UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

TESIS

"INTEGRACIÓN DE UNA RED EMPRESARIAL WLAN 802.11 SEGURA DE ÚLTIMA GENERACIÓN"

QUE PARA OBTENER EL TÍTULO DE
INGENIERA EN TELECOMUNICACIONES

PRESENTA:

ANA LUISA GONZÁLEZ GUERRA

DIRECTOR DE TESIS:
ING. RODOLFO ARIAS VILLAVICENCIO

CIUDAD UNIVERSITARIA, NOVIEMBRE 2013.

A mi mamá Alba Antonia Guerra Salazar por todo su amor y apoyo incondicional

A mi papá Miguel Ángel González Villarreal por el cariño que me tuvo

A mi segunda mamá Elsie Salazar por confiar y creer siempre en mí

A mis hermanos Alba y Eduardo por ser mi ejemplo a seguir

A mis tíos Ma. Luisa, Hugo, Aquiles, Carlos, Licha por estar a mí lado en esta carrera que es la vida

A mi abuelita Esther por su gran cariño

Al amor de mi vida Margarito por estar siempre a mi lado y por todo el cariño y amor que me ha brindado

Y en general a toda mi familia: GRACIAS.

AGRADECIMIENTOS

A la Universidad Nacional Autónoma de México y a la Facultad de Ingeniería, por impulsar mí desarrollo académico, profesional y humano.

A la Empresa por darme la oportunidad de realizar mis investigaciones y pruebas de Tesis

Un especial agradecimiento al Ing. Álvaro Francisco Rojas Martínez por su dedicación, paciencia y tiempo que me brindó.

Al Ing. Rodolfo Arias por su asesoría en la realización de la Tesis.

A mis profesores de Ciencias Básicas y del área de Telecomunicaciones por darme las bases y conocimientos para desarrollarme profesionalmente.

A mis amigos Nathaly, Vinicio, Efrén y Alfonso por su amistad incondicional, su apoyo y su confianza que depositaron en mí durante toda la licenciatura.

Y a todas las personas que de alguna manera estuvieron en este camino de mi vida estudiantil. A todos ustedes gracias.

CONTENIDO

LISTA DE FIGURAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

CAPÍTULO 5

LISTA DE TABLAS

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

CAPÍTULO 5

Resumen

La evolución e incorporación de las redes de datos en la sociedad; así como, los dispositivos *(hardware)* que lo constituyen, ha impulsado a que los usuarios tengan la necesidad de obtener información desde sus dispositivos móviles en cualquier lugar y en cualquier momento.

Esta inminente tendencia de movilidad ha dado lugar al estudio de las redes WLAN *(Wireless Local Area Network)*[1] y a la estandarización de los diferentes protocolos de implementación como IEEE 802.11 y sus variantes, permitiendo a los administradores de las redes de datos, implementar y dar a sus usuarios acceso a la red inalámbrica a través de sus dispositivos móviles.

La implementación de la tecnología de red WLAN en el sector empresarial es un panorama que ha surgido en los últimos años debido a la creciente demanda de adquisición de dispositivos móviles por parte de los usuarios-empleados y a la transformación de estos dispositivos como equipos de trabajo. Este nuevo panorama exige tener una red WLAN siempre disponible, con una calidad de servicio adecuada y con la facultad de satisfacer las necesidades de los empleados sin dejar a un lado la seguridad de la misma empresa.

En la presente Tesis se realizó un análisis para la integración de lo que se llamará la red WLAN Empresarial Segura. Para ello se realizó un estudio de los elementos de una red WLAN IEEE 802.11, posteriormente se tiene la evaluación de los diferentes proveedores y las soluciones que se ofrecen en el mercado actual cuyo objetivo fue la elección de una solución para el diseño de prototipo de una red WLAN segura con acceso a usuarios invitados y tendencia de movilidad para las redes WLAN de última generación. Adicionalmente, se deja disponible la red WLAN prototipo para implementar BYOD.

[1] En la página 162 se encuentra el Glosario de siglas y acrónimos

Capítulo 1

INTRODUCCIÓN

Preámbulo

En las últimas décadas los sistemas de comunicación han realizado un papel importante en el desarrollo de la sociedad: compartir información en poco tiempo acortando distancias; aunado a esto, la creciente demanda de dispositivos móviles ha promovido una restructuración en las redes de telecomunicaciones, ya que no sólo es necesario dar acceso a la red a un usuario, sino también es indispensable dar seguridad y calidad en los servicios que se ofrecen.

Las tecnologías de los sistemas de comunicación con las que actualmente se cuentan, permiten a los usuarios tener disponibles, a través de dispositivos móviles, diferentes tipos de servicios como: llamadas y videollamadas en tiempo real, transferencia y almacenamiento de datos, entre otros; permitiendo al usuario mejorar su rendimiento en tiempo y costos.

En el ámbito empresarial, la alta demanda para acceder a la red WLAN corporativa a través de dispositivos móviles y la integración de colaboración entre empleados de distintas empresas para la realización de proyectos conjuntos, exige una correcta reestructuración en la red WLAN corporativa para dar acceso y administrar a usuarios internos e invitados conservando la seguridad de los datos empresariales y la integridad de la misma red.

1.1 Presentación

Las redes alámbricas o cableadas fueron el resultado de la necesidad de disponer de un sistema para la conexión de un grupo de computadoras y dispositivos, compartiendo entre sí servidores, correo electrónico, aplicaciones, impresora, etc.; sin embargo, generalmente esto representa una fuerte inversión debido a la colocación de cableado para la interconexión de equipos y un dinamismo limitado debido al mismo cable, por lo que las redes de área local (LAN) comenzaron a carecer de funcionalidad con el surgimiento de las nuevas tecnologías inalámbricas.

De acuerdo con el informe de la OCDE, *Internet Economic Outlook 2012* a través del estudio de Cisco [1] para el año 2015 el tráfico generado por dispositivos inalámbricos superará considerablemente al realizado por los dispositivos alámbricos. En la actualidad, los equipos que utilizan una red alámbrica representan el 46 % de todo el tráfico IP y los equipos que navegan a través de una red inalámbrica, representan un 54 %.

Al hablar de redes inalámbricas, es necesario mencionar los estándares IEEE (por sus siglas en inglés: *Institute of Electrical and Electronics Engineers)* y en particular los referidos a IEEE 802.11 [2] que han contribuido a consolidar las redes inalámbricas como parte esencial de la infraestructura de las redes empresariales; aunado a ello, actualmente las corporaciones se encuentran ante el nuevo panorama de movilidad que implica una reestructuración en las redes WLAN tradicionales, esto con el fin de garantizar la disponibilidad, QoS, seguridad de los nuevos servicios y aplicaciones a través de dispositivos móviles en un ambiente corporativo.

Una correcta reestructuración de la red WLAN permite desplegar una infraestructura empresarial capaz de soportar aplicaciones de última generación, integrarse con nuevos dispositivos y ofrecer una movilidad persistente a los usuarios. La integración de las nuevas tecnologías para obtener un mayor rendimiento en la empresa, tiene el propósito de brindar a sus empleados y colaboradores una mejor experiencia de movilidad, capacidad, rendimiento y cooperación laboral a través de sus dispositivos móviles.

Esta nueva arquitectura en las redes WLAN trae consigo diversas ventajas de interoperabilidad y movilidad ante las nuevas tendencias tecnológicas; así mismo, es necesario preparar este nuevo escenario tomando en cuenta las vulnerabilidades con las que se podría enfrentar la red corporativa y por consiguiente, considerar algunos puntos

críticos como la seguridad informática y la administración de la red inalámbrica empresarial.

1.2 Planteamiento del problema

Hoy en día las empresas se enfrentan a un nuevo panorama de movilidad; esto es, la integración de dispositivos móviles como puntos de trabajo móviles, dando lugar a la eliminación de lugares de trabajo fijos, e incorporando nuevos elementos como colaboración y reducción de costos.

La integración de una red WLAN en el entorno empresarial presenta diversas ventajas, además de una reducción de costos por el cableado que se realiza en redes LAN, permite la incorporación de los nuevos dispositivos móviles que hoy en día se encuentran en el mercado; sin embargo, esto también representa un nuevo reto para los administradores del área de las Tecnologías de la Información (TI).

El panorama que hoy en día presenta una empresa (véase Figura 1.1) es la siguiente:

- Un gran porcentaje de empleados internos y externos a la red WLAN cuentan con un dispositivo móvil.

- La colaboración de trabajo exige dar permisos de acceso a usuarios invitados.

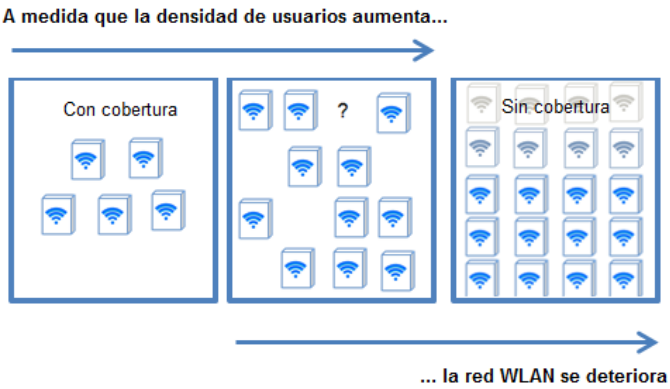


Figura 1.1 Densidad de usuarios móviles en una red WLAN empresarial

- El problema de administración aumenta cuando no se sabe quién o quiénes están haciendo uso de la red WLAN empresarial.

- La calidad de los servicios disminuye con el aumento de usuarios haciendo uso de la red WLAN al mismo tiempo y sin distinción del tipo de servicio.

- La integridad de la información corporativa se encuentra en un punto crítico.

Todos los puntos mencionados anteriormente, muestran la exigencia de realizar una reestructuración e implementación de red, para adecuarse a una nueva generación de redes WLAN empresariales. Es por ello que se busca establecer una infraestructura para que la administración de la red WLAN corporativa tenga la capacidad de ofrecer acceso a usuarios internos e invitados con los recursos necesarios como: disponibilidad, QoS, movilidad, fácil uso y seguridad de los recursos corporativos.

1.3 Objetivo

Con la realización de la presente Tesis se pretende desarrollar un prototipo de diseño de una red WLAN IEEE 802.11 empresarial segura que permita a dos grupos de usuarios, internos e invitados, tener acceso a los recursos corporativos a través de sus dispositivos móviles incorporando QoS y seguridad a la red WLAN empresarial.

El diseño involucra en todo caso una restructuración e implementación de la red inalámbrica corporativa ya existente y en la preparación de la misma para las nuevas tendencias inalámbricas; esto mediante la selección adecuada de soluciones que se encuentran actualmente en el mercado para lograr dicha infraestructura, así como la implementación de seguridad, movilidad, disponibilidad y calidad en el servicio que dará la nueva red WLAN.

Así mismo, el planteamiento de la red WLAN empresarial pretende aumentar la eficiencia de administración de la red por parte de las áreas de TI, con la implementación de

políticas, perfiles y monitoreo que permitirán tener un control considerable de los dispositivos móviles que ingresen a la red WLAN.

1.4 Metodología

Se realizará un amplio análisis de las recomendaciones y mejores prácticas para la integración de redes inalámbricas empresariales que se proponen en las publicaciones para el estándar IEEE 802.11, utilizando como fuentes de dicho análisis organizaciones especializadas en redes inalámbricas como Wi-Fi Alliance [3], IEEE [4], ITU (por sus siglas en inglés: *International Terlecommunication Union*) [5], revistas de seguridad corporativa, libros especializados, entre otros, con el objetivo de analizar las características y soluciones que se proponen para la integración de colaboración laboral a través de dispositivos móviles en una red WLAN segura.

Con base en esta información, se identificarán los puntos clave que permitan realizar la infraestructura de red WLAN corporativa que se desea integrar y que cumpla con las características de seguridad que una empresa necesita hoy en día para salvaguardar su información.

Se implementará la infraestructura diseñada realizando pruebas correspondientes con una marca de TI en un ambiente de pruebas para verificar su funcionamiento y correcta implementación; así mismo, se integrará un sistema de monitoreo para la detección de intrusos en la red, proporcionando un grado más de seguridad para la empresa.

Para su implementación y pruebas, el proyecto de Tesis se llevará a cabo en una empresa piloto (la cual no mencionaré por nombre por cuestiones de seguridad) denominada a partir de ahora como la Empresa Financiera, quien prestará de sus recursos e infraestructura para la realización del proyecto.

1.5 Contribución y relevancia

Se pretende que el proyecto a realizar cumpla con las expectativas de mejorar la red WLAN, cuyo diseño es el que actualmente se encuentra desplegado en la mayoría de las empresas, como en el caso de la Empresa Financiera; y dar solución a la creciente demanda de ingreso a la red WLAN a través de dispositivos móviles poniendo en peligro la seguridad de los recursos internos corporativos.

Además, se buscará tener una mejor administración en la red WLAN, integrar nuevas tecnologías y dejar preparada la red WLAN para la implementación de nuevas tendencias inalámbricas que permitirán al usuario hacer uso de dispositivos móviles para aumentar su eficiencia laboral y tener una nueva experiencia de trabajo colaborativo.

1.6 Estructura de la tesis

La presente Tesis se encuentra dividida en 6 capítulos, los cuales incorporan desde los aspectos básicos de la integración de una red WLAN hasta el prototipo de diseño para la integración de una red WLAN IEEE 802.11 de última generación segura. A continuación se describe el contenido de cada capítulo.

En el capítulo 2, se presentan las características generales que componen a una red WLAN IEEE 802.11 describiendo aspectos generales como su arquitectura, elementos, protocolos, tipos de redes WLAN y los servicios que proporciona.

En el capítulo 3, se determinan las consideraciones que se deben tener en cuenta para la integración de una red WLAN IEEE 802.11 empresarial, dando un enfoque particular a los elementos que conforman la seguridad de la red WLAN corporativa y ofreciendo un conocimiento general de la movilidad en redes inalámbricas.

En el capítulo 4, se describen las tendencias inalámbricas existentes para la creación de una red WLAN empresarial de última generación; así mismo, se hace un análisis de las

soluciones existentes en el mercado para la integración de usuarios invitados a la red WLAN Financiera y el planteamiento de incorporación de tendencia BYOD.

En el capítulo 5, se realiza un prototipo de diseño para la integración de la solución inalámbrica evaluada y la integración de la tendencia Acceso a Usuarios Invitados para la estructuración de una red WLAN corporativa de última generación.

En el capítulo 6, se presentan las conclusiones del prototipo de red WLAN 802.11 empresarial para la integración de Acceso a Usuarios Invitados y se plantean los trabajos futuros para este proyecto.

Capítulo 2

RED WLAN IEEE 802.11

Por muchos años las redes alámbricas han permitido la efectiva interconexión entre dispositivos; sin embargo, actualmente la creciente demanda de dispositivos móviles y la movilidad que representan, exigen una correcta estructuración de las redes WLAN para soportar las nuevas tendencias inalámbricas.

Con la implementación y evolución del estándar IEEE 802.11 en sus diversas variantes, se han logrado establecer redes de comunicaciones inalámbricas capaces de dar acceso a un amplio número de usuarios; de hecho, las estadísticas afirman el aumento exponencial de dispositivos móviles y con ello la demanda de servicios que se solicitan.

Un diseño eficaz de una red WLAN IEEE 802.11 permite sentar las bases para la implementación de soluciones que brindarán la integración de soluciones de administración y control de los recursos para cumplir con las demandas de seguridad y ancho de banda que hoy en día solicitan los usuarios.

Por consiguiente, en este capítulo se describirán los aspectos básicos que conforman una red WLAN 802.11; así como, la introducción a las características generales que conforman la centralización de los puntos de acceso.

2.1 Antecedentes

Los sistemas de redes locales alámbricos o cableados LAN (véase Figura 2.1a), corresponden a la interconexión física tangible para la comunicación entre dispositivos. En sus inicios, este tipo de sistemas eran los más utilizados para la interconexión de dispositivos locales, ya sea de una red doméstica o una red empresarial, cuyo objetivo radicaba en el intercambio de información y el compartir recursos; no obstante, la evolución de las tecnologías de comunicación, la necesidad de movilidad por parte del usuario y el aumento de ancho de banda para la utilización de recursos, promueve a la transformación de las redes LAN.

Las redes inalámbricas (véase Figura 2.1b), dan solución a algunas de las necesidades presentes en las redes LAN, para convertirlas en redes con mayor eficiencia, capacidad y mayor rendimiento. Considerando que las empresas (cualquier tipo de sector de desarrollo) necesitan brindar sus recursos eficientemente y, en demanda a la incorporación y evolución de dispositivos de comunicación móviles, ha sido necesario y resulta práctico adoptar las redes inalámbricas de área local (WLAN).

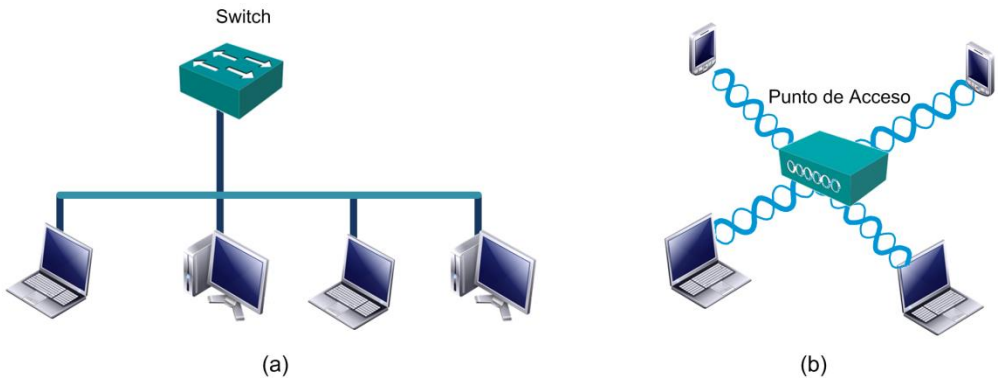


Figura 2.1 Red: (a) LAN; (b) WLAN

2.1.1 Ventajas de las redes inalámbricas

Las redes inalámbricas ofrecen algunas ventajas sobre las redes cableadas, entre las principales se encuentran las siguientes:

- **Movilidad.** La red WLAN permite a los usuarios disponer de los recursos en cualquier lugar y en cualquier momento dentro de la cobertura que proporciona la red.

- **Rango de cobertura.** El área de cobertura que abarca la red WLAN es considerablemente mayor que en redes LAN. Las señales de RF (radiofrecuencia) permiten a los usuarios acceder a los recursos dentro de la cobertura de la red sin la necesidad de utilizar cables para poder llegar a ella.

- **Flexibilidad.** Es posible reubicar los equipos de trabajo sin realizar una modificación radical en el cableado de la red y en caso de ser necesario, agregar eficientemente más puntos de acceso a la red existente.

- **Escalabilidad y compatibilidad.** Las redes inalámbricas pueden ser escalables gracias a la compatibilidad entre los estándares IEEE 802.11. La implementación de nuevas tecnologías inalámbricas se logra de una forma más rápida y eficiente.

- **Robustez.** Las redes WLAN permiten la integración de un número mayor de usuarios, cuestión que las redes LAN no pueden compartir.

- **Inversión en instalación.** Se puede lograr una considerable reducción monetaria al utilizar este tipo de redes, ya que no es necesario invertir en la conexión entre los dispositivos finales y la red. Además, cuando se desea reestructurar la red inalámbrica, la inversión de instalación física es mínima dado que no es necesario realizar obras para tirar o ranurar muros por la instalación de cables.

2.1.2 Cobertura de las redes inalámbricas

De acuerdo con el rango o distancia de alcance (véase Figura 2.2) las redes inalámbricas pueden clasificarse de la siguiente manera [6]:

- Redes inalámbricas de área personal (WPAN), IEEE 802.15.

- Redes inalámbricas de área local (WLAN), IEEE 802.11.
- Redes inalámbricas de área metropolitana (WMAN), IEEE 802.16.
- Redes inalámbricas de área global (WWAN), IEEE 802.1.

Las redes WPAN cubren un área de aproximadamente diez metros, los bajos índices de transmisión de datos tienen como resultado un bajo consumo de energía haciendo que esta tecnología sea adecuada para la transferencia de datos entre dispositivos móviles a través de especificaciones como *bluethoot*, *zigbee,* infrarrojo, etc.

Las redes WLAN trabajan a través del estándar IEEE 802.11. Proveen una cobertura de área local de cientos de metros; por lo general, este tipo de redes son las que se utilizan para ser instaladas en edificios u oficinas.

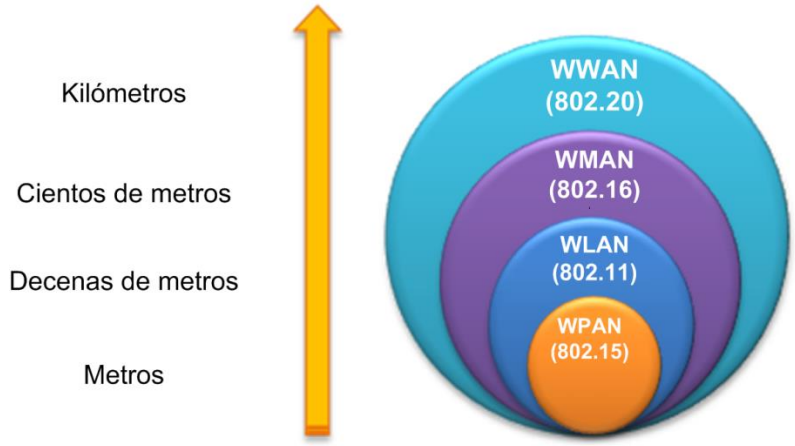


Figura 2.2 Clasificación de redes inalámbricas

A diferencia de las anteriores redes, WMAN interconecta las comunicaciones entre edificios logrando una cobertura mucho mayor que va desde los cientos de metros hasta pocos kilómetros. Finalmente, la red WWAN se presenta en sistemas inalámbricos que tienen un alcance global como son los sistemas de telefonía móvil.

2.2 Estándares IEEE 802.11

La tecnología 802.11, también conocida como Wi-Fi, es un mecanismo de conexión de dispositivos electrónicos que utiliza ondas de RF para permitir la transferencia de datos en distancias de decenas de metros.

Sus orígenes se remontan a cuando las empresas tecnológicas comenzaron a construir redes inalámbricas y dispositivos para aprovechar el espectro radioeléctrico disponible; sin embargo, debido a que se carecía de un estándar inalámbrico en común la compatibilidad entre dispositivos era escasa. En el año de 1997 fue constituida y aprobada a través de la IEEE la norma 802.11 la cual, tuvo como finalidad homologar la tecnología para evitar la incompatibilidad entre dispositivos. Dos años más tarde, se formó a través de un grupo de importantes empresas la organización Alianza *de* Compatibilidad Ethernet Inalámbrica (WECA, por sus siglas en inglés: *Wireless Ethernet Compatibility Alliance*, actualmente *Alliance Wi-Fi)* cuyo propósito es el de promover los estándares inalámbricos IEEE 802.11 que a continuación se describen [7,8].

- **Estándar IEEE 802.11**

Es la versión original del estándar IEEE 802.11, cuya velocidad de transmisión entre 1 y 2 Mbps dependiendo del fabricante, se utilizaba para transmisiones por señales infrarrojas operando en la banda de 2.4 GHz. Su principal debilidad en el modo de operación consistía en que la mayor parte de la velocidad de transmisión se utilizaba para la codificación, cuyo propósito era aumentar la calidad de transmisión; sin embargo, esto produjo problemas de interoperabilidad entre los equipos de diferentes marcas. Actualmente este estándar está en desuso.

- **Estándar IEEE 802.11a**

El estándar 802.11a utiliza como base los mismos protocolos que el estándar original. A diferencia del anterior, su banda de operación es de 5 GHz con una velocidad máxima de 54 Mbps y una velocidad real de transferencia de 24.7 Mbps aproximadamente. Cuenta con 12 canales no solapados: 8 para red inalámbrica y 4 para conexiones punto a punto.

La especificación, utiliza un esquema de modulación conocida como OFDM[2] que es especialmente adecuado para usar en entornos de oficina.

Las desventajas en la utilización de este estándar radican en la incompatibilidad con equipos del estándar 802.11b y en el alcance, dado que en interiores se reduce la distancia de cobertura.

- **Estándar IEEE 802.11b**

Utiliza la técnica de transmisión por modulación DSSS[3] definida en el estándar original. Su velocidad máxima de transmisión es de 11 Mbps, en la práctica, esta velocidad es de aproximadamente 5.5 Mbps y 7.1 Mbps trabajando sobre TCP y UDP respectivamente; operando en la banda de frecuencia de 2.4 GHz, misma que es utilizada por otros aparatos electrónicos que se encuentran operando en esta banda de frecuencia comercial.

- **Estándar IEEE 802.11g**

El tercer estándar IEEE 802.11g utiliza una banda de 2.4 GHz (mismo que el estándar 802.11b) con codificación OFDM y opera a una velocidad máxima teórica de 54 Mbps que en promedio es de 22 Mbps de velocidad real de transferencia (similar al estándar 802.11a). Cuenta con una compatibilidad con el estándar 802.11b y trabaja a las mismas frecuencias que éste. Su desventaja reside en la reducción de la velocidad de transmisión al trabajar varios dispositivos bajo el mismo estándar.

- **Estándar IEEE 802.11n**

IEEE 802.11n se basa en los estándares anteriores de la familia IEEE 802.11. Tiene un aumento en su rendimiento y una complejidad mayor que los estándares anteriores. Trabaja en las bandas de operación de 2.4 y 5 GHz, con un incremento significativo en la velocidad máxima de transmisión de 54 Mbps a un máximo de 248 Mbps.

[2,3] La modulación OFDM y DSSS se definirán más adelante en el presente Capítulo.

Los equipos de estándares anteriores solo utilizan una antena simultáneamente para transmisión y recepción, en el estándar IEEE 802.11n se utilizan múltiples antenas para las funciones de transmisión, recepción o ambas a lo que se le conoce como múltiple entrada-múltiple salida (MIMO)[4].

En la Tabla 2.1 se resumen las características de los anteriores estándares.

Tabla 2.1 Comparación entre los principales estándares IEEE 802.11

Estándar	Banda de operación	Velocidad teórica máxima de transmisión*	Tipo de modulación	Rango aproximado (interiores)*	Rango aproximado (exteriores)*
802.11	2.4 GHz	2 Mbps	DSSS/ FHSS	---	---
802.11a	5 GHz	54 Mbps	OFDM	10 m	---
802.11b	2.4 GHz	11 Mbps	DSSS	50 m	200 m
802.11g	2.4 GHz	54 Mbps	OFDM	27 m	75 m
802.11n	**2.4 y 5 GHz**	**248 Mbps**	**MIMO**	**70 m**	**250 m**

*Valores obtenidos de [7] y [8].

2.2.1 Red WLAN IEEE 802.11n

La implementación del estándar 802.11n a la red WLAN trae consigo diversas ventajas como: mayor velocidad de transferencia, mayor alcance y una mayor cobertura que la que ofrecen los estándares anteriores de la familia IEEE 802.11.

Tradicionalmente, la transmisión de una señal inalámbrica podía verse afectada por las reflexiones que ocurren en su trayecto ocasionando una importante pérdida de datos; el estándar 802.11n basa su tecnología en MIMO [9] a través del cual se logra un incremento en la tasa de transmisión ya que utiliza la propagación multitrayectoria para aumentar su rendimiento.

Para lograr dicho rendimiento, IEEE 802.11n utiliza diversas técnicas de multiplexación para aumentar la velocidad de datos global y la relación señal a ruido (SNR)[5]. Para conocimiento del lector se describe a continuación, en forma general, la técnica

[4] MIMO, corresponde a una técnica de modulación espacio-temporal utilizada para aumentar la velocidad de datos. Esta técnica se definirá en el siguiente tema del presente Capítulo.
[5] SNR, es definida como el margen que hay entre la potencia de la señal que se transmite y la potencia del ruido que interfiere con dicha señal.

multiplexado por división espacial (SDM) la cual es la técnica que se asocia con más frecuencia a MIMO.

- **Multiplexación por División Espacial**

En esta técnica, la señal a transmitir se divide en varias secuencias de datos que se emiten a la misma frecuencia por medio de cada una de las antenas transmisoras. Puesto que las secuencias contienen datos distintos, la velocidad global de transmisión de datos del sistema aumenta. En condiciones óptimas, un sistema MIMO con dos antenas de transmisión y dos de recepción duplica la velocidad de transmisión de datos que se puede alcanzar en un sistema con una sola antena.

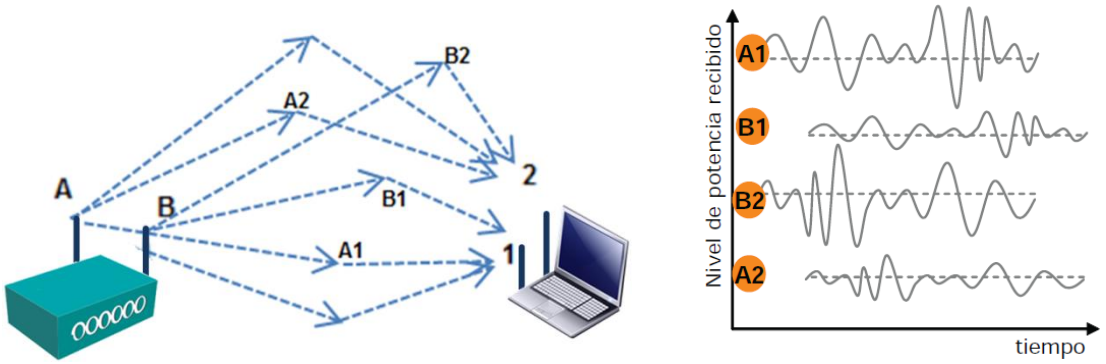


Figura 2.3 Multiplexación por división espacial

En la Figura 2.3 se muestra que cada antena receptora (1 y 2), recibe una señal dominante A1 y B2 respectivamente. Cuando el sistema asume este esquema, SMD puede aprovecharlo mediante la transmisión de distintas señales desde cada antena, sabiendo que cada señal se recibirá con una ligera interferencia una de la otra; en este caso, la señal B1 y A2 provocan una cierta degradación en la señal dominante.

2.3 Arquitectura de una red WLAN 802.11

La arquitectura del estándar IEEE 802.11 consiste en el conjunto de especificaciones para la tecnología de redes WLAN. La Figura 2.4, muestra la integración de este estándar con

el modelo de sistema abierto de interconexión (OSI), el cual abarca la capa física (PHY) y la capa de enlace de datos con sus dos subcapas [10].

<table>
<tr><td colspan="7">802.11 LLC</td><td></td></tr>
<tr><td>802.3
(MAC)</td><td colspan="6">802.11 MAC</td><td>MAC</td></tr>
<tr><td>802.3
(PHY)</td><td>802.11
FHSS</td><td>802.11
DSSS</td><td>802.11a
OFDM</td><td>802.11b
DSSS</td><td>802.11g
OFDM</td><td>802.11n
MIMO</td><td>PHY</td></tr>
</table>

Figura 2.4 Arquitectura IEEE 802.11 con referencia en el modelo OSI

2.3.1 Capa física IEEE 802.11

La capa física ofrece tres tipos de técnicas de transmisión de datos digitales por RF y una para infrarrojo (el presente trabajo solo se enfocará en la transmisión por RF). Para RF, dos de las tres primeras técnicas de transmisión, se basan en el concepto de espectro disperso (SS) el cual, consiste en un ensanchamiento forzado de la señal a transmitir a lo largo de un ancho de banda mucho más amplio que el ancho de banda mínimo requerido de la información que se quiere enviar. Como resultado, la potencia total transmitida no varía pero la señal se hace más inmune a las interferencias y al ruido ambiente (véase Figura 2.5).

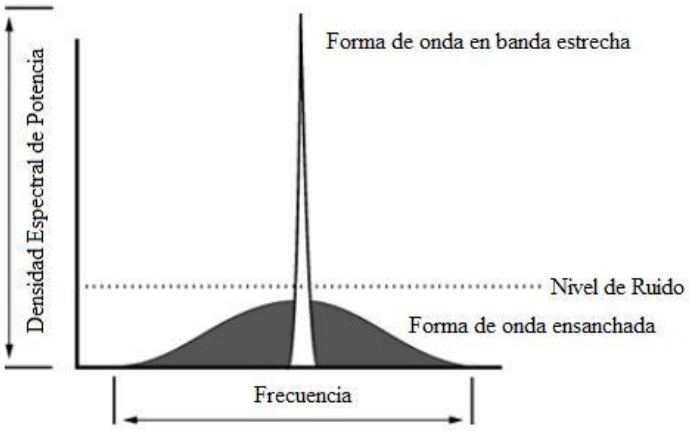


Figura 2.5 Espectro disperso

En los siguientes puntos, se indican las características generales de las técnicas de transmisión para señales de RF.

- **Espectro Disperso por Salto de Frecuencia**

El mecanismo de la técnica de espectro disperso por salto de frecuencia (FHSS) se basa en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo, posterior a este tiempo, la frecuencia cambia por lo que la transmisión se realiza en una frecuencia distinta. Una vez que termina el tiempo del intervalo a transmitir, nuevamente se realiza un salto de frecuencia de acuerdo con la secuencia pseudoaleatoria que tanto el emisor como el receptor conocen (véase Figura 2.6).

El estándar IEEE 802.11 define la modulación por desplazamiento de frecuencia (FSK)[6] para la transmisión FHSS, con una velocidad de 1 Mbps ampliable a 2 Mbps.

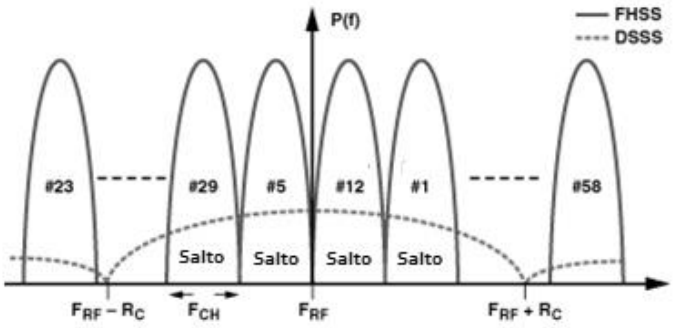


Figura 2.6 Técnicas de transmisión FHSS y DSSS

- **Espectro Disperso por Secuencia Directa**

Espectro disperso por secuencia directa (DSSS), es una técnica que se utiliza para codificar la señal digital que se desea transmitir, utiliza un código pseudorruido el cual aumenta el ancho de banda de transmisión y reduce la densidad espectral dando como resultado un espectro muy parecido al del ruido (véase Figura 2.6).

[6] FSK, es una técnica de transmisión digital de información binaria (ceros y unos) utilizando dos frecuencias diferentes.

Esta señal, al ser recibida en el otro extremo, es decodificada solo por el receptor destino y es descartada por los demás como ruido, esto es posible ya que el receptor destino usa una réplica local del código de pseudorruido usado por el emisor.

Los métodos de modulación empleados para la técnica DSSS es: modulación por desplazamiento diferencial de fase binaria (DBPSK)[7] y modulación por desplazamiento diferencial de fase en cuadratura (DQPSK)[8], que proporcionan una velocidad de transferencia de 1 y 2 Mbps respectivamente.

- **Multiplexación por División en Frecuencias Ortogonales**

Denominado OFDM por sus siglas en inglés, consiste en la multiplexación de múltiples subportadoras ortogonales en frecuencia. Los datos se dividen en varios flujos o canales en paralelo (uno para cada subportadora) las cuales se modulan con sus correspondientes técnicas (véase Figura 2.7).

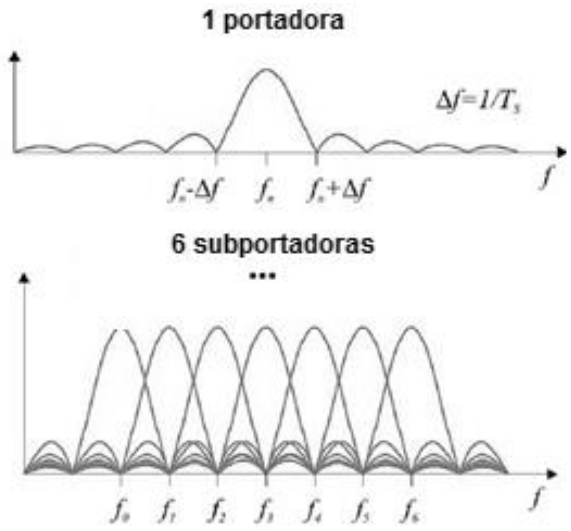


Figura 2.7 Técnica de transmisión OFDM

Su principal ventaja sobre los sistemas anteriores es la resistencia sobre la distorsión por atenuación en frecuencias altas en los cables metálicos, así como las interferencias y desvanecimiento por multipropagación (*fading*).

[6,7] DPSK, es un esquema de modulación digital que utiliza patrones de bits para cambiar la fase de una onda. DBPSK y DQPSK son variantes de este esquema.

Las técnicas de modulación empleadas en OFDM son las siguientes:

- Usando modulación por desplazamiento de fase binaria (BPSK)[9] se obtiene una velocidad de transferencia de 6 Mbps. Con modulación por desplazamiento de fase en cuadratura QPSK[10] dobla la cantidad de datos codificados produciendo una velocidad de transferencia de 12 Mbps.

- Usando 16-QAM[11] y 64-QAM[12] (16 y 64 Nivel de modulación de amplitud en cuadratura*)* se logra una velocidad de transferencia de 24 Mbps y 54 Mbps respectivamente.

2.3.2 Capa de enlace de datos IEEE 802.11

La capa de enlace de datos del modelo OSI provee un tránsito de los datos confiable sobre un enlace físico de red. Diferentes especificaciones de la capa de enlace de datos definen diferentes redes y características de protocolos, tales como [13]:

- **Direccionamiento físico.** Define cómo los dispositivos físicos son direccionados en la capa de enlace de datos.

- **Topología de red.** Las especificaciones de la capa de enlace de datos también definen cómo es que los dispositivos físicos serán físicamente conectados (bus, anillo, malla, estrella, etc.).

- **Notificación de error.** La notificación de error emite una alerta de los protocolos de las capas superiores cuando un error de transmisión ha ocurrido.

- **Secuencia de tramas.** Incluye el reordenamiento de las tramas que fueron transmitidas fuera de secuencia.

[8,9] PSK, modulación angular que consiste en hacer variar la fase de la portadora entre un número de valores discretos. BPSK y QPSK son variantes de este tipo de modulación.

[10,11] QAM, modulación de la señal portadora en amplitud y fase. 16-QAM y 64-QAM son variantes.

- **Control de flujo.** El control de flujo incluye una moderación de la transmisión de datos de tal manera que el dispositivo receptor no se sobresature con más tráfico que el que puede manejar a un tiempo.

La IEEE ha subdividido la capa de enlace de datos en dos subcapas:

- Control de enlace lógico (LLC)
- Control de acceso al medio (MAC)

2.3.2.1 Control de Enlace Lógico

La subcapa LLC de la capa de enlace de datos, administra las comunicaciones entre dispositivos sobre un solo enlace en una red. El control de enlace lógico, coloca información en la trama la cual permite identificar qué protocolo de capa de red está usando la trama. Esta información permite que varios protocolos de la Capa 3 del modelo OSI, utilicen la misma interfaz de red y los mismos medios.

Las funciones que realiza LLC [11] son las siguientes:

- **Servicios proporcionados a la capa de red**

LLC proporciona el servicio de transferencia de datos; es decir, se realiza la entrega de datos de la capa de red a la capa de enlace de datos en el dispositivo de origen, y en el dispositivo destino se realiza la entrega de datos de la capa de enlace de datos a la capa de red.

- **Entramado de la información**

LLC encapsula en un formato específico la información que proviene de la capa de red; además, delimita el principio y fin de cada trama.

- **Control de errores**

El flujo de información es dividido en tramas, con la introducción de códigos de comprobación de redundancia cíclica (CRC)[13] se realiza una comprobación de la trama para determinar si los datos transmitidos son correctos o erróneos.

- **Recuperación de información**

A nivel de LLC, se asegura que todas las tramas sean entregadas en el orden correcto a la capa de red destino, en el caso de que una trama no haya sido entregada o se haya detectado como errónea, es posible que el dispositivo emisor pueda transmitirla nuevamente Válido sólo para protocolos orientados a conexión como el protocolo de control de transmisión (TCP). En el protocolo de datagramas de usuario (UDP), no se realiza el control de errores ni la recuperación de información.

- **Control de flujo**

Para evitar una saturación en el dispositivo receptor debido a la sobrecarga de flujo, se utilizan técnicas de realimentación de tal forma que el emisor no envía nuevas tramas al receptor hasta que éste le informe que puede hacerlo.

2.3.2.2 Control de acceso al medio

La subcapa MAC de la capa de enlace de datos, administra el protocolo de acceso al medio físico de red. Las especificaciones IEEE definen las direcciones MAC que permiten que varios dispositivos se identifiquen sin repetición entre unos y otros en la capa de enlace de datos.

La arquitectura MAC del estándar IEEE 802.11 se compone de la función de coordinación distribuida [11, 14].

[13] CRC, código de detección de errores el cual permite detectar cambios en los datos.

- **Función de Coordinación Distribuida**

La función de coordinación distribuida (DCF) determina cuándo una estación puede transmitir a través del medio inalámbrico. Su funcionamiento se basa en técnicas de acceso al medio. El algoritmo de acceso al medio WLAN es conocido como acceso múltiple por detección de portadora con evasión de colisiones (CSMA/CA)[14].

De acuerdo con la Figura 2.8 el proceso es el siguiente:

1. Antes de transmitirse la información a través del medio inalámbrico, la estación determina si el medio está disponible u ocupado.

2. Si el medio no está ocupado durante un tiempo IFS[15], el dispositivo puede comenzar a transmitir.

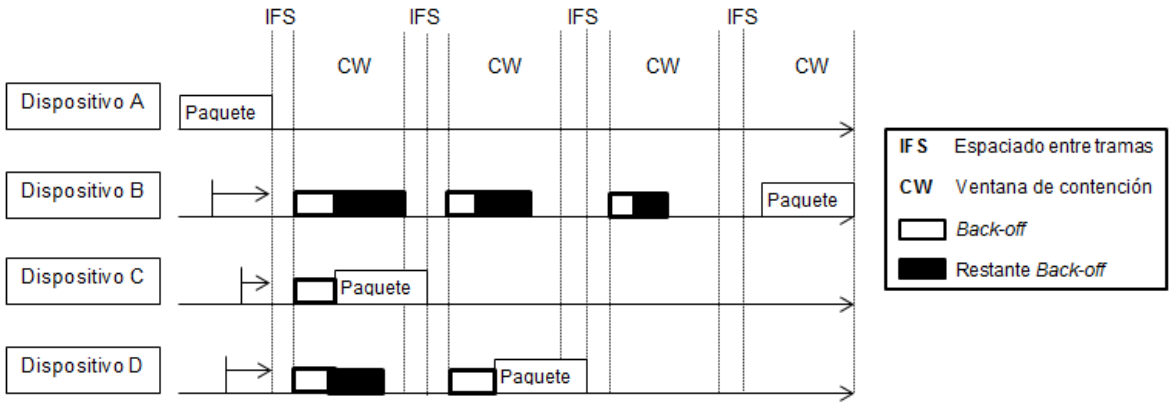


Figura 2.8 Acceso al medio en la capa MAC (CSMA/CA)

3. Por el contrario, si durante el intervalo IFS el medio se determina ocupado, entonces la estación debe esperar un intervalo de tiempo más como se indica en el siguiente punto.

