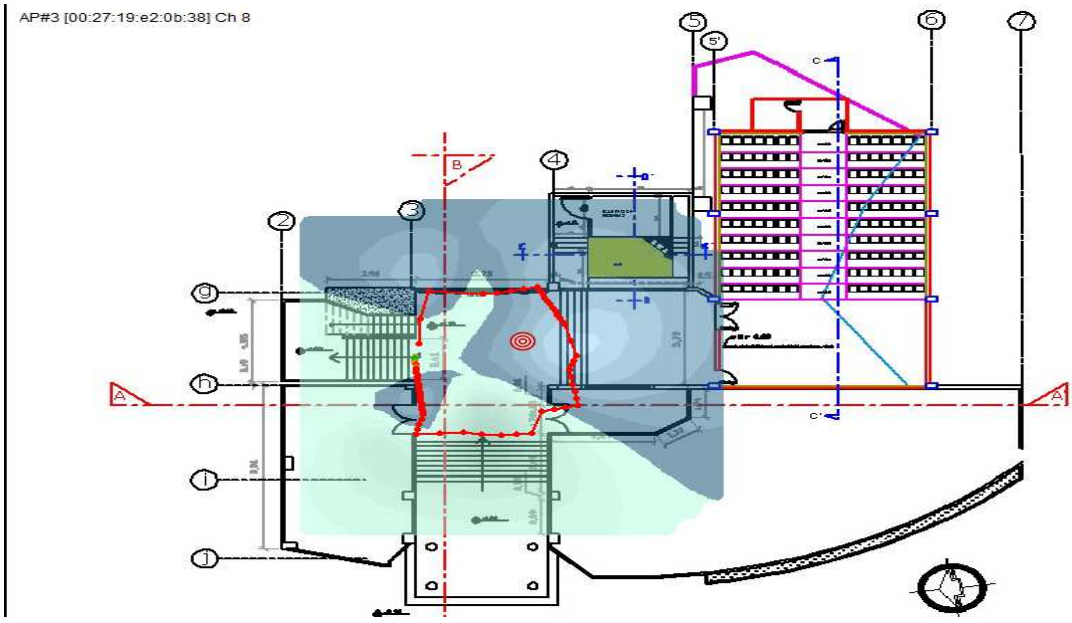


Figura 4.8 Primera planta, Facultad Jurisprudencia UCSG

Fuente: Autores

Segunda Planta: En la figura 4.9 se muestra una cobertura aproximada del 80% del área total.

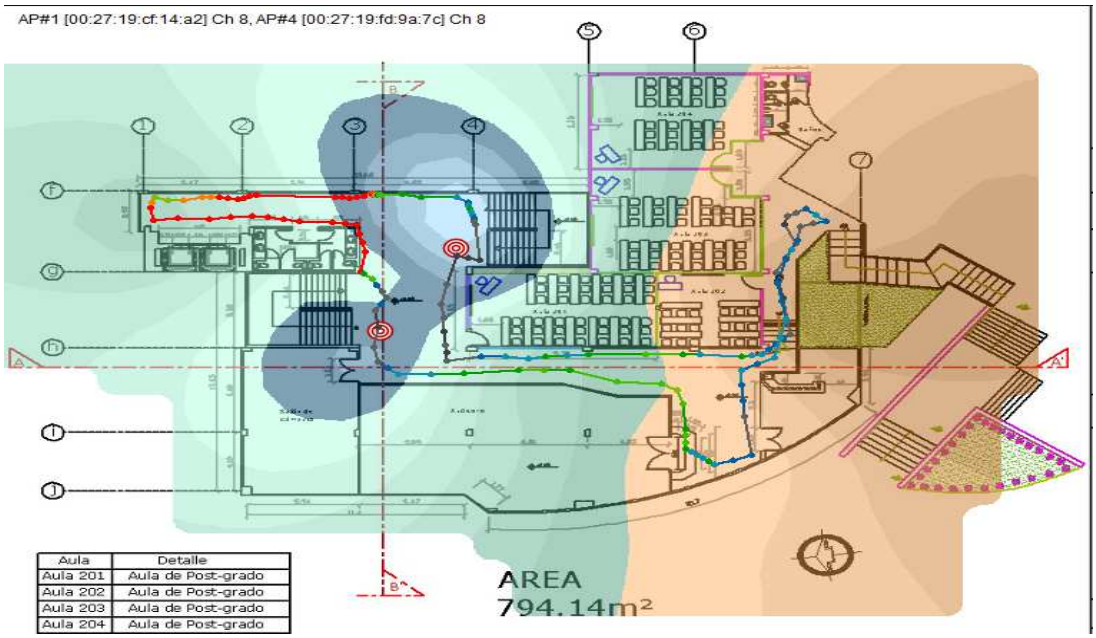


Figura 4.9 Segunda planta, Facultad Jurisprudencia UCSG

Fuente: Autores

Tercera Planta: En la figura 4.10 se muestra una cobertura aproximada del 90% del área total.

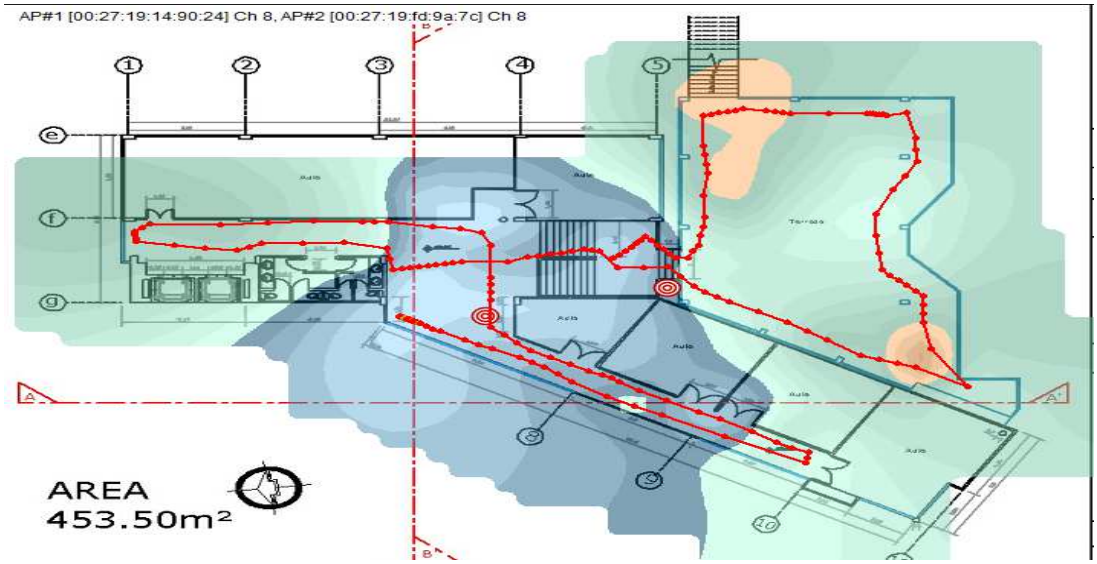


Figura 4.10 Tercera planta, Facultad Jurisprudencia UCSG

Fuente: Autores

Cuarta Planta : En la figura 4.11 se muestra una cobertura aproximada del 90% del área total.

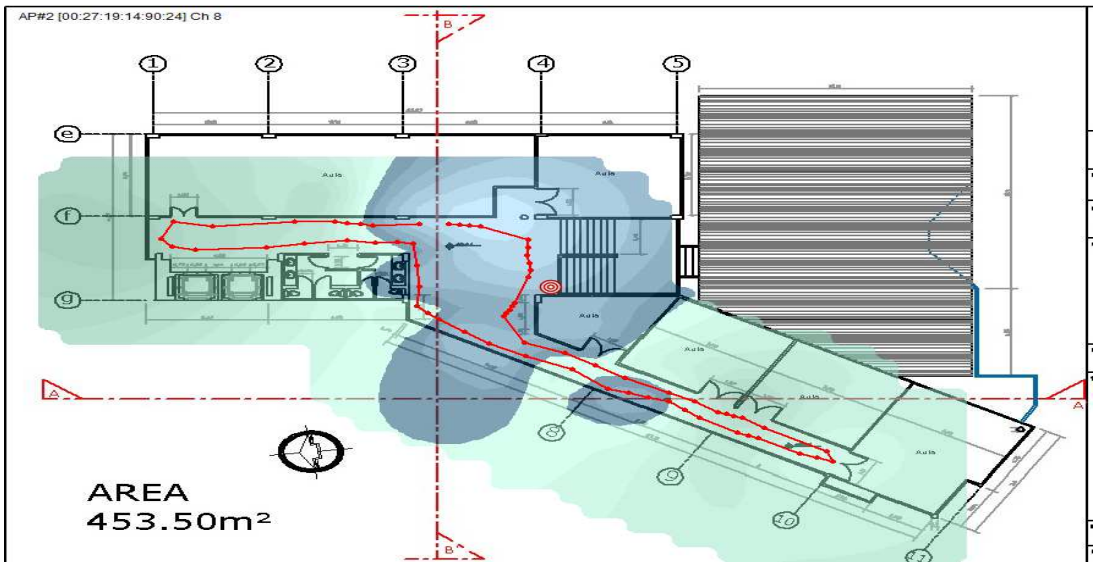


Figura 4.11 Cuarta planta, Facultad Jurisprudencia UCSG

Fuente: Autores

Quinta Planta: En la figura 4.12 se muestra una cobertura aproximada del 40% del área total.

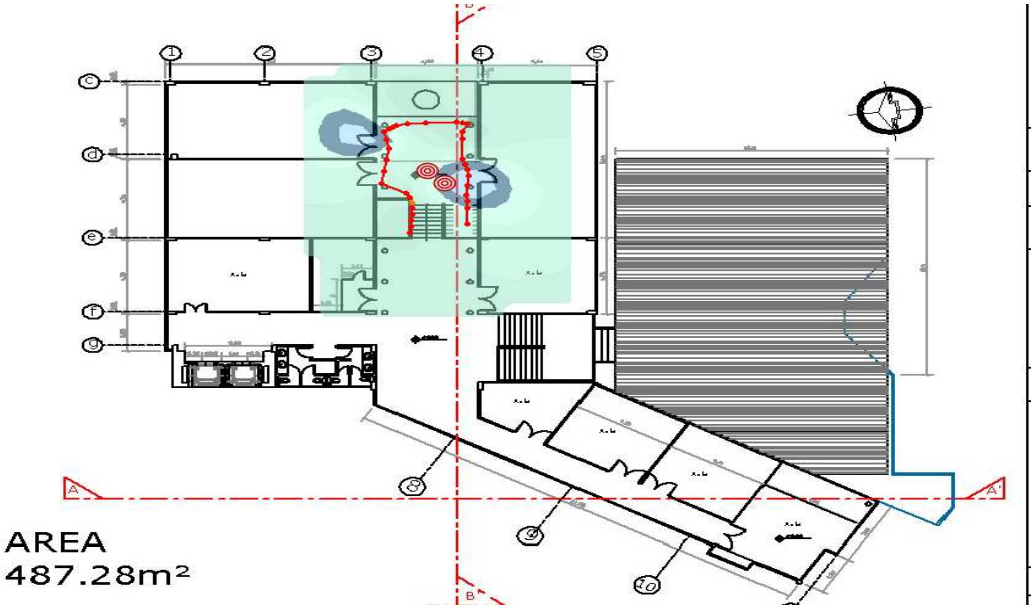


Figura 4.12 Quinta planta, Facultad Jurisprudencia UCSG

Fuente: Autores

Sexta Planta: En la figura 4.13 se muestra una cobertura aproximada del 20% del área total.

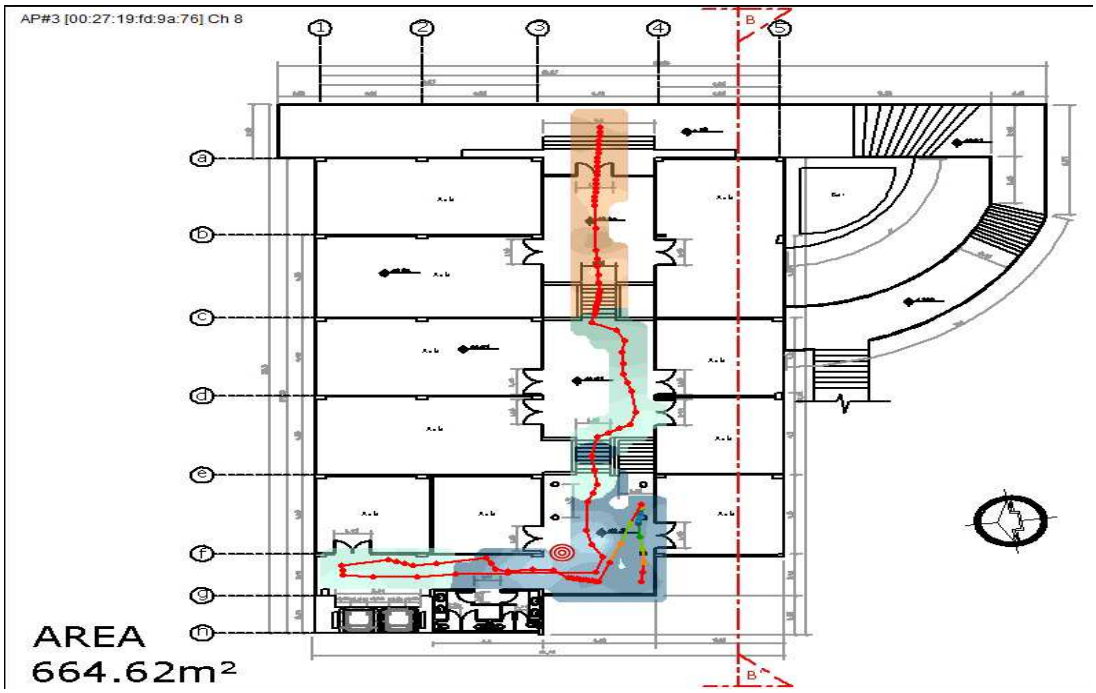


Figura 4.13 Sexta planta, Facultad Jurisprudencia UCSG

Fuente: Autores

Se encontró que en esta facultad existen 6 equipos configurados en canal 8 y uno en canal 12, esta configuración de canales aplicadas en los equipos inalámbricos impide que exista una buena cobertura e incluso los equipos inalámbricos tienden a bloquearse entre ellos como se muestra en la figura 4.14.

SSID	AP#	Name	MAC	Ch	Security	Mode	Ave SNR	Max SNR	Min SNR	# Assoc Points	# Non-Assoc Points
Juris_WiFi	AP #1		00:27:19:14:90:24	Ch 8	Clear	Infra	42	55	12	0	343
Juris_WiFi	AP #2		00:27:19:fd:9a:7c	Ch 8	Clear	Infra	58	81	13	0	354
Juris_WiFi	AP #4		00:27:19:cf:14:a2	Ch 8	Clear	Infra	27	40	12	0	305
Juris_WiFi	AP #5		00:27:19:e2:0b:38	Ch 8	Clear	Infra	14	18	11	0	144
Juris_WiFi	AP #6		00:27:19:fd:9a:76	Ch 8	Clear	Infra	19	40	11	0	202
Juris_WiFi	AP #10		00:27:19:cf:14:a2	Ch 12	Clear	Infra	21	30	13	0	18
Juris_WiFi	AP #32		00:27:19:14:97:a2	Ch 8	Clear	Infra	12	12	12	0	1

Figura 4.14 Access Point encontrado, Facultad de Jurisprudencia UCSG

Fuente: Autores

A continuación en la tabla 4.2 se muestra la cantidad de clientes simultáneos de la Facultad de Jurisprudencia.

Tabla 4.2 Listado de dispositivos Conectados Facultad Jurisprudencia

Fuente: Autores

ID	ClientName	MAC Address	Assigned IP	Lease Time
1	Sylkita	90-27-E4-A6-56-6F	192.168.1.183	01:47:15
2	BLACKBERRY-E877	CC-55-AD-6A-D9-87	192.168.1.101	01:44:57
3	android-f7db5b0770b25b59	3C-43-8E-B8-09-7A	192.168.1.100	00:59:48
4	BLACKBERRY-C7DC	30-7C-30-2A-BC-96	192.168.1.103	00:53:28
5	BLACKBERRY-C3DA	CC-55-AD-50-50-EA	192.168.1.123	00:51:38
6	BLACKBERRY-9AB5	40-6A-AB-AC-E2-47	192.168.1.106	01:57:25
7	Unknown	D0-C1-B1-19-4E-38	192.168.1.107	00:09:52
8	Unknown	74-45-8A-F0-DA-4A	192.168.1.114	00:52:57
9	BLACKBERRY-737E	80-60-07-CA-76-48	192.168.1.109	01:14:45
10	BLACKBERRY-4482	A8-6A-6F-72-D9-A9	192.168.1.110	00:46:35
11	Unknown	E0-C9-7A-4B-D6-B4	192.168.1.111	01:08:45
12	BLACKBERRY-B518	1C-69-A5-1A-C8-D2	192.168.1.113	00:53:46
13	android-2e4447178d1bf00b	D8-B3-77-57-84-3E	192.168.1.115	00:03:49
14	Unknown	D4-4B-5E-80-0E-44	192.168.1.116	00:04:05
15	BLACKBERRY-ECFC	A0-6C-EC-39-07-81	192.168.1.117	00:18:28
16	BLACKBERRY-E1AC	A0-6C-EC-3F-A7-23	192.168.1.118	01:46:07
17	android-b6d8dd07b8bfdbfd	00-08-CA-A7-CB-F2	192.168.1.149	01:56:23
18	BLACKBERRY-697E	80-60-07-20-C3-89	192.168.1.162	01:06:14
19	Unknown	9C-02-98-C6-20-CB	192.168.1.191	00:16:06
20	BLACKBERRY-1584	80-60-07-FC-AB-1D	192.168.1.124	00:52:49
21	BLACKBERRY-3C0D	70-D4-F2-D7-F0-DE	192.168.1.126	00:01:59
22	PLAYBOOK-506D	A0-6C-EC-CD-60-2C	192.168.1.104	00:07:17

23	Francisco	B8-C7-5D-A1-93-A4	192.168.1.127	01:01:49
24	Unknown	F8-D0-BD-BA-44-71	192.168.1.129	01:02:07
25	Unknown	CC-08-E0-DB-E7-03	192.168.1.130	00:52:24
26	Alexas-iPod	60-FB-42-17-8E-3A	192.168.1.102	01:00:24
27	BLACKBERRY-B0FB	A8-6A-6F-6D-DC-FB	192.168.1.132	01:21:20
28	android-f5113fcaf446282d	20-02-AF-26-47-D9	192.168.1.133	01:26:30
29	BLACKBERRY-96E8	F4-0B-93-79-86-65	192.168.1.134	00:10:00
30	Unknown	14-7D-C5-81-78-4D	192.168.1.108	01:01:27
31	Denisse-iPad	E0-B9-BA-B9-8D-36	192.168.1.171	01:01:31
32	Madeleine-Erazo	8C-FA-BA-6F-62-42	192.168.1.137	01:03:23
33	BLACKBERRY-FFDE	00-26-FF-61-12-EC	192.168.1.138	00:05:57
34	luis-HP	E0-2A-82-A8-D5-4D	192.168.1.139	00:22:39
35	MARLI-VAIO	94-39-E5-A9-FF-46	192.168.1.140	01:25:14
36	BLACKBERRY-B991	2C-A8-35-A7-3A-7F	192.168.1.145	01:16:34
37	iPad-de-Jossue	8C-FA-BA-C9-B8-37	192.168.1.144	00:31:15
38	Unknown	00-F4-B9-50-26-D1	192.168.1.172	01:43:03
39	BLACKBERRY-30EC	00-26-FF-C0-A0-49	192.168.1.119	01:05:40
40	BLACKBERRY-D342	40-6A-AB-F7-5A-16	192.168.1.148	01:40:43
41	BLACKBERRY-9947	3C-74-37-B8-63-FB	192.168.1.184	01:19:44
42	Jorgevela5	4C-B1-99-E2-98-F3	192.168.1.150	01:37:14
43	Nana	18-E7-F4-E0-83-04	192.168.1.159	01:12:23
44	BLACKBERRY-3EC0	40-5F-BE-BA-E7-7D	192.168.1.153	01:50:20
45	BLACKBERRY-8303	30-69-4B-B6-05-80	192.168.1.147	00:45:09
46	Unknown	B8-FF-61-19-F9-EC	192.168.1.156	00:53:10
47	Unknown	00-25-48-6E-FE-B1	192.168.1.157	00:16:32
48	Unknown	B0-65-BD-6F-8E-10	192.168.1.158	00:28:37
49	BLACKBERRY-4268	14-74-11-8E-BE-D7	192.168.1.121	01:58:47

50	iPhone	DC-2B-61-8E-DB-8D	192.168.1.173	01:35:38
51	Unknown	00-F4-B9-47-F9-7C	192.168.1.166	00:05:55
52	iPhone4s	68-09-27-32-AC-56	192.168.1.167	00:35:37
53	Unknown	28-D1-AF-DF-8F-D7	192.168.1.168	00:37:59
54	User1	00-1E-65-72-86-DA	192.168.1.169	00:09:13
55	BLACKBERRY-2223	30-7C-30-53-D8-61	192.168.1.170	00:12:52
56	BLACKBERRY-8DC9	2C-A8-35-8D-48-8A	192.168.1.136	01:57:17
57	Panchito	CC-08-E0-AE-25-69	192.168.1.143	01:30:55
58	Unknown	58-55-CA-76-87-EA	192.168.1.146	01:42:44
59	annis-ipod	8C-7B-9D-51-E6-F5	192.168.1.174	00:13:49
60	BLACKBERRY-327B	68-ED-43-08-CA-FC	192.168.1.175	00:17:02
61	Oscar	5C-95-AE-2B-1E-E7	192.168.1.176	00:36:17
62	Unknown	C0-9F-42-BB-18-16	192.168.1.177	00:18:44
63	BLACKBERRY-2BF7	40-5F-BE-5D-88-B5	192.168.1.178	00:22:17
64	Margarita-PC	00-16-44-A0-40-6B	192.168.1.179	01:44:56
65	Gabriela-DM	70-73-CB-6B-CA-68	192.168.1.180	00:30:27
66	Unknown	7C-C3-A1-80-C6-40	192.168.1.181	00:41:49
67	BLACKBERRY-0CC9	CC-55-AD-19-70-F3	192.168.1.182	00:43:05
68	android-97be2f45a74d4c1d	58-C3-8B-62-4D-F0	192.168.1.152	01:48:39
69	Unknown	B0-65-BD-3E-24-A8	192.168.1.190	01:50:44
70	android-118c5b2158265dff	28-98-7B-D7-56-51	192.168.1.185	00:50:58
71	Unknown	BC-85-1F-DD-11-E8	192.168.1.186	00:52:03
72	KarOx	B8-C7-5D-B0-E2-BC	192.168.1.187	00:57:35
73	Miguel-angel	68-09-27-2D-98-7F	192.168.1.188	00:58:11
74	Unknown	04-54-53-6B-B4-44	192.168.1.189	00:58:32
75	Unknown	8C-77-12-1F-F1-BC	192.168.1.192	01:54:59
76	BLACKBERRY-3189	30-7C-30-27-E7-EE	192.168.1.193	01:59:30

77	Unknown	0C-77-1A-13-2A-27	192.168.1.194	01:59:06
78	IPHONE-4-PABLO	40-A6-D9-C2-A8-7A	192.168.1.195	01:56:16
79	BLACKBERRY-3EC9	A0-6C-EC-33-14-79	192.168.1.196	01:57:44
80	PC-PC	78-E4-00-73-75-1A	192.168.1.197	01:57:54

Cabe destacar que se encontraron 80 clientes simultáneos en este *router* y debido a que este equipo es de tipo casero se inhibe con frecuencia. La tabla de direcciones MAC del equipo no tiene soporte para tantos clientes DHCP y por este motivo los usuarios no pueden conectarse una vez que se excede el límite soportado por el *router*.

Facultad de Arquitectura

Planta Baja: En la figura 4.15 se muestra una cobertura aproximada del 60% del área total.

