UNIVERSIDAD SAN FRANCISCO DE QUITO

Colegio de Ciencias e Ingeniería

Estudio y Diseño de la Red Inalámbrica provista para el Nuevo Aeropuerto de Quito (NAIQ)

Rubén Darío Moreno Dueñas

Fausto Vasco, Ing., Director de tesis

Tesis de grado presentada como requisito para la obtención del Título de Licenciado en Redes y Sistemas Operativos

Quito, Noviembre de 2012

UNIVERSIDAD SAN FRANCISCO DE QUITO

Colegio de Ciencias e Ingeniería

HOJA DE APROBACIÓN DE TESIS

Estudio y Diseño de la Red Inalámbrica provista para el Nuevo Aeropuerto de Quito (NAIQ)

Rubén Darío Moreno Dueñas

Nombre: …… ……..

Director de Tesis

Miembro del Comité de Tesis

Nombre: …… ……..

Miembro del Comité de Tesis

Nombre: …… ……..

Miembro del Comité de Tesis

Nombre: …… ……..

Miembro del Comité de Tesis

Nombre: …… ……..

Decano del Colegio de Tecnologías

Quito, Noviembre de 2012

Firma:

Nombre:
C.I.:
Fecha:

Dedicatoria

A quien la quiera.

Agradecimiento

A mi Padre, quien me ha brindado su apoyo incondicional toda la vida, por su amor y ejemplo de vida. A mi Madre, a quien debo el haber aprendido el valor condición única para materializar los sueños, la disciplina. A Fausto Vasco, quien durante toda la carrera me ha apoyado inmensamente como profesor y como ser humano. A la USFQ, institución partícipe en mi formación como profesional y humano.

RESUMEN

En la actualidad, la tecnología de las Redes Inalámbricas se ha constituido en una parte sustancial en el vasto mundo de las Telecomunicaciones y Tecnologías de la Información. Tal es su actual importancia, que la demanda en Empresas Públicas y Privadas, Hospitales, Hoteles, Aeropuertos, Universidades, etc., es creciente en tanto toda Empresa depende de su Red para que sus operaciones, gestión y servicio sean llevadas a cabo con éxito.

El presente trabajo es una muestra de esta creciente demanda, y en este caso, del tratamiento que se dio al requerimiento proveniente del Nuevo Aeropuerto Internacional de la ciudad de Quito en su necesidad de desarrollar una Red Inalámbrica que cumpla con los más altos estándares de calidad, compatibilidad, confiabilidad, redundancia y cobertura para sus usuarios, que se estima, alcanzarían los seis millones de pasajeros por año.

Es menester de este trabajo, mostrar el proceso previo de estudio de los requerimientos acorde a la infraestructura de Red Inalámbrica siguiendo estándares de industria y revisión del equipamiento disponible en el mercado para el cumplimiento de dichos antecedentes. Asimismo, se demuestra el proceso de desarrollo del Diseño de Red, los cuales cumplen con estándares de mejores prácticas: redundancia, seguridad, encriptación y transparencia al usuario final.

ABSTRACT

Nowadays, the technology of wireless networks has become a substantial part in the vast world of Telecommunications and Information Technology. Such is its actual importance, that demand in Public and Private Companies, Hospitals, Hotels, Airports, Universities, etc., is growing considerably as every company relies on its network capabilities so its operations, management tasks and services can be accomplished successfully.

The present work is an example of this growing demand, and in this case, the treatment given to the request from the New International Airport of Quito's need for developing a wireless network that meets the highest standards of quality, compatibility, reliability, redundancy and coverage for its users, which are estimated to reach six million passengers per year.

The task of this work is to show the previous process of studying the requirements according to the wireless network infrastructure which follows industry standards, the process of researching the available equipment in the market to fulfill this requirement. It is also shown the development process of network design, which met best practices-standards such as: redundancy, security, encryption and transparency to the end user.