4. Una vez que se determina que el medio aún se encuentra ocupado, la estación ejecuta el algoritmo *Backoff,* el cual, determina un tiempo aleatorio adicional de

[14] Protocolo de acceso al medio empleado en redes inalámbricas.
[15] Es definido por el estándar IEEE 802.11 como un conjunto de intervalos de tiempo de espera preestablecidos para evitar colisiones y poder implementar un sistema de prioridades.

espera de acuerdo con la ventana de contención (CW) y cuyo objetivo es reducir la probabilidad de colisiones.

5. Durante el tiempo *Backoff* la estación continúa escuchando el medio, si al finalizar este intervalo de tiempo el medio se encuentra libre la estación podrá comenzar a transmitir, en caso contrario, el algoritmo continuará ejecutándose con un CW con valor doble que CW-1 cuyo rango será desde CWmín hasta CWmáx.

En un entorno inalámbrico CSMA/CA puede presentar dos principales problemas:

- **Problema de los nodos ocultos**

La estación cree que el canal está libre pero en realidad está ocupado por otra estación que no oye.

En la Figura 2.9 se presenta lo siguiente: la ET1 y la ET3 desean comunicarse con la ET2, ambas estaciones envían una trama, puesto que la ET1 y la ET3 no se encuentran en el rango de alcance las dos transmiten al mismo tiempo originando una colisión en la ET2.

- **Problema de los nodos expuestos**

La estación cree que el canal está ocupado; sin embargo, está libre ya que en realidad la estación que está escuchando no interfiere con la transmisión de la estación que quiere transmitir.

Ejemplificando lo anterior (véase Figura 2.9), la ET3 envía una trama a la ET2, mientras que la ET4 no transmite trama alguna a la ET5 ya que cree escuchar el canal ocupado.

Para resolver los anteriores problemas, se implementa el protocolo RTS/CTS (Solicitud de envío/Libre para envío). En el cual el transmisor y receptor intercambian tramas de control antes de que el transmisor envíe algún dato. El proceso de RTS/CTS es el siguiente:

1. Cuando una estación desea transmitir, primero envía al receptor una solicitud RTS en donde se indica la longitud de la trama de datos y el tiempo que la estación transmisora desea controlar el medio. La estación receptora escucha la solicitud y

almacena localmente el valor de tiempo en un vector de asignación a la red (NAV) el cual va a ser utilizado como un temporizador decreciente.

2. El receptor responde a la estación emisora con una trama CTS la cual indica, al igual que la trama RTS, el tiempo que se utilizará el canal para la trasmisión de los datos.

3. Una vez que la estación transmisora recibe la trama CTS, comienza a enviar la trama de datos. Si la trama es recibida correctamente la estación receptora enviará un acuse de recibido (ACK), si el ACK no es enviado durante un intervalo de tiempo preestablecido se enviará nuevamente la trama de datos.

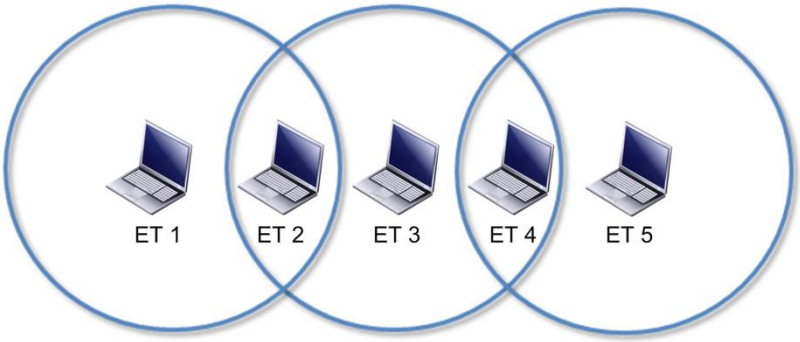


Figura 2.9 Problema de los nodos ocultos y expuestos

2.4 Elementos de una red WLAN 802.11

Una red WLAN puede ser de diversos tipos y tan simple o compleja como sea necesario; está conformada por los siguientes componentes principales (véase Figura 2.10): el medio físico, las estaciones de trabajo inalámbricas, punto o puntos de acceso, *router* y *switch*.

- **Medio Físico**

Una red WLAN, al igual que una red LAN, requiere un medio físico a través del cual pasan las señales de transmisión. En lugar de utilizar un cable par trenzado o cable de fibra

óptica, las redes WLAN utilizan luz infrarroja o RF cuyo medio de transmisión es el aire.

- **Estaciones de Trabajo Inalámbricas**

Las estaciones de trabajo inalámbricas (nombradas como ET) son dispositivos de usuario (*laptops, smartphones, tablets,* etc) que se encuentran conectados a una red WLAN a través de una tarjeta de red, generalmente ya integrada en el dispositivo.

- **Punto de Acceso Inalámbrico**

Un punto de acceso inalámbrico (AP) es un dispositivo que se comunica mediante señales radioeléctricas con estaciones inalámbricas. El AP es el encargado de coordinar la comunicación entre las estaciones inalámbricas que están conectados a él. En su modo de funcionamiento básico actúa a nivel de enlace (Capa 2 del modelo OSI) como un puente (*bridge)* basándose en las direcciones MAC del tráfico para su encaminamiento.

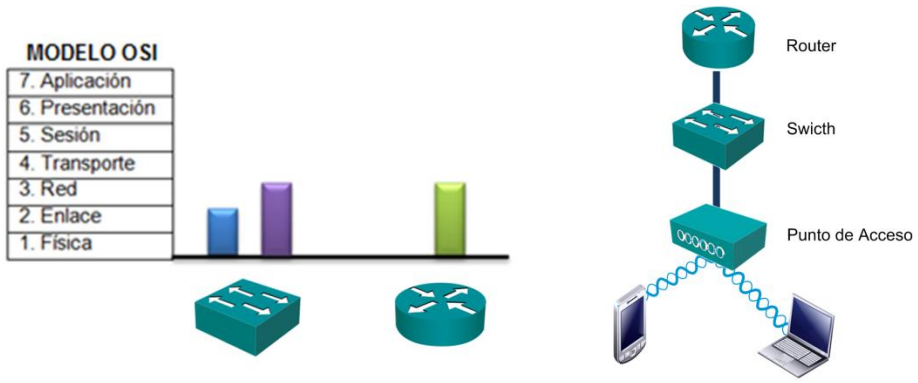


Figura 2.10 Elementos básicos de una red WLAN 802.11

- ***Router***

Los *router*, son dispositivos que trabajan a nivel de Capa 3 del modelo OSI. A diferencia de los *switch* que no les es posible salir más allá de la red, los *router* envían paquetes de datos de una red a otra.

Cuando un dispositivo intenta realizar una conexión con otro dispositivo cuya dirección de red no es la misma a la que pertenece, el *router* interviene como un tercero quien se encarga de interconectar a estos dos dispositivos. El *router*, mantiene una comunicación continua con otros *routers*, por medio de algoritmos y protocolos intercambia información y aprende como llegar a las diferentes redes que conforman una gran red por lo que conoce la topología lógica de la red. Con base en las tablas de ruteo, las cuales son mapas de la localización de las diversas redes, el *router* puede decidir por qué interfaz enviar la información.

- ***Switch***

Los *switch* son dispositivos que trabajan a nivel de Capa 2 del modelo OSI. En su funcionamiento, los *switch* asocian cada dispositivo conectado a su puerto a través de direcciones de Capa 2 (direcciones MAC), una vez que ha aprendido las direcciones correspondientes a cada uno de sus puertos, la información es enviada solamente a la dirección destino correspondiente.

Dentro de estos dispositivos, también es posible encontrar *switch* de Capa 3. Un *switch* de Capa 3 cuenta con niveles de control y seguridad con los que un *router* normalmente cuenta; aunado a ello, incorpora la capacidad de definición de VLAN[16], a través de las cueles se añaden mecanismos de seguridad para prevenir que un usuario indeseado se conecte a la red.

2.5 Tipos de redes WLAN 802.11

Comúnmente se utilizan dos tipos de redes WLAN 802.11: redes del tipo *Ad-Hoc* y de Infraestructura. En general, las redes WLAN 802.11 empresariales tienen como base una red WLAN de infraestructura.

[16] En el Capítulo 3, se hará referencia a este concepto.

2.5.1 Red WLAN *Ad-Hoc*

Las redes *Ad-Hoc* también conocidas como redes de conexión punto a punto (P2P) [12] son redes donde las ET se conectan entre ellos sin la necesidad de un AP o un servidor utilizando una tarjeta WLAN (véase Figura 2.11). El rango de las redes *Ad-Hoc* está determinado por el rango de cobertura de cada ET inalámbrica; cada dispositivo estará conectado a otro siempre y cuando se encuentre dentro del área de cobertura de la ET a la cual se desea comunicar. De acuerdo con su función las redes *Ad-Hoc*, pueden clasificarse de la siguiente manera:

- Redes móviles *Ad-Hoc*
- Redes inalámbricas *mesh*
- Redes de sensores

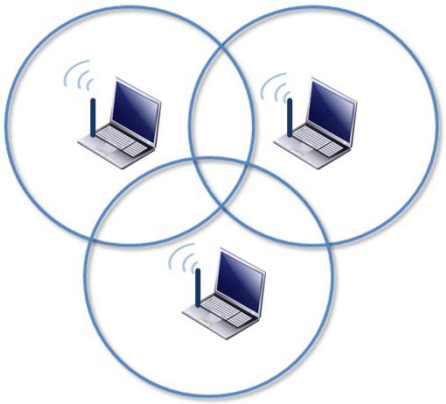


Figura 2.11 Red Ad-Hoc

Por lo general, este tipo de redes inalámbricas son de uso doméstico. La presente Tesis no tiene como objetivo este tipo de redes, sólo se menciona para conocimiento del lector.

2.5.2 Red WLAN de infraestructura

A diferencia de la red anterior, las redes WLAN de infraestructura se distinguen por el uso de uno o más AP. Cada ET inalámbrica se conecta a un AP a través de un enlace inalámbrico como se muestra en la Figura 2.12.

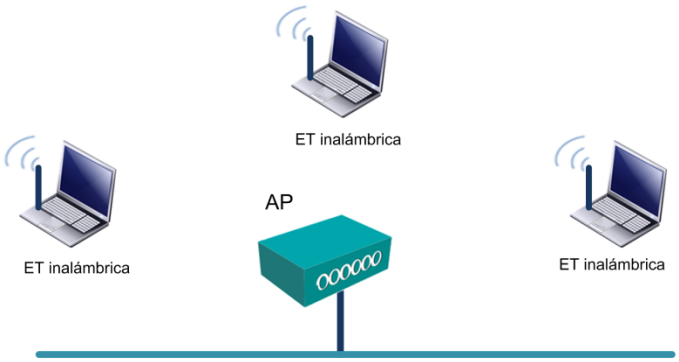


Figura 2.12 Red WLAN de infraestructura

A continuación se describen los componentes que conforman la arquitectura de una red WLAN de infraestructura desarrollado por IEEE 802.11 [2]:

- **Conjunto de Servicios Básicos**

Un conjunto de servicios básicos (BSS), es definido por un grupo de ET cuyos usuarios se encuentran asociados a un AP el cual, coordina la comunicación y todo el tráfico desde y hacia las ET inalámbricas.

La característica fundamental del BSS consiste en el establecimiento de un servicio de ID (*IDentifier*), comúnmente conocido como identificador de conjunto de servicios (SSID). El SSID es una cadena alfanumérica con un máximo de 32 caracteres, que identifica a una ET como parte de la red; es decir, cualquier ET inalámbrica que se encuentre conectada a la misma red WLAN tendrá el mismo SSID.

- **Conjunto De Servicio Extendido**

Una de las limitaciones de BSS es el alto número de usuarios de las ET inalámbricas utilizando el mismo AP lo que indica un claro congestionamiento en la red. Es por ello que se establece el conjunto de servicios extendidos (ESS). Este servicio está conformado por un grupo de AP los cuales están configurados con el mismo SSID para crear un sistema de distribución WLAN (véase Figura 2.13), esto permite una serie de recursos opcionales como el *roaming* entre células.

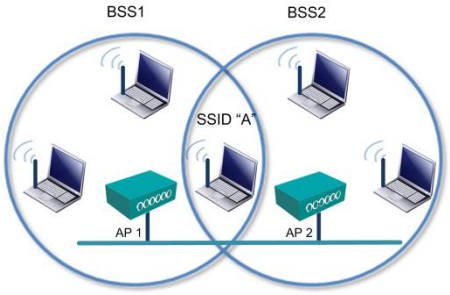


Figura 2.13 Conjunto de servicios extendidos

En la Figura 2.14 se muestran dos ESS con sus respectivos AP; obsérvese que cada una de las ESS difunde a través de sus AP un SSID diferente. Mientras las ET inalámbricas se encuentren dentro de la cobertura de difusión, éstas podrán conectarse a través de los AP a cada una de las redes difundidas. Ejemplificando lo anterior, una ET asociada a un AP con un SSID "A" sólo podrá tener comunicación con las que se encuentren asociadas al mismo SSID o ESS "A"; por otro lado, lo mismo sucede con las ET inalámbricas asociadas con la ESS "B".

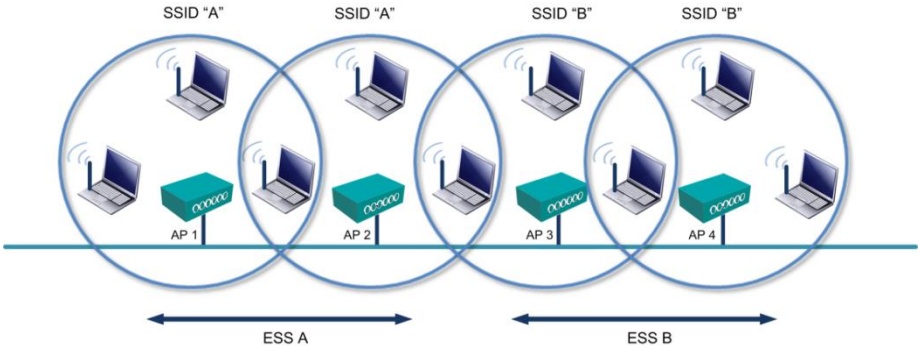


Figura 2.14 Múltiples ESS

2.6 Servicios IEEE 802.11

El estándar IEEE 802.11 define nueve tipos de servicios que debe proporcionar una red WLAN dentro de dos categorías: estaciones de servicio (SS) y el sistema de servicios de distribución (DSS) [2, 13, 14].

2.6.1 Estaciones de servicio

El estándar IEEE 802.11 define los servicios para proporcionar funciones entre las estaciones de trabajo. La idea principal de las estaciones de servicio (SS) es prestar funciones de seguridad a los datos de la WLAN. En los siguientes puntos, se mencionan las características generales de las SS.

- **Autenticación**

En redes WLAN es necesario comprobar la identificación de un usuario antes de asociarlo con la red inalámbrica. La autenticación, busca confirmar la identidad del usuario destino, comprobando que éste sea quien dice ser ante los registros o perfiles almacenados en la estación donde la información se origina. Dicha verificación del usuario se maneja convencionalmente por medio de otro servicio, denominado control de acceso (AC), el cual se encarga de recibir ciertos parámetros sobre la identidad del cliente; por ejemplo, un nombre de usuario y una clave o contraseña, y a partir de éstos iniciar el proceso de autenticación.

- **Desautenticación**

Es el proceso de terminación de una autenticación. En redes seguras, es importante la desautenticación puesto que, es la responsable de borrar todas las claves almacenadas que se relacionaban con esa conexión de red inalámbrica. Mientras que la autenticación es necesaria antes de autorizar el uso de la red, la desautenticación genera la terminación de la asociación en curso.

- **Privacidad**

Asegura que los datos transmitidos a través de un canal inalámbrico no sean leídos por otro diferente al dispositivo receptor.

- **Entrega de Unidad de Servicios de Datos MAC**

La entrega de unidad de servicios de datos MAC (MSDU) asegura que la información en la unidad de datos de la trama MAC sea distribuida entre los AP del servicio MAC.

2.6.2 Sistema de servicios de distribución

Los cinco servicios de distribución DSS, que se emplean para mover datos alrededor de la estructura de la red son: asociación, disociación, reasociación, distribución e integración. A continuación se describen de forma general cada uno de los DSS.

- **Asociación**

En la asociación, las ET inalámbricas se registran con los AP anunciando su identidad y capacidad (velocidad, potencia, etc), el sistema de distribución puede utilizar la información de estos registros para determinar qué AP puede utilizar para alcanzar la estación móvil, en el caso de que las estaciones no se encuentren registradas éstas no pertenecerán a la red.

- **Disociación**

Este servicio es utilizado para terminar una asociación existente. Cuando una ET realiza la petición de este servicio, todos los datos de movilidad de la ET son eliminados por lo que la ET queda desconectada de la red.

- **Reasociación**

Cuando una estación se mueve de un área BSS a otra área BSS, el servicio de reasociación permite a la ET transferir la asociación entre dos AP.

- **Distribución**

Este servicio es utilizado por una red de infraestructura BSS cada vez que se realiza una transmisión. Cuando un dispositivo transmite y la trama ha sido aceptada por el AP, éste utiliza el mismo sistema de distribución para enviar los datos a su destino.

- **Integración**

Este servicio permite la conexión del mismo sistema de distribución con una red distinta a IEEE 802.11.

2.6.3 Servicios de infraestructura

Los servicios de infraestructura son de vital importancia en las redes WLAN, éstos son la base para la conectividad de la red inalámbrica y sus aplicaciones. Entre estos servicios se encuentran el sistema de nombres de dominio (DNS) y la configuración dinámica de *host* (DHCP).

- **Sistema de Nombres de Dominio**

El sistema DNS es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. La principal función de este sistema consiste en traducir las direcciones IP[17] a nombres de dominio.

- **Configuración Dinámica de *Host***

La función de este servicio se encuentra definida en el RFC[18] 2131 [15]. Permite a los usuarios de una red WLAN adquirir automáticamente los parámetros de configuración de la red como son: dirección IP, dirección de *Gateway,* máscara de red, etc.

Cuando una red es muy extensa, la integración de DHCP permite un ahorro de tiempo y gestión. En este servicio, un servidor denominado servidor DHCP contiene un rango de direcciones IP las cuales se van asignando automáticamente a los usuarios, de igual forma si una dirección IP es liberada lo concentra en su base de datos para poder ser asignada a otro usuario que desee ingresar a la red.

Además, DHCP permite la configuración de direcciones IP de reserva, esta estructura permite proporcionar la misma dirección IP a un usuario asegurando que a ningún otro dispositivo se le asignará dicha dirección IP.

[17] Direcciones que constan de cuatro octetos de números binarios.

[18] Ver glosario de siglas y acrónimos

2.7 Controladores WLAN

Anteriormente, las redes WLAN eran implementadas por un cierto número de AP autónomos repartidos en puntos donde sólo se necesitaba realizar una cobertura inalámbrica. Con este tipo de sistemas autónomos o distribuidos (véase Figura 2.15), es posible cubrir ciertas tareas que demanda el usuario, siempre y cuando, el número de dispositivos sea el mínimo; aunado a ello, se tiene la desventaja sobre estos sistemas al requerir de una configuración y administración individual de los AP.

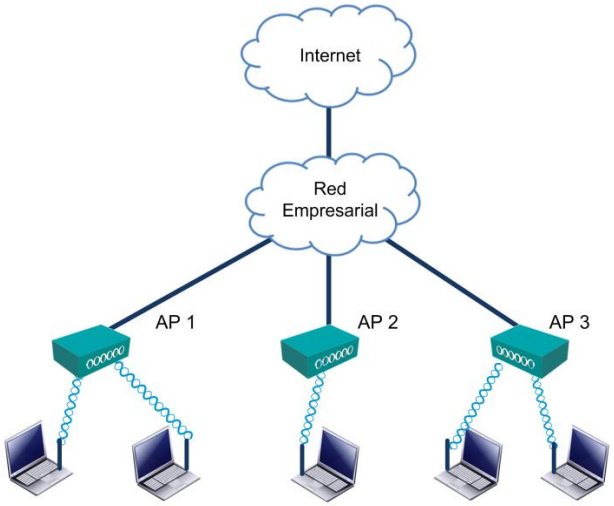


Figura 2.15 Sistema WLAN autónomo

Cuando se maneja un esquema complejo como es el de las redes WLAN empresariales, en donde su demanda de servicios y el número de usuarios es notablemente mayor, es ineludible tener en consideración que los AP no pueden actuar de forma independiente; por lo que es necesario un controlador inalámbrico LAN (WLC) para la gestión centralizada de varios AP en una red inalámbrica (véase Figura 2.16) [16, 17].

La idea de implementar un WLC es simplificar las tareas de operación en la red WLAN; así como, ofrecer una arquitectura centralizada, y mantener una gestión y configuración controlada de los AP en cuyo entorno son conocidos como antenas inteligentes, ya que su función principal reside en recibir y transmitir el tráfico inalámbrico. A partir de este

momento, en la presente Tesis, los AP que actúen en un sistema centralizado serán identificados como puntos de acceso ligero (LAP)[19].

WLC ofrece diversas funciones (dependientes del modelo del WLC), entre ellas se encuentran: proporcionar servicios a usuarios invitados, centralizar el trabajo de filtrado, mantener QoS, autenticación y cifrado, e implementación de un servicio de monitoreo para la administración y prevención de posibles ataques informáticos.

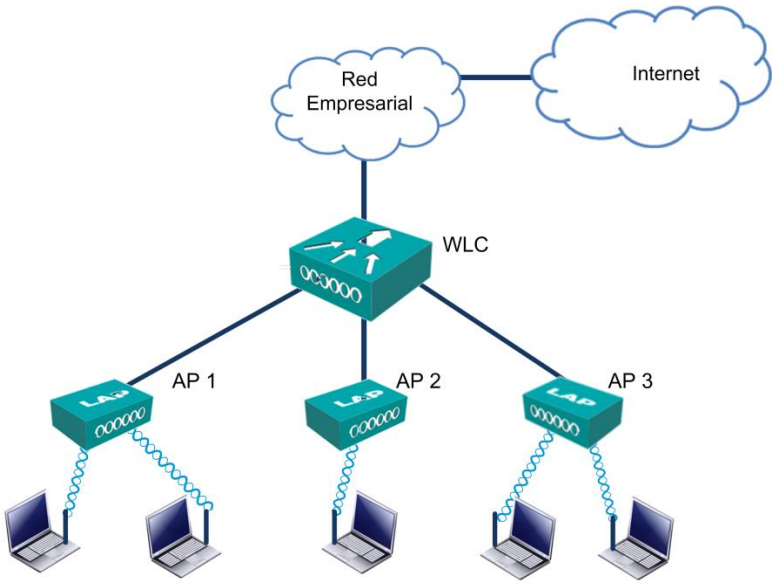


Figura 2.16 Sistema WLAN centralizado

Para habilitar el funcionamiento de los LAP a través del WLC se establecen los siguientes protocolos de red:

- Protocolo ligero para puntos de acceso (LWAPP)
- Control y aprovisionamiento de los puntos de acceso inalámbrico (CAPWAP)

Éstos se encargarán de proporcionar los mecanismos de gestión centralizada para varios AP en una red WLAN. En los siguientes dos temas, se darán a conocer las características generales que estos protocolos ofrecen para la implementación de un sistema centralizado y su diferencia de operación.

[19] En la literatura se asigna este nombre para los AP que solamente se encargan de recibir y transmitir señales de RF. También puede ser encontrado como LWAP.

2.7.1 Protocolo LWAPP

Las redes empresariales crecen continuamente en su infraestructura, lo que induce a un aumento en la gestión de sus dispositivos de acceso a la red. A través del protocolo LWAPP, aprobado como estándar por la IETF (por sus siglas en inglés: *Internet Engineering Task Force*) en la RFC 5412 [18], el WLC realiza la gestión centralizada de varios AP.

A continuación, se presentan las características de un sistema centralizado WLC basado en LWAPP.

- **Administración**

En sus inicios, las redes WLAN se componían de varios AP independientes distribuidos en los diferentes pisos de un edificio de una empresa, cada AP necesitaba de una supervisión y configuración individual, lo que implicaba una administración compleja y un aumento de recursos.

WLC a través de LWAPP presenta las siguientes características de administración de la red WLAN.

- Las operaciones de los LAP se reducen a recibir y transmitir el flujo de información.
- La configuración realizada a través del WLC se genera para todos los LAP.
- Centraliza la configuración y administración de los LAP.

- **Escalabilidad**

La implementación de nuevos LAP a la red se vuelve una operación de menor esfuerzo; tan pronto el LAP se registra en el WLC, los usuarios inalámbricos internos pueden hacer uso de este.

- **Seguridad**

En cuestión de seguridad, el sistema WLC basado en LWAPP ofrece varias ventajas sobre un sistema individual de AP, entre estas podemos encontrar:

- **Control.** El tráfico inalámbrico entra a la red a través del WLC en lugar de enviarlo a los múltiples AP tradicionales, por lo que la inspección del tráfico se controla de una forma más eficiente.
- **Autenticación.** WLC es el responsable de actuar como punto de autenticación.
- **Configuración.** Nadie puede alterar la configuración de los LAP ya que esto sólo se realiza desde el WLC a través de ciertos parámetros de seguridad.
- **Detección de AP maliciosos.** WLC implementa el sistema de detección de intrusos (IDS) para detectar los AP no identificados que desean unirse a la red.

LWAPP tiene dos tipos principales de tráfico:

- **Control.** Un canal de control se utiliza para la configuración, cifrado, autenticación, gestión de *firmware*, etc.
- **Datos.** El tráfico inalámbrico, encapsulado, se envía entre el LAP y el WLC.

- **Movilidad**

Cuando se habla de redes WLAN, el panorama que se desea es la movilidad de la ET inalámbrica entre las diferentes áreas que conforman a una empresa.

Cada WLC utiliza un túnel LWAPP, cuya función permite controlar la información de las ET móviles; a través de esto y de protocolos adicionales, es posible la interacción entre los WLC y la disponibilidad para *roaming* o movilidad[20].

2.7.2 Protocolo CAPWAP

CAPWAP, es un estándar que permite la gestión centralizada de un conjunto de LAP a través del WLC. CAPWAP basa su protocolo en un conjunto de RFC[21].

[20] En el Capítulo 3 se profundizará el tema de movilidad en redes WLAN.

CAPWAP se fundamenta en los mismos principios que LWAPP y al igual que este, permite la distinción entre el tráfico de datos y el de control. A diferencia de LWAPP, CAPWAP adiciona el establecimiento de seguridad en la capa de transporte (DTLS) definido en el RFC 4347 [19], el cual proporciona un túnel de seguridad en el envío de datos del tráfico de control. Aunado a ello, CAPWAP ofrece un nivel de seguridad en el cifrado del proceso de autenticación entre el LAP y el WLC (proceso que debe ser configurado en ambos elementos). Además, a través de las listas de control de acceso (ACL) preestablecidas, se evita la asociación de los AP no deseados a la red WLAN.

El proceso que lleva se realiza entre el LAP y el WLC a través de CAPWAP, es el siguiente:

1. **Descubrimiento.** Es el estado inicial de un LAP informando a los WLC que quiere realizar una comunicación a través de un protocolo en específico. Mientras tanto, el WLC se encuentra esperando una solicitud de descubrimiento de algún LAP. Una vez que el WLC ha recibido dicha petición por parte del LAP, el WLC pasa a la fase de Adquisición, sin responder aún. Tras el envío de respuesta por parte del WLC (en el caso de que la solicitud haya sido aceptada), el LAP se traslada a la misma fase que el controlador.

2. **Adquisición.** En esta fase, ambos dispositivos definen los protocolos de cifrado que utilizarán durante su comunicación; posteriormente el WLC se mueve al estado de Protección. En la Figura 2.17 se muestran los mensajes que se intercambian entre ambos dispositivos una vez que se ha emitido el mensaje de *"Client Hello"* emitido por el LAP.

3. ***Client Hello*.** El cliente (en el escenario CAPWAP, es el LAP) está enviando en el *client hello* una lista de todas sus algoritmos de cifrado que soporta, así como un valor aleatorio que se utiliza posteriormente para calcular el material clave utilizado para el cifrado CAPWAP.

4. ***Hello Verify Request/ Client Hello.*** Se realiza un intercambio de *cookies*[22] para evitar la denegación de servicio (DoS)[23] debido a un posible ataque a la red.

[21] Documento(s) que contiene un protocolo de red Internet, aprobado y regulado por la IETF *(Internet Engineering Task Force)*.
[22] Una *cookie* es una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.
[23] DoS puede generarse por la saturación del sistema debido al excesivo envío de solicitudes que impide que el sistema pueda resolver solicitudes reales.

5. ***Server Hello* / Certificado.** El servidor (en el escenario CAPWAP, es el WLC) selecciona el algoritmo de cifrado de la lista proporcionada y responde con su certificado y un valor aleatorio para el cliente (LAP).

6. **Certificado / *ClientKeyExchange* / *ChangeCipherSpec*.** Una vez que se ha seleccionado el modo de cifrado y se han validado los certificados, el cliente envía la *ClientKeyExchange* seguido por el protocolo de registro *ChangeCipherSpec. ChangeCipherSpec* notifica a la otra parte, que todos los registros posteriores se cifran por el método definido

7. ***Server-Change Cipher Spec*.** El servidor responde con un *Change Cipher Spec*, lo que significa que a partir de ahora, los datos enviados en ambas direcciones están cifrados. La sesión DTLS está plenamente establecida.

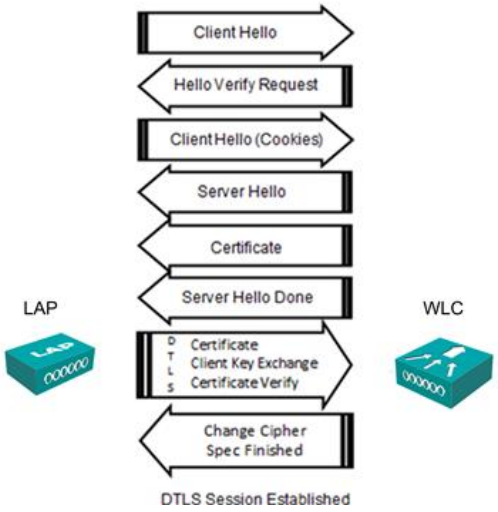


Figura 2.17 Establecimiento de CAPWAP y túnel DTLS

8. **Protección**. Esta fase establece un túnel cifrado. Una vez que se realizó el intercambio de mensajes anteriormente señalados, el WLC envía un mensaje de término indicando que el intercambio de mensajes DTLS ha finalizado. Posteriormente, el LAP se traslada a la fase de Protocolo de Control Negociado.

9. **Protocolo de Control Negociación**. Finalmente, ambos dispositivos comenzarán a comunicarse a través del protocolo previamente acordado.

2.7.3 Redundancia

En una red WLAN, también es preciso establecer mecanismos de protección frente a fallos, tanto en los LAP como en los mismos WLC. En caso de fallas, la red WLAN debe ser apta de estabilizar su sistema; los WLC[24] deben ser capaces de identificar la falla e indicar a los LAP que incrementen su potencia de radiación para cubrir las zonas afectadas (en el siguiente tema se ampliará este concepto).

En el caso de que un WLC tenga alguna falla, el sistema también debe ser capaz de que otro WLC asuma el control de los LAP asociados en el WLC caído.

A continuación, se muestran tres esquemas de redundancia en un sistema LWAPP [20].

- **Arquitectura N+N**

En esta arquitectura, se encuentran dos WLC (véase Figura 2.18). Algunos AP están configurados en el controlador A como primario y al B como secundario; los otros puntos de acceso están configurados para que el controlador B sea el primario mientras que A es el secundario.

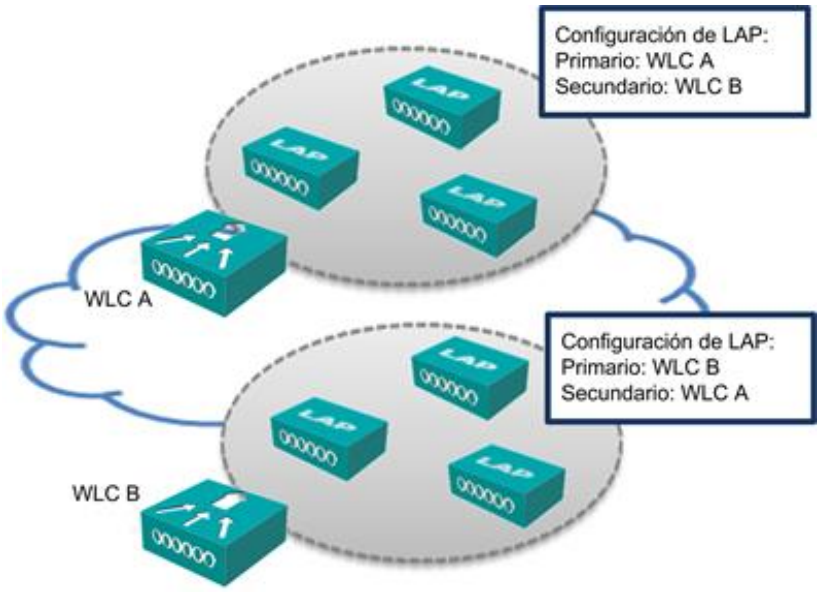


Figura 2.18 Arquitectura de redundancia N+N

[24] Un sistema de dos o más WLCs es denominado WCS *(Wireless Control System)*, su función se basa en administrar y monitorear los WLCs que se encuentren en su sistema de red inalámbrica.

Con este esquema es preciso equilibrar la carga de los controladores y tomar en consideración que en el caso de una falla en la red en que uno de los WLC caiga, el otro WLC asumirá los AP asociados del controlador que está sin funcionar. Por lo que hay que tomar en cuenta que el WLC secundario tenga la suficiente capacidad para tomar el control de todos los AP.

- **Arquitectura N+1**

En esta configuración, se coloca un WLC redundante, dicho controlador actúa como *backup* para los múltiples WLC. Cada LAP, se encuentra configurado con un WLC primario y un controlador secundario o *backup* (véase Figura 2.19). El inconveniente con este tipo de arquitectura, es el exceso de solicitudes, en el caso de que más de un WLC fallara. Aunque es poco probable este esquema de fallas, es conveniente evaluar un panorama de esta magnitud.

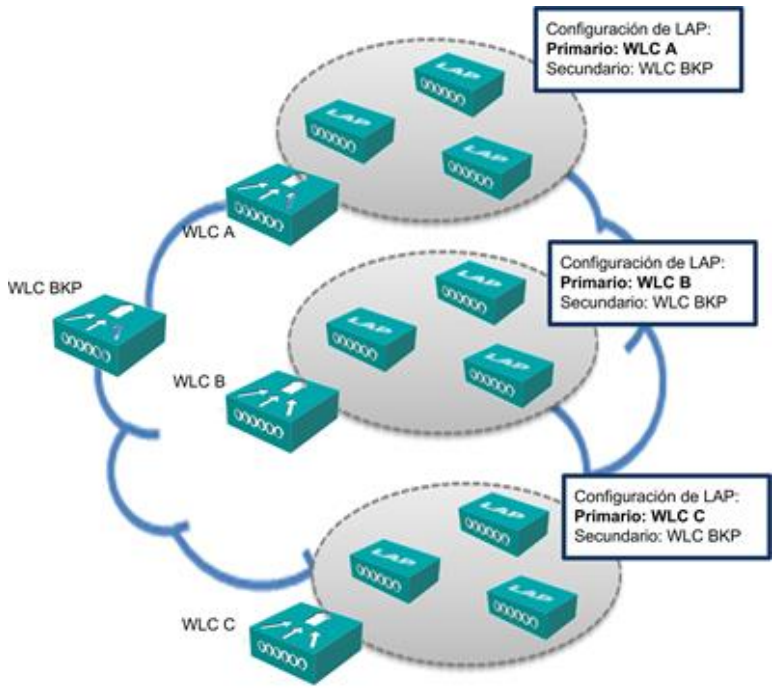


Figura 2.19 Arquitectura de redundancia N+1

La arquitectura consiste en una combinación de las anteriores configuraciones, algunos LAP están configurados a un controlador primario A y otros a un controlador secundario B;

aunado a ello se coloca un WLC secundario, que en este caso es un controlador *backup* (véase Figura 2.20). De esta forma varios LAP pueden ser redirigidos al WLC de *backup,* en caso de que el controlador secundario no soporte tantos LAP.

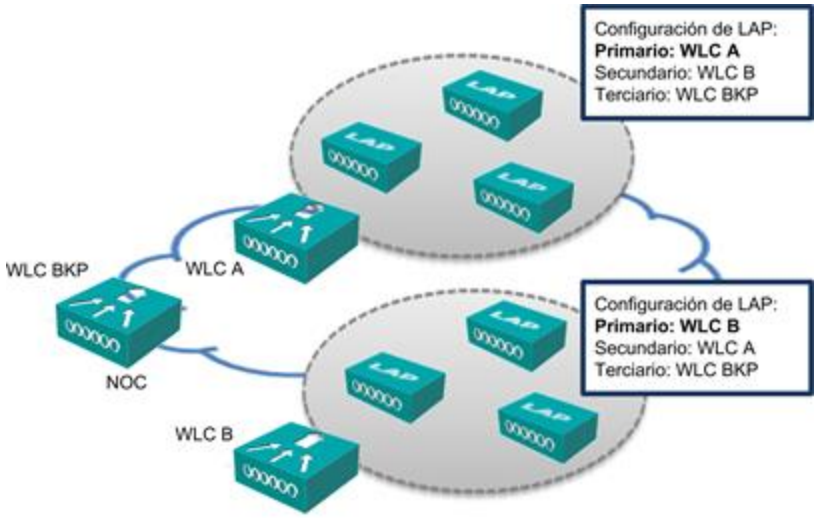


Figura 2.20 Arquitectura de redundancia N+N+1

2.7.4 Gestión de recursos de radio

Un su gestión, el WLC actúa como un sistema de administración de señales de RF en tiempo real. A través del sistema de gestión de recursos de radio (RRM) [21] es posible analizar continuamente la red WLAN entorno a las señales de RF cuyas características componen el tráfico en la red inalámbrica, la cobertura y la carga de usuarios en cada LAP, las interferencias por obstáculos y entre canales, etc.

Al recibir información constantemente del panorama de RF, RRM puede reconfigurar periódicamente el entorno de RF de tal forma que la red WLAN trabaje de manera más eficiente.

En sus principales funciones, RRM ofrece lo siguiente:

- **Control de recursos de radio.** Detección y configuración automática de nuevos WLC y LAP al añadirlos a la red WLAN.

- **Control de potencia transmitida (TPC)**. Se proporciona a través de los LAP la suficiente energía para alcanzar los niveles de cobertura deseados y de igual forma evitar interferencias de canales entre los LAP. Por medio de su algoritmo, TPC se encarga de aumentar o disminuir la potencia del LAP en respuesta al constante monitoreo del medio de RF.
- **Asignación dinámica de canales (DCA)**. A través de WLC la asignación de canales se realiza de manera dinámica para evitar interferencias entre canales. WLC ofrece en su operación, la desactivación de DCA y TPC para administrar y asignar de manera estática los canales y potencia de los LAP.

En resumen, RRM mantiene un monitoreo de RF constante sobre la red inalámbrica lo que permite establecer una red WLAN con capacidad y rendimiento óptimo.

Capítulo 3

CONSIDERACIONES PARA LA INTEGRACIÓN DE UNA RED EMPRESARIAL WLAN 802.11 SEGURA

El crecimiento y evolución de las tecnologías móviles tiende a que las compañías tengan la posibilidad de transformar sus redes cableadas en inalámbricas; siguiendo las tendencias de movilidad e integración para mayor rendimiento, fiabilidad, eficiencia y calidad en los servicios, lo que se traduce hoy en día en una empresa competitiva, tecnológicamente hablando.

Existen diferentes formas de estructurar una red WLAN, las cuales dependen del sector de desarrollo donde se esté implementando la misma; no obstante, toda empresa requiere que su red corporativa sea capaz de garantizar la disponibilidad de los recursos empresariales para dispositivos móviles; desplegando en la misma red, un conjunto de características como confiabilidad, seguridad, redundancia, compatibilidad, escalabilidad y gestión de la red.

En este capítulo se establecerán las consideraciones de seguridad necesarias para la incorporación de una correcta solución inalámbrica a la red WLAN 802.11 Empresarial, de tal forma que se logre un reparto de ancho de banda eficiente que permita a los usuarios, a través de las nuevas tecnologías inalámbricas, hacer uso de los medios corporativos de una forma rápida y segura sin centralizar los recursos de la red sobre otros.

3.1 Red WLAN 802.11 empresarial

En el capítulo anterior, se mencionaron las características básicas para la integración de una red WLAN, ahora compete mencionar las consideraciones que se deben tener en cuenta para la integración de la misma, enfocándose desde un punto de vista de una red WLAN empresarial segura.

La red WLAN empresarial debe proporcionar un conjunto amplio de servicios, ofreciendo a los usuarios de los dispositivos móviles un acceso seguro y siempre disponible en cualquier lugar del área de trabajo y en cualquier momento.

Las consideraciones de integración de la red WLAN corporativa (véase Figura 3.1) en que se enfocará la presente Tesis son:

- Capacidad
- Cobertura
- Rendimiento
- Seguridad
- Movilidad

Figura 3.1 Integración de una red WLAN 802.11

Cuando se habla de la integración o reestructuración de una red WLAN empresarial no es construir desde cero la red; es tomar las arquitecturas y recomendaciones ya existentes e integrarlas con las nuevas soluciones a la nueva red inalámbrica corporativa.

3.2 Capacidad y cobertura de una red WLAN 802.11 empresarial

Dos aspectos que deben ser considerados en la integración de una red WLAN empresarial son la capacidad y cobertura que proporcionará la misma.

- **Capacidad.** Será definido como el flujo de tráfico de la red WLAN; el cual, es variable dependiendo del número total de usuarios que el sistema inalámbrico puede conectar al mismo tiempo y de los recursos que los mismos usuarios demanden a la red inalámbrica.
- **Cobertura.** Corresponde al área geográfica donde se otorgarán los servicios de red inalámbrica.

Diversos factores pueden afectar la capacidad de tráfico y la cobertura de la red; entre ellos se encuentran: el tipo de antenas que se van a utilizar a través de los AP, el umbral mínimo de recepción que un dispositivo debe tener para recibir la información emitida por el transmisor, la potencia máxima con la que pueden operar las antenas transmisoras, la ubicación de los AP para lograr una cobertura lo más amplia posible, etc.

3.2.1 Antenas

Las antenas son dispositivos, por lo general metálicos, que conforman a un sistema de comunicaciones; por medio de éstas, es posible realizar la emisión y recepción de ondas electromagnéticas a través de un medio de transmisión libre como el aire.

En el área de las redes WLAN, las antenas se encuentran generalmente integradas en los AP y en cada una de las ET móviles.

La integración de las antenas es de vital importancia en la cobertura de una red WLAN, puesto que de no considerarlas en los AP, no se podrá conseguir una efectiva y máxima cobertura en los radios de alcance, llevando como consecuencia una mayor inversión al implementar más AP en el área de cobertura que se desea lograr.

Habitualmente, el proveedor de dispositivos de red WLAN integra una tabla de las características con las que cuenta un AP. En la Figura 3.2 se presenta un fragmento de las especificaciones de un AP *Cisco Aironet 1130 Series* [22], obsérvese que el AP mencionado, trabaja en el estándar IEEE 802.11n. De acuerdo al proveedor de servicios inalámbricos y al tipo de AP las características cambian.

