



**FACULTAD DE INGENIERIA Y CIENCIAS AGROPECUARIAS
CARRERA DE SISTEMAS DE COMPUTACIÓN E INFORMÁTICA**

**ANÁLISIS Y DISEÑO DE UNA RED WIRELESS PARA LA
UNIVERSIDAD DE LAS AMÉRICAS CAMPUS PRINCIPAL – TORRE
CHILE UTILIZANDO LA TECNOLOGÍA WIRELESS SWITCHING**

Trabajo de Titulación presentado en conformidad a los requisitos establecidos
para optar por el título de Ingeniero de Sistemas

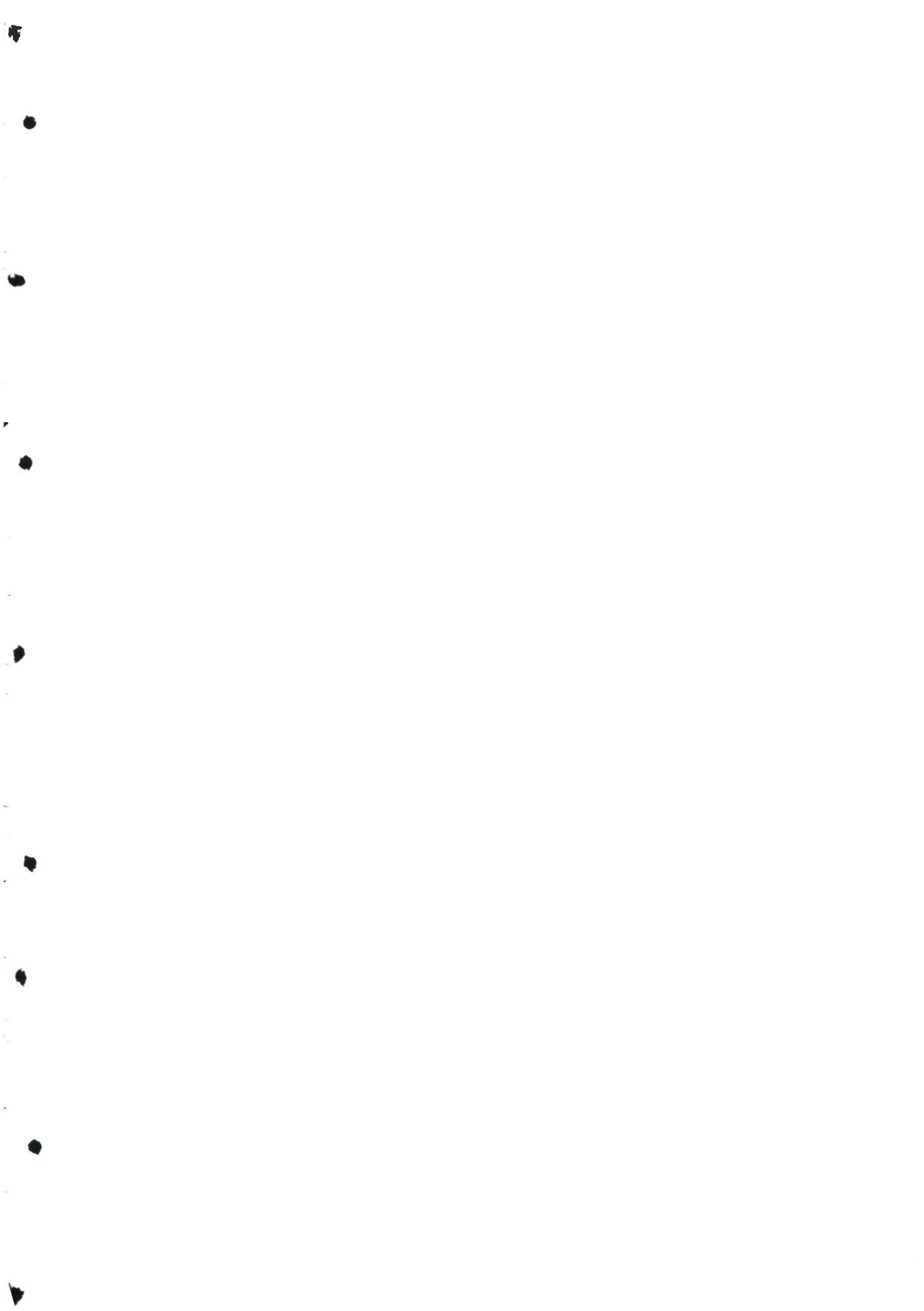
Profesor Guía:

Ingeniera Doris Yáñez

Autor:

David Segarra

2009



DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el/la estudiante, orientando sus conocimientos para un adecuado desarrollo del tema escogido, y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.”

Daniela

Nombre, Apellido

Título

Número Cédula

171205067-1

Ing. Electrónica y Telecomunicaciones

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”

David Segarra

Nombre, Apellido

Número Cédula

1714823976

AGRADECIMIENTO

A mis papás, Milton y Sonya,
por su apoyo incondicional
no solo en mi carrera sino
a lo largo de mi vida.

DEDICATORIA

A mis papás, Milton y Sonya,
y a mis abuelos, Alfredo y Gladys,
siempre los llevo en mi corazón.

RESUMEN

El trabajo presentado en esta tesis abarca en primera instancia una investigación de la actual red computacional inalámbrica de la Universidad de las Américas, campus Colón, ubicada en Quito - Ecuador, con el objetivo de evaluar, entre otros, su eficiencia y calidad, dos parámetros extremadamente importantes que una entidad educativa del prestigio de la UDLA debe cumplir a cabalidad, para satisfacer la demanda de comunicación y aumentar la productividad tanto de sus estudiantes como de su cuerpo docente y administrativo.

Al haberse obtenido como conclusión en base a la investigación realizada, que existe una falencia en las actuales condiciones de la red inalámbrica del Campus Colón, se plantea el segundo objetivo que es el realizar el análisis y diseño de una nueva red inalámbrica que cumpla con las métricas de las actuales redes inalámbricas, como son un ambiente gestionado y sobre todo seguro, estos parámetros otorgan un mejor nivel de servicio lo que se traduce en una ventaja para los usuarios y un mejor nivel de administración que a su vez representa una ventaja para los encargados de la red.

ABSTRACT

The work presented in this thesis includes first of all an investigation of the current computer wireless net of the University de las Americas, Colon campus, located in Quito, in Ecuador, with the purpose to evaluate, among others, its efficiency and quality, these are two extremely important parameters that an educational prestige entity of UDLA should totally complete in order to satisfy the communication demand and to increase the productivity of its students as much as of its educational and administrative body.

Obtaining the conclusion based on the investigation carried out that a default exists under the current conditions of the wireless net of the Colon Campus, the second objective is to carry out the analysis and design of a new wireless net that fulfils the metrics of the current wireless nets, such as a negotiated and mainly secure environment, these parameters grant a better service level that gives an advantage for the users and a better administration level which represents an advantage for those in charge of the net.

Tabla de Contenidos

Capítulo 1

1	Perfil del Proyecto	10
1.1	Introducción de la Universidad	10
1.1.1	Organización	10
1.2	Tecnología de la Universidad	11
1.2.1	Laboratorios y Equipos	11
1.2.2	Redes y Comunicaciones	12
1.2.3	Servicios.....	15
1.3	Necesidades Tecnológicas Actuales.....	16
1.4	Justificación	17

Capítulo 2

2	Redes Inalámbricas	20
2.1	Introducción	20
2.2	Historia de las redes inalámbricas	21
2.2.1	Definición	22
2.2.2	Propósito de las redes inalámbricas.....	23
2.2.3	Evolución.....	24
2.2.4	Ventajas de las Redes Inalámbricas	25
2.2.5	Desventajas de las Redes Inalámbricas	26
2.3	Estándares Existentes.....	27
2.3.1	IEEE 802.11	28
2.3.2	IEEE 802.11b.....	28
2.3.3	IEEE 802.11a.....	28
2.3.4	IEEE 802.11g.....	29
2.3.5	IEEE 802.11n.....	30
2.3.6	Otros Estándares	30
2.3.7	WiMAX	32
2.4	Hardware o Dispositivos de red	33

2.4.1	Dispositivos del lado del cliente.....	33
2.4.2	Dispositivos de la WLAN	36
2.5	Topologías de Redes Inalámbricas.....	39
2.5.1	Topología de Infraestructura Básica.....	39
2.5.2	Topología de Infraestructura Extendida	40
2.5.3	Topología Ad-hoc.....	40
2.6	Seguridad en WLAN.....	41
2.6.1	Tipos de amenazas.....	41
2.6.2	Mecanismos de Seguridad	42
2.6.3	Estándares de Seguridad en WLAN.....	44
2.6.4	VPN.....	48
2.6.5	VLAN.....	49
2.7	Nuevas Tecnologías Emergentes	50
2.7.1	<i>Wireless Lan Switching</i>	50

Capítulo 3

3	Análisis.....	54
3.1	Introducción.....	54
3.2	Análisis De La Situación Actual	54
3.2.1	Identificación De Servicios	55
3.2.2	Identificación De Aplicaciones	57
3.2.3	Infraestructura Física.....	57
3.2.4	Infraestructura Lógica	59
3.2.5	Ventajas Y Desventajas.....	60
3.3	Análisis de Requerimientos	61
3.3.1	Diseño De La Encuesta	61
3.3.2	Análisis de los Resultados.....	67
3.3.3	Requerimientos	74

Capítulo 4

4	Diseño de la Red Wlan	76
4.1	Requerimientos de Diseño	76
4.2	Selección de Tecnología y Productos	77
4.2.1	Selección de Estándar	77
4.2.2	Frecuencia y Velocidad de Transmisión.....	77
4.2.3	Throughput.....	78
4.2.4	Rango de Cobertura	79
4.2.5	Solución Wireless Switching	80
4.3	Ubicación de la Red	86
4.4	Densidad de Usuario	87
4.5	Consideraciones de Seguridad	87
4.5.1	Arquitectura.....	88
4.6	Interferencias.....	91
4.7	Pruebas	91
4.7.1	AP Patio (Bajos de la Torre Chile).....	92
4.7.2	AP Biblioteca.....	97
4.7.3	Ap Torre Chile.....	102
4.8	Diseño de la Solución.....	104
4.8.1	Puntos de Acceso	106
4.8.2	Equipo Gestión Centralizada	115
4.8.3	Servidor Radius Y De Base De Datos.....	115
4.9	Análisis de Costos	115
4.9.1	Equipos Activos	115
4.9.2	Sistema de Cableado Estructurado.....	115
4.9.3	Instalación y Configuración de Equipos Activos.....	116

Capítulo 5

5	Conclusiones Y Recomendaciones.....	117
5.1	Conclusiones.....	117
5.2	Recomendaciones.....	118

1 Perfil del Proyecto

1.1 Introducción de la Universidad

La Universidad de las Américas, UDLA, fundada en 1993 por un grupo de empresarios ecuatorianos y chilenos es hoy en día miembro de la más grande red privada de instituciones de educación superior, la Laureate International Universities¹, se encuentra ofreciendo sus servicios académicos en nuestro país capacitando a los futuros profesionales y líderes del Ecuador.

Actualmente cuenta con dos sedes, una en la Av. Colón y 6 de Diciembre, Campus Colón, fue el campus principal de la universidad en sus inicios, dado el su rápido crecimiento, en la actualidad la Universidad de las Américas se ha trasladado a su nueva sede Norte, ubicada en la avenida de los Granados, un sitio estratégico, de fácil acceso.

Es así como ahora, en el Campus Colón, el que hasta hace poco fue el campus principal, funciona todo lo referente a los Colegios de Tecnologías.

1.1.1 Organización

La UDLA, Universidad de las Américas, está constituida por una organización jerárquica, a la cabeza se encuentran el Rector, Vicerrector académico, Decano y el Coordinador Académico, para cada una de las diferentes especialidades que brinda la universidad, así mismo consta de docentes, estudiantes y personal administrativo.

La universidad consta de más de **4000** estudiantes, 3300 pertenecientes a pregrado, y 700 pertenecientes al colegio de tecnologías, así mismo la universidad ofrece posgrados y la posibilidad de cursar los diferentes

¹ Laureate International Universities: es una red de instituciones académicas privadas, acreditadas a través de varios países, que ofrece a los estudiantes un amplio rango de programas de educación superior

semestres en campus alrededor de América y el mundo en donde la universidad tiene sus sedes a través de la red Laureate.

1.2 Tecnología de la Universidad

La Universidad de las Américas cuenta con la más moderna tecnología en lo referente a plataforma informática y de comunicaciones, poniéndose a la par de las más prestigiosas universidades alrededor del mundo, no solo hace uso de esta tecnología para el mejoramiento y optimización de recursos y productividad, sino que la inversión realizada en este ámbito está encaminada al forjamiento de profesionales de la mejor calidad.

Además de todo lo mencionado, la Universidad de las Américas posee desde hace 2 años la Academia D-Link y actualmente se ha agregado la Academia Cisco, ofreciendo estas importantes certificaciones internacionales tanto para el público en general y con mayor razón para los estudiantes de Sistemas de la universidad convirtiéndose en la actualidad estas certificaciones como un “*must*”² para todo ingeniero o estudiante de carreras afines.

1.2.1 Laboratorios y Equipos

La Universidad de las Américas, en sus 2 sedes, Granados y Colón, consta de una moderna infraestructura en cuanto a tecnología. Posee además un muy organizado departamento de Tecnología el cual es el encargado de suministrar y administrar tanto los equipos como la logística y el conocimiento para echar a andar la plataforma informática que una universidad de la calidad de la UDLA posee, encargándose por supuesto de asignar, mantener y administrar computadoras, estaciones de trabajo y demás equipos y componentes que conforman dicha plataforma.

² Must: Expresión en idioma inglés que denota una necesidad.

En total la Universidad de las Américas tiene más de 700 estaciones de trabajo, 560 de las cuales se encuentran en su sede Granados distribuidos en 8 laboratorios de Pcs³, de 25 estaciones cada uno y 4 laboratorios Mac que en total suman 72 estaciones, además se tienen 100 estaciones más asignadas al personal administrativo además de una Pc por cada una de las aulas, estas suman 95 en total, también se cuenta con 24 estaciones en el área de biblioteca.

Por otro lado, en el campus Colón existen 5 laboratorios de Pcs, que suman alrededor de 80 estaciones de trabajo, además de 2 laboratorios de Mac que entre ellos suman 16 estaciones, existen 10 Pcs asignadas al personal administrativo, y 4 estaciones más para profesores, también hay 10 laptops en existencia para usos varios y se cuenta con 10 Pcs en el área de biblioteca, es decir un total de 140 estaciones de trabajo.

1.2.2 Redes y Comunicaciones

La Universidad de las Américas posee y hace uso de una Red de Área Local (LAN⁴) la cual soporta y provee diversos servicios a los diferentes usuarios, los más utilizados y relevantes son Internet, Correo Electrónico, servicios web y transferencia de datos.

La topología, que se adaptó a las necesidades de la universidad y que ahora se encuentra en uso, es la de Estrella, a su vez existe un enlace dedicado entre Granados y Colón de 2 Mbps por fibra óptica.

El MDF⁵ se encuentra ubicado en la sede Granados, y existe en la actualidad un IDF⁶ en la sede Colón ambos unidos con el enlace dedicado descrito anteriormente.

³ Pc: del Inglés, Personal Computer

⁴ LAN: del inglés, Local Area Network

⁵ MDF: del inglés, Main Distribution Facility

⁶ IDF: del inglés, Intermediate Distribution Facility

1.2.2.1 Tecnología de Red

La universidad de las Américas hace uso de la tecnología Ethernet en su red de área local, ya que brinda una alta velocidad en transmisión de datos, de hasta 100 mbps, el medio físico de transmisión es el cable utp categoría 5e.

1.2.2.2 Segmentación

La transmisión de los datos a través de los diversos puntos de la red de la universidad de las Américas esta a cargo de switches los cuales a su vez son los encargados de gestionar las diferentes Vlans (Virtual Local Area Networks) en las que la red se encuentra segmentada según las características o clasificación de los usuarios, basada en las funciones de los mismos.

1.2.2.3 Direccionamiento

Un controlador de dominio se encarga del direccionamiento y otorga a cada uno de los distintos equipos una dirección ip dinámica a través del servicio de DHCP⁷ (Dynamic Host Configuration Protocol), la dirección asignada es única para cada estación de trabajo o equipo de comunicación a lo largo de la universidad.

La universidad de las Américas posee y hace uso de seis direcciones públicas para lo que son sus servicios web, como son la pagina web de la universidad, consulta de notas, faltas, horarios, syllabus, etc. por parte de los estudiantes y también una interfaz web para registro de notas accedido por los profesores, todos estos servicios pueden ser accedidos desde el internet. El correo electrónico también hace uso de estas direcciones públicas.

⁷ DHCP: del inglés, Dynamic Host Configuration protocol

1.2.2.4 Equipos de Red

Por motivos de redundancia existen actualmente dos Proveedores de Servicios de Internet (ISP⁸) que llegan a las instalaciones de la Universidad de las Américas, campus Granados, los equipos de los ISPs se conectan a un ruteador⁹, este a su vez a la DMZ¹⁰, la DMZ se conecta con el servidor Isa que a su vez se conecta con el core principal, el switch¹¹ principal se conecta a su vez con el switch de cada piso, el medio físico con el que se conecta el switch de cada piso con cada tarjeta de red o NIC¹², que es la interface mediante la cual una estación de trabajo (Pc) se conecta con la red, es el cable UTP categoría 6A, capaz de transmitir hasta 1 Gbps¹³.

De manera similar, mediante un enlace dedicado de 2 Mbps¹⁴, mediante 2 Vlans¹⁵, una para Estudiantes y una para Administrativos, el campus Granados se enlaza con el campus Colón, llega a un ruteador, este a su vez a 2 switches capa 2, uno para estudiantes y otro para administrativos, este se conecta con los servidores DHCP y Active Directory¹⁶ que son réplicas de los ubicados en Granados, también hay un servidor de impresión. Los switches a su vez se conectan respectivamente con las NICS de las estaciones de trabajo dependiendo su función.

⁸ ISP: del inglés, Internet Service Provider

⁹ Ruteador: dispositivo de red que permite el enrutamiento de paquetes entre redes

¹⁰ DMZ: del inglés, Demilitarized Zone es la red localizada entre la red local y el Internet

¹¹ Switch: dispositivo de red para establecer interconexión de redes de computadoras

¹² NIC: del inglés, Network Interface Card

¹³ Gbps: Gigabit por segundo

¹⁴ Mbps: Megabits por segundo

¹⁵ Vlan: del Inglés, Virtual Lan

¹⁶ Active Directory: Implementación de Microsoft para su servicio de directorio de usuarios

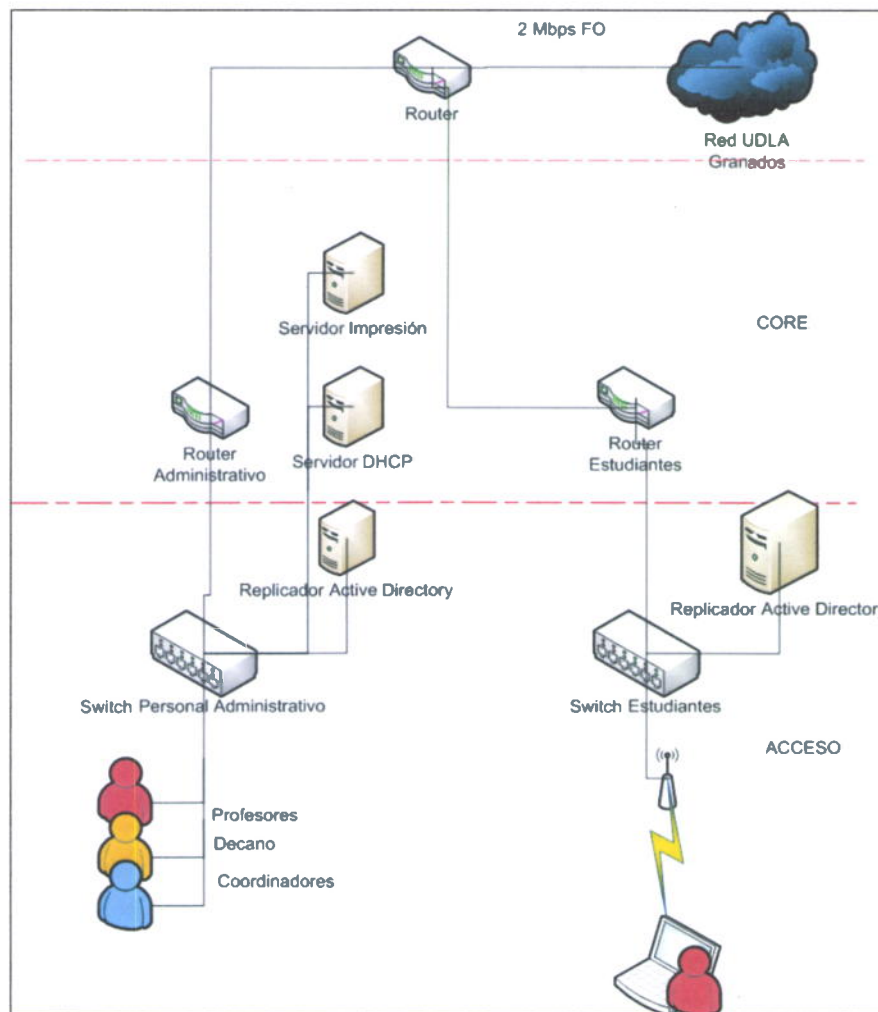


Figura 1- 1 Diagrama de Red UDLA Campus Colón

1.2.3 Servicios

Dado que la red de la universidad de las Américas se encuentra correctamente estructurada, todas las estaciones de trabajo están conectadas a la misma, razón por la cual pueden acceder a los diferentes servicios que la red ofrece, compartir información, aplicaciones, etc., de esta forma la red computacional de la universidad se vuelve una poderosa herramienta de trabajo para la optimización de recursos.

Entre los servicios que ofrece actualmente la red están los siguientes:

Cuota de disco duro, o espacio de almacenamiento, es espacio de disco duro en el servidor que tienen profesores y personal administrativo en donde pueden guardar y acceder a la información desde cualquier lugar de la lan.

Internet, en conformidad con las políticas de la Universidad, las diferentes estaciones de trabajo pueden o no tener salida a Internet, a su vez la utilización de este es controlado por medio de políticas de acceso al mismo.

ERP¹⁷ Académico, el SAES es el ERP que utiliza la universidad para el control académico, a este tienen acceso los profesores y personal administrativo dependiendo de su función.

Correo Electrónico, actualmente el correo electrónico está disponible para el personal docente y administrativo, en el futuro se implementará este servicio para los estudiantes.

1.3 Necesidades Tecnológicas Actuales

La universidad de las Américas, tuvo un crecimiento exponencial desde que empezó a prestar sus servicios en nuestro país, razón por la cual, fue escalando a la par en lo que a tecnología se refiere, sin embargo dadas las limitaciones físicas, desde octubre del 2008 la Universidad se trasladó a su campus Granados, en donde se tomaron en cuenta todas las necesidades tecnológicas actuales y futuras tomando en cuenta su constante crecimiento, por lo que está de más decir que el campus Granados no necesita, al menos por el momento, ninguna consideración en este sentido.

Por otro lado, el campus Colón, tiene una infraestructura actual muy sólida que daba servicio hasta mediados del año anterior a más de 4000 usuarios, y dado el traslado de la sede principal y mencionando que actualmente el campus Colón sirve a los diferentes colegios de tecnologías, el número de usuarios se redujo a una cuarta parte, es decir alrededor de 800 usuarios, por lo que la infraestructura actual de red es más que suficiente, sin embargo, el punto débil de esta infraestructura es su red inalámbrica, ya que no cubre por completo las instalaciones, razón por la cual se busca hacer el análisis y el diseño para mejorar y optimizar la actual red inalámbrica de la universidad.

¹⁷ ERP: del Inglés, Enterprise resource planning

1.4 Justificación

Varios son los factores que han llevado a la realización de este trabajo, el más importante es que la actual red inalámbrica de la universidad, específicamente del campus Colón, a pesar de que se encuentra sobre una sólida y bien estructurada red LAN, es muchas de las veces ineficiente y de escasa calidad, ofreciendo cobertura solamente en muy limitados espacios de la universidad, es por esto que se vuelve imperioso el estudio y diseño de una nueva red inalámbrica que haga uso de los estándares y tecnologías disponibles a la fecha, y que sobre todo, brinde servicio en todos los puntos del campus Colón, incluyendo por supuesto el interior de los diferentes cursos en donde la falta de señal se vuelve más evidente y necesaria.

Así mismo se hace evidente la cada vez mayor cantidad de usuarios de dispositivos móviles, entre los que tenemos computadores portátiles, pdas¹⁸, y en la actualidad hasta teléfonos celulares con la capacidad de unirse a redes inalámbricas WiFi¹⁹, todos estos dispositivos se convierten en una herramienta más productiva cuando se unen y comparten los servicios de la red, ya que ayudan también a la descongestión de los diferentes laboratorios de la universidad pudiendo los diferentes usuarios hacer uso de sus propios dispositivos portátiles desde cualquier punto de la universidad.

En la actualidad la necesidad de movilidad y accesibilidad a los servicios de red es muy alta, es por esto que una WLAN²⁰ o red inalámbrica, de alta calidad y cobertura es fundamental en un ambiente como el de una universidad, la nueva WLAN de la universidad de las Américas campus Colón, pretende dar un excelente servicio y cobertura tanto a estudiantes como a personal administrativo y docente haciendo uso de forma transparente de las nuevas tecnologías inalámbricas, utilizando los recursos y servicios de la LAN sin importar su ubicación física dentro de los límites de las instalaciones del

¹⁸ PDA: del Inglés, Personal Digital Assistant

¹⁹ WiFi: marca de la WiFi Alliance para certificar productos basados en el estándar 802.11

²⁰ WLAN: del inglés, Wireless LAN

campus Colón, manteniendo a todos los usuarios de esta localidad en continua comunicación.

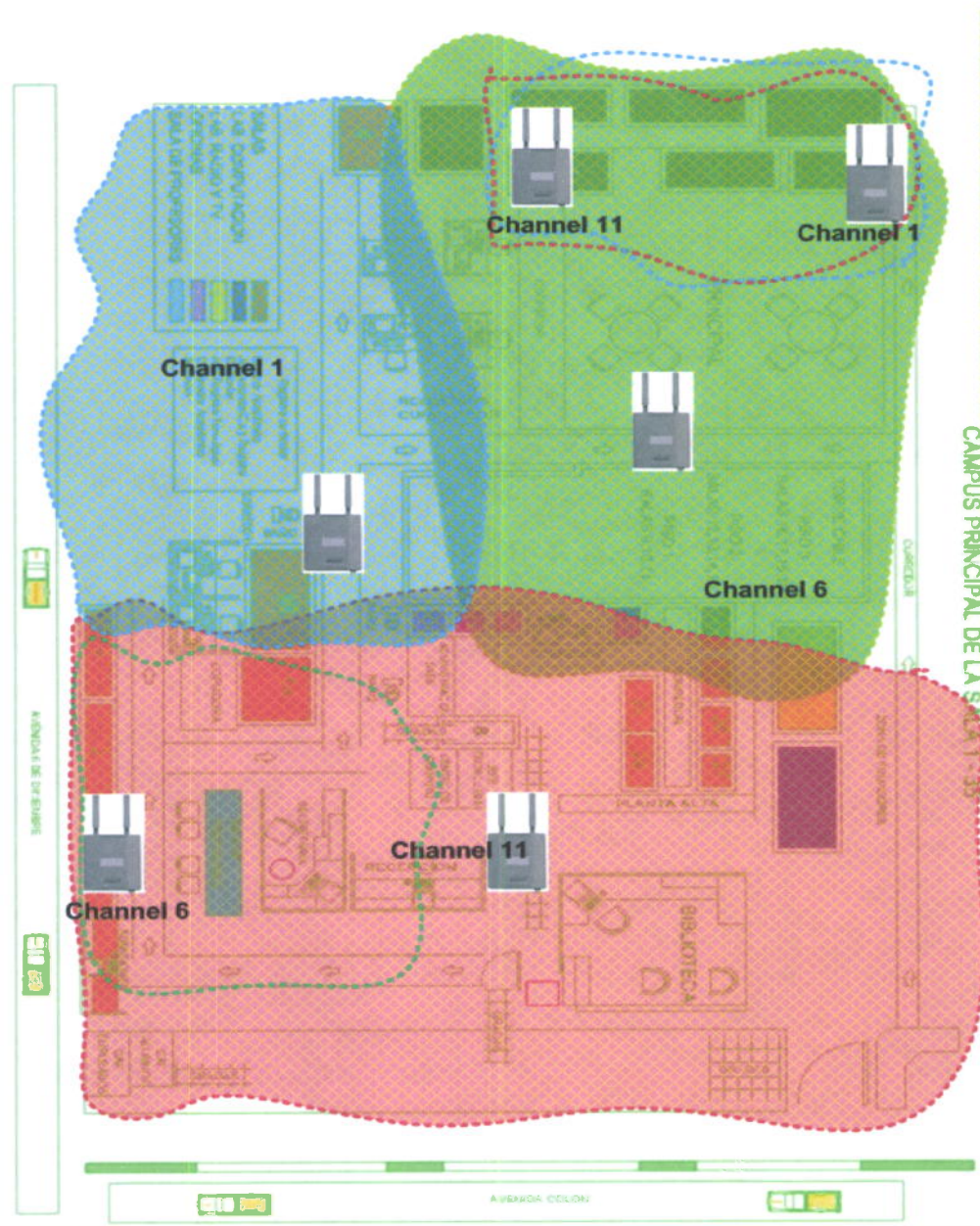


Figura 1- 2 Área de Cobertura de la Red Inalámbrica

El proyecto pretende abarcar en su totalidad las tres diferentes áreas del campus Colón, esto es el área o edificio Principal, la Torre Chile y el Anexo, para lo que se hará uso de los puntos de acceso y/o antenas necesarias para cubrir eficientemente todas las áreas.