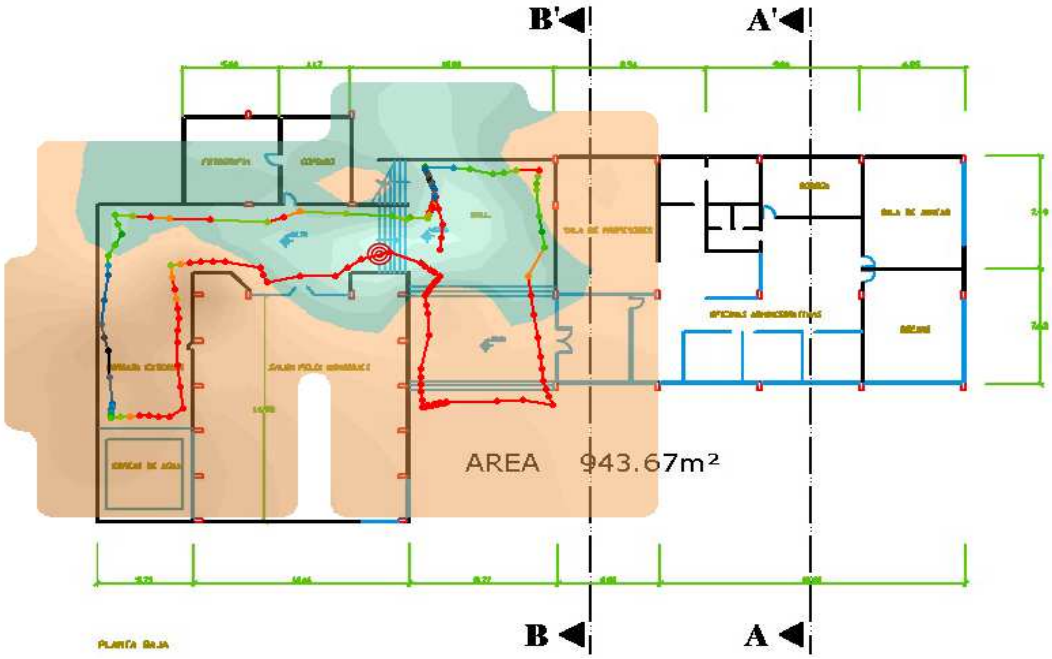


Figura 4.15Planta Baja, Facultad Arquitectura UCSG

Fuente: Autores

Primera Planta: En la figura 4.16 se muestra una cobertura aproximada del 80% del área total.

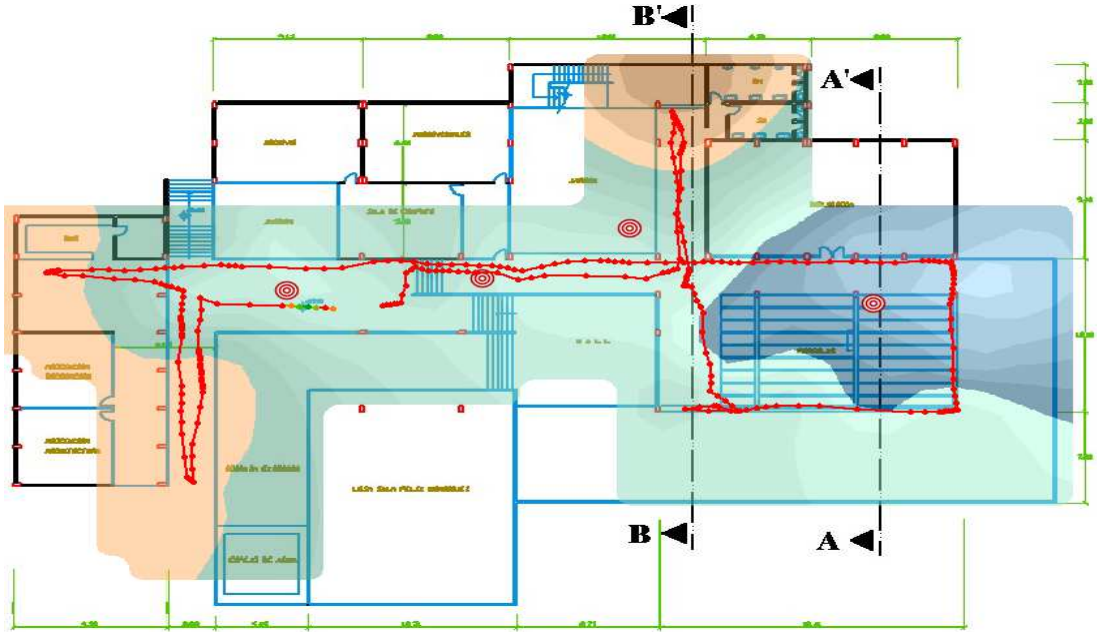


Figura 4.16Primera planta, Facultad Arquitectura UCSG

Fuente: Autores

Segunda Planta: En la figura 4.17 se muestra una cobertura aproximada del 80% del área total.

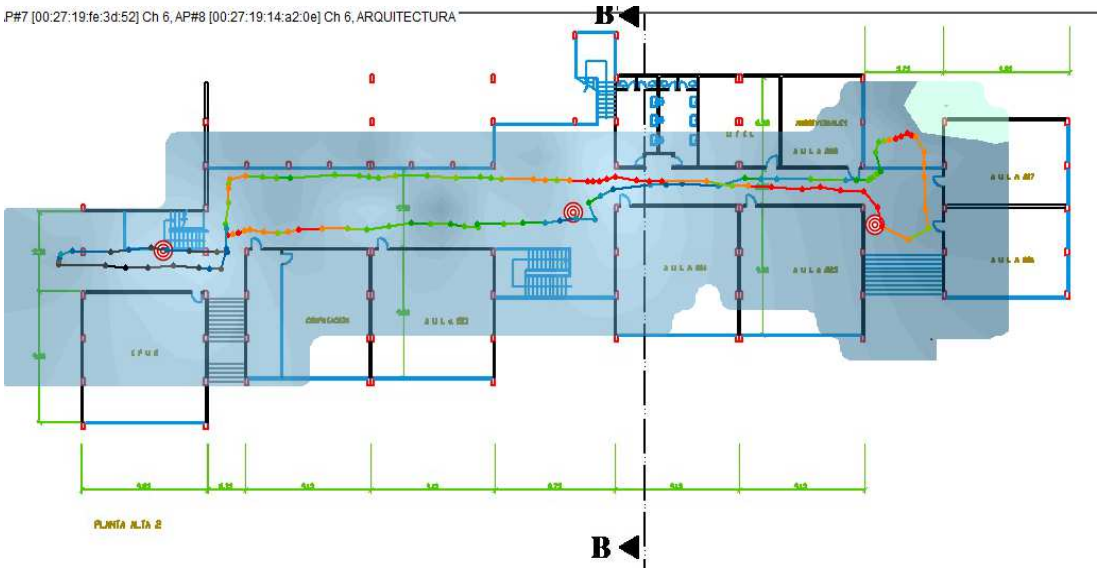


Figura 4.17 Segunda planta, Facultad Arquitectura UCSG

Fuente: Autores

Tercera Planta: En la figura 4.18 se muestra una cobertura aproximada del 80% del área total.

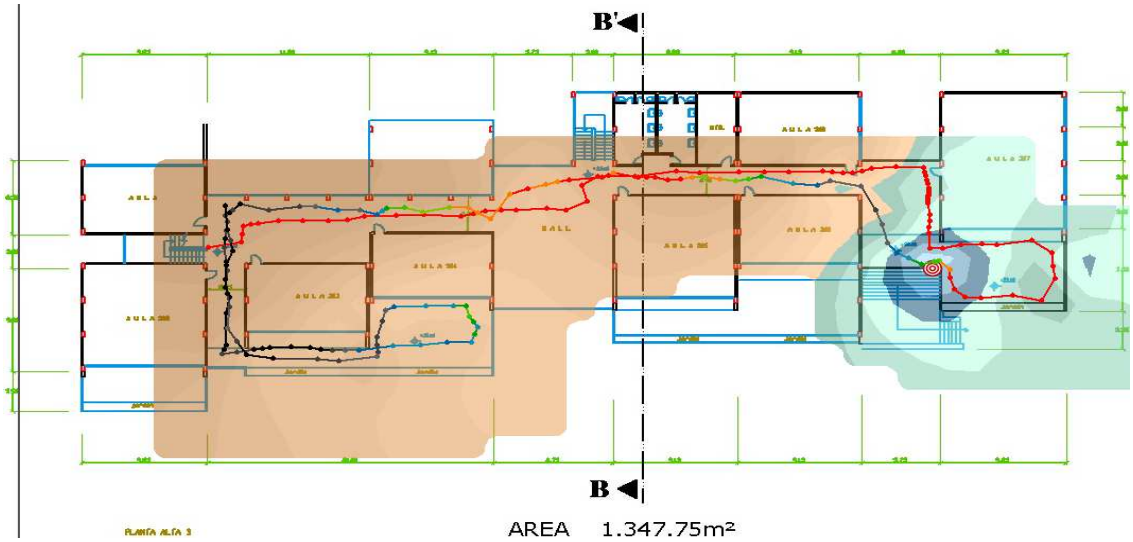


Figura 4.18 Tercera planta, Facultad Arquitectura UCSG

Fuente: Autores

Cuarta Planta: En la figura 4.19 se muestra una cobertura aproximada del 80% del área total.

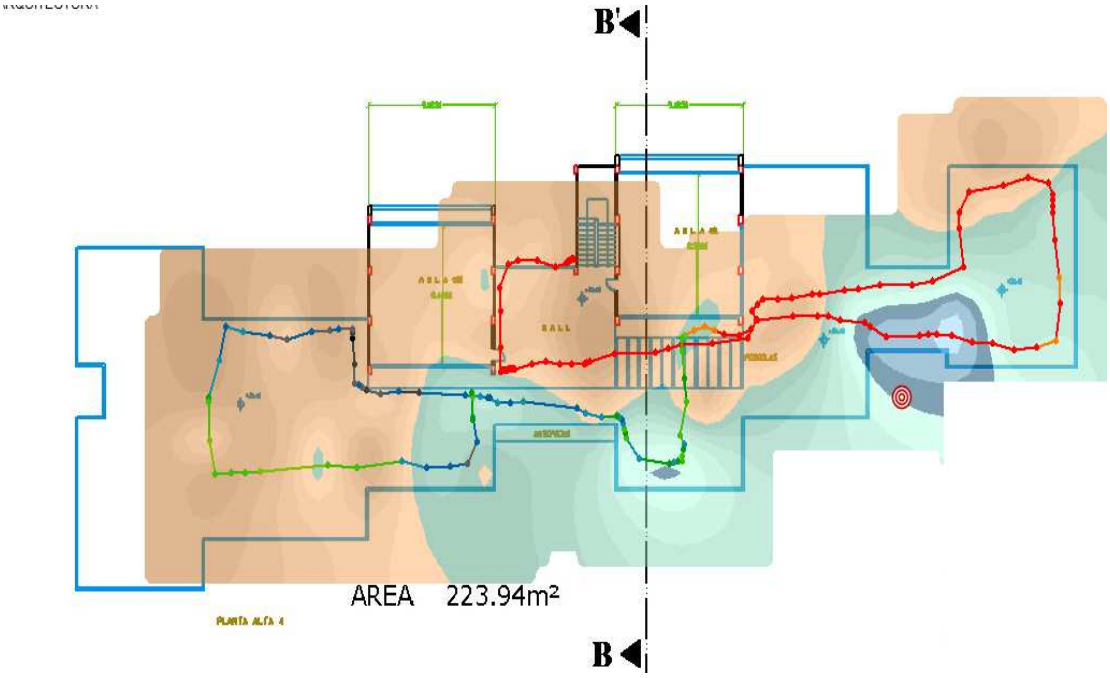


Figura 4.19 Cuarta planta, Facultad Arquitectura UCSG

Fuente: Autores

En el análisis de la red inalámbrica de esta Facultad, se encontró que existen equipos inalámbricos sin la adecuada configuración de SSID (*Service Set IDentifier*, Identificador de Servicio). Además se puede observar que no existe una asignación correcta de canales tal como se muestra en la figura 4.20.

SSID	AP#	Name	MAC	Ch	Security	Mode	Ave SNR	Max SNR	Min SNR	# Assoc Points	# Non-Assoc Points
	AP #7		00:27:19:fe:3d:52	Ch 6	Clear	Infra	51	75	14	0	122
	AP #8		00:27:19:14:a2:0e	Ch 6	Clear	Infra	34	72	12	0	111
	AP #9		00:90:4b:7e:e1:33	Ch 12	WEP	Ad hoc	14	21	12	0	88
	AP #16		00:27:19:fd:9f:a2	Ch 6	Clear	Infra	21	40	12	0	43
ARQUITECTURA	AP #15		00:27:19:fe:45:0a	Ch 6	Clear	Infra	24	46	12	0	77

Figura 4.20 Access Point encontrado, Facultad de Arquitectura UCSG

Fuente: Autores

Facultad Educación Técnica

Área Administrativa: En la figura 4.21 se muestra una cobertura aproximada del 50% del área total.

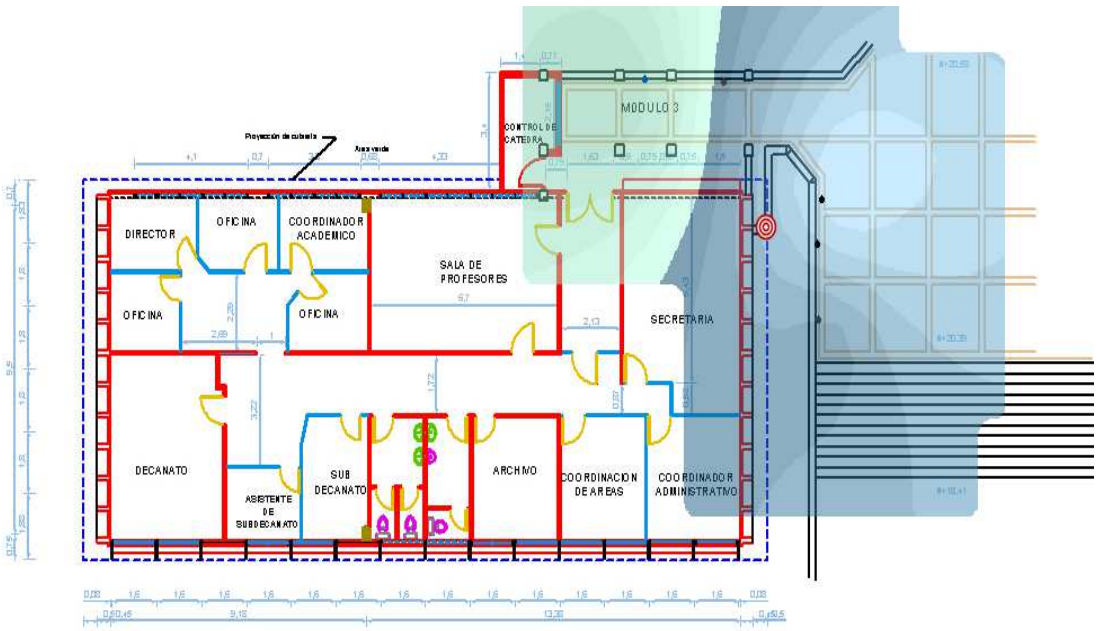


Figura 4.21 Administración, Facultad Educación Técnica UCSG

Fuente: Autores

Aulas de la Facultad Técnica: En la figura 4.22 se muestra una cobertura aproximada del 70% del área total.

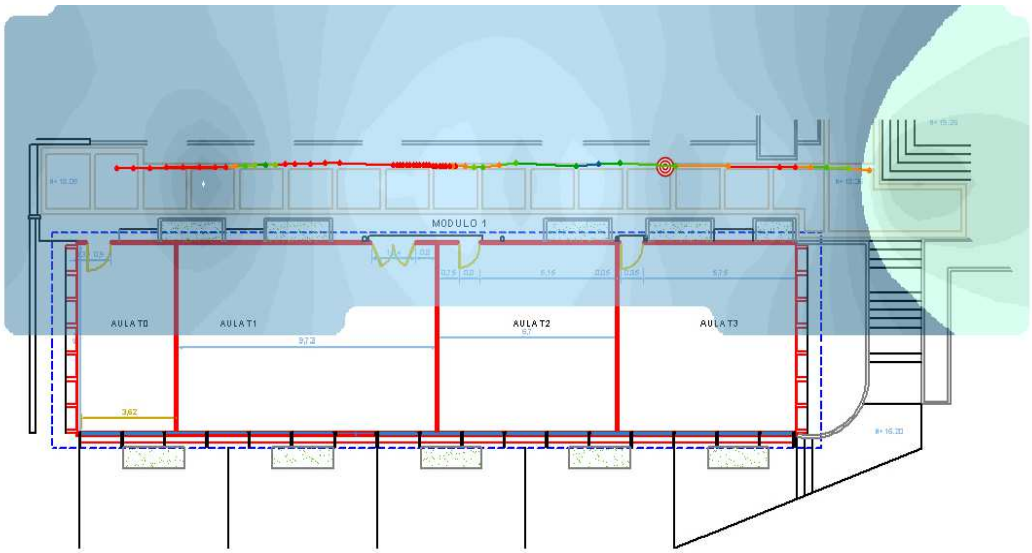


Figura 4.22 Aulas, Facultad Educación Técnica UCSG

Fuente: Autores

Laboratorios de Electricidad : En la figura 4.23 se muestra una cobertura aproximada del 80% del área total.

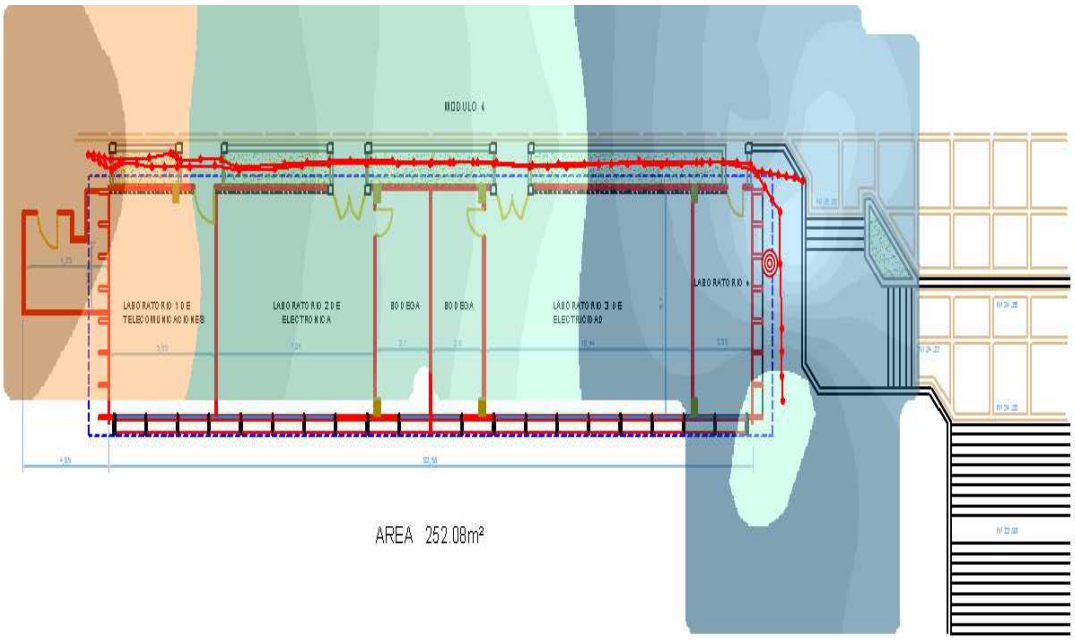


Figura 4.23Laboratorios de Electricidad, Facultad Educación Técnica UCSG

Fuente: Autores

Aulas de Facultad Técnica Planta Baja

En la figura 4.24 se muestra una cobertura aproximada del 50% del área total.

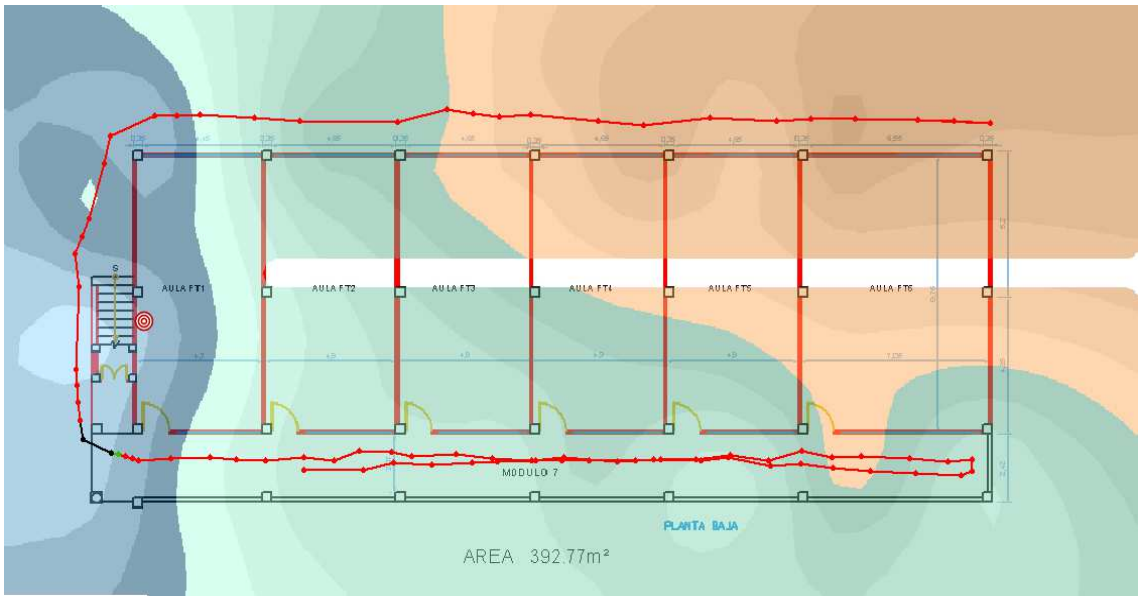


Figura 4.24 Aulas Planta Baja, Facultad Educación Técnica UCSG

Fuente: Autores

Aulas de Facultad Técnica Planta Alta

En la figura 4.25 se muestra una cobertura aproximada del 60% del área total.

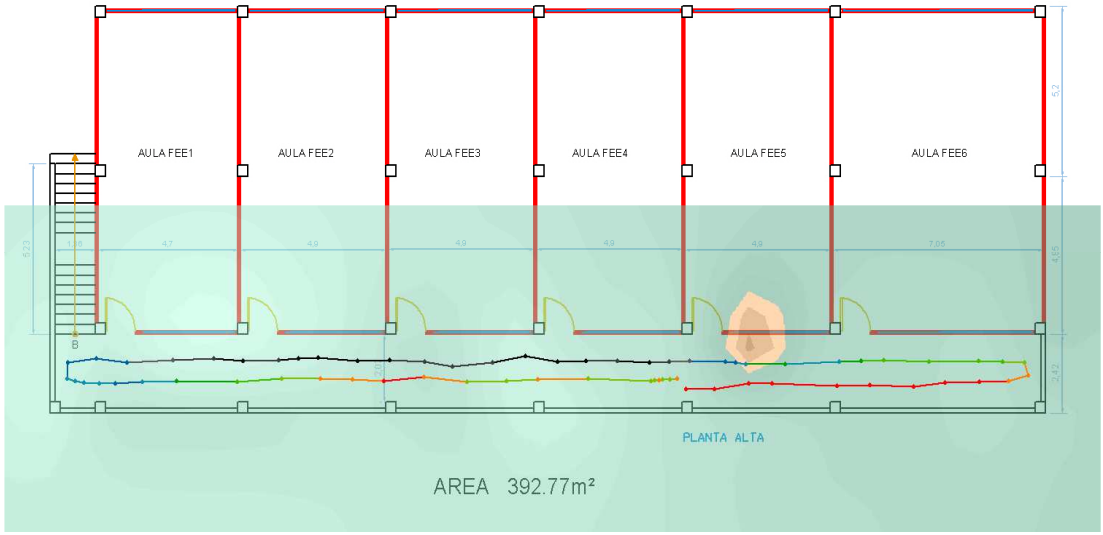


Figura 4.25 Aulas Planta Alta, Facultad Educación Técnica UCSG

Fuente: Autores

Laboratorios de computación de la Facultad Técnica: En la figura 4.26 se muestra una cobertura aproximada del 80% del área total.