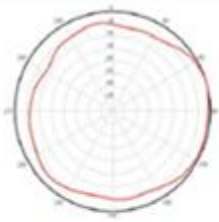
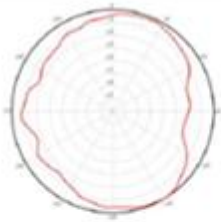
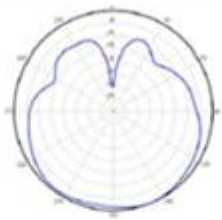
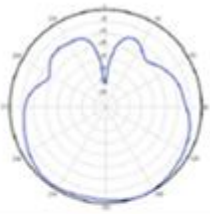
2.4GHz Plano de radiación horizontal	5 GHz Plano de radiación horizontal	2.4GHz Plano de radiación vertical	5 GHz Plano de radiación vertical
			
Rango de Frecuencias		• 2.4- 2.5 GHz • 5.15-5.85 GHz	
Ganancias		• 2.4 GHz: 4dBi • 5 GHz: 3dBi	
Polarización		Lineal, Vertical	
Azimuth (3dB Ancho de haz)		Omnidireccional	
Elevación (3dB Ancho de haz)		• 2.4 GHz: 120° • 5 GHz: 120°	
Conector de antena		Integrado	
Montaje		Integrado	
Tipo de Antena		Omnidireccional	

Figura 3.2 Fragmento de hoja de especificaciones: Cisco Aironet 1130 Series Integrated Antenna

En las siguientes secciones, se darán a conocer los tipos y propiedades generales de las antenas que integran a los AP.

3.2.1.1 Características

Existen diversas características que definen a una antena, las cuales deben ser consideradas al momento de su integración en un sistema de comunicaciones inalámbrico. A continuación se describen las características más importantes de las antenas que componen a los AP y sus consideraciones para su correcta integración en una red WLAN.

- **Ancho de banda**

El ancho de banda es la diferencia entre la frecuencia máxima y frecuencia mínima de operación de una antena; dicho de otra manera, es el intervalo de frecuencias dentro del cual una antena puede funcionar "satisfactoriamente".

En redes WiFi la frecuencia de operación se encuentra en 2.4 GHz (IEEE 802.11b/g/n) y 5 GHz (IEEE 802.11a/n).

- **Potencia y ganancia**

La ganancia de una antena es la relación entre la potencia que entra en una antena y la potencia que sale de esta. Ésta es comúnmente referida en dBi[25].

Una combinación inadecuada de nivel de potencia y ganancia de la antena puede provocar una potencia por encima de la permitida por el dominio regulador, en el caso de México, ANSI (por sus siglas en inglés: *American National Standard Institute)*. En la Tabla 3.1 se indican los niveles máximos de potencias y ganancias permitidos.

- **Polarización**

Es referido a la orientación del campo eléctrico que se irradia de una antena. Los dos tipos de polarización que existen son lineal y elíptica o circular; en la primera, los elementos de la entena se encuentran en un plano horizontal o vertical; en la segunda, si una antena describe un campo eléctrico que gira circularmente, la antena estará elíptica o

[25]dBi, es referido a la comparación de cuánta energía sale de la antena en cuestión, comparada con la que saldría de una antena isotrópica (antena que irradia con la misma intensidad de potencia en todas las direcciones).

circularmente polarizada.

Tabla 3.1 Nivel de potencia y ganancia máxima de una antena

Dominio regulador	Ganancia de antena (dBi)	Nivel de potencia máxima (mW)
ANSI ($EIRP^*_{máx} = 4\ W$)	0	100
	2.2	100
	5.2	100
	6	100
	8.5	100
	12	100
	13.5	100
	21	20

Fuente: *Channels, Power Levels, Antenna Gains*, Apendix B, Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for MS-DOS, p. 3. Consultado en www.cisco.com.
* Potencia isotrópica radiada equivalente (EIRP), es la potencia transmitida multiplicado por la ganancia de la antena transmisora.

- **Patrón de radiación**

Una de las características más importantes de una antena es su patrón de radiación. Éste es una representación gráfica de los campos radiados por la antena en función de la dirección del espacio.

- **Ancho de haz**

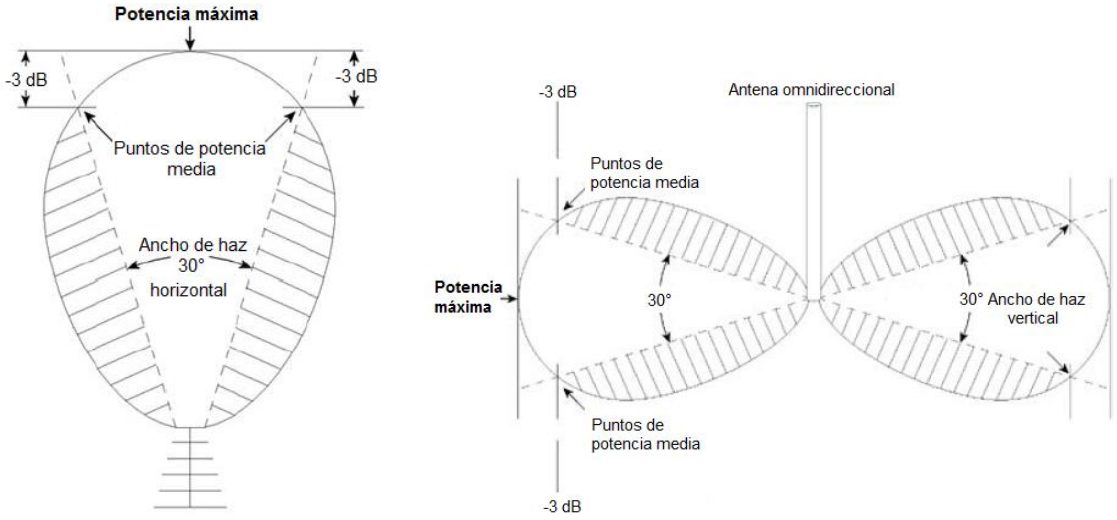
El ancho de haz *(beamwidth)* del lóbulo principal de una antena, indica que tan directiva es ésta. Mientras menor sea el ancho de haz (en grados) la antena concentrará más su energía en el lóbulo principal.

El ancho de haz se puede especificar en dos dimensiones:

- **Ancho de haz horizontal (alrededor de la antena).** Esta antena tiene un lóbulo principal que se extiende hacia fuera desde la parte frontal de la antena. La Figura 3.3a muestra un ejemplo del patrón horizontal de una antena direccional.
- **Ángulo de cobertura vertical (por encima y por debajo de la antena).** Esta antena tiene un lóbulo principal que se extiende hacia fuera en todas las

direcciones de la antena. La Figura 3.3b muestra un ejemplo del patrón vertical de una antena omnidireccional.

Obsérvese en la Figura 3.3 que el ancho de haz, se encuentra representado como la separación angular entre los dos puntos de potencia media (-3 dB) en el lóbulo principal del patrón de radiación de la antena.



(a) (b)

Figura 3.3 Ancho de haz: (a) horizontal; (b) vertical

3.2.1.2 Tipos de antenas

Existen diferentes tipos de antenas para su uso a través de los AP que operan en las bandas de frecuencia de 2.4 GHz y 5 GHz. Cada tipo de antena ofrece diferentes capacidades de cobertura; en los siguientes puntos se muestran, de forma general, las características y patrones de radiación que clasifican a las antenas.

Los tipos de antenas son diversos, un ejemplo de su clasificación es la siguiente:

- **Frecuencia y tamaño.** La longitud de onda es diferente de acuerdo con la frecuencia de operación en la que se desee trabajar; dado lo anterior, las antenas son de diferentes tamaños para radiar las señales de acuerdo a su longitud de onda. En el caso de redes inalámbricas que utilizan las bandas de frecuencia de 2.4 GHz y 5 GHz, la longitud de onda es de 12.5 cm. y 6 cm, respectivamente.

- **Directividad.** De acuerdo a su directividad, las antenas pueden clasificarse como omnidireccionales, sectoriales o directivas (véase Figura 3.4). Las antenas omnidireccionales están constituidas de un solo brazo rectilíneo irradiante en posición vertical, este tipo de antenas irradian aproximadamente con la misma intensidad los 360° del plano horizontal. Las antenas sectoriales, irradian en un área específica, su ancho de haz oscila entre los 60° y 180°. Las antenas directivas tienen un ancho de haz más angosto y por lo tanto una ganancia mayor que las antenas sectoriales.

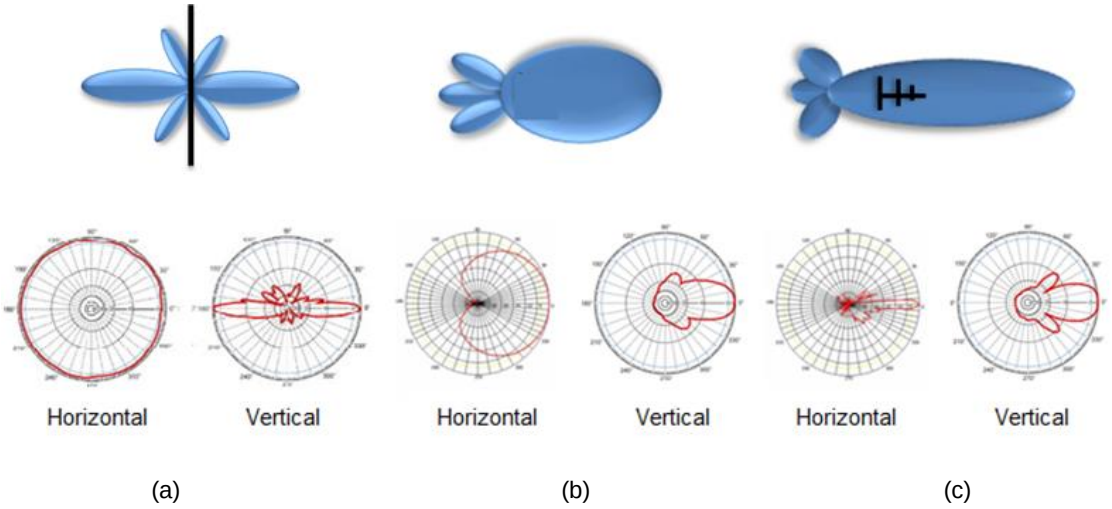


Figura 3.4 Tipos de antenas: (a) omnidireccional; (b) sectorial; (c) direccional

- **Aplicaciones.** De acuerdo a su aplicación, las antenas pueden clasificarse de diversas maneras. En el área de redes WLAN, los AP tienden a hacer redes punto a multipunto utilizando antenas omnidireccionales que irradian en todas las direcciones o antenas sectoriales que se enfocan en un área limitada.

3.3 Rendimiento en una red WLAN empresarial

En el ámbito empresarial, el rendimiento de una red WLAN constituye una parte fundamental en la productividad de la empresa dado que, como consecuencia de un bajo rendimiento de la red WLAN, los usuarios no pueden acceder de forma eficiente a los servicios. Los factores que pueden alterar el rendimiento de la red WLAN son diversos, algunos dependen de la configuración con la que se realizó la red inalámbrica misma, mientras que otros son factores físicos que son independientes de la infraestructura lógica de la red WLAN; sin embargo, con un correcto diseño es posible aminorarlas.

El rendimiento de una red puede ser definido como el número de paquetes recibidos en un intervalo de tiempo; por lo que, los usuarios pueden ver el rendimiento de la red corporativa como qué tan rápido pueden acceder a los servicios, de ahí la importancia de tener un buen rendimiento en la red WLAN: mayor rendimiento es igual a mayor rapidez y mayor rapidez es igual a mayor eficiencia laboral.

3.3.1. Problemas de rendimiento en una red WLAN empresarial

Los principales problemas de rendimiento que pueden afectar una red WLAN de alta densidad, como lo son las redes corporativas, están comprendidos en la siguiente clasificación:

- Interferencias:
    - Entre canales
    - Por señales de RF
    - Por obstáculos

- Demanda excesiva de servicios:
    - Voz
    - Datos

- Vídeo

Cada uno de los puntos de las anteriores clasificaciones provoca individualmente o en conjunto una disminución del rendimiento de la red inalámbrica. Es por ello de la importancia de tener en cuenta estos factores al integrar una red WLAN empresarial.

En los siguientes subtemas, se mencionarán brevemente las características de cada uno de los problemas que pueden alterar el rendimiento de la red WLAN.

3.3.1.1 Interferencias

Las tres principales causas de interferencias que deben ser tomadas en cuenta para la integración de una red WLAN son:

- **Interferencia entre canales**

Bajo los estándares del estándar IEEE 802.11, se definen los canales de frecuencia para las comunicaciones inalámbricas, su objetivo es determinar el rango de frecuencias de cada canal en el que trabajan los dispositivos inalámbricos para que no interfieran entre sí; sin embargo, debido a la técnica SS, empleada para la transmisión de datos, el ancho de banda se expande entre canales contiguos provocando la interferencia entre canales; en otras palabras, si dos dispositivos emplean canales contiguos estos crearán interferencia entre sí provocando una disminución del rendimiento en la red WLAN.

Para evitar interferencias entre canales; por ejemplo, en la banda de 2.4 GHz se permite tener solamente tres canales no interferentes. La Figura 3.5 muestra gráficamente la disposición de canales y el espaciado entre estos; obsérvese que los mejores canales a utilizar son el 1, 6 y 11 puesto que no se crean interferencia entre ellos; además, no existe un traslape entre canales y se cuentan con una banda de guarda de 3 MHz.

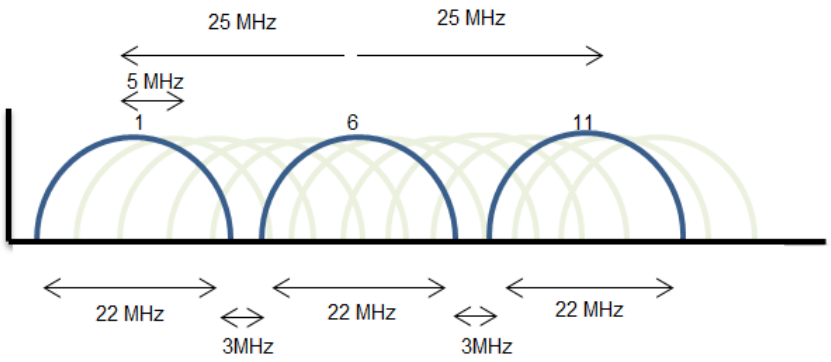


Figura 3.5 Canales en la banda de operación de 2.4 GHz

En la práctica, el administrador de la red WLAN debe tomar en cuenta la asignación de canales para evitar disminución de la potencia de la señal debido a dicha interferencia. En la Figura 3.6 se encuentran tres AP colocados en las bandas de frecuencia de 1, 6 y 11; obsérvese que no hay traslape en la señal.

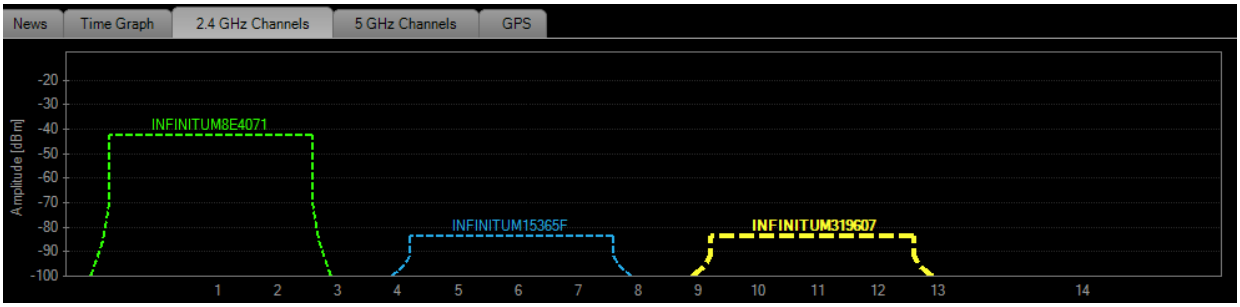


Figura 3.6 Distribución de canales para tres AP

La tecnología 802.11n internacionalmente permite trabajar dualmente en las dos bandas frecuencia de 2.4 GHz y 5 GHz, la primera cuenta con 14 canales con 22 GHz de ancho de banda cada uno y la segunda cuenta con 30 canales con 20 GHz de ancho de banda cada uno. Para mayor detalle de los canales de operación IEEE 802.11n utilizados en México, véase Tabla 3.2.

Tabla 3.2 Canales de operación IEEE 802.11n a 2.4 GHz y 5 GHz

Localización de canales IEEE 802.11n								
2.4 GHz			**5 GHz**					
Canal	Frecuencia [GHz]	Mx	Canal	Frecuencia [GHz]	Mx	Canal	Frecuencia [GHz]	Mx
1	2.412	X	184	4.920		100	5.500	X
2	2.417	X	188	4.940		104	5.520	X
3	2.422	X	192	4.960		108	5.540	X
4	2.427	X	196	4.980		112	5.560	X
5	2.432	X	208	5.040		116	5.580	X
6	2.437	X	212	5.060		120*	5.600	X
7	2.442	X	216	5.080		124*	5.620	X
8	2.447	X	36	5.180	X	128*	5.640	X
9*	2.452	X	40	5.200	X	132*	5.660	X
10*	2.457	X	44	5.220	X	136*	5.680	X
11*	2.462	X	48	5.240	X	140*	5.700	X
12	2.467		52	5.260	X	149	5.745	X
13	2.472		56	5.280	X	153	5.765	X
14	2.484		60	5.300	X	157	5.785	X
			64	5.320	X	161	5.805	X

Fuente: *Cisco Aironet 1130 Series Integrated Antenna*, IEEE 802.11 a/b/g/n Wi-Fi Standards and Facts, pp. 5-6. Consultado en www.cisco.com.
*Utilizados en áreas internas y externas

- **Interferencia por señales de RF**

Las redes WLAN son susceptibles a una gran cantidad de dispositivos y aparatos que operan en las bandas de operación del estándar IEEE 802.11, tal es el caso de los aparatos eléctricos como teléfonos inalámbricos, analógicos o el horno de microondas, los cuales interfieren y degradan el nivel de señal esperada e inclusive es posible que deshabiliten las operaciones del AP.

- **Interferencia por obstáculos**

La cobertura que ofrece un AP depende del fabricante y es posible conocer su potencia de transmisión a través de las hojas de especificaciones; sin embargo, es necesario recordar que este patrón de radiación fue realizado en condiciones ideales; esto es, sin tomar en cuenta los obstáculos que se pueden encontrar en condiciones reales como en el edificio de una empresa. Descrito lo anterior, otra de las consideraciones para la

integración de la red WLAN, es saber con qué materiales se encuentra construido el lugar donde serán instalados los AP, puesto que cuando las ondas electromagnéticas atraviesan algún material, se debilitan o atenúan. En la Tabla 3.3, se muestra la atenuación provocada por algunos materiales de construcción para las bandas de frecuencia del estándar IEEE 802.11n.

Tabla 3.3 Atenuación por materiales de construcción

Material de construcción	2.4 GHz Atenuación [dBi]	5 GHz Atenuación [dBi]
Puerta de madera sólida 4.5 cm.	6	10
Puerta de madera hueca 4.5 cm.	4	7
Puerta interior de oficina con ventana 4.5 cm/1.5 cm.	4	6
Puerta de acero 4.5 cm.	13	25
Puerta de acero 4.5 cm.	19	32
Pared de ladrillo	6	10
Pared de concreto 45 cm.	18	30
Pared exterior de concreto 68 cm.	53	45
Divisor de vidrio 1.5 cm.	12	8
Pared interior hueca 10 cm.	5	3
Pared interior hueca 15 cm.	9	4
Pared interior solida 13 cm.	14	16
Mármol 5 cm.	6	10
Vidrio a prueba de balas 2.5 cm.	10	20
Panel exterior doble de vidrio recubierto 2.5 cm.	13	20
Ventana exterior de vidrio 1.5 cm.	7	6
Ventana interior de oficina 2.5 cm.	3	6
Vidrio de seguridad 1 cm.	3	2
Vidrio de seguridad 2.5 cm.	13	18

Fuente: *Attenuation Properties of Common Building Materials,* 3Com Corporation, Corporate Headquarters, 2005, p.6. Consultado en http://es.scribd.com.

3.3.2 Demanda de servicios

Actualmente las redes WLAN corporativas tienen la tendencia de ser redes convergentes a través de las cuales, ya no sólo se establece tráfico de datos, ahora se ha adicionado las comunicaciones de voz y vídeo.

La alta demanda de peticiones de los servicios multimedia, por parte de los usuarios, tiene como consecuencia el congestionamiento en la red y una QoS pobre cuando ésta no está preparada. En este punto es necesario extender el concepto de QoS, el cual se definirá como la capacidad de la red WLAN para proporcionar un mejor servicio a un usuario, grupo de usuarios o servicios específicos.

QoS proporciona un servicio diferenciado para seleccionar un tipo de tráfico en la red sobre las diversas tecnologías proporcionando los siguientes beneficios:

- Permite a los administradores de la red WLAN establecer niveles de servicio de acuerdo al tipo de usuario en la red.
- Los recursos de la red WLAN son compartidos de manera más eficiente.
- Establece la incorporación de servicios multimedia.
- Prioriza el tráfico e impide la monopolización de los recursos.
- Incorpora la clasificación de tráfico.
- Gestiona y minimiza la congestión de la red inalámbrica.
- Permite un control de *jitter* y latencia.

En redes WLAN, la calidad de servicio define el rendimiento de un sistema de transmisión y la disponibilidad de sus servicios. Para que una red inalámbrica pueda incorporar QoS, debe de tener una alta disponibilidad.

QoS es determinado por tres factores: latencia, *jitter* y pérdida como se detalla a continuación [23]:

- **Latencia o retardo**. Es la cantidad de que tarda un paquete para llegar a un punto de recepción final desde el extremo de envío. Este periodo de tiempo es denominado también como retardo de extremo a extremo.
- ***Jitter* o retardo de la varianza.** Es la diferencia en la latencia de extremo a extremo entre los paquetes. Por ejemplo, si un paquete necesita 210 ms para

atravesar la red desde el punto final de la fuente al punto final de destino, y el siguiente paquete necesita 150 ms para realizar el mismo viaje, el *jitter* se calcula como 60 ms.

- **Pérdida de paquetes.** Es una medida comparativa de paquetes no transmitidos satisfactoriamente y recibidos, contra el número total que se transmitieron. La pérdida se expresa como el porcentaje de paquetes que no llegaron a su destino.

3.3.2.1 Implementación de QoS en redes WLAN 802.11

La implementación de calidad de servicio (QoS) se basa en la clasificación del tráfico inalámbrico; esto permite a los dispositivos de operación (WLC), reconocer los diferentes tipos de tráfico que circulan por la red WLAN y aplicar las políticas de prioridad de acuerdo al servicio solicitado o al grupo de personas que utilizan la red.

Para poder implementar QoS en dispositivos de Capa 2 y 3 del modelo OSI, se requiere de un protocolo que permita clasificar el tráfico utilizando el encabezado de la trama. Para redes WLAN se define el protocolo IEEE 802.11e [24], el cual proporciona un mecanismo para QoS a nivel de MAC, este procedimiento consiste en la utilización de tres bits del encabezado de la trama para identificar el tipo de tráfico que se transmite por la red.

3.3.2.2 Niveles de prioridad de tráfico multimedia

Para poder establecer diferentes tipos de tráficos en el medio inalámbrico, el estándar IEEE 802.11e define la posibilidad de trabajar hasta con 8 clases de servicio diferentes. Para acelerar la adopción de tecnologías de calidad de servicio en redes IEEE 802.11 y mientras se aprobaba el estándar, la *Alliance Wi-Fi* desarrolló WMM *(WiFi MultiMedia)*.

WMM es una reformulación de los 8 niveles de prioridad originales de IEEE 802.11e agrupados en cuatro categorías. De esta forma, el tráfico que circula por la red WLAN puede tener prioridad sobre algunos servicios.

WMM introduce la prioridad de tráfico basándose en la definición de cuatro categorías de acceso: platino, oro, plata y bronce (véase Tabla 3.4). Cuanta más alta es la prioridad, mayor es la probabilidad de que el tráfico sea transmitido en primer lugar. De esta manera, el tráfico de clase platino será enviado antes que el oro, el plata o el bronce.

A continuación se muestran las características generales que definen a los niveles de QoS:

- **Platino.** Garantiza una alta calidad de servicio para voz sobre redes inalámbricas.
- **Oro.** Soporta aplicaciones de alta calidad de vídeo.
- **Plata.** Integra un 30 % del ancho de banda total (configuración por defecto).
- **Bronce.** Proporciona el mínimo porcentaje de ancho de banda reservado para los servicios de los clientes.

Tabla 3.4 Niveles de QoS

WMM	Alianza Wi-Fi	802.11e	Ancho de banda reservado
Voz	Platino	6 o 7	70 %
Vídeo	Oro	4 o 5	50 %
Best effort	Plata	1 o 2	30 %
Background	Bronce	0 o 3	20 %

Fuente: Mangold, et. al., *Analysis of IEEE 802.11e for QoS support in wireless LANs*, Wireless Communication, Journal & Magazines, vol. 10, December 2003, pp.40-50.

En la práctica, el administrador de la red puede configurar un nivel de QoS y posteriormente aplicar los perfiles a las redes WLAN difundidas; de tal manera que la configuración predeterminada en los perfiles es ejecutada a los dispositivos de los usuarios asociados a la WLAN. Además, el administrador puede crear funciones de QoS para especificar diferentes niveles de ancho de banda para los usuarios internos e invitados.

3.4 Seguridad de una red WLAN 802.11 empresarial

Hasta este punto, las consideraciones para la integración de una red WLAN 802.11 se han enfocado en tratar de asegurar una conexión entre un dispositivo móvil y un LAP para hacer uso de los recursos corporativos y evitar interferencias que puedan provocar una significativa disminución de la potencia de la señal y por consecuencia no tener acceso a la red WLAN. En las siguientes secciones, corresponde centrar la atención en lo que es la seguridad de las redes WLAN, el cual es el punto crítico en la integración de una red WLAN corporativa, ya que de ésta depende la integridad que conforma a la empresa.

De acuerdo a un estudio de seguridad realizado por la organización WTIA *(Wireless Technology Industry Association)* [29], la seguridad de las empresas se ve de la siguiente manera: un 58 % se considera segura, mientras que un 20 % es poco segura; con los avances en las soluciones para establecer seguridad en las redes WLAN sería de esperar que no hubiera empresas que se consideraran inseguras; sin embargo, un 22 % se encuentra en esta clasificación (véase Figura 3.7).

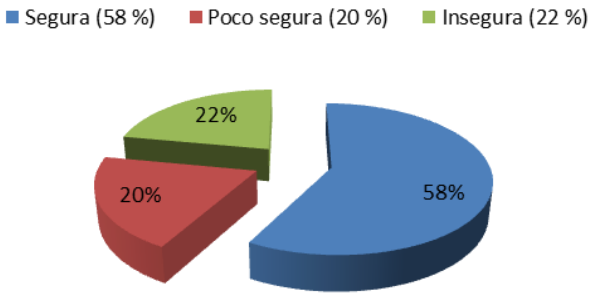


Figura 3.7 Seguridad en redes WLAN empresariales [29]

La solución a la seguridad en redes WLAN corporativas depende de protocolos, herramientas y políticas de seguridad que se implementen; y estas a su vez, van a corresponder a la capacidad del sistema de red, ya que una excesiva implementación en la seguridad puede reducir la rapidez y disponibilidad del sistema.

En la Tabla 3.5 se muestra los requisitos necesarios para integrar una red WLAN corporativa segura.

Tabla 3.5 Requisitos de seguridad en redes WLAN 802.11 empresariales

Requisitos de seguridad en redes WLAN 802.11 empresariales.		
Ingeniería Social	• Conocimiento de las normas de seguridad que los integrantes de la empresa deben saber.	
Autenticación y cifrado	• 802.1x • EAP (EAP-TLS, EAP-TTLS)	• RADIUS • WPA2
Protección y control de acceso a la red	• NAC/NAP	• ACS
Detección y protección de intrusos	• WIPS	
Aplicaciones de seguridad	• Firewall • DMZ	

3.4.1 Ingeniería social

La seguridad de la red inalámbrica, no reside solamente en las herramientas de seguridad que la empresa aplique a la red WLAN, también depende de cómo el usuario maneje la información; para ello, se debe comunicar y hacer que los empleados concienticen que la información de la empresa es intransferible y mientras se tomen las medidas correspondientes, éstos apoyarán en la seguridad de la red WLAN corporativa.

Algunas de las recomendaciones que se deben ofrecer a los usuarios de las redes WLAN son:

- Evitar transferir la información a personal que no sean parte de la empresa.
- No divulgar información secreta como contraseñas administrativas.
- Evitar la instalación de puntos de acceso no avalados por la empresa.
- Comunicar al administrador en caso de extravío del dispositivo móvil que se encuentre activo en la red.
- **Evitar transferir certificados digitales en medios de almacenamiento como USB (*Universal Serial Bus*).**

3.4.2 Autenticación y cifrado

En las redes WLAN empresariales es imprescindible tener una medida de seguridad mayor que en una red doméstica. El establecimiento de los siguientes parámetros de seguridad permite establecer las bases para mantener la seguridad de los datos corporativos.

El cifrado, es el modo en que los datos son codificados a medida que se envían por la red por medio de protocolos como WPA2. La autentificación a diferencia del cifrado, definirá el modo en que el dispositivo móvil en sí se identifica en la red; es decir, es el medio en el que el usuario demuestra ser quien dice ser. En seguridad de redes, existen tres formas de autenticar a un usuario o dispositivo; dependiendo del número de formas que se utilicen para autenticar es el grado de seguridad mayor o menor que se proporciona.

Formas de autenticación:

- **Algo que se sabe.** Es el método más conocido, este realiza una pregunta y solo el usuario o dispositivo que se quiere autenticar debe ser el único capaz de responderla, su grado de seguridad depende de los elementos de entrada (ejemplo, el nombre de usuario y contraseña).

- **Algo que se tiene.** Este método, valida al usuario a través de algún elemento único al que solo ese usuario debería tener acceso; por ejemplo, una tarjeta inteligente, un *token* de seguridad o un certificado digital, este medio concede la identidad al que lo posea.

- **Algo que se es.** Debe ser una característica exclusiva del usuario o el dispositivo que se desee identificar. Una huella dactilar en el caso del usuario o una dirección MAC en el caso de un dispositivo (aunque este último puede ser fácilmente clonado).

Para garantizar un nivel de seguridad aceptable, es necesario implementar por lo menos dos de las tres formas de autenticación mencionadas anteriormente.

3.4.2.1 Arquitectura IEEE 802.1x

El estándar IEEE 802.1x [26] realiza el control de acceso a una red WLAN por medio de un proceso de autenticación basada en puertos. Es importante señalar que este estándar no es en sí mismo un método de autenticación, por lo que su empleo se realiza en conjunto con protocolos de autenticación y cifrado para llevar a cabo la verificación de las credenciales del usuario (forma de autenticación) así como, la generación de claves de cifrado.

El proceso de autenticación de IEEE 802.1x consiste en la autorización o denegación de acceso a la red WLAN de acuerdo a las credenciales del usuario, a través de un servidor de autenticación y mediante el protocolo EAP.

Los elementos que intervienen en la arquitectura de un sistema IEEE 802.1x son:

- **Autenticador.** Corresponde al AP cuya función es llevar a cabo el intercambio de tráfico entre el solicitante y el servidor de autenticación. En el caso en que se tiene un sistema centralizado, los WLC son los que funcionan como autenticador.

- **Solicitante.** Usuario con una ET móvil que solicita acceder a los servicios de la red.

- **Servidor de autenticación.** Se encarga de autenticar las credenciales del usuario e indica si el usuario está autorizado para acceder a los servicios de la red.

En la Figura 3.8, se muestra la arquitectura de autenticación de una red WLAN donde la interacción entre el solicitante y el autenticador corresponde al estándar IEEE 802.1x. En la función de solicitante, un usuario pide acceso a los servicios que puede tener desde el puerto del autenticador.

El protocolo entre el autenticador y el servidor de autenticación es RADIUS (por sus siglas en inglés: *Remote Authentication Dial-In User Server*). Durante el proceso, el WLC (autenticador de la red WLAN) se encargará de solicitar las credenciales del usuario, antes de permitir el acceso a los servicios que puede tener el usuario desde el puerto autenticador, a petición del servidor RADIUS. Una vez revisadas las credenciales del

usuario, el servidor de autenticación responde al autenticador si el solicitante tiene autorización para el acceso a los servicios del autenticador o es denegado el acceso.

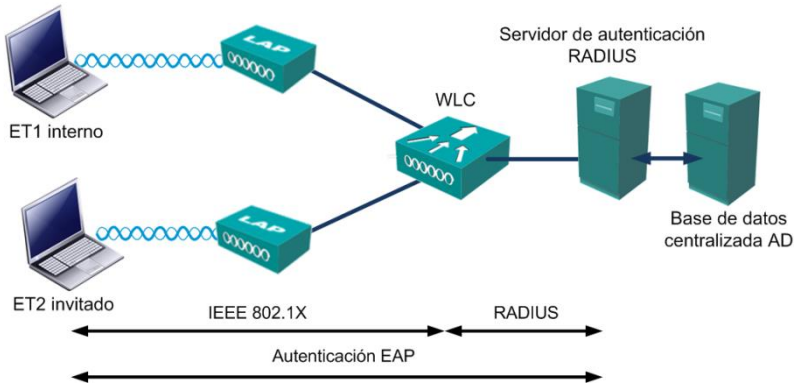


Figura 3.8 Arquitectura de autenticación IEEE 802.1x y EAP basada en RADIUS

3.4.2.2 Sistema de autenticación RADIUS

El proceso de un sistema de autenticación a través de RADIUS se establece de la siguiente manera: cuando un usuario entrega sus credenciales la validación de las mismas se lleva a cabo contra un servidor de autenticación, en este caso un servidor RADIUS. El servidor RADIUS los contrastará contra una base de datos de usuario centralizada, que puede residir en el mismo servidor RADIUS o en un directorio activo (AD), para comprobar si el usuario es un usuario válido o no. Una vez corroborada la veracidad de la identidad del usuario, el acceso se le permite y puede hacer uso de la red y sus servicios. Además, el sistema puede adaptar la conexión ofreciendo los niveles de calidad de servicio correspondientes de acuerdo al perfil del usuario o grupo de usuarios.

La arquitectura de un mecanismo de autenticación a través de RADIUS, permite centralizar el proceso de autenticación a través de un servidor RADIUS único y un una base de datos centralizados, en lugar de mantener una base de datos de usuarios válidos repartida en los diferentes AP de la red WLAN, como se harían en redes WLAN de generaciones anteriores.

El proceso de intercambio de mensajes de autenticación entre el usuario y el servidor RADIUS consiste en los siguientes puntos, véase Figura 3.9:

- El proceso inicia cuando un usuario se conecta a la red a través de un LAP e introduce sus credenciales, ya que el WLC se las solicita.
- A continuación el WLC envía un mensaje de petición de acceso (*RADIUS Access Request*) al servidor que contiene acceso a la base de datos donde se almacenan las credenciales, el puerto de conexión, la identidad del WLC y un mensaje autenticador.
- El servidor se basará en la dirección origen del paquete, la identidad del WLC y el autenticador para determinar si el WLC está autorizado para llevar a cabo peticiones.
- En caso afirmativo, el servidor buscará en la base de datos un identificador de usuario que coincida con el enviado en la petición. Si lo encuentra, lo contrastará y comprobará el tipo de acceso asociado al perfil del usuario.
- Si el usuario es autenticado y aprobado para utilizar el servicio, el servidor le envía un mensaje de acceso autorizado, *RADIUS Access-Accept*. En caso contrario se le enviará un mensaje de acceso rechazado, *RADIUS Access-Rejected*, y el WLC desconectará al usuario.

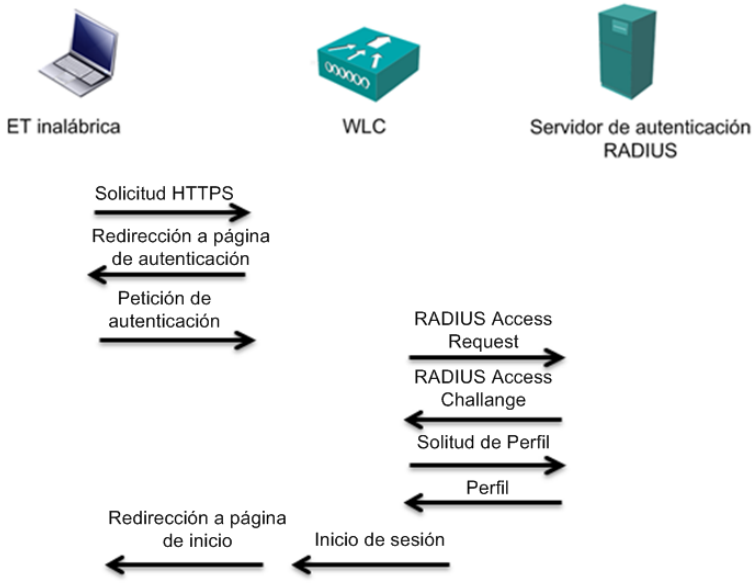


Figura 3.9 Intercambio de mensajes RADIUS

3.4.2.3 Protocolo de autenticación extensible EAP-TLS y EAP-TTLS

El empleo del protocolo de autenticación extensible (EAP) permite llevar a cabo una autenticación de punto a punto a través de los métodos de autenticación como certificados y tarjetas inteligentes. Cuando un usuario interno se conecta a una red WLAN, a través de una estructura IEEE 802.1x utilizando EAP, tanto en el servidor RADIUS como el solicitante deben llevar a cabo la verificación de credenciales, de esta forma EAP deja establecido una autenticación fuerte.

Durante el proceso de autenticación, EAP genera lo que se denominará "llaves de cifrado"[26] para mantener el intercambio de mensajes durante la autenticación con un grado de seguridad mayor al cifrar dichos mensajes. Las llaves están divididas en dos grupos [27]:

- **Llave de sesión *(Pairwise key)*.** Se establece de manera única para la asociación y comunicación *unicast* de una ET inalámbrica y WLC.
- **Llave de grupo *(Groupwise key)*.** Se establece en todas las ET inalámbricas y el WLC para establecer una comunicación *multicast* y *broadcast*.

Sucinto, EAP se encarga de transportar los métodos de autenticación entre la ET inalámbrica y el servidor de autenticación RADIUS, mientras que IEEE 802.1x define cómo enviar EAP sobre la red inalámbrica. En conjunto, estos dos mecanismos forman una fuerte estructura de autenticación.

Existen diferentes tipos de EAP, la Tabla 3.6 muestra una síntesis de las características de los métodos de autenticación EAP soportados por IEEE 802.1x.

Ya que se desea establecer una red WLAN segura, la presente Tesis se enfocará en el método EAP con certificados. El protocolo EAP con seguridad en la capa de transporte (EAP-TLS) es uno de los métodos más seguro ya que utiliza certificados X.509 [28], estándar emitido por el sector de normalización de las telecomunicaciones (ITU-T, por sus siglas en inglés: *ITU-Standarization Sector Telecommunications)*, para autenticar tanto al

[26] También encontrado en la literatura como claves de cifrado.

usuario como al servidor autenticador (RADIUS). Estos certificados son emitidos por una autoridad de certificación (CA) de la empresa, quien se encarga de asignar una cuenta de usuario o una cuenta de equipo en el servicio de AD.

Tabla 3.6 Métodos de autenticación EAP

EAP	Autentica-ción del servidor	Autenticación del cliente	Generación de claves	Seguridad de las credenciales	Reautenti-cación rápida	Túnel seguro	Compatible con WPA, WPA2
MD5	No	Contraseña hash	No	Débil	No	No	No
LEAP	Contraseña hash	Contraseña hash	Si	Fuerte	No	No	Si
TLS	Certificado X.509	Certificado X.509	Si	Fuerte	Si	No	Si
TTLS	**Certificado X.509**	**PAP, CHAP, MSCHAPv2, cualquier EAP**	**Si**	**Fuerte**	**Si**	**Si**	**Si**

Fuente: Pellejero, et. al., *Seguridad en Redes WLAN,* Conozca lo esencial para su empresa, Colección Guías Técnicas,Sociedad para la Promoción y Reconversión Industrial, pp.4. Consultado en www.euskadinnova.net/documentos/303.aspx - España.

EAP establece a través del protocolo SSL-TLS una conexión segura por medio de un canal cifrado entre el usuario y el servidor de autenticación RADIUS, el cual se basa en tres fases:

- **Negociación.** El usuario de la ET móvil y el servidor RADIUS determinan los algoritmos de cifrado que se utilizarán para autenticar y cifrar la información.
- **Autenticación y llaves.** Los extremos se autentican mediante certificados digitales e intercambian las llaves (pública y privada) para el cifrado.
- **Transmisión segura.** Se inicia el tráfico de información cifrada y autenticada.

En la Figura 3.10 se muestra, a manera de ejemplo, la interacción entre el usuario y el servidor RADIUS a través del protocolo EAP-TLS.

Obsérvese que a través de este esquema se crea una conexión más segura al identificar al usuario; sin embargo, mantiene una debilidad: los certificados así como los mensajes

de aceptación y denegación de la conexión son enviados a través de la interfaz sin ser cifrados lo que implica que un atacante informático pueda suplantar la identidad del usuario.

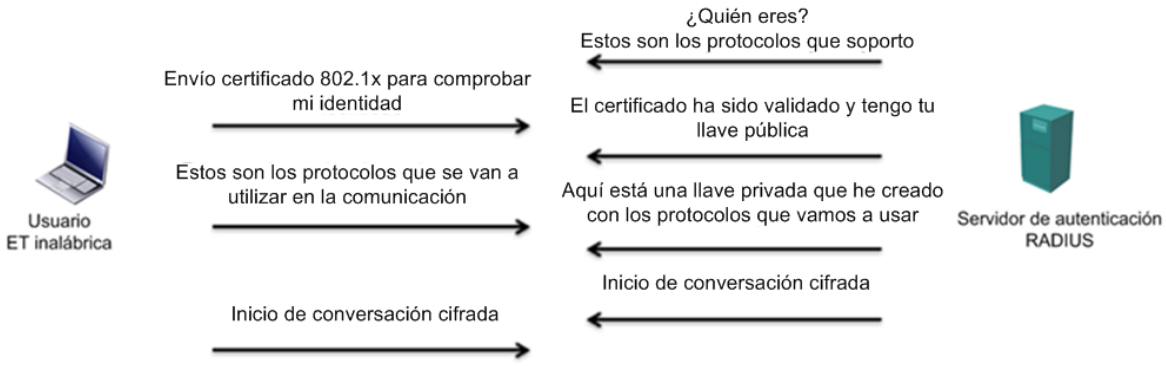


Figura 3.10 Esquema de funcionamiento del protocolo EAP-TLS

Como solución a las debilidades de EAP-TLS, se emplea el protocolo EAP con túnel de seguridad en la capa de transporte (EAP-TTLS*)*. En un sistema EAP-TTLS, se autentica al usuario en el sistema con las credenciales basadas en nombre de usuario y contraseña y se cifran las credenciales de usuario para garantizar la protección de la comunicación inalámbrica.

A diferencia del anterior protocolo, EAP-TTLS soporta métodos adicionales de autenticación; aunado a esto, requiere de una gestión menor al requerir de certificados sólo en el servidor de autenticación RADIUS en lugar de configurar el certificado en cada una de las ET inalámbricas.

El proceso de autenticación a través de EAP-TTLS se realiza en dos etapas como se muestra en la Figura 3.11. En la primera fase, el usuario obtiene un canal de comunicación seguro denominado túnel TLS (no es necesario que el cliente se identifique) y en la segunda fase, las credenciales de autenticación cifradas son enviadas. Si las credenciales no son válidas el canal creado se destruye y se deniega el acceso a la red WLAN.