La finalidad de este trabajo no es solamente la de hacer el diseño de la red inalámbrica del campus Colón de la Universidad de las Américas utilizando la

actual tecnología, es sobre todo buscar la mejor solución posible a un problema determinado haciendo uso de los conocimientos y competencias adquiridas a través de todos los años de carrera.

2 Redes Inalámbricas

2.1 Introducción

En los últimos años millones de usuarios de computadores personales, periféricos y tecnología informática en general han sido partícipes de la evolución y desarrollo de la tecnología, pasando desde enormes computadores sin capacidad de comunicación entre ellos, monitores monocromáticos, grandes y pesados cpus con muy bajas velocidades de procesamiento hasta las actuales computadoras portátiles o notebooks de increíble poder de procesamiento, monitores ultra brillantes con miles de millones de colores y múltiples dispositivos de comunicación incorporados.

Los avances han sido rápidos y hasta cierto punto impresionantes, ahora se recuerda con un poco de gracia y hasta nostalgia aquellos disquetes²¹ de 5 ¼ pulgadas en los cuales se intercambiaba juegos como Prince of Persia con los amigos y que se arrugaban fácilmente en las mochilas y luego los modernísimos en aquella época disquetes de 3 ½ pulgadas en los que al principio de la carrera se presentaban los deberes a los profesores, mismos que funcionaban solo un 50% de las veces, es por esto que a pesar de toda la rapidez de las actuales computadoras personales y la enorme cantidad de periféricos y otros adelantos computacionales que inundan el mercado, han sido 3 las tecnologías que han revolucionado la computación en sí, transformando a los sistemas de computo personal en toda una herramientas de comunicación, trabajo compartido, y hasta entretenimiento, estas 3 tecnologías son las redes LAN, la WLAN y la Internet.

Las redes de área local LAN suplieron la necesidad que se tenía de compartir información entre computadores, el increíble potencial de esta tecnología no tardo en generar la cantidad de servicios que ahora son parte de nuestra vida cotidiana, las redes WAN expandieron aun más estas posibilidades, el internet es ahora una herramienta básica, imprescindible de comunicación,

²¹ Disquete: Antiguo medio de almacenamiento con 1.2 o 1.4 Megabytes de capacidad

entretenimiento, información, comercio, es un sinónimo de globalización, pero la necesidad de movilidad siempre estuvo presente y la tecnología WLAN pudo satisfacer esta necesidad convirtiéndose en una de las más importantes tecnologías de la actualidad.

2.2 Historia de las redes inalámbricas

La historia de las redes inalámbricas como tales, se puede remontar al año 1971, fue desarrollada en sus inicios por la universidad de Hawaii, el propósito de la misma fue el de unir o enlazar 4 islas sin el uso de cables telefónicos, este primer sistema fue llamado ALOHANET y su velocidad de operación era de 9600 bits²² por segundo, a este sistema también se le considera como base de la tecnología de red de área local cableada o ethernet²³. Sin embargo los inicios o bases se pueden remontar hace mas de cien años, cuando Guglielmo Marconi, físico e inventor italiano, fue el primero en transmitir con éxito ondas de radio.

En los años 80 empezaron a utilizarse redes inalámbricas para el intercambio de información entre computadores, estas primeras redes inalámbricas utilizaban la tecnología de transmisores y receptores de infrarrojo, no tuvieron éxito ya que se requería siempre un paso directo o vista directa entre el receptor y el trasmisor debido a que el infrarrojo no atraviesa objetos sólidos, además de que el ancho de banda es muy bajo.

A principios de los años 90 se empieza a usar la radio frecuencia para crear redes inalámbricas, ya que finalmente el poder de procesamiento de los chips era el suficiente para poder gestionar la información transmitida, sin embargo los componentes para crear estas redes eran marcas propietarias y no existía compatibilidad entre ellas, es decir no se podían comunicar unas con otras.

²² Bit: Acrónimo de Binary Digit es un dígito del sistema de numeración binario.

²³ Ethernet: Estándar de redes de computadoras IEEE 802.3

A mediados de los 90 nace el estándar IEEE²⁴ 802.11 que es el estándar para las comunicaciones inalámbricas. El estándar es ratificado en 1997, luego de 6 años de estar en proceso de creación .

Para este entonces la comunicaciones eran lentas, el estándar 802.11 proporcionaba velocidades de entre 1 y 2 megabits por segundo (Mbps) y un cifrado rudimentario llamado WEP²⁵ o Privacidad Equivalente al Cableado, trabajaba en la banda de los 2.4 Ghz²⁶.

En el año 1999 aparece el estándar 802.11b, la diferencia es que la velocidad se incrementa a los 11Mbps.

En julio de 1999 Macintosh pone al alcance de la mano de usuarios comunes y público en general su tecnología inalámbrica bautizándola como Airport y utilizando el estándar IEEE 802.11b, consistía en una tarjeta de red inalámbrica que podía ser conectada en varios modelos de computadores Macintosh valorada en aquel entonces en 100 usd, y un punto de acceso (AP²⁷), llamado Estación Base AirPort valorado en 300 usd. Les tomó más de un año poder llegar a esos precios al resto de fabricantes de dispositivos inalámbricos.

2.2.1 Definición

Las redes inalámbricas o WLAN son redes cuya principal característica es la de formar una LAN o ser parte de una LAN sin el uso de cables.

En la actualidad tanto computadoras de escritorio como computadoras portátiles y varios otros dispositivos portátiles pueden acceder a las WLANs por medio de una tarjeta inalámbrica que a su vez se comunica con los diferentes dispositivos de red inalámbricos.

²⁴ IEEE: del Inglés, Institute of Electrical and Electronics Engineers

²⁵ WEP: del Inglés, Wired Equivalent Privacy

²⁶ Ghz: Giga hertz, 1000 hertz que es la unidad de frecuencia del Sistema Internacional de Unidades

²⁷ AP: del Inglés, Access Point

2.2.2 Propósito de las redes inalámbricas

Las WLANs o redes inalámbricas tienen un sinnúmero de aplicaciones, uno de los más comunes es simplemente el de ampliar o expandir, en términos de usuarios, las redes LAN actuales, ya que muchas de las veces las redes LAN cableadas tienen algunas limitantes, como el alto costo del cableado, y en algunos casos, como el de edificios históricos, la prohibición de tendido de cableado externo. El propósito más importante que es el de simplemente brindar movilidad a los usuarios. Por todas estas razones es que las redes inalámbricas constituyen una solución fácil y rápida para solventar este tipo de situaciones.

Las WLAN constituyen la forma más conveniente de unir dos LANs en un área metropolitana, es decir, redes que se encuentren a varios kilómetros de distancia, haciendo uso de antenas, lo que siempre resulta más conveniente y económico que el uso de cableado.

En una infraestructura de red ya establecida, se convierte en el método más sencillo y económico de agregar nuevos usuarios a la red, ya sean estos usuarios de pcs de escritorios o de computadores portátiles, ya que en la actualidad pueden adquirirse tarjetas de red inalámbricas para ambas arquitecturas.

Las redes inalámbricas pueden ser implementadas en cualquier tipo de ambientes o lugares de trabajos, las encontramos a diario en nuestros hogares, oficinas, empresas, universidades, etc., también en sitios públicos como aeropuertos, restaurantes y en nuestro medio ya hay algunos "HotSpots" que no son más que lugares o sitios públicos en donde uno puede hacer uso del internet en forma gratuita por medio de la tecnología inalámbrica. Las redes inalámbricas pueden cubrir áreas tan pequeñas como un solo cuarto hasta varios kilómetros cuadrados usando varios *Acces Points* en modo "overlapping"²⁸.

²⁸ Overlapping: Modo en que dos o mas AP's pueden sobreponer su señal sin que haya interferencia

Las actuales tecnologías están poco a poco logrando que las velocidades de transmisión de datos lleguen a las mismas velocidades de las redes cableadas, con la ventaja de no estar físicamente atado a las mismas, además de que satisfacen rápida y eficazmente el aumento en la demanda de usuarios de una red dada.

2.2.3 Evolución

En el año de 1999 se unen dos grandes empresas, Nokia y Symbol Technologies para crear la WECA²⁹, Alianza de Compatibilidad Ethernet Inalámbrica, para el año 2003 esta organización cambio su nombre a Wi-Fi Alliance. La finalidad de esta organización era la de crear una marca o nombre de producto que sea un estándar en la industria de los equipos inalámbricos, y sobre todo que garantice la compatibilidad entre los fabricantes de equipos de tecnología inalámbrica.

Para el año 2000 la hasta ese entonces llamada WECA certifica el estándar 802.11b bajo el nombre de marca "Wi-Fi" para garantizar la interoperabilidad de equipos. Esto significa que todos los equipos que tenían el sello de "Wi-Fi" tenían la garantía de que trabajaran unos con otros sin ningún tipo de problema a pesar de que estos equipos sean de fabricantes diferentes. Entre algunos de las compañías que apoyan al estándar están Nokia, 3Com, Apple Computer, Cisco Systems, Dlink. En la actualidad suman más de 150 compañías.

Haciendo una analogía, Wi-Fi es el término que se acuñó para las redes inalámbricas así como es Ethernet para las redes LAN, resulta mucho más sencillo hablar de una red Wi-Fi que de una red IEEE 802.11 o de una red Ethernet en lugar de una red IEEE 802.3.

Además hay que tomar en cuenta que la única diferencia que existe entre una red Ethernet y una red Wi-Fi es la forma en que transmiten las tramas³⁰, es por esta razón que una red inalámbrica 802.11 es totalmente compatible con una

²⁹ WECA: del Inglés, Wireless Ethernet Compatibility Alliance

³⁰ Trama: Trama de red es una unidad de envío de datos, o lo que es lo mismo un paquete de datos.

red 802.3 o Ethernet, lo que a su vez garantiza que todos los servicios de las redes LAN pueden ser utilizados en una red WLAN.

2.2.4 Ventajas de las redes inalámbricas

Las redes Inalámbricas tienen una serie de ventajas entre las que podemos mencionar las siguientes:

Las redes inalámbricas son de fácil instalación, en el sentido de que no se necesitan sino pocos elementos de red, en el más simple de los casos con solamente 2 computadoras equipadas con sus respectivas NICs³¹ inalámbricas podemos formar una red. Esto nos ayuda a compartir archivos de una manera sencilla.

Las redes inalámbricas son de rápida instalación, al igual que en el punto anterior con una WLAN los tiempos de puesta en marcha son mucho menores, ya que no tenemos que estar pensando en diversos factores como por ejemplo el cableado y todas las molestias que conlleva.

Las redes inalámbricas casi siempre generan muchos menores costos y menos recursos en cuanto a personal técnico que las redes convencionales, ya que no incurrimos en elementos como cableado, el mismo que hasta la fecha tiene un costo relativamente elevado.

Las redes inalámbricas tienen un punto fuerte que es la escalabilidad, ya que simplemente con una rápida configuración podemos agregar usuarios a nuestra red, siempre y cuando sus dispositivos tengan tarjetas de red inalámbricas. Al contrario, con una LAN siempre dependemos de los puntos de red habilitados que a su vez dependen de los uno o más switches de los que se encuentre conformada la red.

Otra de las ventajas de las redes inalámbricas es la movilidad que otorgan al usuario, ya que rompen con el esquema de estar físicamente atado a la red

³¹ NIC: del Inglés, Network Interface Card

mediante un medio físico que viene a ser el cable y estar por tanto siempre en un lugar estático.

También otorgan mucha mayor disponibilidad de la red, ya que puede hacerse uso de los varios dispositivos personales para acceder a la red, como laptops, netbooks, pdas, teléfonos celulares con capacidades WiFi, etc.

Todas estas ventajas han contribuido tanto para brindar una mayor comodidad al usuario como para satisfacer necesidades existentes que a su vez contribuyen con un aumento de la productividad de las empresas, ya que el uso de las WLANS puede ayudar a realizar tareas que antes resultaban muy difíciles.

2.2.5 Desventajas de las redes inalámbricas

El primer y más grande punto a tratarse en cuanto a las desventajas de esta tecnología es la seguridad, ya que al no tener que estar físicamente conectado a la red, un usuario malintencionado puede tener acceso a la misma desde cualquier lugar tanto dentro como fuera de la organización o del sitio en donde se encuentre implementada la red inalámbrica.

En algunos casos la velocidad es considerada como una desventaja, pero en la actualidad con el estándar IEEE 802.11n que se encuentra en borrador, se trata de alcanzar velocidades de hasta 108 Mbps, teóricamente, lo que llegaría a igualar la velocidad de las redes IEEE 802.3 100 base t, aunque no de las LAN Gigabit Ethernet que están empezando a popularizarse, y que como su nombre lo indica alcanzan velocidades de hasta mil Mbps. Sin embargo hay que tomar siempre en cuenta que en el caso de las redes inalámbricas esta velocidad de transmisión es teórica y depende de muchos factores entre ellos el número de usuarios que se encuentren conectados a un ruteador o acces point y que hagan uso concurrente de la misma, es decir que se encuentren transmitiendo información simultáneamente.

Con respecto a este tema también hay que considerar que muchas de las aplicaciones para las que se hace uso de las redes inalámbricas no requieren de un extremadamente grande ancho de banda, ya que para servicios como internet, correo electrónico, video conferencia y hasta juegos en línea, las redes inalámbricas de 54 mbps cubren perfectamente estas necesidades, por lo que la velocidad se convierte en una desventaja solo en algunos escenarios específicos, como por ejemplo el de intercambio masivo de información.

Otra de las desventajas de las redes inalámbricas es que al trabajar por medio de las radio frecuencias y las mismas viajar por el aire, estas son muy susceptibles a la interferencia que puede ser provocada por cualquier equipo eléctrico que se encuentre cerca de las fuentes de trasmisión o recepción o en el camino de las mismas, esta interferencia se ocasiona cuando estos equipos se encuentran operando a la misma frecuencia que la red Wi-fi.

2.3 Estándares existentes

Como es evidente los estándares han ayudado a lograr el rápido desarrollo de la industria en general y por su puesto en nuestro caso específico de las redes inalámbricas al garantizar la compatibilidad entre todos los fabricantes de dispositivos, esto a su vez ha producido que los costos sean cada vez más asequibles y por supuesto que cada vez mas usuarios hagan uso de esta tecnología en prácticamente cualquier área.

IEEE es el Instituto de Ingenieros Eléctricos y Electrónicos, está compuesta por más de 350.000 miembros entre estudiantes y profesionales de más de 35 países, y es la institución que se encarga de crear, desarrollar y poner al servicio de desarrolladores de tecnología y fabricantes los distintos estándares en la industria de la ingeniería eléctrica, las comunicaciones, computación y demás disciplinas electrónicas.

Cuando hablamos del término IEEE 802 nos referimos en concreto a las redes computacionales en forma general, y cuando hablamos del término IEEE

802.11 estamos ya refiriéndonos en concreto a las redes inalámbricas o tecnología Wi-Fi.

Aquí se trataran todos los estándares que se han producido hasta el día de hoy.

2.3.1 IEEE 802.11

Como se mencionó anteriormente, el estándar IEEE 802.11 fue introducido a principios de los años 90 y ratificado en el año 1997 convirtiéndose en el primer estándar de WLAN, sus principales características son que trabajaba en la banda de los 2.4 Ghz, a velocidades de 1 a 2 mbps.

2.3.2 IEEE 802.11b

El estándar 802.11b es una expansión del estándar 802.11 y fue introducido en julio de 1999, la mayor diferencia de este es que alcanza una velocidad de transferencia de datos de hasta 11 mbps vs los 2 mbps del estándar original. El estándar 802.11 b trabaja de igual manera en la banda de los 2.4 Ghz.

Un dato importante es que al trabajar en los 2.4 Ghz, algunos electrodomésticos que trabajan en el mismo rango de frecuencias como el microondas o los teléfonos inalámbricos pueden crear interferencias, sin embargo la solución a este problema no es otra que el tenerlos a una considerable distancia entre ellos.

2.3.3 IEEE 802.11a

El estándar 802.11a es una segunda extensión del estándar original 802.11, fue desarrollado al mismo tiempo que el estándar 802.11b, difieren el uno del otro en 2 aspectos fundamentales, el estándar IEEE 802.11a alcanza velocidades de hasta 54 mbps, 5 veces más rápido que el estándar b, además

trabaja en la frecuencia de los 5 Ghz. Esto último acarrea tanto ventajas como desventajas, la principal ventaja como se ha visto ya es que alcanza una velocidad mucho mayor, además no existe tanta interferencia como en la frecuencia de los 2.4 Ghz, la desventaja principal es que al trabajar en los 5 Ghz, el rango de alcance o distancia que puede existir entre dispositivos es mucho menor, la diferencia es bastante notable, hablamos de 90 m aproximadamente en línea de vista del estándar b vs 20 m aproximadamente en línea de vista del estándar a. El estándar 802.11 a fue ratificado en el año 2002 y un punto importante es que no existe interoperabilidad entre estos dos estándares.

A pesar de haber sido desarrollados al mismo tiempo, el estándar IEEE 802.11 a fue menos popular dado sus elevados precios con respecto al estándar b, esto también provocó que se haga una diferencia o especialización entre ellos, de tal forma se tomó al estándar a como el ideal para empresas u oficinas y el estándar b el ideal para el uso en el hogar.

2.3.4 IEEE 802.11g

En el año 2002 y 2003 aparece un nuevo estándar que trata de combinar los anteriores a y b en uno solo, se trata del estándar IEEE 802.11g, esta vez alcanza una velocidad de 54 mbps y trabaja en el rango de los 2.4 Ghz para tener un mayor alcance. Además es compatible con el estándar b, lo que significa que un *acces point* que soporta la norma g puede trabajar sin problemas con tarjetas o NICs inalámbricas que trabajen en la norma b y viceversa.

Al trabajar en la banda de los 2.4 Ghz los aparatos eléctricos como teléfonos y microondas pueden causar interferencias.

2.3.5 IEEE 802.11n

Es el estándar más nuevo que existe actualmente, aunque la realidad es que aun sigue en borradores, está diseñado para mejorar el estándar g aumentando el ancho de banda o velocidad de transmisión de datos a 100 mbps o más, esto lo realiza mediante el uso de múltiples señales y antenas, llamada tecnología MIMO³², trabaja tanto en la banda de los 2.4 como la de los 5 ghz.

Cuando se encuentre finalizado el estándar además de ofrecer mayor velocidad de transmisión también tendrá un mejor rango de señal o alcance debido a su intensidad de señal, además se espera que su señal sea más resistente a la interferencia proveniente de fuentes exteriores y por su puesto será compatible con el estándar g y el a.

A la fecha, ya se encuentran a la venta tanto ruteadores inalámbricos como computadores portátiles equipados con Nics que ya soportan el estándar n.

2.3.6 Otros estándares

Existen algunas variantes del estándar 802.11, tales como:

802.11c

El estándar 802.11 c fue luego introducido como un suplemento del estándar d, este estándar cumple con el propósito de hacer operaciones de "bridging" o enlace entre bridges³³ o puentes inalámbricos o entre APs mediante la capa MAC del modelo OSI.

802.11d

El estándar 802.11d es también llamado "Estándar de Armonización Global" y es usado en países donde otros estándares de la familia 802.11 no están permitidos operar, es decir, fue concebido para permitir la interoperabilidad

³² MIMO: del Inglés, multiple-input and multiple-output

³³ Bridge: dispositivo de interconexión de redes de computadores que conecta dos segmentos de red.

entre distintos dispositivos permitiendo que intercambien información en rangos de frecuencia que permita el país de origen del dispositivo.

802.11e

El estándar 802.11e es una mejora significativa del estándar 802.11 ya que añade una característica llamada QoS³⁴ o Calidad de Servicio, esta función permite dar preferencia a aplicaciones que requieran transmitir información en tiempo real, como son la voz sobre ip o video sobre ip.

802.11f

El estándar 802.11f es una recomendación para los fabricantes de puntos de acceso inalámbricos, con el fin de que exista interoperabilidad entre puntos de acceso de distintos fabricantes, a su vez esto permite que un usuario en movimiento pueda cambiar de punto en acceso mientras se encuentra en movimiento a pesar de que estos APs sean de marcas diferentes.

802.11h

El estándar 802.11h cumple con el objetivo de crear interoperabilidad entre el estándar 802.11 y el estándar "Hiperlan 2" creado en Europa, en la actualidad no sirve exclusivamente para las regulaciones Europeas sino para otros países, uno de sus principales características es la de asegurar que la energía promedio sea la menor posible para reducir la interferencia con las comunicaciones satelitales y de radares.

802.11i

El protocolo 802.11i es básicamente una implementación de seguridad al protocolo 802.11 original, este estándar fue ratificado en junio del 2004 y hace una mejora a la seguridad WEP, que para ese entonces tenía muchas debilidades, reemplazándola por WPA2³⁵ que hace uso del cifrado AES³⁶.

³⁴ QoS: del Inglés, Quality of Service

³⁵ WPA2: del Inglés, Wi-Fi protected Acces o Acceso Protegido a Wi-Fi

³⁶ AES: del Inglés, Advanced Encryption Standard

802.11j

El estándar 802.11j es básicamente lo que el estándar 802.11h es para el mercado Japonés, trabaja al igual que el estándar h en la banda de los 5 Ghz y también en los 4.9 Ghz.

802.11k

El estándar 802.11k es otra mejora al estándar original, en este caso se trata de la administración o gestión de los recursos de radio, define y muestra la información de la red inalámbrica sobre todo los recursos de radio frecuencia para mejorar su funcionamiento en base a la carga o tráfico que está soportando un AP específico, para ponerlo más claro, un dispositivo inalámbrico o terminal como una computadora portátil se conecta al AP geográficamente más cercano ya que recibirá una mejor señal, sin embargo puede darse el caso de que este AP esté saturado de clientes, esta norma ayuda a que el nuevo cliente se conecte a algún otro AP que aunque no tenga tan buena señal como el primero brindará un mejor servicio no solo al nuevo cliente sino a toda la red inalámbrica ya que se estarían manejando más eficientemente los recursos de la red.

2.3.7 WiMAX

Wimax³⁷ o Interoperabilidad mundial para acceso por microondas es una tecnología inalámbrica con el potencial de reemplazar infraestructuras de telecomunicaciones existentes tales como los tendidos de cable de cobre de las compañías de telefonía así como también los tendidos de cable coaxial de las compañías de cable.

Wimax es definido como una acceso inalámbrico de banda ancha de última milla o BWA (*Broadband Wireless Acces*) por sus siglas en Inglés, queriendo ser una alternativa a las compañías de internet que proveen servicios por medio de cable modem o por DSL (*Digital Subscriber Line*).

³⁷ Wimax: del Inglés, *Worldwide Interoperability for Microwave Acces*

Wimax provee un servicio que no requiere línea de vista NLOS (No line of sight) y se extiende desde una estación base hasta una estación subscriptora, también llamada CPE por sus siglas en Inglés, o Customer Premise Equipment.

La infraestructura de Wimax es muy similar a la de las compañías de telefonía celular, haciendo uso de una estación base que da servicio a varios cientos de usuarios a un promedio de 80 kilómetros a la redonda, esto significa que el usuario está siendo parte de una sola gran red por lo que algunos opinan que esto puede ocasionar problemas de seguridad. Se debe pagar una suscripción mensual para recibir el servicio.

Tabla 2- 1 Comparativa Wi-Fi vs WiMAX

Características	Wi-Fi	WiMAX
Área de Cobertura	100 – 300 metros	30 – 40 kilómetros
Velocidad transferencia	Hasta 54 mbps (108 mbps teóricos)	72 mbps
Frecuencia	2.4 – 5 ghz	2.5 – 11 Ghz
Ventaja	Precio	Velocidad y Cobertura

2.4 Hardware o dispositivos de red

Como en toda infraestructura informática, en una red inalámbrica existen varios dispositivos que cumplen con tareas específicas dentro de la misma, como son los dispositivos del lado del cliente, Nics, *bridges* o puentes, *acces points* o puntos de acceso, entre otros.

2.4.1 Dispositivos del lado del cliente

Los dispositivos del lado del cliente como su nombre lo indica son todos los dispositivos de hardware de los que el cliente o usuario utiliza para unirse y hacer uso de los recursos de una red inalámbrica, existen varios tipos de acuerdo a su función.

2.4.1.1 Estaciones de trabajo

Las estaciones de trabajo son las computadoras que facilitan a los usuarios el acceso a los recursos de red, es decir, que están conectadas a la red, la diferencia entre una computadora aislada y una estación de trabajo es que la última posee una tarjeta de red o NIC.

Las dos principales estaciones de trabajo son las siguientes: Pcs de escritorio y laptops/netbooks. En la actualidad las Pcs de escritorio pueden convertirse rápidamente en estaciones de trabajo inalámbricas gracias a las tarjetas de red o NICs PCI³⁸ que son dispositivos internos, van conectados a una ranura PCI de la computadora, a su vez hay otro tipo de adaptadores USB que cumplen con el mismo objetivo, pero en este caso es un dispositivo externo.

Las laptops o computadoras portátiles hace unos años requerían de un adaptador PCMCIA³⁹, en la actualidad tanto laptops como netbooks vienen con su NIC inalámbrica integrada.

2.4.1.2 Nics inalámbricas

Una NIC (Network Interface Card) o Tarjeta de interface de red es el dispositivo que hace la función de conectarse con un punto de acceso, router inalámbrico u otro dispositivo de la red inalámbrica, al ser tarjetas inalámbricas hacen uso de la radio frecuencia en vez del cable utp⁴⁰ o cualquier otro tipo de medio.

Existen varios tipos de Nics Inalámbricas tanto para computadores de escritorio como para laptops. Desde el apareamiento de la tecnología Intel Centrino⁴¹ para computadoras portátiles, las tarjetas de red inalámbricas forman parte de

³⁸ PCI: del Inglés, Peripheral Component Interconnect o Interconexión de Componentes Periféricos

³⁹ PCMCIA: del Inglés, Personal Computer Memory Card International Association

⁴⁰ UTP: del Inglés, Unshielded Twisted Pair

⁴¹ Centrino: Plataforma Intel que consta de procesador, chipset y red inalámbrica

su arquitectura, se goza de esta tecnología desde el año 2003. A continuación una breve descripción de ellas:

Tarjeta interna PCI *Wireless*, como se mencionaba anteriormente, esta tarjeta sirve para poder transformar en estación de trabajo a una computadora de escritorio, es una tarjeta interna.

Tarjetas PCMCIA y ExpressCard⁴², la función de estas tarjetas es la de agregar hardware en computadoras portátiles, en este caso específico agregar una NIC Inalámbrica. La función de estos dos tipos diferentes de tarjetas es el mismo, la diferencia es que la ExpressCard reemplazó a la PCMCIA, es decir, los modelos de laptops antiguos venían con la tecnología PCMCIA y los modernos con ExpressCard.

Adaptador USB *Wireless*, es una solución externa tanto para computadoras de mesa como para computadores portátiles, tan solo debemos conectar el adaptador a un puerto usb⁴³ libre del computador y automáticamente se iniciará la instalación del mismo.