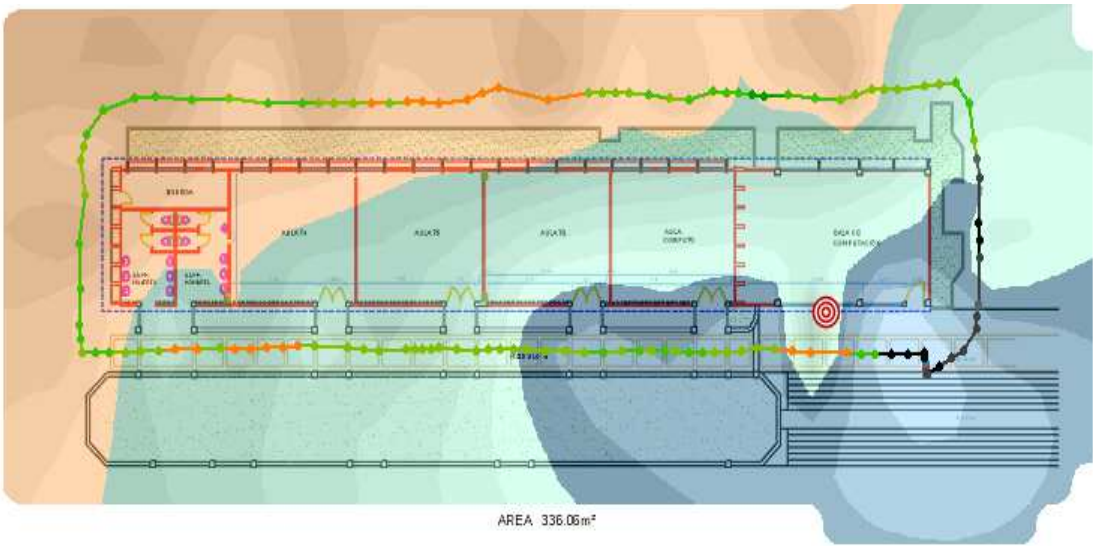


Figura 4.26 Laboratorios de computación, Facultad Educación Técnica UCSG

Fuente: Autores

Laboratorio de Computación: En la figura 4.27 se muestra una cobertura aproximada del 100% del área total.

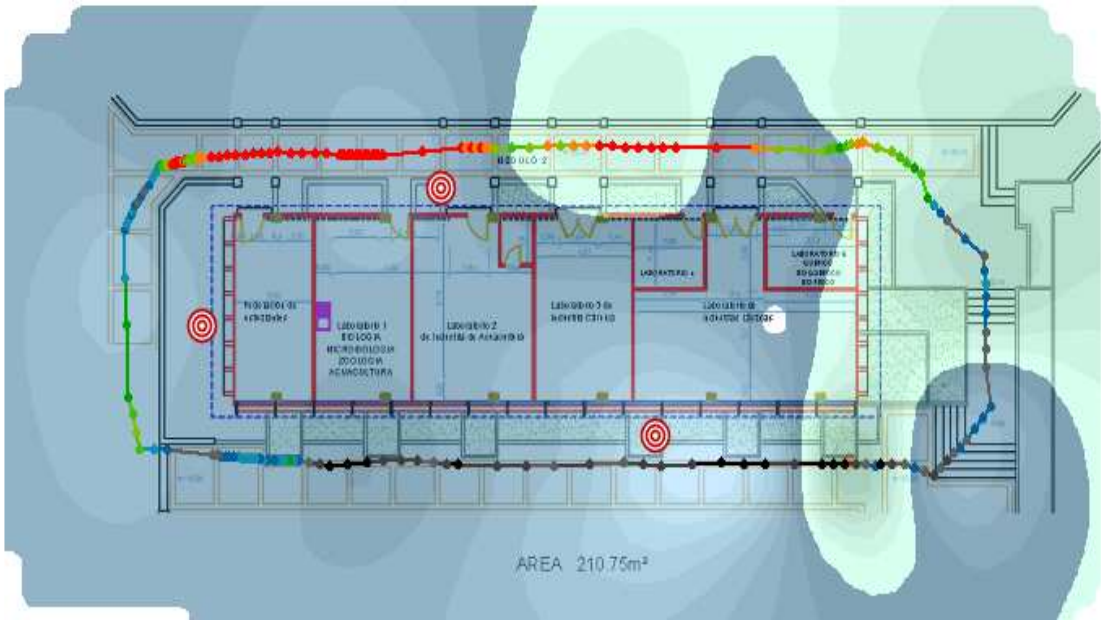


Figura 4.27 Laboratorios de computación, Facultad Educación Técnica UCSG

Fuente: Autores

El área de cobertura de esta facultad esta implementada con APs configurados en el canal 6, no existe mucha interferencia entre ellas porque están dispersos en diferentes edificios. Se muestra a continuación en la figura 4.28 el listado de equipos inalámbricos en el que se detallan las características principales de ellos.

SSID	AP#	Name	MAC	Ch	Security	Mode	Ave SNR	Max SNR	Min SNR	# Assoc Points	# Non-Assoc Points
parqueo_tecnica	AP #5		00:21:27:e5:fd:24	Ch 6	Clear	Infra	31	59	12	0	136
Tecnica 5	AP #6		00:23:cd:f9:10:41	Ch 6	Clear	Infra	24	40	12	0	147
Tecnica 6	AP #17		00:21:27:e6:08:78	Ch 6	Clear	Infra	31	69	11	0	92
Tecnica 7	AP #14		b0:48:7a:a0:8c:38	Ch 6	Clear	Infra	34	53	12	0	198
tecnica1	AP #4		b0:48:7a:a0:89:e0	Ch 4	Clear	Infra	36	60	13	0	226
tecnica2	AP #25		00:21:27:f2:32:52	Ch 6	Clear	Infra	29	52	12	0	139

Figura 4.28 Access Point encontrado, Facultad de Educación Técnica UCSG

Fuente: Autores

Clientes DHCP en *router* de la Facultad de Educación Técnica:

Firmware Version: 3.12.5 Build 100929 Rel.57776n

Hardware Version: WR941N v2/v3 00000000

A continuación en la tabla 4.3 se muestra la cantidad de clientes simultáneos de la Facultad técnica.

Tabla 4.3 Listado de dispositivos Conectados Facultad de Educación Técnica

Fuente: Autores

ID	ClientName	MAC Address	Assigned IP	Lease Time
1	UBNT	00-27-22-12-2C-F6	192.168.9.30	01:39:14
2	Mishelleblacio	00-F4-B9-41-87-AF	192.168.9.31	01:54:14
3	Unknown	D8-75-33-C8-7F-43	192.168.9.62	00:35:55
4	android-19336bb0605d63ce	88-30-8A-15-30-65	192.168.9.33	01:27:11
5	android_d25e718c89c0b26e	70-05-14-82-49-02	192.168.9.80	00:56:09

6	YCAZAs-iPod	BC-67-78-2F-26-F8	192.168.9.34	01:42:35
7	BLACKBERRY-0E55	14-74-11-02-44-DD	192.168.9.64	01:47:10
8	BLACKBERRY-5AA8	A0-6C-EC-13-5C-16	192.168.9.73	00:35:32
9	BLACKBERRY-6E7C	40-5F-BE-53-35-76	192.168.9.38	00:13:34
10	iPhone-de-lU	F0-DC-E2-DE-4A-EA	192.168.9.39	01:52:27
11	iPod-de-Juanjo	18-E7-F4-23-05-D0	192.168.9.40	00:40:09
12	DLB6031	00-15-E9-01-C1-E3	192.168.9.41	01:31:06
13	BLACKBERRY-6EAB	80-60-07-04-90-78	192.168.9.86	01:39:24
14	ipodccc	F0-B4-79-D8-15-91	192.168.9.43	00:38:30
15	Unknown	F8-7B-7A-15-89-7C	192.168.9.69	01:55:14
16	Unknown	28-37-37-C6-4C-A9	192.168.9.45	01:53:34
17	BLACKBERRY-2E2C	A0-6C-EC-77-A0-C4	192.168.9.46	01:49:55
18	iPod	00-26-BB-42-D7-76	192.168.9.47	00:27:33
19	Unknown	D0-C1-B1-C9-2A-15	192.168.9.35	00:04:55
20	Nica-Faggioni	90-27-E4-9D-DF-5A	192.168.9.36	01:42:39
21	Unknown	BC-B1-F3-0D-EE-DE	192.168.9.50	01:46:11
22	Unknown	D4-5D-42-54-B2-3F	192.168.9.37	00:54:55
23	Manuel	D0-23-DB-63-6F-EA	192.168.9.52	00:29:41
24	BLACKBERRY-8B60	14-74-11-69-83-29	192.168.9.53	01:47:15
25	iPad	1C-AB-A7-0D-A4-4D	192.168.9.66	00:08:24
26	BLACKBERRY-C663	40-6A-AB-DF-CF-C8	192.168.9.42	01:59:50
27	BLACKBERRY-75AF	14-74-11-15-F7-BF	192.168.9.56	01:23:09
28	Unknown	A8-E0-18-29-52-B1	192.168.9.57	01:45:32
29	BLACKBERRY-EB88	40-6A-AB-DA-89-D5	192.168.9.65	01:01:23
30	BLACKBERRY-F715	80-60-07-36-95-99	192.168.9.44	00:03:57
31	BLACKBERRY-6A3D	40-5F-BE-BA-E6-62	192.168.9.61	01:04:38
32	Unknown	D4-87-D8-EE-8F-C1	192.168.9.74	01:13:02

33	IPOD-JUANJO	60-FB-42-3D-B1-16	192.168.9.70	00:14:36
34	BLACKBERRY-A5E2	E8-3E-B6-DE-08-19	192.168.9.48	00:01:04
35	Unknown	B0-5C-E5-10-AC-53	192.168.9.67	00:43:50
36	BLACKBERRY-339D	30-7C-30-2E-08-1E	192.168.9.49	00:57:22
37	Unknown	D4-C1-FC-D9-F3-ED	192.168.9.51	01:59:20
38	BLACKBERRY-F0EB	A8-6A-6F-2D-54-9A	192.168.9.71	01:36:10
39	JuanDo	44-D8-84-37-AF-26	192.168.9.32	00:10:50
40	Unknown	F0-E7-7E-0B-AF-B5	192.168.9.72	00:11:20
41	iPhone	C0-9F-42-C6-31-A1	192.168.9.77	00:56:01
42	Karlitas-iPod	70-73-CB-53-94-2F	192.168.9.75	01:50:52
43	android-6bdd7d7f5d6c4b95	5C-0A-5B-C6-A9-9A	192.168.9.78	00:29:00
44	BLACKBERRY-F8BF	40-6A-AB-A1-AA-FB	192.168.9.55	00:43:06
45	Unknown	B0-EC-71-3F-CE-EE	192.168.9.58	01:34:46
46	BLACKBERRY-8327	40-6A-AB-4C-43-BA	192.168.9.59	00:14:13
47	HENRY	C0-9F-42-B7-E1-33	192.168.9.76	01:17:18
48	android-cd51d920d4b05a9f	18-87-96-50-D0-9E	192.168.9.79	00:58:39
49	iPhone-4	48-60-BC-E1-14-7D	192.168.9.68	00:20:40
50	FernanPalacios	70-F3-95-B4-C7-0D	192.168.9.82	00:41:12
51	BLACKBERRY-42F6	40-6A-AB-D6-44-F6	192.168.9.81	00:35:53
52	BLACKBERRY-BF7A	70-AA-B2-A8-19-E5	192.168.9.83	01:46:12
53	Unknown	7C-C5-37-C6-5F-B8	192.168.9.87	00:58:06
54	iCrisss-iPhone	CC-08-E0-56-D4-7C	192.168.9.89	00:44:17
55	Unknown	E8-06-88-50-8B-D9	192.168.9.84	00:17:28
56	BLACKBERRY-8DD7	2C-A8-35-C1-84-77	192.168.9.85	00:17:52
57	BLACKBERRY-0E4E	40-5F-BE-60-29-D0	192.168.9.92	00:19:50
58	BLACKBERRY-4C52	40-5F-BE-A3-98-C4	192.168.9.93	01:44:17
59	BLACKBERRY-77A9	A0-6C-EC-8A-F6-96	192.168.9.94	01:33:40

60	Unknown	04-5A-95-41-2E-DF	192.168.9.95	00:32:54
61	android-530af684b645198f	14-7D-C5-25-CF-BF	192.168.9.96	00:32:29
62	Edwin-Ipod	00-C6-10-A8-C7-3F	192.168.9.97	00:35:11
63	Unknown	9C-4A-7B-40-F3-14	192.168.9.99	01:42:57

Facultad de Filosofía:

Planta Baja: En la figura 4.29 se muestra una cobertura aproximada del 60% del área total.

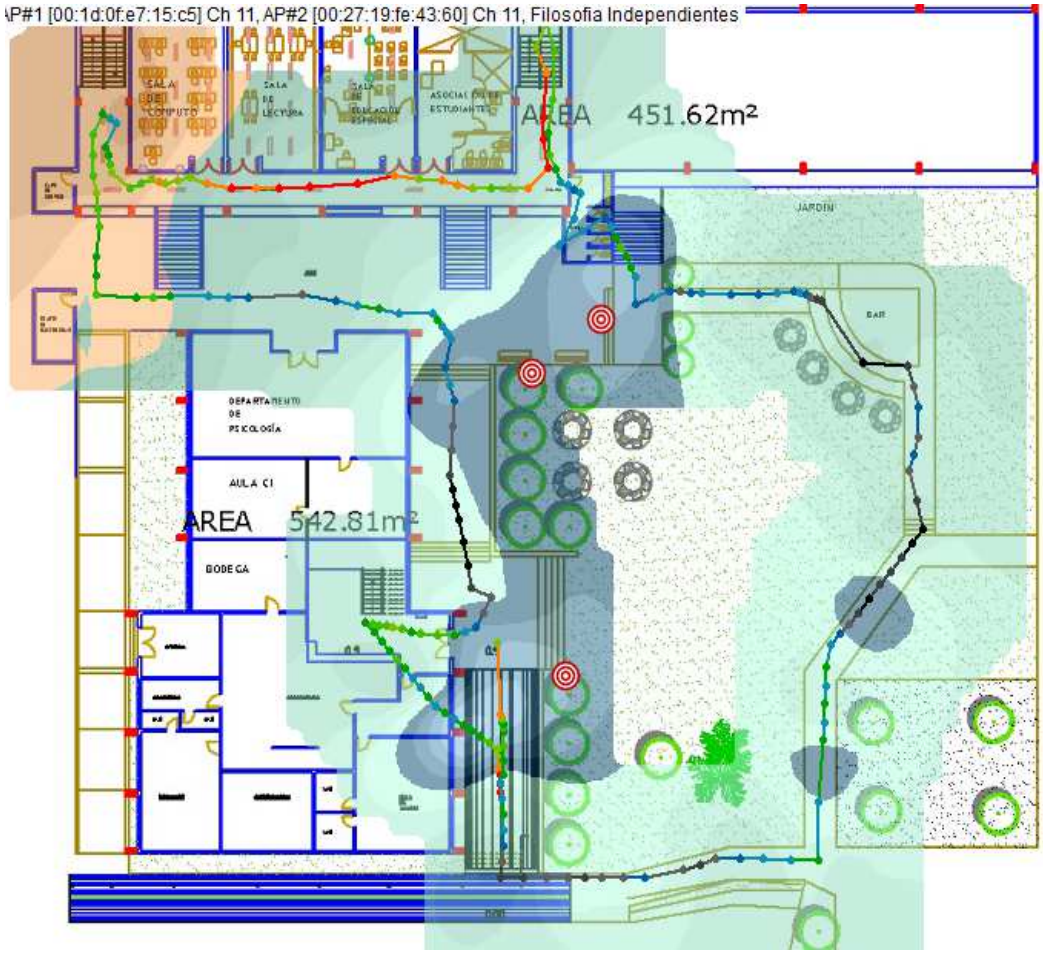


Figura 4.29 Planta baja, Facultad Filosofía UCSG

Fuente: Autores

Primera planta: En la figura 4.30 se muestra una cobertura aproximada del 30% del área total.

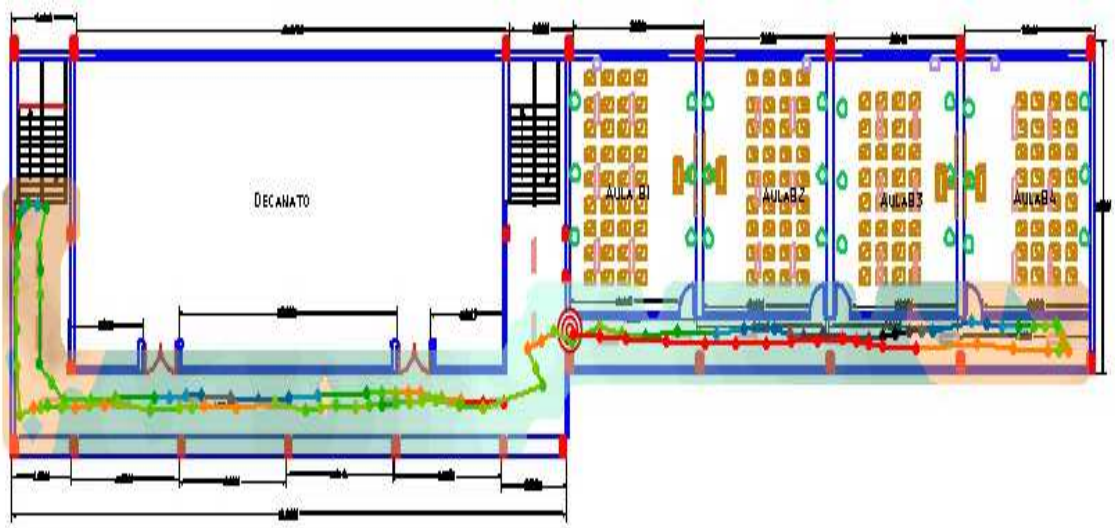


Figura 4.30 Primera planta, Facultad Filosofía UCSG

Fuente: Autores

Segunda planta: En la figura 4.31 se muestra una cobertura aproximada del 30% del área total.

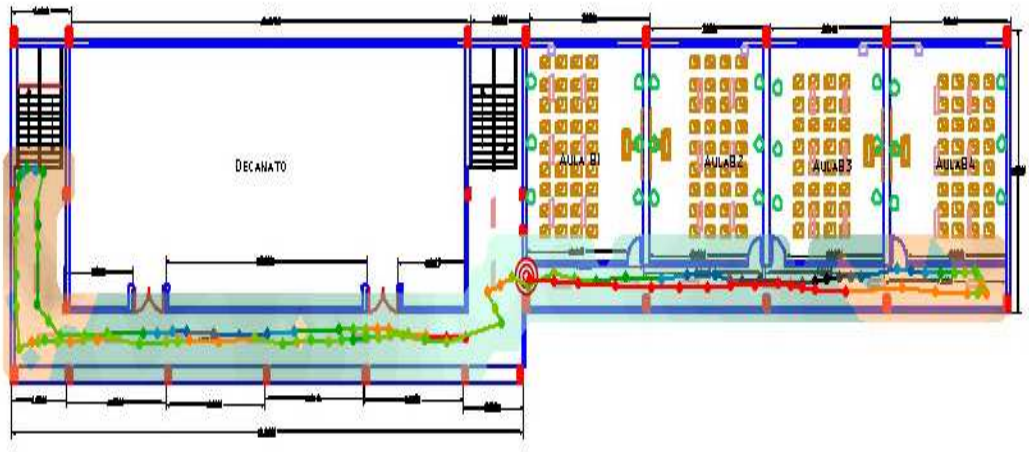


Figura 4.31 Segunda planta, Facultad Filosofía UCSG

Fuente: Autores

Tercera Planta: En la figura 4.32 se muestra una cobertura aproximada del 60% del área total.

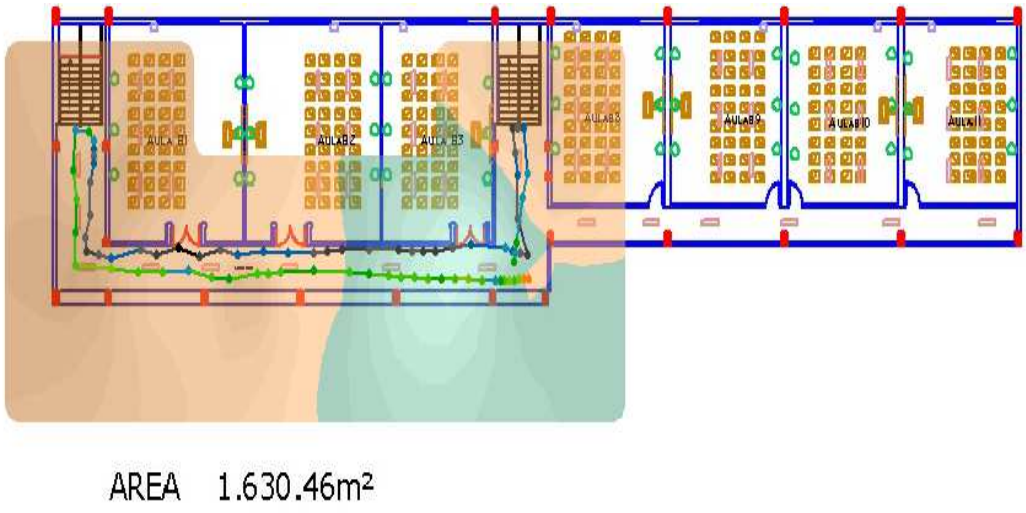


Figura 4.32 Tercera planta, Facultad Filosofía UCSG

Fuente: Autores

Esta Facultad tiene poca cobertura en sus instalaciones, se observa áreas en las que hay la mínima señal para una conexión satisfactoria. Se debe realizar una mejora en la disposición de los equipos y una configuración correcta de los canales como se muestra en la figura 4.33.