Una vez establecida la autenticación, el usuario vinculado al WLC obtiene a partir del servidor DHCP una dirección IP correspondiente a la red virtual de área local (VLAN) asociada y se le permite el tráfico a través del puerto preestablecido. Es importante

destacar, que el LAP no almacenará información para la autenticación del usuario, recuérdese que su función solo consiste en transmitir y recibir información.

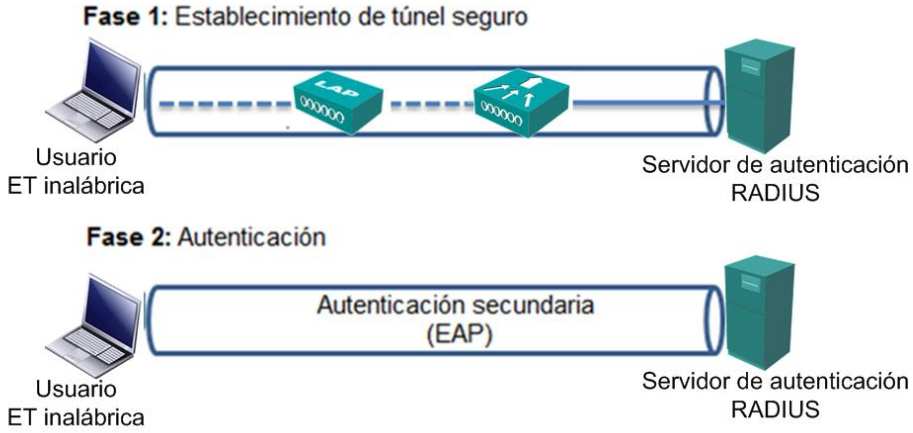


Figura 3.11 Autenticación EAP-TTLS

3.4.2.4 VLANS en redes WLAN

La función de una VLAN consiste en segmentar las redes de forma virtual. Los usuarios de una red se dividen en grupos lógicos; de esta forma, sólo los usuarios de un grupo específico pueden intercambiar datos o acceder a determinados recursos de la red. Esto permite a los administradores de la red WLAN implementar un grado más de seguridad en la red WLAN empresarial al mantener un control de los recursos.

El protocolo que se utiliza principalmente al configurar una VLAN es IEEE 802.1e, que etiqueta cada marco o paquete con bytes adicionales para indicar a qué red virtual pertenece. Aunado a ello, el empleo de VLANs permite implementar niveles de acceso a la red de acuerdo al perfil del usuario y al servicio al que desea acceder.

La tarea anterior es manejada a través del servidor de autenticación RADIUS de la siguiente manera (véase Figura 3.12); cuando un usuario inalámbrico intenta asociarse a un LAP, el LAP envía las credenciales del usuario al servidor RADIUS (solicitadas por el WLC) para su validación. Una vez que la asociación y autenticación es correcta, el

servidor RADIUS emplea atributos al usuario que le permiten decidir el ID de la VLAN que se le debe asignar al usuario.

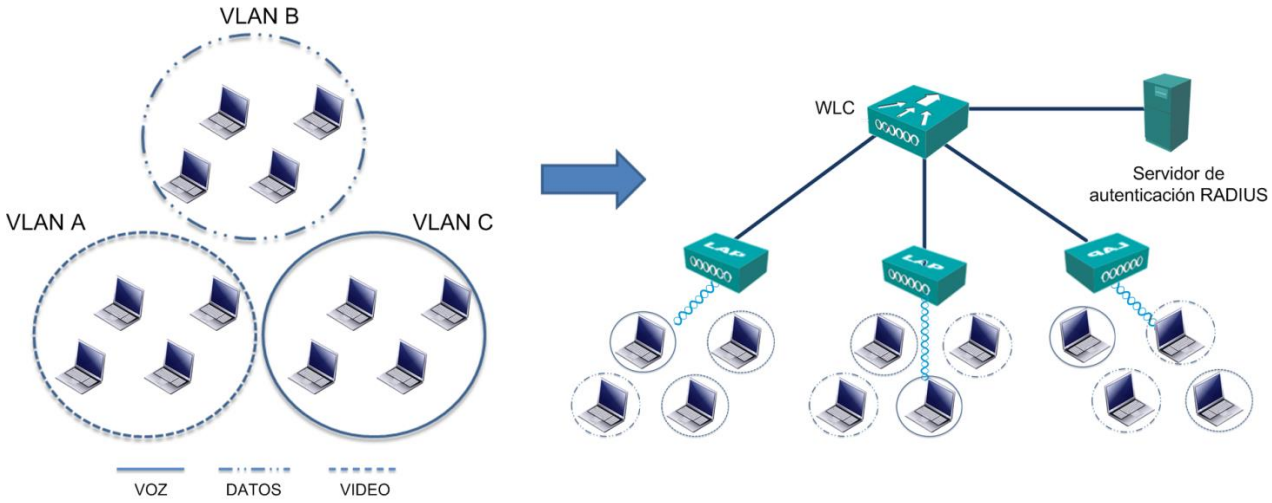


Figura 3.12 Arquitectura de configuración de VLANs

3.4.2.5 Protocolos de cifrado WEP, WPA y WPA2

En un sistema centralizado, como la red WLAN empresarial a implementar, la red inalámbrica suele ser menos vulnerable a ataques informáticos; sin embargo, no se prescinde de estos.

Como solución de la existencia de usuarios no deseados cuyo objetivo es robar la "información vulnerable" y hacer mal uso de esta, se encuentran presentes los protocolos de cifrado; los cuales, se encargan de codificar la información que fluye a través de la red de una forma segura.

De acuerdo con el estudio realizado por Cisco [1] y como se muestra en la Figura 3.13, el 97 % de las redes son protegidas por algún tipo de seguridad, de este porcentaje el 61 % de las redes son protegidas con un protocolo de cifrado como: WPA o WPA2 y el 19 % son protegidas por WEP.

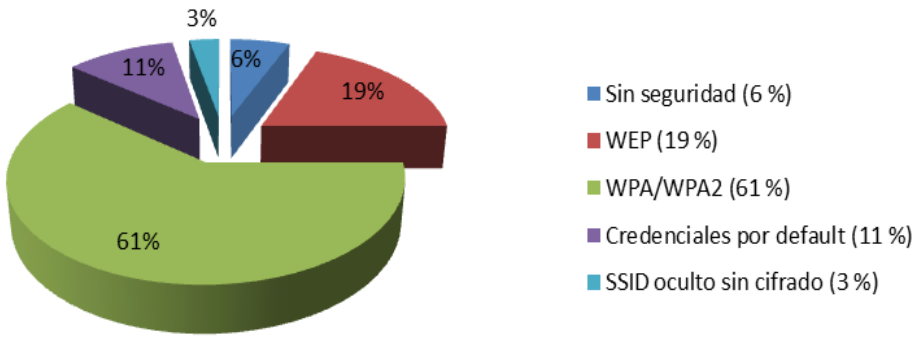


Figura 3.13 Protocolos de cifrado empleados en redes WLAN [1]

- **Protocolo WEP**

El protocolo de privacidad equivalente a cableado (WEP) [29] codifica los datos antes de que fluyan por la red mediante una "clave estática" a través de sus niveles de cifrado de 64, 128 y 256 bits (véase Tabla 3.7).

Tabla 3.7 Niveles de cifrado WEP

Nivel	Número de bits	Número de dígitos hexadecimales
Uno	64	10 dígitos hexadecimales "0 a 9" "A a F"
Dos	128	26 dígitos hexadecimales "0 a 9" "A a F"
Tres*	256	58 dígitos hexadecimales "0 a 9" "A a F"

NOTA: La mayoría de los equipos no soportan un nivel de cifrado WEP de 256 bits.

A medida que la clave tiene una mayor longitud de dígitos más robusto es el cifrado; más no significa que sea más seguro.

En la implementación del protocolo WEP en un sistema de red WLAN, los LAP difunden las redes creadas por los administradores de la misma red en el WLC; dichas redes, son configuradas manualmente con su respectiva clave, de tal forma que cuando un usuario desea conectarse a una red inalámbrica (con un SSID difundido) se le pedirá a éste la clave de la red a la que se desea conectar, misma que el administrador de la red implementó y proporcionó al usuario. Si la clave es correcta se inicia el cifrado de datos.

El protocolo WEP es el mecanismo de autenticación y cifrado más básico y fácil de implementar; sin embargo, también es el método más vulnerable, ya que al utilizar una

"clave estática", un atacante informático novato puede obtener la clave haciendo uso de su esfuerzo y tiempo. Dado que WEP ha sido comprobado como un "protocolo vulnerable" no se recomienda su implementación para una red WLAN segura [30].

- **Protocolos WPA y WPA2**

A diferencia del protocolo anterior, WPA o acceso Wi-Fi protegido, permite el cifrado de datos a través de una "clave dinámica o temporal"; esto es, que la clave preestablecida estáticamente se encuentra cambiando periódicamente lo que propicia que su obtención por un atacante sea más difícil. Un nivel de fortaleza que proporciona este protocolo es la colocación de claves alfanuméricas (con distinción entre mayúsculas y minúsculas) con uso de caracteres especiales, las cuales no tienen una restricción en su longitud.

La *Wi-Fi Alliance* propone dos tipos de protocolos de seguridad WPA para mejorar la calidad de autenticación:

- WPA
- WPA2

Éstos, se encuentran en dos modos: Personal y Empresarial (véase Tabla 3.8). Para objetivos de la Tesis, el tema se enfocará en los métodos WPA y WPA2 en su modo empresarial.

Tabla 3.8 Métodos de cifrado: WPA y WPA2

	WPA	WPA2
Modo personal	Autenticación: PSK Cifrado: TKIP/MIC	Autenticación: PSK Cifrado: AES-CCMP
Modo empresarial	Autenticación: IEEE 802.1x/EAP Cifrado: TKIP/MIC	**Autenticación: IEEE 802.1x/EAP** **Cifrado: AES-CCMP**

Fuente: Andreu, et. al., *Fundamentos y aplicaciones de seguridad WLAN,* Redes WLAN, Ediciones Técnicas Marcombo, p.57. Consultado en Google Books.

Una vez establecida la autenticación, WPA inicia el método de cifrado a través del protocolo de integridad de claves temporales (TKIP), el proceso se realiza mediante una "clave temporal raíz" de 128 bits la cual es compartida por un tiempo por la ET inalámbrica y el WLC. Posteriormente, esta clave se combina con la dirección MAC del dispositivo y se le añade un vector de inicialización (IV) de 16 bits para crear la "nueva clave" con la que se cifrarán los datos.

Aunado a lo anterior, se incorpora el control de integridad del mensaje (MIC) para prevenir que un atacante informático capture, altere y reenvíe los paquetes.

Con cada usuario utilizando WPA, por consecuencia, se tiene una clave única segura para el cifrado de datos.

A diferencia de WPA, WPA2 [32] emplea un algoritmo de cifrado más avanzado conocido como CCMP *(Counter Cipher Mode with Block Chaining Message Authentication Code Protocol).*

CCMP emplea el algoritmo del estándar de cifrado avanzado (AES). A diferencia de TKIP, la integridad de las claves son manejadas por un único componente creado alrededor de AES usando una clave de 128 bits y 10 rondas de codificación, proporcionando de ésta forma la seguridad de los datos para transmisión inalámbrica.

Las ventajas que WPA (en sus versiones) tiene sobre WEP son:

- Mayor nivel se seguridad.
- No es necesario cambiar con frecuencia la clave.
- No se tiene limitaciones en la longitud, caracteres, dígitos y símbolos para establecer una clave WPA y WPA2.
- La clave es dinámica lo que proporciona una mayor seguridad.

Las características que se definen para establecer WPA2 sobre WPA en una red WLAN empresarial son [31]:

- Requerimiento de menor de ancho de banda.

- Menor tiempo de procesamiento.
- Mecanismo de rápido *roaming.*

3.4.3 Control y protección de acceso a la red WLAN

El control y protección para acceder a una red WLAN es un enfoque de seguridad que implica prevenir ataques informáticos, reforzar las políticas de red y administración de los usuarios que intentan acceder a la red inalámbrica empresarial (véase Figura 3.14). La seguridad de la misma red comienza antes de que un usuario pueda acceder a esta.

- **NAC**

Cisco propone en su solución de control de admisión a la red (NAC), un registro de usuarios y protección contra amenazas de seguridad; ésta, utiliza la infraestructura de la red para hacer cumplir a los usuarios, que intentan acceder a la red, con las políticas de seguridad establecidas por la empresa.

NAC identifica, evalúa los dispositivos y determina si éstos cumplen con las políticas implementadas en la red; de no ser así, la solución permite reparar las vulnerabilidades en un estado de cuarentena, tal es el caso de la actualización de un antivirus, de tal forma que el dispositivo cumpla con las políticas de seguridad previamente establecidas.

Figura 3.14 Control y protección de admisión a la red WLAN

- **NAP**

Una herramienta muy útil para las redes empresariales es la protección de acceso a la red (NAP) de Microsoft, ésta permite identificar a los clientes y hacer que cada uno ellos tengan una política la cual permita cumplir con los lineamientos de la empresa; por ejemplo, las reglas de seguridad. Así, en el caso de que alguno de ellos no cumpla con dichas reglas, se le puede aislar y limitar para que cumpla con las normas de conexión.

Esta herramienta se define como una tecnología o arquitectura que permite controlar el acceso de los usuarios a la red, verificando con su identidad el cumplimiento de todas las políticas de seguridad establecidas por la empresa (véase Figura 3.15).

Su funcionamiento consiste en los siguientes pasos:

1. Un usuario se conecta a la red WLAN a través de un dispositivo móvil, cuya autenticación es válida.

2. El servidor de control de acceso (ACS) enviará una lista de *status* de las respuestas de salud (SoHs) al servidor de políticas de red (NPS), para validar a los usuarios. El NPS actúa como un servidor de evaluación de salud.

3. El NPS evaluará el SoHs en función a las políticas de seguridad establecidas y responderá al ACS a través de un *status* de validación de salud (HVS).

4. ACS evalúa los resultados obtenidos. En el caso de los usuarios que cumplen con las políticas empleadas preestablecidas, los dispositivos "*compliance"* podrán hacer uso de la red empresarial.

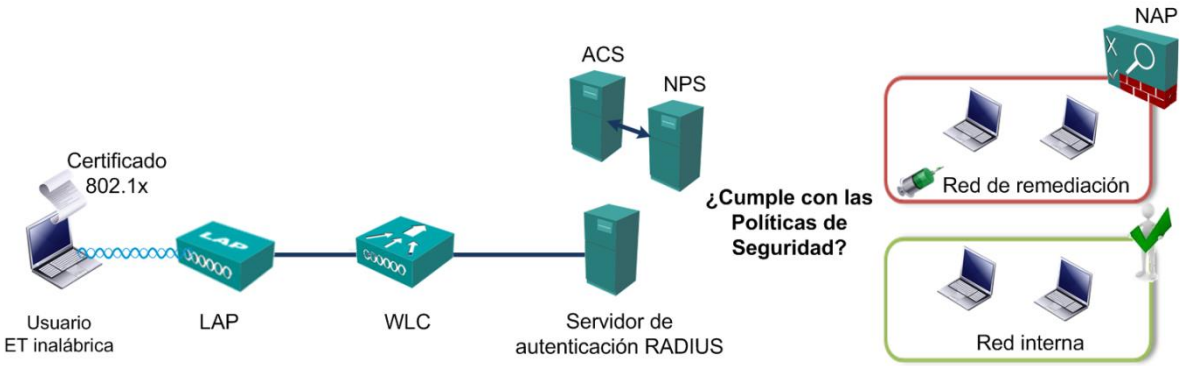


Figura 3.15 Integración de NAP en la arquitectura de red empresarial

5. Si el sistema de control NPS, encuentra que el equipo no cumple con las políticas de seguridad establecidas, sus credenciales no son aceptadas.

6. Al ser denegado el acceso *"non-compliance",* el sistema redirecciona la conexión a una red de remediación, la cual se encarga de corregir las vulnerabilidades encontradas por las cuales el sistema rechazó las credenciales.

3.4.4 Detección y protección de intrusos

El sistema inalámbrico de protección contra intrusos (WIPS) es una herramienta corporativa que proporciona a los administradores de la red WLAN la capacidad de detectar, analizar e identificar las amenazas inalámbricas y gestionar de forma centralizada la mitigación y solución de los problemas de seguridad y rendimiento.

Los componentes con los que cuenta WIPS son configurados de la siguiente manera para lograr que cumplan con su función:

- **Sensores.** Son dispositivos que contienen antenas y radios que exploran el espectro inalámbrico y se instalan a lo largo de zonas que deben protegerse. En el caso de un sistema centralizado, regularmente son los mismos LAP que conforman la infraestructura.

- **Servidor.** El servidor WIPS central analiza los paquetes capturados por los sensores y correlaciona la información que valida contra las políticas definidas por la empresa y clasifica si se trata de una amenaza.

- **Consola.** Proporciona la interfaz de usuario principal en el sistema de administración y presentación de informes, en el caso de una amenaza se notifica de ésta y WIPS toma medidas de protección automática.

En conjunto la integración de una herramienta como WIPS en la infraestructura WLAN permite a los administradores de la red empresarial:

- **Detectar y mitigar puntos de acceso.** WIPS detecta y mitiga los AP no autorizados que intenten acceder a la red con el fin de hacer uso indebido de los recursos corporativos.

- **Detectar ataques cibernéticos.** Analiza el comportamiento del tráfico y realiza la coincidencia de patrones y técnicas considerados como formas de ataques cibernéticos. WIPS envía alertas con la información de posibles ataques a la red WLAN y muestra a través de su consola de administración el lugar geográfico donde se encuentra ubicado el dispositivo no autorizado.

- **Monitorear el rendimiento y optimización.** El bajo rendimiento en la red WLAN afecta su disponibilidad, por lo que WIPS proporciona información sobre el ruido y las interferencias, así como la potencia de la señal de los usuarios, entre otros datos, lo que se utiliza para asignar dinámicamente canales y ajustar la potencia de transmisión en tiempo real del LAP para evitar la interferencia entre canales y minimizar los agujeros de cobertura.

- **Seguimiento y generación de informes**. Todo el tráfico asociado con un ataque es capturado. WIPS, realiza informes de acerca de los posibles ataques para dar un seguimiento de análisis y posibles vulnerabilidades en la red WLAN.

3.4.5 Aplicaciones de seguridad

Cuando se habla de seguridad, es preciso contar con las herramientas que proporcionen la seguridad interna y externa de la red WLAN. La implementación del *firewall* permite establecer una barrera contra las amenazas y ataques informáticos. Su implementación y funcionamiento permite controlar el tráfico de entrada y salida que fluye entre dos o más redes, ayudando a prevenir el acceso de tráfico no autorizado.

Dependiendo de las políticas de seguridad que se deseen implementar existen diferentes técnicas que permiten administrar el tráfico que se desea admitir o denegar en la red corporativa.

3.4.5.1 Tipos de filtrado

De acuerdo al tipo de filtrado (véase Tabla 3.9) se encuentran las características que permiten la posibilidad de evitar o permitir el acceso a la red.

Además de proporcionar una administración con uno o más de un tipo de filtrado, el *firewall*, puede llevar a cabo la traducción de direcciones de red (NAT); es decir, la dirección interna o un grupo de direcciones se traducen en direcciones públicas externas las cuales se envían a través de la red, lo que permite ocultar las direcciones internas que pertenecen a la red corporativa de usuarios que son externos.

Tabla 3.9 Tipos de filtrado

Tipo de filtrado	Característica
Filtrado de paquetes	Direcciones IP o MAC.
Filtrado de aplicaciones	Números de puerto.
Filtrado URL	Sitios Web de acuerdo al URL o palabras clave específicas.
Inspección de estado de paquetes (SPI)	Los paquetes entrantes deben ser respuestas legítimas de los *hosts* internos. Los paquetes no solicitados son bloqueados, a menos que se permitan específicamente.

3.4.5.2 Zona desmilitarizada

Un *firewall* permite controlar y administrar el tráfico de entrada y salida de la red corporativa, lo que crea una línea de defensa entre la red interna y la red externa (*Internet*), este esquema es útil en el sentido que solamente los usuarios que son internos desean acceder a los recursos de la red interna; sin embargo, las nuevas tendencias inalámbricas solicitan acceso a usuarios invitados que quieren acceder a los recursos de la red o simplemente consultar Internet, por lo que es preciso la configuración de una zona desmilitarizada (DMZ) para lograrlo.

Una DMZ es un área de la red que es accesible tanto para los usuarios internos como usuarios invitados, es más segura que la red externa pero menos segura que la red interna. Su configuración está constituida por uno o dos *firewall* en donde se colocan servidores HTTP (protocolo de transferencia de hipertexto); la configuración de un único *firewall* es apropiada para redes que no son tan congestionadas así como para redes pequeñas, sin embargo, para una red más compleja y con una demanda mayor de tráfico como lo es la red empresarial, es adecuado la utilización de dos *firewalls*. [33]

- **Firewall único**

Un firewall único tiene tres áreas, una para la red externa, una para la red interna y otra para la DMZ. Desde la red externa se envía todo el tráfico al firewall. A continuación, se requiere el *firewall* para supervisar el tráfico y determinar qué tráfico debe pasar a la DMZ, qué tráfico debe pasar internamente y qué tráfico debe denegarse por completo (véase Figura 3.16).

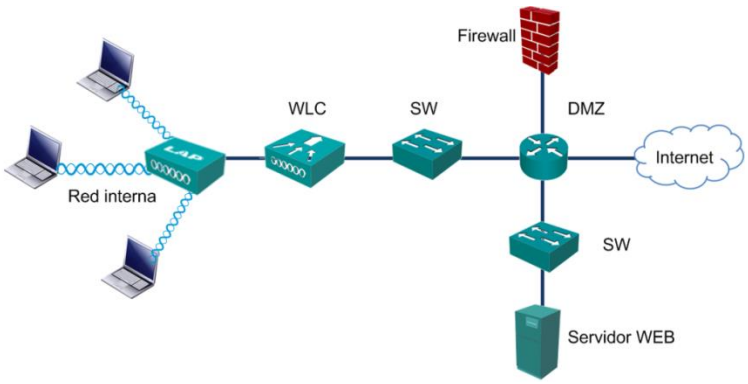


Figura 3.16 Configuración de Firewall único

- **Dos firewalls**

En una configuración de dos *firewall* hay un *firewall* interno y uno externo, con una DMZ ubicada entre ellos (véase Figura 3.17). El *firewall* externo es menos restrictivo y permite al usuario de Internet acceder a los servicios en la DMZ; además, concede al usuario externo cualquier solicitud de atravesar el tráfico. El firewall interno es más restrictivo y protege la red interna contra el acceso no autorizado.

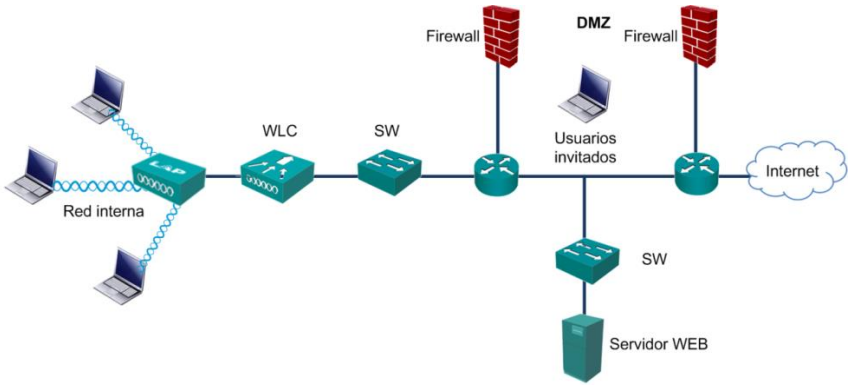


Figura 3.17 Configuración de dos firewall

3.5 Movilidad en redes WLAN

La movilidad en redes WLAN de acuerdo al RFC 2002 *"IP Mobility Support"* [34] emitido por la IETF, es la capacidad que tiene un dispositivo móvil para desplazarse de un lugar a otro. En la presente tesis, movilidad *(roaming)* en la red WLAN empresarial, se referirá a la capacidad de una ET inalámbrica para moverse entre los LAP que integran la red WLAN.

La característica de movilidad en una red empresarial, permite a los usuarios desplazarse de su sitio de trabajo a otro, lo que permite tener una mayor cobertura laboral.

En redes WLAN, se tienen dos casos de movilidad:

- El primer caso consiste en un usuario que desea realizar movilidad de un LAP a otro LAP que se encuentran asociados a un WLC o bien cuando un usuario desea realizar movilidad entre dos LAP que se encuentran asociados a diferentes WLC pero en la misma subred y grupo de movilidad. A lo anterior se le determinará como movilidad en Capa 2.

- El segundo caso corresponde a un usuario que desea moverse entre dos dominios; por ejemplo, el usuario desea establecer comunicación de un LAP que se encuentra en una subred A y después trasladarse a un LAP que se encuentra en una subred B. Lo anterior será referido a movilidad en Capa 3.

El tiempo en que tarda en completarse un proceso de movilidad será denominado como *handover*, dicho proceso en ambos casos planteados, es dependiente de ciertos factores como el proceso de asociación y autenticación en IEEE 802.1x.

En los siguientes temas, se describirán los dos modelos de movilidad y las características que lo constituyen.

3.5.1 Movilidad en Capa 2

El proceso de movilidad en Capa 2, puede definirse a través de los siguientes puntos:

- **Inicio de movilidad**

El mecanismo de inicio de movilidad no se encuentra definido por la IEEE 802.11, por lo que cada fabricante diseña el algoritmo de decisión de movilidad según su criterio con los parámetros que estima convenientes; por ejemplo, cuando la ET inalámbrica se encuentra en los límites del rango de alcance del LAP de origen se establece un mecanismo de movilidad.

- **Descubrimiento de LAP**

El descubrimiento de un LAP al cual asociarse para establecer un proceso de movilidad; éste también se encuentra establecido por el fabricante. Este mecanismo consiste en una exploración del medio (activa o pasiva) para establecer contacto con los LAP (a través del WLC) con los que podría establecer una comunicación

La exploración activa, consiste en una exploración del medio a través de la ET inalámbrica, la cual enviará solicitudes (en cada canal de RF en el que se encuentre configurado) hacia los LAP, esperando una respuesta (durante un lapso de 10 a 20 ms) del WLC y tomando una decisión de cuál LAP es la mejor decisión para comenzar un mecanismo de movilidad.

La exploración pasiva, por otro lado, se define por la no transmisión de tramas, este mecanismo se encarga de que la ET inalámbrica escuche las tramas de señalización que se envían desde cada LAP en cada canal de RF. A través de este mecanismo se trata de encontrar los datos (SSID, la tasa de transferencia, etc.) que ayuden a determinar el LAP a través del cual iniciar un mecanismo de movilidad.

- **Realizar movilidad**

Una vez que se ha definido el LAP en el cual se va a iniciar el mecanismo de movilidad, da comienzo el proceso de movilidad de Capa 2 el cual consiste en los siguientes pasos.

1. El LAP1 determina que probablemente la ET inalámbrica iniciará un proceso de movilidad ya que se encuentra en los límites de cobertura.

2. El LAP comienza a almacenar en un *buffer* los datos destinados del usuario.

3. El LAP1 indica al LAP2 el traslado de la ET inalámbrica hacia su nuevo origen. A través de un paquete *unicast*[27] o *multicast*[28], El LAP1 envía la dirección MAC a su nuevo destino.

4. EL LAP1 envía la información almacenada en el *buffer* hacia el LAP2.

5. Ambos extremos deben actualizar su tabla de direcciones MAC para evitar la pérdida de datos.

NOTA: Recuerde que cuando se habla de procesos en los LAP, éstos se hacen a través del WLC.

3.5.2 Movilidad en Capa 3

La movilidad en Capa 3, corresponde al desplazamiento de una ET inalámbrica entre dos o más diferentes BSS; es decir, tener movilidad en un área ESS. Al igual que en movilidad

[27] *Unicast,* es el envío de información desde un único emisor a un único receptor.
[28] *Multicast,* es el envío de la información en una red a múltiples destinos simultáneamente.

de Capa 2 los parámetros para realizar el mecanismo de movilidad en Capa 3, están definidos por el RFC 2002.

Aunado a las características que anteriormente se mencionaron para movilidad en Capa 2, el mecanismo de movilidad en Capa 3 dispone de nuevos conceptos como se detalla a continuación:

- **Nodo móvil (MN).** MN será referido a la ET inalámbrica que desea realizar un mecanismo de movilidad.

- **Agente regional o doméstico (HA).** Existe en los *switch* de Capa 3, es el encargado de que la ET inalámbrica reciba los paquetes de datos mientras se encuentra en un mecanismo de movilidad.

- **Agente foráneo (FA).** Existe en los *switch* de Capa 3. FA notifica al HA la nueva ubicación de la ET inalámbrica cuyo propósito es la recepción de paquetes desde el HA al MN.

- **Dirección de auxilio (CoA).** Un *router* conectado a nivel local, proporciona a un MN una dirección IP temporal denominada CoA. Esto permite que un HA pueda reenviar mensajes al MN.

A través de la Figura 3.18, se expone el proceso que ejecuta el mecanismo de movilidad en Capa 3:

1. Un MN pertenece a HA si su dirección IP (dirección inicial) pertenece a la misma subred.

2. Cuando MN comienza un mecanismo de movilidad hacia otra subred, el MN se registra con el FA.

3. El FA se comunica con el HA y se establece un túnel entre estos dos para enviar la información al MN .

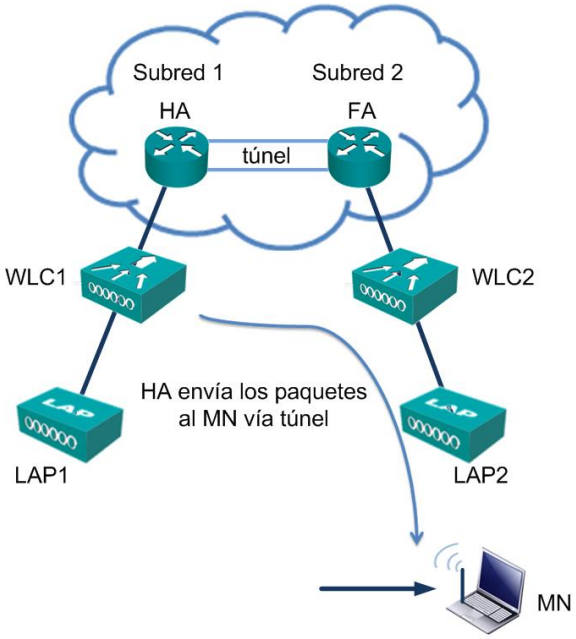


Figura 3.18 Movilidad en Capa 3

4. Cuando un nodo se quiere comunicar con un MN, los paquetes destinados al MN se envían al HA a través de un enrutamiento IP usando la dirección inicial.

5. Estos paquetes son interceptados por el HA, dónde se encapsula la dirección IP inicial y es colocada una dirección IP CoA.

6. Posteriormente, los paquetes son desencapsulados en el extremo final del túnel para eliminar la dirección IP CoA añadida y de esta forma los paquetes son entregados al MN.

3.5.3 Rápida movilidad

Una de las consideraciones que se debe tener en cuenta en el mecanismo de movilidad es la reautenticación. Recuerde que un usuario puede acceder a la red hasta que se ha

autenticado y asociado a través de un servidor de autenticación RADIUS utilizando IEEE 802.1x.

Una vez que el usuario ha decido cambiar de LAP, la ET inalámbrica debe ser autenticada en el nuevo LAP a través del WLC, lo que en un mecanismo de movilidad se identifica como una interrupción de conectividad con la red WLAN debido al tiempo que debe emplearse para realizar la reautenticación.

Para evitar el anterior problema, se puede emplear mecanismos de rápida movilidad (*fast roaming)* a través del estándar IEEE 802.11r-2008 [35] o rápida transición BSS. Éste estándar basa su solución de rápida reautenticación al permitir que la clave o llave de sesión, sea almacenada en *caché* en la red WLAN.

Lo anterior se realza a través del protocolo de cifrado WPA2, el cual soporta el almacenamiento en caché de la llave y autenticación previa. Su proceso permite que el usuario de la ET inalámbrica y el WLC almacene en su memoria caché los resultados obtenidos de la autenticación 802.1x; por lo que al realizar movilidad en la red el proceso de autenticación sólo consistirá en el empleo de una negociación de *handshake* [30], véase Figura 3.19.

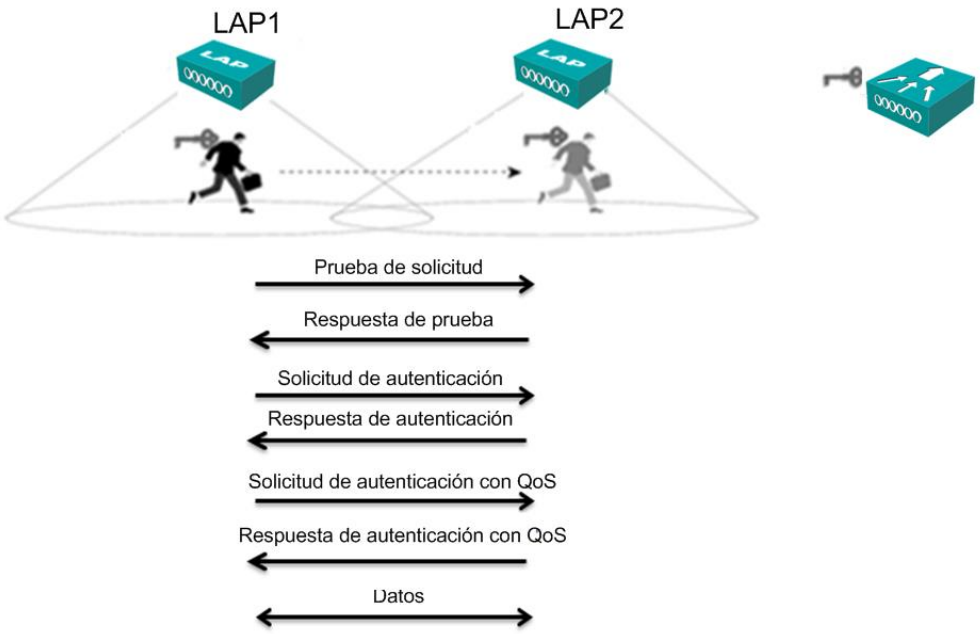


Figura 3.19 IEEE 802.11r-2008. Rápida movilidad

Originalmente el estándar IEEE 802.11 establece que un proceso de movilidad entre una ET inalámbrica y un AP puede tomar por lo menos más de 100 milisegundos. IEEE 802.11r permite que la transición entre los AP tenga una latencia de menos de 50 milisegundos. En una comunicación VoIP el tiempo necesario para mantener una conversación sin cortes de comunicación perceptible es no más de 100 milisegundos. [36]

Capítulo 4

TENDENCIAS Y SOLUCIONES PARA LA NUEVA GENERACIÓN DE RED WLAN 802.11 EMPRESARIAL

La cooperación entre grupos de trabajo para la realización de proyectos y la necesidad de acceder a los recursos de la red inalámbrica a través de los diferentes dispositivos móviles, que hoy en día se encuentran en uso, permite el establecimiento de las nuevas tendencias inalámbricas para la colaboración empresarial.

El empleo de dispositivos móviles, conocido como BYOD, y el acceso a la red WLAN empresarial a través de estos, implica hoy en día un correcto diseño de la red inalámbrica para mantener una eficiente administración y seguridad en la red, con esto se tiene como objetivo la integración de las nuevas tendencias inalámbricas para la última generación de redes WLAN empresariales. Estas nuevas tendencias permitirán tanto a empleados como usuarios invitados tener una nueva experiencia laboral.

Una vez que se ha llegado a este capítulo, ya se cuenta con la información de seguridad que una red WLAN debe tener para salvaguardar la integridad de la empresa, ahora es tiempo de preparar la red inalámbrica para las demandas de tecnología inalámbrica.

En este capítulo se describirán las tendencias inalámbricas existentes para la creación de una red WLAN empresarial; aunado a lo anterior se realiza un análisis de las soluciones existentes en el mercado para la integración de la tendencia de usuarios invitados y el planteamiento de incorporación de la tendencia BYOD.

Rapidez, seguridad, calidad, disponibilidad, movilidad, colaboración, etc. integran las características de un nuevo entorno de redes WLAN empresarial.

4.1 Evolución de las redes WLAN empresarial

La evolución hacia la movilidad es una tendencia básica de la red WLAN corporativa que permite a las empresas impulsar la productividad de sus trabajadores y al mismo tiempo, reducir costos. El cambio de la infraestructura de la red corporativa para lograr movilidad, es un paso que debido a diversos factores, como la seguridad, muy pocas empresas mexicanas han realizado; sin embargo, el conjunto de nuevas tendencias y la demanda de la integración de dispositivos móviles en redes WLAN empresariales requieren de este cambio.

Un panorama de la evolución de las redes WLAN, como se señala a continuación y se ejemplifica en la Figura 4.1, muestra la inminente necesidad de establecer una nueva generación para las redes WLAN empresariales [37, 38].

- **Primera generación WLAN.** Implementación de una red *Ad-Hoc*. Esta primera generación permitió observar los beneficios de utilizar la tecnología inalámbrica, cuya función principal consistió en una primera fase de movilidad al usuario y la evolución de las redes LAN.

- **Segunda generación WLAN.** Como toda tecnología, comenzó a ampliarse el mercado y por consiguiente el nivel de usuarios que demandaban de una conexión inalámbrica aumentó, lo que propició el establecimiento de decenas e incluso cientos de AP para lograr dar servicio a todos los usuarios. El establecimiento de los AP demandaba una gestión descentralizada por lo que la administración de la red, así como su mantenimiento, trajo consigo una red propensa a errores, ya que cada AP no formaba parte de un sistema, es decir, estaba aislado.

- **Tercera generación WLAN.** La introducción de *switches* y *routers* en la red WLAN corporativa se introdujo como un camino para la gestión de la red inalámbrica desde un punto central de control. En este modelo centralizado los LAP forman parte de un sistema dirigido por un controlador (WLC); este ha sido el modelo de implementación predominante durante los últimos años y en conjunto con la red LAN, aún existente, se crea un sistema unificado, por lo que las políticas de seguridad y la gestión de tráfico son implementadas a partir de un controlador centralizado.

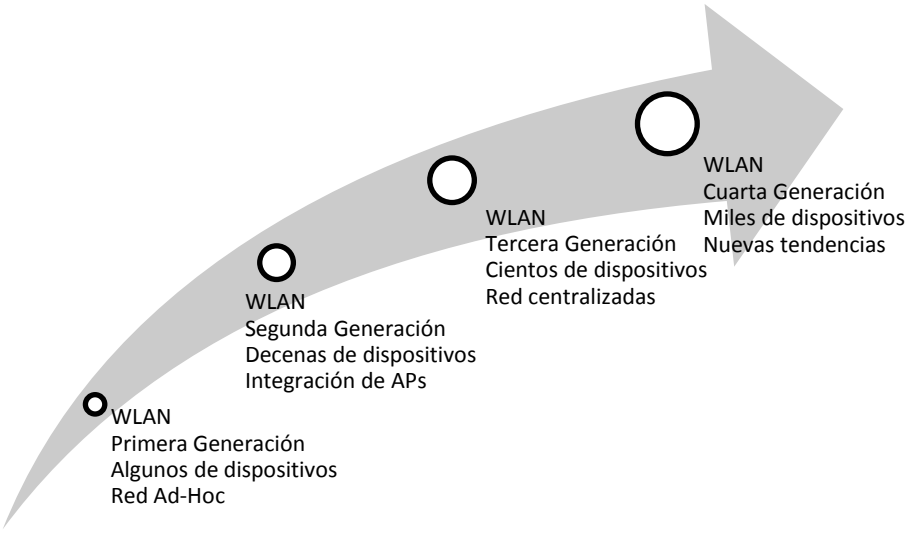


Figura 4.1 Evolución de las redes WLAN

El integrar una red WLAN a un sistema centralizado trajo consigo grandes beneficios para los administradores de TI, logrando a partir de éste, tener un mayor control sobre la red inalámbrica. Debido a que las redes WLAN aún siguen evolucionando y su demanda aumenta considerablemente, la tercera generación de redes WLAN se encuentran con las siguientes limitaciones:

- Gran cantidad de tráfico en la red.
- Limitación en el escalamiento de la red.
- Rendimiento bajo en zonas con más usuarios.
- Baja calidad de servicio bajo.
- Aumento de dispositivos móviles no registrados en la red inalámbrica.

Las anteriores características promueven a una nueva generación de redes WLAN que permita mitigar las anteriores limitaciones, cumplir con la demanda de dispositivos móviles y ofrecer a los usuarios el acceso a los servicios que requieren.

- **Cuarta generación WLAN.** La nueva generación de redes empresariales WLAN IEEE 802.11, debe hacer frente a un nuevo enfoque, una nueva experiencia de

trabajo y colaboración dentro de la empresa. Las características que integran a una red WLAN empresarial de cuarta generación se enlistan a continuación.

- Acceso a la red WLAN a una cantidad de usuarios considerable.
- Red WLAN siempre disponible.
- Calidad de servicio y prioridad de tráfico.
- Gestión de una alta densidad de usuarios inalámbricos.
- Integración de las nuevas tendencias inalámbricas empresariales.
- Mecanismos de seguridad avanzados.
- Gestión y control centralizados.
- Tener usuarios invitados que utilicen la red WLAN corporativa.
- Menor costo de administración que las redes convencionales.

En conjunto con las consideraciones para la integración de una red WLAN corporativa segura (como se vio en el Capítulo 3) y las nuevas tendencias de movilidad, es posible lograr la integración de una red WLAN empresarial de cuarta generación.

Para una red WLAN empresarial de cuarta generación, se despliegan principalmente dos tendencias: la primera, que el usuario pueda tener acceso a los recursos de la red inalámbrica corporativa en cualquier lugar de la empresa y en cualquier momento a través de su dispositivo móvil; y la segunda, una red WLAN que le permita a los "usuarios invitados"[29] tener acceso a Internet a través de la red inalámbrica de la empresa sin ser una amenaza a la red WLAN interna. Esto es en resumen las tendencias BYOD *(Bring Your Own Device)* y Acceso a Usuarios Invitados (*Guest Access Users)*.

[29] Este concepto será definido como un usuario que no trabaja en la empresa; sin embargo, desea acceder a Internet a través de la infraestructura de la red WLAN empresarial.

4.2 BYOD

La gran cantidad de usuarios que tratan de ingresar a la red WLAN empresarial a través de sus dispositivos móviles, en cualquier sector de desarrollo, constituye un reto para los administradores de la red, cuyo objetivo es evitar centralizar los recursos por parte de los usuarios y obtener el control de flujo del tráfico en la red WLAN, así como la identificación de los usuarios que ingresan a través de sus dispositivos móviles sin la intervención de soporte técnico.

BYOD define su tendencia empresarial en el hecho de que hoy en día los empleados traen consigo al lugar de trabajo sus propios dispositivos móviles personales (tales como *smartphones*, *tablets*, *laptops*, etc.) para hacer uso de los recursos de la red WLAN empresarial, lo que provoca un alto impacto en el ancho de banda de la red inalámbrica y en la seguridad de la empresa.

Como se mencionó anteriormente, una de las debilidades de las redes WLAN de tercera generación es el aumento de tráfico en la red corporativa; por lo que ahora, corresponde al desarrollo de las redes WLAN empresariales que puedan manejar de manera eficiente un ancho de banda dedicado y un número cada vez mayor de usuarios accediendo a la red inalámbrica a través de sus dispositivos móviles. BYOD describe la integración de su tendencia como una red convergente de última generación, especialmente que puede unificar el tráfico IEEE 802.11 y gestionar las políticas de los dispositivos móviles.