TABLA DE CONTENIDO

TABLA DE FIGURAS

LISTA DE TABLAS

CAPITULO I

1 Antecedentes

El proyecto del Nuevo Aeropuerto Internacional de Quito, tiene como requerimiento el brindar un servicio de conexión a Internet para sus, aproximadamente, seis millones de usuarios al año. Este trabajo muestra el proceso que conllevó la propuesta hecha al aeropuerto para la provisión del servicio de Internet.

Al ser uno de los aeropuertos más modernos, el requisito para su red inalámbrica comprendía las tecnologías y servicios más avanzados en las áreas de cobertura, administración, seguridad de redes, tiempo de Up-time, redundancia y facilidad o transparencia en la configuración para sus usuarios finales. El requerimiento, aunque principalmente orientado hacia la red inalámbrica, también comprende la provisión de una red de datos cableada destinada a centralizar la administración de los Puntos de acceso (APs) contenidos en esta infraestructura.

1.1 Introducción

Como paso preliminar al diseño de la red inalámbrica propuesta, se hará una descripción detallada de la tecnología Wireless, su funcionamiento, escenarios, mejores prácticas y desafíos.

El estudio preliminar comprende conocer el Espectro de Radio-Frecuencia, las bandas que están disponibles para el uso público de Redes, cómo influyen las frecuencias y técnicas modulación en las velocidades de transmisión. También se describen los inconvenientes que sufren las Redes Inalámbricas debido a distintos tipos de degradación por diferentes fenómenos: absorción, reflexión o interferencia con equipos electrónicos que funcionan en frecuencias similares.

Se exponen también el hardware inalámbrico implementado, es decir, antenas, sus diferentes tipos y su funcionamiento según los escenarios propuestos. A nivel de software, se discuten los protocolos Wireless (802.11) que son estándar en la industria. Finalmente, se muestra los distintos tipos de tecnologías inalámbricas (WLAN, WWAN, WiMax), su aplicación en la actualidad y la manera como el usuario final interactúa con estas infraestructuras.

CAPITULO II

2 Marco teórico

2.1 Tecnología Inalámbrica

La tecnología inalámbrica tiene sus más remotos orígenes en los descubrimientos de Alexander Graham Bell y Charles Sumner en 1880 del fotófono, que era básicamente un aparato que conducía el audio a través de haces de luz moduladas haciendo uso de ondas electromagnéticas (Scientific American, 3). Posteriormente Thomas Edison en 1885 desarrolló un vibrador magnético para transmisión de ondas por inducción (Beals) y, con mayor eficacia, en 1888 Heinrich Hertz descubre las ondas electromagnéticas, base de todas las tecnologías Wireless en la actualidad, ya que a través de estas, se pueden transmitir impulsos eléctricos (Carroll, 8). Es de suma importancia, tras este prefacio histórico, entender el espectro electromagnético, su funcionamiento en las transmisiones y cómo está regulado su uso actual a través del estándar 802.11 desarrollado por el Instituto de Ingenieros Electrónicos y Eléctricos (IEEE-802.11).

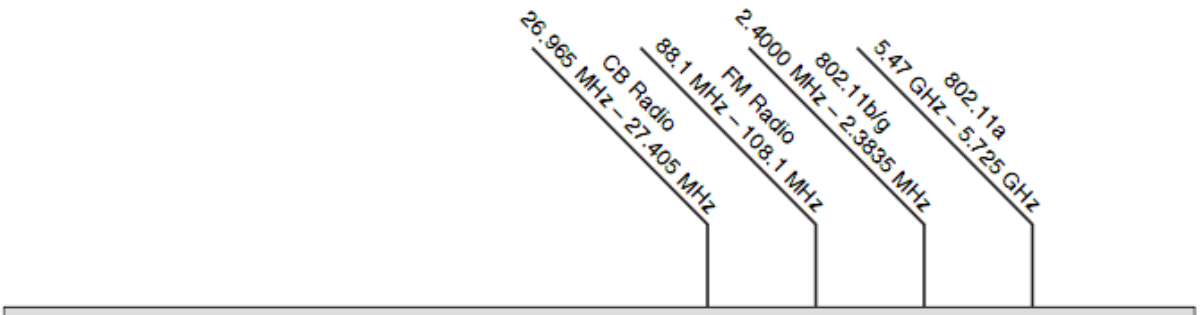
2.1.1 Teoría del Espectro de Radio-Frecuencias (RF)