Adaptador Ethernet inalámbrico, es un aparato que puede funcionar tanto en computadores como en cualquier otro dispositivo que posea un conector Ethernet, el adaptador se conecta al dispositivo por medio de cable utp, convirtiéndose así en un dispositivo inalámbrico, sirve para cualquier dispositivo que tenga un puerto Ethernet, como impresoras, faxes y hasta consolas de video juegos.

2.4.1.3 Otros dispositivos

En la actualidad disponemos de una serie de dispositivos móviles que son capaces de unirse a la red inalámbrica y hacer uso de sus recursos sobre todo de la Internet, a continuación enumeramos algunos:

⁴² ExpressCard: Estándar de hardware que reemplaza las tarjetas PCMCIA

⁴³ USB: del Inglés, Universal Serial Bus

- Pdas⁴⁴ o Asistente Personal Digital, también conocidos como “Palms”
- *Smartphones*, o teléfonos inteligentes, son básicamente una palm con función de teléfono celular integrado.
- Teléfonos celulares con capacidad Wi-Fi, son teléfonos que a pesar de no entrar en la categoría de *smartphones* pueden tener acceso a la red.

2.4.2 Dispositivos de la WLAN

Los dispositivos de la WLAN son los aparatos que harán posible la comunicación entre los dispositivos del lado del cliente y la red o a su vez harán posible la creación de una infraestructura de red inalámbrica.

2.4.2.1 Punto de acceso

Los puntos de accesos también llamados Ap's por sus siglas en Inglés (Access Points) son dispositivos de hardware cuya función es la de hacer de intermediarios o de permitir y gestionar el tráfico de información entre un cliente inalámbrico y la LAN o red local. Dentro de una infraestructura de red inalámbrica pueden haber uno o más puntos de acceso dependiendo del número de clientes o de la distancia que se quiera cubrir, cada punto de acceso crea de esta forma un área de cobertura o celda.

2.4.2.2 Ruteador inalámbrico

Un ruteador inalámbrico no es mas que un punto de acceso con algunas características avanzadas añadidas, las principales sus funciones de ruteador y de firewall, en los actuales modelos existe la posibilidad de que un ruteador pueda actuar exclusivamente como punto de acceso.

⁴⁴ Pda: del Inglés, personal digital assistant

2.4.2.3 Puente inalámbrico

Un puente inalámbrico es un dispositivo cuya finalidad es la de unir dos redes inalámbricas tanto física como lógicamente diferentes, el uso más común que se le da es el de unir dos redes geográficamente distantes, es decir, cuando queremos unir dos redes que se encuentren en 2 edificios diferentes o incluso redes que se encuentren en un mismo edificio pero en pisos no adyacentes, pudiendo llegar a unir redes que se encuentran hasta a 14 km promedio a 54 mbps y hasta 27 km a 11 mbps, pudiendo aumentar estas distancias con el uso de antenas de alto alcance. Naturalmente estos datos son aproximados y dependen de variados factores.

Los puentes funcionan en pares, lo cual es una configuración punto – punto, un dispositivo a cada lado del puente, y también pueden usar una configuración punto multipunto, en este caso uno de los puentes funciona como dispositivo central.

2.4.2.4 Antenas

En términos generales, una antena es la encargada de aumentar la potencia de un transceptor, un transceptor es un dispositivo que hace las veces de trasmisor y receptor al mismo tiempo, estos hacen uso tanto de antenas integradas como de antenas externas, aumentando así tanto la fuerza de la señal como la sensibilidad de la recepción.

La potencia de una antena es medida en decibeles (dB), el rango de potencia de una antena medida en dBs es conocida como ganancia. Un pequeño aumento en los decibeles provoca un gran aumento en la ganancia ya que los dBs aumentan en escala logarítmica.

Fundamentalmente, para lo que son las aplicaciones *wireless* podemos encontrar a las antenas divididas en dos grupos, las antenas direccionales y las omnidireccionales.

Las antenas omnidireccionales son las antenas que tienen la capacidad de irradiar energía prácticamente en cualquier dirección, sin embargo en la realidad una antena omnidireccional no emite energía en todas las direcciones por igual, sino que irradian a 360 grados en el plano horizontal y va adquiriendo una forma de dona, por esta razón en el centro de la "dona" tendremos máxima intensidad de señal llegando a cero mientras más nos alejamos del centro. La única antena omnidireccional que irradia de igual manera en los 3 planos x,y,z es una antena isotrópica, misma que es una antena ideal, no existe en la realidad.

Las antenas direccionales como su nombre lo indica son antenas que tienen un menor ángulo de radiación, orientando la señal en una dirección determinada lo que hace que tenga mucho mayor alcance que una antena omnidireccional. De ahí que mientras más alcance o ganancia tiene una antena direccional menor será su ángulo de irradiación y viceversa. Fuera de la zona de cobertura de la antena direccional no se tiene ningún tipo de señal.

Por su parte las antenas sectoriales son una mezcla entre las dos antes mencionadas, y se las utiliza cuando se necesita un balance de las dos, llegar a largas distancias y a la vez cubrir aéreas extensas, en el grafico 2.1 podemos observar la diferencia entre ellas.

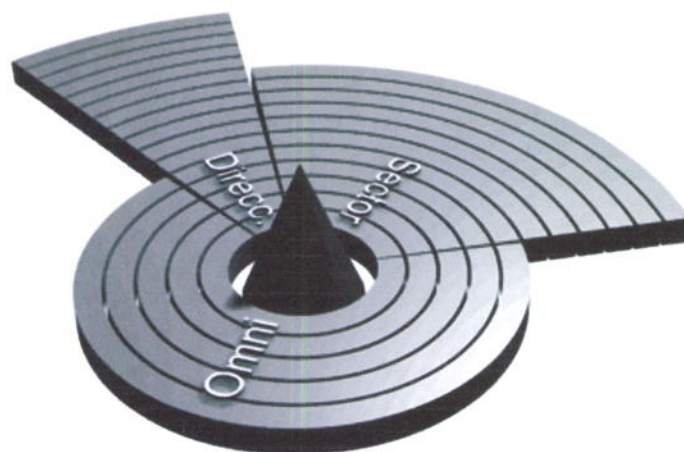


Figura 2- 1 Diferencia de irradiación entre los 3 tipos de antenas

2.5 Topologías de redes inalámbricas

Al igual que en las redes LAN cableadas, la topología no es más que los varios tipos de disposiciones que tendrán los diferentes componentes de la red, es decir, como estarán ubicados unos con respecto de otros. La topología más adecuada para una red en particular depende de factores como el número de hosts⁴⁵ que se van a interconectar, el tipo de acceso al medio físico que se empleará, etc.

Hay dos tipos de topologías a considerar, la topología física y la topología lógica:

La Topología Física no es más que la disposición real de los hosts o estaciones de trabajo y el resto de dispositivos de red, o sea su ubicación física dentro de una oficina, casa, empresa, etc.

La topología lógica es la manera en que los hosts y dispositivos de red se comunican entre sí a través del medio físico, en una red LAN tradicional, el medio físico es el cable, en el caso de las redes inalámbricas como hemos visto no dependemos más que de las radio frecuencias, por lo que tenemos completa movilidad.

Para las redes inalámbricas, tenemos dos topologías bien definidas, la topología o modo Infraestructura y la topología o modo Ad-Hoc.

2.5.1 Topología de Infraestructura Básica

Una Topología de Infraestructura Básica o BSS⁴⁶ se compone de dos o más estaciones de trabajo o nodos inalámbricos también conocidos como STAs⁴⁷ que se hallan interconectados a través de un punto de acceso configurado en modo infraestructura, es decir que los nodos o estaciones de trabajo no se

⁴⁵ Host: termino en Inglés usado para referirse a un computador o usuario conectado a la red

⁴⁶ BSS: del Inglés, Basic Service Set

⁴⁷ STA: del Inglés, Associated Stations

comunican entre ellos directamente, sino que las comunicaciones entre las estaciones y la red cableada se hacen a través del punto de acceso.

Cada BSS tiene un nombre asociado, el cual es llamado SSID por sus siglas en Inglés (Service Set Identifier)

El termino BSS no debe ser confundido con el termino BSA o Basic Service Area por sus siglas en inglés, que se refiere al área de cobertura de un punto de acceso.

2.5.2 Topología de Infraestructura Extendida

Una topología de Infraestructura Extendida también conocida como ESS⁴⁸ no es más que la unión de dos o mas BSSs que se encuentran interconectadas entre si y con la red de área local (LAN) y que aparecen bajo un solo SSID, es decir, lógicamente todos los nodos se encuentran bajo una sola red, en este tipo de topología se puede hacer roaming, es decir trasladarse de un lugar a otro cambiando de AP sin perder la conectividad.

2.5.3 Topología Ad-hoc

Cuando se tiene una red inalámbrica en donde se carece de acces points se habla de una topología Ad-hoc, en este caso una STA hace de "master" entre el resto de STAs conectadas entre si.

Esta topología toma el nombre de IBSS⁴⁹ y sus aplicaciones son las de crear una red inalámbrica rápida y fácilmente, especialmente cuando no se tiene un punto de acceso a mano. Es lo análogo de conectar 2 computadoras entre sí por medio de un cable cruzado.

⁴⁸ ESS: del Inglés, Extended Service Set

⁴⁹ IBSS: del Inglés, Independent Basic Service Set

2.6 Seguridad en WLAN

Como se ha visto a lo largo de los anteriores capítulos las redes inalámbricas son hoy por hoy una herramienta casi imprescindible tanto en la industria y los negocios como en el hogar, sin embargo por el mismo hecho de explotar la facilidad que brinda la tecnología inalámbrica, es decir, una persona no se encuentra físicamente atada por medio de un cable a la red, las WLAN's son mucho más susceptibles de sufrir ataques por lo que la seguridad de este tipo de redes es primordial.

Basta con encender nuestra computadora en la oficina para descubrir una serie de redes inalámbricas de empresas ubicadas en el mismo edificio, o si se posee un dispositivo portátil como una laptop, se puede hacer un recorrido por las calles de Quito y ver que hay zonas prácticamente cubiertas por un sin número de redes inalámbricas, y muchas de las veces, sin ningún tipo de seguridad, un pequeño porcentaje de estas redes tienen nombres genéricos, como dlink , default, etc, o algunas veces nombres de familias, por lo que enseguida se puede dar cuenta de que son redes de hogar, pero un porcentaje mucho mayor pertenece a redes de empresas, lo que nos sugiere que la seguridad en estos casos es tal vez algo deficiente, en el siguiente punto se analiza el por qué de esta aseveración.

2.6.1 Tipos de amenazas

Existen algunos tipos de amenazas que se muestran a continuación:

Escuchas ilegales.- Consiste básicamente en hacer sniffing⁵⁰ a la red inalámbrica, es decir, "escuchar" o interceptar la información que está siendo transmitida, sin que el receptor o el transmisor se percate de ello. Este puede considerarse un ataque pasivo.

⁵⁰ Sniffing: término en Inglés que significa usar un sniffer para capturar tramas de una red

Acceso no autorizado.- Es una amenaza un tanto más peligrosa, ya que el intruso puede ingresar a la red haciéndose aparecer como un usuario autorizado y hacer uso de todos los recursos de la red. Este es considerado un ataque activo.

Interferencias Intencionadas.- Se trata de un tipo de ataque cuya finalidad es la de interrumpir las comunicaciones mediante el uso de dispositivos de radiofrecuencia con la potencia necesaria para mitigar a las señales más débiles en este caso de las estaciones de trabajo o acces points, constituye un ataque por denegación de servicio.

Amenazas Físicas.- Consiste en el daño de la infraestructura física de la red inalámbrica, es decir, danos de ap's, ruteadores, o tarjetas de red, dependiendo del daño pueden causar una reducción de ancho de banda y/o intensidad de la señal hasta llegar a una completa interrupción de la red inalámbrica, los daños pueden ser intencionados o no.

2.6.2 Mecanismos de seguridad

Al igual que en las redes cableadas, no existe una protección ideal, es decir, no podemos confiar en una sola medida de seguridad, sino que por lo general la mejor opción es hacer uso de varias medidas, dependiendo del escenario y de los recursos y herramientas disponibles.

2.6.2.1 Filtrado

El filtrado consiste en determinar que estaciones o dispositivos tendrán acceso a la red inalámbrica y cuales no. Podemos identificar tres tipos de filtrado:

- Filtrado SSID, consiste en darle un nombre o un identificador a nuestra red, que puede constar de uno a treinta y dos caracteres y se lo configura en el acces point o *wireless* router.

- Filtrado MAC⁵¹, consiste en crear una lista de todas las direcciones MAC de las estaciones de trabajo y de los diferentes dispositivos inalámbricos que tendrán acceso a la red. Esta lista debe ser agregada a cada access point que sea parte de la red inalámbrica.

Como es evidente este mecanismo es válido en ambientes pequeños, ya que resulta poco práctico y generaría mucho tiempo el reprogramar cada AP cada vez que se realice un cambio en una red grande, además tampoco constituye un método 100% efectivo ya que existe la posibilidad de extraer una dirección MAC autorizada x medio de un sniffer⁵², ya que estas direcciones viajan sin ningún tipo de criptografía, y luego simplemente alterar la dirección de una NIC cualquiera por esta MAC autorizada.

El filtrado MAC no es parte del estándar 802.11 pero casi la totalidad de los proveedores han incorporado este método de seguridad a sus equipos.

- Filtrado de Protocolos, consiste en filtrar o definir que protocolos son permitidos o denegados para cada usuario.

2.6.2.2 SSID Broadcast

Como se observó al inicio de este capítulo, el SSID es el identificador de una red inalámbrica, resulta muy útil en redes públicas, ya que el SSID realiza un broadcast⁵³ constante de su identificador, lo que permite percatarse de la existencia de una red inalámbrica, sin embargo, si se trata de una red privada, especialmente una red empresarial, el SSID broadcast constituye una invitación a que personas no autorizadas quieran tener acceso a la red, para evitar esto se debe desactivar la opción de broadcast del AP.

⁵¹ MAC: del Inglés, Media Acces Control o control de acceso al medio es el identificador único de una Nic

⁵² Sniffer: programa que captura las tramas de una red

⁵³ Broadcast: difusión, trasmisión de información desde un nodo emisor hacia varios receptores

2.6.2.3 Actualización de los equipos de red

Aunque parezca una nimiedad es una tarea importante el tener tanto acces points como ruteadores y nics con el firmware actualizado, ya que generalmente el fabricante añade funcionalidades y mejoras a sus dispositivos sobre todo en el aspecto de seguridad.

2.6.2.4 Administración remota del AP

Los acces points y routers inalámbricos poseen una opción con la cual podemos administrarlos remotamente, esta función resulta muy útil cuando estamos físicamente distantes de los Ap's, pero también representa una brecha de seguridad, en muchos de los casos es mejor tener esta opción desactivada.

2.6.3 Estándares de seguridad en WLAN

El estándar 802.11 ofrece tres tipos de autenticación y cifrado, que son, WEP, WPA y 802.1x.

2.6.3.1 WEP

WEP o Privacidad Equivalente a Cableado es el sistema de seguridad incluido desde la primera versión del estándar 802.11, y trata de resolver los problemas de seguridad de las redes inalámbricas mediante un sistema de cifrado y autenticación.

El cifrado es manejado a nivel 2 o capa 2 del modelo OSI, está basado en el algoritmo de cifrado RC4⁵⁴ utilizando claves de 64 bits, 40 bits + 24 bits del

⁵⁴ RC4: Sistema de cifrado en flujo más utilizado, el cifrado en flujo realiza un cifrado incremental convirtiendo el texto claro en texto cifrado bit a bit.

vector de iniciación⁵⁵ y también claves de 128 bits, 104 bits + 24 del vector de iniciación.

Fue presentado en el año 1999 pero para el año 2001 las vulnerabilidades del WEP fueron expuestas y hoy en día constituye uno de los mecanismos menos seguros y más fáciles de crackear⁵⁶ con software que está disponible en el internet, como por ejemplo "Airsnot" que ofrecía crackearlo en aproximadamente una hora por lo que en el año 2003 la Wi-Fi Alliance lo reemplazo por WPA (Wi-Fi Protected Acces). Luego de la ratificación en el año 2004 del estándar de seguridad inalámbrica propuesto por la IEEE, el 802.11i, también conocido como WPA2 el WEP fue revocado completamente.

Entre las principales fallas de esta implementación de seguridad, encontramos las siguientes:

La clave compartida que configuramos en nuestro AP es estática, para cambiarla tenemos que hacerlo tanto en el AP como en las estaciones, en la práctica no se la cambia casi nunca.

El IV (vector de iniciación) es de una longitud de 24 bits, muy pequeña, cada trama es cifrada con un IV diferente, pero en una red con alto tráfico es solo cuestión de tiempo hasta que el IV se repita en una trama, si esto ocurre un pirata informático puede obtener texto en claro, con el texto en claro y el texto cifrado y conociendo el funcionamiento del algoritmo RC4 se puede obtener la clave.

2.6.3.2 WPA

WPA o Wi-Fi Protected Acces por sus siglas en Inglés es un estándar que reemplaza al WEP corrigiendo sus vulnerabilidades.

⁵⁵ Vector de iniciación: Bloque de bits requerido para permitir el cifrado en flujo

⁵⁶ Crackear: término en Inglés que significa romper la seguridad de un software o en este caso de la red

Entre las mejoras al estándar anterior, en cuanto al cifrado, WPA hace uso del protocolo de cifrado TKIP (Temporary Key Integrity Protocol) por sus siglas en Inglés, este protocolo cambia la clave compartida entre el AP y el cliente cada cierto tiempo, ya no es una clave estática como en el caso de WEP, sino que la clave es dinámica para cada usuario, por cada sesión y por cada paquete. Además el IV es del doble de tamaño, 48 bits, esto minimiza la reutilización de claves.

En cuanto a la autenticación, WPA hace uso del protocolo 802.1x y EAP, pudiendo operar en dos modos distintos:

- Modo empresarial: Para este modo se necesita un servidor RADIUS⁵⁷, se emplea 802.1x⁵⁸ y EAP⁵⁹ para la autenticación, el servidor radius se encarga del manejo de las claves compartidas para el cifrado de datos, se usa esta modalidad en esquemas que necesiten de un alto nivel de seguridad.
- Modo casero: en esta modalidad se hace uso de PSK (pre Shared Key) y no requiere de un servidor radius, la autenticación se hace al establecer una contraseña en el AP la misma que coincidirá con la contraseña del cliente, es recomendable utilizar contraseñas de más de 20 caracteres.

WPA funciona en los estándares 802.11a, b, g, n, y todo equipo certificado por la Wi-Fi Alliance puede ser actualizado para soportar esta especificación.

Por su lado, WPA2 fue ratificado en el año 2004 por la IEEE en conjunto con la Wi-Fi Alliance y constituye una mejora al WPA y un estándar de seguridad por si mismo, llamado 802.11i. Este estándar hace uso del algoritmo de encriptación AES (Advanced Encryption Standard) y está idealmente pensado

⁵⁷ RADIUS: del Inglés, Remote Authentication Dial-In User Server

⁵⁸ 802.1X: norma del IEEE para el control de acceso a la red, permite la autenticación de dispositivos conectados a un puerto LAN

⁵⁹ EAP: del Inglés, Extensible Authentication Protocol

para empresas con altos requerimientos de seguridad como también para ambientes SOHO (Small Office and Home Office) y al público en general.

2.6.3.3 802.1x

802.1x es un protocolo de control de acceso creado, en un principio, para redes tradicionales, tiene una arquitectura cliente/servidor por lo que es una solución empresarial y está basado en el protocolo de autenticación extensible EAP (Extension Authentication Protocol), que tiene tres componentes principales:

- Solicitante: la estación de trabajo o cliente que pide autorización para ingresar a la red.
- Servidor de autenticación: servidor que contiene la información de usuarios y estaciones de trabajo autorizadas para ingresar a la red. El protocolo 802.1x hace uso de servidores RADIUS, los mismos que originalmente fueron creados para la autenticación de usuarios remotos por conexión telefónica.
- Autenticador: equipo de red que actúa de intermediario entre el solicitante y el servidor RADIUS, puede ser un AP o *Wireless Router*.

La autenticación entre el servidor RADIUS y la estación de trabajo, mediante el uso del protocolo EAP consta de los siguientes pasos:

1. Se inicia el proceso cuando una estación de trabajo o solicitante se asocia a un AP, en este momento se bloquea todo el tráfico a excepción del EAPOL (EAP over LAN), entonces la estación de trabajo envía un mensaje EAPOL START, lo que indica que se quiere iniciar una sesión de autenticación.
2. El autenticador responde con un mensaje EAPOL REQUEST IDENTITY, solicitando a la estación de trabajo que se identifique.
3. El solicitante responde con un mensaje EAPOL RESPONSE IDENTITY donde se incluye el usuario y la clave personal.

4. Cuando el autenticador recibe esta información la encapsula y la manda al servidor RADIUS mediante un mensaje RADIUS ACCES REQUEST
5. Una vez verificada la información del solicitante en el servidor RADIUS, este envía un desafío al AP y este a su vez al solicitante mediante un mensaje EAP REQUEST.
6. El solicitante responde el desafío al autenticador mediante un mensaje EAP RESPONSE (CREDENTIALS) y este lo envía al servidor RADIUS mediante un mensaje RADIUS ACCES RESPONSE.
7. En el caso de ser correcta esta información, el servidor envía un mensaje RADIUS ACCES ACCEPT al autenticador, autorizando acceso completo al solicitante, además en este mensaje otorga un juego de claves WEP dinámicas que servirán para el cifrado de la información, el servidor RADIUS cambia estas claves en un intervalo de 5 minutos aproximadamente.
8. El autenticador envía un mensaje EAP SUCCEES al cliente y empieza la comunicación.

De acuerdo al modo de autenticación del protocolo EAP, se puede clasificar en dos grupos generales, los que hacen uso de certificados digitales y los que hacen uso de contraseñas.

2.6.4 VPN

Una VPN (Virtual Private Network) es una red virtual que se crea dentro de una red real, ya puede ser una LAN o el Internet. El objetivo es crear una red confidencial o segura dentro de una red pública, generalmente Internet, permitiendo al usuario trabajar como si estuviera dentro de su propia red.

En el caso de las WLAN, la VPN es una red interna dentro de la red LAN de la empresa en vez del internet, consiste en una variante del tipo acceso remoto y sirve para aislar zonas y servicios de la LAN.

Una VPN hace uso tanto de técnicas de autenticación como de encriptación y básicamente consiste en poner el *wireless router* o *Acces point* dentro de una VPN, así cuando el usuario inalámbrico o estación de trabajo quiera acceder a la red inalámbrica deberá pasar por el proceso de autenticación de la VPN.

Las VPNS pueden ser creadas tanto por hardware como por software, teniendo en cuenta de que casi todos los sistemas operativos actuales incluyendo Windows, Linux, etc, poseen esta características, por lo que dependiendo de la sensibilidad de la información y del ambiente en el que se halla la red inalámbrica una VPN podría ser una solución económica.

Hay que tomar en cuenta de que todos los acces points que formen parte de la red segura deben estar dentro de la VPN, ya que de no ser el caso se crearía una brecha de seguridad.

2.6.5 VLAN

Una VLAN o Virtual Lan por sus siglas en Inglés constituye otra alternativa al momento de plantear seguridades en redes inalámbricas dada sus características de ser redes lógicamente independientes que coexisten dentro de una red real, en otras palabras, con una VLAN se puede segmentar una red en varias de acuerdo a la necesidad, dando privilegios de acceso individuales a cada una de ellas. De esta forma los usuarios pueden ser clasificados de acuerdo a sus funciones o a la ubicación en la que se encuentren.

En términos generales, para dar esta clasificación según el usuario, se crearia una VLAN diferente de acuerdo al tipo o clasificación, y a cada una de estas VLANs se le asociará un AP que a su vez tendrá su SSID único, es decir, uno propio o diferente de otra VLAN.

2.7 Nuevas tecnologías emergentes

Como se ha visto a lo largo de este capítulo la Tecnología Inalámbrica es una tecnología relativamente nueva, acaba de cumplir 10 años de ser disponible al público en general, y durante estos 10 años ha ido creciendo día a día, siempre innovando, una de estas innovaciones tecnológicas en el campo de la WLANS es el *Wireless Routing* o *Wireless Switching*.

2.7.1 *Wireless Lan Switching*

El *Wireless Switching* es un término acuñado por empresas desarrolladoras de equipos inalámbricos que observaron las necesidades de las SMBs⁶⁰ de tener entre otras funcionalidades un mejor manejo de sus redes WLAN.

Las pequeñas y medianas empresas optaron por hacer uso de la tecnología inalámbrica para obtener acceso a su LAN y en algunos casos incluso han ido más allá reemplazando por completo las redes Ethernet por redes inalámbricas. Como en cualquier empresa o negocio, con el transcurso del tiempo se pueden observar dos constantes que son el incremento de usuarios de la red y el número de servicios que han ido evolucionando con el tiempo, como voz sobre ip. videoconferencia, el uso de diversos dispositivos inalámbricos como teléfonos Wi-Fi, PDA's, etc.

A su vez estos factores crearon nuevos requerimientos, como una cobertura continua de la WLAN en todas las áreas físicas de la empresa o negocio, necesidad de un servicio constante, administración y monitoreo centralizado, y sobre todo la posibilidad de cubrir todos estos aspectos de una forma sencilla y económica.

En la actualidad muchas empresas que hacen uso de una WLAN poseen una infraestructura basada en AP's configurados independientemente, el siguiente

⁶⁰ SMB: del Inglés, Small and Mid Sized Business

cuadro nos muestra todos los requerimientos de las redes WLAN para pequeñas y medianas empresas y la forma tradicional en que se los manejan:

Tabla 2- 2 Requerimientos de las WLANS

Requerimiento	Descripción
Administración y Monitoreo	Maneras practicas y eficientes y sobre todo de bajo costo para administrar y monitorear la red inalámbrica.
Costos de upgrade	Colocar nuevos AP's a medida que hagan falta y actualizar los existentes.
Acceso de Invitados	Proveer acceso temporal a la red a gente o usuarios del exterior manteniendo la seguridad.
Planeación	Métodos de planeación para crear una red inalámbrica basados en en la estructura del lugar físico.
Balaceo de carga	Balaceo automático de usuarios entre AP's
Detección de AP's intrusos	Detección de AP's no autorizados, seguridad.

De esta manera y para solventar todos estos requerimientos es que se crea el concepto de Wilreless Lan Switching cuyo principal componentes es un Switch Wlan, que es un dispositivo central de la red que se lo ubica en el *centro de cómputo*, a este dispositivo se conectaran todos los AP's, ya sea directa o indirectamente, de esta forma el switch estará a cargo de gestionar todas la funciones de los AP's.

Los factores que hay que considerar al momento de crear o mejorar una red inalámbrica son los costos previos a la instalación en los que se incluyen los "site surveys", también se considera el cableado tanto de red eléctrica, el cual alimentará a los Ap's, y sobre todo la reconfiguración de la red actual y la configuración de los nuevos AP's.

El proceso de Wireless Switching trata de facilitar los site survey al incluir dentro de su arquitectura un software de planeamiento inteligente basado en la estructura física de la oficina o empresa incluyendo sus diferentes pisos, además hace uso del estándar IEEE 802.3af o mejor conocido como POE por sus siglas en Inglés o Power Over Ethernet, esta tecnología permite que los AP's reciban energía eléctrica a través del mismo cable UTP lo que elimina la necesidad de tomas eléctricas adicionales.

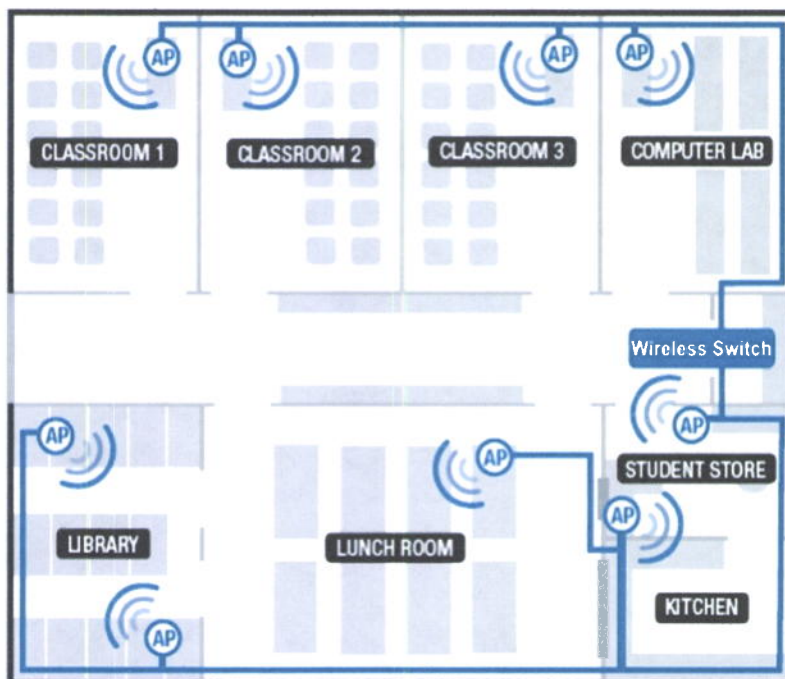


Figura 2- 2 Solución Inalámbrica Centralizada

Otras ventajas de tener una solución integrada es que el sistema nos muestra información de toda la actividad de los usuarios, switches y Ap's, y se pueden generar informes de uso y monitoreo en general de la red inalámbrica, a su vez la configuración de los Ap's es mucho más fácil ya que podemos cargar perfiles con toda la información necesaria como opciones de seguridad a todos los AP's, automatizando y optimizando el proceso, algo importante es que los AP's deben ser soportados o reconocidos por el switch, los diferentes fabricantes ofrecen soluciones integradas, es decir, los switches trabajan con sus Ap's determinados, tanto marca como modelo, esto ayuda a obtener lo mejor de las características de un determinado equipo al trabajar en conjunto con otro que es parte de la solución completa.