Al habilitar BYOD no solo se habla de dar acceso a la red WLAN, esta tendencia también requiere de políticas, seguridad y la capacidad de red inalámbrica que ayuda a los usuarios a obtener el máximo provecho de las aplicaciones y servicios a las que acceden a través de sus dispositivos móviles que llevan al lugar de trabajo. Las soluciones de movilidad BYOD deben ofrecer un control sobre la seguridad de datos corporativos y proporcionar una nueva experiencia de trabajo a los empleados y usuarios externos para fomentar la productividad.

4.2.1 Seguridad y administración BYOD

La integración de BYOD en la empresa implica, por parte de los administradores de la red inalámbrica, una minuciosa incorporación de estrictas políticas que establezcan los requisitos de acceso y seguridad de la red inalámbrica, generalmente a través de perfiles; además, se recomienda un panorama de administración gráfico y tabular que permita la gestión de dispositivos móviles que accedan a la red WLAN empresarial y un soporte técnico mínimo.

En conjunto (véase Figura 4.2), se identifican los siguientes requisitos de seguridad en la integración de BYOD:

- **Transmisión segura de datos.** El cifrado directamente desde el dispositivo a la infraestructura de la red, permite a las compañías compartir sus datos más sensibles a los usuarios de ET móviles.

Figura 4.2 Seguridad y administración BYOD

- **Protección del equipo.** Una capa adicional de seguridad a nivel de dispositivo (para equipos inalámbricos corporativos y propiedad de los empleados) es

fundamental para la protección de los datos confidenciales de la empresa. La gestión de dispositivos móviles permite a los administradores de la red denegar el acceso y borrar de forma remota los datos de dispositivos perdidos o robados.

- **Acceso a la red corporativa y servicios.** BYOD requiere de los departamentos de TI para ofrecer el nivel adecuado de acceso a la red WLAN corporativa, en función del perfil del usuario y el dispositivo. Los usuarios deben ser capaces de acceder a las herramientas, datos y servicios que proporciona la empresa de una forma rápida y sencilla.

4.2.2 Esquema general de BYOD en la integración de políticas

Es importante tomar en cuenta que al realizar la integración de la tendencia BYOD, la red WLAN debe estar sujeta a la seguridad que constituye una red empresarial WLAN 802.11. El primer paso en la incorporación de un esquema BYOD es la determinación del tipo de usuarios (véase Tabla 4.1) que constituirán en forma general a la red inalámbrica ya que la tendencia BYOD implementa sus políticas de seguridad de acuerdo al perfil de los usuarios que ingresan a la red WLAN empresarial.

Tabla 4.1 Tipos de usuarios o perfiles

Tipo de usuario	Permiso	Acceso
BYOD	Red Interna	Acceso total o parcial a los datos de la empresa.
	Servicios Red Interna	Acceso restringido, solo puede acceder a recursos específicos de la red Interna.
Guest	Internet (sugerido)	Acceso únicamente a Internet.
Otro	Denegado	No cumple con las características de autenticación por lo que su acceso es denegado.

De acuerdo a la clasificación de usuarios, a continuación se mencionan dos casos típicos de políticas que una empresa puede aplicar [39].

- **Acceso mejorado**

Este caso se centra en proporcionar diferentes niveles de acceso de acuerdo a las credenciales del dispositivo. Los usuarios que obtienen un certificado y han sido dados de alta a través de un portal de registro tienen acceso a la red basado en el tipo de usuario AD.

- **Acceso completo.** Si el usuario pertenece al grupo de AD Acceso_BYOD.
- **Acceso parcial.** Si el empleado pertenece al grupo Usuarios de dominio AD.
- **Acceso a Internet.** Si el empleado pertenece al grupo de AD Acceso_Internet.

BYOD proporciona la capacidad de identificar el tipo de dispositivo y la prevención de estos dispositivos de conexión a la red.

En la Figura 4.3 se muestra un diagrama de flujo del acceso al nivel de red WLAN de acuerdo al perfil del usuario y del grupo dentro del AD al que pertenece.

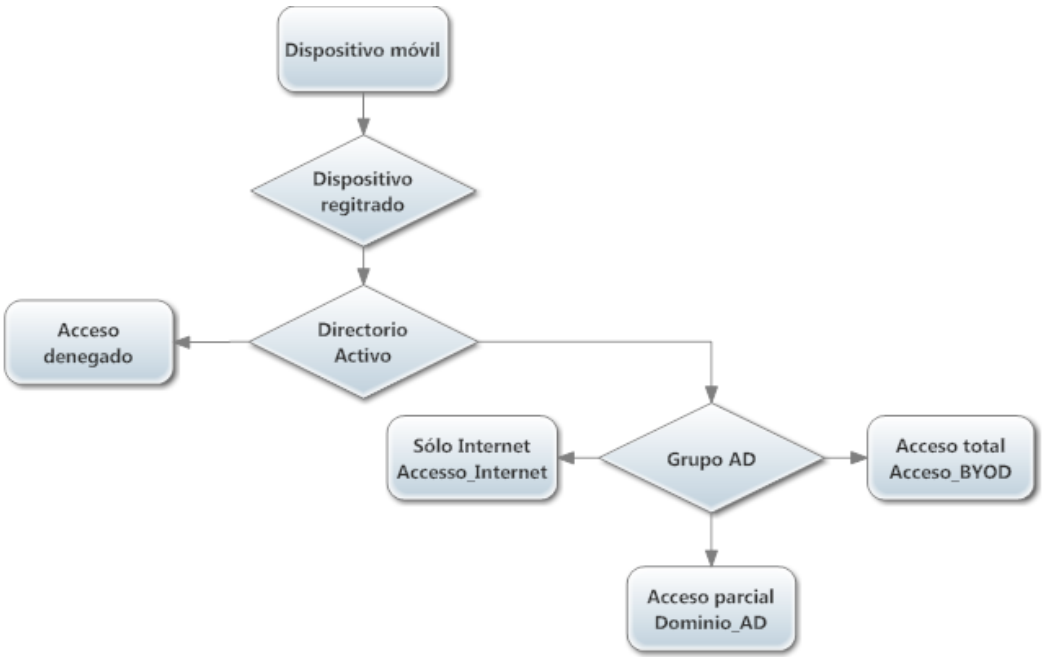


Figura 4.3 Acceso a la red WLAN (BYOD)

- **Acceso limitado**

Este segundo caso, permite gestionar la red WLAN para el acceso de dispositivos BYOD a través de un conjunto de políticas más restrictivas, donde solamente los dispositivos que pertenecen y son gestionados por la empresa puede acceder a los recursos internos de la red inalámbrica y se niega el acceso a cualquier otro dispositivo móvil personal de cualquier usuario no gestionado.

De acuerdo con el perfil y el certificado de autenticación con el que cuentan los dispositivos BYOD (véase Figura 4.4), el usuario tiene acceso a la red interna de la empresa. En este caso se introduce una lista blanca con los datos de los dispositivos inalámbricos que podrán tener acceso.

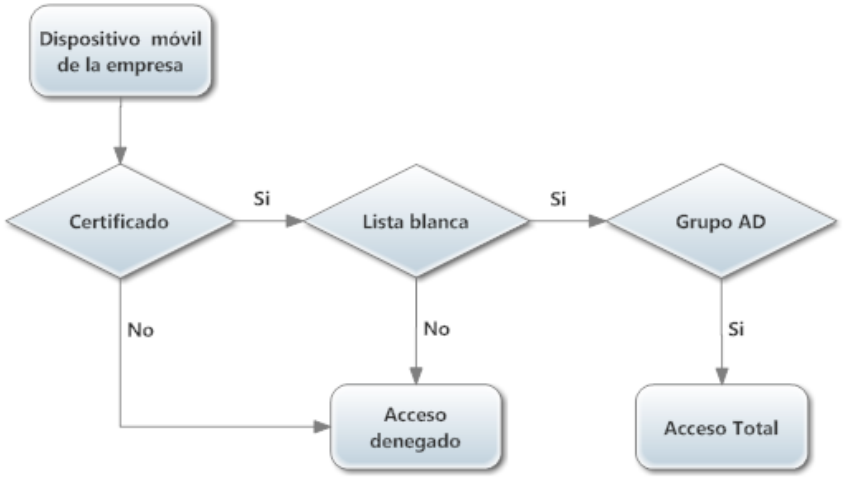


Figura 4.4 Acceso limitado de dispositivos BYOD

4.2.3 Beneficios BYOD

De acuerdo al estudio realizado por Cisco [40], los líderes de TI identificaron tres beneficios que reciben las empresas al integrar esta tendencia.

- **Productividad.** La principal ventaja en la utilización de BYOD es el aumento en la productividad de los empleados ya que existe un mayor rendimiento y colaboración con los demás usuarios al realizar proyectos en conjunto.

- **Satisfacción laboral.** Los empleados quieren generalmente, utilizar los mismos dispositivos para el trabajo que los que usan en sus vidas personales. Cuando se les permite elegir sus propios dispositivos móviles, los empleados se encuentran generalmente más satisfechos en su trabajo.

- **Reducción de costos.** Debido a que los empleados pagan una parte (o la totalidad) de los costos de sus dispositivos móviles, los costos por implementación de dispositivos inalámbricos de trabajo se convierte en el tercer beneficio para la empresa.

4.2.4 Consideraciones BYOD

La nueva tendencia BYOD da un panorama de integración móvil para las redes WLAN empresariales de última generación; sin embargo, su completa adopción se encuentra obstaculizada por la seguridad y las opiniones por parte de expertos de TI para hacer cumplir las reglas establecidas para los usuarios.

La primera consideración que se debe tener en cuenta es la inminente adopción de una clara **política de movilidad** que incluya la tendencia BYOD, esto con el fin de mantener un equilibrio entre la seguridad de la empresa y la seguridad de los usuarios.

La introducción de gestión de dispositivos móviles dentro de ésta política de seguridad permite a los administradores de TI controlar, gestionar y dar soporte técnico a los dispositivos móviles personales.

Aunado a lo anterior, la segunda consideración que se debe tomar en cuenta es la cantidad de usuarios que se desean integrar a través de esta tendencia, ya que su incorporación requiere de un amplio apoyo de soporte técnico lo que generaría un aumento en el tiempo de administración y recursos por parte del área de TI; es por ello, que deben establecerse manuales genéricos para el apoyo al usuario autodidacta y en caso de ser estrictamente necesario, establecer una asesoría personal.

La investigación *"Mobile Consumerization Trends & Perceptions"* [41] afirma que el 46.7 % de las empresas (en los países globalizados del estudio) que han integrado la tendencia BYOD han presentado a través de sus usuarios una brecha en sus datos (fuga de datos) (véase Figura 4.5). Como solución a ello, las empresas en un 45 % han creado restricciones de acceso a la información, mientras que un 43 % opta por instalar un software de seguridad y un 12 % revoca todos los privilegios que BYOD proporciona a los usuarios, ya que mencionan que dicha brecha puede perdurar si no se toman las medidas de seguridad correspondientes.

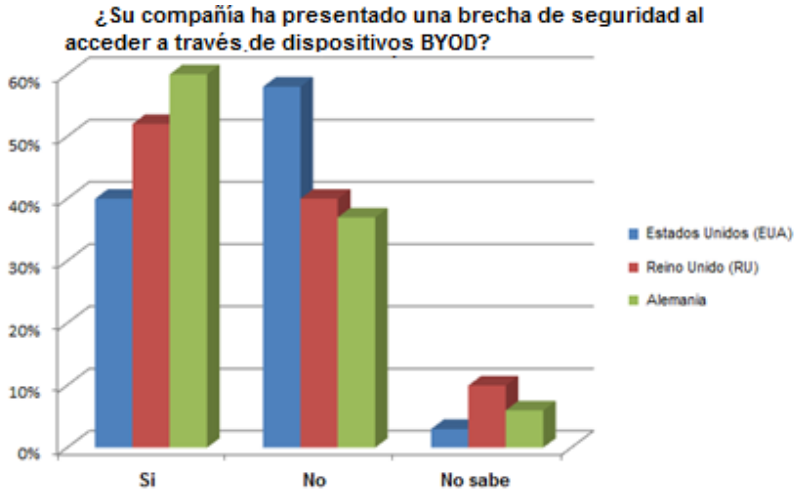


Figura 4.5 Estudio de seguridad BYOD [41]

4.3 Acceso a Usuarios Invitados

El paradigma de colaboración laboral y acceso a usuarios invitados a la red WLAN, coloca al esquema de la red corporativa en un punto crucial, en el que la empresa debe crear un entorno productivo entre sus contratistas, socios y visitantes, y al mismo tiempo, mantener la seguridad de sus usuarios internos y la información contenida en la misma red inalámbrica.

Guest Access Users o Acceso a Usuarios Invitados, es la segunda tendencia para redes WLAN empresariales de última generación para la integración de colaboración

corporativa. Con esta tendencia, los usuarios invitados se les proporcionan acceso a Internet siempre y cuando se encuentren en el rango de cobertura de la red inalámbrica, pero nunca se les da acceso a la red WLAN interna.

El objetivo a lograr con esta tendencia es la seguridad basada en el tipo de usuario que accede a la red WLAN, cumpliendo con este objetivo a través de la separación entre el tráfico interno de la red inalámbrica y el tráfico de usuarios invitados. Dado que el acceso a la red se crea a partir de la misma red WLAN empresarial es indispensable la seguridad de los datos corporativos y la seguridad de la misma red inalámbrica.

La implementación de esta tendencia se basa en la identificación del tipo de usuario que accede a la red WLAN proporcionándole respectivamente calidad de servicio, seguridad y un acceso fácil y rápido.

En la Figura 4.6 se puede observar un diagrama de flujo del funcionamiento de esta tendencia; la autenticación del usuario se lleva a cabo a través de un portal cuyas respectivas credenciales del usuario le permitirán el acceso como usuario invitado. Como medida de seguridad se tiene el registro del usuario en una base de datos; si este se encuentra registrado, el acceso a Internet será autorizado, de lo contrario el acceso es denegado.

Figura 4.6 Diagrama de flujo: WLAN Acceso a Usuarios Invitados

4.3.1 Control de acceso a usuarios invitados

Para tener un mejor control de los usuarios invitados es conveniente establecer una conexión a la red inalámbrica por tiempo limitado, esto con el fin de aumentar la seguridad y disminuir la intervención del área de TI. Una vez que el tiempo de sesión ha expirado, automáticamente se dejará de establecer una conexión con la red WLAN corporativa evitando que el dispositivo móvil sea un portal para atacar el sistema; esto proporciona a los administradores de la red una forma de control de acceso, ya que no tendrán que investigar qué dispositivos, correspondientes a usuarios invitados, aún se encuentran activos consumiendo un ancho de banda que es indispensable para proporcionar a otros usuarios invitados que deseen acceder a la red WLAN empresarial.

4.3.2 Integración de Acceso a Usuarios Invitados

La mayoría de los componentes con los que deben estar integrados la red WLAN empresarial segura para la implementación de Acceso a Usuarios Invitados son los siguientes (véase Capítulo 3, para conocer las características de cada componente):

- Servidores: DNS, DHCP, HTTP y RADIUS
- Servidor de políticas : NAP
- Controlador inalámbrico: WLC
- Control de acceso y listas de acceso: AC Y AD
- Método de autenticación: 802.1x, EAP-TTLS
- Método de cifrado: WPA2 empresarial
- Monitoreo: WIPS
- Firewall: DMZ

Cada componente constituye una parte esencial en la arquitectura de la red WLAN corporativa, la cual proporcionará un alto nivel de seguridad para la integración de la tendencia de Usuarios Invitados.

4.4 Soluciones WLAN

Las soluciones de proveedores de infraestructuras WLAN son diversas, y la integración de las nuevas tendencias en la red WLAN empresarial requiere de múltiples componentes, los cuales pueden verse como resultado de un sistema complejo; además, considérese que la seguridad debe ser efectiva y la gestión de los dispositivos móviles que integrarán a la red inalámbrica requieren del establecimiento de múltiples factores de administración.

La evaluación de los proveedores de soluciones, como objetivo de este documento, comprenderá principalmente implementar la tendencia *Guest Access User* en la red inalámbrica WLAN empresarial de cuarta generación.

En la Tabla 4.2 se enlistan algunos de los proveedores y productos, para la tendencia *Guest Access User*, que actualmente se encuentran en el mercado de soluciones de redes WLAN empresariales.

Tabla 4.2 Proveedores y soluciones WLAN empresariales

Proveedor	Solución
Cisco	Unified Wireless Guest Access Services
HP Networking	HP Procurve Guest Access
Aruba Networks	Aruba's Guest Access Solution Clear Pass Guest
Huawei	---
Motorola Solutions	WiNG 5 Guest Access
Alcatel-Lucent	WLAN Guest Management Software
Ruckus Wireless	Guest Networking
Aerohive	Secure Guest Wi-Fi Access
Meraki*	Wireless Guest Access at the Office
Avaya	Avaya Identity Engines Guest Manager
Juniper Networks	Enterprise Guest Access
Xirrus	Xirrus Access Manager

*Actualmente Meraki se encuentra incorporada a Cisco.

A través del presente trabajo, se llevó a cabo un análisis en diversas fuentes de información para seleccionar el proveedor del software con mayor renombre dentro del mercado.

Las fuentes de información utilizadas fueron análisis técnicos realizados por organizaciones especializadas en computación, tecnologías de la información y seguridad.

A. Gartner

De acuerdo al estudio: *"Magic Quadrant for the Wired and Wireless LAN Access Infrastructure, 2012"* [42] realizado por Gartner (compañía líder en investigación de TI y consultoría), las soluciones de proveedores de infraestructuras WLAN deben emplear en sus soluciones las siguientes características:

- Distribución y administración de reglas para usuarios invitados en redes WLAN.
- *Firewall.*
- Control y protección de acceso a la red, incluidos los servicios de autenticación y autorización.
- WLAN forense.
- Protección contra intrusiones para redes cableadas y redes WLAN.
- Integración de los servicios comunicaciones unificadas.
- Servicios de localización y gestión de activos

En base a sus estudios, Gartner clasifica los proveedores de soluciones de infraestructura WLAN de acuerdo a la capacidad de sus soluciones, innovación, sectores de desarrollo y su demanda en el mercado, y los presenta en su cuadrante (véase Figura 4.7).

El cuadrante se encuentra clasificado en cuatro áreas:

- **Líderes *(Leaders)*.** Satisfacen la demanda y demuestran una visión y cumplimiento de las exigencias para mantenerse dentro del mercado. Por lo general, este tipo de proveedores tienen una gran cantidad de clientes satisfechos con sus soluciones.

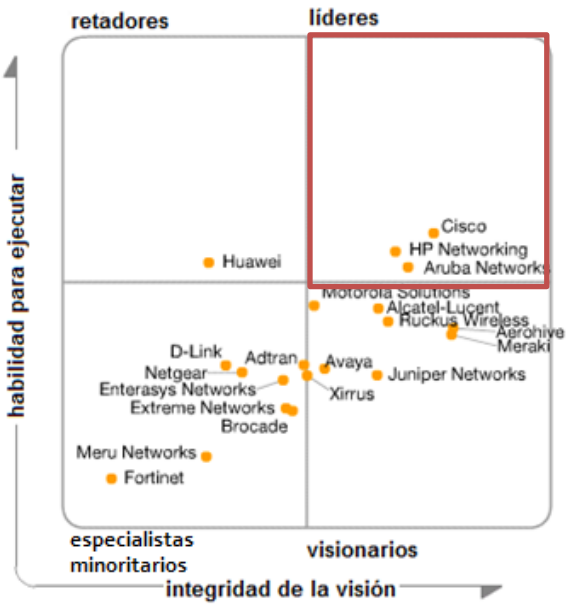


Figura 4.7 Cuadrante Mágico de Gartner: Wired and Wireless LAN Access Infraestructure, 2012 [42]

- **Retadores *(Challengers)*.** Empresas que tienen una fuerte habilidad de ejecución. Cuentan con la capacidad y recursos financieros pero carecen de visión e innovación que el mercado necesita.

- **Visionarios *(Visionaries)*.** Tienen una visión de cómo evolucionará el mercado lo que permite introducir nuevas tecnologías y tendencias. Por lo general, requieren de un apoyo financiero otorgado por empresas líderes.

- **Especialistas minoritarios (*Niche players).*** Se concentra en sectores especializados del mercado, tienen una capacidad de ejecución y un grupo de clientes limitado.

B. Info-Tech research gruop

De acuerdo al estudio *"Vendor Landscape: Wireless LAN, 2012"* [43], realizado por *Info-Tech research group* (compañía líder mundialmente en investigación de TI y consultoría) los proveedores y soluciones de infraestructura WLAN se clasifican de acuerdo a los siguientes criterios de evaluación.

Criterios de evaluación del producto:

- **Características.** La solución proporciona características de funcionalidad básica y avanzada.
- **Facilidad de uso.** La interfaz y las herramientas son intuitivas y fácil de usar.
- **Factible.** Durante los tres primeros años de CTP[30] la solución es económica
- **Arquitectura.** La solución contiene lo que se especifica por el proveedor.

Criterios de evaluación del proveedor:

- **Viable.** El proveedor es rentable y eficiente.
- **Estrategia.** El proveedor se encuentra a la vanguardia con nuevas soluciones factibles para la integración con sus clientes.
- **Alcance.** El proveedor ofrece una cobertura mundial y es capaz de proporcionar un soporte de ventas.
- **Canal.** El proveedor cuenta con estrategias de canal apropiados para abastecer a sus clientes.

De acuerdo a las características anteriormente mencionadas, Info-Tech clasifica los proveedores de soluciones de infraestructura WLAN y los presenta en el cuadrante denominado *The Info-Tech Landscape* (véase Figura 4.8), como se describe a continuación:

- **Campeones *(Champions)*.** Tienen una fuerte presencia en el mercado y son por lo general los creadores de nuevas tendencias para la industria.
- **Pilares del mercado *(Market Pillars).*** Los productos son calificados con un puntaje mayor que la media, de acuerdo a las características establecidas para la evaluación del producto.

[30] El costo total de propiedad, determina los costos (incluyendo soporte, costo de operación, consultoría, etc.) y beneficios relacionados con una compra de equipos y/o programas informáticos.

Figura 4.8 Cuadrante Info-Tech: *The Info-Tech Landscape*, Wireless LAN 2012 [43]

- **Innovadores *(Innovators)*.** El producto demuestra ser innovador por lo que se evalúa como un producto competitivo dentro del mercado.

- **Jugadores emergentes *(Emerging Players)*.** Los proveedores son nuevos en el mercado; sin embargo, tanto el proveedor como sus soluciones demuestra atributos para entrar en el mercado.

C. IDC

IDC *(International Data Corporation)* compañía proveedora mundialmente de inteligencia de mercado, servicios de consultoría y eventos para los mercados de tecnologías de la información tecnológica, de telecomunicaciones y de consumo; reúne en su estudio *"World Wide Enterprise WLAN 2011–2012 Vendor Analysis"* [44] y "*Top Five Worldwide Enterprise WLAN Vendors, 2013*" [45], los resultados de la evaluación de los proveedores de soluciones WLAN empresarial. Tomando como criterio para la evaluación de los proveedores de soluciones inalámbricas los siguientes puntos:

- El fenómeno BYOD y sus implicaciones (incluyendo seguridad).
- La capacidad de manejar datos, voz y aplicaciones de vídeo.
- Respuesta proactiva frente a las tecnologías empresariales emergentes como *"cloud".*

- Opciones para diferentes tipos de despliegue.

En su resultado, IDC presenta a los proveedores de soluciones en un gráfico dividido en dos categorías: capacidad y estrategia. Los analistas de IDC posicionan a los proveedores como el reflejo del despliegue de su capacidad actual que permitan ejecutar su estrategia elegida en el mercado y el cumplimiento con las necesidades del cliente; por otro lado, la estrategia de un proveedor se verá enfocado en diversas áreas las cuales deben cumplir con las necesidades del cliente y al gasto en un periodo de tiempo definido.

En la Figura 4.9, se muestra el posicionamiento de cada proveedor; el tamaño del círculo indica la cuota de mercado del proveedor, mientras que los símbolos "+","-" e "=" indican si el proveedor está creciendo más rápido, menor o igual que el desarrollo global del mercado.

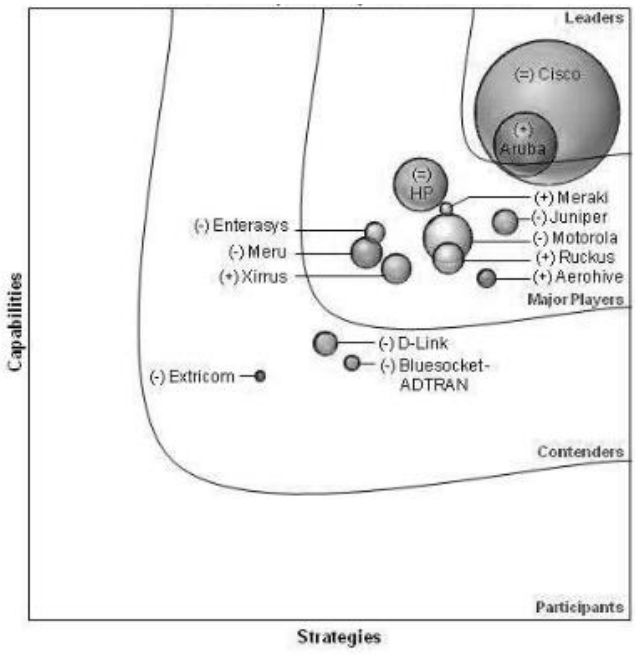


Figura 4.9 Análisis IDC, World Wide Enterprise Vendor Analysis, 2011-2012 [45]

D. Infonetics Research

Infonetics Research es una empresa especializada en consultoría de las TI, la cual ayuda a sus clientes a planificar, crear estrategias, y competir con eficacia en el área de las TIC. En su reporte titulado *"Wireless LAN Equipment and WiFi Phones, 2012"* [46], Infonetics

realiza una evaluación de los diferentes proveedores de soluciones WLAN que se encuentran en el mercado. El informe proporciona el tamaño del mercado, la cuota de mercado, el análisis de los puntos de acceso para la tecnología: 802.11 a / b / g, 802.11n, 802.11ac, controladores WLAN, etc.

En base a IDC, éste clasifica a nivel mundial a los cinco proveedores que cumplen con un puntaje alto, las características mencionadas anteriormente; siendo estas: Cisco, Aruba, Ruckus, HP y Motorola Solutions.

Como resultado de su estudio, Infonetics proporcionó un primer lugar a la empresa Cisco por su alta competitividad siendo éste líder en el mercado; en segundo lugar se encuentra Aruba, y un tercer lugar se otorga simultáneamente a los proveedores HP y Motorola Solutions, y finalmente se tiene al proveedor de soluciones Ruckus con un cuarto lugar.

A partir del siguiente análisis, el estudio del presente proyecto se enfocó a seleccionar a los proveedores de soluciones WLAN (véase Tabla 4.3) que tengan relevancia dentro de los anteiores estudios, como se muestra a continuación:

A. Gartner: que se encuentre dentro del Cuadrante Mágico de Líderes y Retadores.

B. Info-Tech research grupo: que se encuentre dentro del cuadrante de Ganadores.

C. IDC International Data Corporation: que se encuentre dentro del grupo de Líderes y se ubique dentro de los cinco primeros lugares de proveedores de soluciones de WLAN.

D. Infonetics Research: que haya sido evaluado dentro de los tres primeros lugares en el estudio [50].

Tabla 4.3 Evaluación de proveedores de soluciones WLAN empresarial

Proveedor	A	B	C	D
Cisco/Meraki	**Si**	**Sí**	**Si**	**Sí**
HP Networking	**Si**	**Sí**	**Si**	**Sí**
Aruba Networks	**Si**	**Sí**	**Si**	**Sí**
Huawei	No	No	No	No
Motorola Solutions	No	No	Si	Sí
Alcatel-Lucent	No	No	No	No
Ruckus Wireless	No	No	Si	No
Aerohive	No	No	No	No

Tabla 4.4 Continuación

Proveedor	A	B	C	D
Avaya	No	No	No	No
Juniper Networks	No	No	No	No
Xirrus	No	No	No	No
Entrasys	No	No	No	No

De acuerdo al análisis anterior, las soluciones que podrían considerarse líderes en el campo WLAN en base a estos estudios son:

- *Unified Wireless Guest Access Services* del proveedor Cisco Systems.
- *Aruba's Guest Access Solution* del proveedor Aruba Networks.
- *HP ProcurveGuest Access* del proveedor HP Networking.

A partir de este momento centraremos nuestra atención en estos tres proveedores y sus respectivas soluciones líderes en el mercado.

En los siguientes apartados se mostrarán las características generales que ofrece cada proveedor para la implementación de la tendencia Acceso a Usuarios Invitados.

4.4.1 Cisco Systems

Cisco Systems es una empresa líder de TI a nivel mundial cuya función radica en la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones. Para la implementación de un sistema de acceso a usuarios inalámbricos, Cisco propone la solución ***Unified Wireless Guest Access Services*** [47].

En su configuración, la solución de Acceso de Usuarios Invitados debe ser implementada de forma correcta a través de las medidas de seguridad correspondientes para lograr un resultado satisfactorio. Los beneficios que se encuentran en esa solución son:

- Autenticación y autorización de control de usuarios invitados en función a la fecha, duración y ancho de banda.

- Se ofrece un mecanismo de auditoría para controlar quién está utilizando, o ha utilizado, la red.
- Se elimina la necesidad de designar áreas especiales donde se encontrarán los usuarios invitados.
- Su arquitectura se basa en un “controlador ancla”.

Como se muestra en la Figura 4.10, cuando un usuario interno desea ingresar a la red WLAN empresarial interna, su dispositivo es direccionado a la VLAN correspondiente; sin embargo, para un usuario invitado el método es diferente ya que el tráfico se redirecciona a través del controlador ancla y se envía a la DMZ, que como se puede observar en dicha figura, cumple con las expectativas de seguridad al no permitir a un usuario invitado ingresar a los datos corporativos.

El usuario invitado se encontrará en una zona segura donde es posible acceder a Internet a través de la red inalámbrica corporativa pero sin acceso a la información interna de la empresa.

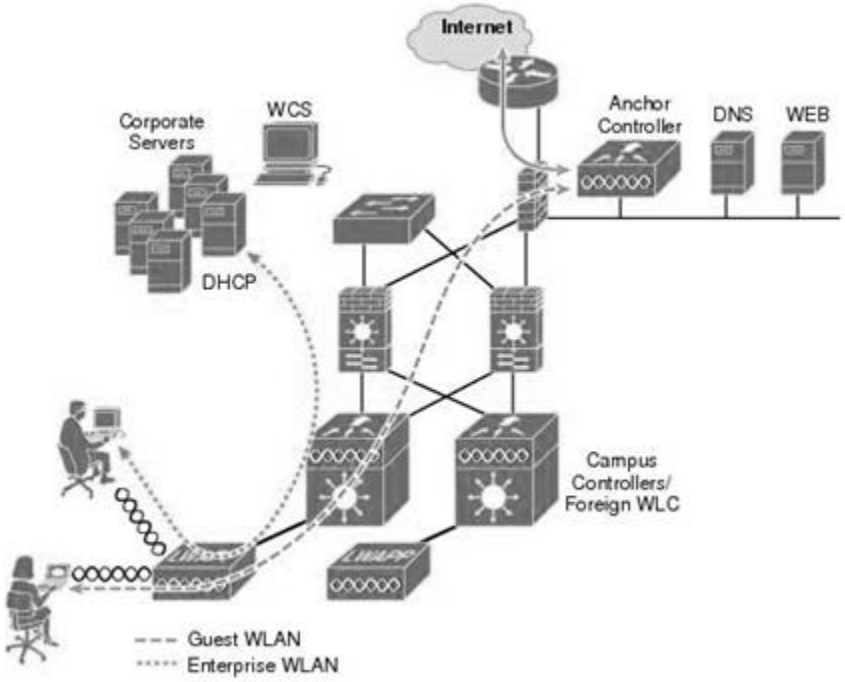


Figura 4.10 Arquitectura Cisco: Unified Wireless Guest Acccess Solution [47]

4.4.2 Aruba Networks

Aruba Networks, Inc. es un proveedor de redes WLAN y equipos de última generación de redes de acceso. Para la implementación de un sistema de acceso a usuarios, Aruba propone la solución ***Aruba's Guest Access Solution*** [48]**.**

Aruba, en su solución, ofrece una forma segura para el acceso de usuarios invitados a la red WLAN empresarial. La seguridad que proporciona se basa en:

- **Separación de tráfico.** Los administradores de la red pueden configurar diferentes políticas de seguridad para usuarios internos e invitados, por ejemplo, a los usuarios invitados se les puede dar acceso a la red WLAN empresarial sin darles todos los privilegios de la red corporativa que se le otorgan a los usuarios internos.

- **Datos de uso y auditoría.** Aruba proporciona un historial de los usuarios que utilizan la red, cuando lo utilizan y cómo se utiliza.

- **Portal cautivo.** Los dispositivos tienen acceso a la red hasta que un navegador web se abre e introducen las credenciales de autenticación; dicho proceso es protegido a través de SSL. El portal puede ser diseñado por los administradores de la red WLAN corporativa.

En la Figura 4.11, se observa la arquitectura que Aruba propone para la implementación de su solución El *router Core* es el responsable del encaminamiento de todo el tráfico hacia y desde los controladores de movilidad.

El controlador principal es responsable de la configuración y la gestión de la movilidad de dominio y los controladores locales; así como de la gestión de los LAP, quienes detectan automáticamente el controlador principal mediante una consulta DNS.

Esta arquitectura permite crear cuentas temporales de autenticación y de esta forma el usuario invitado puede acceder a la red desde el portal cautivo. Todos los usuarios invitados están restringidos al uso de la red WLAN interna de acuerdo a las políticas de seguridad implementadas por la empresa.

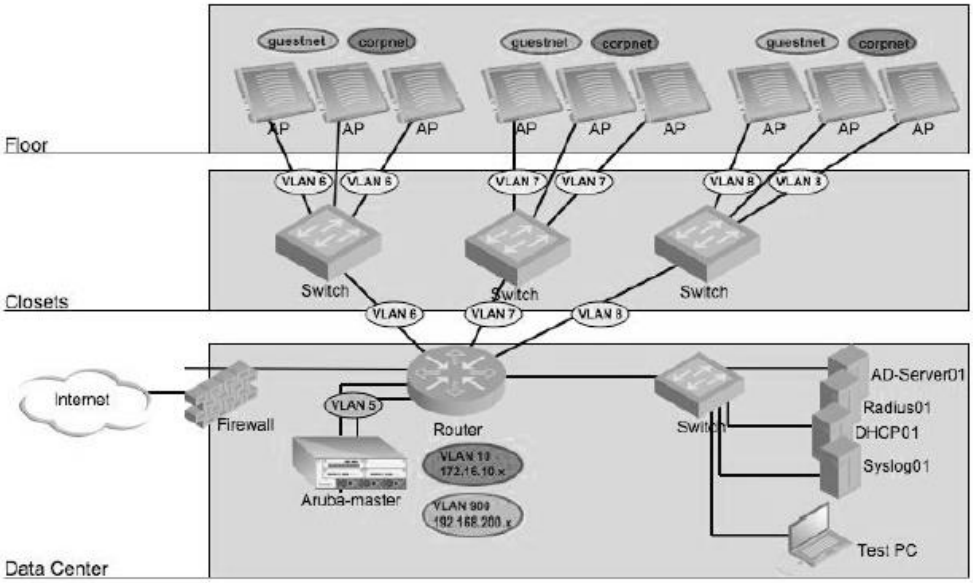


Figura 4.11 Arquitectura Aruba: Guest Acccess Solution [48]

4.4.3 HP Networking

HP Networking brinda servicios a clientes empresariales y gubernamentales para la integración de soluciones a redes WLAN. Para la implementación de un sistema de acceso a usuarios, HP propone la solución ***HP Procurve Guest Acess*** en conjunto con ***HP Intelligent Managament Center*** [49].

A través de estas soluciones, HP ofrece los siguientes puntos de administración:

- Control de políticas asociadas con la identidad del usuario invitado.
- Autenticación del usuario a través de un portal cautivo
- Gestión de usuarios a través de las redes unificadas.
- Implementación de redundancia *"always on network access".*
- Calidad de servicio.
- Prevención de intrusos.

En la Figura 4.12 se muestra la arquitectura de las soluciones que promueve HP para la integración del acceso a usuarios invitados. Cuando un usuario invitado desea acceder a

la red se registra en el portal cautivo de la empresa, una vez que las credenciales han sido autenticadas el usuario puede acceder solamente a Internet a través de la VLAN creada anteriormente por el administrador en los *switch* correspondientes.

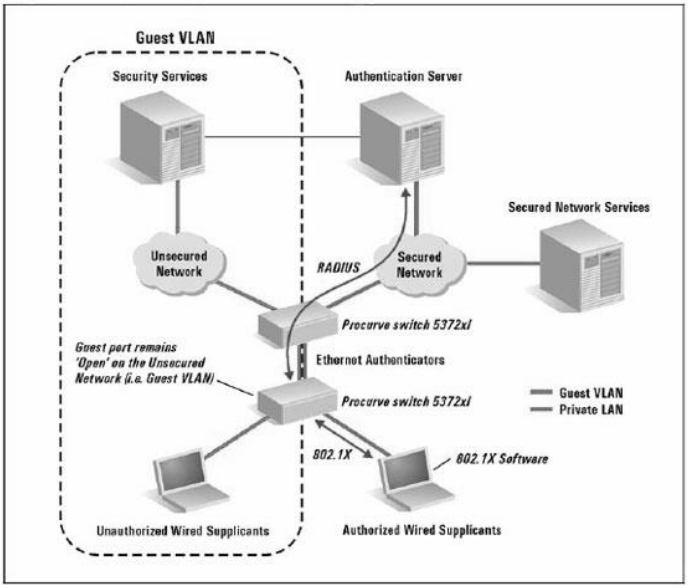


Figura 4.12 Arquitectura HP: Procurve Guest Acess e Intelligent Management Center [49]

4.5 Evaluación y elección de la solución

La evaluación de las soluciones propuestas por los tres proveedores más competitivos en el mercado y una toma de decisión para la integración de la tendencia de acceso a usuarios invitados e incorporación futura de BYOD, promueve a un análisis detallado de los productos.

De acuerdo a las características más importantes expuestas por los administradores de la Empresa Financiera, la integración de soluciones en la red WLAN empresarial segura de última generación se constituyen a través de las Tablas 4.5 y 4.6; en las cuales, se muestra la comparación entre los proveedores: Cisco Systems, Aruba Networks y HP Networking.

Tabla 4.5 Cumplimiento de características básicas

	Características	Cisco	Aruba	HP
Hardware	• 802.11n • AP multi-radio • Antenas MIMO	**Sí**	**Sí**	Sí
Inteligencia	• Priorización de tráfico • QoS • Gestión automática del espectro de RF	**Sí**	**Sí**	Sí
Administración	• Políticas de acceso • Gestión de recursos e incidentes	**Sí**	**Sí**	Sí
Seguridad	• Estándares basados en autenticación y cifrado • Detección de intrusos	**Sí**	**Sí**	Sí
Acceso a Invitados	• Acceso a Internet de usuarios invitados	**Sí**	**Sí**	Sí

Fuente: Report, Vendor Landscape: Wireless WLAN, *"There's an ideal mate for every enterprise – pick yours"*, Info-tech research group, 2012. Consultado en http://www.infotech.com/.

Tabla 4.6 Cumplimiento de características avanzadas

	Características	Cisco	Aruba	HP
Administración	• Gestión unificada de redes LAN Y WLAN	**Sí**	**Sí**	Sí
Monitoreo	• Visibilidad de RF en tiempo real de los AP. • Localización de usuarios y puntos de acceso.	**Sí**	**Sí**	Sí
BYOD	• Características específicas de los dispositivos móviles. • Creación de políticas.	**Sí**	**Si**	No*
Prevención de Intrusos	• Sistema de prevención de intrusos a la red WLAN. • Localización de intrusos.	**Sí**	**Sí**	Sí
Controlador WLAN	• Centralización de los AP	**Sí**	**Sí**	Sí
Autenticación	• Portal cautivo • 802.1x • RADIUS/AD/LDAP.	**Sí**	**Sí**	Sí
Auto log-out	• Desactivación automática de la cuenta de usuario invitado a término del tiempo de acceso.	**Sí**	**Sí**	No
Informes	• Tiempo de actividad del usuario en la red WLAN	**Sí**	**Sí**	No

Fuente: Report, Vendor Landscape: Wireless WLAN, *Choose the right WiFi solution – from more than just thin air*, Info-tech research group, 2012. Consultado en http://www.infotech.com/.
*No se encuentra desarrollada totalmente

De acuerdo a las características evaluadas, en las anteriores tablas, los proveedores que cumplen con los requisitos planteados por la Empresa Financiera pertenecen a Cisco y Aruba con su correspondiente solución.

4.5.1 Rendimiento de soluciones en un ambiente de pruebas

Para la elección entre los dos proveedores de soluciones inalámbricas (Cisco y Aruba), se realizó una investigación del rendimiento de los componentes de acceso a la red de las soluciones en un ambiente de pruebas. En los siguientes puntos se describirán, de forma general, las pruebas a las que fueron sometidos los dispositivos de acceso que componen a la soluciones a través de la empresa certificadora Miercom, 2013 [50][51].

Los productos en evaluación se enlistan a continuación.

- Controladores
  - Cisco WLC 5760 Serie
  - Aruba WLC 7240 Serie

- Puntos de acceso
  - Cisco AP 3600 Serie
  - Aruba AP 13x Serie

NOTA: Los modelos en los grupos de evaluación representan la competencia de productos entre sus versiones correspondientes.

El ambiente de pruebas realizado por la Empresa Certificadora se empleó a través de:

- Ixia IxChariot[31], se utilizó para la prueba de calidad de servicio de voz en la simulación de llamadas de VoIP y en la prueba de rendimiento de los dispositivos AP para la simulación de tráfico de datos voz y vídeo.

- El Centro de Pruebas de Spirent[32] fue utilizado para las pruebas de carga.

[31] Para mayor referencia diríjase a la página del proveedor: http://www.ixiacom.com

- Las pruebas de QoS en vídeo se realizaron con *VLC Media Player* como la transmisión (aplicación para Apple MacBook Pro portátiles).
- Las pruebas de QoS se realizaron bajo el mismo esquema de RF para los productos de ambas soluciones.
- El Cisco AP 3600 utiliza el protocolo CAPWAP IP / UDP.

NOTA: Los resultados de las pruebas se basan en la opinión media de los expertos que conforman a la Empresa Certificadora.

1. Rendimiento de WLC

El rendimiento teórico propuesto por el fabricante, indica que Aruba WLC 7240 soporta 40 Gbps; a diferencia de éste, Cisco WLC 5760 maneja un rendimiento alrededor de 60 Gbps.

Para la realización de la prueba, Miercom colocó un ambiente de pruebas con tráfico IMIX[33], el resultado obtenido demostró que Cisco WLC 5760 ofrece un rendimiento considerablemente mayor sobre Aruba WLC 7240. En la Figura 4.13 se observa el resultado del rendimiento entre los WLC de Aruba y Cisco proporcionado por la Empresa Certificadora.