Para poder hacer transmisiones sobre el aire, que es el medio utilizado por los dispositivos inalámbricos, la IEEE desarrolló un estándar que define el uso de frecuencias no licenciadas (públicas) para la comunicación en Redes de Área Local Inalámbricas (WLANs). Esta especificación 802.11 define las operaciones de envío y

recepción usando la misma frecuencia en modo Half-Duplex, es decir, no permitiendo el proceso de envío-recepción al mismo tiempo sino, uno a la vez (Carroll, 8).

2.1.1.1 Bandas de frecuencia no licenciada

Para el control de las trasmisiones hechas sobre el espectro de Radio-Frecuencias, existen autoridades encargadas de administrar el uso de las frecuencias y asignarlas a distintos medios como radio, televisión o redes inalámbricas. Dichas autoridades son definidas por regiones o países como por ejemplo: Federal Communications Commission para los Estados Unidos, Conference of European Post and Telecommunications para Europa, Consejo Nacional de Telecomunicaciones (CONATEL) para Ecuador (Carrión, 1), entre otras. Las bandas de frecuencias no licenciadas, están disponibles para el uso en Redes de Área Local (WLAN) aunque varían de región en región. La siguiente figura muestra las frecuencias dentro del espectro usadas, que específicamente se encuentran entre los rangos de 900-MHz, 2.4-GHz y 5-GHz (Carroll, 9).



The Entire Electromagnetic Radio Spectrum										
ELF	SLF	ULF	VLF	LF	MF	HF	VHF	UHF	SHF	EHF
3 Hz 30 Hz	30 Hz 300 Hz	300 Hz 3 kHz	3 kHz 30 kHz	30 kHz 300 kHz	300 kHz 3 MHz	3 MHz 30 MHz	30 MHz 300 MHz	300 MHz 3 GHz	3 GHz 30 GHz	30 GHz 300 GHz

Figura 1: Uso del Espectro Electromagnético.

Fuente: Carroll, CCNA Wireless Official Guide, 10.

Sin embargo, dependiendo de la ubicación geográfica, el uso de las frecuencias no licenciadas cambia según lo definido por la autoridad de la región, por ende tenemos la siguiente distribución en Estados Unidos, Japón y Europa (Carroll, 10):

Europe	USA	Japan	Frequency
2.4 GHz	900 MHz		
	2.4 GHz ISM		2.0–2.4835 GHz
		2.4 GHz	2.0–2.495 GHz
CEPT A	UNII-1	5.15–5.25 GHz	5.15–5.25 GHz
CEPT A	UNII-2		5.25–5.35 GHz
CEPT B	UNII-2 Extended		5.47–5.7253 GHz
	ISM		5.725–5.850 GHz
		5.0 GHz	5.038–5.091 GHz
		4.9 GHz	4.9–5.0 GHz

Figura 2: Distribución del Uso de Frecuencias.

Fuente: Carroll, CCNA Wireless Official Guide, 10.

2.1.1.2 Técnicas de modulación

Las Redes Inalámbricas usan la modulación para poder enviar datos a través del medio. Los datos son codificados y luego son transportados a través de señales de ondas moduladas que consisten principalmente de tres porciones distintas: Amplitud, Frecuencia y Fase. Las técnicas de modulación encontradas en las redes inalámbricas son las siguientes: Secuencia Directa del Espectro Amplio (DSSS), Multiplexación por División de Frecuencia Ortogonal (OFDM) y Entrada Múltiple/Salida Múltiple (MIMO) (Carroll, 12).