Figura 2-3 Monitoreo de la Red Inalámbrica

Además, esta forma centralizada de administrar la red inalámbrica nos brinda la facilidad de observar gráficamente en consola el tráfico de los Ap's y en el caso de que un Ap este caído tomar acciones pertinentes rápidamente.

3 Análisis

3.1 Introducción

En este capítulo se realizará un análisis de la situación actual de la red WLAN de la Universidad de las Américas campus COLON y de los requerimientos para la nueva red WLAN.

En el análisis de la situación actual de la red WLAN, se identificará los servicios y aplicaciones brindadas y la infraestructura tecnológica. Este análisis determinará las ventajas y desventajas de la red actual, y definirá la reutilización de equipos de la misma.

El análisis de los requerimientos de servicios comienza con la determinación del nivel de servicio brindado por la red alámbrica e inalámbrica mediante una encuesta la cual está sólidamente fundamentada en este capítulo. Posteriormente se determinan los servicios que demandan los usuarios y el nivel de servicio en cuanto a rendimiento, disponibilidad, seguridad, capacitación, cobertura y soporte técnico que deberá tener la red inalámbrica a diseñarse.

3.2 Análisis de la situación actual

En el análisis de la situación actual, se hará un estudio de los servicios y aplicaciones disponibles en la red; y de la infraestructura tecnológica, esta incluirá información física y lógica de la red. En la parte física de la red incluirá equipos activos y pasivos de la red, tecnologías WAN y velocidades. La parte lógica incluirá direccionamiento IP, protocolos de enrutamiento, protocolos de administración de la red y la seguridad utilizada.

Actualmente se tiene para la red de estudiantes 3 Mb de velocidad de Internet a través del ISP Impstat (Global Crossing) y 1 Mb para la red administrativa.

3.2.1 Identificación de servicios

En la red UDLA se brinda los servicios de correo electrónico, portal WEB, DNS, de Directorio, DHCP, de Impresión y acceso a Internet, el mismo que incluye, navegación, FTP y Telnet. Los servicios de DHCP e impresión se brindan localmente desde la red UDLA Campus Colón, el resto de servicios son brindados desde la Granja de servidores ubicados en la UDLA Campus Granados.

3.2.1.1 Correo electrónico

El correo electrónico brinda los servicios de mensajería electrónica interna así como también comunicación externa. Este servidor se encuentra ubicado en el Campus Granados y alberga cuentas de profesores, personal administrativo y estudiantes.

Dentro de la administración de las cuentas de correo, la UDLA posee procedimientos que norman la creación de nuevos usuarios, el mantenimiento de las mismas, el envío de correo masivo y monitoreo del servidor para detectar problemas y solucionarlos.

3.2.1.2 Portal web

El portal Web es un servicio utilizado por los usuarios internos para acceder a información local y por usuarios externos para acceder a la información web pública de la UDLA. Este equipo tiene como propósito ser un servidor de base de datos y aplicaciones. Se encuentra ubicado en la UDLA Campus Granados.

3.2.1.3 Servicio DNS (Domain Name Service)

El DNS permite a los usuarios de red utilizar nombres jerárquicos sencillos para comunicarse con otros equipos y resolver las direcciones requeridas por los

usuarios de la UDLA. Este servidor se encuentra ubicado en la UDLA Campus Granados manteniendo una réplica en el campus Colon, aqui se registran todas las máquinas con dirección IP y nombre de equipo en el archivo de zona.

3.2.1.4 Servicio de directorio

Es una aplicación o un conjunto de aplicaciones que almacena y organiza la información sobre los usuarios de una red de ordenadores, sobre recursos de red, y permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red. Además, los servicios de directorio actúan de manera transparente entre los usuarios y los recursos compartidos. El servicio de directorio utilizado es el Active Directory de Microsoft. Este servidor se encuentran en la red de la UDLA campus Granados. Existen dos servidores de replicación en Colón para administrativo y estudiantes respectivamente.

3.2.1.5 Servicio de DHCP (Dynamic Host Configuration Protocol)

Es un servicio de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente mediante el protocolo DHCP. Existe un servidor de DHCP en Colón que brinda este servicio a los usuarios de la red.

3.2.1.6 Servicio de impresión

Permite la gestión centralizada de las impresiones en una red. En la red de Colón existe un servidor de Impresión. Los usuarios de la red se conectan con este servidor para obtener los servicios.

3.2.1.7 Acceso a internet

El acceso a Internet es brindado a todos los usuarios de la red de la UDLA, a través de este se ofrecen los siguientes servicios:

3.2.1.7.1 File Transfer Protocol FTP

FTP es uno de los servicios de la UDLA utilizado para enviar o descargar cualquier tipo de archivo en la red.

3.2.1.7.2 Telnet

TELNET es un servicio brindado en la UDLA con el fin de establecer conexión a un terminal remoto.

3.2.2 Identificación de aplicaciones

Las diferentes aplicaciones que son ofrecidas a los usuarios de la red UDLA Campus Colón se encuentran disponibles a través de sus portales WEB, por lo cual consideraremos a las aplicaciones parte del servicio HTTP brindado a los usuarios de la red.

3.2.3 Infraestructura física

El diseño de la red actual lo analizaremos en base al diseño de red jerárquico, que se compone de tres capas: Core, Distribución y Acceso. La red de la UDLA Campus Colón, es una red pequeña, posee sólo dos capas: Core y Acceso.

A continuación se muestra el diagrama de red de la UDLA Campus Colón con los equipos activos.

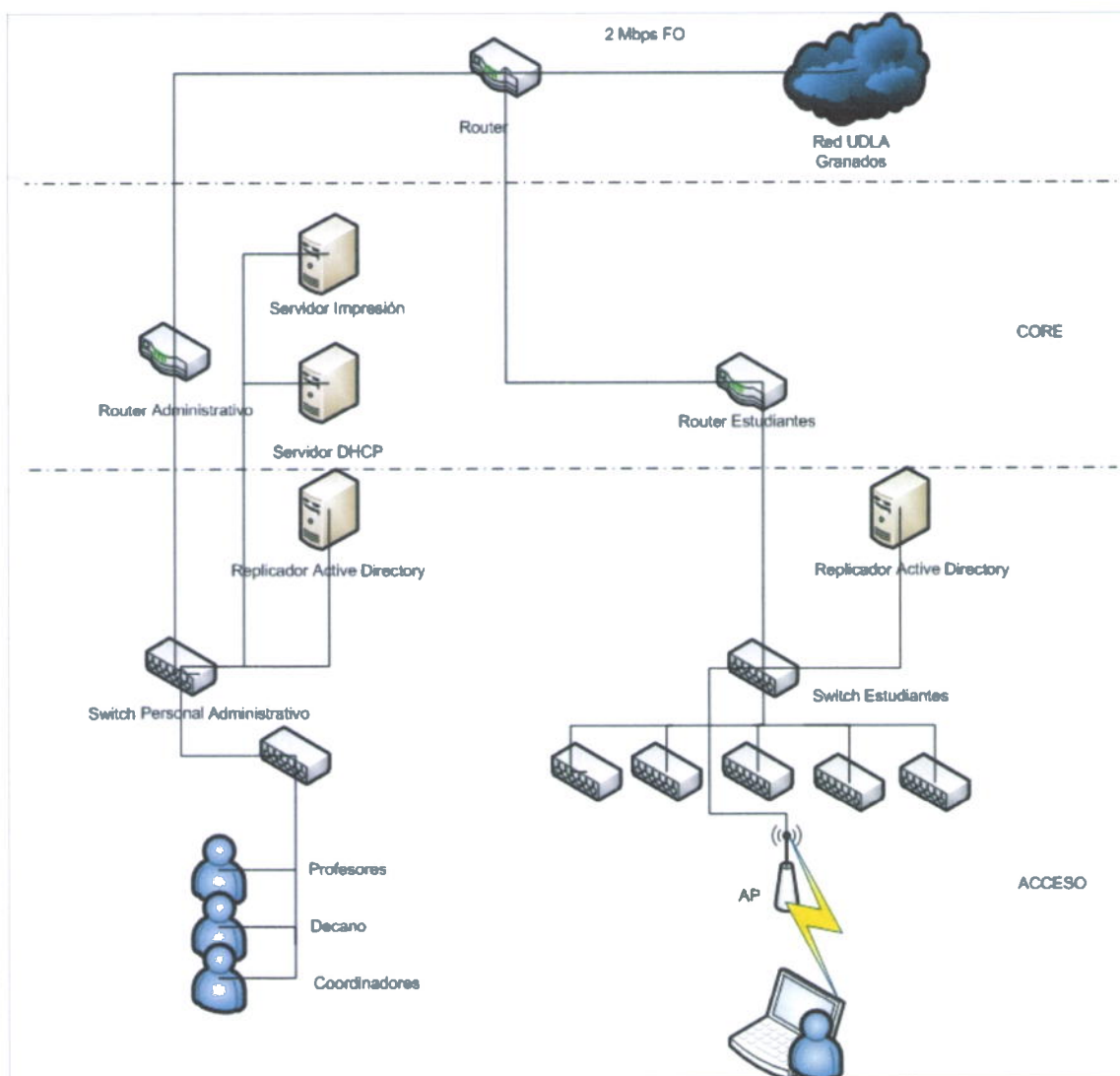


Figura 3- 1 Diagrama de Red UDLA Campus Colón⁶¹

Los equipos activos de la red son:

- 1 Switch 3COM 3300 para personal Administrativo
- 1 Switch Dlink 1228 para personal Administrativo
- 2 Switch 3COM 2024 para Estudiantes.
- 1 Switch Dlink 1228 para Estudiantes
- 1 Router Cisco 800 Series para interconexión con la UDLA Granados.
- 1 Router Cisco 600 Series para Estudiantes
- 1 Router para personal Administrativo

⁶¹ Fuente: Departamento Sistemas Universidad de las Américas

- 3 Switches en 2 laboratorios del Campus y una Sala de admisiones.
- Acces Point Dlink

Existen 4 servidores en la red: Servidor DHCP; Servidor Replicador de Active Directory de Estudiantes y de Personal Administrativo; y Servidor de Impresión. A continuación se detalla los servidores de Colón:

Tabla 3- 1 Servidores en la red del Campus Colón⁶²

SERVIDOR	EQUIPO	UBICACIÓN
Active Directory Replicador Administrativo	IBM X SERIES 220	Campus Colón
Active Directory Replicador Estudiantes	IBM X SERIES 235	Campus Colón
DHCP	IBM X SERIES 220	Campus Colón
Impresión	Dell Optiplex 745	Campus Colón

Existen 1 enlace WAN de 2 Mbps hacia la red UDLA Campus Granados, esta conexión entrega los servicios especificados en el punto 3.2.1 a la red UDLA Campus Colón.

La parte pasiva de la red está conformada por un sistema de cableado estructurado de estándar EIA/TIA 568 A. La categoría de cable utilizado es 5e. Este tipo de cableado permite velocidades de hasta 1000 Mbps con el estándar 802.3 ab 1000 Base T. Este Sistema de Cableado Estructurado es utilizado en la red de la UDLA Campus Colón para velocidades de 100 Mbps.

3.2.4 Infraestructura lógica

El direccionamiento utilizado en la red de la UDLA Campus Colón, es una dirección de red de clase A para la red de personal administrativo, igualmente se utiliza para la de estudiantes. Estas direcciones son:

- 192.168.8.x Para Personal Administrativo.

⁶² Fuente: Departamento de Sistemas Universidad de las Américas Sede Colón

- 192.168.24.x Para Estudiantes.

Estas dos redes tienen comunicación por el Router central, el cual realiza las funciones de enrutamiento entre las dos redes. Se usa un enrutamiento estático para la comunicación entre las dos redes.

No existen dispositivos de seguridad como firewalls, IPS, IDS, etc en la red de Colón. La seguridad es gestionada a nivel de routers y switches de la red. Una mayor seguridad no es necesaria debido a que Colon es física y lógicamente una subred de Granados y toda la seguridad es gestionada desde ahí.

No se utilizan protocolos de gestión estandarizados como SNMP para la gestión de los equipos de una manera centralizada. Se utiliza telnet para realizar la gestión remota de los equipos independientemente.

3.2.5 Ventajas y desventajas

3.2.5.1 Ventajas

- Existe una infraestructura LAN que puede ser utilizada para la implementación de la red WLAN.
- En la red UDLA, los servicios y aplicaciones brindadas se encuentran en un nivel aceptable de rendimiento, esto no generará un punto de falla cuando se esté analizando el rendimiento de la red WLAN.
- Existe segmentación de redes, es decir se tiene dos redes: Estudiantes y Personal Administrativo. Esto facilita la seguridad y la gestión entre las dos redes.
- Los switches son equipos administrables y operan bajo la mayoría de estándares actuales de bridges, como 802.1X, 802.1p y 802.1q.

3.2.5.2 Desventajas

- La red UDLA Campus Colón no posee switches PoE, por lo cual se buscará una alternativa para proveer energización a los Puntos de Acceso. Se priorizará que la energización sea centralizada, por las facilidades de implementación.
- No existen equipos de seguridad como firewall, IPS, e IDS, dentro del Campus Colón. Esta seguridad está implementada a nivel de routers.
- No existen Servidores de autenticación 802.1X, localmente.
- La red WLAN actual no ofrece esquemas de disponibilidad, seguridad, ancho de banda. Solo existe un Punto de Acceso que no ofrece cobertura a todos los sitios de la UDLA Campus Colón.

3.3 Análisis de requerimientos

El objetivo de este análisis es determinar la percepción de estudiantes, profesores y personal administrativo en cuanto a rendimiento, disponibilidad, seguridad, capacitación y soporte técnico de los servicios que brinda la red inalámbrica. En base a este análisis se determinan los requerimientos de servicios que estarán disponibles, el alcance físico y el nivel de servicio para la red Wireless-LAN a ser diseñada. Para formalizar este análisis se realiza una investigación basada en encuestas y entrevistas. Se incluye un punto dedicado al diseño de la encuesta realizada, el mismo que abarca sus objetivos, metodología y elaboración, para posteriormente realizar el análisis de los resultados de la misma.

3.3.1 Diseño de la encuesta

Actualmente la red cableada e inalámbrica brinda a todos los miembros de la comunidad universitaria servicios de: correo electrónico, servicios web, acceso

a Internet (navegación web, mail, chat), acceso a sitios Web internos de la UDLA. Los usuarios de la red de la UDLA son estudiantes, profesores, personal administrativo. Para determinar los requerimientos de servicios, es necesario definir el nivel de servicio brindado en la red inalámbrica de la UDLA con el fin de optimizarlo según las necesidades reales de los usuarios utilizando tecnología inalámbrica. El estudio se basa en la realización de una encuesta a estudiantes, profesores y personal administrativo. Los resultados de esta encuesta son el instrumento que permite evaluar el nivel de servicio que brinda la red inalámbrica de la UDLA, la percepción del usuario sobre la gestión realizada en la red, la acogida de una nueva red Wireless LAN para el Campus y su alcance físico.

3.3.1.1 Objetivos de la encuesta

Los objetivos de la encuesta son los siguientes:

- Determinar la frecuencia de uso de los Servicios de la red.
- Determinar la percepción de los usuarios sobre la calidad del servicio, según métricas de rendimiento, disponibilidad, seguridad, soporte técnico de la red inalámbrica actual.
- Determinar el interés de los usuarios de contar con una nueva red inalámbrica.
- Determinar el alcance físico de la red inalámbrica.
- Determinar los servicios y aplicaciones que el usuario necesita que estén disponibles.
- Determinar las prioridades del usuario, referente al servicio WLAN a brindar.

3.3.1.2 Metodología

Los temas a tratarse para la realización de la encuesta son: tipo de estudio, población, muestra y recolección de datos. El tipo de estudio es descriptivo. Las variables definidas para el estudio se han clasificado en seis grupos: la

frecuencia de uso de los servicios de red; la calidad de los servicios mediante métricas de rendimiento, cobertura, disponibilidad, seguridad, capacitación y soporte técnico; el interés del usuario de contar con una nueva red inalámbrica; la ubicación física; servicios y aplicaciones disponibles en la nueva WLAN; y prioridades en el servicio WLAN. El universo de la población objeto de estudio constituyen 50 profesores, 30 administrativos y 700 estudiantes matriculados en el período Marzo – Agosto 2009⁶³. La población objeto de estudio se estratificó en: estudiantes, profesores y personal administrativo. En el siguiente cuadro se resume lo mencionado anteriormente:

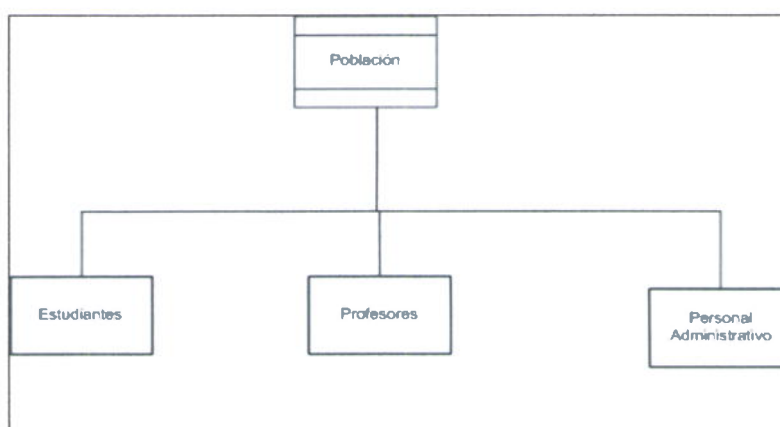


Figura 3- 2 Espacio Muestral

Para determinar el tamaño de la muestra de cada estrato, se utilizó la fórmula que se explica en la tabla 3-2.

Parámetro	Descripción
	$n = \frac{k_{\alpha}^2 p * q * N}{(e^2 * (N - 1)) + k_{\alpha}^2 * p * q}$
N	El tamaño de la población (número total de posibles encuestados)
k_{α}	Es una constante que depende del nivel de confianza que asignemos. El nivel de confianza indica la probabilidad de que los resultados de la investigación sea cierta. Nivel de confianza del 75% es una constante de 1.15
α	Nivel de Confianza que indica la probabilidad de que los resultados de nuestra

⁶³ Fuente: Director de la Escuela de Tecnología de la UDLA.

	investigación sean ciertos con una probabilidad de $\alpha\%$
e	Error muestral deseado, es la diferencia que puede haber entre el resultado que obtenemos preguntando a una muestra de la población y el que obtendríamos si preguntáramos al total de ella.
p	Proporción de individuos que poseen en la población las características de estudio. Este dato es generalmente desconocido y se suele suponer que $p=q=0.5$ que es la opción más segura.
q	Proporción de individuos que no poseen esa característica, es decir, es $1-p$
n	Tamaño de la muestra (número de encuestas que vamos a hacer)

Tabla 3- 2 Fórmula para determinar el tamaño muestral⁶⁴

La estimación del tamaño de la muestra se ha definido con un nivel de confianza del 75%, un error de estimación del 0,1 y p, q igual a 0,5. Los resultados de aplicar la fórmula anterior a los diferentes estratos se puede observar en la tabla 3-2.

Tabla 3- 3 Tamaño de la muestra para los diferentes estratos⁶⁵

ESTRATOS	N	$k\alpha$	α	e	p	q	n
Estudiantes	700	1.15	75%	0,12	0,5	0,5	22
Profesores	50	1.15	75%	0,12	0,5	0,5	15
Personal Administrativo	30	1.15	75%	0,12	0,5	0,5	13

La recopilación de datos se planificó de acuerdo al tipo de estrato. Las encuestas a los estudiantes se las realizó después de horas de clases y con ayuda de profesores en las distintas carreras, semestres y horarios. Los profesores fueron encuestados en sus oficinas al igual que el personal administrativo.

⁶⁴ Fuente: <http://www.feedbacknetworks.com/cas/experiencias/sol-preguntar-calculador.htm>

⁶⁵ Fuente: <http://www.feedbacknetworks.com/cas/experiencias/sol-preguntar-calculador.htm>

3.3.1.3 Elaboración

Para la elaboración de la encuesta se define su estructura y cada uno de los apartados del cuestionario. En la estructura se detallan las partes en las cuales se divide la encuesta. En el cuestionario se describen los temas tratados en la encuesta y cada una de las preguntas con su respectiva justificación.

3.3.1.3.1 Estructura

El formulario de la encuesta consta de dos partes. La primera parte proporciona información sobre la frecuencia de uso de la red LAN y WLAN de la UDLA y la calidad de servicio que provee. La segunda parte está encaminada a recopilar información sobre el interés del usuario de contar con una nueva red inalámbrica y la ubicación de la misma. La estructura del formulario se detalla a continuación:

1. Tipo de Usuario
2. I PARTE: Datos acerca de la red de la UDLA.
3. II PARTE: Datos acerca de la red inalámbrica a diseñarse.

El tipo de respuestas utilizadas corresponden a: texto, opción múltiple y numéricas, estas últimas siguen una escala de 1 a 5 para homogenizar las respuestas.

3.3.1.3.2 Cuestionario

El cuestionario comprende una descripción de cada uno de los temas tratados en la encuesta para que quede sólidamente fundamentada.

Tabla 3- 4 Significado de Preguntas de encuesta

CUESTIONARIO	
APARTADO	PREGUNTAS Y JUSTIFICACIÓN
Tipo de	1.1. Indique a que grupo pertenece Identificar el tipo de usuario para poder clasificarlo en los siguientes estratos:

Usuario	estudiantes, profesores y personal administrativo.	
	1.2. Indique su horario de mayor permanencia en la Universidad.	
	Determinar el horario de permanencia de los usuarios.	
I PARTE: Datos acerca de la red de la UDLA.		
Servicios y Aplicaciones	2.1 Que servicios o aplicaciones de la red LAN de la UDLA utiliza? Especifique el horario en el que los utiliza.	
	Determinar la frecuencia de uso de los Servicios y Aplicaciones de la red en los horarios de 7AM-1PM, 1PM-7PM,7PM-10PM	
	2.2 Que servicios o aplicaciones de la red WLAN de la UDLA utiliza? Especifique el horario en el que los utiliza.	
	Determinar la frecuencia de uso de los Servicios y Aplicaciones de la red WLAN en los horarios de 7AM-1PM, 1PM-7PM,7PM-10PM	
Nivel de Servicio	3.1 Cómo considera el ancho de banda de la red inalámbrica? Valorar el rendimiento de la red WLAN, Según una escala de 1 a 5	
	3.2 Cómo considera la cobertura brindada por la red inalámbrica? Valorar la cobertura de la red WLAN, Según una escala de 1 a 5	
	3.3 Está la red inalámbrica disponible cuando quiere utilizarla? Valorar la disponibilidad de la red WLAN, Según una escala de 1 a 5	
	3.4 Considera que la red inalámbrica protege la confidencialidad y la integridad de su información? Valorar la seguridad de la red WLAN, Según una escala de 1 a 5	
	3.5 Como consideraría al nivel de servicio brindado por la red inalámbrica: Valorar la satisfacción del usuario de la red WLAN, según una escala de 1 a 5	
	3.6 Ha solicitado soporte a los técnicos del centro de computo? Determinar si han solicitado soporte técnico de la red WLAN.	
	3.7 Si la respuesta anterior es positiva, Usted considera que el soporte técnico recibido del personal del centro de computo es? Valorar el soporte técnico recibido de la red WLAN, Según una escala de 1 a 5	
	3.8 Ha recibido cursos de capacitación de los servicios y aplicaciones que brinda la red? Valorar la capacitación brindada sobre la red WLAN, según una escala de 1 a 5	
	II PARTE: Datos acerca de la red inalámbrica a diseñarse	
	Interés del usuario	4.1 Desearía usted contar con una nueva red inalámbrica en el campus? El objetivo es determinar el interés del usuario para implementar una nueva red inalámbrica
		4.2 En donde le gustaría contar con esta red inalámbrica? Determinar el alcance físico de la red inalámbrica donde los usuarios requieran el servicio; de esta manera podremos establecer los requerimientos de acceso.

Servicios y Aplicaciones	4.3 Que servicios o aplicaciones desearía que se encuentren disponibles en la red inalámbrica de la UDLA
	Determinar los servicios y aplicaciones disponibles en la red inalámbrica
Prioridades del servicio	4.4 Qué aspectos usted considera importantes para esta nueva red inalámbrica. Marque con una X, lo considerado por usted.
	Determinar las prioridades del servicio para el usuario.

3.3.2 Análisis de los resultados

Una vez concluida la fase de recolección de datos a través de la encuesta planteada, se realiza la tabulación de los datos obtenidos.

3.3.2.1 Frecuencia de uso de los diferentes servicios y aplicaciones

Las figuras a continuación desde la 3-3 hasta la 3-4 muestran los servicios y aplicaciones de la red LAN y WLAN más utilizadas por los encuestados. La figura 3-5 muestra el horario de mayor consumo de estos servicios y aplicaciones.

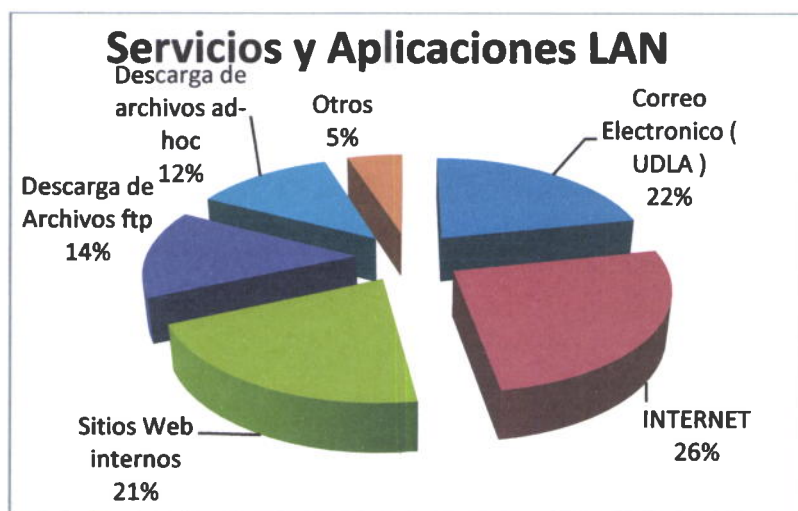


Figura 3- 3 Servicios y Aplicaciones más utilizadas en la red LAN de la UDLA

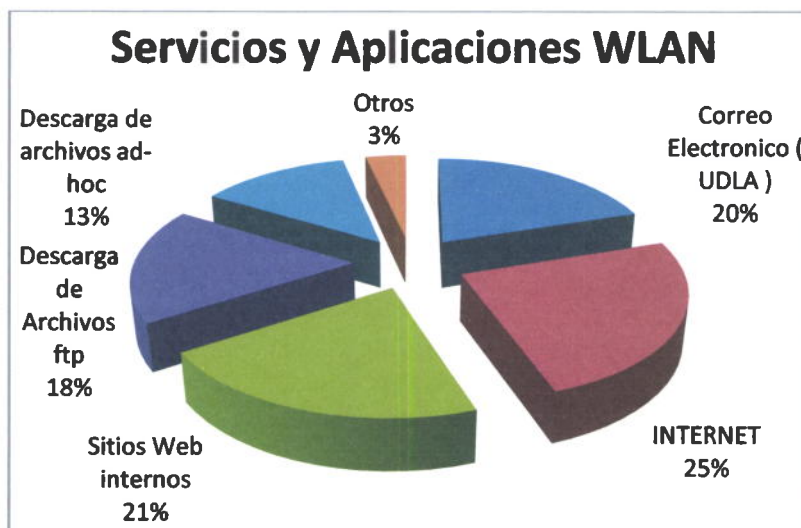


Figura 3- 4 Servicios y Aplicaciones más utilizadas en la red WLAN de la UDLA

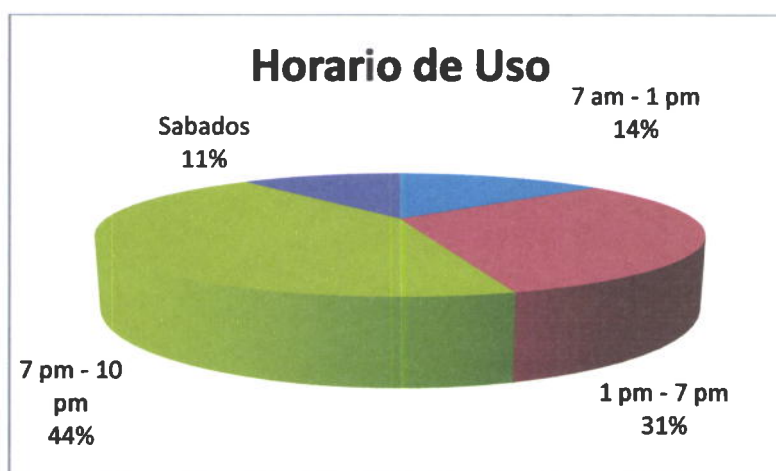


Figura 3- 5 Horarios de utilización de los servicios

El servicio más utilizado por el personal de la UDLA es la navegación http con el 45 % en la red LAN y 46% en la red WLAN, se considera la navegación http al parámetro de Sitios Web internos e Internet. El correo electrónico muestra valores del 20%. Luego sigue descarga de archivos FTP.