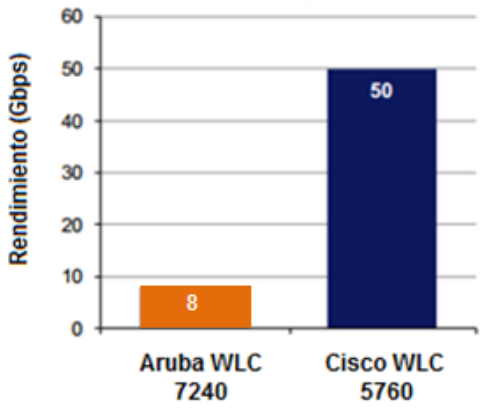


Figura 4.13 Rendimiento Aruba WLC 7240 vs Cisco WLC 5760 [51]

[32] Para mayor referencia diríjase a la página del proveedor: http://www.spirent.com
[33] En un ambiente de pruebas, IMIX es la inyección de flujo de datos (que se tendría en condiciones reales sobre una red datos) a través de diferentes tamaños de paquetes.

2. Calidad de voz sobre IP (VoIP)

De acuerdo con el informe, en una red de prueba sin una carga de tráfico, tanto Aruba WLC 7240 como Cisco WLC 5760 realizaron una transmisión de llamada de voz sobre IP a una velocidad de 64 kbps con una calidad aceptable.

Como segundo punto de la prueba, Miercom marca el ingreso de un flujo de tráfico considerable (red congestionada) lo que provocó una pérdida de paquetes de voz, dando como resultado una disminución notable en la calidad de voz para el caso de Aruba comparado con Cisco, éste último mantuvo dentro del rango su calidad en VoIP, refiérase a la Figura 4.14.

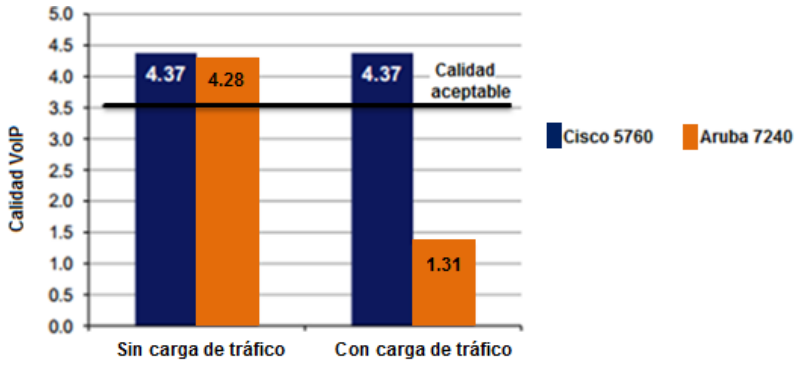


Figura 4.14 Calidad de VoIP [51]

NOTA: Los rangos de calidad son los siguientes: 0-1 imposible comunicar; 1-2 comunicación pobre; 2-3 comunicación pasable; 3-4 comunicación buena: 4-5 comunicación perfecta

3. Calidad de servicio en vídeo

En la prueba de la calidad de servicio en vídeo la Empresa Certificadora indica su sistema de pruebas con dos dispositivos inalámbricos (*Apple MacBook Pro Laptops*) accediendo a la red WLAN a través de los AP y con la reproducción de un vídeo con una carga de tráfico considerable.

El resultado de la prueba (véase Figura 4.15) permite observar una caída en la calidad de vídeo con una carga de tráfico del 60 % para Aruba; en contraste, Cisco, mantiene la calidad en su servicio de vídeo con un 83 % de carga de tráfico.

Figura 4.15 Calidad de servicio en vídeo [51]

4. Rendimiento de dispositivos AP

Para probar el rendimiento de que ofrecen los puntos de acceso a la red, la Empresa Certificadora planteó el esquema de un Cisco WLC 5760 en conjunto con tráfico de voz datos y vídeo para la prueba de Cisco AP 3600 y Aruba AP 13x.

La Empresa certificadora midió el rendimiento del AP a través de un dispositivo inalámbrico a prueba, para este caso *Android Smart Tablet* modelo *Motorola Xoom*. En la Figura 4.16, (dónde el dispositivo a prueba es colocado a una distancia cada vez mayor del origen del AP) se observa como resultado, que el Cisco AP 3600 mantiene un nivel de rendimiento mayor que el Aruba AP 13x.

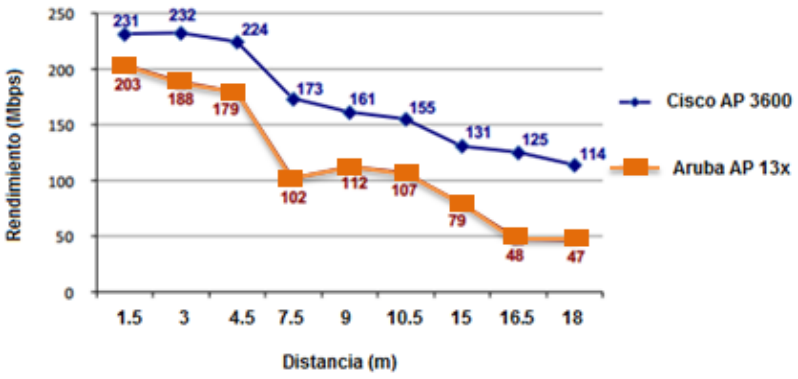


Figura 4.16 Rendimiento de los AP [51]

5. Ahorro de batería en dispositivo inalámbrico a prueba

En la última prueba que certifica Miercom, la evaluación de ahorro de batería en dos dispositivos inalámbricos a prueba (mismos modelos que en el punto anterior) permite

observar la eficiencia de cada uno de los AP evaluados. En dicha prueba se analiza el tiempo de descarga de un archivo de 11 GB a través del protocolo FTP[34]. Los indicadores para determinar un resultado fueron: el tiempo total de descarga y la cantidad de batería en la *SmartTablet* necesaria para realizar dicha tarea.

La prueba inició a una distancia de 13 metros del AP a prueba con un porcentaje de batería al 75 %, con un brillo en el dispositivo del 70% y sin uso de ahorro de energía.

Los resultados, a través de Aruba AP-13x el archivo se descargó en 70 minutos y a través de Cisco AP 3600 se realizó la misma acción en 52 minutos. En la Figura 4.17 se puede observar el porcentaje de caída de ambas *Tablets* respecto a cada AP a prueba.

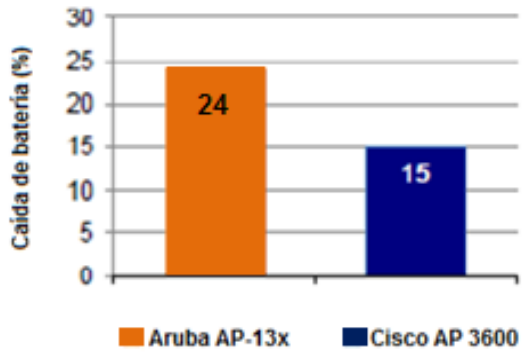


Figura 4.17 Caída de batería en *Tablet* [51]

4.5.2 Solución final

Con las anteriores evaluaciones de los productos preliminares (Cisco y Aruba) para la solución inalámbrica correspondiente a cada una de ellas; podría mencionarse que la mejor solución para la implementación de Acceso a Usuarios Invitados en la Empresa Financiera es la proporcionada por el proveedor de Cisco, ya que cumple con la infraestructura de seguridad que se demanda y las pruebas de rendimiento por parte de la Empresa Certificadora resultaron ser exitosas.

[34] Protocolo utilizado para la transferencia de archivos entre sistemas interconectados a la red de datos.

Capítulo 5

PROTOTIPO DE DISEÑO DE UNA RED WLAN 802.11 EMPRESARIAL SEGURA DE CUARTA GENERACIÓN

El prototipo de diseño de una red WLAN IEEE 802.11 segura, en su ámbito empresarial, propone un planteamiento minucioso y un esquema que resulte práctico para la administración del mismo.

Restructurar una red WLAN en un plan de desarrollo de movilidad es transformar el panorama de la red empresarial. La tecnología inalámbrica es y tiene que ser considerada como una herramienta de productividad para la empresa, a través de la cual los empleados puedan acceder a las aplicaciones y hacer uso de los recursos en cualquier lugar del área laboral y en cualquier momento.

La implementación de un prototipo red WLAN empresarial de cuarta generación permitirá integrar las nuevas tecnologías y tendencias WLAN que se encuentran en el mercado de soluciones inalámbricas y establecer las bases para el futuro crecimiento de la red empresarial.

En este capítulo se diseña un prototipo de diseño para la integración de la solución inalámbrica evaluada y la integración de Acceso a Usuarios Invitados para la estructuración de la red Empresarial.

5.1 Nueva perspectiva

La evolución hacia la movilidad en la Empresa depende de una base en el desarrollo de la tecnología de comunicación inalámbrica. En sus inicios la tecnología Wi-Fi comenzó como un concepto de “poder tener” movilidad y de esto, se ha convertido rápidamente en una “necesidad imprescindible” de comunicación. Los usuarios al mirar en su entorno el desarrollo de la tecnología inalámbrica, esperan que su Empresa les proporcione los servicios inalámbricos básicos que ellos requieren para acceder a la red WLAN a través de sus dispositivos móviles. Esta perspectiva por parte de los empleados (ahora denominados usuarios) tiene como consecuencia serias implicaciones para la Empresa, ya que debe crear un esquema de comunicación inalámbrica seguro para el beneficio de sus usuarios así como para la Empresa misma.

La movilidad es un medio complejo de componentes independientes; la Empresa se ha encargado de ver este nuevo panorama de comunicación a través de la colaboración por parte de las áreas de TI y la adopción de una estructura de políticas de seguridad para la integración de las nuevas tendencias. En la incorporación del prototipo de red WLAN, se contemplan los puntos señalados en la Figura 5.1.

Figura 5.1 Perspectiva de red WLAN Empresarial

El esquema de movilidad de la Empresa es más que sólo servicios de movilidad sin relación alguna. Su enfoque se encuentra en la incorporación de las aplicaciones y herramientas que permitan a los usuarios no sólo conectarse a la red WLAN empresarial sino integrarse en un ambiente laboral colaborativo de aplicaciones y herramientas unificadas.

El objetivo es una experiencia continua donde los usuarios puedan acceder de manera eficiente a sus recursos informáticos; así como un acceso seguro, al proporcionar un servicio de comunicación a Internet a usuarios invitados, abriendo así la frontera de colaboración empresarial.

5.2 Situación actual

En su momento, la situación actual de la Empresa Financiera presentaba un esquema de infraestructura de comunicaciones independientes; es decir, un sistema de red WLAN con una administración descentralizada (véase Figura 5.2), dónde los AP se encontraban sin una administración eficiente y siendo puntos vulnerables comprometían a la Empresa Financiera a posibles ataques informáticos.

La velocidad en que los empleados adquieren sus dispositivos móviles inalámbricos tales como *tablets* y *smartphones* para acceder a la red WLAN empresarial, compromete a la empresa a disponer de una nueva perspectiva de la infraestructura de red inalámbrica; obligando de esta forma a contemplar un prototipo de diseño de red WLAN en el cual se colocará una infraestructura de red WLAN centralizada para su administración y otorgar a los usuarios acceso a las aplicaciones y recursos de manera eficiente y con una calidad de servicio aceptable, considerando puntualmente, la seguridad y el rendimiento de la red Empresarial.

Figura 5.2 Situación actual de la red Empresarial

5.3 Propuesta de diseño de Red WLAN 802.11

Una vez analizados los aspectos que conforman a una red empresarial WLAN 802.11 segura y las características que la Empresa Financiera requiere para su infraestructura, es posible realizar una propuesta de diseño.

Los puntos clave que se considerarán para el prototipo son:

- Red WLAN siempre disponible (redundancia adecuada, 2 WLC anclas, 2 WLC foráneos, AP operando en un sistema centralizado)

- La red debe de cubrir un 95% de las áreas donde se proporcionará sus servicios a los usuarios. Con una velocidad mínima de al menos 5.5 Mbps (para un sistema 802.1b) o 22 Mbps (para un sistema 802.11a/g). Implementación del protocolo 802.11n

- Sistema inalámbrico con incorporación de EAP-TTLS 802.1x para usuarios internos y WPA2 con portal de autenticación para usuarios invitados.

- Red WLAN centralizada con una estructura de LAP administrados por un controlador WLAN con recursos preparados para la integración de:
    - Prioridad de tráfico
    - Disponibilidad de servicio a una red con alta densidad de tráfico
    - Seguridad de los recursos corporativos
    - Adaptación automática de velocidad y potencia de transmisión

- La integración de herramientas de monitoreo, permitirán tener un control de los dispositivos, así como información de posibles intentos de cambios no deseados al sistema a través de alarmas emergentes.

- El sistema WLAN debe ser compatible con la red existente y ser restructurada para la integración de las futuras tendencias inalámbricas.

- Integración del prototipo de diseño con la red existente.

- Implementación de la tendencia Acceso a Usuarios Invitados a través de la solución de red WLAN escogida en el análisis de soluciones WLAN (para mayor referencia diríjase al Capítulo 4).

- Incorporación del prototipo de diseño de red WLAN empresarial a través de los dispositivos de acceso a la red de la compañía proveedora de soluciones WLAN Cisco.

NOTA: La integración de éste diseño es a través de las soluciones inalámbricas Cisco, por lo que se descarta el correcto funcionamiento con la implementación de otros proveedores de soluciones WLAN.

El prototipo de red WLAN empresarial enfocará su arquitectura en un sistema centralizado con la integración de la tendencia de Acceso a Usuarios Invitados. De acuerdo a la infraestructura con la que actualmente cuenta la Empresa Financiera y con las necesidades que demanda, se diseña el siguiente prototipo de red WLAN IEEE 802.11, véase Figura 5.3.

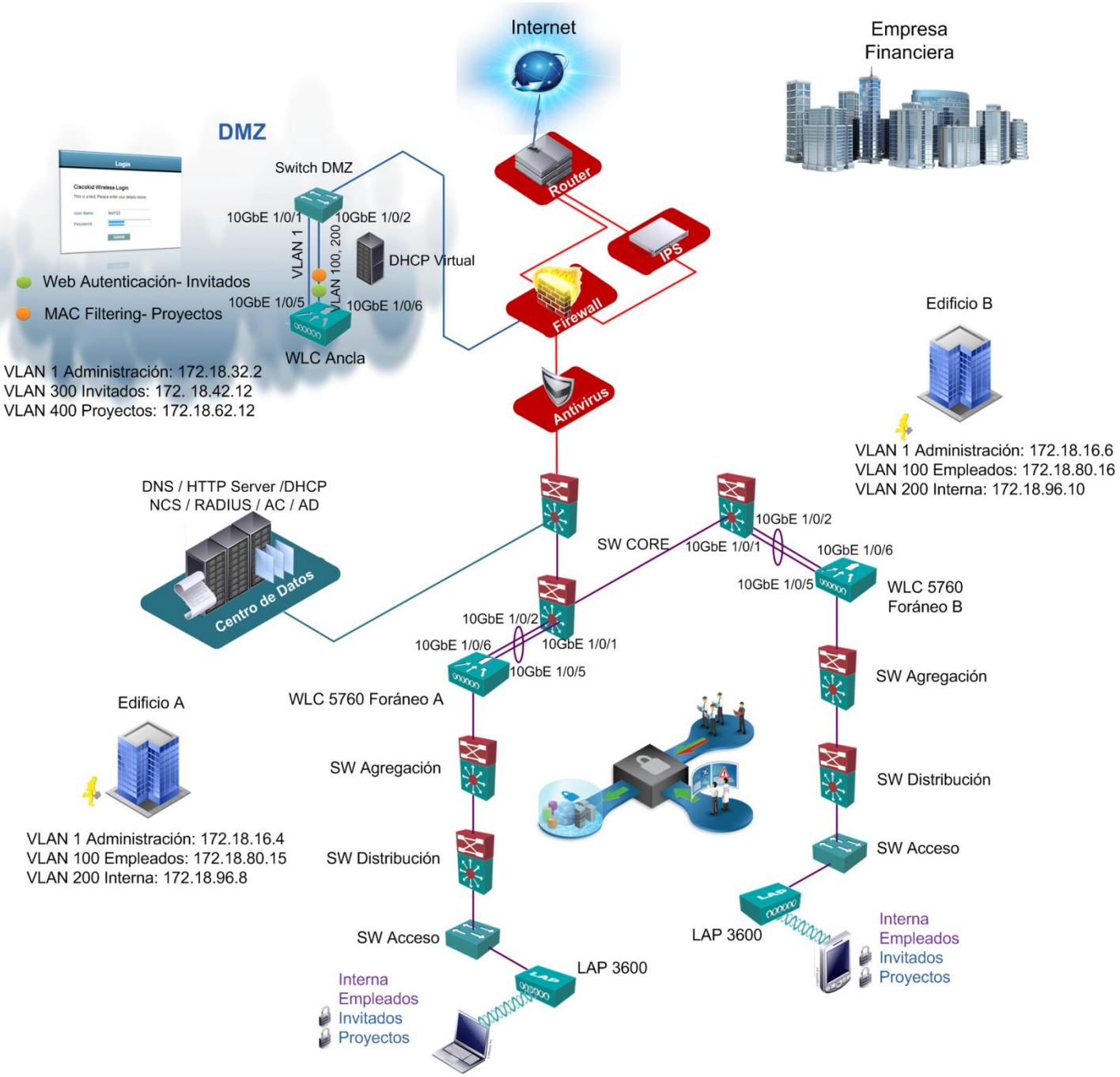


Figura 5.3 Prototipo de diseño de red WLAN IEEE 802.11

En los siguientes puntos se describirán los elementos y configuración de los mismos para la implementación del prototipo de diseño en la Empresa Financiera.

5.3.1 Puntos de Acceso en un sistema centralizado.

En este diseño de prototipo de red WLAN empresarial, los AP o LAP para un sistema centralizado, se encargaran de establecer la comunicación entre el WLC y el usuario (interno y/o invitado). Recuerde que en este sistema, los LAP son simples antenas cuya función reside en transmitir y recibir el flujo de datos.

En la Figura 5.4, se muestra un diagrama generalizado de la interconexión entre el LAP y el WLC.

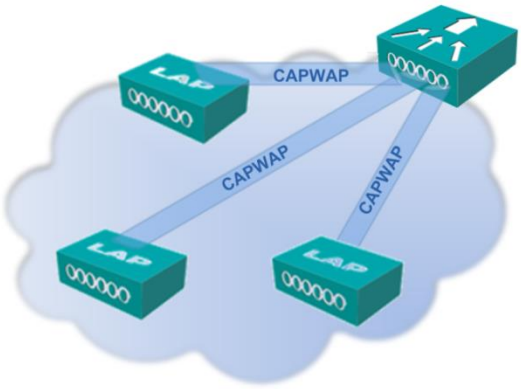


Figura 5.4 Conexión entre los LAP y WLC

La introducción del protocolo CAPWAP en el diseño de red WLAN centralizada permite realizar las siguientes características entre el WLC y el LAP:

- Establecimiento de túnel en la transmisión de datos
- Conexión en Capa 2
- Proceso de descubrimiento del LAP en el WLC
- Sistema de detección de intrusos (detección de AP maliciosos)

Otras funcionalidades que establece el LAP a través del WLC son:

- Asociación y reasociación de los usuarios(movilidad a nivel de Capa 2)
- Autenticación
- 802.11x/ EAP-TTLS/ RADIUS

NOTA: Los puertos UDP 5246 y 5247 se encuentren habilitados para lograr el proceso de asociación entre el LAP y el WLC.

- **Estructura física del Cisco AP 3600**

Para la implementación de los puntos de acceso en la arquitectura de red WLAN Empresarial, se eligieron (de acuerdo al estudio realizado anteriormente) los dispositivos AP del proveedor Cisco de la serie 3600. A continuación se muestra en la Figura 5.5 la estructura física y la distribución de puertos.

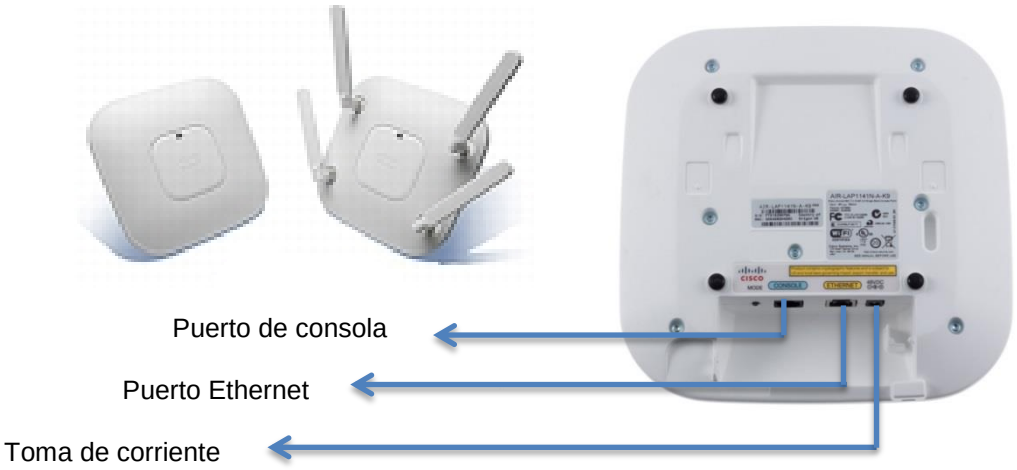


Figura 5.5 Cisco AP 3600 Series

NOTA: El modelo presentado es el elegido por la empresa a través de estudio; sin embargo, en el mercado se encuentran con diferentes características y costos.

5.3.1.1 Parámetros de inicio

El proceso de descubrimiento y asociación se describen en el Capítulo 2 de la presente Tesis, en este punto dirigiremos nuestra atención a la configuración de los LAP.

Dentro de la GUI del WLC Foráneo A podemos observar los dispositivos LAP que se encuentran asociados a dicho controlador (véase Figura 5.6). Para ejemplificar el proceso, se mostrará la configuración de un solo LAP; mismo proceso se realizó con todos los LAP del sistema inalámbrico.

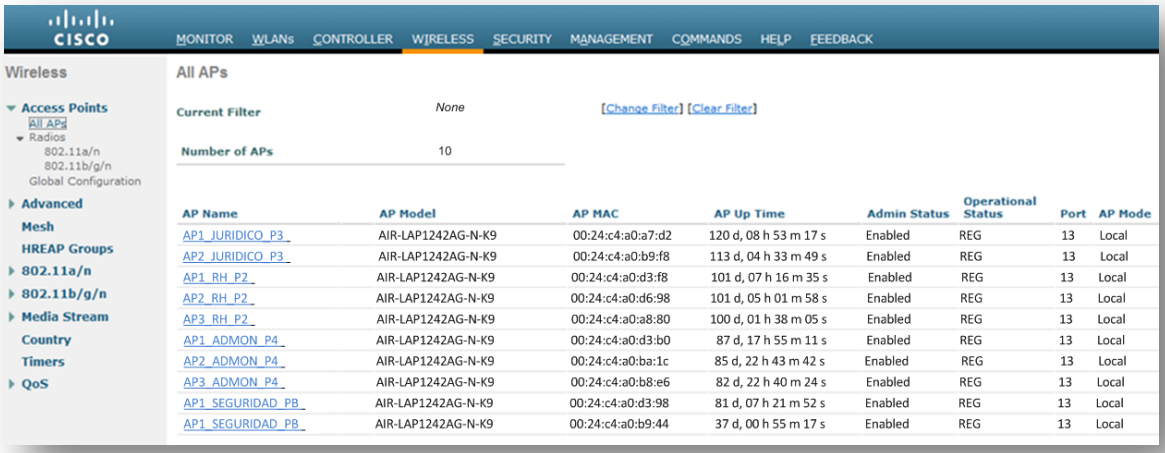


Figura 5.6 Despliegue de los LAP en el WLC Foráneo A

NOTA: En su primera configuración el nombre del LAP es visto en la lista de los LAP por su dirección MAC.

Una vez descubierto, seleccionamos un LAP y comenzamos a configurarlo a través de la pestaña ***Wireless*** en la opción ***Access Points > All APs> Global Configuration***. Entre los datos requeridos se encuentra el nombre y ubicación del LAP, se habilitó el estado de administración y el modo ***local*** indicando que este LAP se encuentra administrado por el WLC A; así mismo, se habilitó el modo ***WIPS*** para su función de sensor de intrusos (véase Figura 5.7).

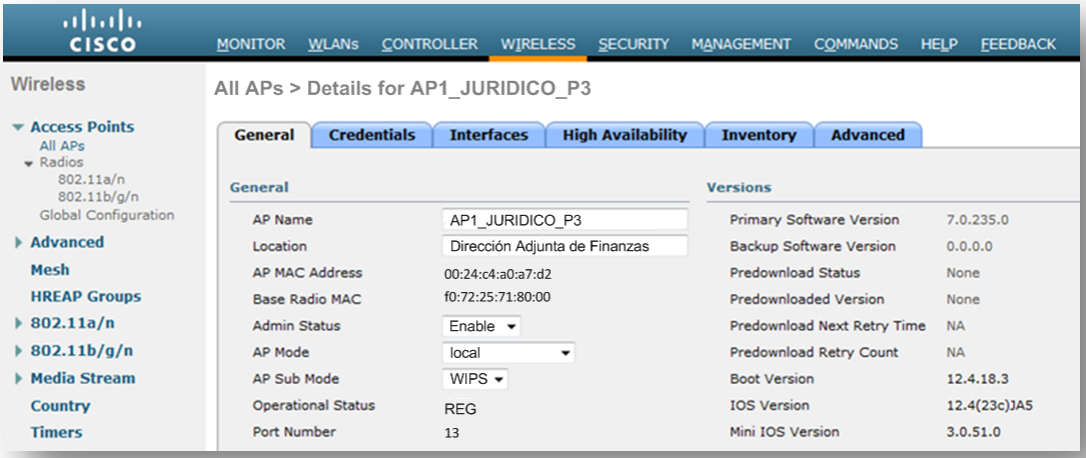


Figura 5.7 Configuración general del LAP AP1_JURIDICO_P3

Como siguiente punto definiremos el WLC primario del LAP, en este caso será el WLC Foráneo A. Para integrar un sistema redundante entre los WLC y los LAP, se recomienda establecer al WLC Foráneo B como controlador secundario. Es decir, si el WLC foráneo A fallara, el WLC foráneo B se establecerá como el controlador del LAP en configuración.

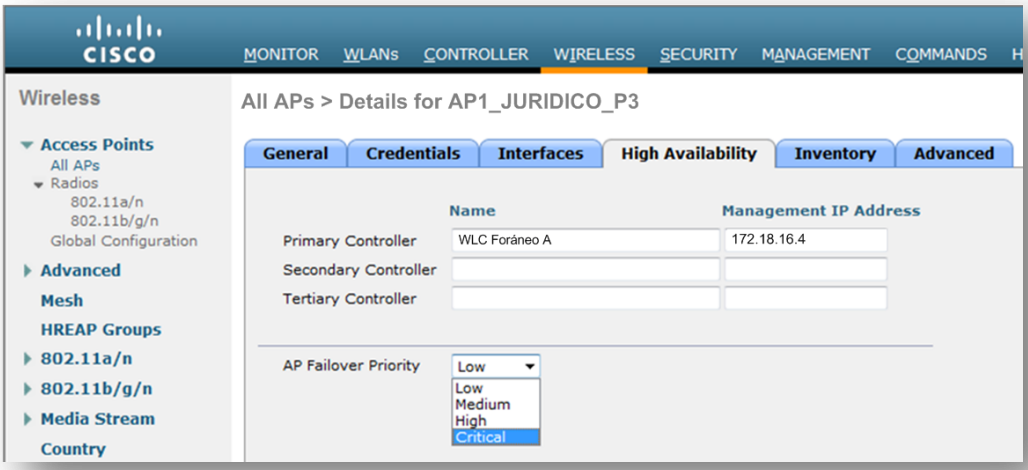


Figura 5.8 Configuración de WLC primario

5.3.1.2 Colocación física de los LAP

En la colocación de los LAP es preciso realizar un previo estudio de factibilidad para establecer la correcta implementación física de los LAP, que incluye:

- Cableado estructurado
- Condiciones de temperatura
- Levantamiento de información, ente otros.

En los edificios de varios pisos, cómo es el caso de la Empresa Financiera, es recomendable comprobar la superposición de canales entre las áreas de cobertura en los pisos donde se colocarán los LAP. En la Figura 5.9, se muestra la colocación física del LAP AP1_JURÍDICO_P3.

NOTA: Los estudios de factibilidad para la Empresa Financiera, resultaron exitosos por lo que no fue necesario hacer adecuaciones de cableado estructurado ni adecuaciones eléctricas para este proyecto

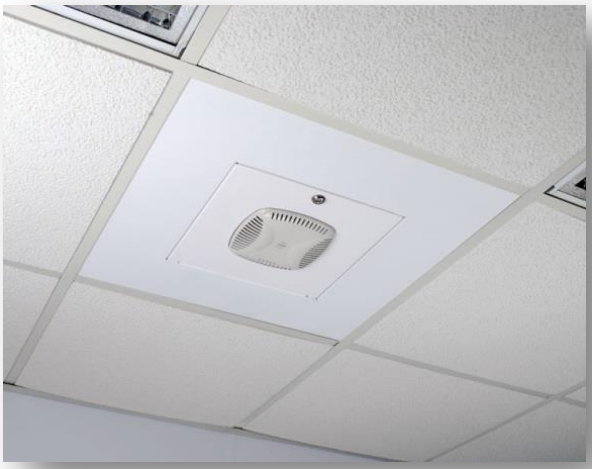


Figura 5.9 Colocación física del LAP AP1_JURÍDICO_P1

5.3.1.3 Asignación dinámica de parámetros de RF

La selección de canales se puede realizar de dos formas:

- **Manual.** El usuario define a través de la GUI las características y canales de RF para cada uno de los LAP a implementar.

- **Dinámico.** La estructura de LAP junto con el WLC crean un sistema de monitoreo de RF, el cual permite escanear todos los LAP y definir automáticamente los canales de RF. De esta manera la potencia de cada uno de los LAP se ajusta automáticamente de tal forma de que no interfieran entre ellos mismos y logren una cobertura lo más amplia posible evitando zonas de sombra o interferencia.

NOTA: Se recomienda utilizar la selección de canales de forma dinámica, esto con el fin de evitar errores en la asignación de canales y constante administración.

Para este proyecto se realizó la configuración automática de selección de canales, ésta se define a través de la GUI, en la pestaña ***Wireless*** en la opción ***802.11 a/n > RRM***

La configuración que se muestra en la Figura 5.10, se encuentra conformada por diferentes bloques de información, como se describen a continuación.

- **Grupo de RF**

Permite determinar si el controlador en proceso (WLC Foráneo A) desea unirse al Grupo de RF con otros controladores; en este caso, se establecerá al WLC Foráneo B como miembro del grupo. Dado que se establecerá movilidad de Capa 2 entre los WLC, la función del WLC Foráneo A y B (independientemente) será sensar el medio de RF y obtener información a través de sus LAP asociados para optimizar los parámetros de cobertura en cada uno de los edificios.

En su funcionamiento, los LAP se encargan de transmiten paquetes de RRM con información de la potencia y SNR en la que encuentran trabajando, éstos paquetes contienen el nombre del Grupo de RF (grupo al cual se asociación los LAP y WLC) y el tiempo de latencia. El intercambio de mensajes entre LAP vecinos son validados entre ellos mismos a través de la información del campo de ***Group Name*** antes de enviar los mensajes al WLC.

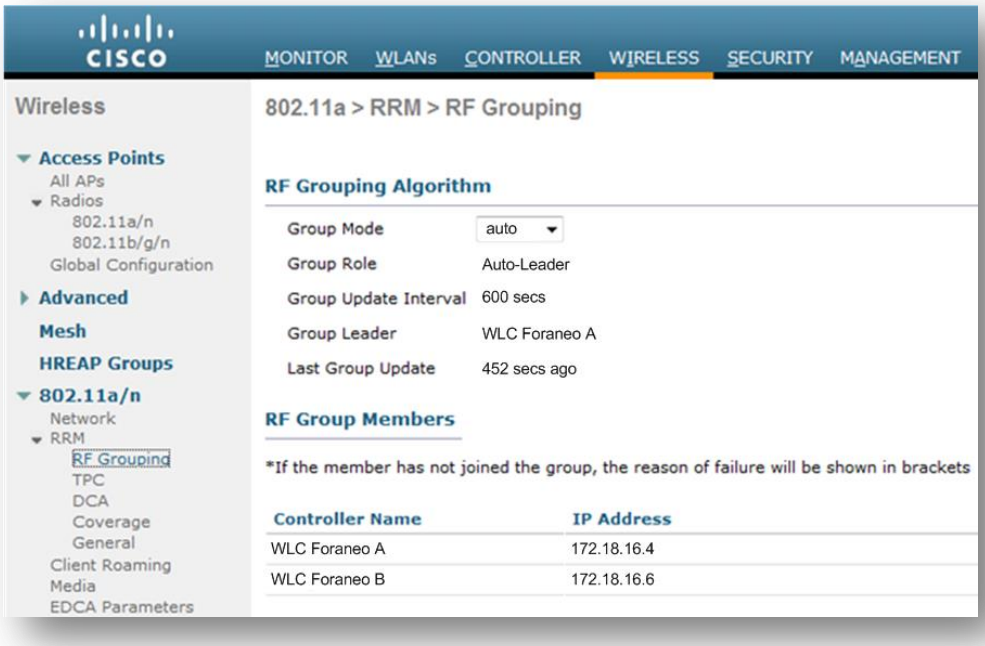


Figura 5.10 Asignación dinámica de parámetros de RF

- **Asignación de canales de RF**

Esta sección de configuración permite establecer la selección de canales de forma automática o manual (en este caso será automática). Además permite establecer parámetros como el porcentaje de solapamiento entre coberturas de los LAP.

Para observar a trevés de CLI el proceso de asignación automática de canales, véase Anexo A. Configuración automática del canal de RF

- **Asignación de nivel de potencia de transmisión**

En esta sección la configuración del nivel de potencia de transmisión puede ser asignada de forma manual o automática (de igual forma que en los canales, se recomienda establecerla de forma automática). En su funcionamiento de RRM los LAP a través del WLC ajustan automáticamente su nivel de potencia de transmisión para cubrir la mayor área de cobertura posible.

- **WIPS**

Una vez establecidos los parámetros anteriores; la solución propuesta establece un sistema de monitoreo para la prevención de intrusos inalámbricos. La integración del sistema WIPS como interfaz de visualización, nos proporciona una vista (Edificio A en el Piso 3) de los patrones de radiación de los LAP: AP1_JURIDICO_P3 y LAP AP2_JURIDICO_P3; obsérvese en la Figura 5.11 que esta interfaz indica un nivel de potencia menor en la zona central debido a las pérdidas por obstáculos, en este caso son paredes de concreto de aproximadamente 45 cm.

Aunado a lo anterior, obsérvese los dos puntos en cuadro azul señalados con su dirección MAC c7:4b:65:e4:33:00 y 04:45:e8:1c:35 respectivamente corresponden a los usuarios autorizados que actualmente se encuentran conectados al LAP; por el contrario, marcado con un círculo rojo con la dirección MAC 88:45:D9:AA:78:36, es referido a la detección de un intruso. Es importante verificar los detalles de la alarma emitida, puesto que WIPS detecta diversos tipos de posibles ataques tal es el caso de RF *Jamming* y DoS, *Man in the Middle*, etc.

Cabe señalar que al establecer este sistema de monitoreo se deben tener en cuenta las siguientes consideraciones:

- Los mapas de cada uno de los pisos de los edificios dónde se colocaron los LAP se insertaron manualmente en alguno de los siguientes formatos: DWD, BAK, DDWT, DWF, WMF.

- Los obstáculos se colocan manualmente en cada uno de los mapas de acuerdo al tipo de material de construcción (para mayor referencia de atenuación de la señal por materiales de construcción, diríjase al Capítulo 2).
- Las dimensiones entre los mapas deben ser proporcionales entre ellos.
- En su implementación, se debe establecer cuáles son los LAP asociados a cada uno de los pisos que conforman los edificios.

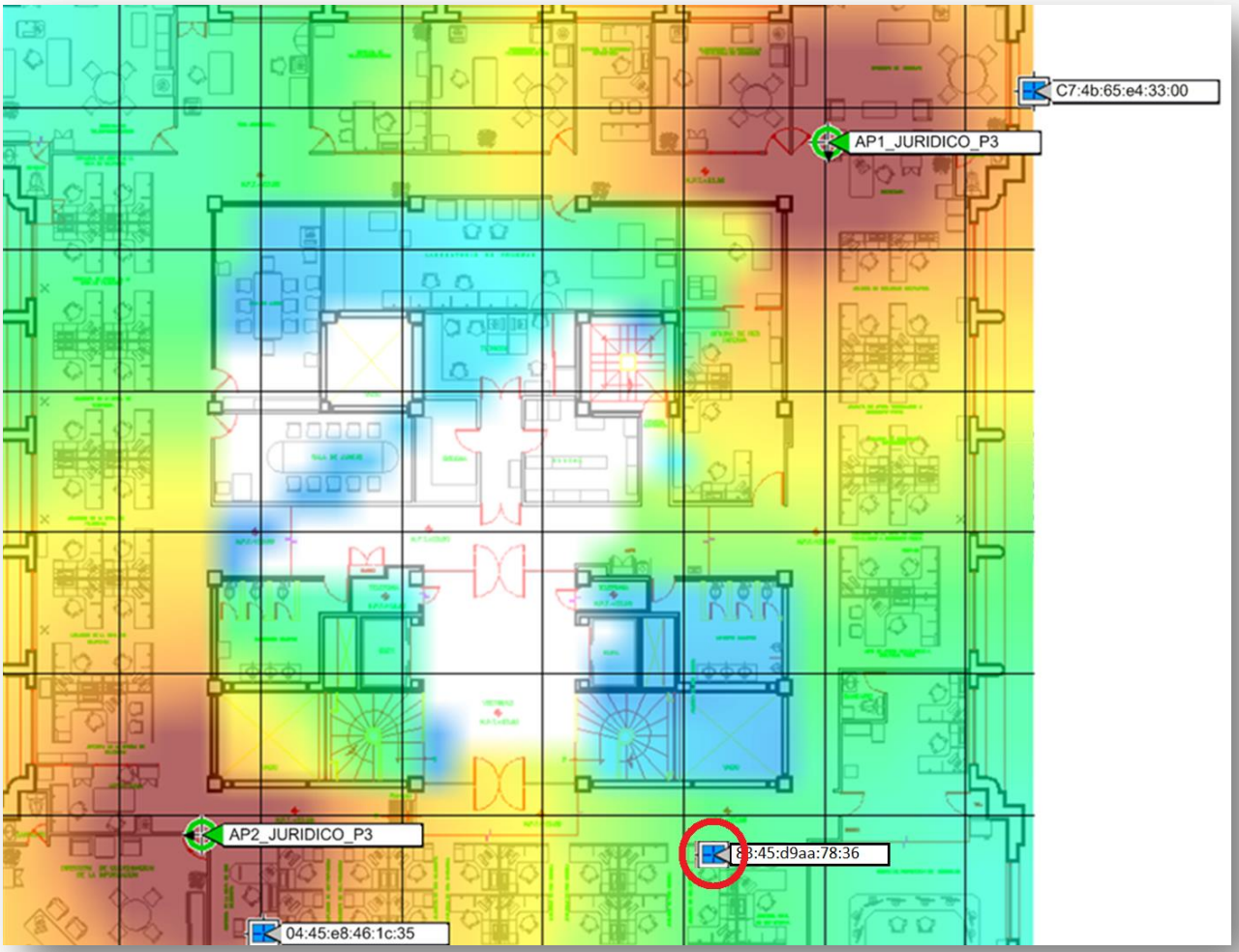


Figura 5.11 Sistema de monitoreo inalámbrico, WIPS

5.3.2 Controladores inalámbricos WLC

Los controladores inalámbricos son la parte esencial dentro de nuestro prototipo de red WLAN Empresarial Financiera, a través de ellos, se pretende centralizar los recursos y LAP para obtener un mejor desempeño y administración de la red WLAN, aunado a lograr el objetivo de integrar el Acceso a Usuarios Invitados a la red inalámbrica.

Los controladores que se manejarán en este diseño son los siguientes:

- **Controlador WLAN Foráneo (*Foreign* WLC)**

Se encargará de centralizar los LAP y dar acceso a la red interna (SSID internos o de red interna) a los usuarios de la Empresa Financiera. De igual forma sirve como puente para los usuarios que intentan conectarse a la red externa o Internet. Básicamente, el tráfico pasa a través de ellos por medio de un túnel hasta redirigirlo al WLC Ancla quien realmente permite el flujo de tráfico de los usuarios Invitados.

- **Controlador WLAN Ancla (*Anchor* WLC)**

Para establecer un sistema de Acceso a Usuarios Invitados, se introduce el WLC Ancla a la infraestructura de red WLAN Empresarial. Éste será el responsable de encaminar el tráfico del usuario invitado a la red de Internet.

El establecimiento de la DMZ en este punto del diseño permite que el usuario no quede totalmente expuesto a una red insegura como lo es propiamente Internet.

Al establecer políticas de seguridad es posible otorgar confianza al usuario, éstas políticas pueden ser tan sencillas o complicadas como la Empresa misma lo demande; para el prototipo de red WLAN de la Empresa Financiera, estas reglas incluyen un filtrado de direcciones *Web* de destino así como un portal de autenticación del usuario.

Algunos de los puertos permitidos sin poner en riesgo significativo a la red WLAN Empresarial se muestran en la Tabla 5.1.

Tabla 5.1 Puertos de acceso

Puerto	Tipo de comunicación
UDP 16666	Comunicación entre WLC*
IP ID 97	Tráfico de datos de los usuarios EoIP
TCP 161 y 162	SNMP
UDP 69	TFTP
TCP 80 y/o 443	HTTP y HTTPS
TCP 23 y 22	SSH y Telnet

* Véase Grupos de movilidad

- **Estructura física del Cisco WLC 5760**

Para la implementación de los controladores en la arquitectura de red WLAN Empresarial, se eligieron (de acuerdo al estudio realizado anteriormente) los dispositivos WLC del proveedor Cisco de la serie 5760. A continuación se muestra en la Figura 5.12 la estructura física y la distribución de puertos.

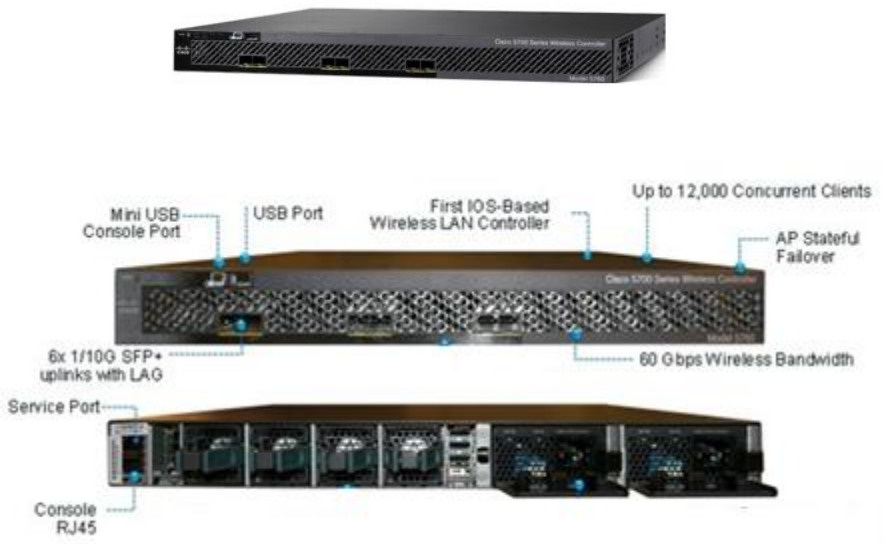


Figura 5.12 Estructura física del Cisco WLC 5760

NOTA: Este solo es un modelo de equipo del proveedor Cisco; sin embargo, estos dispositivos se encuentran de diferentes modelos y capacidades.