SSID	AP#	Name	MAC	Ch	Security	Mode	Ave SNR	Max SNR	Min SNR	# Assoc Points	# Non-Assoc Points
FILOSOFIA	AP #3		00:1d:0f:e7:15:c5	Ch 11	Clear	Infra	23	42	14	0	41
FILOSOFIA	AP #5		00:27:19:fe:43:60	Ch 11	Clear	Infra	24	34	16	0	28
FILOSOFIA	AP #6		00:21:27:f2:30:c4	Ch 11	Clear	Infra	30	54	14	0	65
FILOSOFIA	AP #20		00:27:19:fe:43:60	Ch 0	Clear	Infra	22	35	15	0	48
Filosofia Independientes	AP #4		00:23:cd:da:f5:8e	Ch 11	Clear	Infra	21	30	12	0	30

Figura 4.33 Access Point encontrado, Facultad Filosofía UCSG

Fuente: Autores

En la tabla 4.4 se muestra el listado de clientes inalámbricos promedio conectados en la facultad de filosofía

Firmware Versión: 3.9.13 Build 090930 Rel.51043n

Hardware Versión: WR1043N v1 00000000

Tabla 4.4 Listado de dispositivos Conectados Facultad de Filosofía

Fuente: Autores

ID	ClientName	MAC Address	Assigned IP	Lease Time
1	BLACKBERRY-6080	3C-74-37-85-A1-E9	192.168.1.122	01:36:59
2	Anita-Cesa	7C-D1-C3-40-95-04	192.168.1.106	00:39:12
3	BLACKBERRY-A89B	70-D4-F2-24-DF-5B	192.168.1.101	01:39:17
4	iPad-de-mac	C4-2C-03-DC-93-35	192.168.1.165	01:48:18
5	BLACKBERRY-6562	F4-0B-93-C3-A3-3B	192.168.1.103	01:58:55
6	Princesa	10-9A-DD-08-79-F0	192.168.1.169	01:52:38
7	android_6080b79ed7d542f9	00-23-76-D8-CD-AA	192.168.1.178	00:45:42
8	Unknown	F8-D0-BD-66-1A-CA	192.168.1.138	00:20:43
9	Sanalepinlla	88-C6-63-85-B7-6F	192.168.1.105	00:32:57
10	Unknown	00-07-AB-09-F2-34	192.168.1.115	00:30:23
11	iPhone	44-D8-84-0E-35-8F	192.168.1.116	01:46:48
12	android_6da57dac6390f610	90-C1-15-EF-D5-79	192.168.1.123	01:44:35
13	PcArq20	00-1F-3C-6D-C5-5A	192.168.1.114	01:22:48
14	Unknown	04-FE-31-2F-90-FC	192.168.1.100	01:32:49
15	PINEJO	00-26-4A-47-EF-B7	192.168.1.155	01:52:12
16	Unknown	00-21-19-DE-07-B1	192.168.1.102	00:03:37
17	android-6f4dc1a86108c265	38-AA-3C-42-DF-10	192.168.1.192	01:13:39
18	BLACKBERRY-F9F7	1C-69-A5-09-D8-D9	192.168.1.119	01:42:37
19	Unknown	78-CA-04-34-91-FF	192.168.1.104	01:51:17
20	PC-PC	78-E4-00-73-75-1A	192.168.1.112	01:59:05
21	Users-iPhone	00-26-B0-AB-12-53	192.168.1.159	01:08:50

22	Unknown	14-7D-C5-2F-0B-0D	192.168.1.124	01:07:08
23	BLACKBERRY-C88D	70-AA-B2-21-0E-D7	192.168.1.125	00:34:53
24	Blondi	BC-67-78-2D-90-94	192.168.1.110	00:55:23
25	BLACKBERRY-3139	70-AA-B2-9A-5F-51	192.168.1.132	01:52:57
26	BLACKBERRY-0963	40-6A-AB-B2-58-EC	192.168.1.190	01:12:49
27	Unknown	68-09-27-8F-74-B7	192.168.1.117	01:49:00
28	Unknown	0C-77-1A-13-2A-27	192.168.1.113	01:58:37
29	Unknown	F4-8E-09-43-68-6D	192.168.1.118	00:36:53
30	Unknown	94-51-03-FB-C7-1B	192.168.1.135	00:38:06
31	iPod-de-Pedrow	70-73-CB-71-DD-7F	192.168.1.136	00:17:54
32	Oscar	24-AB-81-F5-D6-8C	192.168.1.137	01:04:50
33	Unknown	9C-4A-7B-DB-91-73	192.168.1.139	00:03:55
34	Unknown	00-23-B4-EB-BB-5C	192.168.1.140	01:41:20
35	BLACKBERRY-EA78	3C-74-37-AD-9F-BE	192.168.1.129	01:04:53
36	BLACKBERRY-17F2	E8-3E-B6-9D-7C-67	192.168.1.121	01:45:32
37	Hp	D0-DF-9A-0B-91-D9	192.168.1.130	01:51:30
38	BLACKBERRY-7D8A	14-74-11-00-35-74	192.168.1.146	00:32:27
39	BLACKBERRY-86AE	14-74-11-10-EC-8B	192.168.1.147	00:23:35
40	Kathy	00-F4-B9-41-5F-F6	192.168.1.134	01:52:12
41	android-780724fb049c1b6d	BC-85-1F-ED-98-12	192.168.1.126	01:30:05
42	Unknown	A8-E0-18-41-F7-A5	192.168.1.131	01:09:08
43	Unknown	D4-87-D8-EE-8F-6F	192.168.1.150	01:42:11
44	PcArq16	00-1F-3C-03-77-21	192.168.1.152	01:37:01
45	Unknown	10-40-F3-A6-02-84	192.168.1.153	01:13:31
46	MYPC	C4-17-FE-20-16-91	192.168.1.166	01:00:37
47	BLACKBERRY-563A	E8-3E-B6-3E-DE-14	192.168.1.144	01:06:59
48	Jorge-Rendon-J	00-21-E9-37-2D-6F	192.168.1.156	00:36:54

49	Unknown	7C-D1-C3-42-0F-B7	192.168.1.157	00:37:00
50	Unknown	78-CA-39-8F-8E-6C	192.168.1.184	01:44:35
51	josue	7C-D1-C3-45-4E-76	192.168.1.142	00:19:55
52	Sebas	40-A6-D9-41-D3-5A	192.168.1.161	01:56:41
53	BLACKBERRY-8F6F	30-69-4B-AA-53-E1	192.168.1.162	00:28:08
54	Unknown	2C-D2-E7-52-DA-2B	192.168.1.177	01:58:29
55	BLACKBERRY-6DE5	A8-6A-6F-1D-3E-F0	192.168.1.164	00:51:26
56	Unknown	E4-CE-8F-29-03-0E	192.168.1.151	01:07:26
57	BLACKBERRY-1CE0	30-69-4B-3A-C4-1E	192.168.1.168	00:50:13
58	BLACKBERRY-8D98	40-6A-AB-EC-27-0A	192.168.1.133	01:59:49
59	BLACKBERRY-9606	F4-0B-93-6A-39-BA	192.168.1.163	01:27:41
60	BLACKBERRY-EDB8	30-69-4B-A0-A8-73	192.168.1.167	01:51:18
61	BLACKBERRY-FAA6	70-D4-F2-4C-41-C6	192.168.1.173	01:02:16
62	BLACKBERRY-64C4	80-60-07-13-93-5B	192.168.1.149	01:14:23
63	BLACKBERRY-8355	CC-55-AD-DB-C8-99	192.168.1.174	00:56:40
64	android-2c9b79055f4c4032	00-37-6D-BF-88-26	192.168.1.170	01:10:14
65	Unknown	94-63-D1-80-1B-E3	192.168.1.175	01:13:15
66	android_81564ac1cad44a5e	84-00-D2-4F-FA-3A	192.168.1.127	01:48:40
67	MaJoo	F0-DC-E2-40-A6-C5	192.168.1.182	01:24:31
68	BLACKBERRY-26A1	3C-74-37-9C-B4-15	192.168.1.195	01:41:43
69	Ivan-Zuniga	00-F4-B9-D5-35-F1	192.168.1.172	01:11:10
70	Unknown	94-20-53-85-77-54	192.168.1.108	01:57:30
71	Unknown	98-D6-BB-DE-4E-65	192.168.1.176	01:12:04
72	Estefy	AC-81-12-46-27-E2	192.168.1.111	01:57:04
73	BLACKBERRY-AF9A	A8-6A-6F-C4-12-2A	192.168.1.171	01:23:40
74	Gabriela-PC	C4-17-FE-B1-52-3E	192.168.1.194	01:24:18
75	BLACKBERRY-AE99	30-69-4B-FE-72-DC	192.168.1.181	01:22:07

76	BLACKBERRY-73CA	80-60-07-CA-77-69	192.168.1.188	00:52:25
77	BLACKBERRY-59BF	14-74-11-50-2E-16	192.168.1.183	01:15:32
78	BLACKBERRY-E27D	A0-6C-EC-7D-26-ED	192.168.1.185	01:36:40
79	MININT-HU5PGOJ	8C-A9-82-84-2D-F2	192.168.1.193	01:03:05
80	Unknown	0C-74-C2-51-43-41	192.168.1.179	00:56:43
81	Unknown	50-CC-F8-A3-30-01	192.168.1.196	00:05:06
82	user-HP	D0-DF-9A-0D-7E-3C	192.168.1.197	01:23:25
83	Unknown	70-DE-E2-3F-56-76	192.168.1.186	01:46:47
84	Android_359637031604743	90-21-55-E2-7C-5F	192.168.1.154	01:46:39

Facultad de Ingeniería

Planta Baja: En la figura 4.34 se muestra una cobertura aproximada del 60% del área total.

Figura 4.34 Planta Baja, Facultad de Ingeniería UCSG

Fuente: Autores

Segunda Planta: En la figura 4.35 se muestra una cobertura aproximada del 60% del área total.

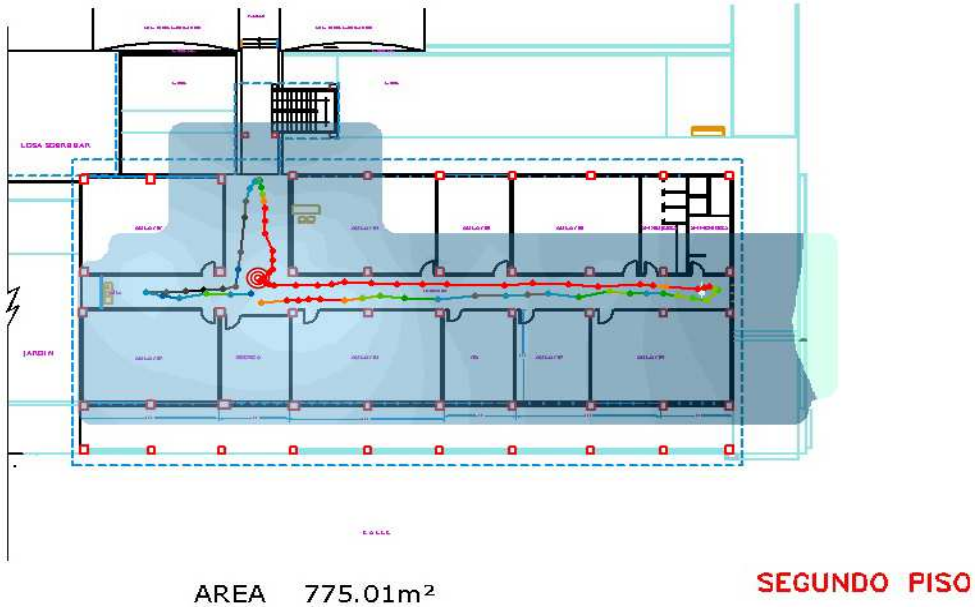


Figura 4.35 Segunda planta, Facultad de Ingeniería UCSG

Fuente: Autores

Tercera Planta: En la figura 4.36 se muestra una cobertura aproximada del 70% del área total.

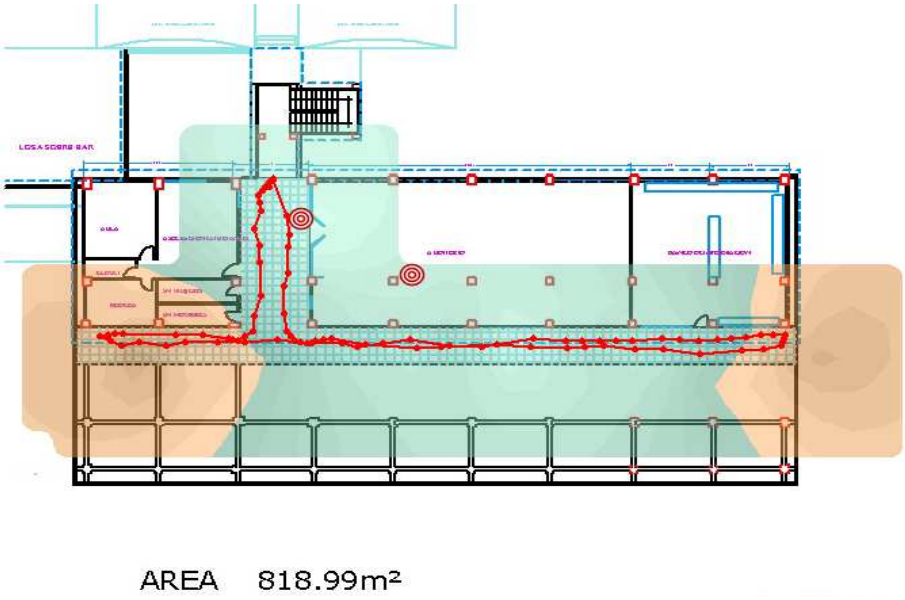


Figura 4.36 Planta Baja, Facultad de Ingeniería UCSG

Fuente: Autores

Edificio Nuevo Primera Planta: En la figura 4.37 se muestra una cobertura aproximada del 50% del área total.

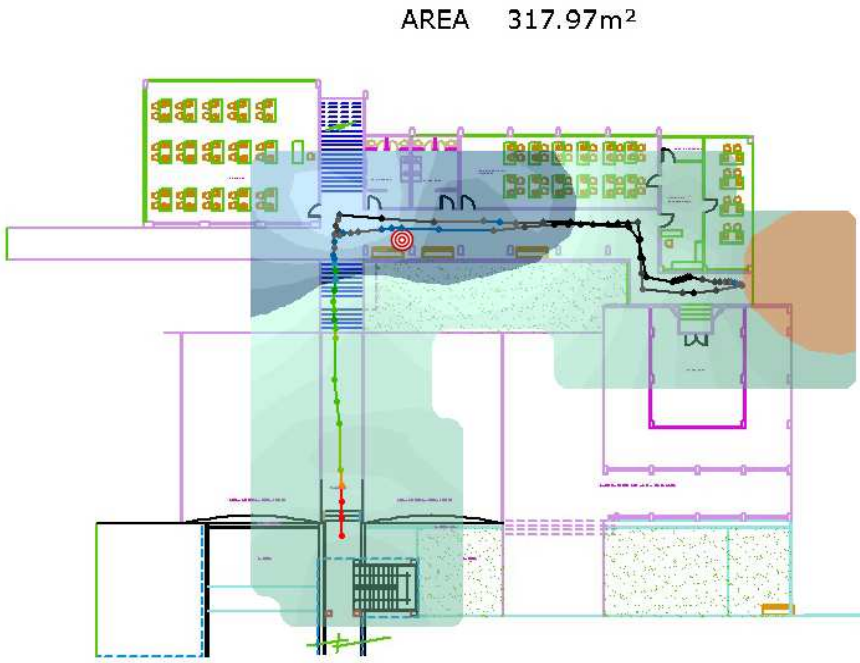


Figura 4.37 Edificio Nuevo Primera planta, Facultad de Ingeniería UCSG

Fuente: Autores

Edificio Nuevo Segunda Planta: En la figura 4.38 se muestra una cobertura aproximada del 60% del área total.

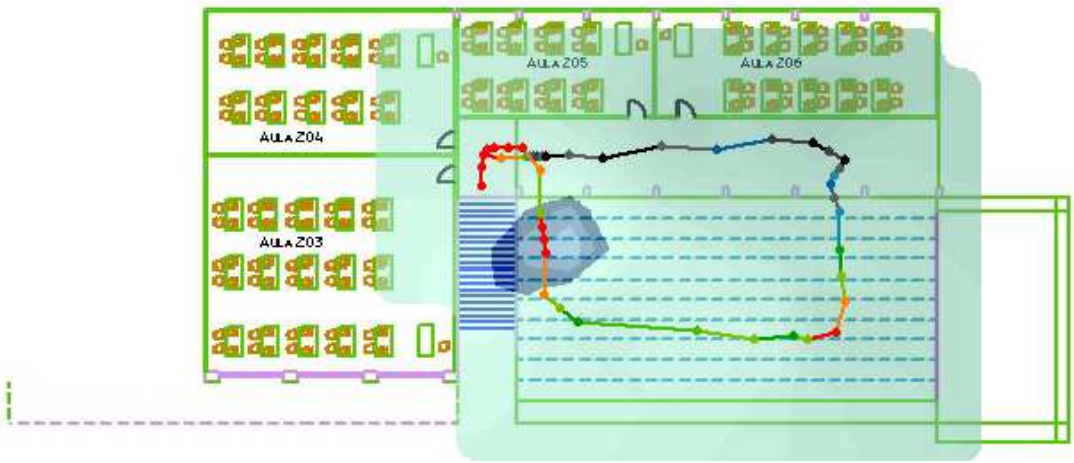


Figura 4.38 Edificio Nuevo Segunda Planta, Facultad de Ingeniería UCSG

Fuente: Autores

Se encontró en esta Facultad que la señal en el tercer piso es sumamente baja, es necesario asignar equipos en mejor disposición física y cantidad. La configuración de canales en los equipos inalámbricos es correcta, se muestra a continuación el listado de equipos inalámbricos encontrados en la facultad en la figura 4.39.

SSID	AP#	Name	MAC	Ch	Security	Mode	Ave SNR	Max SNR	Min SNR	# Assoc Points	# Non-Assoc Points
WiFiING04	AP #5		00:23:cd:da:f2:f8	Ch 6	Clear	Infra	47	62	30	0	43
WIFIING01	AP #1		00:25:9c:52:1e:e0	Ch 11	Clear	Infra	21	27	14	0	42
CIDT	AP #3		00:25:9c:52:24:96	Ch 1	Clear	Infra	17	32	12	0	38
WiFiING02	AP #6		00:23:cd:f9:11:0d	Ch 6	Clear	Infra	16	25	12	0	22

Figura 4.39 Access Point encontrado, Facultad Ingeniería UCSG

Fuente: Autores

En la tabla 4.5 se muestra el listado de conexiones encontradas en el *router* inalámbrico de la Facultad:

Tabla 4.5 Listado de dispositivos Conectados Facultad de Ingeniería

Fuente: Autores

ClientName	**Interface**	**IP Address**	**MAC Address**	**Expires Time**	
	LAN	10.10.10.4	A8:7B:39:F3:4F:9A	07:42:53	
Gabbys-IPod	LAN	10.10.10.6	B8:C7:5D:82:52:72	22:40:16	
BLACKBERRY-8683	LAN	10.10.10.15	80:60:07:95:53:2F	07:22:35	
	LAN	10.10.10.16	78:CA:04:BD:A0:BB	23:50:53	
Fredy-G	LAN	10.10.10.25	88:C6:63:79:BD:28	04:25:56	
BLACKBERRY-B8BE	LAN	10.10.10.33	CC:55:AD:98:FE:B5	20:57:48	
PERSONAL	LAN	10.10.10.38	5C:AC:4C:90:9B:06	03:16:43	
	LAN	10.10.10.41	D0:C1:B1:C9:21:F1	06:12:49	

	LAN	10.10.10.44	9C:02:98:5E:01:4E	23:34:37	
Álvaro-PC	LAN	10.10.10.48	68:A3:C4:B4:F6:9F	21:22:42	
	LAN	10.10.10.49	B8:D9:CE:22:EF:B3	07:21:42	
tetel	LAN	10.10.10.52	BC:67:78:15:63:AE	00:24:05	
BLACKBERRY-B575	LAN	10.10.10.54	E8:3E:B6:5A:66:D1	00:25:14	
claro-PC	LAN	10.10.10.55	E0:CA:94:94:CB:DF	03:12:18	
	LAN	10.10.10.56	18:46:17:32:06:C9	22:38:48	
android_9f9c9ce83650f9f0	LAN	10.10.10.57	40:4D:8E:C0:E3:C8	05:27:20	
JULIO	LAN	10.10.10.58	04:1E:64:11:8C:6D	05:59:11	
BLACKBERRY-87CE	LAN	10.10.10.59	A0:6C:EC:60:35:07	05:59:50	
android-e084d95720cb950f	LAN	10.10.10.61	5C:0A:5B:C8:E2:1D	06:13:45	
BLACKBERRY-A563	LAN	10.10.10.62	14:74:11:21:F2:8C	20:56:34	
	LAN	10.10.10.63	CC:05:1B:53:B4:98	20:08:43	
	LAN	10.10.10.65	50:CC:F8:A3:30:01	22:31:19	
BLACKBERRY-D4E6	LAN	10.10.10.66	2C:A8:35:3F:37:F8	23:14:59	
PC-PC	Wireless	10.10.10.67	78:E4:00:73:75:1A	23:57:22	

Facultad de Especialidades Empresariales

Planta Baja: En la figura 4.40 se muestra una cobertura aproximada del 80% del área total.

Figura 4.40, Planta Baja, Facultad Especialidades Empresarial UCSG

Fuente: Autores

Primera planta: En la figura 4.41 se muestra una cobertura aproximada del 80% del área total.

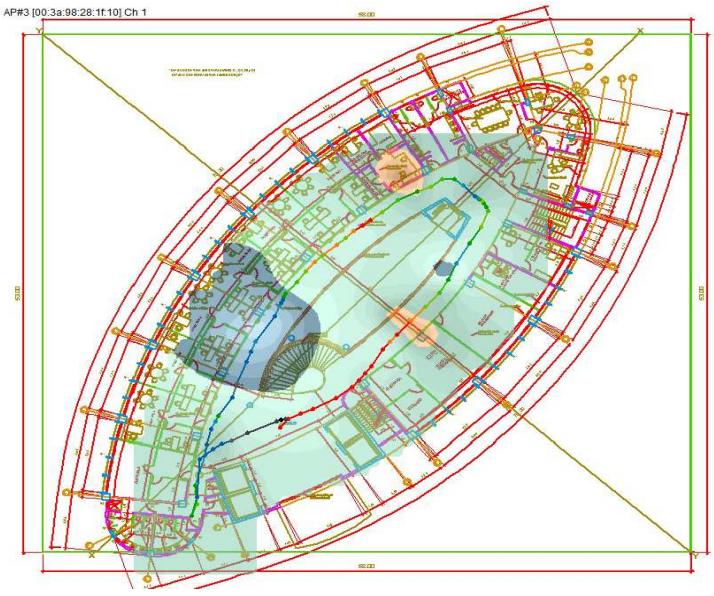


Figura 4.41, Primera planta, Facultad Especialidades Empresarial UCSG

Fuente: Autores

Segunda planta: En la figura 4.42 se muestra una cobertura aproximada del 80% del área total.

Figura 4.42, Segunda planta, Facultad Especialidades Empresarial UCSG

Fuente: Autores

Tercera planta: En la figura 4.43 se muestra una cobertura aproximada del 80% del área total.

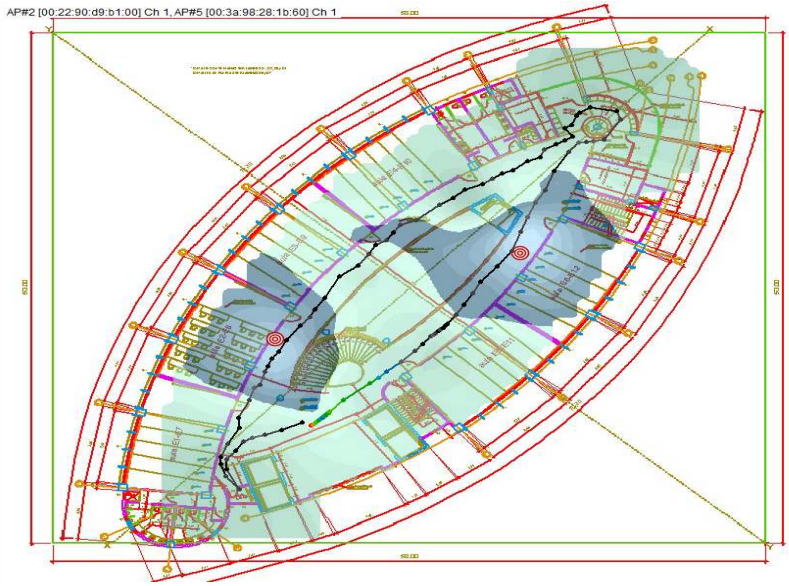


Figura 4.43, Tercera planta, Facultad Especialidades Empresarial UCSG

Fuente: Autores

Cuarta planta: En la figura 4.44 se muestra una cobertura aproximada del 80% del área total.

Figura 4.44, Cuarta planta, Facultad Especialidades Empresarial UCSG

Fuente: Autores

Quinta planta: En la figura 4.45 se muestra una cobertura aproximada del 80% del área total.

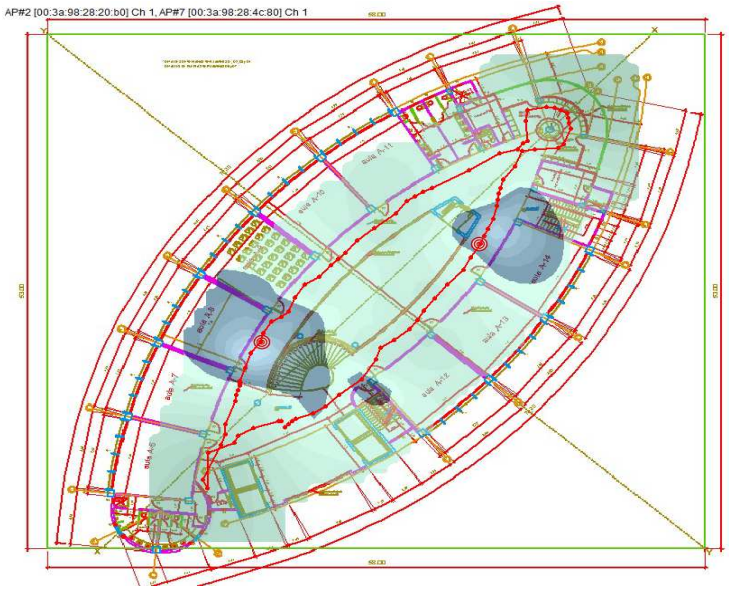


Figura 4.45, Quinta planta, Facultad Especialidades Empresarial UCSG

Fuente: Autores

Sexta planta: En la figura 4.46 se muestra una cobertura aproximada del 80% del área total.