3.3.2.2 Percepción del nivel de servicio

Las figuras desde la 3-6 hasta la 3-13 muestran la percepción de los usuarios sobre la red actual inalámbrica, con respecto a las métricas de Ancho de Banda, Cobertura, Disponibilidad, Seguridad, Servicio WLAN, Uso y Calidad de ayuda técnica, e Información de servicios disponibles.

3.3.2.2.1 Ancho de banda

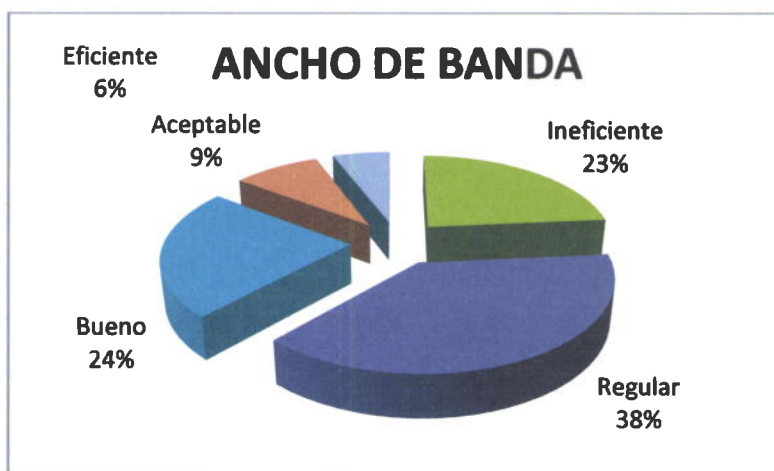


Figura 3- 6 Nivel de Servicio – Ancho de Banda

El 38 % de los encuestados consideran al ancho de banda disponible en la red WLAN regular, el 23% considera ineficiente. Estos resultados muestran el 61% de los encuestados consideran al servicio como Regular e Ineficiente.

3.3.2.2.2 Cobertura

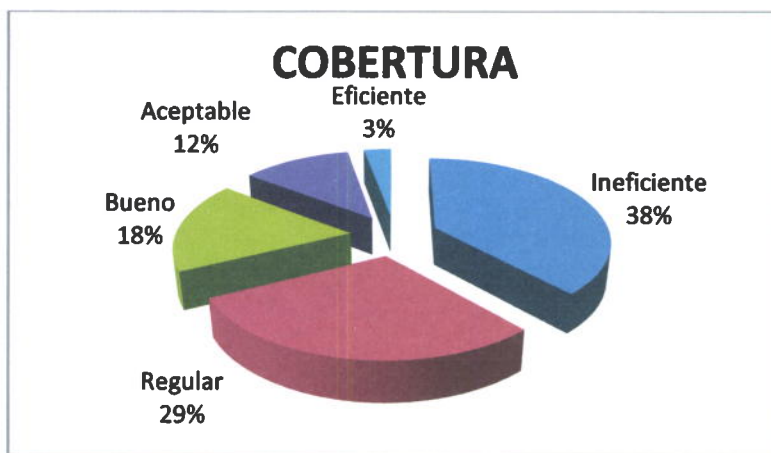


Figura 3- 7 Figura 3-6: Nivel de Servicio – Cobertura

El 38 % de los encuestados consideran a la cobertura de la red WLAN Ineficiente, el 29% considera Regular. Estos resultados muestran que el 67% de los encuestados consideran a la cobertura de la red WLAN como Regular e Ineficiente.

3.3.2.2.3 Disponibilidad.

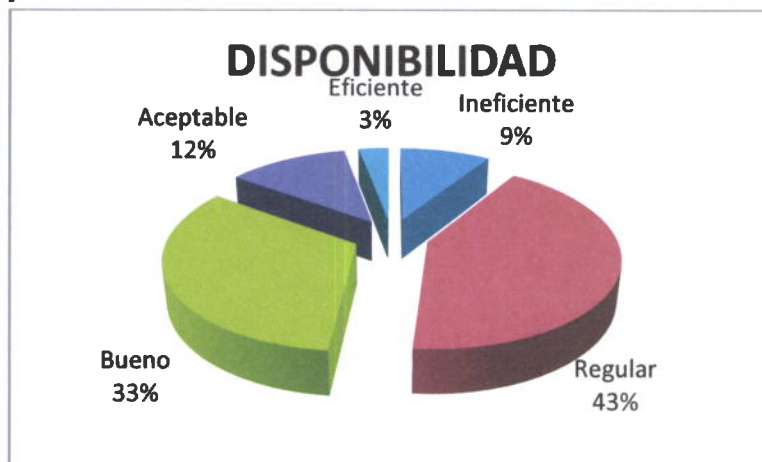


Figura 3- 8 Nivel de Servicio – Disponibilidad

El 43 % de los encuestados consideran a la cobertura de la red WLAN Regular, el 9% considera Ineficiente. Estos resultados muestran que el 52% de los encuestados consideran a la disponibilidad de la red WLAN como Regular e Ineficiente.

3.3.2.2.4 Seguridad

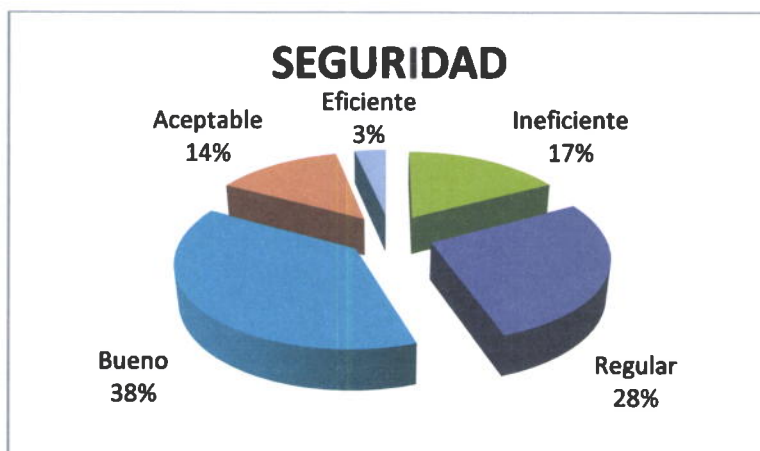


Figura 3- 9 Nivel de Servicio – Seguridad

El 38 % de los encuestados consideran a la seguridad de la red WLAN Bueno, el 28% considera Regular. Estos resultados muestran que el 67% de los encuestados consideran a la seguridad de la red WLAN como Bueno y Regular.

3.3.2.2.5 Percepción del servicio WLAN

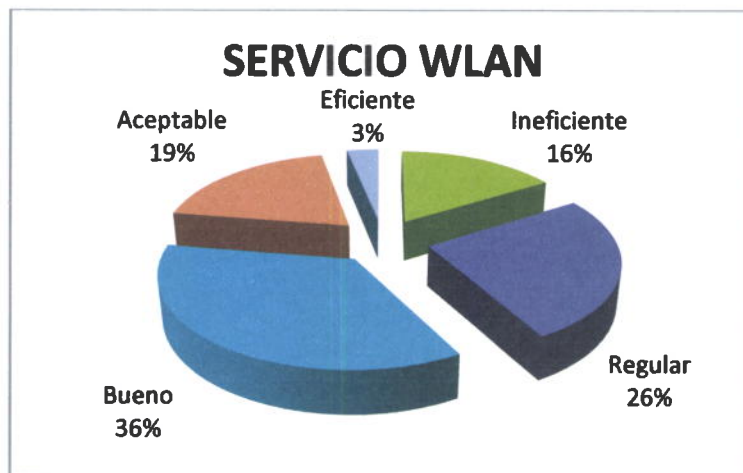


Figura 3- 10 Nivel de Servicio – Percepción del usuario

El 38 % de los encuestados consideran a la seguridad de la red WLAN Bueno, el 26% considera Regular. Estos resultados muestran que el 64% de los encuestados consideran al servicio de la red WLAN como Bueno y Regular.

3.3.2.2.6 Ayuda técnica del servicio WLAN

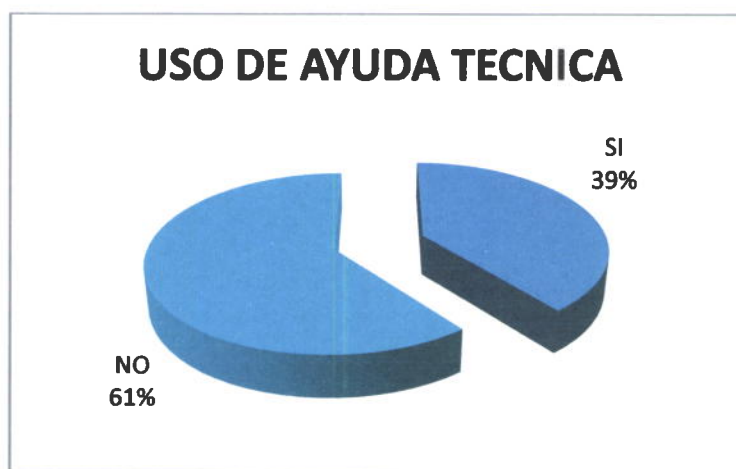


Figura 3- 11 Nivel de Servicio – Utilización de ayuda técnica

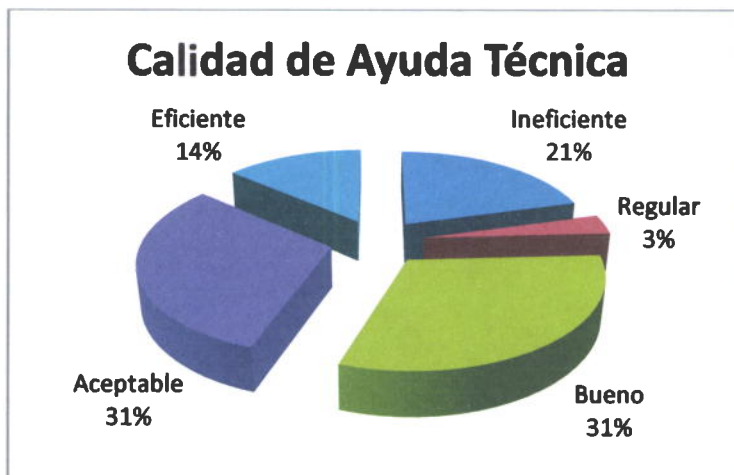


Figura 3- 12 Nivel de Servicio – Calidad de la Ayuda técnica

El 39 % de los encuestados alguna vez han solicitado ayuda técnica sobre el servicio de la red WLAN, de estos usuarios el 62% consideran al servicio Bueno y Aceptable.

3.3.2.2.7 Capacitación

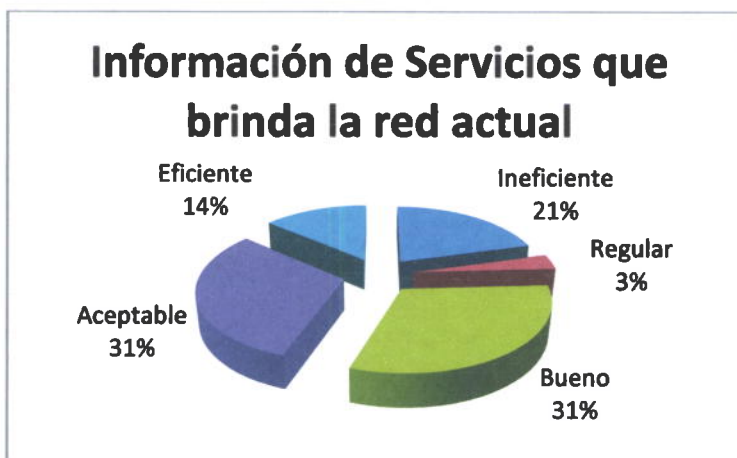


Figura 3- 13 Nivel de Servicio – Información de Servicios

El 62 % de los encuestados consideran que la capacitación brindada acerca de los servicios de la red WLAN son Aceptable y Bueno.

3.3.2.3 Interés del usuario

La figura 3-14 muestra el interés del usuario para la implementación de una nueva red WLAN en el Campus Colón de la UDLA.

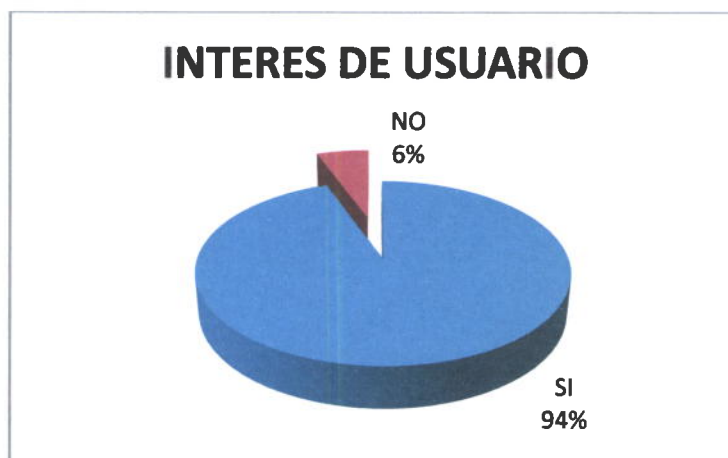


Figura 3- 14 Interés del usuario para la nueva red WLAN

El 94% de los encuestados se considera interesado en la implementación de una nueva red inalámbrica, estos valores están de acuerdo a la percepción del usuario al servicio brindado por la red WLAN actual, el cual en conclusión la mayoría considera a los diferentes parámetros del servicio como Regular e Ineficiente.

3.3.2.4 Ubicación de la red Inalámbrica

La figura 3-15 muestra los sitios físicos más importantes para el usuario donde la nueva red WLAN deberá servir

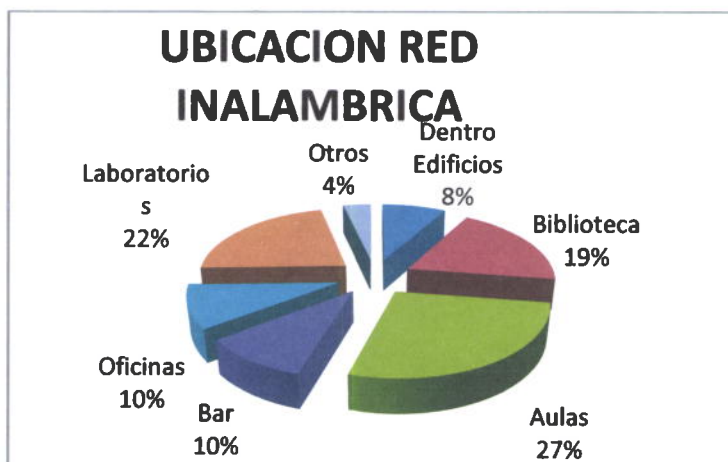


Figura 3- 15 Interés del usuario para la nueva red WLAN

La mayoría considera indispensable tener el servicio inalámbrico en todas las instalaciones internas de los edificios del Campus Colón.

3.3.2.5 Prioridades del servicio

La figura 3-16 muestra el interés del usuario en los diferentes parámetros que deberá tener la nueva red WLAN.

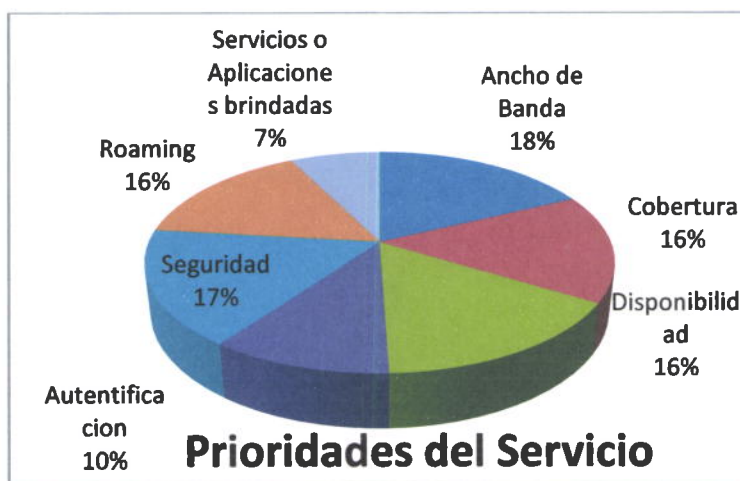


Figura 3- 16 Prioridades del Servicio

Los encuestados consideran al Ancho de Banda, la Disponibilidad, Seguridad, Roaming y Cobertura como los parámetros más importantes a considerar en la nueva red WLAN.

3.3.3 Requerimientos

Una vez finalizado el análisis de los resultados de la encuesta se han determinado: Los requerimientos de servicios y aplicaciones y el nivel de servicio de nueva red WLAN a diseñar; y la ubicación física de los Puntos de Acceso.

3.3.3.1 Requerimientos de servicios y aplicaciones

El acceso a Internet y navegación web a servidores internos son los servicios prioritarios en el diseño de la red inalámbrica en los horarios de 7 pm a 10 pm según el análisis de los resultados de la encuesta.

3.3.3.2 Requerimientos de nivel de servicio

Mediante las encuestas se ha determinado la percepción que tienen los usuarios sobre el nivel de servicio brindado por la WLAN actual. Los datos mostrados en la etapa del análisis reflejan el descontento de los usuarios en cuanto a las métricas seleccionadas para el estudio. También los usuarios muestran mayor interés en unas métricas que en otras que debería tener el nivel de servicio brindado por la nueva red WLAN a diseñar. Estos parámetros son: Ancho de Banda, Disponibilidad, Seguridad, Roaming y Cobertura

3.3.3.3 Requerimientos de nivel de servicio

El 94 % de la comunidad universitaria de la UDLA desea contar con una nueva red inalámbrica en el Campus Colón. De acuerdo a los datos obtenidos de las encuestas, la cobertura de la nueva red WLAN deberá ser en todos los edificios, y en todos sus interiores. Los encuestados no muestran mucho interés en la cobertura en exteriores.

4 Diseño de la Red Wlan

Este capítulo comprende el diseño de la infraestructura tecnológica de la red WLAN para el campus Colón de la UDLA. La propuesta contempla requerimientos de diseño, selección de tecnologías y productos, consideraciones de seguridad, densidad de clientes y ubicación de la red.

El objetivo de este estudio es ofrecer una solución de alto rendimiento, escalable, disponible y segura que permita brindar niveles de servicio adecuados. Se realiza un resumen de los requerimientos de diseño, un análisis comparativo de estándares para la adecuada selección de equipos, un análisis de seguridad, análisis del número de potenciales usuarios y la ubicación de los equipos inalámbricos dentro de las instalaciones de la UDLA campus COLON.

4.1 Requerimientos de diseño

Según la encuesta realizada en el capítulo III literal 3.3.3, acerca de los requerimientos que debería tener la red inalámbrica estos deberían ser:

Disponibilidad, obtenida con un sistema de redundancia y cobertura. El sistema propuesto incluye puntos de acceso en frecuencias separadas. El diseño apropiado de las áreas de cobertura incluye roaming y la adecuada selección de antenas.

Escalabilidad, para que el diseño de red sea escalable debe tener la capacidad de adaptarse a nuevos requisitos de acuerdo a las necesidades de los usuarios, ampliándose tanto en tamaño como en número de usuarios y aun así poder funcionar correctamente.

Interoperabilidad, es lograda a través de los estándares 802.1b y 802.1g. Es preciso que los dispositivos sean interoperables entre ellos así como también con los recursos de la red.

Rendimiento, depende del número de usuarios, de la cobertura, de las atenuaciones, y de los cuellos de botella de la parte cableada de la red.

Seguridad, es lograda en la red con tecnologías que permitan la confidencialidad e integridad de la información, y con la autenticación de cada uno de los usuarios.

4.2 Selección de tecnología y productos

4.2.1 Selección de estándar

La selección del estándar apropiado 802.11a, 802.11b, u 802.11g es fundamental para el diseño de la red inalámbrica. La tecnología 802.11n no será considerada en este análisis, porque se espera tener la versión final del estándar, estimado para noviembre del 2009, aunque muchos fabricantes ya la implementan en sus productos, aun están basados en los borradores del estándar, y por cualquier problema de interoperabilidad, se espera la versión final.

A continuación se realiza una comparación de las principales características de los estándares anteriormente mencionados para posteriormente determinar la mejor opción para el diseño de la red inalámbrica.

4.2.2 Frecuencia y velocidad de transmisión

El estándar 802.11g transmite a 54 Mbps y ofrece la ventaja de ser compatible con los equipos 802.11b que transmiten a 11 Mbps y operan en la misma banda de frecuencia de 2.4 GHz. Esto significa que las tarjetas clientes 802.11b trabajan con puntos de acceso 802.11g, y viceversa. Los dos estándares trabajan en 11 canales, de los cuales solo 3 no se sobreponen, 1,6 y 11. El estándar 802.11a transmite a 54 Mbps a una frecuencia de 5 GHz y tiene de 8 a 23 canales. Los radios de 802.11b/g y 802.11a no interactúan entre sí debido al espectro y técnicas de modulación.

El estándar 802.11a provee las siguientes velocidades de transmisión: 6, 9, 12, 18, 24, 36, 48 y 54 Mbps. El estándar 802.11b transmite a velocidades de 1, 2, 5.5 y 11 Mbps; mientras que el 802.11g proporciona velocidades de transmisión compatibles con 802.11b con velocidades adicionales de 6, 9, 12, 18, 24, 36,48 y 54 Mbps.

4.2.3 Throughput

El throughput es la cantidad de información que se transmite de un lugar a otro en una unidad de tiempo. El throughput es menor a la velocidad de transmisión debido a los siguientes factores:

- **El medio físico:** El medio inalámbrico (aire) no es confiable y puede hacer que se pierdan paquetes y existen retransmisiones.
- **Medio compartido:** Los mecanismos para acceder al medio pueden reducir el rendimiento.
- **Protocolos:** En caso de TCP, se espera un ACK (acuse de recibo) para continuar con el envío de información.
- **Usuarios:** El número de usuarios conectados afectará al throughput.

En la siguiente tabla se observa la velocidad de transmisión teórica y el throughput.

Tabla 4- 1Throughput

Estándar	Velocidad de transmisión (Mbps)	Throughput (Mbps)
802.11b	11	5
802.11g	54	22
802.11a	54	27

El throughput por usuario es el throughput total de una frecuencia dada (canal) dividida para los usuarios en esta frecuencia. Este throughput por usuario determina el máximo throughput teórico que una aplicación o usuario puede utilizar.

Tabla 4- 2Throughput por usuario

Estándar	Velocidad de transmisión (Mbps)	Throughput (Mbps)	Número de usuarios	Throughput promedio por usuario
802.11b	11	5	10	500 Kbps
802.11g	54	25	10	2.5 Mbps
802.11a	54	27	10	2.7 Mbps

4.2.4 Rango de cobertura

La tabla a continuación provee una comparación de las velocidades de transmisión relativas y los rangos de cobertura asociados con los estándares 802.11a y 802.11 b/g. Estos son los rangos máximos, los valores varían dependiendo del ambiente, mientras más obstrucciones se encuentren el rango disminuye.

Tabla 4- 3 Cobertura

Rango de Cobertura y Velocidad de Transmisión	INTERIORES				EXTERIORES			
	802.11a		802.11g		802.11a		802.11g	
	24 m	54 Mbps	30 m	54 Mbps	30 m	54 Mbps	112 m	54 Mbps
45 m	48 Mbps	34 m	48 Mbps	91 m	48 Mbps	140 m	48 Mbps	
60 m	36 Mbps	39 m	36 Mbps	130 m	36 Mbps	170 m	36 Mbps	
69 m	24 Mbps	47 m	24 Mbps	152 m	24 Mbps	210 m	24 Mbps	
76 m	18 Mbps	56 m	18 Mbps	168 m	18 Mbps	250 m	18 Mbps	
84 m	12 Mbps	66 m	12 Mbps	183 m	12 Mbps	300 m	12 Mbps	
91 m	9 Mbps	79 m	9 Mbps	190 m	9 Mbps	400 m	9 Mbps	
100 m	6 Mbps	99m	6 Mbps	198 m	6 Mbps	500 m	6 Mbps	

El hardware que se utilizará en la red inalámbrica se determina antes de empezar el diseño tomando en cuenta que el estándar escogido será 802.11g. Las características de velocidad, throughput, cobertura y seguridad entre los estándares 802.11g y 802.11 a son similares. Finalmente se escogió el estándar 802.11g por la compatibilidad ofrecida hacia equipos con el estándar 802.11b. La mayoría de equipos tienen tarjetas inalámbricas que utilizan este estándar.

4.2.5 Solución Wireless Switching

4.2.5.1 Equipo Gestión Centralizada

En el diseño de la red WLAN de la UDLA se considerará un equipo para la administración centralizada de los Puntos de Acceso a instalarse, y este equipo permitirá que la red WLAN sea una solución escalable y permita convertir gradualmente la red WLAN en un entorno unificado y gestionado de forma centralizada, ya que, a medida que la red Wireless aumenta en tamaño, su gestión se hace más difícil. Este equipo deberá ofrecer una gestión centralizada de políticas, con prestaciones como el ajuste automático de canales y potencia de transmisión ante eventuales fallos de un determinado punto de acceso, el balanceo de carga cuando aumente o disminuya el número de usuarios en un sitio determinado y el roaming transparente L2/L3 de alta velocidad sin cortes a nivel inalámbrico. De la misma forma, que permita la priorización de paquetes de datos sensibles a demora.

Además se necesitará utilizar un equipo que provea suministro de energía a todos los Puntos de Acceso a instalarse en la UDLA, con la finalidad de que el despliegue sea rápido y económico.

A continuación se exponen los principales modelos de tres fabricantes diferentes que son los que mejor han desarrollado la tecnología de gestión centralizada.

Tabla 4- 4 Equipo Gestión Centralizada

Marca	DLINK	CISCO	3COM
Modelo	DWS-3024L	4402	WX2200
Gestión Centralizada	Si	Si	Si
Roaming	Si	Si	Si
Ajuste automático canales	Si	Si	Si
Gestión de potencia	Si	Si	Si
Provee POE	Si	Usar patch panel	Usar patch panel
Puertos de Uplink Gigabit	4	2	2
Número Máximo de Aps	24	25	24

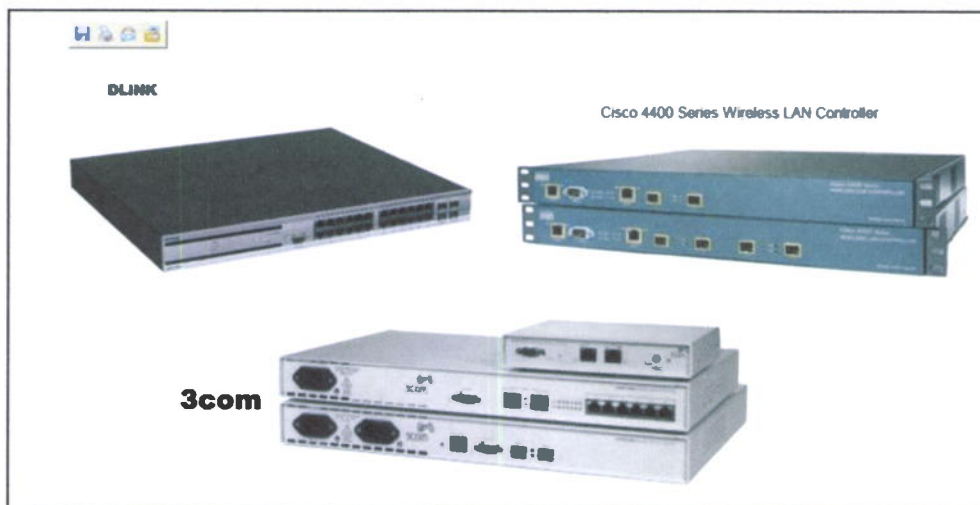


Figura 4- 1 Equipo Gestión Centralizada

Solución Cisco (Cisco Unified Wireless Network)

Escalabilidad: el controlador cisco serie 4400 puede controlar entre 12 y 100 APs, dependiendo del tamaño del lugar de implementación, también de esta opción depende el precio del controlador.