Las siguientes son características de los puertos del WLC 5760:

- Un Puerto de servicio: RJ-45 10/100/1000 Gigabit Ethernet

- Dos puertos de Consola: RJ45 y Mini USB

- Seis puertos de distribución: 6 10 Gigabit Ethernet, a través del cual puede manejar múltiples LAP. Cisco WLC 5760 soporta un máximo de 1000 LAP y hasta 12,000 usuarios bajo demanda.

5.3.2.1 Parámetros de inicio del WLC

Para iniciar la configuración del WLC, se tienen dos modos de ingreso: modo de consola a través del puerto de Consola RJ45 y con ayuda de la Interfaz de Línea de Comandos (CLI) o por medio de la Interfaz Gráfica de Usuario (GUI).

Es recomendable que en este punto, los administradores de la Red WLAN mantengan disponible una lista de las IP de los dispositivos a implementar y características del WLC; a manera de ejemplo, obsérvese la que se muestra en la Tabla 5.2 para el WLC Ancla.

Tabla 5.2 Direccionamiento del WLC Ancla

Dispositivo	VLAN	Dirección IP
Servidor DHCP	1	172.18.32.2
Pool de direcciones “Invitados”	300	172.18.42,20-172.18.42.120
DNS Server	NA	200.23.242.201/ 200.23.242.193
Default *Router*	Gateway	172.18.48.1 / 172.18.48.2
VLAN Administración	1	172.18.32.2
VLAN Invitados	300	172.18.48.12
VLAN Proyectos	400	172.18.64.12
Características WLC Ancla		
Máscara de red	255.255.240.0	
Dirección MAC	0026.0b04.596b	

En un esquema general los siguientes son los parámetros de arranque iniciales más importantes para tomar en cuenta en la configuración del WLC. Véase Anexo A para observar la línea de comandos para la configuración del WLC Ancla.

- Nombre de usuario y contraseña
- Nombre del Grupo de Movilidad *
- Región.
- Dirección de NTP.
- Interface de Administrador (VLAN, IP, DHCP, Puerto).
- Interface Virtual (1.1.1.1)
- Infraestructura a permitir 802.11 (a, b, g, n).

* NOTA: Este parámetro no podrá ser modificado en sesiones posteriores a menos que el equipo vuelva a su modo de inicio para su configuración.

Una vez ingresados los parámetros solicitados para la configuración del WLC Ancla se guardaron los cambios y se reinició el sistema. Para acceder nuevamente a la sesión de administración para continuar con la configuración a través de la GUI, se ingresa el usuario y contraseña (véase Figura 5.13).

Figura 5.13 Pantalla de inicio del WLC a través de la GUI

5.3.2.2 Configuración general del WLC

Para conocer las características generales de configuración del WLC (ejemplificando se utilizará el WLC Ancla), la GUI nos muestra a través de su interfaz, la opción dinámica de revisar y en dado caso, modificar las características del WLC. En la Figura 5.14 se muestra la configuración general para el WLC Ancla.

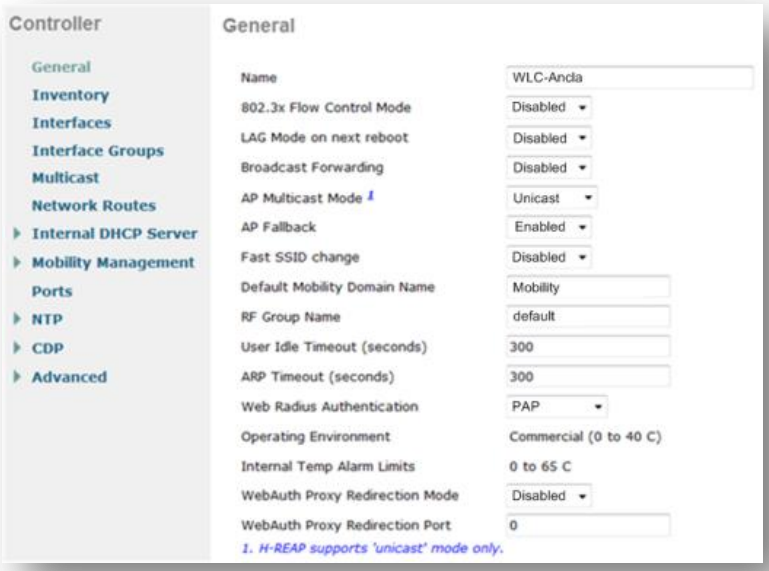


Figura 5.14 Configuración general del WLC Ancla

5.3.2.3 Interfaces WLC

En el concepto de interfaz, se tienen dos tipos: interfaces físicas y lógicas, como se describen a continuación.

1. Una interfaz física WLC o puerto es una entidad física que se utiliza para las conexiones en el controlador. Cada puerto del Cisco WLC puede ser configurado como un enlace troncal IEEE 802.1Q el cual permitirá transportar más de una VLAN entre dispositivos de red.

2. En general existen cuatro tipos de interfaces lógicas disponibles en el WLC (para el modelo Cisco 5760).

- **Interfaz de administración *(Managment interface)*.** Esta interfaz se utiliza para las comunicaciones a nivel de Capa 2 entre WLC y el LAP en la red. También es la interfaz utilizada para terminar túneles EoIP que se originan a partir de los controladores foráneos. Es importante establecer el direccionamiento IP en la misma subred en los WLC para poder implementar movilidad en Capa 2.

- **Interfaz de puerto de servicio *(Service-Port)*.** Se asigna estáticamente por el sistema sólo al puerto de servicio físico. Este puerto es generalmente reservado para gestionar la red en caso de falla.

- **Interfaz virtual *(Virtual Interface)*.** La literatura recomienda definir dicha interfaz con una dirección IP 1.1.1.1, ésta interfaz se utiliza para apoyar la gestión de movilidad; así mismo, se utiliza como la dirección de origen cuando el controlador ancla dirige a los usuarios invitados al portal web de autenticación. Esta dirección IP debe ser definida de igual forma para todos los WLC miembros del grupo de movilidad esto con el fin de permitir la movilidad sin fisuras.

- **Interfaz dinámica *(Dynamic Interface)*.** Se definen cada una de las interfaces de las redes WLAN a difundir; el WLC 5760 puede soportar hasta 64 interfaces dinámicas. Estas interfaces son designadas por el administrador de red WLAN y son análogas a las VLAN.

NOTA: La creación de las interfaces de administración y virtual se crean en la configuración inicial del WLC

En la Figura 5.15 se muestra la relación entre interfaces.

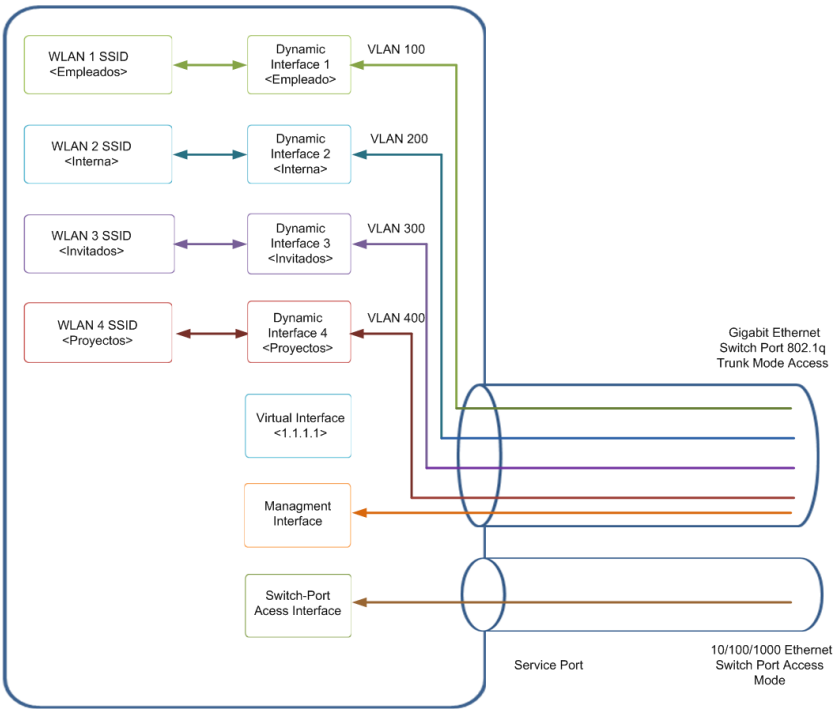


Figura 5.15 Interfaces WLC

En general, una interfaz lógica se creó de la siguiente manera, en la opción de ***Controller*** dentro de la GUI se accedió a la pestaña ***Interfaces*** y se seleccionó ***New.*** SeInsertó el nombre de la interfaz a añadir y la VLAN a la que pertenece.

Dado que en la configuración del WLC se crearon las interfaces de Administrador, Virtual y Puerto de Servicio. A manera de ejemplo, a continuación se indica cómo se creó una de las interfaces dinámica para el WLC Ancla, véase Figura 5.16.

Figura 5.16 Interfaz dinámica *Invitados*

Una vez creado el nombre de la interfaz Invitados y la VLAN a la que pertenece se colocó la información específica que definirá a la interfaz, refiérase a la Figura 5.17 para observar la información proporcionada para la interfaz Invitados.

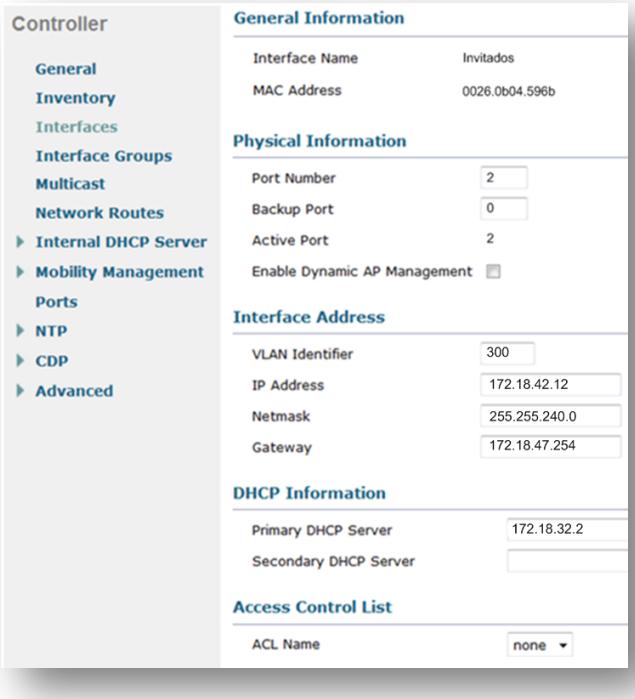


Figura 5.17 Información general de la interfaz dinámica Invitados

El mismo proceso se realizó para la interfaz Proyectos. Quedando la sección de interfaces como se muestra en la Figura 5.18.

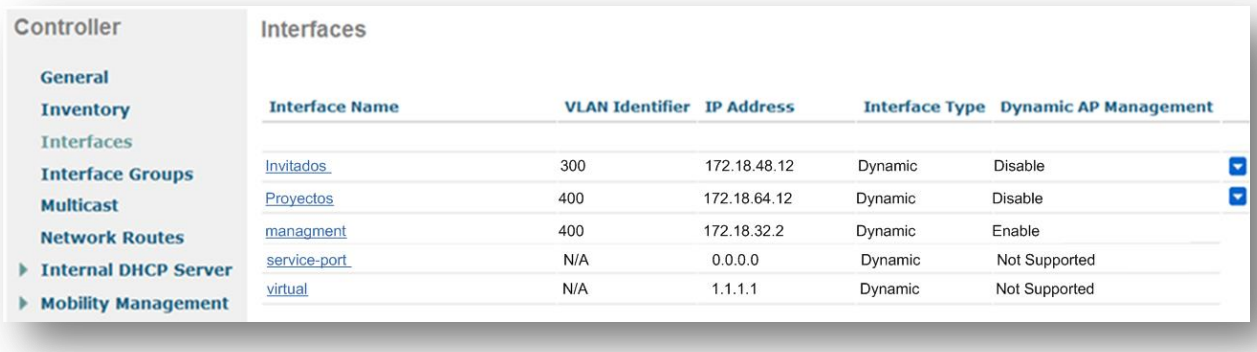


Figura 5.18 Lista de interfaces dentro del WLC Ancla

5.3.2.4 Creación y configuración de redes WLAN

Una red WLAN asocia un SSID a una interfaz dinámica la cual se configuró en este caso con la seguridad correspondiente. A continuación se mostrarán los pasos generales que se siguieron para la creación de una red WLAN la cual tendrá difusión a través del SSID "Invitados".

Para iniciar la configuración, nos dirigimos a la pestaña WLAN en la GUI y se seleccionó ***Create New>Go*** como se muestra en la Figura 5.19.

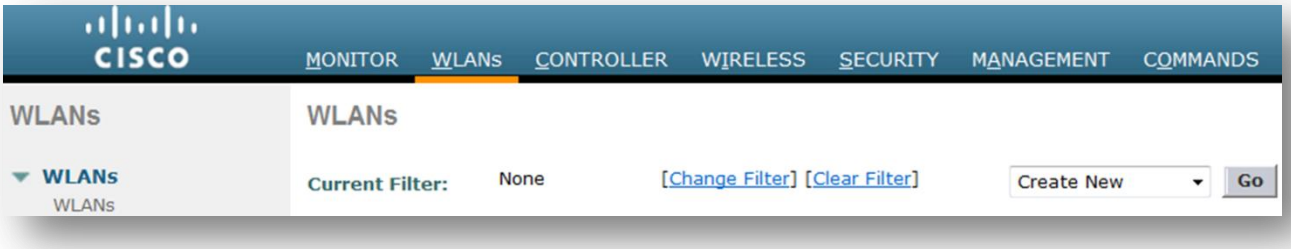


Figura 5.19 Creación de una red WLAN

La página que se despliega es como la observada en la Figura 5.20; dentro de ésta se procedió a llenar los campos de datos solicitados con la información de la red WLAN, en este caso la red WLAN Invitados

NOTA: Para el WLC Ancla se tienen dos redes WLAN: Invitados y Proyectos; para generalizar, sólo se dará la explicación para la red Invitados.

Figura 5.20 Creación de red WLAN Invitados

Hasta este momento se creó el SSID Invitados, véase Figura 5.21, su estado ya se encuentra activo. Ahora corresponde integrar las políticas de seguridad así como de QoS.

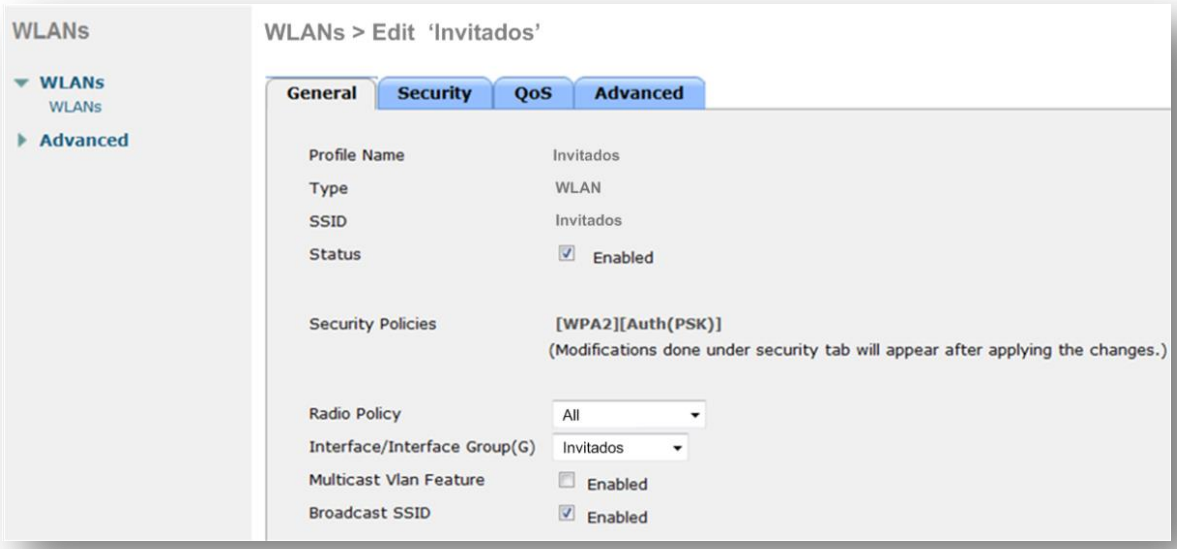


Figura 5.21 Configuración general de la red WLAN Invitados

Para la red de Invitados se dispondrá de seguridad de capa 2 y capa 3 (véase Figura 5.22 y 5.23) en la primera, se establece una autenticación WPA+WPA2 con un cifrado y políticas AES, y con una llave de autenticación PSK.

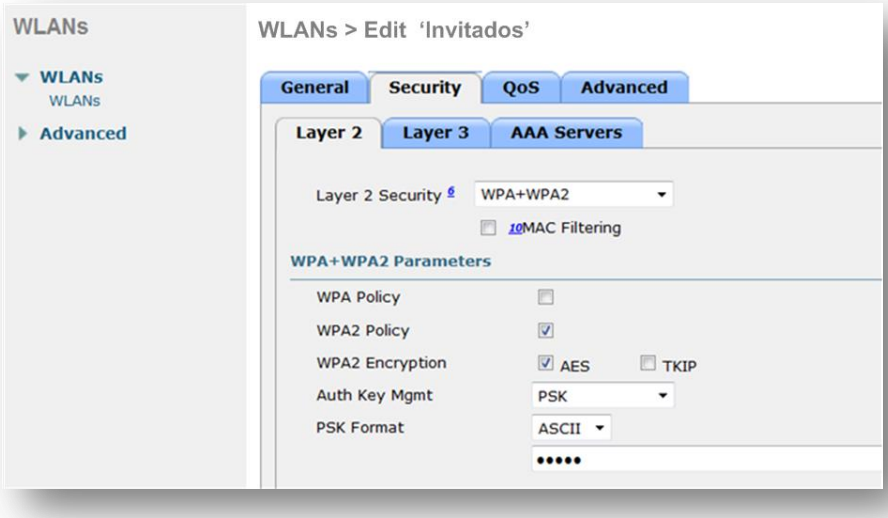


Figura 5.22 Configuración de seguridad en Capa 2

En Capa 3 se establecen las políticas de autenticación para que el usuario invitado acceda a la red DMZ a través del portal Web de autenticación (véase configuración del portal Web).

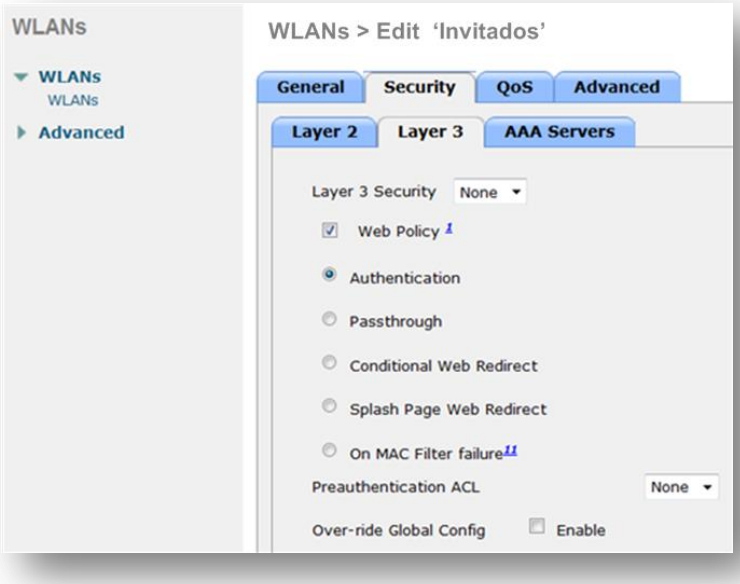


Figura 5.23 Configuración de seguridad en Capa 3

La configuración de los servidores AAA (Autenticación, Autorización, Auditoría) quedará establecida por los valores preestablecidos (véase Figura 5.24), ya que en esta red WLAN Invitados no estamos configurando una autenticación tipo IEEE 802.1x

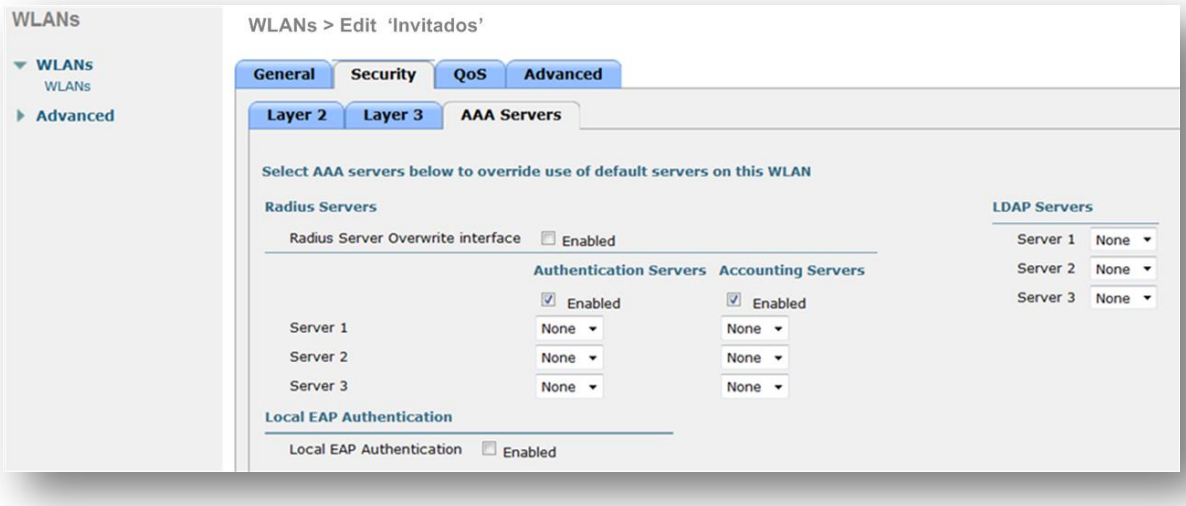


Figura 5.24 Configuración por *default* de AAA

En el establecimiento de calidad de servicio para la red de Invitados, ésta se definirá con un nivel Plata; es decir, manejará un 30 % de ancho de banda de la red inalámbrica para la red de usuarios invitados, véase Figura 5.25.

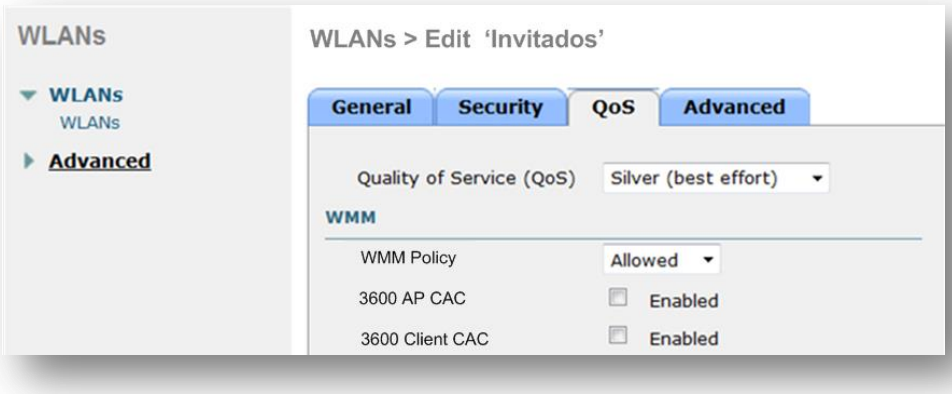


Figura 5.25 Configuración de QoS para la red WLAN Invitados

NOTA: Se realizó el mismo procedimiento para todas las redes WLAN que se desean difundir a través del WLC correspondiente

5.3.3 Servidor DHCP

Para las redes WLAN internas, es decir, en los WLC foráneos, se establece el siguiente tipo de servidor DHCP.

- **Interno.** El servidor interno de direccionamiento proporciona direcciones DHCP a los usuarios inalámbricos de las redes WLAN internas y LAP. Cuando se desea utilizar el servidor DHCP interno para el caso de los WLC Foráneos, debe establecerse la dirección IP del servidor DHCP al cual se encuentre conectada la red WLAN.

En el caso de la red de Invitados, el WLC actúa como un agente de retransmisor de DHCP para los usuarios asociados a la WLAN Invitados y Proyectos se presenta el siguiente servidor DHCP.

- **Virtual.** El sistema operativo del WLC está diseñado para otorgar direccionamiento a la red de Invitados como un servidor DHCP a través de un *pool* de direcciones IP. Además, cada WLC Ancla aparece como un agente de servidor DHCP el cual se encarga de direccionar a los usuarios Invitados a la IP virtual de la página Web del portal.

Las principales ventajas que se obtienen al incorporar el anterior diseño de operación del DHCP, sobre el WLC Ancla son:

- Se elimina la necesidad de realizar solicitudes DHCP más allá del WLC.
- Al convertirse el WLC en parte del proceso de DHCP, el controlador inalámbrico mantiene actualizado una base de datos de las direcciones MAC/ IP de los clientes conectados a las redes WLAN, lo que le permite hacer cumplir con las políticas de DHCP y mitigar una posible suplantación de IP o de ataque DoS

Para su funcionamiento dentro de la red inalámbrica Empresarial, el DHCP Virtual se configuró para cada una de las interfaces dinámicas del WLC Ancla (ej. Invitados, Proyectos). Y en el caso de las interfaces de los WLC Foráneos, se estableció el direccionamiento del DHCP Interno.

5.3.3.1 Configuración DHCP

En la interfaz GUI, se seleccionó la pestaña ***Controller*** y se ingresó en la opción ***Internal DHCP Server > DHCP Scoope > New***. En este caso se colocó el nombre de la interfaz DHCP_Invitados, véase Figura 5.26.

Figura 5.26 Creación de DHCP en la red WLAN Invitados

A continuación, se colocaron los elementos requeridos para la integración del DHCP en la interfaz Invitados (véase Figura 5.27).

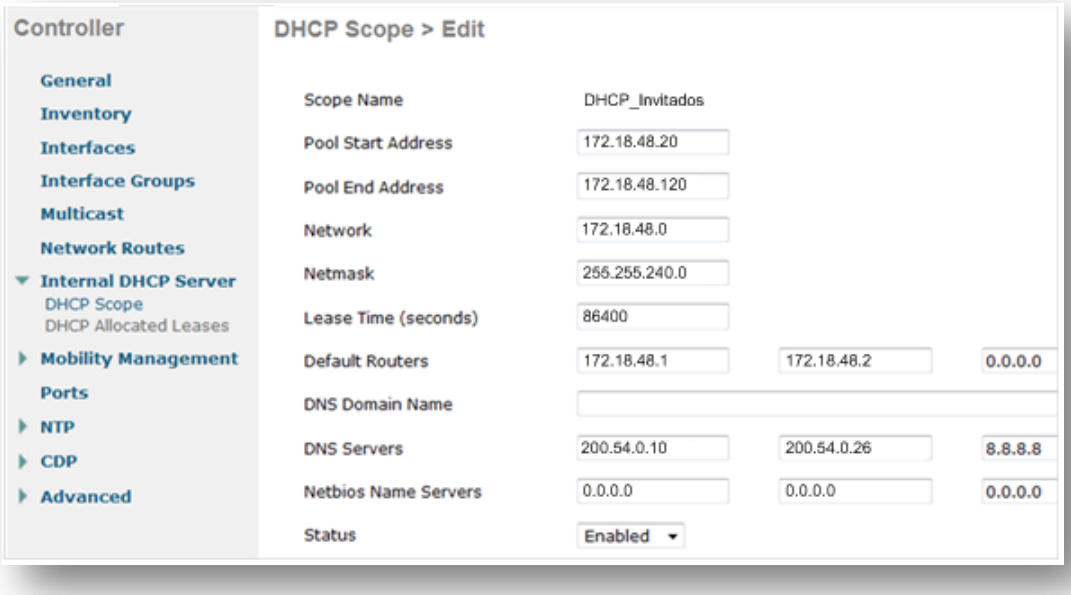


Figura 5.27 Configuración de DHCP en la red WLAN Invitados

A través del mismo procedimiento de configuración y con sus respectivos elementos, se creó el DHCP para cada una de las interfaces del WLC Ancla como se muestra en la Figura 5.28. Obsérvese que cada una de las redes WLAN se encuentra configurado con un *pool* de direcciones dinámicas, éstas fueron definidas para soportar un número de 100 usuarios invitados por SSID.

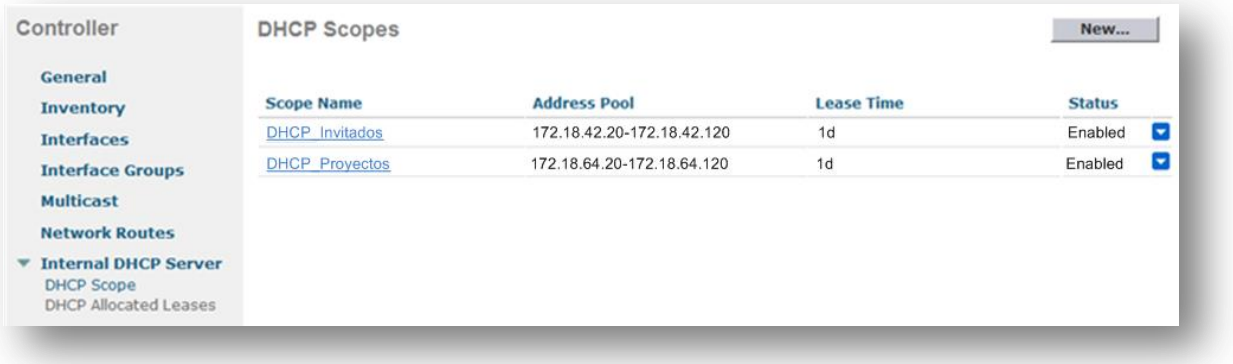


Figura 5.28 Lista de DHCP en interfaces del WLC Ancla

5.3.4 Movilidad y Grupos de Movilidad

La movilidad es una de las principales razones dentro del prototipo de diseño de red WLAN. En este caso, la movilidad será referida a la capacidad que tiene el sistema inalámbrico para permitir que el usuario final pueda establecer comunicación a través de su dispositivo móvil en los diferentes puntos de acceso distribuidos en los edificios de la Empresa Financiera.

En un primer escenario, el proceso de movilidad que se establece en este proyecto es manejado a nivel de Capa 2; es decir, el usuario puede moverse entre dos LAP conectados a un mismo WLC o dos LAP conectados a WLC diferentes respectivamente.

Cuando los usuarios inalámbricos asociados se autentican en el WLC a través de un LAP, los datos del dispositivo móvil son colocados en una base de datos, esta entrada incluye entre los datos más importantes la MAC del dispositivo inalámbrico, dirección IP, tipo de seguridad, QoS y el LAP al cual se encuentra asociado. El WLC utiliza esta información para gestionar el tráfico para y desde el usuario (véase Figura 5.29).

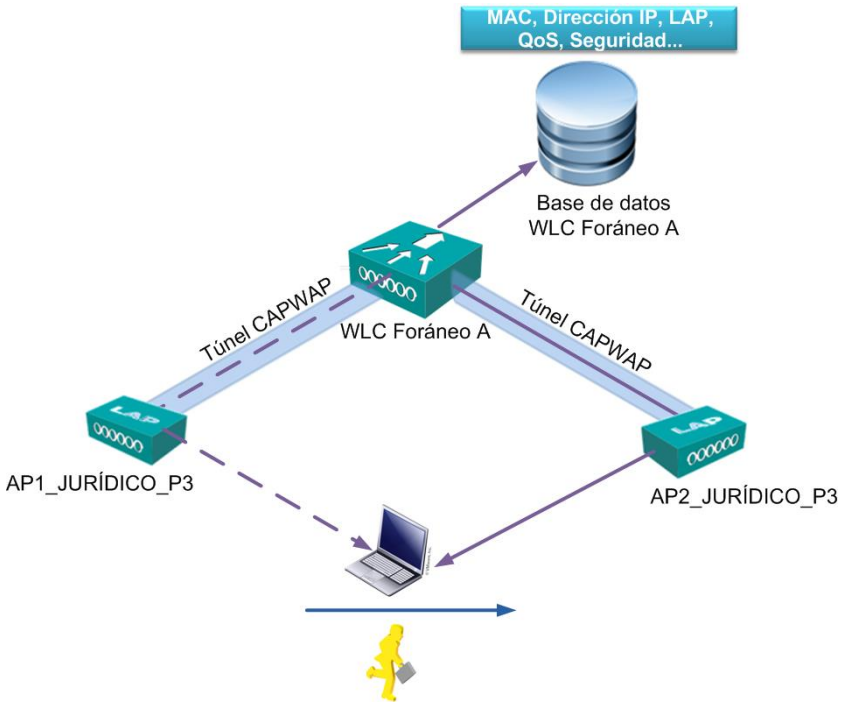


Figura 5.29 Movilidad entre dos LAP

Cuando el usuario inalámbrico realiza un proceso de movilidad de un LAP a otro LAP en un mismo WLC, éste simplemente actualiza su base de datos con en el nuevo el usuario y LAP asociado.

El segundo esquema de movilidad en Capa 2 es referido a un usuario que se desplaza del WLC Foráneo A al WLC Foráneo B.

Antes de especificar el proceso anteriormente mencionado se tienen las siguientes recomendaciones para una mejor implementación de movilidad en Capa 2:

- Todos los controladores deben tener sus interfaces WLAN con un direccionamiento IP en la misma subred.
- Debe existir conectividad IP entre las interfaces de administración de los WLC perteneciente al grupo Mobility (para este esquema).
- Es necesario que todos los controladores que se utilicen para crear movilidad en Capa 2 tengan el mismo nombre del grupo de movilidad.

Una vez establecidas las anteriores condiciones, el proceso de movilidad entre dos LAP que se encuentran en diferentes WLC se ilustra en la Figura 5.30, en el cual se observa el

intercambio de mensajes MME (*Mobility Message Exchange*) en los cuales se tiene la información de las credenciales del usuario para actualizar la base de datos del WLC B con los datos del usuario del WLC A.

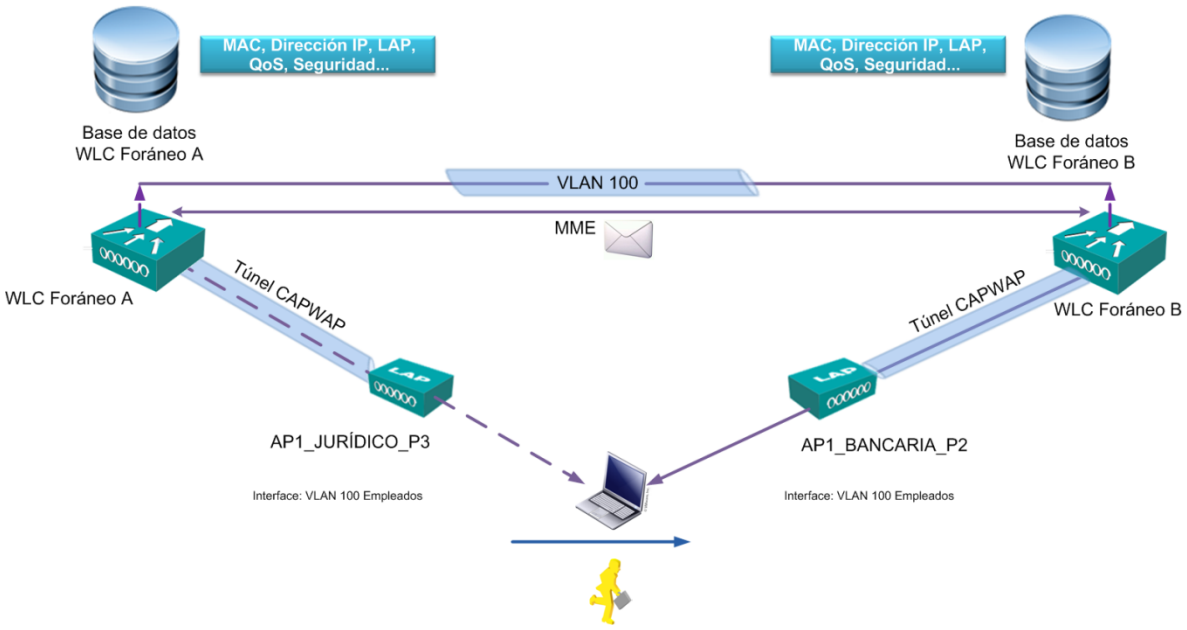


Figura 5.30 Movilidad intra-WLC

- **Grupos de movilidad**

Los grupos de movilidad son grupos de WLC que en conjunto actúan como una sola WLC virtual intercambiando información de los LAP e información de RF. Un WLC dentro de un dominio de movilidad es capaz de tomar sus propias decisiones sobre los datos recibidos de los otros miembros del grupo de movilidad, en lugar de confiar únicamente en la información contenida en sus LAP asociados y clientes conectados a éstos.

El propósito principal de un grupo de movilidad es la creación de un dominio WLAN virtual (a través de múltiples WLC) con el fin de proporcionar una visión global de un área de cobertura inalámbrica.

Para su comunicación, el grupo de movilidad forma un conjunto de túneles autenticados entre los WLC miembros de dicho grupo, de éste modo los WLC pueden comunicarse directamente entre ellos, véase Figura 5.31.

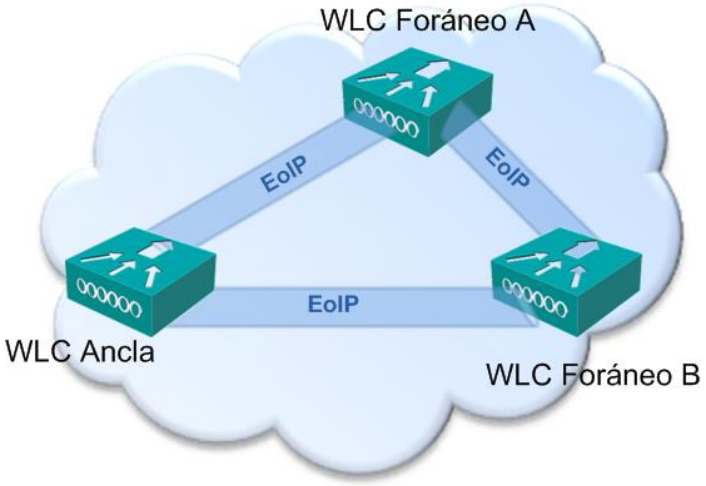


Figura 5.31 Grupo de Movilidad

5.3.4.1 Configuración de Grupo de Movilidad

Antes de comenzar la creación del grupo de movilidad para el Prototipo de red WLAN Empresarial, se recomienda (por literatura) tener en consideración los siguientes puntos:

- Con fines de escalabilidad, un grupo de movilidad puede soportar hasta 24 controladores y 3600 LAP.
- Los WLC no tienen que ser del mismo modelo; sin embargo, se recomienda que los WLC tengan la misma versión de *firmaware*.
- Es indispensable que el grupo de movilidad mantenga la mima dirección IP virtual (definido como 1.1.1.1).
- **Cada WLC debe tener el mismo nombre de dominio del grupo de movilidad** (en este caso se definió como **Mobility**) y es preciso definir cada WLC en la lista de los demás como un miembro dentro de la lista de compañeros del grupo de movilidad.
- Para que los usuarios inalámbricos internos puedan moverse sin problemas entre los LAP, es necesario configurar todas las redes WLAN con los niveles de

seguridad idénticos.

El objetivo en este punto será la configuración de uno de los WLC Foráneos en el Grupo de Movilidad, definido en la configuración inicial del WLC Ancla como **Mobility**, Dentro de la interfaz GUI, en la pestaña ***Controller***, se eligió la opción ***Mobility Managment > Mobility Groups > New***.

El procedimiento para la integración del WLC foráneo dentro del grupo Mobility, se muestra en la Figura 5.32. En este caso la dirección IP, corresponderá a la IP de Administración del WLC Foráneo A.

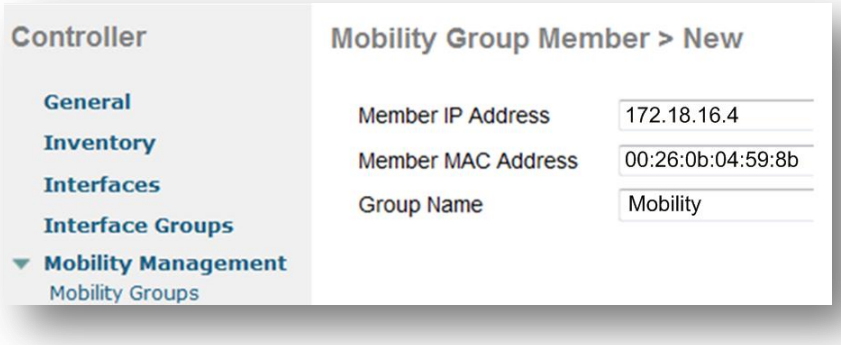


Figura 5.32 Grupo de movilidad: *Mobility*

Ingresado el WLC foráneo A al Grupo de Movilidad, es posible observar dentro de la GUI la lista de los WLC que pertenecen a dicho grupo. Como se puede observar en la Figura 5.33, el Grupo se encuentra conformado por el WLC Ancla y el WLC Foráneo A y el WLC foráneo B el cual se ingresó posteriormente al grupo.

NOTA: Se realizó la misma operación en cada uno de los WLC.

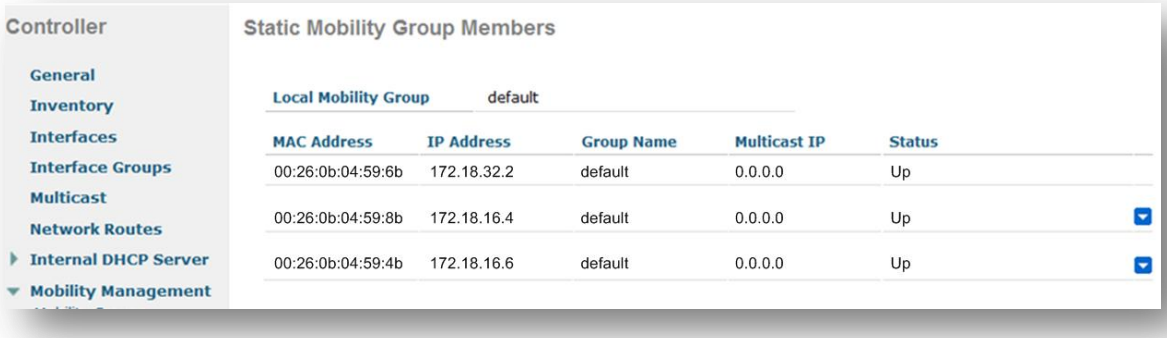


Figura 5.33 Lista de los WLC que pertenecen al grupo *Mobility*

5.3.4.2 Configuración del Ancla

En la configuración del Ancla, se definirá quién es el controlador Ancla, nótese que hasta este momento sólo se le dio el nombre de WLC Ancla a uno de los controladores que conforman el diseño más no se ha definido su rol dentro de los WLC foráneos y en el mismo WLC Ancla.

A continuación se indicará el establecimiento de la arquitectura de anclaje dentro del WLC Foráneo A y en el mismo WLC Ancla.