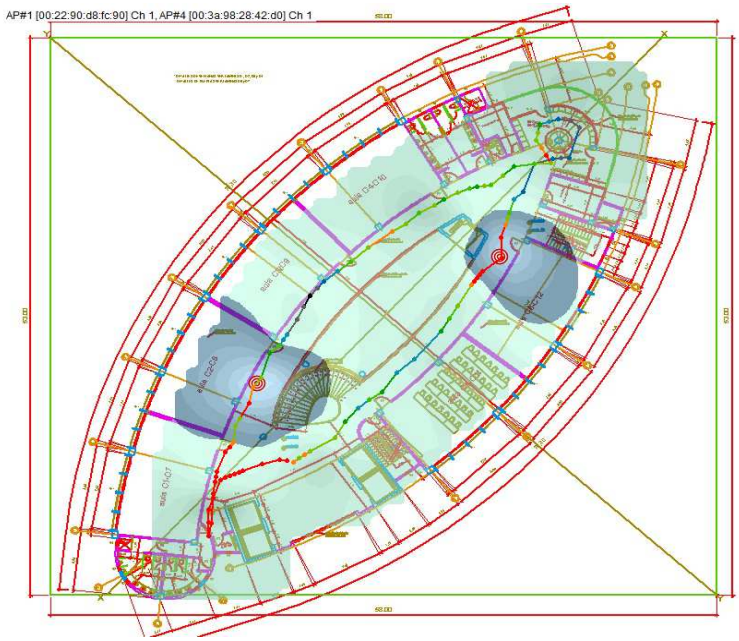


Figura 4.46, Sexta planta, Facultad Especialidades Empresarial UCSG

Fuente: Autores

Septima planta: En la figura 4.47 se muestra una cobertura aproximada del 80% del área total.

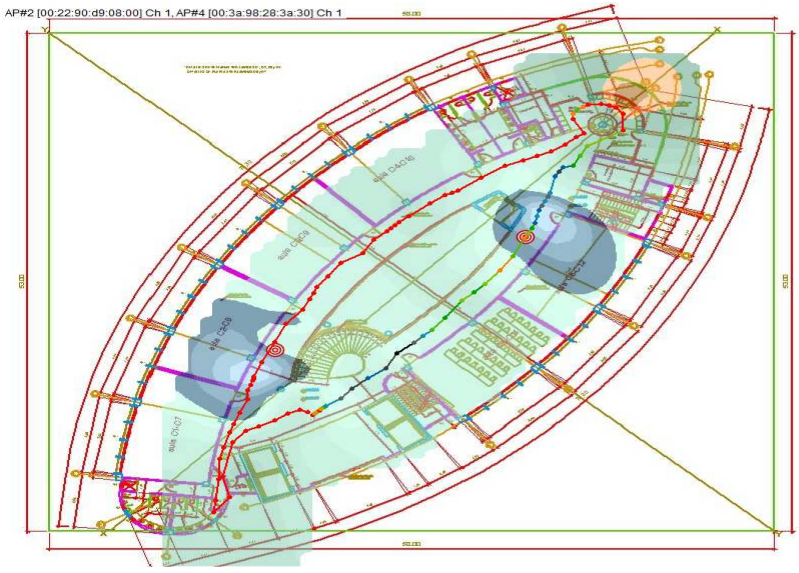


Figura 4.47, Septima planta, Facultad Especialidades Empresarial UCSG

Fuente: Autores

Octava planta: En la figura 4.48 se muestra una cobertura aproximada del 80% del área total.

Figura 4.48, Octava planta, Facultad Especialidades Empresarial UCSG

Fuente: Autores

Novena planta: En la figura 4.49 se muestra una cobertura aproximada del 80% del área total.

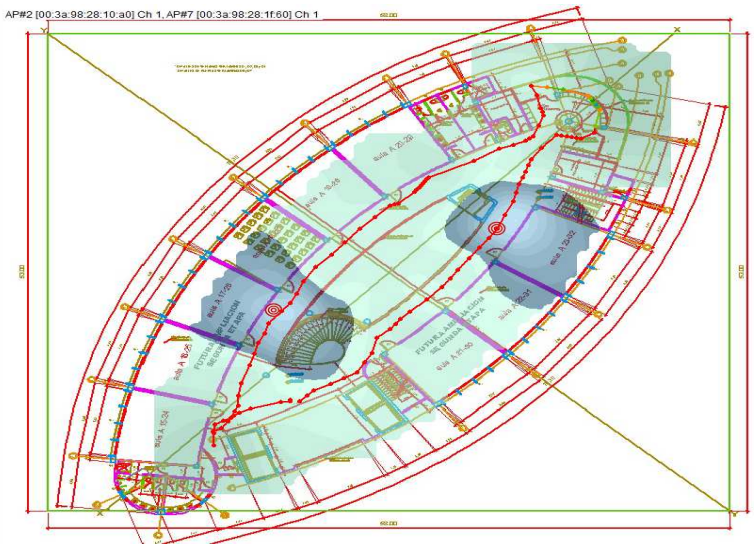


Figura 4.49, Novena planta, Facultad Especialidades Empresarial UCSG

Fuente: Autores

Décima planta: En la figura 4.50 se muestra una cobertura aproximada del 80% del área total.

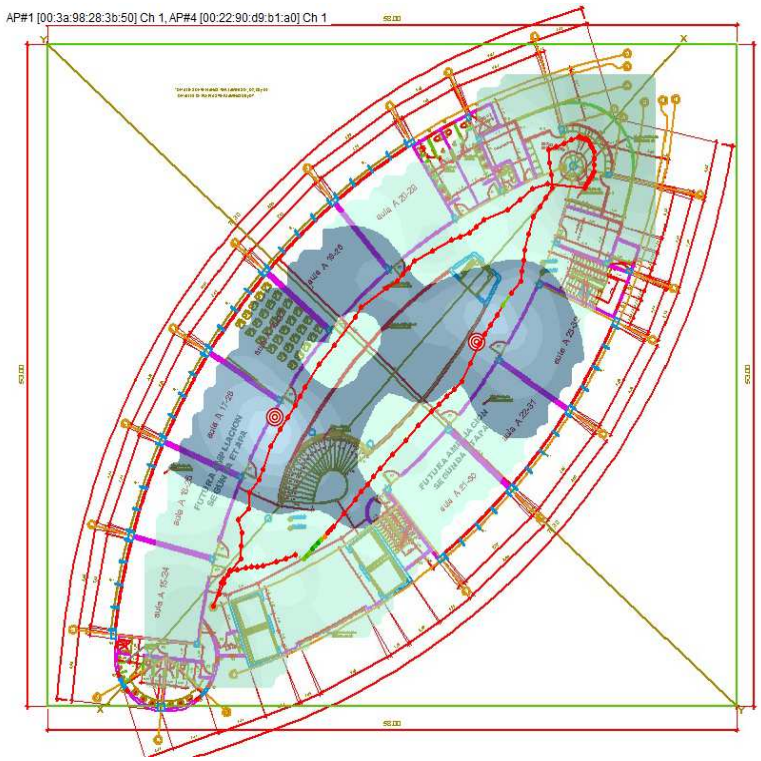


Figura 4.50 Décima planta, Facultad Especialidades Empresarial UCSG

Fuente: Autores

El edificio de la Facultad de Especialidades Empresariales consta de una red inalámbrica formada por equipos marca CISCO. Esta red consta de un equipo controlador de la serie 4400, el cual administra los 22 AP ubicados en los 11 niveles. Según se muestra en las gráficas de análisis de cobertura, existen niveles en los que solo un equipo se encuentra activo. Todos los equipos *wireless* que operan en este edificio se encuentran funcionando en el canal 1 como se muestra en la figura 4.51

SSID	AP#	Name	MAC	Ch	Security	Mode	Ave SNR	Max SNR	Min SNR	# Assoc Points	# Non-Assoc Points
cswlance	AP #1		00:3a:98:28:3b:50	Ch 1	Clear	Infra	44	73	23	0	117
cswlance	AP #2		00:3a:98:28:3a:00	Ch 1	Clear	Infra	24	44	12	0	70
cswlance	AP #3		00:3a:98:28:4d:b0	Ch 1	Clear	Infra	22	39	12	0	73
cswlance	AP #4		00:22:90:d9:b1:a0	Ch 1	Clear	Infra	46	74	14	0	114
cswlance	AP #5		00:3a:98:28:1f:60	Ch 1	Clear	Infra	29	50	13	0	98
cswlance	AP #6		00:3a:98:28:10:a0	Ch 1	Clear	Infra	30	51	12	0	94
cswlance	AP #7		00:22:90:d9:08:00	Ch 1	Clear	Infra	20	40	12	0	58
cswlance	AP #8		00:22:90:d8:fc:90	Ch 1	Clear	Infra	18	29	12	0	44
cswlance	AP #9		00:3a:98:28:20:b0	Ch 1	Clear	Infra	18	26	12	0	35
cswlance	AP #10		00:3a:98:28:42:d0	Ch 1	Clear	Infra	20	33	13	0	43
cswlance	AP #13		00:3a:98:28:3a:30	Ch 1	Clear	Infra	21	39	12	0	60
cswlance	AP #14		00:3a:98:28:3c:d0	Ch 1	Clear	Infra	18	28	13	0	32
cswlance	AP #23		00:3a:98:28:4c:80	Ch 1	Clear	Infra	15	23	12	0	22
cswlance	AP #25		00:3a:98:28:1b:60	Ch 1	Clear	Infra	15	18	12	0	14
cswlance	AP #28		00:3a:98:28:3f:50	Ch 1	Clear	Infra	13	15	12	0	6
cswlance	AP #30		00:3a:98:28:3d:80	Ch 1	Clear	Infra	15	22	12	0	24
cswlance	AP #31		00:3a:98:28:1f:10	Ch 1	Clear	Infra	15	18	12	0	12
cswlance	AP #32		00:22:90:d9:b1:00	Ch 1	Clear	Infra	15	20	12	0	15

Figura 4.51 Access Point encontrados Facultad Especialidades Empresariales

Fuente: Autores

En este edificio se realizó la captura de información en el equipo controlador, con el fin de confirmar el ancho de banda utilizado en la facultad y conocer la cantidad de usuarios simultáneos en la red. A continuación se muestran las gráficas obtenidas en el periodo de captura.

En la figura 4.52 se observa de color verde la velocidad con la que se recibe la información en relación al tiempo real en que se realizó y de color violeta la velocidad de transmisión.

Se observa en la figura 4.53 el ancho de banda utilizado en la red inalámbrica y la cantidad de clientes simultáneos que en el instante de la captura sumaban 122 clientes inalámbricos en el edificio. La captura fue realizada en el horario de mayor tráfico en la Facultad.

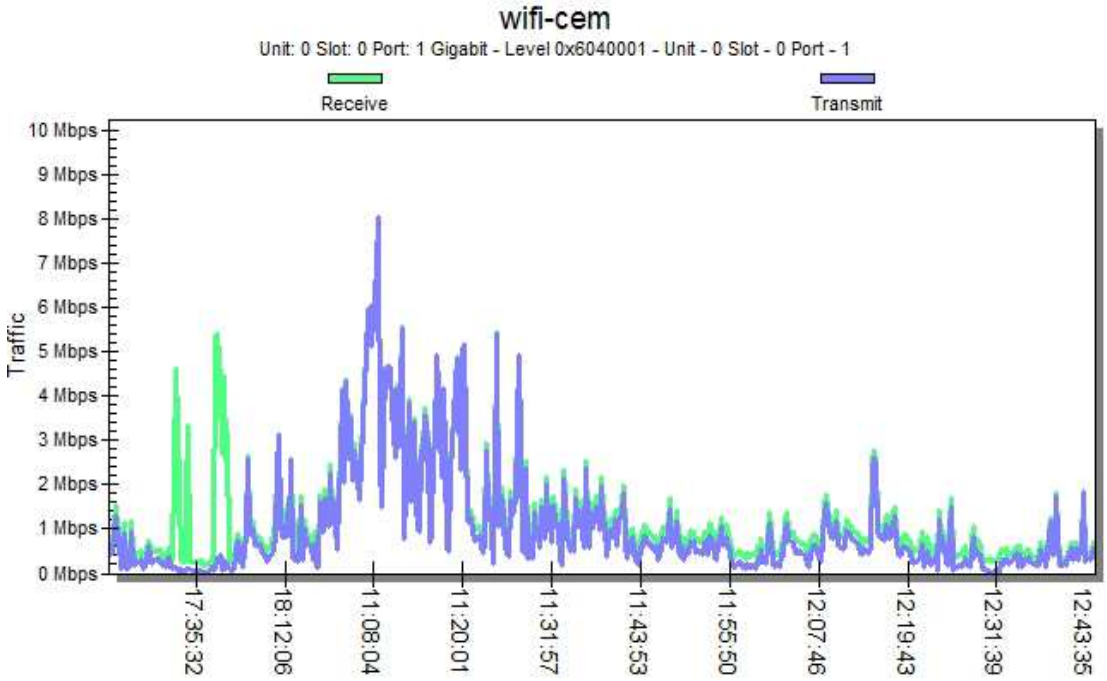


Figura 4.52, Facultad de Empresariales, Análisis de tráfico en el *Wireless* LAN *Controller*

Fuente: Autores

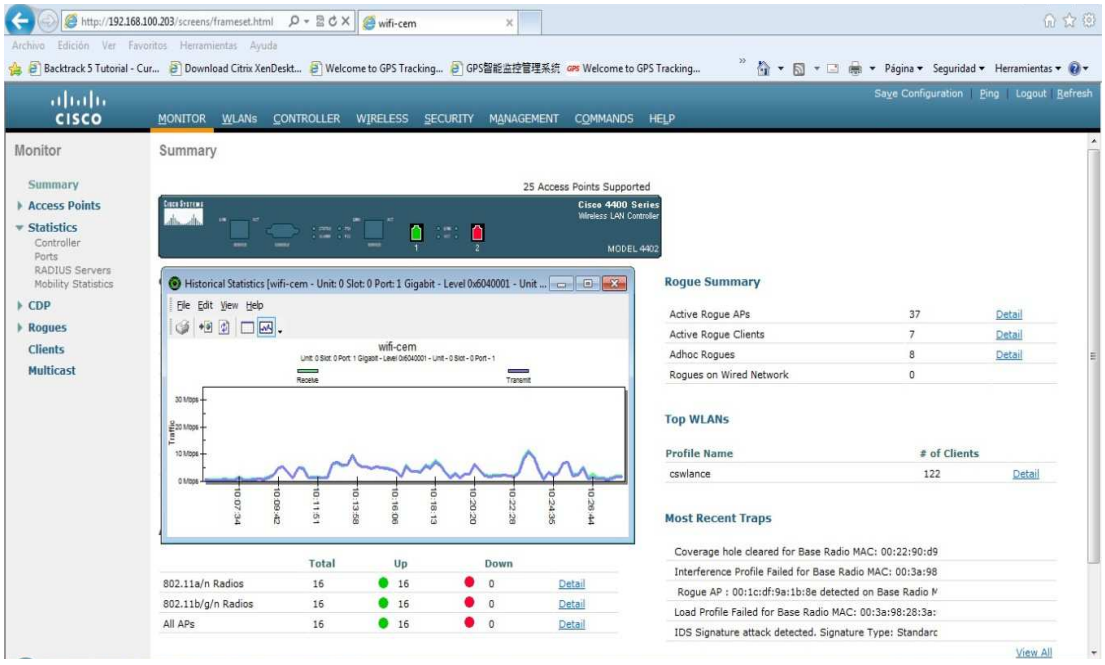


Figura 4.53, Facultad de Empresariales, estadísticas de tráfico y número de clientes

Fuente: Autores

Análisis de tráfico: Para ésta parte de la auditoría se conectó un computador con el software Observer entre la capa de distribución y acceso de la red inalámbrica para realizar un análisis de los requerimientos de tráfico utilizados a lo largo de la red wireless.

Este equipo estuvo realizando la captura de información durante tres días, para realizar el análisis se tomó como muestra un archivo del día 19 de Octubre del 2012 en el horario de 12:35 pm. Hasta 13:10 pm.

Basado en los datos obtenidos se obtuvieron estadísticas interesantes que permiten conocer el comportamiento de la red inalámbrica en horario de congestión.

En la primera gráfica tomada Figura 4.54 se observa el porcentaje de utilización de la red con la cantidad aproximada de paquetes por segundo. Se aprecia que existen picos de utilización máxima que ocasionan condiciones de error que se detallarán a continuación.

El ancho de banda disponible de 5 Mbps que actualmente tiene la red *wireless* se encuentra al máximo de su capacidad de uso, una de las principales razones es que no se cuenta con limitaciones de ancho de banda en las aplicaciones o protocolos utilizados por los usuarios de la red. Como se pudo apreciar en la captura de tráfico del WLC de la facultad de Especialidades Empresariales existe un tráfico promedio de 3 Mbps, tomando en cuenta la alta densidad de usuarios de esta red.

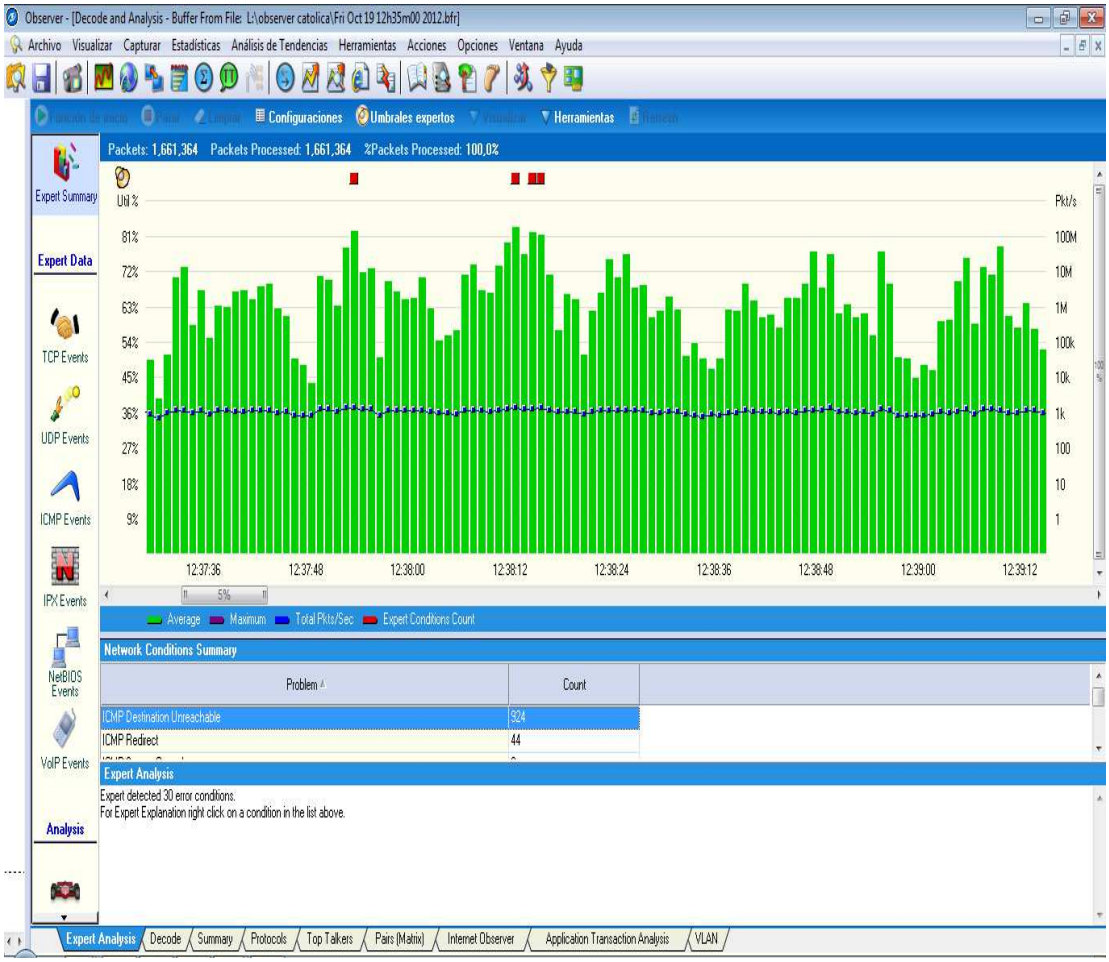


Figura 4.54, Campus UCSG, conteo de errores en transmisión

Fuente: Autores

En lo que corresponde a eventos TCP se muestra en la figura 4.55 los equipos detectados en la red que provocan gran cantidad de retransmisiones de paquetes, según se nota el protocolo de comunicación entre estos equipos es HTTPS. El error de retransmisiones se da cuando el equipo receptor de una comunicación TCP no recibe correctamente los paquetes de información, entonces este receptor pide al equipo emisor que transmita nuevamente el paquete de datos no recibido. Esta condición de error es muy frecuente en redes saturadas.

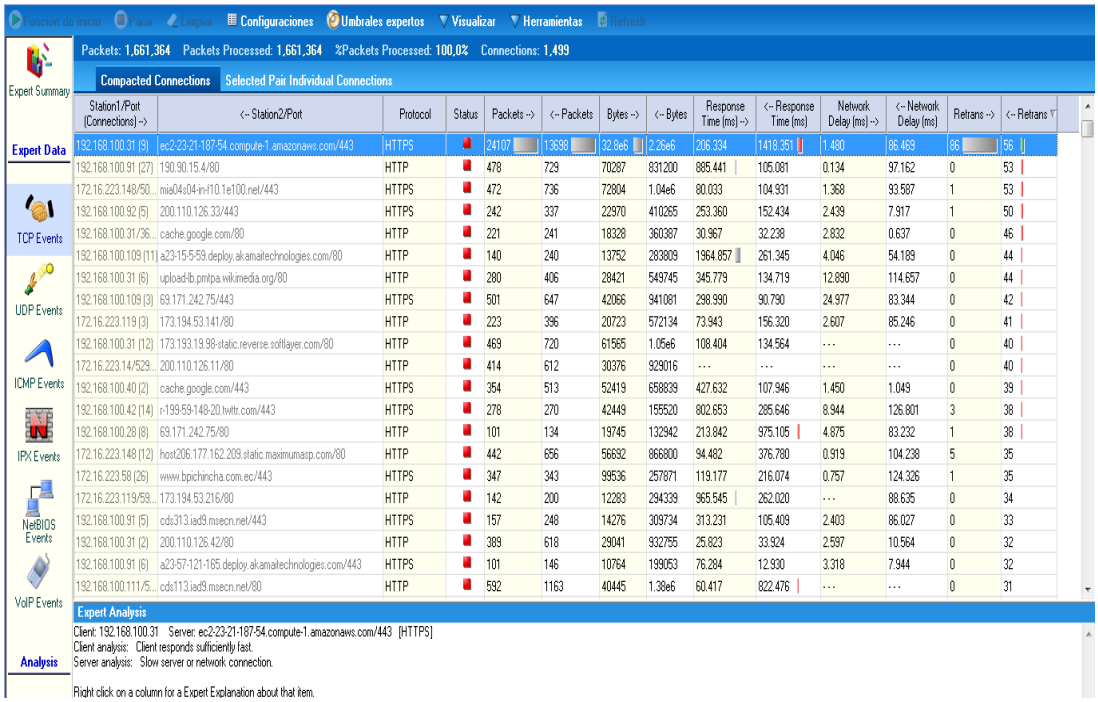


Figura 4.55, Campus UCSG, medición de tiempos de respuestas.

Fuente: Autores

En los eventos UDP se observa en la figura 4.56 que existen peticiones de resolución de nombres que no son completadas correctamente a causa de la lentitud de la red.

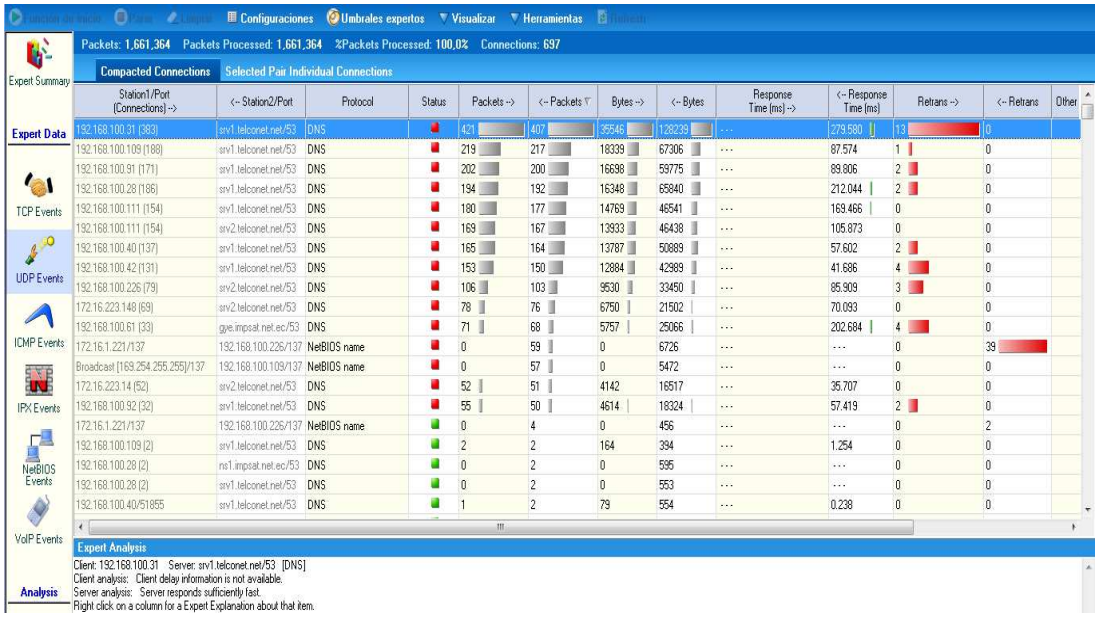


Figura 4.56, Campus UCSG, retransmisiones detectadas

Fuente: Autores

En la figura 4.57 se presenta la distribución de protocolos en la red, se puede destacar que el 99% corresponde al protocolo IP.