Planeamiento: Posee un software herramienta de planeamiento creado en sociedad con Motorola.

Capacidades de Aps: Una característica importante de este controlador es que soporta Aps autónomos de otras marcas como 3Com y Proxim.

Precio: Un AP Cisco Aironet 1130 G cuesta alrededor de los 500 a 600 usd, el controlador alrededor de los 7000 y 8000 usd para 25 Aps, el sistema de administración llamado WCS (Wireless Control System) que es software que debe ser instalado en un servidor Windows Server o Linux tiene un valor adicional de 1000 usd para 100 Aps.⁶⁵

Tabla 4- 5 Costo de la solución Cisco (Solo equipos)

Equipo	Cantidad	Precio	Total
Cisco Wireless Controller	1	7000	7000
Wireless Control System (Sw)	1	1000	1000
Aps Aironet 1130g	1	520	520
Total			8520

⁶⁵ Fuente: Computer Shopper, se comparan precios entre los más importantes distribuidores a nivel mundial

Cisco es una solución extremadamente robusta, que comprende tres componentes, los APs, el controlador inalámbrico Cisco Wireless Controller y el WCS; en la sede Norte o campus Granados se optó por usar esta infraestructura, sin embargo debido a los altos costos de esta solución para un número relativamente bajo de usuarios a servir en el campus Colón se optará por una plataforma más económica.

Solucion 3com (3Com Wireless LAN Mobility System)

La solución 3Com consta del controlador inalámbrico 3Com Wireless LAN Controller , switch 3Com Wireless LAN Switch WX1200, el software 3Com Wireless Switch Manager y los Aps 3Com wireless LAN Managed Access Points (MAPs). Un dato importante es que el Controlador y el switch son hardware separado.

Escalabilidad: el 3Com Wireless LAN Controller está inicialmente configurado para soportar 24 MAPs, en el caso de requerir mas MAPs se los puede incrementar en grupos de 24 hasta llegar a un total de 192 MAPs. Cada upgrade de 24 MAPs tiene un costo adicional.

Planeamiento: La solución 3Com no ofrece una herramienta de planeamiento.

Capacidades de Aps: Una característica particular de los APs 3com modelo 3850 es que pueden ser configurados como bridges para unir 2 edificios.

Precio: El 3Com Wireless LAN Controller se encuentra entre los 5000 y 7000 usd, el Wireless LAN Switch WX1200 se encuentra entre los 2000 y 3000 usd, el 3Com Wireless Switch Manager se encuentra alrededor de los 3500 usd y cada MAP se encuentra a 250 usd.⁶⁶

Tabla 4- 6 Costo de la solución 3Com (Solo equipos)

Equipo	Cantidad	Precio	Total
3Com Wireless Lan Controller	1	6000	6000
Wireless Lan Switch	1	2000	2000
3Com Wireless Switch Manager (Sw)	1	3500	3500
Aps 3Com 2750	1	250	250
Total			11750

⁶⁶ Fuente: Computer Shopper, se comparan precios entre los más importantes distribuidores a nivel mundial

3Com es otra marca de mucho peso en el ambiente del networking, y como se puede observar el costo es más elevado al de Cisco debido a los múltiples componentes que conforman la solución.

Solución D-link

La solución D-Link resulta más transparente ya que consta solo de dos componentes que son el Wireless Switch DWS-3024L y los Access Points DWL-3500AP

Entre las principales funciones del Wireless Switch D-link está la gestión centralizada de la red inalámbrica y sus avanzadas políticas de seguridad, así como el control unificado de todos los puntos de acceso conectados al switch, pueden ser hasta 24 en total, para esto cuenta con su software de administración Smart WLAN Manager que se puede ejecutar desde cualquier pc conectado a la red. En el caso de requerir mas APs solo se incrementan los switches en cascada.

Esta solución ofrece una gestión centralizada de políticas, ya que es posible administrar los puntos de acceso desde el switch, con prestaciones como el ajuste automático de canales y potencia de transmisión ante eventuales fallos de un determinado punto de acceso, cuando un AP es apagado o reporta ausencia en la red, los APs mas próximos incrementan su potencia un 20% para solventar el problema.

Asimismo, permite la priorización de paquetes de datos sensibles a demora, una prestación especialmente indicada para aplicaciones de VoIP y otras que exigen mayor ancho de banda. La gestión de la seguridad de los puntos de acceso podrá realizarse desde el propio switch.

Este Switch incorpora la tecnología Gigabit Ethernet en sus 24 puertos, además de POE en todos sus puertos.

Otro aspecto interesante de esta plataforma es que los APs no deben estar necesariamente conectados al Wireless Switch, por lo que se puede en el caso de necesitarlo, hacer uso de los diversos switches.

En cuanto a precios, el Wireless Switch DWS-3024L tiene un precio de 3630 usd y cada AP DWL-3500AP 286 usd.⁶⁷

Tabla 4- 7 Costo de la solución D-Link (Solo equipos)

Equipo	Cantidad	Precio	Total
Wireless Switch DWS-3024L	1	3630	3630
DWL-3500AP	1	286	286
Total			3916

Luego de este análisis tanto de características técnicas como de costos, se procede a escoger D-Link ya que presentó como solución a estas necesidades la Integración de todas las Soluciones en una Wireless LAN conectada a la red existente y además por sus precios aceptables, se evidencia de inmediato casi un 50% menos costo que los otros fabricantes.

Es así como la Universidad de las Américas implementará en su sede Colón un Wireless Switch D-Link DWS-3024L este dispositivo le permite al Departamento de Sistemas conocer las características de cada Access Point que compone la red, el número de usuarios que se encuentran conectados en cada sector y solucionar los posibles problemas que se puedan presentar gracias a los reportes que envía.

Siguiendo con la línea D-Link, también se implementarán Access Point D-Link DWL-3500AP, que es el modelo compatible con el Wireless Switch DWS-3024L, distribuidos en todo el campus; estos equipos son diseñados especialmente para instalaciones en interiores, los cuales ofrecen opciones seguras para que los administradores de la infraestructura desarrollen una red inalámbrica robusta y gestionable; además sus dos antenas proporcionan una óptima cobertura inalámbrica.

⁶⁷ Fuente: Computer Shopper, se comparan precios entre los más importantes distribuidores a nivel mundial

Adicional a esto, el Switch realiza de manera automática el control de potencia e interferencia de la red, facilita la administración del ancho de banda y de los Access Points, para optimizar el tráfico de información. A través de esta solución el campus Colón puede configurar y mantener la red, gracias a la plataforma de gestión centralizada que ofrecen los equipos D-LINK.

4.2.5.2 Puntos de acceso

Al ser una plataforma propietaria, la solución Wireless Switch Dlink debe trabajar con sus propios Ap's, sin embargo se observaron las opciones de los mismos tres diferentes fabricantes, únicamente con el fin de constatar y ratificar el por qué de la elección de esta solución:

Tabla 4- 8 Equipos Puntos de Acceso Inalámbricos

EQUIPOS PUNTO DE ACCESO INALAMBRICO			
DATOS DE FABRICACION			
Marca	DLINK	CISCO	3COM
Modelo	DWL-3500AP	Aironet 1130 G	AP2750
ESPECIFICACIONES			
PUERTOS			
LAN	1 RJ-45 10 100BASE-TX Ethernet MDI MDK	Autosensing S02.3 and 100Base-T Ethernet	Autosensing 802.3 and 100Base-T Ethernet
Puerto de alimentación	Si	Si	Si
ESTANDARES SOPORTADOS			
Certificación	Wi-Fi, WPA2 Personal y WPAa Empresarial	Wi-Fi, WPA2 Personal y WPAa Empresarial	Wi-Fi, WPA2 Personal y WPAa Empresarial
Protocolos	IEEE 802.11b, 802.11g	IEEE 802.11 a, b, 802.11g	IEEE 802.11b, 802.11g
ACCESO AL MEDIO			
Frecuencias de Funcionamiento	2.4 - 2.4835 Ghz	2.4 - 2.4835 Ghz	2.4 - 2.4835 Ghz
Modulación	DSSS y OFDM	DSSS y OFDM	DSSS y OFDM
Protocolo de Acceso al Medio	CSMA/CA	CSMA/CA	CSMA/CA
Rango de Operación	Hasta 100 m	Hasta 100 m	Hasta 100 m
Antena	Dual 5 dBi Removable con conector R-SMA	3.0 dBi	2dBi
SEGURIDAD			
Encriptación 1	128 bit WPA/WPA2 con TKIP AES	128 bit WPA/WPA2 con TKIP AES	128 bit WPA/WPA2 con TKIP AES
Encriptación 2	64/128 bit y 152 bit	64/128 bit y 152 bit	64/128 bit y 152 bit
	WEP Llave compartida	WEP Llave compartida	WEP Llave compartida
CONFIGURACION Y ADMINISTRACION			
Interface de Usuario	Web-Browser	Web-Browser	Web-Browser
ALIMENTACION			
Power of Ethernet	Si	Si	Si

Tipo de Corriente	DC	DC	DC
Potencia	6.24	9.91 W	6W
Potencia de Transmisión Inalámbrica	22 dBm	17 dBm	20 dBm



Figura 4- 2 Puntos de Acceso DLINK, 3COM y CISCO

Como se puede observar el equipo DLINK ofrece mayor cobertura por su máxima potencia de transmisión de 22 dBm y además posee la mayor ganancia con sus dos antenas de 5 dBi, las cuales además son desmontables y en caso de requerir mayor ganancia se las puede sustituir.

4.3 Ubicación de la red

De acuerdo al análisis de requerimientos realizado en el capítulo anterior se considerará la ubicación de los puntos de Acceso dentro y fuera de los edificios. Dentro de los edificios, se demanda el servicio en aulas, bibliotecas, laboratorios, oficinas y en el bar. La ubicación fuera de los edificios contempla el espacio recreativo debajo de la torre Chile.

4.4 Densidad de usuario

El ancho de banda que se asigna a cada uno de los usuarios de la red inalámbrica depende del número de usuarios concurrentes por punto de acceso, el número de usuarios recomendados por punto de acceso es de 20 a 25, referencia tomada para el proyecto. Para la ubicación de los puntos de acceso se ha estimado el número de usuarios concurrentes por espacio físico en las horas cuando la red tiene mayor demanda de usuarios.

El número de usuarios concurrentes que se conectarán a un Punto de Acceso se define por el porcentaje de personas que desean el servicio en determinada ubicación, este valor fue obtenido por las encuestas realizadas en el punto 3.3.2.4 y por número de promedio de personas en cada ubicación, los resultados son los siguientes:

Tabla 4- 9 Densidad de Usuarios

Ubicación	Promedio Personas	% Personas desean Servicio WLAN	Número de Usuarios
Aulas y Laboratorios	35	27% -22%	10 -8
Oficinas	3	10%	1
Biblioteca	50	19%	10

Se considerará un número de usuarios de 10 por aula, laboratorio y biblioteca. Las oficinas no se considerará en el diseño debido a que es un valor bajo. Estos resultados entregan una aproximación del número de personas que desean el servicio en estos lugares.

4.5 Consideraciones de seguridad

El principal requerimiento de seguridad que se debe considerar para la red inalámbrica es la reducción de los riesgos asociados, tales como: interceptación del tráfico de red, acceso a la red de usuarios no autorizados, entre otros. La solución propuesta consta de los elementos que se describen a continuación:

Puntos de Acceso: Los puntos de acceso deben basarse en el estándar 802.11i con la utilización del sistema WPA-2(WIFI Protect Access) Enterprise, es decir

se utilizará para la gestión de claves TKIP (Temporal Integrity Protocol), este protocolo permite la gestión de claves dinámicas. Además para la autenticación de usuarios se utilizará 802.1x. Este sistema WPA-2 Enterprise utiliza para la confidencialidad y la integridad de la información, un protocolo basado en AES.

Servidor Radius: Recibe las solicitudes de autenticación de los clientes reenviadas por los puntos de acceso y los verifica en la base de datos. Los puntos de acceso utilizan 802.1x para comunicarse con el servidor RADIUS.

Base de Datos: La información de los usuarios se encuentra almacenada en una base de Datos la que guarda de forma centralizada las cuentas de usuarios con sus características y claves. Si no se dispone de un servidor de base de datos, se puede utilizar el servicio de directorio LDAP (**Lightweight Directory Access Protocol**).

4.5.1 Arquitectura

El esquema lógico del componente de seguridad inalámbrico para la WLAN se muestra en la figura 4-3.

El proceso de autenticación y autorización de un usuario para acceder a la red es el siguiente:

1. El cliente inalámbrico solicita al punto de acceso permiso para establecer una conexión y acceder a la red. Para ello le envía una solicitud con su clave privada.
2. El punto de acceso está configurado para reenviar la solicitud al servidor RADIUS con la utilización del protocolo 802.1x.
3. El servidor RADIUS, consulta al servidor de base de datos o al directorio LDAP para comprobar los datos del usuario y su validez.
4. El servidor RADIUS determina si el usuario tiene acceso a la red y envía la autorización al punto de acceso.

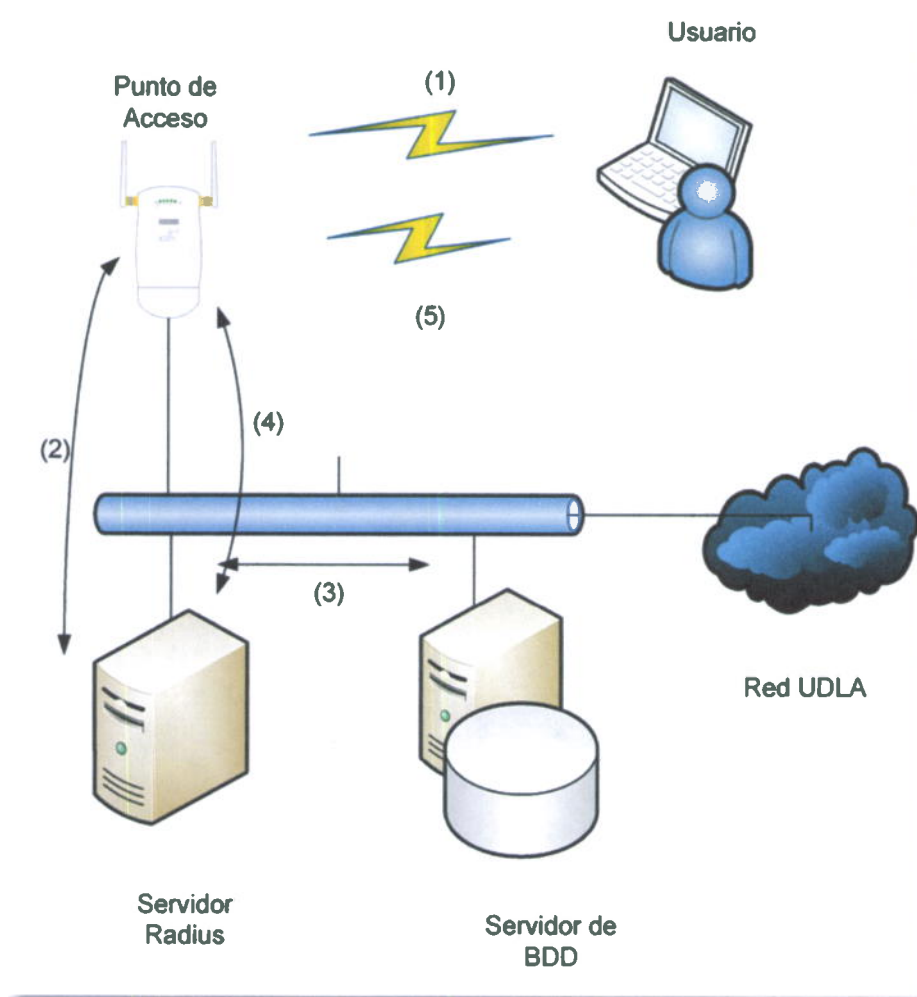


Figura 4- 3 Arquitectura de Seguridad

5. El punto de acceso inicia un intercambio de claves para establecer un cifrado de sesión con el cliente, permitiéndole así acceder a la red de forma segura.

En la red inalámbrica de la UDLA – Colón se utilizará la versión de software libre de un servidor RADIUS, cuyo nombre es FreeRadius, concretamente la versión estable 2.1.6. Se decidió la utilización de este software debido a su costo cero y porque es utilizado por muchas compañías que se encuentran ubicadas dentro de las 500 mejores empresa de la revista FORTUNE.

El servidor de Base de Datos será de software libre. MySQL ha sido escogido por ser su costo cero y por ser una base de datos estable, y que cumple con

los requerimientos de rendimiento necesarios para la implementación de la seguridad 802.1x.

Estos dos servidores serán almacenados en un equipo con Sistema Operativo Linux.

A continuación se exponen las características de Hardware del Servidor escogido para la solución de la red inalámbrica de la UDLA.

Tabla 4- 10 Servidor

CARACTERISTICAS SERVIDOR HP ML350 G6	
Procesador	
Descripción de procesador	(1) Quad-Core Intel® Xeon® E5420 Processor (2.50 GHz, 80 Watts, 1333 FSB)
Cantidad de procesadores	1
Velocidad del procesador	2.50 GHz
Tipo de procesador	(1) Quad-Core Intel® Xeon® E5420 Processor (2.50 GHz, 80 Watts, 1333 FSB)
"Front Side Bus" del procesador	1333 MHz
Memoria	
Memoria estándar	2 GB (2 x 1GB) standard
Características de protección de memoria	Online Spare; Mirrored Memory; Advanced EFF
Descripción de cache	12MB (2 x 6MB) Level 2 cache
Conexión de red	
Controlador de red	Embedded NC373i Multifunction Gigabit Server Adapter
Almacenamiento	
Capacidad de almacenamiento	1.168TB SFF SAS; 480GB SFF SATA
Controlador de almacenamiento	Smart Array E200i/128 BBWC Controller (RAID 0/1/1+0/5)
Conexión de almacenamiento estándar	Hot plug SFF SAS; Hot plug SFF SATA; Hot plug 3.5-inch SAS; Hot plug 3.5-inch SATA
Características de sistema	
Detalle de administración remota	Integrated Lights-Out 2 (iLO 2)
Software	
Software de administración remota	Integrated Lights-Out 2 (iLO 2)

4.6 Interferencias

Las interferencias pueden ser:

- Interferencia CoCanal: Es una interferencia que se presenta cuando dos Puntos de Acceso transmiten en la misma banda de frecuencias.
- Interferencia Intercanal: Es una interferencia que se presenta cuando un Punto de Acceso transmite en una banda de frecuencias diferente a la banda de frecuencias del Punto de Acceso utilizado.

Estos dos tipos de interferencia pueden limitar con severidad la capacidad de la red inalámbrica. Por estos motivos se diseñará la red inalámbrica de la UDLA ubicando los Puntos de Acceso de la siguiente manera:

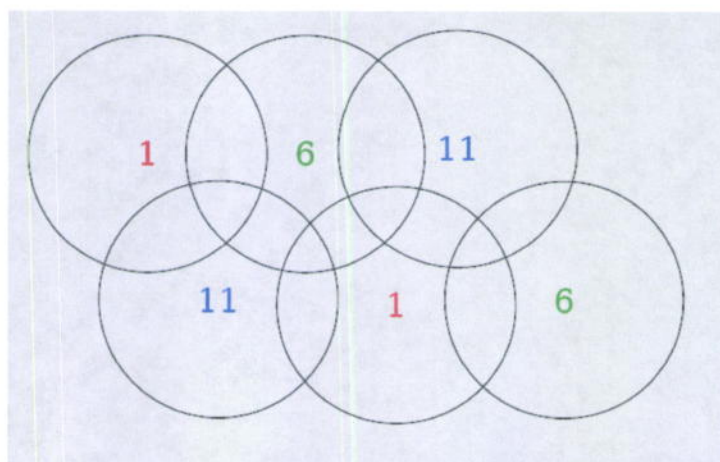


Figura 4- 4 Interferencias

4.7 Pruebas

Con el equipo seleccionado en el punto 4.2.6, se procede a realizar pruebas. Se utilizó el software Ekahau Mapper⁶⁸. Con este software se obtuvo las figuras de la cobertura de los Puntos de Acceso. Los puntos de Acceso fueron ubicados en tres posiciones: Patio (Bajos de la Torre Chile), Biblioteca y Torre Chile. Según los diagramas de cobertura en el Patio y Biblioteca se seleccionaron 5 puntos en los cuales se hicieron mediciones de: Throughput⁶⁹,

⁶⁸ Ekahau HeatMapper es una herramienta gratis para el mapeo fácil y rápido de la cobertura de redes Wi-Fi

⁶⁹ Para la medición del throughput en los puntos se utilizó la herramienta QCheck e Iperf

Recepción de Señal⁷⁰ y Tiempos de Respuesta⁷¹. En la Torre Chile se ubicó un solo punto debido a que toda el área tiene buena recepción. A continuación se muestran estos resultados:

4.7.1 AP Patio (Bajos de la Torre Chile)

Área de Cobertura para el Primer Punto de Acceso

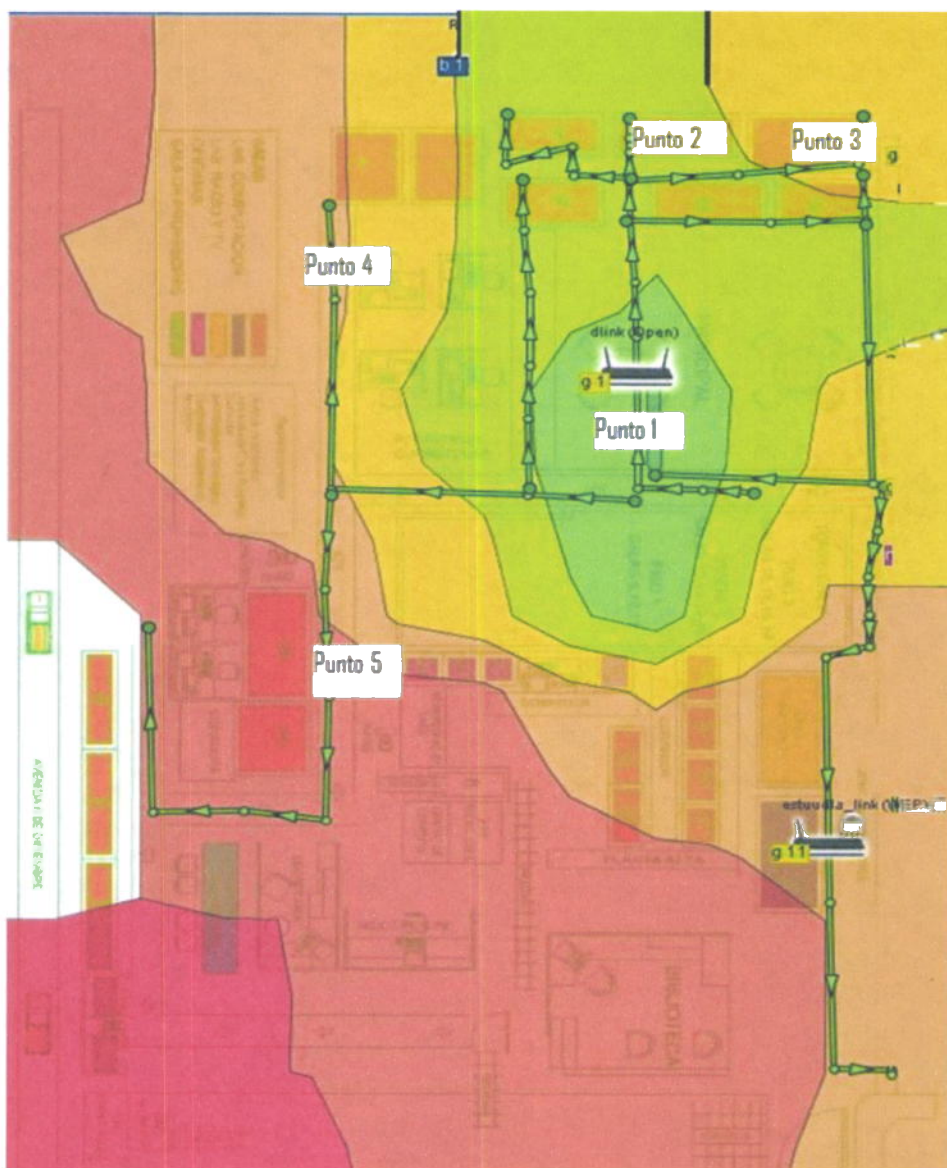


Figura 4- 5 Área Cobertura Primer Punto de Acces

⁷⁰ Para la medición de recepción de la señal se utilizó la herramienta de software VistaStumbler

⁷¹ Para la medición de los tiempos de respuesta se utilizó la herramienta ping.exe

4.7.1.1 Throughput

Tabla 4- 11 Throughput con herramienta Qcheck

Punto	Mediciones (Mbps)										Mínimo	Máximo	Promedio
	1	2	3	4	5	6	7	8	9	10			
1	18.60	19.51	18.18	19.04	20	18.60	19.04	18.40	19.50	19.87	18,18	20	19.07
2	15.38	15.09	14.81	15.09	14.81	13.79	17.93	15.40	16.50	14.98	13.79	17.93	15.38
3	12.5	13.33	14.03	15.38	12.12	13.79	11.11	12.45	13.56	13.45	11.11	15.38	13.17
4	9.09	10	13.11	11.59	10.95	12.50	9.09	9.56	9.87	9.03	9.03	13.11	10.48
5	0.20	0.23	0.21	0.69	0.14	0.04	0.34	0.45	0.52	0.65	0.04	0.69	0.35

Tabla 4- 12 Intervalos y Throughput con herramienta Iperf

Punto	Intervalo	Bytes Transf.	Throughput
1	10	24.0	20.10
2	10	23.7	19.90
3	10	15.8	13.30
4	13.1	8.02	5.14
5	11.8	.176	0.12

```

C:\>iperf -s
Server listening on TCP port 5001
[CP window size: 8.00 KByte (default)]

[148] local 192.168.0.1 port 5001 connected with 192.168.0.200 port 3904
[ ID] Interval      Transfer      Bandwidth
[148] 0.0-10.0 sec  24.0 MBytes  20.1 Mbits/sec
[168] local 192.168.0.1 port 5001 connected with 192.168.0.200 port 3905
[ ID] Interval      Transfer      Bandwidth
[168] 0.0-10.0 sec  23.7 MBytes  19.9 Mbits/sec
[176] local 192.168.0.1 port 5001 connected with 192.168.0.200 port 4162
[ ID] Interval      Transfer      Bandwidth
[176] 0.0-10.0 sec  15.8 MBytes  13.3 Mbits/sec
[164] local 192.168.0.1 port 5001 connected with 192.168.0.200 port 4516
[ ID] Interval      Transfer      Bandwidth
[164] 0.0-13.1 sec  8.02 MBytes  5.14 Mbits/sec
[168] local 192.168.0.1 port 5001 connected with 192.168.0.200 port 4611
[ ID] Interval      Transfer      Bandwidth
[168] 0.0-11.8 sec  176 KBytes   122 Kbits/sec

```

Figura 4- 6 Intervalos y Throughput con herramienta iperf

4.7.1.2 Sensibilidad de la señal

Tabla 4- 13 Recepción de señal

Punto	Sensibilidad de Recepción (dbm)	Velocidad de conexión (Mbps)
1	-50	54
2	-65	48
3	-70	24
4	-80	18
5	-85	5.5

4.7.1.3 Tiempos de respuesta

Tabla 4- 14 Tiempos de Respuesta

Punto	Mínimo (ms)	Máximo (ms)	Promedio (ms)
1	1	98	2
2	2	2	2
3	1	28	2
4	1	1779	30
5	2	1339	101