- **Anclaje entre el WLC Foráneo A y el WLC Ancla**

El proceso de anclaje se realiza para cada una de las WLAN que conforman al WLC Foráneo, en este caso se tienen las redes WLAN con los siguientes SSID: Empleados, Interna, Invitados y Proyectos.

Dentro de la GUI, se seleccionó la opción de ***Mobility Anchors*** como se muestra en la Figura 5.34 y se eligieron las redes WLAN con SSID “Invitados” y “Proyectos” las cuales se alojarán en el WLC Ancla para dar sólo acceso a Internet.

Figura 5.34 Lista de las WLAN del controlador WLC foráneo A

En la opción de ***Mobility Anchor Create*** se insertó la dirección IP de Administración del WLC Ancla (véase Figura 5.35). De esta forma quedará establecido que el usuario que acceda a la red WLAN Invitados a través del WLC Foráneo A será anclado al WLC Ancla el cual le proporcionará salida a Internet a los usuarios invitados.

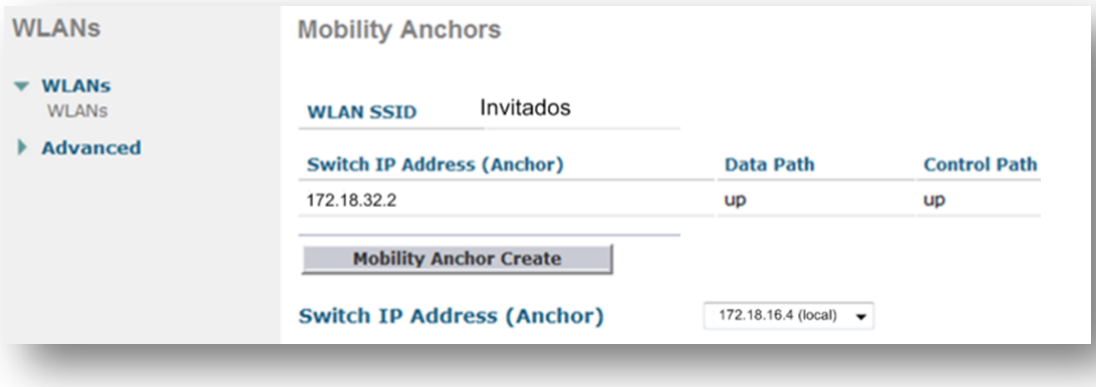


Figura 5.35 Anclaje de la red WLAN Invitados del WLC Foráneo A

El mismo procedimiento se realizó para la red WLAN Proyectos y en cada uno de los controladores Foráneos como se muestra en la Figura 5.36.

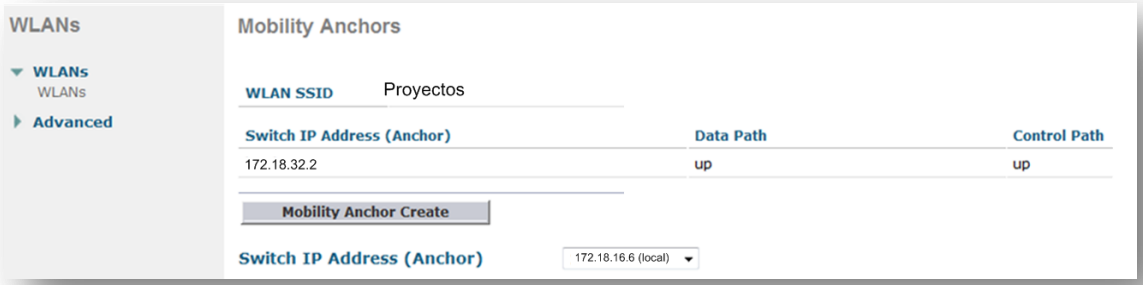


Figura 5.36 Anclaje de la red WLAN Proyectos del WLC Foráneo B

- **Anclaje en el WLC Ancla**

En este segundo proceso se define el anclaje en el WLC Ancla, el cual corresponde definir que el WLC Ancla es la misma ancla para el proceso de Acceso a Usuarios Invitados.

Ingresando a la GUI del WLC Ancla, observamos las redes WLAN definidas (véase Figura 5.37). Al contrario del WLC foráneo, en este caso se define la dirección del ancla como la dirección IP de administración (172.18.32.2) del mismo WLC Ancla

Para su configuración, en la opción de ***Mobility Anchor Create*** se estableció, como ya se mencionó anteriormente, la dirección IP de Administración del mismo WLC Ancla.

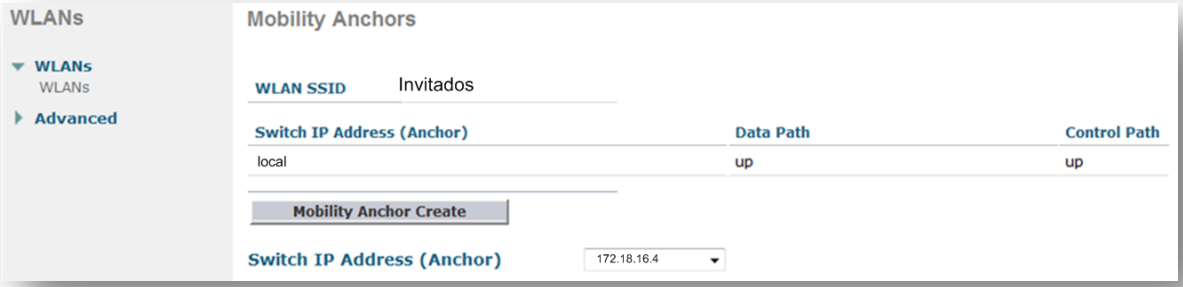


Figura 5.37 Anclaje de la red WLAN Invitados del WLC Ancla

De esta forma queda establecido el esquema general de la comunicación entre los WLC foráneos y el WLC Ancla.

5.3.5 Portal de autenticación

El portal Web de autenticación se encuentra directamente asociado al WLC Ancla. Cuando una red WLAN está configurado para emplear la política de autenticación vía Web (preestablecida en la configuración de la red WLAN Invitados) automáticamente la solicitud se redirige al portal de autenticación de la Empresa (véase Figura 5.38).

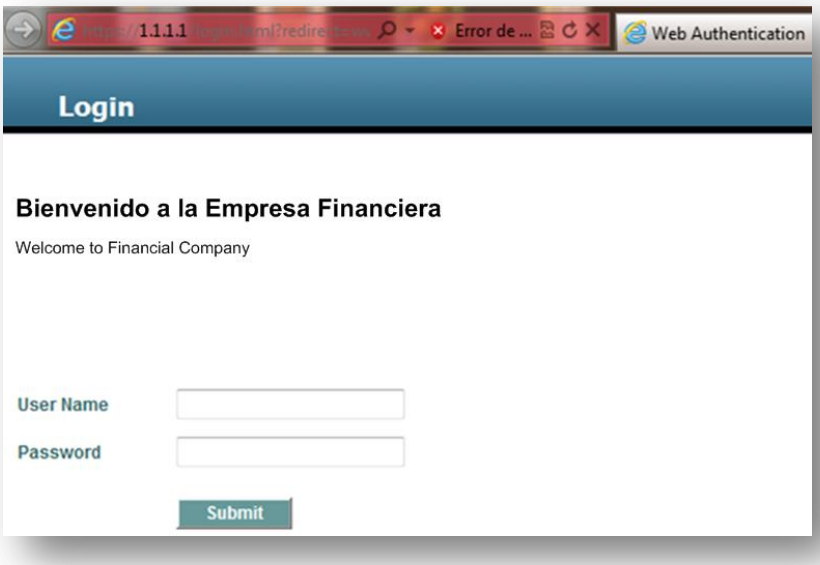


Figura 5.38 Portal de autenticación de la Empresa Financiera

5.3.5.1 Configuración del Portal de Autenticación

Para la configuración del Portal de Autenticación, se accedió dentro de la GUI del WLC Ancla y se seleccionó (como se observa en la Figura 5.39) en la pestaña ***Security*** la opción ***Web Auth > Web Login Page.***

La opción de ***Internal (Default)*** se eligió refiriéndose a que el portal de autenticación se encontrará dentro del Servidor Web Interno. En la configuración de la interfaz del portal se colocaron los mensajes que proporcionarían información acerca del portal. Aunado a lo anterior, se proporciona la opción de redirigir al usuario a una página principal después de haber sido exitosa la autenticación, para este caso se redirigió a la dirección web de la Empresa Financiera.

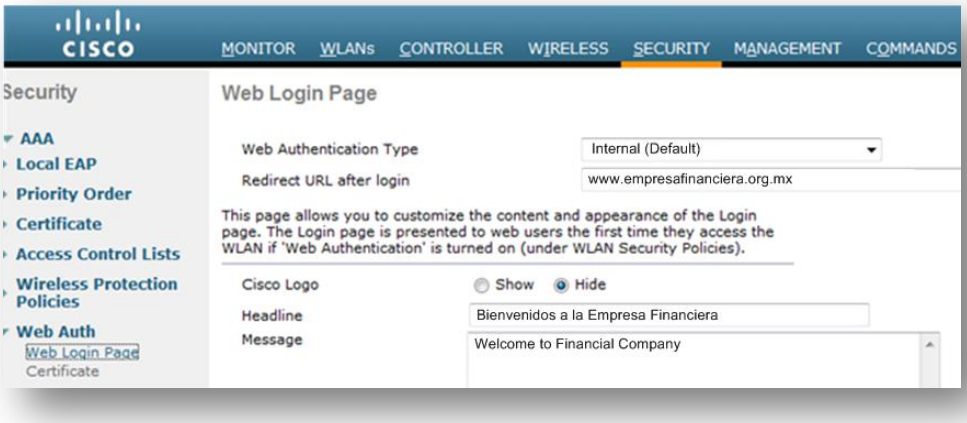


Figura 5.39 Configuración del Portal de Autenticación

5.3.5.2 Creación de credenciales

La forma de autenticación que empleará el usuario invitado consistirá en la introducción de sus credenciales en el portal de autenticación. A partir de la GUI, el administrador de red puede crear dicha credencial basada en usuario y contraseña (véase Figura 5.40).

Al utilizar este sistema, se tienen tres ventajas principales:

- Se establece un tiempo predeterminado para el acceso a la red de Invitados, lo que permite a los administradores no invertir recursos en desactivar las cuentas que se encuentren sin operar.

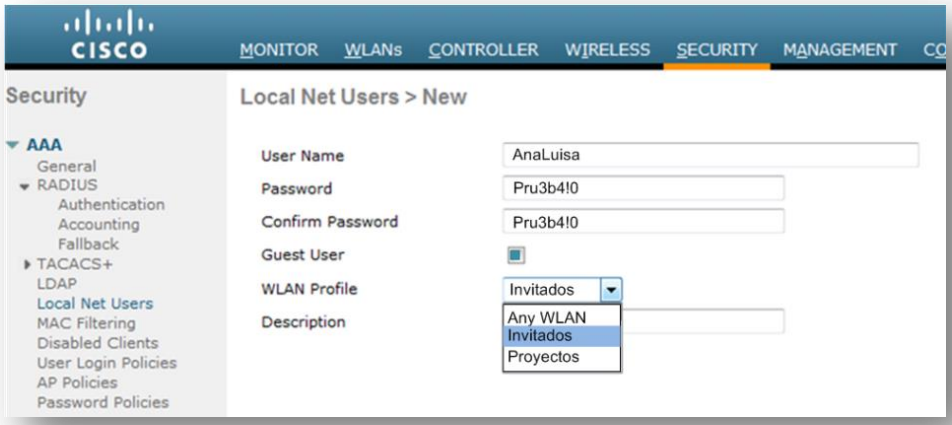


Figura 5.40 Credencial de Usuario Invitado

- Como se mencionó anteriormente el WLC permite establecer un control de MAC y direcciones IP, lo que proporciona un grado de seguridad al dejar establecido que sólo el dispositivo del usuario invitado con el que accedió por primera vez a la red de Invitados podrá establecer nuevamente una sesión.

- Dado que el WLC maneja un sistema de alarmas de intrusión a la red, por ejemplo DoS, la interfaz GUI permite bloquear al usuario que se encuentra interfiriendo en la red WLAN.

NOTA: La creación de las credenciales estará asignada por el área de Telecomunicaciones (área encargada de proporcionar, entre sus actividades, soporte técnico de la red WLAN)

5.4 Resultados del prototipo de diseño de red WLAN 802.11

El prototipo de diseño de red WLAN 802.11 segura y su integración dentro de la red Empresarial, permitió establecer como resultado un conjunto de características como se enlistan a continuación.

- Se centralizó la red WLAN, permitiendo a los administradores de la red inalámbricas establecer políticas claras de seguridad y monitoreo.

- Se estableció la tendencia de Acceso a Usuarios Invitados, otorgando seguridad a la red interna inalámbrica y permitiendo a los usuarios invitados establecer una comunicación inalámbrica desde sus dispositivos inalámbricos y así obtener una mejora en la colaboración empresarial.

- La incorporación de la Tendencia, señalada en el punto anterior, permitió a los administradores de la red tener un control de los usuarios invitados que intentan acceder a la red WLAN.

- Queda establecido un diseño de red WLAN para integrar la solución BYOD, cuyo objetivo de la Empresa Financiera es la integración de correo electrónico y acceso a aplicaciones internas de la Empresa.

- La seguridad de la red WLAN se establece en un grado fuerte; ya que al implementar autenticación tanto para usuarios invitados (a través del portal de autenticación por medio del protocolo WPA2) como usuarios internos (a través de certificados 802.1x) el flujo de datos se realiza a través de un sistema seguro.

- La incorporación de movilidad en los edificios proporciona una nueva perspectiva de trabajo al establecer una amplia cobertura en las áreas de trabajo.

- Al establecer QoS en este sistema centralizado, se establece un servicio diferenciado al tráfico el cual permite gestionar los recursos de la red de una forma más eficiente.

- La implementación del sistema de monitoreo queda establecido en su etapa inicial. Al ser puesto en prueba dentro del diseño de red se obtiene información de los LAP y usuarios que se encuentran conectados a la red WLAN dando una perspectiva dinámica para la administración de los LAP y la conexión a los mismos por parte de los usuarios.

Capítulo 6

CONCLUSIÓN

Investigación, estudio de mercado, planteamiento, estructuración y puesta en prueba, son los elementos que engloban el proyecto: "Integración de una red empresarial WLAN 802.11 segura de última generación".

Este trabajo trae consigo un conjunto de información referenciada de los aspectos generales para la integración de una red WLAN en el ámbito empresarial. La recaudación de datos actuales del mercado de soluciones inalámbricas, su diseño e implementación permitió establecer políticas de seguridad y la centralización de su infraestructura para la administración de la red WLAN de la Empresa Financiera.

La aplicación de conocimientos, estrategia, visualización de diseño, a través de la Empresa piloto, permite dejar esta Tesis como elemento principal para la implementación de redes WLAN empresariales de cuarta generación.

Presentado lo anterior, en este capítulo se presentan las conclusiones del prototipo de red WLAN 802.11 empresarial segura para la integración de la tendencia de Acceso Usuarios Invitados y el planteamiento de futuros trabajos para este proyecto.

6.1 Conclusiones

La tecnología WLAN ha permitido el establecimiento de diversos diseños de red inalámbrica, su incorporación definida a través de los estándares IEEE 802.11 permite la implementación de las diversas soluciones de tecnología inalámbrica en las redes empresariales independientemente de los proveedores de soluciones WLAN.

El impulso de este proyecto fue debido al aumento exponencial e incorporación de dispositivos de comunicación inalámbricos en la Empresa Financiera, lo que tuvo como consecuencia un alto impacto en la seguridad y en salvaguardar la información sensible.

El alto consumo de recursos multimedia y el panorama de dar acceso a través de la red inalámbrica interna a usuarios externos permitió establecer las bases necesarias para la propuesta, diseño y reestructuración de red WLAN Empresarial segura que hoy se muestra en la presente Tesis.

El panorama de movilidad que se establece y la incorporación de usuarios invitados a la Empresa Financiera permitieron establecer el conjunto de políticas de seguridad necesarias y la centralización de administración de la red inalámbrica de la Empresa.

El impacto obtenido en primera instancia fue la eficiente administración y la disminución de recursos por parte del área de Telecomunicaciones para establecer acceso a la red inalámbrica. Consecuentemente, se logró establecer una administración de los recursos multimedia al establecer QoS dentro del servicio y eliminar la centralización de dichos recursos por unos cuantos usuarios.

Se abrió un nuevo panorama de movilidad al dar acceso a Internet a Usuarios Invitados, a través de sus propios dispositivos móviles, no sin antes salvaguardar la red interna y establecer políticas de seguridad para dar acceso a los mismos usuarios a través de un portal de autenticación, mismo que es controlado por un WLC Ancla que permite a través de su interfaz dar un seguimiento de monitoreo de los dispositivos que se encuentran accediendo a Internet desde el esquema *Invitados.*

La introducción de conceptos como controladores permitió esencialmente, la incorporación de este prototipo de diseño de red inalámbrica; mismos dispositivos que permiten establecer el conjunto de políticas de seguridad (siempre y cuando la empresa cuente con elementos como DHCP, RADIUS, DNS, AC, AD, etc).

La tecnología de AP centralizados, no solo disminuyó la carga de procesamiento de tráfico de la red inalámbrica en éstos, si no también se encargó de establecer un mecanismo de auto configuración de RF al emplear mecanismos de autocanalización y monitoreo del medio de RF para establecer sus características como antena transmisora-receptora y aumentar el área de cobertura y disminuir la disminución de potencia por interferencia.

El mercado de las soluciones WLAN es amplio y los proveedores que promueven estas soluciones son variados; sin embargo, es responsabilidad de los ingenieros de la red WLAN empresarial establecer el mejor dimensionamiento y crear un estudio de mercado para la solución que mejor se adapte a las necesidades de la empresa, sin dejar de lado el aspecto de la seguridad, eficiencia e impacto que tendrá la solución.

Particularmente la Empresa Financiera contaba con la disponibilidad e infraestructura base para lograr la implementación y puesta a prueba del prototipo de diseño de red establecido; sin embargo, es de suma importancia establecer el factor económico con el que cuenta la empresa y la disponibilidad de sus recursos.

El esquema a prueba, presentado en este trabajo, da pie a proyectos futuros para mejorar el sistema expuesto, lo que indica que se deja abierto al lector propuestas novedosas para continuar el proyecto de incorporación de dispositivos a una red empresarial WLAN 802.11 segura de cuarta generación, tomando en consideración las bases de este documento para su implementación en el ámbito empresarial.

6.2 Trabajos futuros

Para puntualizar en lo referente a trabajos futuros; en el caso de la red WLAN de la Empresa Financiera se establecen las siguientes actividades como puntos más importantes:

- Incorporación de un WLC Ancla del lado del Edificio B de la Empresa Financiera, cuyo objetivo es la incorporación de redundancia entre controladores Ancla.

- Implementación del sistema WCS (*Wireless Control System*) el cual permitirá el establecimiento de administración de todos los controladores que integren el sistema.

- Establecimiento de la herramienta de NAC/NAP a nivel de WLAN.

- Explotación y puesta a punto de los recursos de prevención de intrusos en una red inalámbrica en su solución WIPS (para el caso del proveedor Cisco).

- Simulación de pruebas de penetración.

- Integración de red IEEE 802.11ac

- Integración BYOD

ANEXO A.

Configuración automática del canal de RF

```
show>ap auto-rf 802.11b <AP1_JURÍDICO_P3>
Number of Slots . . . . . . . . . . . . . . . . . . . . . . 2
AP Name . . . . . . . . . . . . . . . . . . . . . . . . . . <AP1_JURÍDICO_P3>
MAC Address . . . . . . . . . . . . . . . . . . . . . . . . 00:24:C4:a0:a7:d2
Radio Type . . . . . . . . . . . . . . . . . . . . . . . . .
RADIO_TYPE_80211b/g
Noise Information
Noise Profile . . . . . . . . . . . . . . . . . . . . . . PASSED
Channel 1 . . . . . . . . . . . . . . . . . . . . . . . . -93 dBm
Channel 2 . . . . . . . . . . . . . . . . . . . . . . . . -90 dBm
.
.
.
Channel 11 . . . . . . . . . . . . . . . . . . . . . . . . -95 dBm
Interference Information
Interference Profile . . . . . . . . . . . . . . . . . . FAILED
Channel 1 . . . . . . . . . . . . . . . . . . . . . . . . -69 dBm @ 31 % busy
Channel 2 . . . . . . . . . . . . . . . . . . . . . . . . -58 dBm @ 26 % busy
.
.
.
Channel 11. . . . . . . . . . . . . . . . . . . . . . . -68 dBm @ 26 % busy
Load Information
Load Profile . . . . . . . . . . . . . . . . . . . . . . PASSED
Receive Utilization . . . . . . . . . . . . . . . . . . . 0 %
Transmit Utilization . . . . . . . . . . . . . . . . . . . 0 %
```

```
Channel Utilization . . . . . . . . . . . . . . . . . . . 26 %
Attached Clients . . . . . . . . . . . . . . . . . . . . 2 clients
Coverage Information
Coverage Profile . . . . . . . . . . . . . . . . . . . . . PASSED
Failed Clients . . . . . . . . . . . . . . . . . . . . . . 0 clients
Client Signal Strengths
RSSI -100 dBm. . . . . . . . . . . . . . . . . . . . . . . 0 clients
RSSI -92 dBm . . . . . . . . . . . . . . . . . . . . . . . 0 clients
.
.
.
RSSI -52 dBm . . . . . . . . . . . . . . . . . . . . . . . 1 clients
Client Signal To Noise Ratios
SNR 0 dBm . . . . . . . . . . . . . . . . . . . . . . . . . 0 clients
SNR 5 dBm . . . . . . . . . . . . . . . . . . . . . . . . . 0 clients
SNR 10 dBm . . . . . . . . . . . . . . . . . . . . . . . . 0 clients
.
.
.
SNR 45 dBm . . . . . . . . . . . . . . . . . . . . . . . . 1 clients
Nearby APs
Radar Information
Channel Assignment Information
Current Channel Average Energy . . . . . . . . . . . . . -68 dBm
Previous Channel Average Energy . . . . . . . . . . . . . -51 dBm
Channel Change Count . . . . . . . . . . . . . . . . . . 21
Last Channel Change Time . . . . . . . . . . . . . . . . Thu Jun 27
17:18:03 2013
Recommend Best Channel . . . . . . . . . . . . . . . . . 11
RF Parameter Recommendations
Power Level . . . . . . . . . . . . . . . . . . . . . . . 1
RTS/CTS Threshold . . . . . . . . . . . . . . . . . . . . 2347
Fragmentation Threshold . . . . . . . . . . . . . . . . . 2346
```

ANEXO B

Configuración General del WLC Ancla

```
Would you like to enter the initial configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help. Use ctrl-c to
abort configuration dialog at any prompt. Default settings are in square
brackets '[]'.

Basic management setup configures only enough connectivity for management
of the system, extended setup will ask you to configure each interface on
the system

Would you like to enter basic management setup? [yes/no]: yes

Configuring global parameters:

Enter host name [Controller]: WLC Ancla
```

The enable secret is a password used to protect access to privileged EXEC and configuration modes. This password, after entered, becomes encrypted in the configuration.

Enter enable secret: **XXXXX**

The enable password is used when you do not specify an enable secret password, with some older software versions, and some boot images.

Enter enable password: **XXXXX**

The virtual terminal password is used to protect access to the router over a network interface. Enter virtual terminal password: **Cisco123**

Configure a NTP server now? [yes]: **yes**

Enter ntp server address : **172.18.37.254**

Enter a polling interval between 16 and 131072 secs which is power of **2:16**

Do you want to configure wireless network? [no]: **yes**

Enter mobility group name: **Mobility**

Enter the country code[US]:**US**

Configure SNMP Network Management? [no]: **no**

Current interface summary

Any interface listed with OK? value "NO" does not have a valid configuration

Enter interface name used to connect to the

management network from the above interface summary: **TenGigabitEthernet1/0/4**[service port)

Configuring interface GigabitEthernet1/0/4: Configure IP on this interface? [no]: **yes**

IP address for this interface: **192.168.2.50**

Subnet mask for this interface [255.255.0.0] : **255.255.255.0**

Glosario de siglas y acrónimos

AC	(*Access Control)* Control de Acceso
ACL	*(Access Control List)* Lista de Control de Acceso
ACS	*(Access Control Server)* Servidor de Control de Acceso
ACK	*(Acknowledgment)* Acuse de recibo
AD	*(Active Directory)* Directorio Activo
AES	*(Advanced Encryption Standard) Estándar de Cifrado Avanzado*
ANSI	*(American National Standard Institute)* Instituto Nacional Estadounidense de Estándares
AP	*(Access Point)* Punto de Acceso Inalámbrico
BPSK	*(Binary Phase Shift Keying)* Modulación por desplazamiento de fase binaria
BSS	*(Basic Service Set)* Conjunto de Servicios Básicos
BYOD	*(Bring Your Own Device)*
CA	*(Certification Authority)* Autoridad de Certificación

CAPWAP *(Control and Provisioning of Wireless Access Points)*
Control y Aprovisionamiento de los Puntos de Acceso Inalámbrico

CCMP *(Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)*

CLI *(Command Line Interface)* Interfaz de Línea de Comandos

CSMA/CA *(Carrier Sense Multiple Access with Collision Avoidance)*
Acceso Múltiple por Detección de Portadora con Evasión de Colisiones

CW *(Contention window)* Ventana de contención

CRC *(Cyclic Redundancy Check)* Comprobación de Redundancia Cíclica

CoA *(Care of Address)* Dirección de Auxilio

DBPSK *(Differential Binary Phase Shift Keying*)
Modulación por desplazamiento diferencial de fase binario

DCA *(Dynamic Chanel Assigment)* Asignación Dinámica de Canales

DCF *(Distributed Coordination Function)* Función de Coordinación Distribuida

DHCP ***(****Dinamic Host Configuration Protocol)* Configuración Dinámica de Host

DMZ *(Demilitarized Zone) Zona Desmilitarizada*

DNS *(Domian Name System)* Sistema de Nombres de Dominio

DoS *(Denial of Service)* Denegación de servicio

DQPSK *(Differential Quadrature Phase Shift Keying)*
Modulación por desplazamiento diferencial de fase en cuadratura

DSS *(Distribution Sytem Service)*
Sistema de Servicios de Distribución

DSSS *(Direct Secuence Spread Spectrum)*
Espectro Disperso por Secuencia Directa

DTLS *(Datagram Transport Layer Security)*
Seguridad de la Capa de Transporte del Datagrama

EAP *(Extensible Authentication Protocol)*
Protocolo de Autenticación Extensible

EAP-TLS *(EAP-Transport Layer Security)*
EAP con Seguridad en la Capa de Transporte

EAP-TTLS *(EAP-Tunneled Transport Layer Security)*
EAP con Túnel de Seguridad en la Capa de Transporte

EIRP *(Equivalent Isotropically Radiated Power)*
Potencia Isotrópica Radiada Equivalente

ET Estación de Trabajo inalámbrica

ESS *(Extended Service Set)* Conjunto De Servicio Extendido

FA *(Foreign Agent)* Agente Foráneo

FHSS *(Frecuency Hoping Spread Spectrum)*
Espectro disperso por salto de frecuencia

FSK *(Frequency Shift Keying)* Modulación por desplazamiento de frecuencia

FTP *(File Transfer Protocol)* Protocolo de Transferencia de Archivos

GUI *(Graphical User Interface)* Interfaz Gráfica de Usuario

HA *(Home Agent)* Agente Regional o Doméstico

HTTP *(Hypertext Transfer Protocol)* Protocolo de Transferencia de Hipertexto

HVS *(Health Validation Status)* Estado de Validación de Salud

ID *(IDentifier)* Identificador

IDS *(Intrusion Detection System)* Sistema de Detección de Intrusos

IEEE *(Institute of Electrical and Electronics Engineers)*
Instituto de Ingenieros Eléctricos Electrónicos

IETF *(Internet Engineering Task Force)*
Fuerza de Tareas de Ingeniería de Internet

IFS *(Inter-Frame Space)* Espaciado entre tramas

ITU (*International Telecommunication Union*)
Unión Internacional de Telecomunicaciones

ITU-T (*ITU-Standarization Sector Telecommunications)*
UIT-Sector de Normalización de las Telecomunicaciones

IV *(Initialization Vector)* Vector de inicialización

LAN *(Local Area Network)* Red de Área Local

LAP (*Lightweight Access Point)* Punto de Acceso Ligero

LLC	*(Logical Link Control)* Control de Enlace Lógico
LWAPP	(*Lightweight Access Point Protocol)* Protocolo Ligero para Puntos de Acceso
MAC	*(Media Access Control)* Control de Acceso al Medio
MIC	*(Message Integrity Code)* Código de la Integridad del Mensaje
MIMO	*(Multiple-Input Multiple-Output)* Múltiple entrada-Múltiple salida
MN	*(Mobile Node)* Nodo Móvil
MSDU	*(Service Data Unit* or *MSDU)* *Entrega de Unidad de Servicios de Datos MAC*
NAC	*(Network Admission Control) Control de Admisión a la Red*
NAP	*(Network Access Protection)* Protección de Acceso a la Red
NAT	*(Network Address Translation) Traducción de Dirección de Red*
NAV	*(Network* Allocation *Vector)* Vector de asignación a la red
NPS	*(Network Policy Server) Servidor de Políticas de Red*
P2P	*(Peer to peer)* Conexión punto a punto
OFDM	*(Orthogonal Frequency Division Multiplexing)* Multiplexación por División en Frecuencias Ortogonales
OSI	(*Open System Interconnection*) Sistema Abierto de Interconexión
QAM	*(Quadrature Amplitude Modulation)* *M*odulación de amplitud en cuadratura
QPSK	*(Quadrature Phase Shift Keying)* Modulación por desplazamiento de fase en cuadratura
QoS	*(Quality of service)* Calidad de Servicio
RADIUS	*(Remote Authentication Dial-In User Server)*
RFC	*(Request for comments)* Petición de comentarios
RTS/CTS	*(Request to Send and Clear to Send*) Solicitud de envío/Libre para envío
RRM	*(Radio Resource Management)* Gestión de Recursos de Radio
SDM	*(Spatial Division Multiplexing)* Multiplexado de División Espacial

SNR	*(Signal Noise to Ratio)* Relación Señal a Ruido
SoHs	*(State of Healt Responses)* Estado de las respuestas de salud
SS	*(Spread Spectrum) Espectro Disperso*
SS	*(Station Services)* Estaciones de Servicios
SSID	*(Service Set IDentifier)* Identificador de Conjunto de Servicios
SSL	*(Secure Sockets Layer)* Capa de Conexión Segura
TCP	*(Transmission Control Protocol)* Protocolo de Control de Transmisión
TPC	*(Transmit Power Control)* Control de Potencia Transmitida
TKIP	*(Temporal Key Integrity Protocol)* Protocolo de Integridad de Claves temporales
UDP	*(User Datagram Protocol)* Protocolo de Datagramas de Usuario
USB	*(Universal Serial Bus)* Bus Universal en Serie
VLAN	*(Virtual Local Area Networks) Red Virtual de Área Local*
WCS	*(Wireless Control System) Sistema de Control Inalámbrico*
WECA	*(Wireless Ethernet Compatibility Alliance*) Alianza *de* Compatibilidad Ethernet Inalámbrica
WEP	*(Wired Equivalent Privacy)* Privacidad Equivalente a Cableado
WIPS	*(Wireless Intrusion Prevention System)* Sistema Inalámbrico de Protección contra Intrusos
Wi-Fi	(*Wireless Fidelity*) Fidelidad Inalámbrica
WLAN	*(Wireless Local Area Network)* Red Inalámbrica de Área Local
WLC	(Wireless LAN Controller) Controlador Inalámbrico LAN
WMAN	*(Wireless Metropolitan Area Network)* Red Inalámbrica de Área Metropolitana
WMM	*(WiFi MultiMedia)*
WPA	*(Wi-Fi Protected Acces)* Acceso Wi-Fi Protegido
WPAN	*(Wireless Personal Area Network)* Red Inalámbrica de Área Personal
WPA2	*(Wi-Fi Protected Acesss 2) Acceso Wi-Fi Protegido 2*

WWAN (Wireless Wide Area Network) Red Inalámbrica de Área Extendid

Referencias

[1] Cisco, White Paper, *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010–2015. Cisco Systems.* February 2011.
<http://newsroom.cisco.com/dlls/ekits/Cisco_VNI_Global_Mobile_Data_Traffic_Forecast_2010_2015.pdf>
Consultado el 5 de Noviembre de 2012.

[2] IEEE 802.11™-2012, IEEE Standard for Information Technology, *Telecommunications and information exchange between systems Local and metropolitan area networks. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.*

[3] Wi-Fi
http://www.wi-fi.org/

[4] IEEE
http://www.ieee.org,

[5] ITU
http://www.itu.int/es/

[6] *Wireless Safety: Wireless5 Safety Certification,* Course Technology, Cengagi Learning, EC Council, 2010, pp. 6-9.
Consultado en *Google Books*, 13 de Noviembre de 2012.

[7] Search Mobile Computing, *802.xx Fast Reference*, February 2006.
<http://searchmobilecomputing.techtarget.com/feature/802xx-Fast-Reference>
Consultada el 17 de Noviembre de 2012.

[8] Air 802*, IEEE 802.11 a/b/g/n Wi-Fi Standards and Facts*, s.f.
<http://www.air802.com/files/802-11-WiFi-Wireless-Standards-and-Facts.pdf>
Consultada el 17 de Noviembre de 2012.

[9] Peter Thornycroft, Aruba Networks, *Designed for Speed Network Infrastructure in an 802.11n World,* October 2007.
<http://www.arubanetworks.com/pdf/technology/whitepapers/wp_Designed_Speed_802.11n.pdf >
Consultada el 19 de Noviembre de 2012.

[10] Hunn, Nick, *Essentials of Short-Range Wireless*, Cambrideges Essentials Series, Cambridege.Univerity Press, 2010, p. 116.
Consultado en *Google Books*, 21 de Noviembre de 2012.

[11] Chen, Hsiao-Hwa y Mohsen Guizani, *Next Generation Wireless Systems and Networks*, Ed. Wiley, 2006, pp. 215-219.
Consultado en *Google Books*, 28 de Noviembre de 2012.

[12] Syngress Publishing Inc., *Building a Cisco Wireless Lan*, Ed. Global Knowledge, 2002, p.330
Consultado en *Google Books*, 30 de Noviembre de 2012.

[13] Gast, Matthew S., Creating & Administering Wireless Network, *802.11 Wireless Networks: The Definitive Guide*, 2nd Edition, Ed. O'Really, 2005, pp. 27-28.
Consultado en *Google Books*, 30 de Noviembre de 2012.

[14] Wu, Hongyi y Yi Pan, *Medium Access Control in Wireless Networks,* Series Editors: Wirless Networks and Mobile Computing, Ed. Nova Science Publisher Inc.,2008 ,pp. 224-225.
Consultado en *Google Books*, 1 de Diciembre de 2012.

[15] Bucknell University, *RFC 2131: Dynamic Host Configuration Protocol,* IETF, Network Working Group, March 1997.
< http://www.ietf.org/rfc/rfc2131.txt>
Consultada el 5 de Diciembre de 2012.

[16] J. Jacobsen, Ole, *Wireless LAN Switches*, The Internet Protocol Journal, vol 9, no. 3, September 2006, pp. 1-14.
Consultada el 9 de Diciembre de 2012.

[17] Gress, Mark y Lee Jhonson, *Deploying and Troubleshooting Cisco Wireless LAN Controllers: A Practical Guide to Working with the Cisco Unified Wireless Solutions*, Cisco Press, Ed. Pearson, November 2009, pp.11-34.
Consultada en *Safari Books Online* el 11 de Diciembre de 2012.

[18] Calhoun, et. al, *RFC 5412: Lightweight Access Point Protocol,* Independent Submission, February 2010.
< http://tools.ietf.org/html/rfc5412>

[19] Rescorla, et. al, *RFC 4347: Datagram Transport Layer Security,* Network Working Group, April 2006.
< http://tools.ietf.org/html/rfc4347>
Consultada el 17 de Diciembre de 2012.

[20] *Cisco Guide: 440X Series Wireless LAN Controllers Deployment Guide*, Cisco Systems Inc., 2006, pp. 72-84.
<http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html >
Consultada el 17 de Diciembre de 2012.

[21] Lammle, Todd, *CCNA Wireless Study Guide: IUWNE Exam 640-721*, Ed. Serious Skills, s.f., pp. 259-260.
Consultado en Google Books, 19 de Diciembre de 2012.

[22] Hoja de especificaciones para Cisco Aironet 1130 Series.
Consultada en www.cisco.com el 10 de Enero de 2012.

[23] Cisco, *CiscoEnterprise Mobility 4.1 Design Guide: Cisco Unified Wireless QoS,* Cisco Systems, Inc, April 2012, pp. 139-149.
Consultada en Safari Books Online el 10 de Enero de 2013.

[24] Mangold, et. al., *Analysis of IEEE 802.11e for QoS support in wireless LANs*, Wireless Communication, Journal & Magazines, vol. 10, december 2003, pp.40-50.
Consultada el 12 de Enero de 2013.

[25] WTIA, *Report on WiFi Adoption and Security Survey 2012,* july 2012.
< http://www.safewifi.hk/files/WiFi_adoption_and_security_survey_2012.pdf>
Consultada el 15 de Enero de 2013.

[26] IEEE 802.1X, *IEEE Standard for Information Technology, Port Based Network Access Control.*
< http://grouper.ieee.org/groups/802/1/pages/802.1x.html/>
Consultada el 21 de Diciembre de 2012.

[27] Stanley, et. al, *RFC 4017: Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs,* Network Working Group, Agere Systems, Intel Corporation, Intel Systems, March 2005.
< https://tools.ietf.org/html/rfc4017>
Consultada el 13 de Enero de 2013.

[28] Cooper, et. al, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, Network Working Group, May 2008
< http://tools.ietf.org/html/rfc5280>
Consultada el 13 de Enero de 2013.

[29] Microsoft TechNet, *Configuración de redes inalámbricas IEEE 802.11 de Windows XP para el hogar y la pequeña empresa*, Microsoft Corporation, mayo 2005.
<http://www.microsoft.com/latam/technet/productos/windows/windowsxp/wifisoho.mspx>
Consultada el 20 de Febrero de 2013.

[30] Lehembre, Guillaume, Seguridad Wi-Fi – WEP, WPA y WPA2, 2006.
< http://www.haking9.org>
Consultada el 20 de Febrero de 2013.

[31] Li, Peng, et al, *Effect of WPA2 Security on IEEE 802.11n Bandwith and Round Trip Time in Peer-Peer Wireless Local Area Networks*, IEEE Xplore Digital Library, 2011.
<http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5763598>
Consultada el 21 de Febrero de 2013.

[32] Microsoft TechNet, *Wi-Fi Protected Access 2 (WPA2) Overview*, Microsoft Corporation, Microsoft Corporation, 2005.
<http://technet.microsoft.com/library/bb878054>
Consultada el 21 Febrero de 2013.

[33] CCNA V4.0 Exploration 1. *Aspectos básicos de Networking*, Cisco Systems.
Consultada el 1 de Marzo de 2013.

[34] Perkins, C., *RFC 2002: IP Mobility Support,* Network Working Group, IBM, October 1996.
< http://www.ietf.org/rfc/rfc2002.txt>
Consultada el 7 de Marzo de 2013

[35] IEEE 802.11r-2008. *Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Fast Basic Service Set (BSS).*

[36] Cisco live*, Presentation: Voice Over Wi-Fi, Deployment Recomdations and best practices*, Cisco Systems, Inc, 2012.
Consultada el 20 de Enero de 2013.

[37] Zeus Kerravala, *Bring-Your-Own-Device Requires New Network Strategies*, ZK Research A Division of Kerravala Consulting, September 2012.
<http://www.xirrus.com/cdn/pdf/zeusk_byod_requires_new_network_strategies>
Consultada el 24 de Marzo de 2013.

[38] Zeus Kerravala, *Pervasive Mobility Drives the Need for Wireless LAN Evolution,* ZK Research A Division of Kerravala Consulting, September 2012.
< http://twileshare.com/uploads/Pervasive_Mobility_WLAN_Evolution_2011.pdf >
Consultada el 24 de Marzo de 2013.

[39] Cisco, *Cisco Bring Your Own Device (BYOD) Smart Solution Design Guide*, Cisco, Inc., December 2012.
<http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byoddg.html>
Consultada el 27 de Marzo de 2013.

[40] Bradley, et. al., *BYOD: A Global Perspective Harnessing Employee-Led Innovation*, Survey Report, Cisco IBSG, 2012.

<https://www.cisco.com/web/offer/gist_ty2_asset/BYOD_Horizons_Global_080912.pd>
Consultada el 29 de Marzo de 2013.

[41] Harris, et.al., *Mobile Consumerization Trends & Perceptions*, IT Executive and CEO Survey, Trend Micro, Inc., February 2012.
<http://www.trendmicro.ae/media/wp/wp01_decisive-analytics-full-consumerization-report-en.pdf>
Consultada el 10 de Abril de 2013.

[42] Zimmerman, Tim y Mark Fabbi, *Magic Quadrant for the Wired and Wireless LAN Access Infrastructure*, Gartner, Inc., ID:G00234282, June 2012.
<http://www.gartner.com/technology/reprints.do?id=1-1AX5XXB&ct=120614&st=sb>
Consultada el 10 de Abril de 2013.

[43] Info Tech, *Vendor Landcape: Wireless LAN,* Info Tech Research Group, Inc., 2012.
<http://www.enterasys.com/company/literature/Info-Tech-WLAN-Vendor-Landscape.pdf>
Consultada el 12 Abril de 2013.

[44] Mehra, Roith, *Competitive Analysis, Worldwide Enterprise WLAN 2011-2012 Vendor Analysis,* International Data Corporation IDC, 2012.
<http://www.wit.co.th/pdf/Aruba/aruba_IDC_MarketScape_Worldwide_Wirelesss_LAN_2011-2012.pdf>
Consultada el 12 Abril de 2013.

[45] IDC, Top Five Worldwide Enterprise WLAN Vendors, Revenue Market Shares, 2011 Q4 and 2012 Q4, International Data Corporation IDC, 2013.
< http://www.icharts.net/chartchannel/top-five-worldwide-enterprise-wlan-vendors-revenue-market-shares-2011-q4-and-2012-q4_m3uyipec>
Consultada el 13 de Abril de 2013.

[46] Business Wire, *Infonetics Research: It's Official: Wireless LAN is the Hottest Market in Enterprise Networking,* Business Wire, March 2012.
< http://sip-trunking.tmcnet.com/news/2012/03/20/6201870.htm>
Consultada el 18 de Abril de 2013.

[47] Cisco, *Cisco Unified Wireless Guest Access Services,* Cisco, Inc.
<http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byoddg.html>
Consultada el 22 de Abril de 2013.

[48] Aruba, WLAN Secure Guest Access: Configure secure guest WLAN access, Aruba Networks, Inc., Airwave.
< http://www.arubanetworks.com>
Consultada el 23 de Abril de 2013.

[49] HP ProCurve, *Network Security Solutions: Guest VLANs*, HP Networking, 2009.
<http://www.hp.com/rnd/pdf_html/guest_vlan_paper.htm>
Consultada el 23 de Abril de 2013.

[50] Miercom, *Lab Testing Summary Report. Product category: Wireless Access Points,* Report SR120306, March 2012.
< http://www.miercom.com/pdf/reports/20120306.pdf>
Consultada el 14 de Mayo de 2013.

[51] Miercom, *Lab Testing Summary Report. Product category: Wireless Controllers,* Report 130508, May 2013.
< http://miercom.com/pdf/reports/20130508.pdf>
Consultada el 17 de Mayo de 2013.