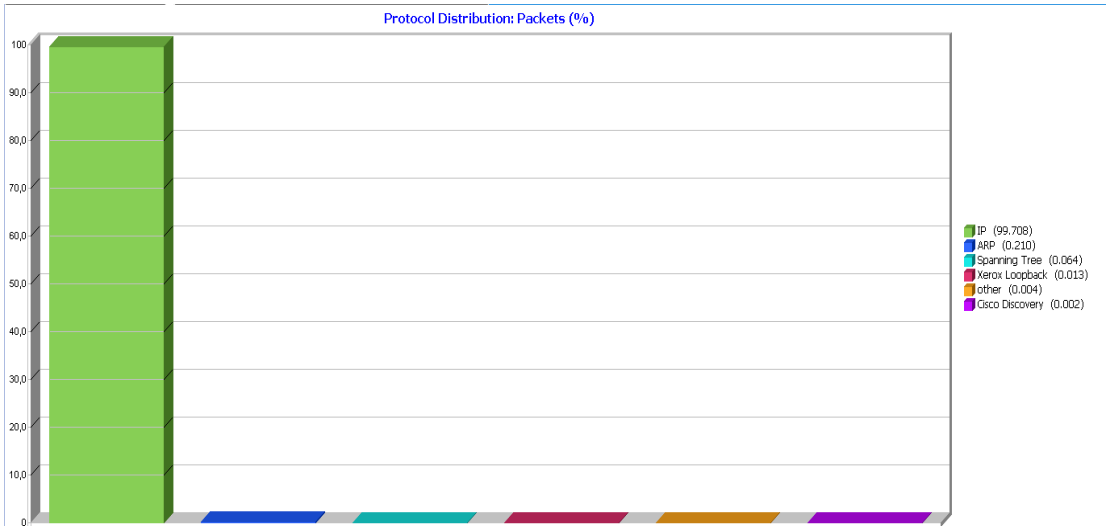


Figura 4.57, Campus UCSG, distribución de protocolos

Fuente: Autores

En la clasificación del Protocolo IP se tiene las estadísticas mostradas en la figura 4.58:

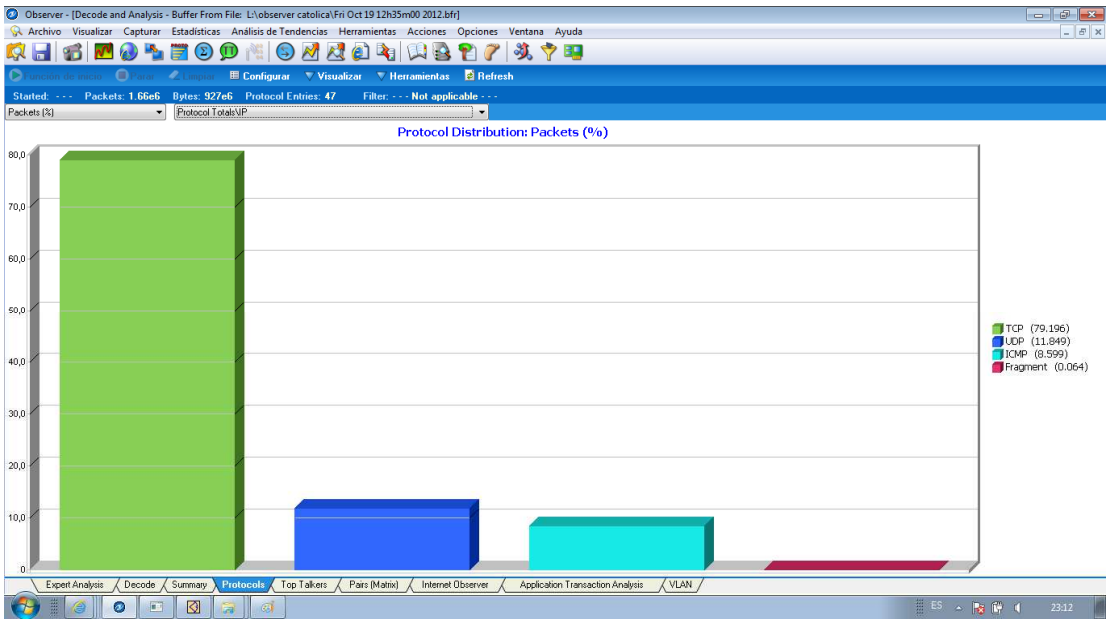


Figura 4.58, Campus UCSG distribución de protocolos IP

Fuente: Autores

En la clasificación TCP están los siguientes protocolos mostrados en la figura 4.59:

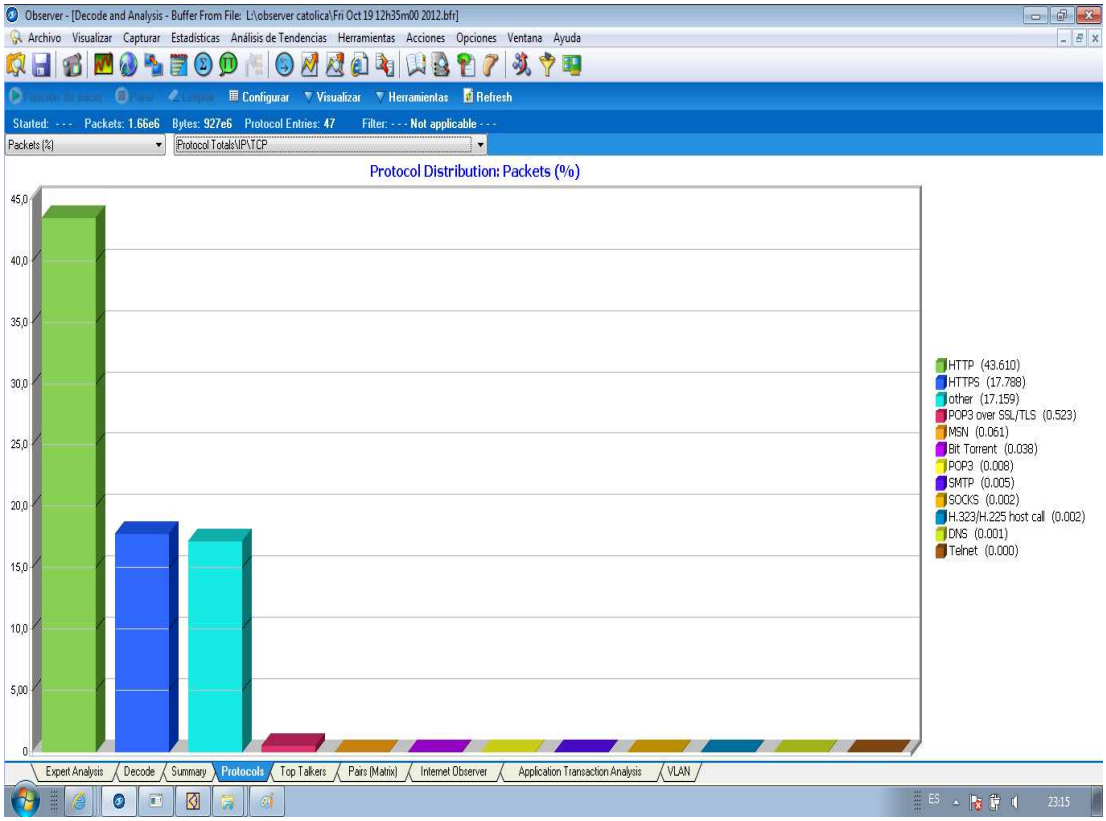


Figura 4.59, Campus UCSG, distribución de protocolos TCP

Fuente: Autores

Se obtiene de las capturas realizadas que los protocolos HTTP y HTTPS son los más utilizados en la red, luego se encuentran otros protocolos tales como POP3, MSN, SMTP, H323, DNS, TELNET y otros no identificados.

En lo que corresponde a protocolos UDP se puede observar paquetes de los protocolos más conocidos como: DNS, NTP, RIP, H323, L2TP, entre otros.

Esto se detalla en la figura 4.60.

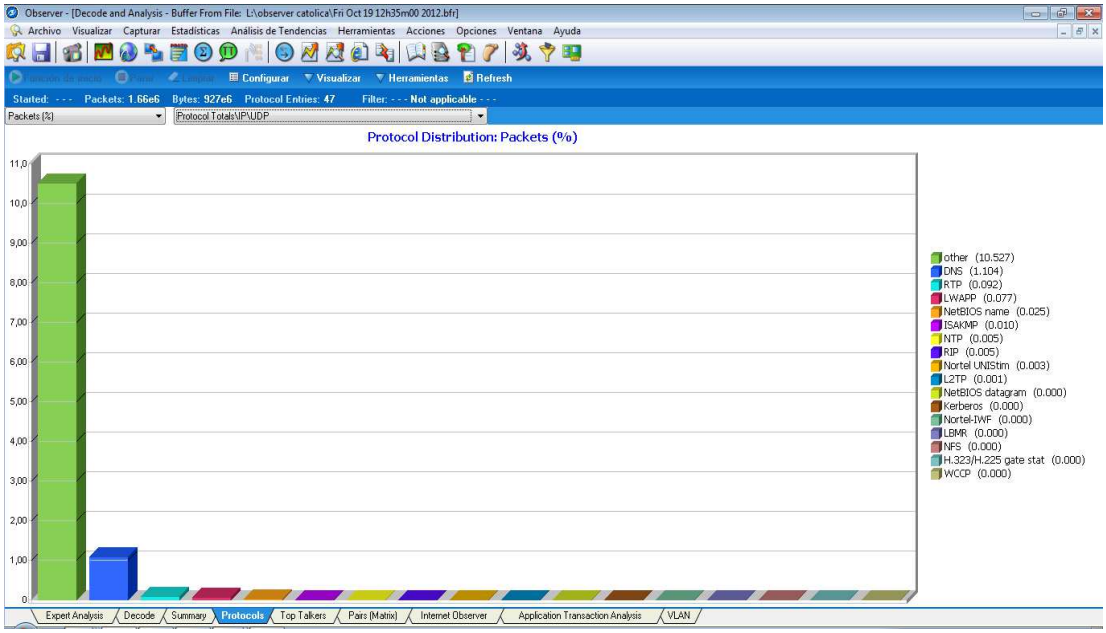


Figura 4.60, Campus UCSG, distribución de protocolos UDP

Fuente: Autores

La siguiente figura 4.61 detalla los equipos que generan mayor cantidad de tráfico dentro de la infraestructura de red inalámbrica, se muestra la dirección IP de cada equipo para fácil identificación.

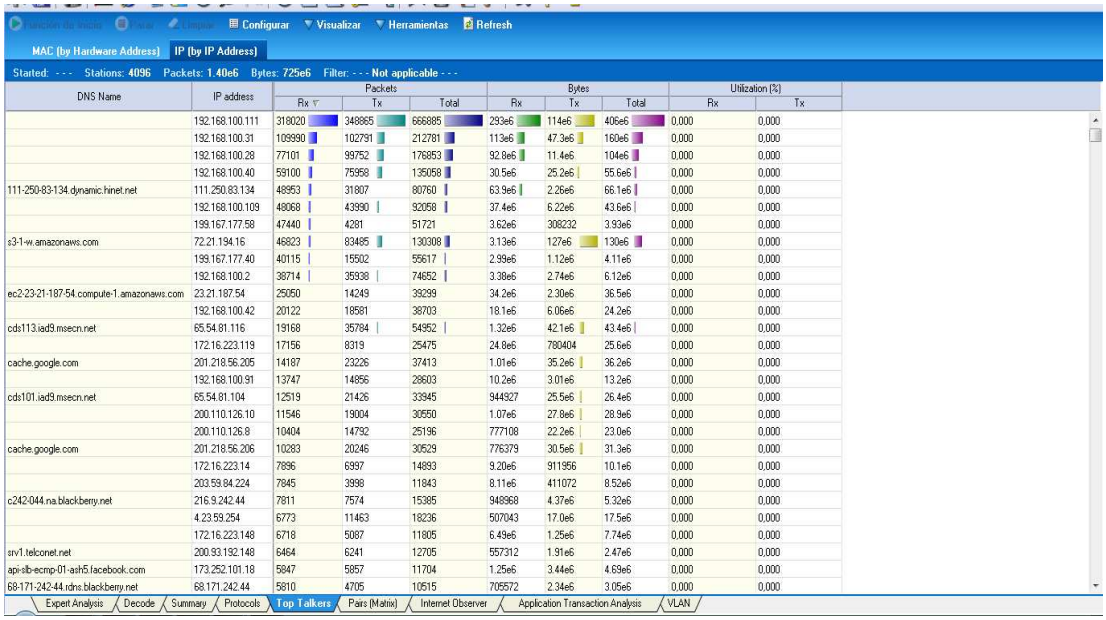


Figura 4.61, Campus UCSG, equipos con alto nivel de tráfico.

Fuente: Autores

A continuación se muestra el resumen de eventos de error encontrados antes del *switch* de acceso hacia la red inalámbrica.

Se observa en el detalle que existe gran cantidad de retransmisiones de paquetes TCP y UDP, al igual que respuestas lentas y conexiones de baja velocidad que son provocadas por un canal de Internet saturado.

Cabe destacar que los errores encontrados son de una muestra de aproximadamente 45 minutos

En el resumen de eventos encontrados existen 62 conexiones TCP establecidas lentamente, 135 respuestas TCP lentas, 135 retransmisiones, 23 procesos de conexiones TCP lentas, 924 Destinos ICMP no alcanzados, 2 paquetes ICMP bloqueados, 44 paquetes redirigidos posiblemente a causa de alguna regla de *Firewall*, 30 paquetes ICMP caducados en tránsito.

Adicional a esto hay un máximo de utilización excedida de la red en un 80%. Hay problemas de enrutamiento entre equipos de la red que deben ser analizados con mayor profundidad, estos problemas pueden ser causados por errores en asignación de direccionamiento en las capa de distribución.

4.2.3. Informe de resultados del análisis

Luego del proceso de análisis a las facultades del campus UCSG se ha podido identificar varias fallas de diseño e implementación en la red actual que impiden tener un servicio inalámbrico óptimo.

La cobertura al interior de la mayoría de las facultades logra cumplir las expectativas de diseño para el servicio inalámbrico brindado, excepto algunas en las cuales se requiere ubicar los equipos necesarios para expandirla.

Interferencia entre canales inalámbricos: El problema que se encuentra presente en la mayoría de los sitios a lo largo del campus UCSG es la configuración equivocada de los canales de frecuencia en que operan los AP. Como se puede observar en el análisis realizado los equipos que brindan la conexión inalámbrica, en la mayoría de los escenarios, se encuentran operando en el mismo canal de frecuencias provocando interferencias en la transmisión y recepción de información por este medio. La figura 4.62 Muestra la interferencia entre canales.

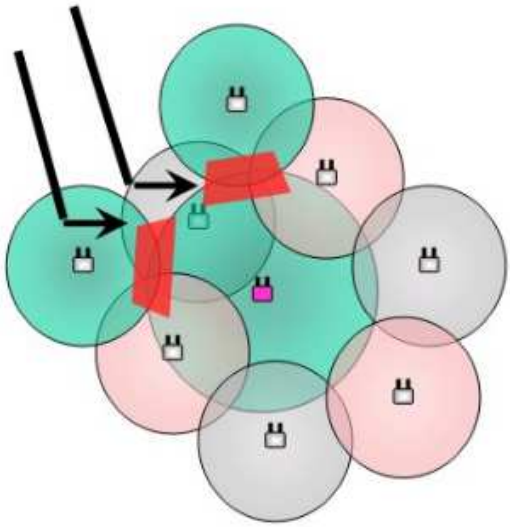


Figura 4.62 – Interferencia entre canales

Fuente: http://blog.merunetworks.com/blog/2009/09/80211n-wlan-architectures-think-different/

En un diseño adecuado se debe controlar las frecuencias en las que se configuran los AP que se encuentran cercanos, de esta manera reducir las interferencias. De acuerdo a los rangos de frecuencias en las que opera cada canal se puede determinar la manera de realizar las configuraciones, en la figura 4.63 se muestra esta información.

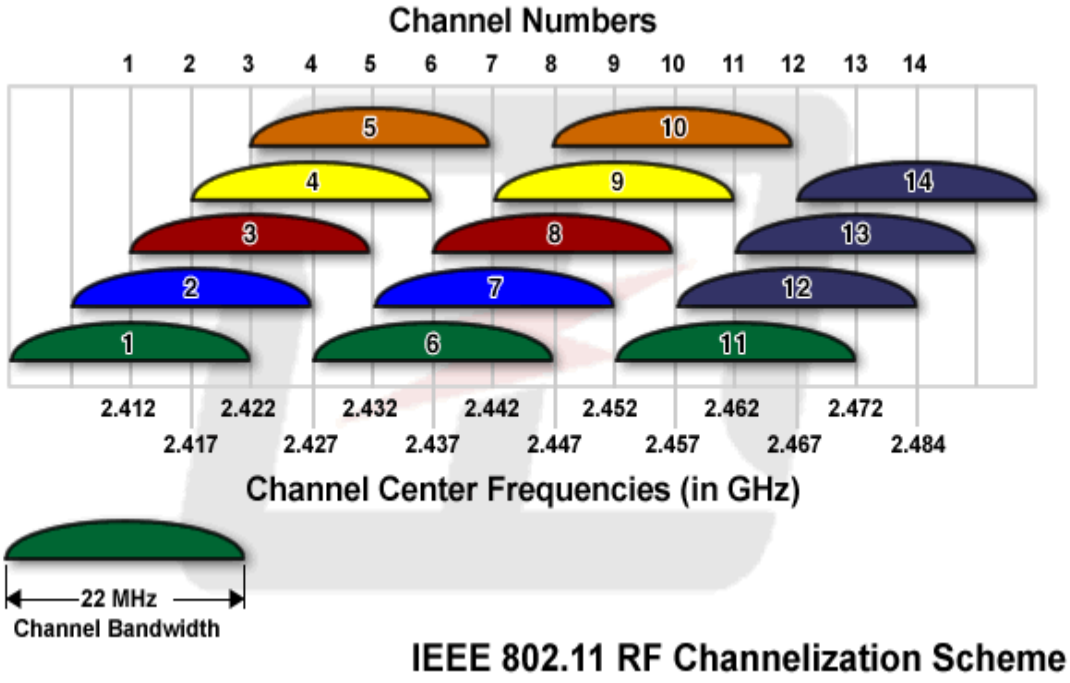


Figura 4. 63– Frecuencia de Canales WiFi

Fuente: http://www.l-com.com/content/Bandpass_Filters_FAQ.html

Siguiendo estas indicaciones relacionadas a la configuración de canales en los AP se podría aprovechar de mejor manera los recursos actuales del campus UCSG, existen otras consideraciones que se deben tomar en cuenta.

Equipos con capacidades limitadas: Se pudo detectar además que los equipos *router* utilizados en las facultades muestran inconvenientes al tratar de cumplir con los requerimientos de direccionamiento IP solicitado por los usuarios del servicio inalámbrico, debido a que una vez que se encuentra llena la tabla de MAC *Address* no puede aceptar más conexiones y en algunos casos deja de funcionar adecuadamente.

Se debe utilizar equipamiento adecuado en la infraestructura de la red *wireless* del campus UCSG, que cumpla con las expectativas de servicio esperado por los usuarios.

Zonas sin cobertura: Como se ha podido evidenciar en el análisis realizado existe mínima y en ocasiones una cobertura nula en las zonas abiertas del campus UCSG, siendo ésta una gran debilidad en el diseño debido a la gran cantidad de usuarios ubicados en estos sectores.

Roaming: Ésta es una característica mostrada en la gráfica 4.64 es muy importante al momento de diseñar soluciones *wireless* dentro de un campus, permite la movilidad dentro de la infraestructura sin que el usuario tenga que cambiar configuraciones o conectarse manualmente a redes inalámbricas disponibles.

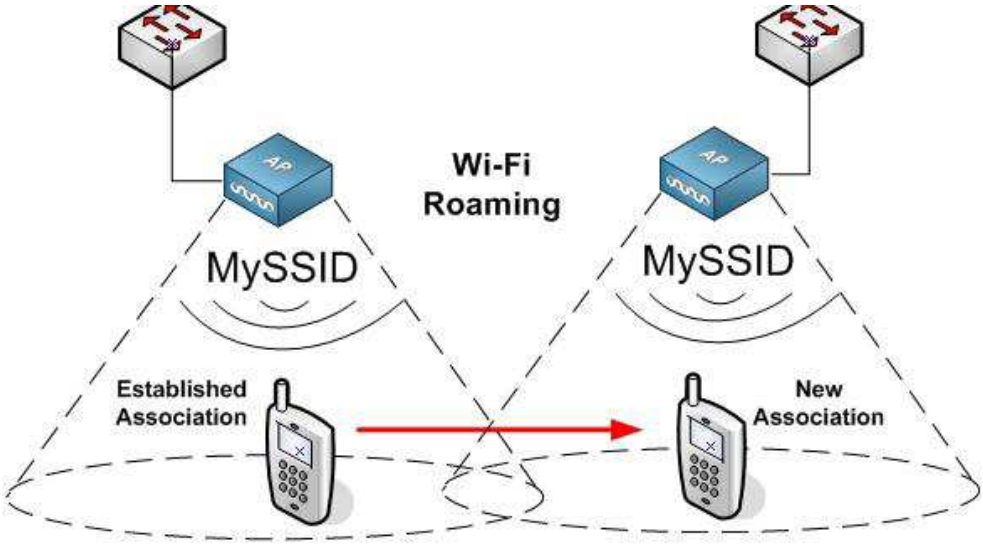


Figura 4.64 –WiFi Roaming

Fuente: http://revolutionwifi.blogspot.com/2011/12/wi-fi-roaming-analysis-part-1.html

Actualmente no se encuentra implementada en el diseño *wireless*, será considerada en la etapa de diseño.

4.3. Diseño de solución *wireless*

Para dar inicio al diseño de la nueva solución *wireless* del campus UCSG debemos definir lo que permanecerá activo de la infraestructura actual, evaluando de ésta

manera todos los equipos que operan en las diferentes capas del modelo jerárquico con la finalidad de aprovecharlos a su totalidad. Principalmente se debe enfocar la capa de acceso implementada y evaluar en esta sección los *switches* que concentran los equipos inalámbricos por cada facultad. Existen algunas características de estos equipos que son necesarias para la implementación de redes *wireless*. Se considera en el diseño la capacidad de *roaming* a lo largo de la red *wireless*, para esto es necesario que existan áreas de *overlap* del 10% entre las señales emitidas por los AP que permitan el paso entre celdas sin mayor incidencia para el usuario final. Es muy importante para la implementación de este *feature* la debida configuración de los canales de frecuencia en la que operan los AP.

Se adoptará un esquema *wireless* conocido como *controller based solution* mostrado en la figura 4.65. Este esquema depende de un controlador donde se administra la configuración de cada AP, de esta manera la configuración se obtiene automáticamente y es actualizada dinámicamente en caso de existir cambios. Todo esto es posible gracias al protocolo LWAPP (*Lightweight Access Point Protocol*) por medio del cual se establece comunicación entre los AP y los WLC (*Wireless LAN Controller*, Controlador de LAN inalámbrica).

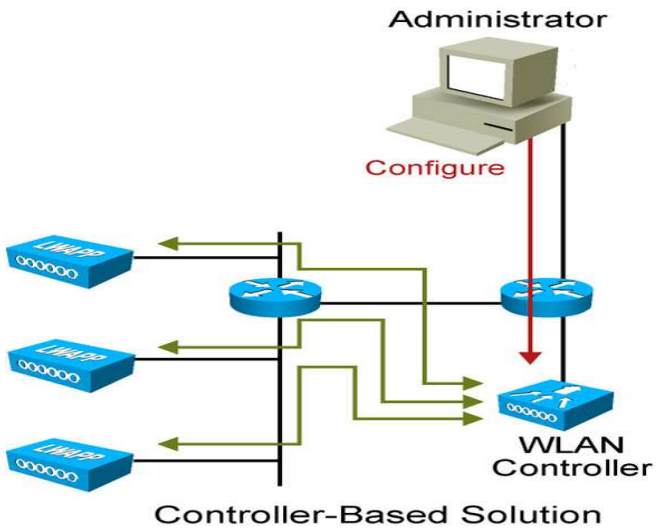


Figura 4.65 –Controller Based Solution

Fuente: http://www.lammle.com/blog/118/cisco-unified-wireless-networks-cuwn/

4.3.1. Equipamiento

A continuación se detallará el equipamiento considerado para el diseño de la nueva red del campus de la UCSG.