4.7.1.4 Mediciones



Figura 4- 7 Mediciones en el Punto 1

4.7.2 AP Biblioteca

Área de Cobertura para el Punto de Acceso de la biblioteca

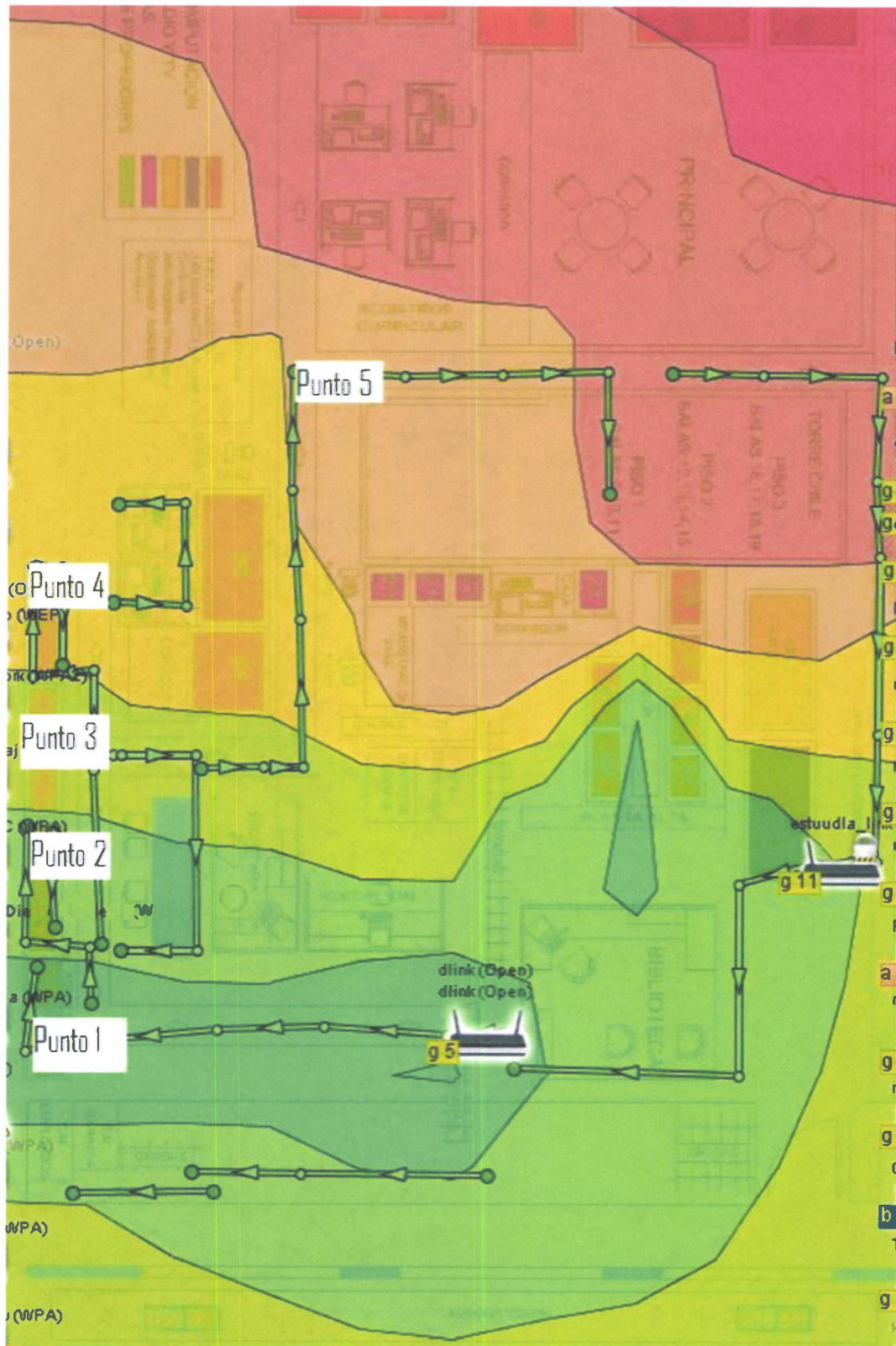


Figura 4-12 Mediciones Señal Punto de Acceso Biblioteca

4.7.2.1 Throughput

Tabla 4- 15 Mediciones Throughput con herramienta Qcheck

Punto	Mediciones (Mbps)										Mínimo	Máximo	Promedio
	1	2	3	4	5	6	7	8	9	10			
1	24.50	24.10	24.31	24.60	24.46	24.34	24.23	24.65	24.34	24.36	24.10	24.65	24.38
2	22	20.72	22.70	23.30	23	21.76	21.87	20.78	21.23	22.56	20.72	23.30	21.99
3	12.50	12.80	7.60	8.80	11.14	13.56	10.54	11.23	10.65	10.98	7.60	13.56	10.98
4	3.59	4.80	4.90	5.50	4.26	5.60	4.30	6.70	7.30	5.60	3.59	7.30	5.25
5	0.14	0.24	2.70	2.19	0.76	0.34	0.43	0.98	0.45	1.54	0.14	2.70	0.98

Tabla 4- 16 Mediciones Throughput con herramienta Iperf

Punto	Intervalo	Bytes Transf.	Throughput
1	5.9	16.4	23.40
2	4.9	11.5	19.80
3	2.5	3.22	10.70
3	10	13.7	11.50
3	8.1	11.7	12.00
4	6.2	5.53	7.43
5	6	1.57	2.20

```

C:\>iperf -s
-----
Server listening on TCP port 5001
TCP window size: 8.00 KByte (default)
-----
[148] local 192.168.0.1 port 5001 connected with 192.168.0.25 port 50142
[ ID] Interval      Transfer      Bandwidth
[148] 0.0- 5.9 sec  16.4 MBytes  23.4 Mbits/sec
[172] local 192.168.0.1 port 5001 connected with 192.168.0.25 port 50149
[ ID] Interval      Transfer      Bandwidth
[172] 0.0- 4.9 sec  11.5 MBytes  19.8 Mbits/sec
[160] local 192.168.0.1 port 5001 connected with 192.168.0.25 port 50157
[ ID] Interval      Transfer      Bandwidth
[160] 0.0- 2.5 sec   3.22 MBytes  10.7 Mbits/sec
[156] local 192.168.0.1 port 5001 connected with 192.168.0.25 port 50158
[ ID] Interval      Transfer      Bandwidth
[156] 0.0-10.0 sec  13.7 MBytes  11.5 Mbits/sec
[152] local 192.168.0.1 port 5001 connected with 192.168.0.25 port 50159
[ ID] Interval      Transfer      Bandwidth
[152] 0.0- 8.1 sec  11.7 MBytes  12.0 Mbits/sec
[160] local 192.168.0.1 port 5001 connected with 192.168.0.25 port 50166
[ ID] Interval      Transfer      Bandwidth
[160] 0.0- 6.2 sec   5.53 MBytes   7.43 Mbits/sec
[148] local 192.168.0.1 port 5001 connected with 192.168.0.25 port 50172
[ ID] Interval      Transfer      Bandwidth
[148] 0.0- 6.0 sec   1.57 MBytes   2.20 Mbits/sec

```

Figura 4-13 Mediciones Throughput con herramienta Iperf

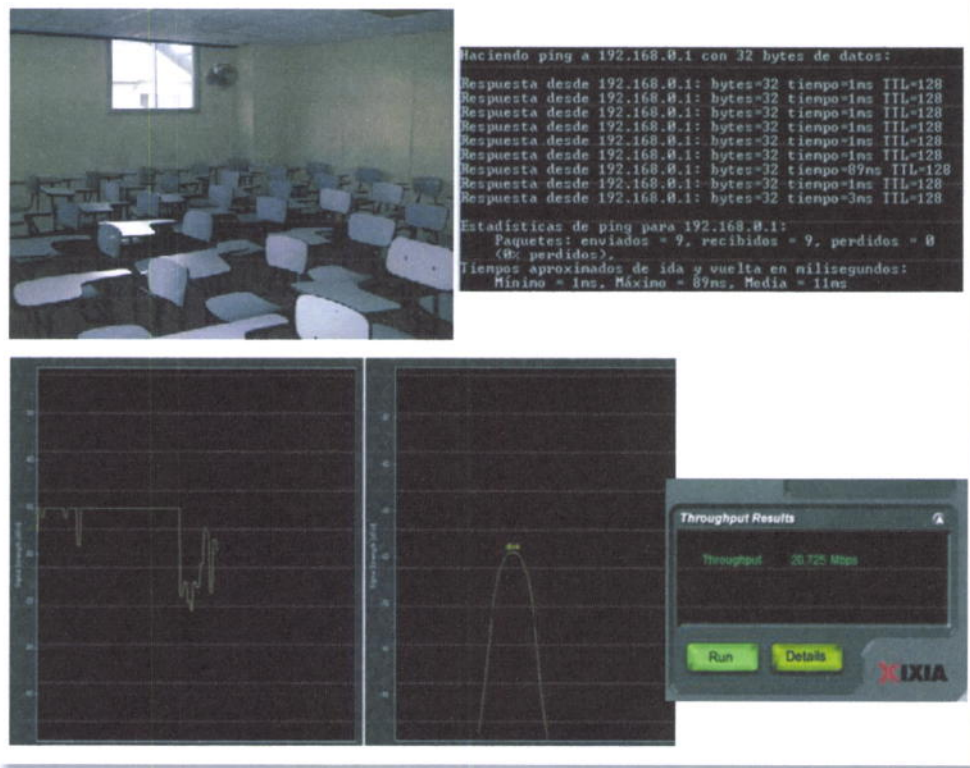


Figura 4-15 Mediciones en el Punto 2

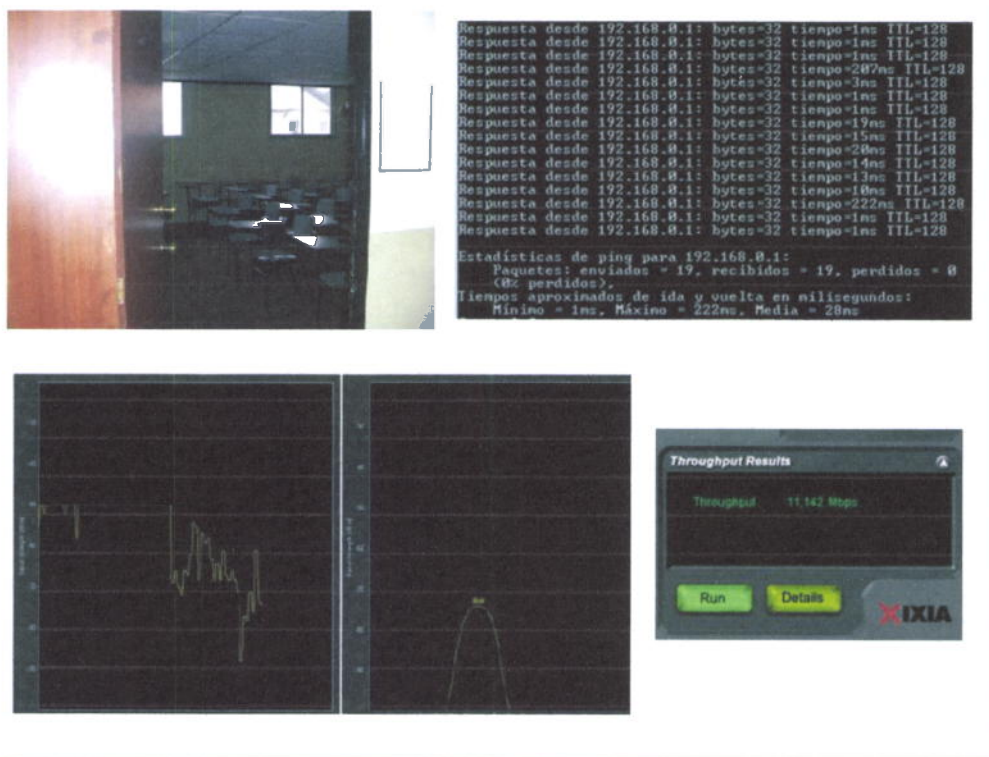


Figura 4-16 Mediciones en el Punto 3

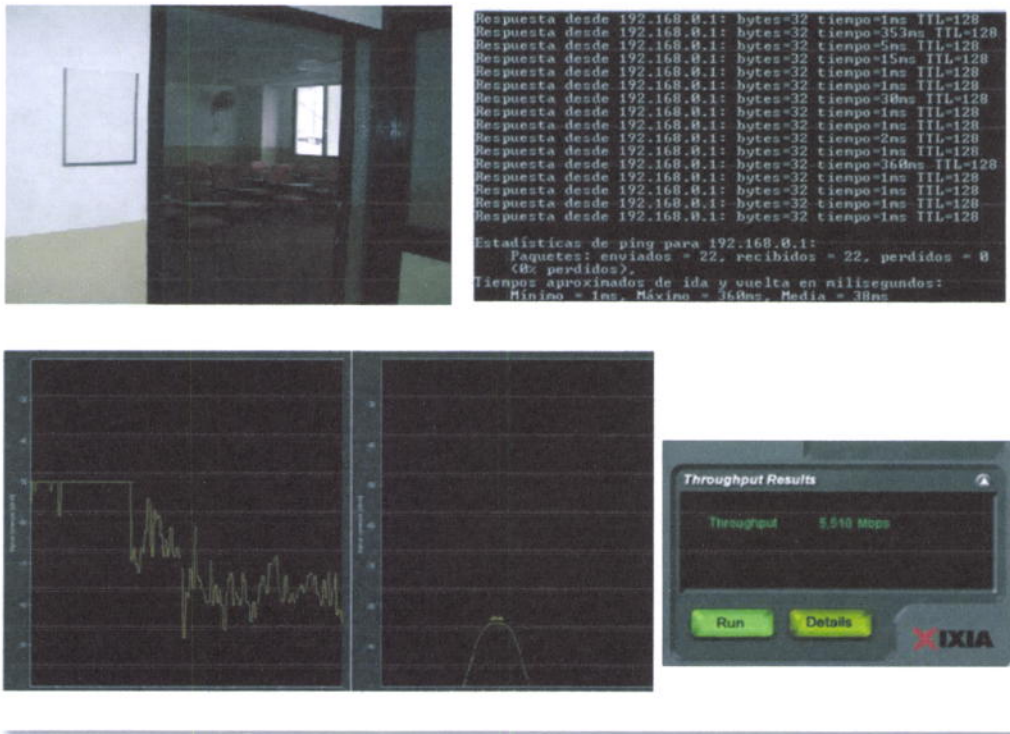


Figura 4-17 Mediciones en el Punto 4



Figura 4-18 Mediciones en el Punto 5

4.7.3 Ap Torre Chile



Figura 4-19 Mediciones Señal en Torre Chile

4.7.3.1 Throughput

Tabla 4- 19 Intervalos y Throghput con herramienta IPERF

Punto	intervalo	Bytes Transf.	Throughput
1	10	24.5	20.6
1	10	22.9	19.2
1	10	22.6	19,0
1	13.1	20.5	17.2

```

Administrador: Símbolo del sistema - iperf -s
C:\>iperf -s
Server listening on TCP port 5001
TCP window size: 8.00 KByte (default)

[148] local 192.168.0.1 port 5001 connected with 192.168.0.200 port 1083
[ ID] Interval      Transfer     Bandwidth
[148] 0.0-10.0 sec  24.5 MBytes  20.6 Mbits/sec
[172] local 192.168.0.1 port 5001 connected with 192.168.0.200 port 1279
[ ID] Interval      Transfer     Bandwidth
[172] 0.0-10.0 sec  22.9 MBytes  19.2 Mbits/sec
[160] local 192.168.0.1 port 5001 connected with 192.168.0.200 port 1280
[ ID] Interval      Transfer     Bandwidth
[160] 0.0-10.0 sec  22.6 MBytes  19.0 Mbits/sec
[156] local 192.168.0.1 port 5001 connected with 192.168.0.200 port 1312
[ ID] Interval      Transfer     Bandwidth
[156] 0.0-10.0 sec  20.5 MBytes  17.2 Mbits/sec

```

Figura 4-20 Mediciones Throughput con herramienta Iperf

4.7.3.2 Sensibilidad de la señal

Tabla 4- 20 Recepción de Señal

Punto	Sensibilidad de Recepción (dbm)	Velocidad de conexión (Mbps)
1	-55	54

4.7.3.3 Tiempos de respuesta

Tabla 4- 21 Tiempos de Respuesta

Punto	Mínimo (ms)	Máximo (ms)	Promedio (ms)
1	1	76	5

4.7.3.4 Mediciones

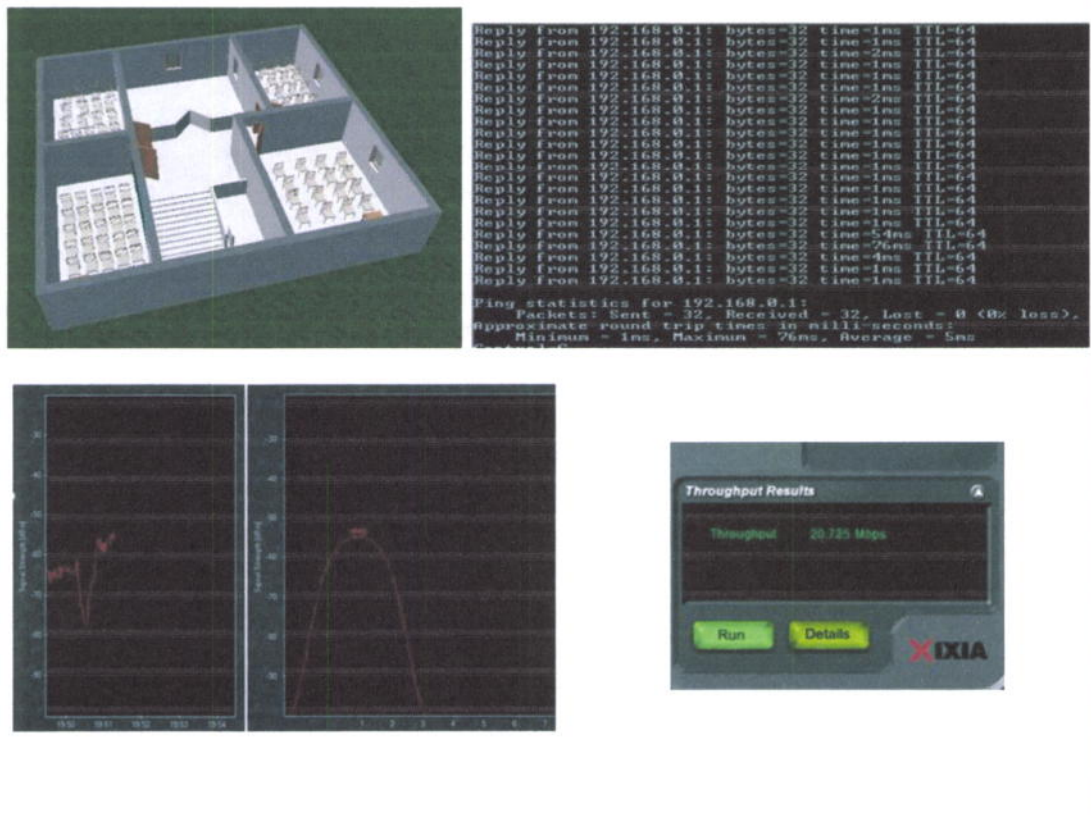


Figura 4-21 Mediciones en el Punto 1

4.8 Diseño de la solución

La red inalámbrica LAN de la UDLA – COLON, constará de los siguientes equipos de red:

- Puntos de Acceso.
- Equipo de Gestión Centralizada.
- Servidor RADIUS y Base de Datos.

El diagrama de Red es el siguiente:

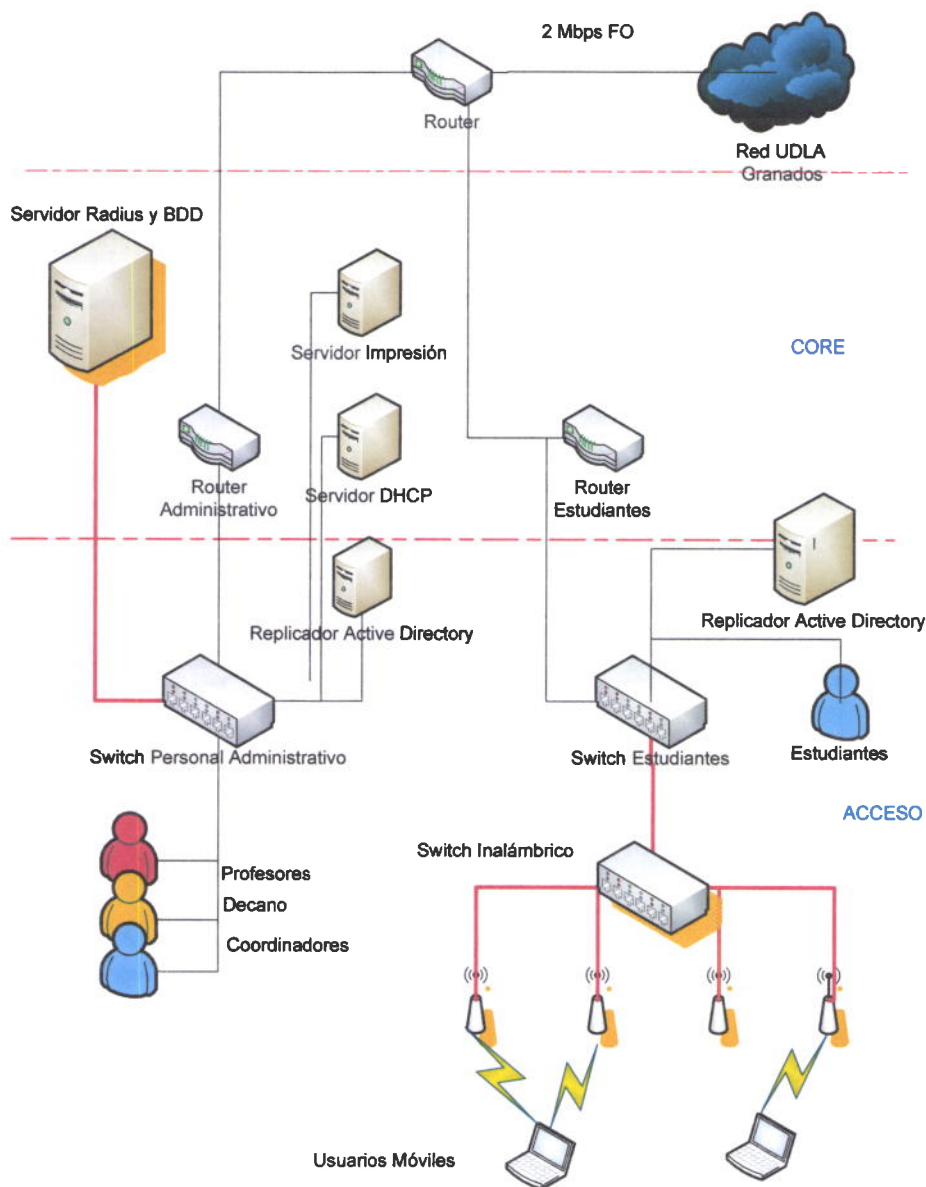


Figura 4-22 Diseño de la Solución

Los equipos con sombra anaranjada son los que serán integrados a la red LAN de la UDLA para dar los servicios de Internet y aplicaciones de la red interna a los usuarios móviles.

Los Puntos de Acceso darán acceso a los usuarios móviles a la red de la UDLA. El switch inalámbrico hará las tareas de roaming, gestión de RF, gestión de configuraciones, alimentación PoE a los Puntos de Acceso, y reenvío de solicitudes de Autenticación y Autorización hacia el servidor RADIUS. El

servidor RADIUS dará autenticación y autorización a los usuarios móviles para que tengan acceso a la red.

4.8.1 Puntos de acceso

En el punto 4.2.6 se seleccionó el equipo DLINK DWL-3500AP. Con estos equipos se procede a realizar el diseño. El número de usuarios por Punto de Acceso que se usará es de 25 usuarios por Punto de Acceso⁷², esto se basa en que los APs son similares a los hubs, es decir que el canal es compartido por todos los clientes conectados al AP..

Para la determinación de la cantidad de los Puntos de Acceso necesarios para la solución y su ubicación se considerará lo siguiente:

- La cobertura de cada Punto de Acceso debe solaparse con el otro. En el punto 4.4 se determinó proveer un Ancho de Banda mínimo de 256 kbps por usuario, si por Punto de Acceso tenemos 25 usuarios, el throughput total mínimo que se debe cumplir es de 6400 kbps (6.25 Mbps). En las pruebas para determinar el throughput en los diferentes puntos con las herramientas Qcheck e Iperf, se verifica que hasta el Punto 3 se obtienen estos valores, por lo tanto se considerará para el diseño la cobertura de cada Punto de Acceso hasta el punto 3. (Color Amarillo)
- Puntos de Acceso adyacente utilizarán canales diferentes.
- El número de usuarios a dar el servicio.

4.8.1.1 Planta baja

Para la ubicación inicial de los Puntos de Acceso se consideró lugares estratégicos donde estos dispositivos logren cubrir toda el área del campus UDLA – Colón. El diseño inicial consideró dos Puntos de Acceso, luego de las

⁷² Recomendaciones de Diseño del Documento Enterprise Mobility 3.0 Design Guide de Cisco System, San José, CA, USA, 2007

pruebas realizadas con el Punto de Acceso se incluyó un tercer Punto de Acceso para cumplir con los requerimientos de cobertura del Campus.

A estas tres áreas de cobertura se les asignaron diferentes canales para evitar la interferencia cocanal. Estos canales fueron 1, 6, 11. El máximo número de canales que permite el estándar 802.11g es 3. El gráfico de cobertura inicial fue la siguiente:

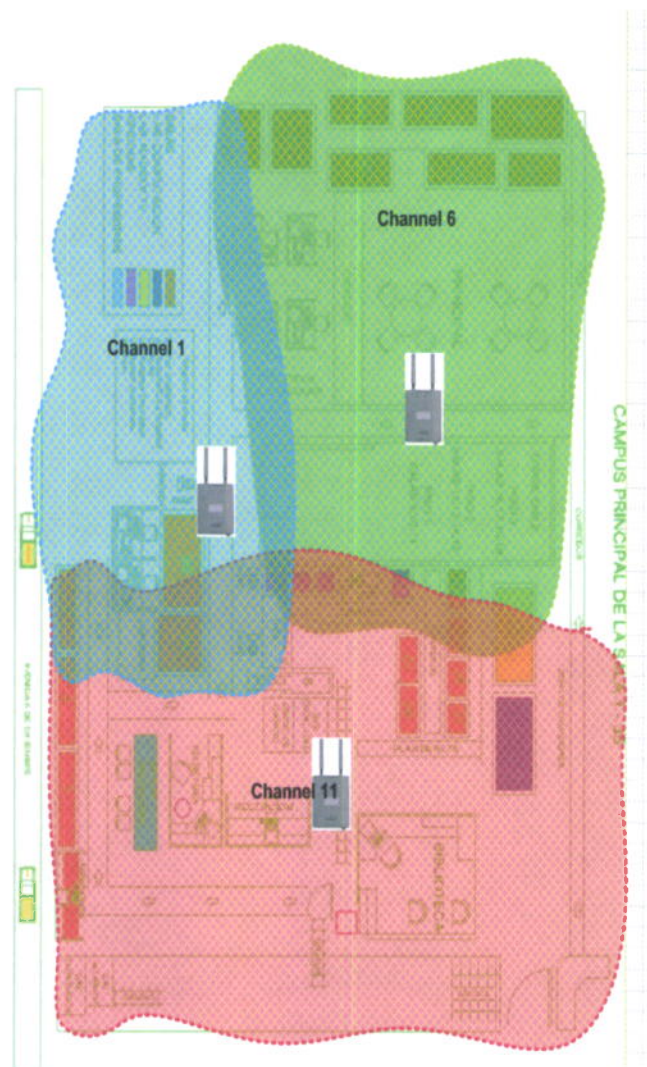


Figura 4-23 Planta Baja

El número de usuarios a dar el servicio es el siguiente:

Tabla 4- 22 Número de Puntos de Acceso necesarios

Área	Número Aulas	Usuarios por Aula ⁷³	Usuarios con servicio	Número de Usuarios por P.A.	Número de P. A.
Channel 1	2	10	20	25	1
Channel 6	8	10	80	25	3
Channel 11	5	10	50	25	2

En este diseño no se considera la Planta Baja de la Torre Chile debido a que este será considerado en el diseño de la Torre.