WLC: Los dispositivos WLC ejecutan varias funciones dentro de las redes *wireless*, como: políticas de seguridad, administración de señales RF, calidad de servicio, *roaming*, etc. Operan en conjunto con los AP y los sistemas de gestión para brindar servicio a aplicaciones inalámbricas. Proveen el control, escalabilidad, confiabilidad, y seguridad a los administradores de red para que se pueda contar redes escalables.

La serie 4400 de Cisco (figura 4.66) son diseñados para medianas y grandes empresas brindando soporte y administración de hasta 100 equipos AP.

Figura 4.66 –WLC 4404

Fuente: http://www.frontierpc.com/wireless-networking/wifi-wireless-access-points/wireless-lan-controller/cisco/aironet-4404-wireless-lan-controller-11079987.html

Access Points: La serie de AP 1240 de Cisco está diseñada para ambientes ásperos donde es necesaria cierta versatilidad de antenas. Los componentes de su estructura le permiten operar en ambientes donde se soportan altas temperaturas.
Este equipo (figura 4.67) posee la capacidad de adaptar 2 antenas para ampliar la cobertura como sea requerido, para esto se cuenta con varios modelos de antenas con las que se podrá obtener los resultados esperados.

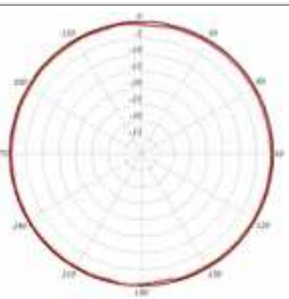
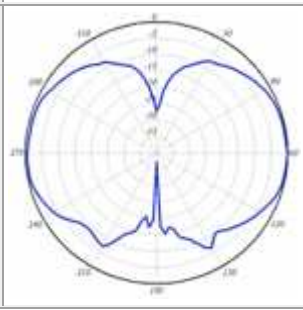
Figura 4.67 –Access Point 1242AG

Fuente: http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6521/product_data_sheet0900aecd8031c844.html

Antenas: En este diseño tenemos dos escenarios en los que se implementará la red *wireless*, para esto debemos considerar diferentes antenas que cumplan con las necesidades de los usuarios. A continuación se muestran las características técnicas de las antenas sugeridas en las tablas 4.6 y 4.7

Tabla 4.6 Descripción técnica antena AIR-ANT2422DG-R

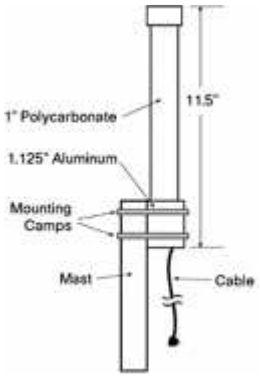
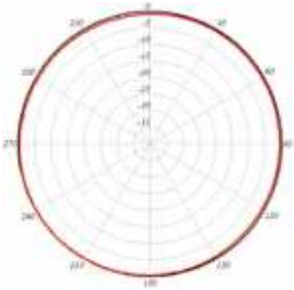
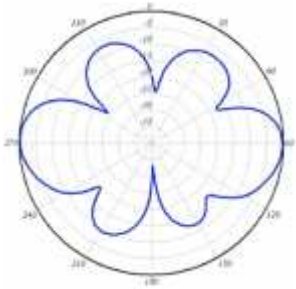
Fuente: Autores

Dimensions	**Azimuth Plane Radiation Pattern**	**Elevation Plane Radiation Pattern**
		
Frequency Range	2.4-2.484 GHz	
VSWR	Less than 2:1	
Power	5 watts	

Gain	2.2 dBi
Polarization	Linear
Azimuth 3dB Beamwidth	Omnidirectional
Elevations 3dB Beamwidth	65 degrees
Antenna Connector	RP-TNC
Cable Length	None
Dimensions	3.9 in.
Mounting	To RP-TNC Connector

Tabla 4.7 Descripción técnica antena AIR-ANT2506

Fuente: Autores

Dimensions and Mounting Specifications	**Azimuth Plane Radiation Pattern**	**Elevation Plane Radiation Pattern**
		
Frequency Range	2.4-2.83 GHz	
VSWR	Less than 2:1, 1.5:1 Nominal	
Gain	5.2 dBi	
Polarization	Vertical	

Azimuth 3dB Beamwidth	Omnidirectional 360 degrees
Elevations Plan (3dB Beamwidth)	36 degrees
Antenna Connector	RP-TNC
Cable Length	3 ft (91 m)
Dimensions	11.5 in. x 1.125 in. (29.21 cm x 2.85 cm)
Mounting	Mast mount - indoor/outdoor

***Switches*:** Una de las características requeridas en diseño wireless y de voz es la de poder brindar la energía eléctrica para el funcionamiento de los equipos a través del cableado UTP, esta característica conocida como PoE (*Power over Ethernet*, Energía sobre Ethernet) puede ser solicitada en los *switches* Cisco.

Utilizando PoE se obtienen varias ventajas, entre las principales: reducción de tendido eléctrico que puede causar interferencias junto al cableado de red y los equipos que obtienen energía de esta manera continuarán operando mientras el *switch* esté encendido.

Figura 4.68 –*Switch* Cisco PoE

Fuente: http://www.cisco.com/web/DE/presse/kmu-news.html

Gestión: Cisco cuenta con una herramienta de gestión avanzada llamada *WCS* (*Wireless Control System*, Control de Sistema Inalámbrico) para topologías *wireless*

con la que es posible monitorear, desarrollar, planear y corregir problemas en cualquier tipo de red. Incluyendo el enfoque *life-cicle* se logra:

- Reducir los costos de operación.
- Mejora la eficiencia de IT por medio de su interfaz gráfica fácil de usar.
- Reduce los requerimientos de personal para administración de la red.
- Mejora el rendimiento de redes *wireless* mitigando las interferencias RF.

4.3.2. Facultades

Por medio del análisis obtenido se puede identificar las posiciones que servirán para ubicar los equipos AP en el interior de cada facultad. Es necesario mencionar que a lo largo del análisis realizado se observó que no hay problemas notables en cobertura de espacio físico en la mayoría de las facultades.

El error más usual es la configuración de canales de frecuencia de operación de los AP dentro de cada facultad, por lo que se debe tener mucho cuidado durante la fase de implementación. Este tipo de problemas son fácilmente reconocidos por un WLC que administre la red *wireless*, por eso su importancia y recomendación de uso.

Facultad de Ciencias Médicas

En esta facultad se ha realizado una reubicación de los AP para optimizar el uso de equipos. Con la configuración adecuada de los canales de frecuencia 1 y 6 se reduce totalmente la interferencia que se encontró durante la fase de análisis.

Se ubican 2 equipos AIR-AP1242AG por cada piso de la facultad con antenas tipo AIR-AT2422DB-R.
En las figuras 4.69 y 4.70 se muestran las posiciones sugeridas para los AP en los edificios de esta facultad, las posiciones mostradas son replicadas en cada piso.

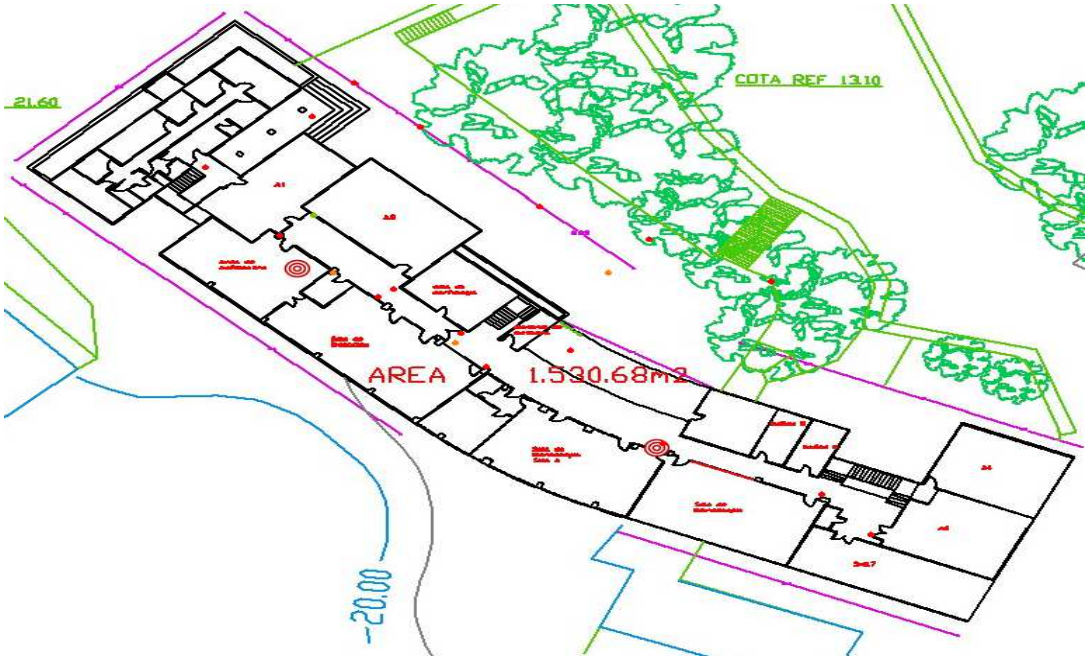


Figura 4.69 –Ubicación de AP planta baja

Fuente: Autores

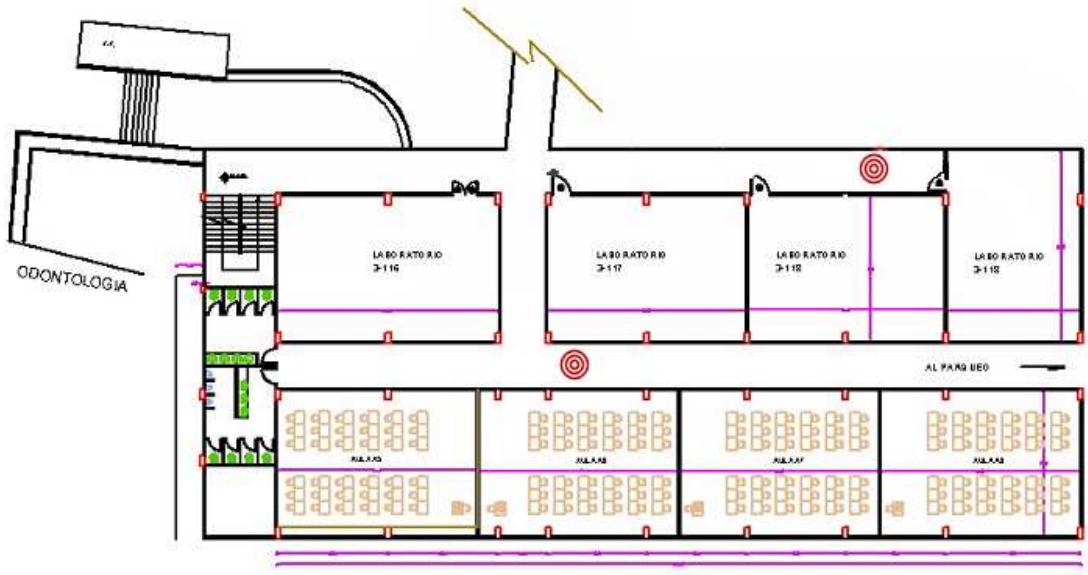


Figura 4.70 –Ubicación de AP planta baja del nuevo edificio.

Fuente: Autores

Facultad de Jurisprudencia

La cobertura brindada por los equipos que se encuentran en funcionamiento en esta facultad es buena, como se sugiere en la figura 4.71 se debe mejorar la cobertura de los pisos superiores. Existen dos aspectos que se deben mejorar, uno de ellos es la configuración errada en los canales de frecuencia en la que operan los equipos y el otro sería la limitación en la cantidad de direcciones MAC que soporta el *router* encargado de brindar direccionamiento IP a los usuarios dentro de la facultad.

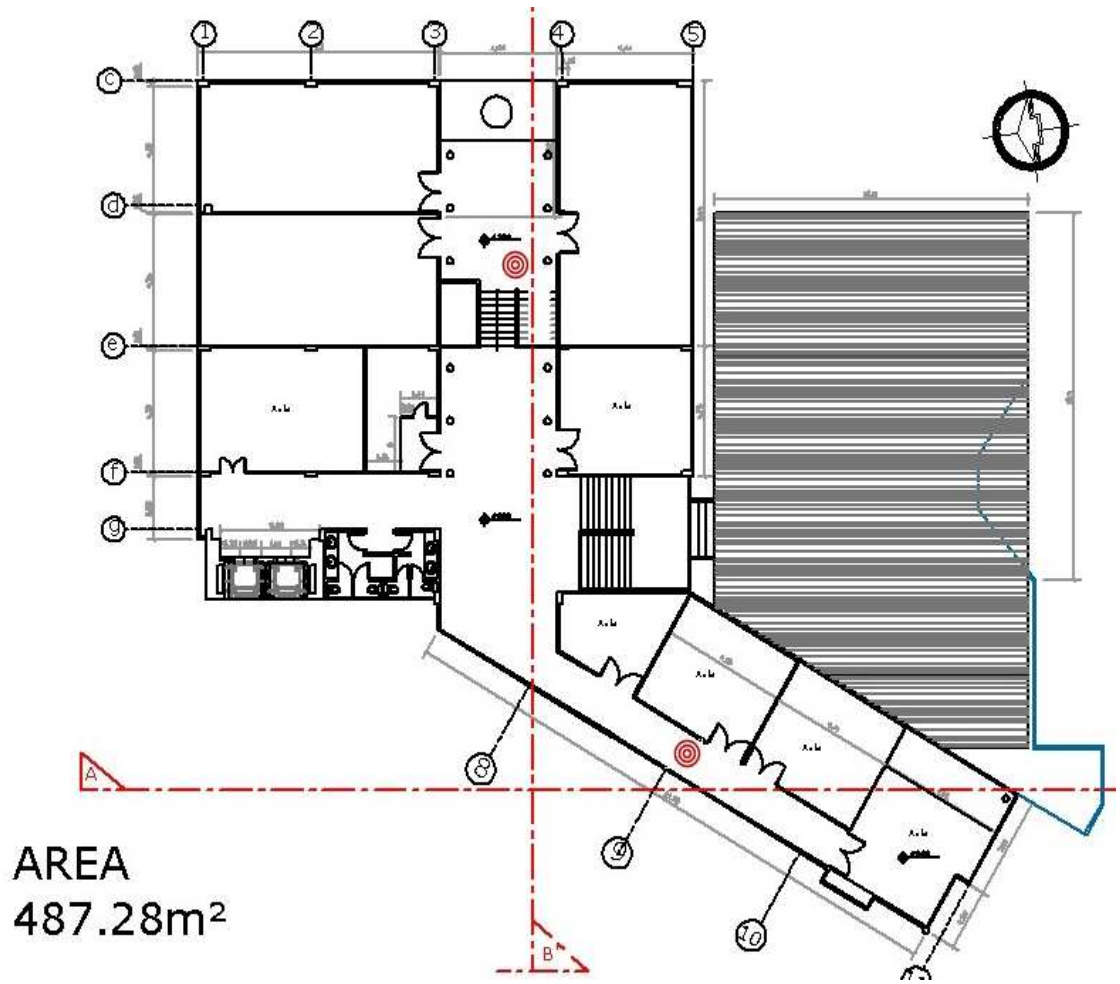


Figura 4.71 –Ubicación de AP quinta planta

Fuente: Autores

Facultad de Arquitectura

En esta facultad se prestó mucha atención a la cobertura limitada de señal inalámbrica en los pisos 3, 4 y planta baja. Se necesita colocar los AP adecuadamente para brindar cobertura en el área. La figura 4.72 muestra las posiciones sugeridas. La correcta configuración de canales es importante para el correcto funcionamiento de la red, en este caso se hará uso de los canales 1, 6 y 11 tomando en cuenta la interacción entre cada uno de los niveles del edificio.

Figura 4.72 –Ubicación de AP planta baja y planta alta 3

Fuente: Autores

Facultad Técnica

En la Facultad Técnica se ha reestructurado la ubicación de los equipos AP logrando reducir la cantidad necesaria. Es cierto que no existían problemas de interferencia entre canales por la separación de los equipos en esta facultad, es recomendado utilizar la separación de 5 canales de frecuencia en equipos inalámbricos cercanos para evitar estos problemas. La figura 4.73 muestra las posiciones sugeridas.

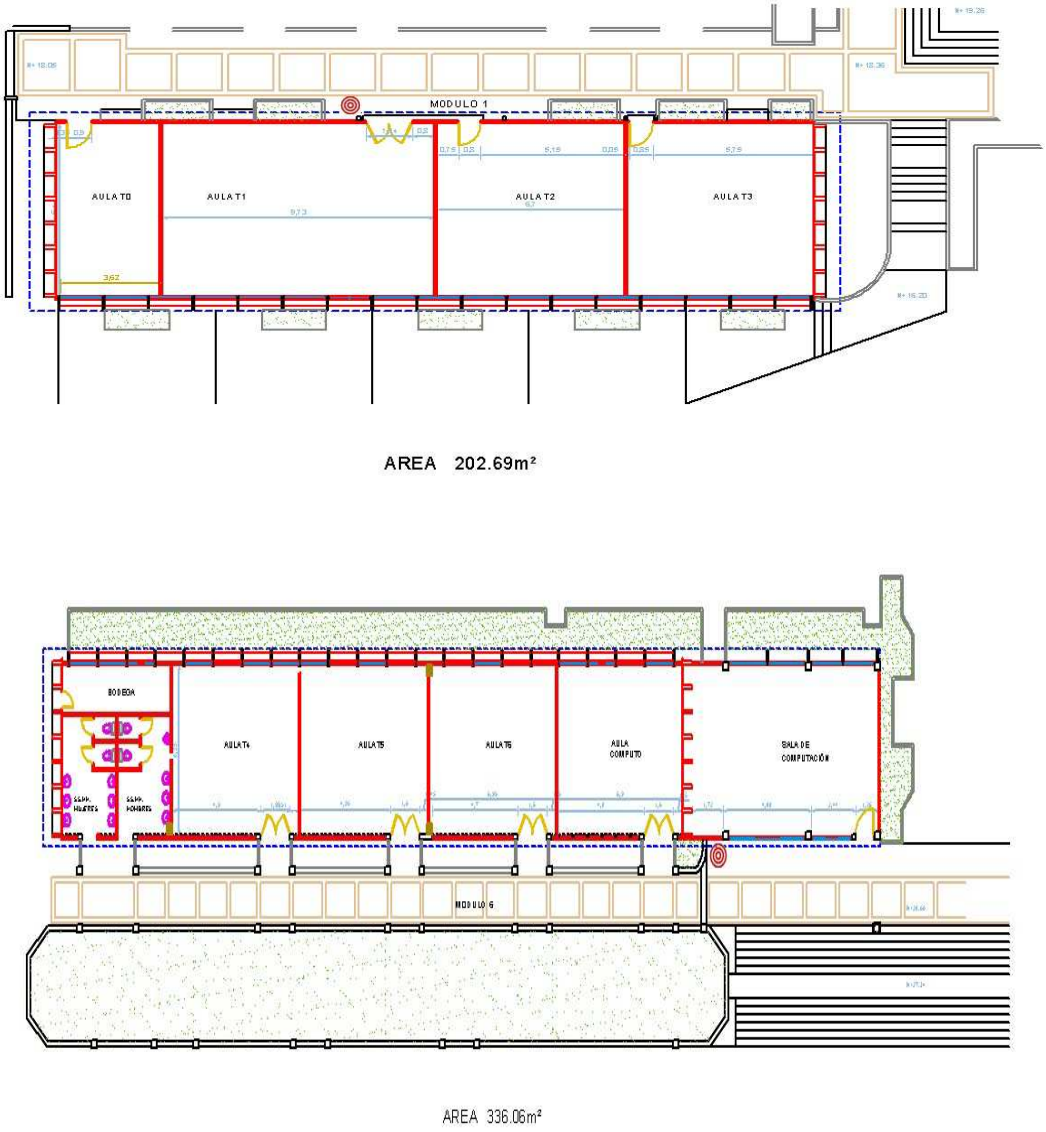


Figura 4.73 –Ubicación de AP en pisos de aulas

Fuente: Autores

Facultad de Filosofía

Se debe reubicar los equipos de la planta baja y configurar adecuadamente los canales de frecuencia utilizados. En los pisos 1, 2 y 3 hay que mejorar la cobertura ubicando más equipos y configurando los canales adecuados por la interacción entre pisos. La figura 4.74 muestra las posiciones sugeridas.

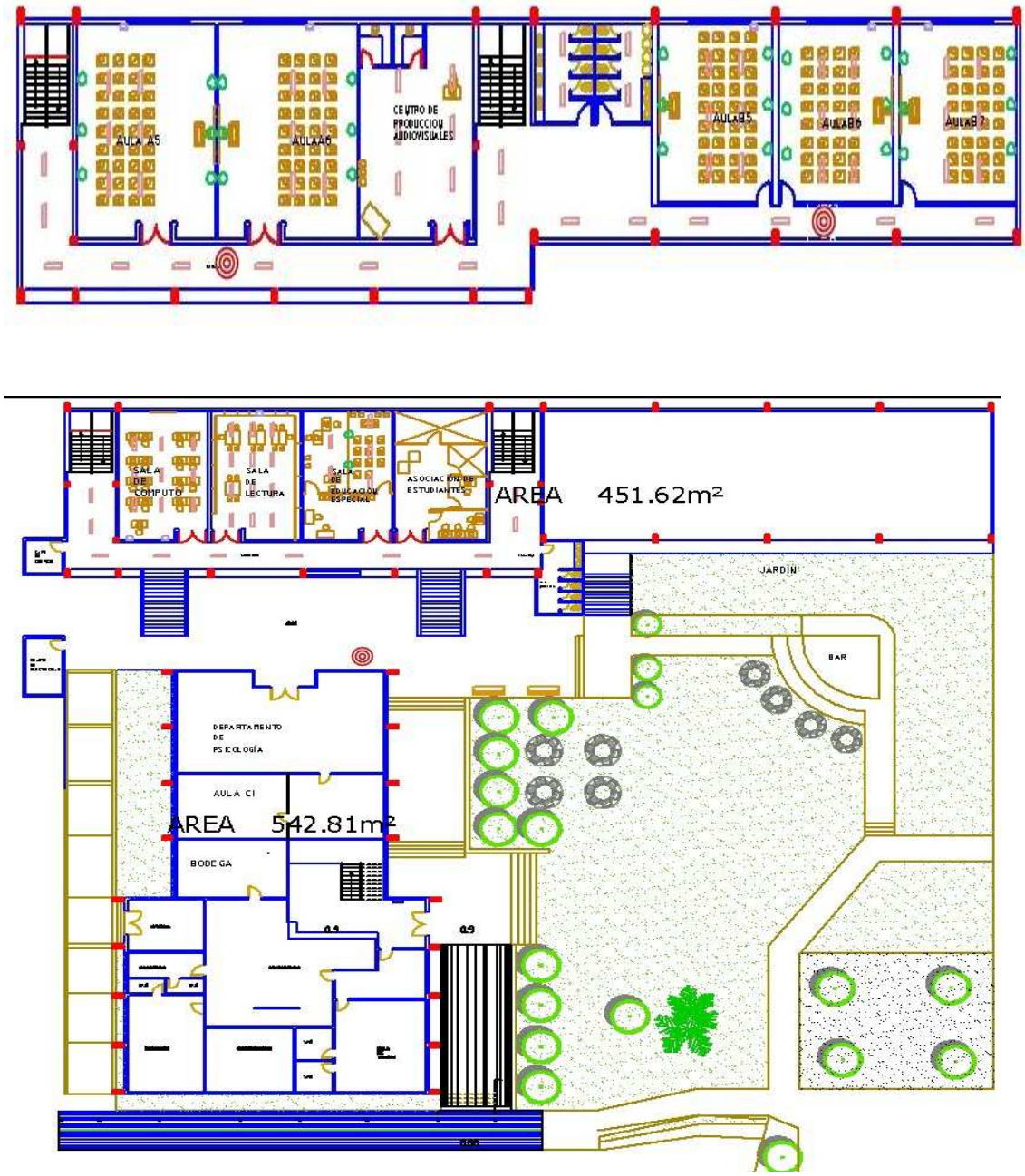


Figura 4.74 –Ubicación de AP en pisos de aulas y planta baja

Fuente: Autores

Facultad de Ingeniería

En esta facultad se debe mejorar la ubicación de los equipos AP para lograr obtener la cobertura total de la misma, principalmente en el tercer piso como se muestra en la figura 4.75. Existe una configuración adecuada de los canales de frecuencia por lo que se aprovecha al máximo los equipos que operan en el área.