El diseño final fue el siguiente:

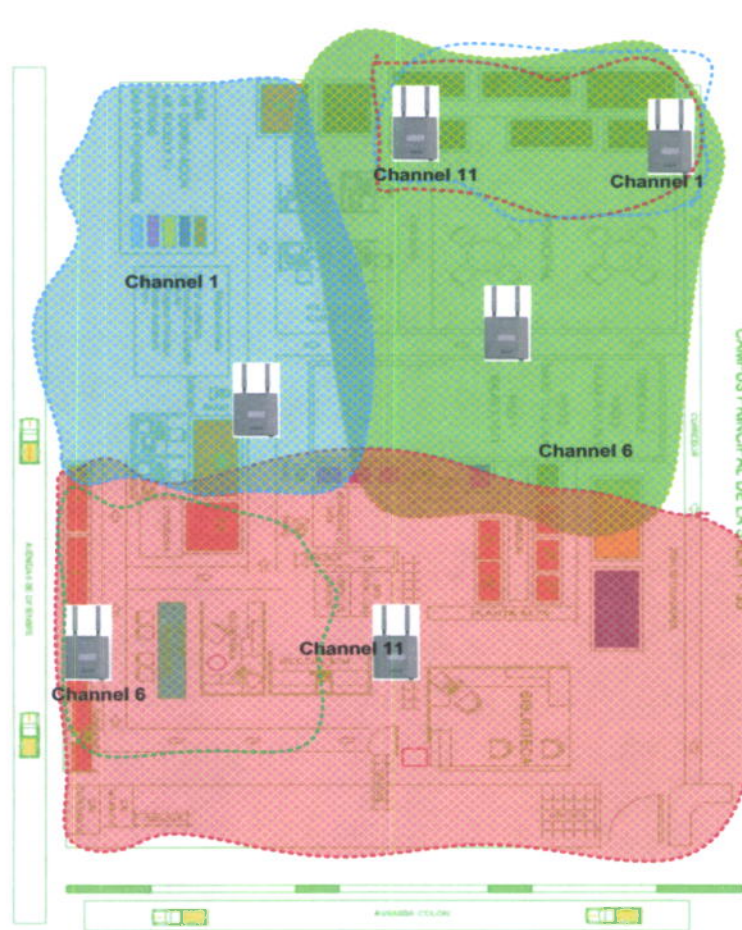


Figura 4-24 Solución Planta Baja

⁷³ En el punto 4.4 se determinó el número de usuarios por Aula, laboratorio, y Biblioteca.

Se considera Puntos de Acceso con antenas direccionales para dar servicio a las aulas del sector a la cual cubren. El Wireless Switch configurará la potencia necesaria en los Puntos de Acceso para lograr la cobertura solicitada.

El número de Puntos de Accesos necesarios en la planta Baja es el siguiente.

Tabla 4- 23 Puntos de Acceso necesarios Planta Baja

Equipos	Antena	Cantidad
Punto Acceso 3500 AP	Omni direccional	3
Punto Acceso 3500 AP	Direccional	3

4.8.1.2 Segundo piso

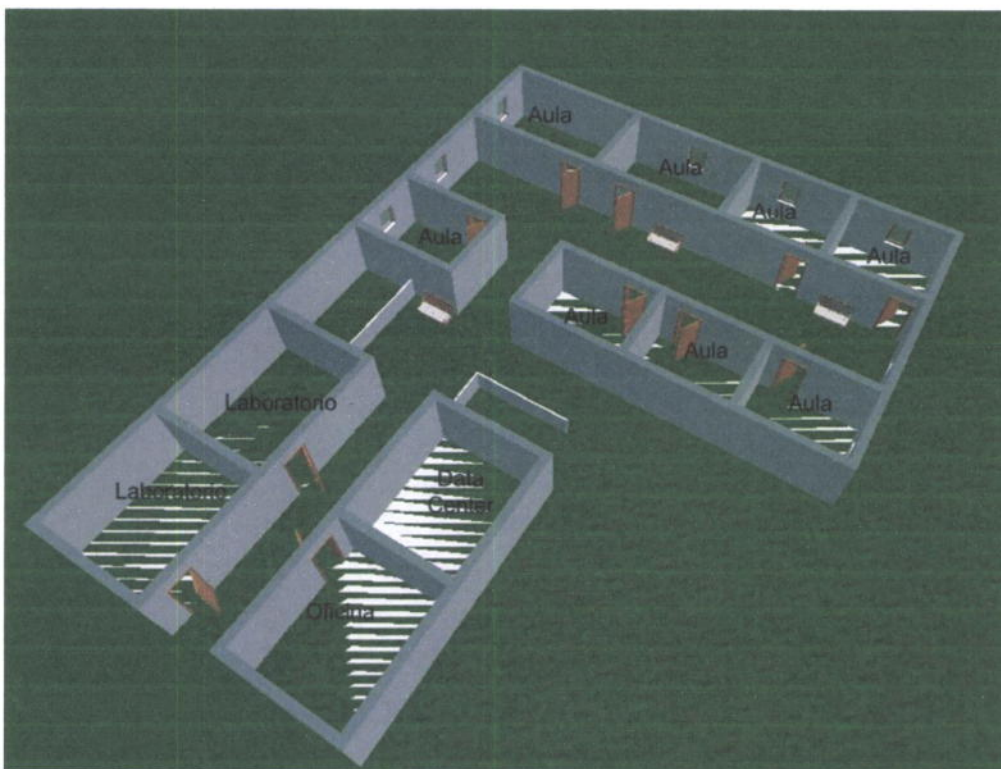


Figura 4-25 Segundo Piso

La determinación del número de Puntos de Acceso se basará en el número de usuarios que se necesita servir.

El número de usuarios a dar el servicio es el siguiente:

Tabla 4- 24 Puntos de Acceso y usuarios

Área	Número Aulas	Usuarios por Aula	Usuarios con servicio	Número de Usuarios por P.A.	Número de P. A.
Segundo Piso	10	10	100	25	4

La ubicación de los Puntos de Acceso, considerando cobertura solapada y la utilización de canales diferentes entre áreas de cobertura adyacentes, es el siguiente:

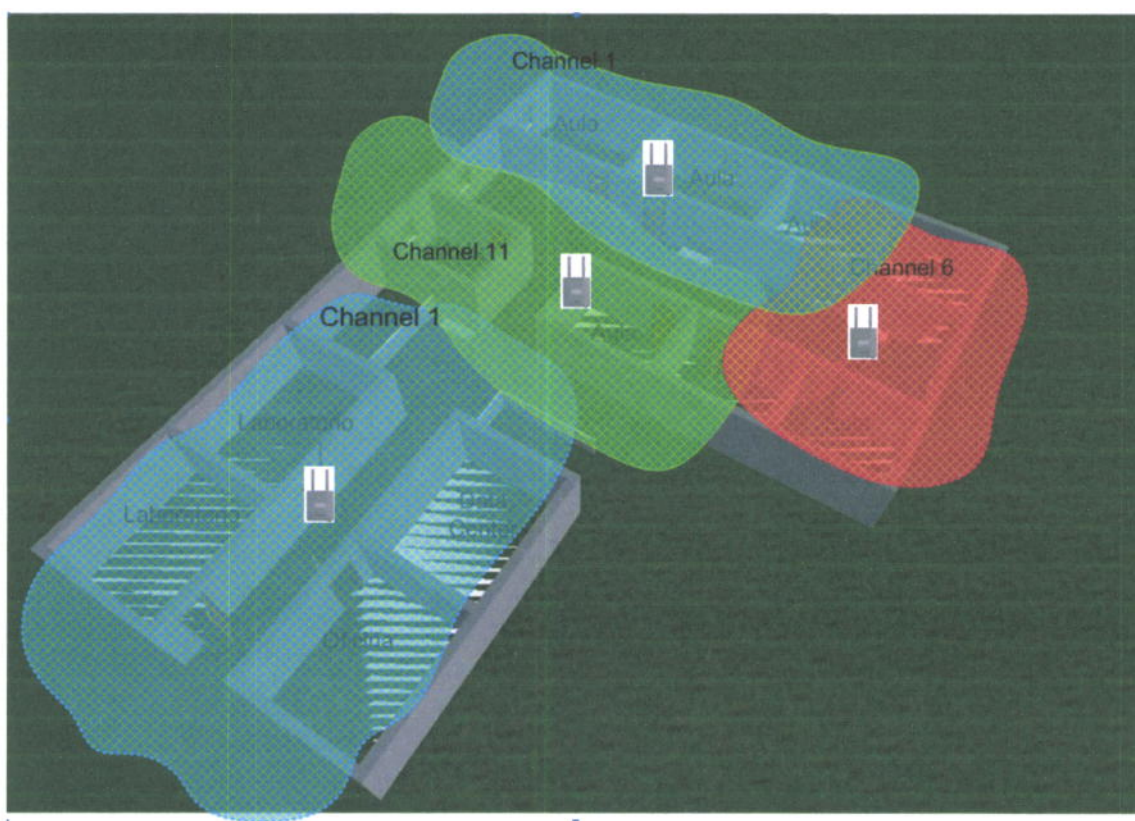


Figura 4-26 Ubicación Puntos de Acceso

El Wireless Switch configurará la Potencia necesaria para cumplir con el diseño propuesto.

El número de Puntos de Acceso en el segundo Piso es el siguiente:

Tabla 4- 25 Puntos de Acceso en Segundo Piso

Equipos	Antena	Cantidad	Ubicación
Punto Acceso 3500 AP	Omni direccional	4	Segundo Piso

4.8.1.3 Torre Chile

La ubicación de los Puntos de Acceso será por piso. El diseño inicial consideró la ubicación de un Punto de Acceso por piso. Las mediciones realizadas en todos los puntos entregan como resultado una calidad buena de la señal con valores de throughput mayor a 16 Mbps. En la figura 4-28 se muestra el diseño inicial:

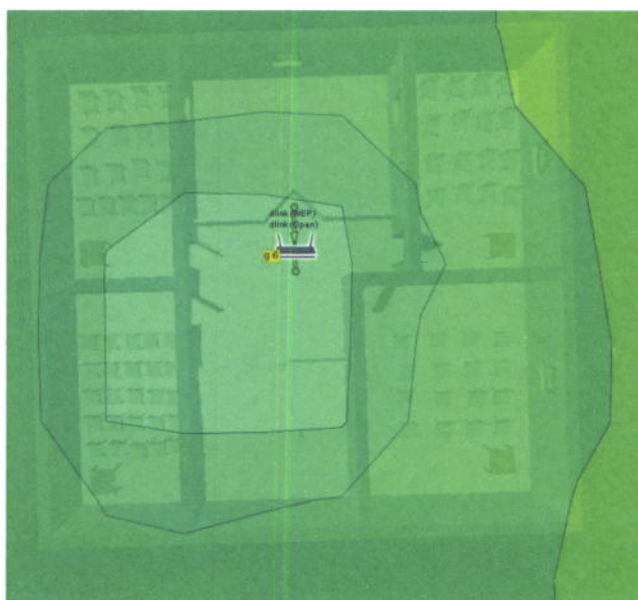


Figura 4-27 Torre Chile

Para cumplir con los valores de número de clientes a dar servicio, se considerará que cada piso de la torre Chile posee 4 aulas. En la tabla 4-24 se calcula el número de Puntos de Acceso por piso.

Tabla 4- 26 Puntos de Acceso por piso en Torre Chile

Área	Número Aulas	Usuarios por Aula	Usuarios con servicio	Número de Usuarios por P.A.	Número de P. A.
Piso 1	4	10	40	25	2
Piso 2	4	10	40	25	2
Piso 3	4	10	40	25	2

En el diseño inicial la calidad de la señal fue Excelente en todos los puntos del Piso, se procede a reubicar para posicionar en cada piso dos Puntos de Acceso para cubrir simétricamente todos los puntos de cada piso.

El diseño final fue el siguiente.

4.8.1.3.1 Piso 1

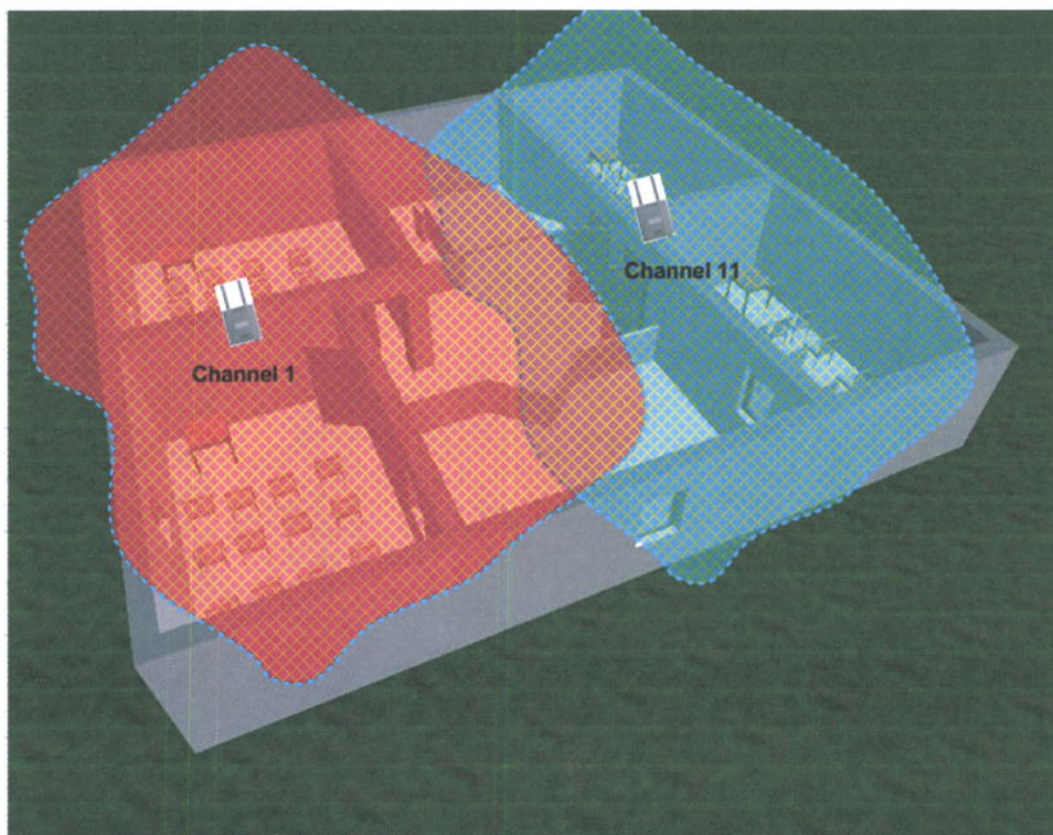


Figura 4-28 Primer piso Torre Chile

Figura 4-28 Ubicación de los Puntos de Acceso en el Piso 1.

Según el punto 4.8.1, en la planta baja de la torre Chile existe cobertura del Punto de Acceso con Canal 6. Los puntos de Acceso a instalarse en el piso 1 utilizarán los canales 1 y 11. El Wireless Switch configurará los Puntos de Acceso automáticamente para bajar el área de cobertura y para minimizar la interferencia cocanal entre los Puntos de Acceso de cada piso

4.8.1.3.2 Piso 2

Los dos puntos de Acceso a instalarse en el piso 2 utilizarán los canales 1 y 6. El Wireless Switch configurará los Puntos de Acceso automáticamente para bajar el área de cobertura y para minimizar la interferencia cocanal entre los Puntos de Acceso de cada piso.

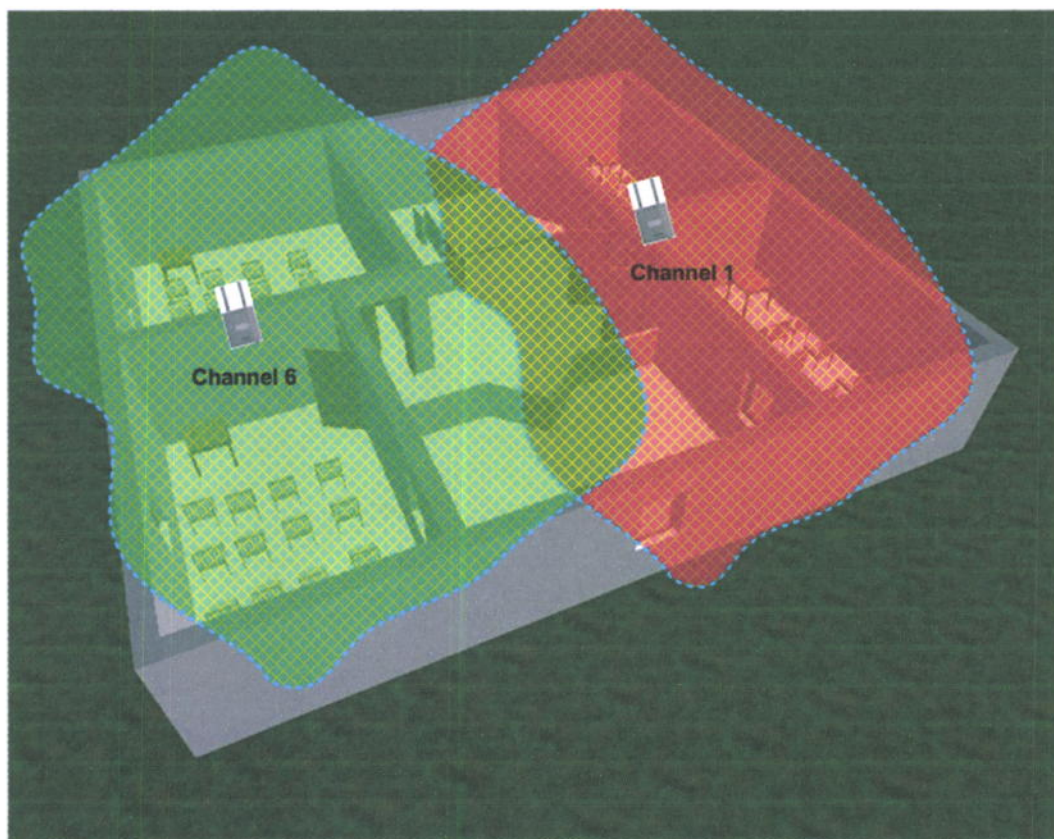


Figura 4-29 Segundo piso Torre Chile

4.8.1.3.3 Piso 3

Los dos puntos de Acceso a instalarse en el piso 3 utilizarán los canales 6 y 11. El Wireless Switch configurará los Puntos de Acceso automáticamente para bajar el área de cobertura y para minimizar la interferencia cocanal entre los Puntos de Acceso de cada piso.



Figura 4-30 Tercer piso Torre Chile

El número de Puntos de Acceso en la Torre Chile es el siguiente:

Tabla 4- 27 Puntos de Acceso en Torre Chile

Equipos	Antena	Cantidad	Ubicación
Punto Acceso DWL 3500 AP	Omni direccional	2	Piso 1
Punto Acceso DWL 3500 AP	Omni direccional	2	Piso 2
Punto Acceso DWL 3500 AP	Omni direccional	2	Piso 3

4.8.2 Equipo Gestión Centralizada

El diseño de la red inalámbrica incluye la utilización de 16 Puntos de Acceso. El número de usuarios a dar servicio es 400. Se necesita un Equipo de Gestión Centralizada, el wireless Switch DLINK DWS-3024L, tiene un máximo de 48 Puntos de Acceso y 512 usuarios inalámbricos.

4.8.3 Servidor radius Y de base de Ddatos

En este diseño se necesitará la inclusión de un servidor que almacenará el Servidor RADIUS y la Base de Datos.

4.9 Análisis de costos

4.9.1 Equipos activos

A continuación se muestra un resumen de los equipos activos necesarios para la implementación del diseño de la red Wireless de la UDLA.

Tabla 4- 28 Costos de los equipos activos de la red.

Fabricante	Número de Parte	Descripción	Cantidad	Precio Unitario	Total
DLINK	DWL-3500AP	Corporate Indoor Access Poit 802.11g, 54/108Mbps PoE Support	16	286	4576
DLINK	DWS-3024L	24-port Gigabit L2+ PoE WLAN Switch with 4 Combo SFP	1	3630	3630
L-com	RE11DP-RSP	2.4 GHz 11 dBi Dual Diversity Antenna - 3ft RP-SMA Plug Connector	3	27.99	83.97
HP	HP ML350 G6	Quad-Core Intel® Xeon® E5420 Processor, 2 GB RAM(2 x 1GB) standard	1	2200	2200
Total					10489.97

4.9.2 Sistema de cableado estructurado

Para la instalación de los puntos de Acceso se necesitará la instalación de 16 Puntos de Red a continuación se muestra una tabla con estos costos. Los dos Puntos de Acceso de la parte de atrás del campus Colón necesitarán amplificadores, debido a que la distancia desde el Data Center excede los 100 metros. Según las revisiones realizadas en el capítulo III sobre el cableado estructurado actual, no existen Puntos de Red en los sitios donde se ubicarán los AP's.

Tabla 4- 29 Costos del Sistema de Cableado Estructurado para los Puntos de Acceso

Descripción	Cantidad	Precio Unitario	Total
Instalación de Puntos de Red Cat 6	16	80	1280
Amplificadores Ethernet	2	30	60
Total			1340

4.9.3 Instalación y configuración de equipos activos

En la siguiente tabla se muestran los costos por la instalación y configuración de los equipos solicitados en el diseño.

Tabla 4- 30 Costos por Instalación y Configuración de los Equipos

Descripción	Número de Equipos	Hora x Equipo	Total Horas	Costo Hora	Total
Instalación y Configuración de Puntos de Acceso	16	1	16	50	800
Instalación y Configuración de Switch Inalámbrico	1	1	1	50	50
Instalación y Configuración de Servidor	1	4	4	50	200
Total					1050

El costo total de la implementación de la red Wireless LAN de la UDLA Campus Colón es USD. 12879.97, como se observa en la tabla 4-31.

Tabla 4- 31 Resumen de Costos

Descripción	Costo
Costo de Equipos Activos	10489.97
Costo de Instalación Cableado Estructurado	1340
Costo de Instalación y Configuración de Equipos Activos	1050
Total	12879.97

5 Conclusiones y Recomendaciones

5.1 Conclusiones

Una vez elaborado el análisis y diseño de red inalámbrica para el CAMPUS COLON de la Universidad de las Américas, se pudo concluir que:

Con respecto a la red inalámbrica actual;

La red inalámbrica actual de la Sede Colón de la Universidad de las Américas resulta bastante ineficiente, ya que cubre solo una muy pequeña área del edificio.

La red inalámbrica actual consta de un solo AP ubicado en la Biblioteca de la universidad, lo que resulta completamente limitado, en términos de servicio, ya que por recomendaciones de los fabricantes, un AP puede servir a un máximo de veinte a veinticinco usuarios de una manera optima, por lo que un solo Acces Point resulta insuficiente.

La red inalámbrica actual posee una seguridad poco confiable, ya que utiliza un password como protección, mismo que podría ser detectado a través de un sniffer y difundirse a personas ajenas a la universidad que puedan hacer mal uso de la red y además el SSID es visible, por lo que cualquier persona mal intencionada podría intentar ingresar a la red de la universidad.

Actualmente no existe un esquema claro de uso de la red inalámbrica, es más un bajo porcentaje tanto de profesores como de estudiantes conoce de la existencia de esta red por lo que no hacen uso de ella.

Al tener en la actualidad un servicio mas bien deficiente en lo que respecta a la red inalámbrica de la sede colon de la Universidad de las América se concluye que es indispensable el tomar acciones pertinentes, como el reemplazo por una nueva plataforma para el servicio de red wireless.

5.2 Recomendaciones

De acuerdo a la investigación que se realizó en la sede Colón, se pueden ofrecer las siguientes recomendaciones:

La Universidad de las Américas, como una universidad líder en educación superior debe mejorar la plataforma informática en su sede Colón, específicamente en lo que se refiere a la red inalámbrica, ya que esta tecnología es hoy en día indispensable en todo ámbito y sobre todo es un servicio que debe gozar de una excelente calidad para el uso de sus alumnos, cuerpo docente y administrativo.

Se recomienda la utilización de la plataforma unificada, por las razones mencionadas a lo largo de los capítulos dos y cuatro, ya que esta solución integrada incluye ventajas desde potenciar las características individuales de los equipos hasta la completa administración de la red inalámbrica.

Es indispensable que las medidas de seguridad y procedimientos de administración de la red inalámbrica del Proyecto planteado sean conocidos por cada uno de los usuarios y administradores de la red inalámbrica, ya que es la única manera de mantener el correcto funcionamiento de la misma.

Es importante que el personal encargado de la administración de la red conozca acerca de la tecnología inalámbrica y todos los detalles de su implementación, así como los sistemas de gestión, los procedimientos de administración y las políticas de seguridad.

Para la gestión y aprovisionamiento de la red inalámbrica, se sugiere trabajar con las herramientas de administración proporcionadas por el fabricante de la tecnología, ya que éstas proporcionan una mejor interacción con los equipos de la red inalámbrica.

Bibliografía

Vladimirov, Andrew., (2005), Hacking Wireless, Seguridad de redes inalámbricas, Anaya, Madrid

Gralla, Preston., (2007), Como funcionan las redes inalámbricas, Anaya Multimedia, Madrid

Miller, Stewart., (2004), Seguridad en WiFi, McGrawHill, España

Red, Neil., (2003), 802.11 (Wi-Fi) Manual de Redes Inalámbricas, McGrawHill, México

Engst, Adam., (2003), Introducción a las redes inalámbricas, Anaya Multimedia, Madrid

<http://www.telepieza.com/wordpress/2008/05/12/los-diferentes-dispositivos-wifi-para-pc-tarjetas-pcmcia-usb-adaptadores/>

<http://www.noticias.com/reportaje/conectividad-valor-estrategico-negocios-89c.html>

<http://www.cfo.com/article.cfm/3009282?f=related>

<http://www.telepieza.com/wordpress/2008/05/12/los-diferentes-dispositivos-wifi-para-pc-tarjetas-pcmcia-usb-adaptadores/>

<http://www.34t.com/Unique/WiFiAntenas.asp?TA=O>

<http://antenasparatodos.blogspot.com/2008/05/antena-isotropica.html>

<http://web.frm.utn.edu.ar/medidase2/varios/dB.pdf>

<http://alumno.ucol.mx/al058284/decibeles.htm>

<http://wireless-network.wireless-computer-networking.com/dBi.htm>

<http://www.monografias.com/trabajos6/ante/ante.shtml>

<http://www.portalpmr.com/articulos/diferencia-ganancia-dbd-dbi-vp14.html>

http://www.electronguia.com.ar/Radio/Temas/Fundamentos_de_antenas1.htm

<http://mx.geocities.com/alfonsoaraujocardenas/topologias.html>

http://es.wikipedia.org/wiki/Espectro_electromagn%C3%A9tico

<http://mecfunnet.faii.etsii.upm.es/difraccion/dif0.html>

<http://www.creatublog.aquiguatemala.com/2006/02/14/onda-portadora-y-modulacion/>

<http://www.ciencia.net/VerArticulo/?idTitulo=Onda%20portadora>

<http://www.redeya.com/electronica/tutoriales/radio/radio.htm>

<http://es.kioskea.net/contents/wifi/wifitech.php3>

<http://www.monografias.com/trabajos14/wi-fi/wi-fi.shtml>

<http://amentis81.googlepages.com/t%C3%A9cnicasdemodulaci%C3%B3nwifi>

Orthogonal Frequency Division Multiplexing (OFDM)

http://www.microsoft.com/latam/technet/seguridad/guidance/lan/peap_int.mspx

<http://emgloindustrial.wordpress.com/category/wlan/>

<http://www.lcu.com.ar/sniffing/>

<http://camyna.com/2005/06/21/rompiendo-contrasenas-wep-con-aircrack-en-una-red-wifi/>

http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf

<http://elladodelmal.blogspot.com/2008/08/atacar-wpawpa2-psk-parte-i-de-iv.html>

<http://www.adslzone.net/tutorial-44.18.html>

http://www.securitytechnet.com/resource/rsc-center/vendor-wp/interlink/EAP_Methods_for_Wireless.pdf

<http://www.networkworld.com/newsletters/wireless/2001/00960610.html>

http://www.arturosoria.com/eprofecias/art/wireless_seguridad.asp

http://www.netgear.co.uk/common/pdfs/Wireless_LAN_White_Paper.pdf

http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps6366/prod_press_coverage0900aecd804b93f4.pdf

http://www.3com.com/products/en_US/detail.jsp?tab=features&sku=3CRWX220095A&pathtype=purchase

<http://www.3com.com/other/pdfs/products/en/3com-400950.pdf>