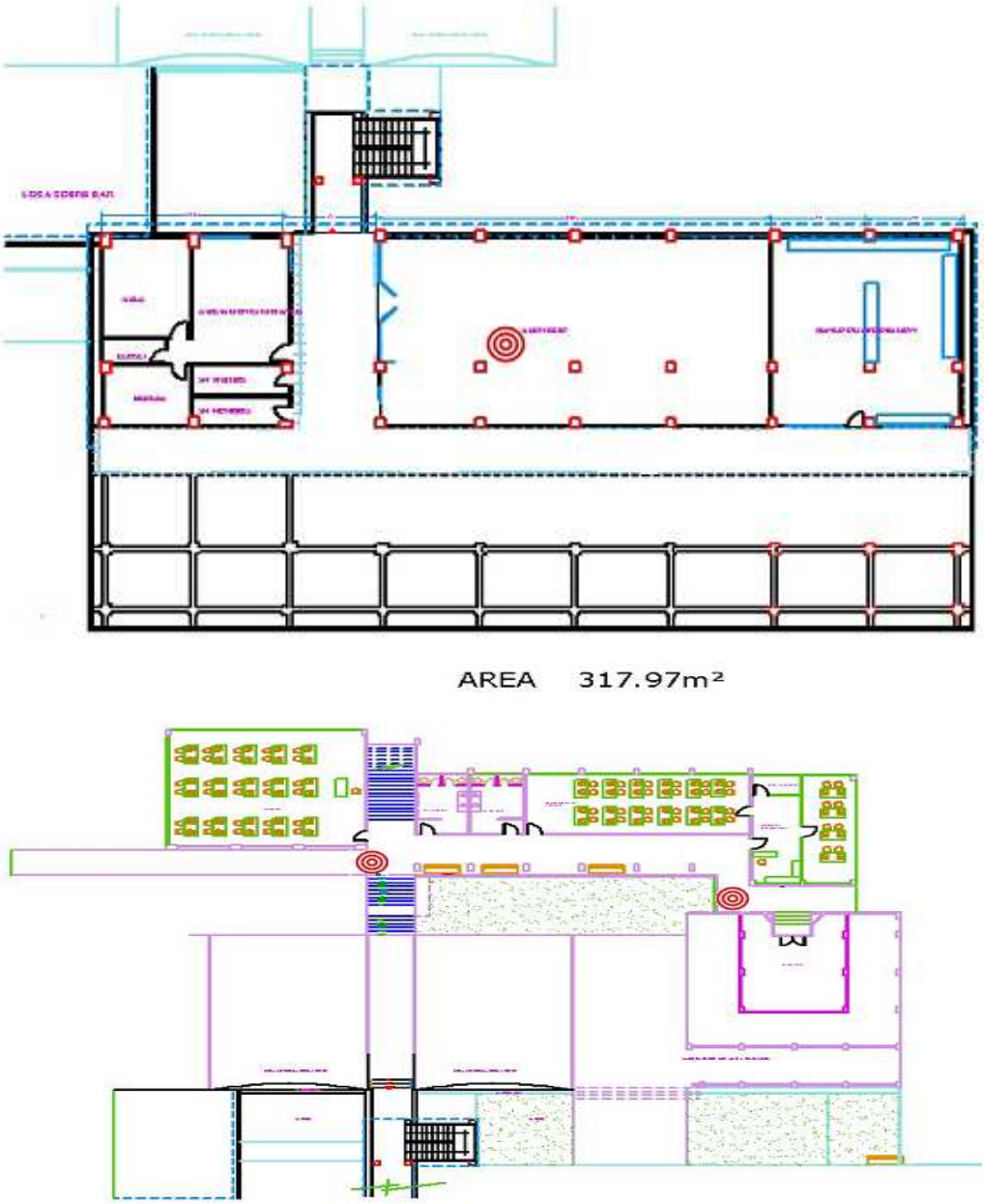


Figura 4.75 –Ubicación de AP en primera planta y 3er piso

Fuente: Autores

Facultad de Empresariales

Esta facultad cuenta con un diseño de red inalámbrica Cisco actualmente, durante el proceso de análisis se pudo observar la evolución del mismo con ciertos cambios realizados en la implementación.

La cobertura del área ofrecida en cada nivel de esta facultad es casi perfecta debido a la ubicación de los equipos AP a lo largo de la misma, se debe recalcar nuevamente la configuración de los canales de frecuencia debido a que todos los equipos se encuentran operando en el mismo canal.

Zonas abiertas

Se ha establecido 2 ubicaciones para los AP destinados a brindar cobertura en las zonas abiertas del campus UCSG mostradas en la figura 4.76 y 4.77. Los modelos de los equipos AP utilizados es Cisco 1242AG con 2 antenas omnidireccionales AIR-ANT2506.

Figura 4.76 –Zonas abiertas sin cobertura

Fuente: Autores

Figura 4.77 – Zonas abiertas sin cobertura

Fuente: Autores

A continuación en la figura 4.78 y 4.79 se muestran las pruebas de cobertura obtenidas desde las ubicaciones antes descritas para las zonas abiertas. Es importante mencionar que para estos equipos se necesitará conexiones tipo PoE debido a la dificultad de realizar cableado eléctrico hasta cada uno de los puntos.

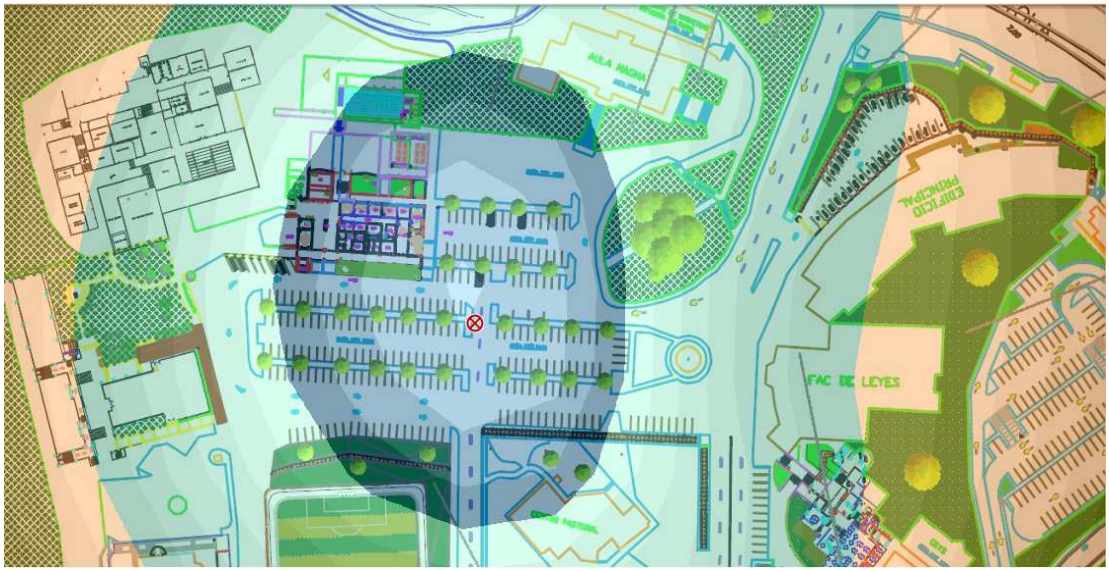


Figura 4.78 – Pruebas de cobertura en zonas abiertas

Fuente: Autores

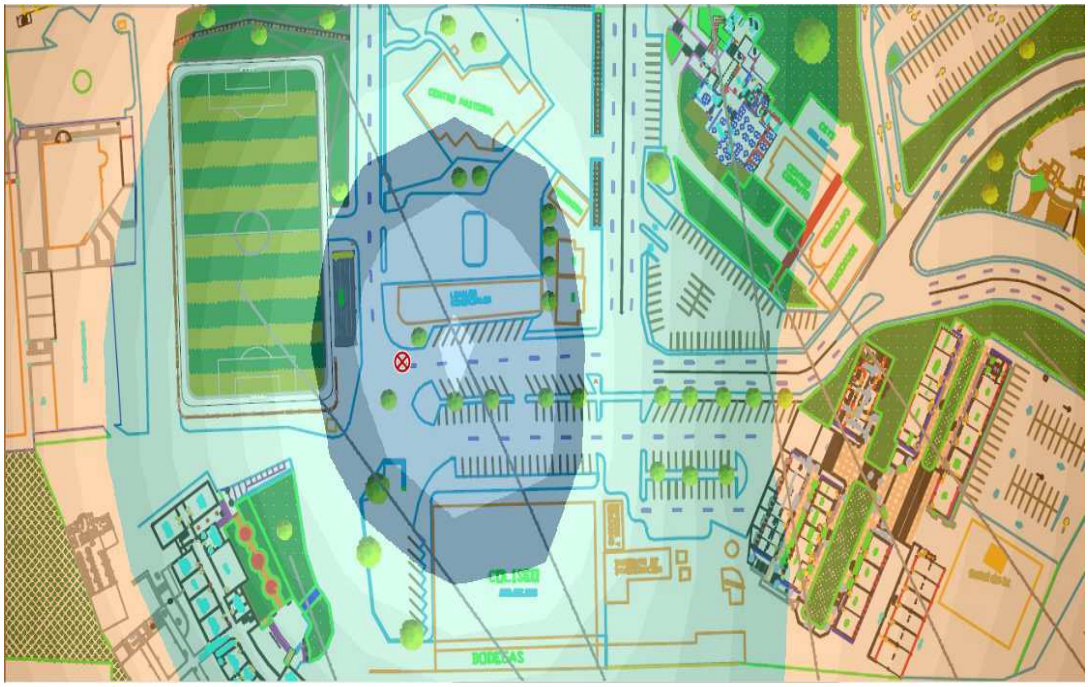


Figura 4.79 –Pruebas de cobertura en zonas abiertas

Fuente: Autores

El tipo de antenas utilizadas en este sector es muy importante debido al amplio espacio físico que requiere cobertura, se necesitan antenas potentes que puedan brindar el servicio como es esperado.

4.4. Presupuesto

Se plantean dos opciones de presupuestos, la tabla 4.8 es una propuesta con un solo modelo de AP, los que actualmente la universidad tiene instalados en la Facultad de Empresariales, mientras que en la tabla 4.9 se proponen dos modelos de AP de una serie menor pero igual con buena capacidad en la que las antenas ya están integradas diferentes a la primera propuesta.

Tabla 4.8 Presupuesto del Diseño propuesto de la Red *Wireless* del campus UCSG, opción 1

Fuente: Autores

Código	Descripción	#	P. Unit	Subtotal	Descuento	Total
AIR-ANT2422DG-R	2.4 GHz 2.2 dBi Straight Dipole Antenna Gray, RP-TNC	146	19,0	2.774,00	832,20	1.941,8
AIR-ANT2506.	2.4 GHz, 5.2 dBi Mast Mount Omni Ant w/RP-TNC Connector	4	159,0	636,00	190,80	445,2
AIR-LAP1242AG-A-K9	802.11ag LWAPP AP Dual 2.4,5GHz RP-TNC FCC Cnfg	75	899,0	67.425,00	20.227,50	47.197,5
AIR-CT5508-50-K9	Cisco 5508 Series Wireless Controller for up to 100 APs	1	39.995,0	39.995,00	11.998,50	27.996,5
SF200-24P	Cisco 200 Series Smart Switches 24 puertos PoE	2	375	749,98	224,99	525
SG200-08P	Cisco 200 Series Smart Switches 8 puertos PoE	5	220	1.099,95	329,99	769,9
-	Mano de obra punto de red cat 5e	30	100,0	3.000,00	900,00	2.100,0
-	Mano de obra punto eléctrico	30	40,0	1.200,00	360,00	840,0
Total				**116.879,93**		**81.816**

Tabla 4.9 Presupuesto del Diseño propuesto de la Red *Wireless* del campus UCSG, opción 2

Fuente: Autores

Código	Descripción	#	P. Unit	Subtotal	Descuento	Total
AIR-ANT2506.	2.4 GHz, 5.2 dBi Mast Mount Omni Ant w/RP-TNC Connector	4	159,00	636,00	190,80	445,20
AIR-LAP1242AG-A-K9	802.11ag LWAPP AP Dual 2.4,5GHz RP-TNC FCC Cnfg	2	899,00	1.798,00	539,40	1.258,60
AIR-AP1131AG	802.11ag LWAPP AP Integrated Antennas FCC Cnfg	73	699,00	51.027,00	15.308,10	35.718,90
AIR-CT5508-50-K9	Cisco 5508 Series Wireless Controller for up to 100 APs	1	39.995,00	39.995,00	11.998,50	27.996,50
SF200-24P	Cisco 200 Series Smart Switches 24 puertos PoE	2	374,99	749,98	224,99	524,99
SG200-08P	Cisco 200 Series Smart Switches 8 puertos PoE	5	219,99	1.099,95	329,99	769,97
	Mano de obra punto de red cat 5e	30	100,00	3.000,00	900,00	2.100,00
	Mano de obra punto eléctrico	30	40,00	1.200,00	360,00	840,00
Total				**99.505,93**		**69.654,15**

Las opciones antes presentadas del presupuesto requerido para la implementación del diseño de red *wireless* corresponden a una oferta local realizada por un importador de la ciudad de Guayaquil, es decir que es el precio de los equipos necesarios entregados en el Ecuador.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Para el desarrollo de este trabajo de investigación se estableció la fundamentación teórica de las redes inalámbricas en el capítulo 3, abarcando la arquitectura en general, los componentes de *hardware* y *software.*

Se evaluó la red *wireless* del campus UCSG mediante las herramienta de monitoreo *Solarwinds Network Performance Monitor, Observer y Visiwave.* Luego del análisis realizado a la red se obtuvo el diagnóstico de la situación de la infraestructura inalámbrica en el campus de la UCSG, habiéndose detectado problemas que afectan su desempeño y calidad de servicio a los usuarios finales.

La interferencia entre canales de frecuencia de operación de los equipos *wireless* es uno de los factores que impide la transmisión de información de manera correcta. Es muy común instalar equipos AP o *routers* inalámbricos sin cambiar sus configuraciones por defecto, esto ocasiona que en la mayoría de los casos se ocasione la interferencia dado que dos equipos cercanos se encuentran operando en el mismo canal.

El equipamiento utilizado para la asignación de direccionamiento IP en las facultades no es el adecuado ya que acepta una cantidad limitada de conexiones, las cuales no son suficientes para cumplir con los requerimientos de los usuarios. Las capacidades limitadas de estos equipos se deben a que están destinados al uso en hogares principalmente, en donde no se espera una gran cantidad de usuarios simultáneos.

Existen zonas abiertas dentro del campus UCSG donde se encuentran grupos de usuarios que muchas veces no tienen acceso a la red *wireless* debido a la cobertura limitada que existe. Al existir áreas sociales que se encuentran fuera de las facultades

es necesario tomar en cuenta los requerimientos de cobertura a futuro en estos lugares.

En base a los resultados obtenidos se procedió a diseñar una nueva red WLAN que mejore la situación actual del acceso inalámbrico, utilizando tecnología cisco, la cual ofrece ventajas en la administración del equipamiento implementado por medio del uso de herramientas de gestión de redes, las cuales permiten conocer el estado de los equipos, resolver problemas rápidamente, aplicar configuraciones por medio del uso de *scripts*. De esta manera se logra mejorar notablemente la calidad de servicio y el tiempo de respuesta en caso de problemas de la infraestructura de la red.

Mediante las guías de diseño recomendadas por Cisco se puede obtener mejores resultados en el desarrollo e implementación de proyectos de redes. De igual forma haciendo uso de las prácticas recomendadas por cada tecnología, en *wireless* específicamente las consideraciones sobre canales de frecuencia son muy importantes.

El diseño propuesto se enfoca en la solución a los problemas determinados y la expansión de la cobertura de la red *wireless* actual.

En base al diseño propuesto se estableció un presupuesto para una futura implementación y se analizó la mejor propuesta económica para implementar una red que cubra el campus.

De esta manera se cumplió el objetivo general planteado en este trabajo que consistía en diseñar una red WLAN para ampliar la cobertura dentro del campus de la UCSG con equipos marca Cisco, para mejorar el acceso inalámbrico que es de gran utilidad para docentes y estudiantes.

Recomendaciones

Haciendo uso de las guías de diseño mencionadas en esta tesis se podrá obtener mejores resultados en el desarrollo e implementación de redes, es muy importante seguir un esquema para alcanzar el objetivo de manera eficaz y eficiente.

1. Se debe configurar adecuadamente los canales de frecuencia en los que operan los equipos inalámbricos y con mucho más cuidado cuando están juntos dentro de las facultades. Existe una manera efectiva de solucionar este problema y es utilizar una separación de 4 canales en los equipos en los que exista *overlap* de señales, por ejemplo: usar los canales 1 y 6 o 6 y 11.

2. Revisar las características técnicas de los equipos que otorgan las direcciones IP de los usuarios para comprobar que posean la capacidad de brindar las conexiones necesarias. Esto se comprueba con la cantidad de direcciones MAC que puede soportar el equipo.

3. El diseño sugiere 2 ubicaciones para ubicar equipos AP con la suficiente potencia en sus antenas para dar cobertura a las zonas abiertas en las que se encuentran concentrados los usuarios del campus UCSG.

4. Se recomienda un incremento del ancho de banda disponible para la red *wireless* del campus UCSG considerando por lo menos 2 Mbps por facultad a la que se presta el servicio, teniendo al final un ancho de banda de 14 Mbps disponibles para esta red.

GLOSARIO

WLAN (Wireless Local Area Network, Red de Área Local Inalámbrico)

UMTS (Universal Mobile Telecommunications System, Sistema Universal de Telecomunicaciones moviles)

ETSI (European Telecommunications Standards Institute, Instituto Europeo de Normas de Telecomunicaciones**)**

PYMES (pequeña y mediana empresa)

PDAs (Personal Digital Assistants, Asistente Digital Personal)

ITU-R (International Telecommunicacion Union- Radiocommunication Sector, Unión internacional de Telecomunicaciones -Sector Radiocomunicaciones).

IEEE (Institute of Electrical and Electronic Engineers, Instituto de Ingenieros Electricos y Electrónicos).

WECA (Wireless Ethernet Compatibility Alliance, Alianza de compatibilidad Ethernet Inalámbrica).

ISM (Industrial Scientific and Medical, Industrial Científica y Médica)

UNII (Unlicensed National Information Infrastructure**,** Infraestructura de Información Nacional Sin Licencia).

ADSL (Asymmetric Digital Subscriber Line, Línea de abonado digital asimétrica)

RF (Radio Frecuency, Radiofrecuencia)

IR (Infrared, Infrarrojas).

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance, Múltiple acceso por detección de portadora evitando colisiones.

HCF (Hybrid Coordination Function, Función de Coordinación Híbrida).

EDCA (Enhanced Distributed Channel Access, Función Mejorada de Distribución de Acceso al Canal).

HCCA, HCF (Controlled Channel Access, Función HCF de Control de Acceso al Canal).

QoS (Quality of Service, Calidad de Servicio).

OFDM (Orthogonal Frequency Division Multiplexing, Multiplexación por División de Frecuencias Ortogonales).

WPAN (Wireless Personal Area Network, Red Inalámbrica de Area Personal).

POS (Personal Operating Space, Espacio de Trabajo Personal)

VPN (Virtual Private Networks, Red Privada Virtual

FHSS (Frequency Hopping Spread Spectrum, Salto de Frecuencia de Espectro Ensanchado)

DSSS (Direct Sequence Spread Spectrum, El espectro ensanchado por secuencia directa)

AAA (Authentication Autorization and Accounting, Autenticación Autorización y Contabilización**).**

BSS (Basic Service Set, Grupo de Servicio Básico).

DS (Distribution System, Sistema de Distribución)

IBSS, Independent Basic Service Set, Grupo de Servicio Básic Independiente

SSID (Service Set Identifier, Identificador de conjunto de servicios.

MAC ("Medium Access Control" o Control de Acceso al Medio)

ACL (Access Control List, listas de control de acceso

WEP (Wired Equivalent Privacy, Privacidad Equivalente a Cableado).

DSL (Dynamic Security Link, Enlace de Seguridad Dinamico)

EAP (Extensible Authentication Protocol, Protocolo de Autenticación Extensible).

IPSec (Internet Protocol Security, Protocolo de Seguridad de Internet)

TKIP (Temporal Key Integrity Protocol, Protocolo de Integridad de Clave Temporal)

RSN (Robust Network Security, Red Segura Robusta)

DHCP (Dynamic Host Configuration Protocol, Protocolo Configuración Dinámica de Servidor**).**

PAN (Personal Area Network, Redes de Area Personal)

MAN (Metropolitan Area Network, Red de Area Metropolitana)

WAN (Wide Area Network, Red de Area Amplia)

MBWA (Mobile Broadband Wireless Access, Banda Ancha Inalambrica)

SNMP (Simple Network Management Protocol, Protocolo Simple de Administración de Red)

VLAN (Virtual Local Area Network, Red de área local virtual)

MAC (Medium Access Control, Control de Acceso al Medio),

CSMA (Carrier Sense Multiple Access, Acceso Múltiple por Detección de Portadora).

WECA (Wireless Ethernet Compatibility Alliance, Alianza de compatibilidad Ethernet Inalámbrica).

GPS (Global Positioning System, Sistema de Posicionamiento Global)

DHCP (Dynamic Host ConfigurationProtocol, protocolo de configuración dinámica de host)

BIBLIOGRAFIA

Unexpected, s. (s.f.). *solarwinds*. Recuperado el 10 de noviembre de 2012, de http://www.solarwinds.com/network-performance-monitor.aspx.

valencia, U. P. (02 de 12 de 2010). *Hstoria de la Informática*. Recuperado el 10 de noviembre de 2012, de http://histinf.blogs.upv.es/2010/12/02/historia-de-las-redes-inalambricas/

Visiwave. (2012). Recuperado el 10 de noviembre de 2012, de http://www.visiwave.com/

Cisco Systems. (2004). *Cisco at 20 years*. Recuperado el 24 de julio de 2012, de Cisco at 20 years: http://www.cisco.com/web/learning/netacad/cisco20/cisco20.html

Rodríguez, E. (24 de Diciembre de 2007). *Historia de Cisco*. Recuperado el 24 de Julio de 2012, de Historia de Cisco: http://www.maestrosdelweb.com/principiantes/historia-de-cisco/

Systems, C. (2010). *Designing Cisco Network Service Architectures.* San José, CA: Cisco Systems Learning.

Systems, C. (s.f.). *Enterprise Mobility 4.1 Design Guide*. Recuperado el 16 de noviembre de 2012, de Enterprise Mobility 4.1 Design Guide: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch2_Arch.html

Bluetooth Technology . (2008). Recuperado el 14 de Octubre de 2012, de http://www.bluetooth.com/Pages/Bluetooth-Home.aspx

COIT, G. d. (2008). La situación de las tecnologías WLAN basadas en el estándar IEEE 802.11 y sus variantes ("Wi-Fi"). España.

Guerrero, J. A. (Mayo de 2007). Redes Inalambricas Wireless LAN. Tesis de Grado . Hidalgo, Mexico: Universidad Autonoma del estado de Hidalgo.

IEEE. (2012). IEEE standards 802.11. Recuperado el 22 de Octubre de 2012, de http://www.ieee802.org/11/

Villacrés Ortiz, J. E. (2006). Estudio de la tecnologia UWB (Ultra Wide Band) en redes inalambricas de comunicaciones. Tesis de Grado . Sangolqui, Ecuador: ESPE.

Wi-Fi Alliance. (s.f.). Recuperado el 14 de octubre de 2012, de http://www.wi-fi.org

Yerovi, A. Y. (2010). Estudios de QoS sobre WLAN utilizando el estandar 802.11e aplicado a transmisiones de sistemas Multimediales en tiempo real. Tesis de Grado . Riobamba, Ecuador: ESPOCH.