DSSS es la técnica de modulación usada por ejemplo en el estándar 802.11b, para efectuar el envío de datos. La señal transmitida se difunde por toda la frecuencia del espectro que está en uso, por ejemplo, si transmitimos en el canal uno, la señal portadora se difunde a lo largo de toda la frecuencia que este caso es 22-MHz, obteniendo así el rango entre 2.401 a 2.423 GHz.

Los datos deben ser codificados para la transmisión sobre el medio. Básicamente la codificación se traduce como convertir los datos en señales de radio-frecuencia y viceversa (Carroll, 12). La modulación, por otro lado es la característica de las ondas de radio-frecuencia que contienen los datos previamente codificados. La modulación en DSSS puede tomar como estrategia la amplitud, frecuencia o cambio de fase, entendiéndose ésta, como el tiempo entre picos de una señal (Carroll, 14).

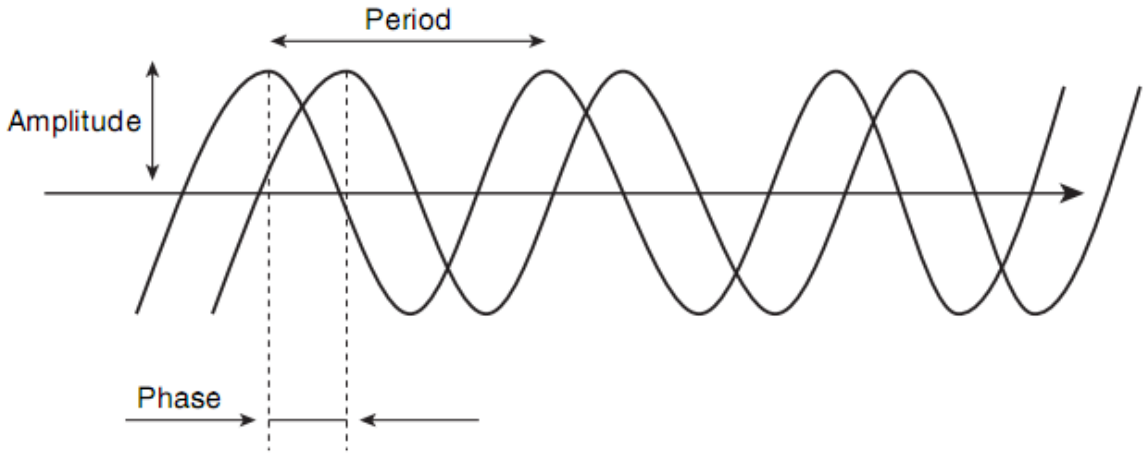


Figura 3: Amplitud, Frecuencia y Fase.

Fuente: Carroll, CCNA Wireless Official Guide, 15.

DSSS puede enfrentarse sin embargo, a pérdidas a consecuencia del desvanecimiento multi-trayectoria de la señal. Este desvanecimiento de la señal se produce a causa de la desviación de la señal sobre el medio de propagación compartido que es el aire, entre distintas señales causando que las ondas se reflejen y lleguen en tiempos no sincronizados (Carroll, 39). Como una solución planteada a esta clase de atenuación está la técnica de modulación conocida como Multiplexación por División de Frecuencia Ortogonal (OFDM).

OFDM es una de las aplicaciones del esquema de transmisión de datos paralela que reduce la pérdida causada por la atenuación al multiplexar la transmisión de datos en varias sub-señales o canales, de menor velocidad cada una, pero que mitigan el problema de la atenuación. (Prasad, 370). El esquema de transmisión de OFDM es el mejor ejemplo de la transmisión paralela multi-portadora de señales. La palabra “ortogonal” para el caso de OFDM indica la relación matemática precisa existente

entre las frecuencias de este sistema que ahorra ancho de banda (Prasad, 372). La siguiente figura ilustra el proceso de multiplexar la señal:

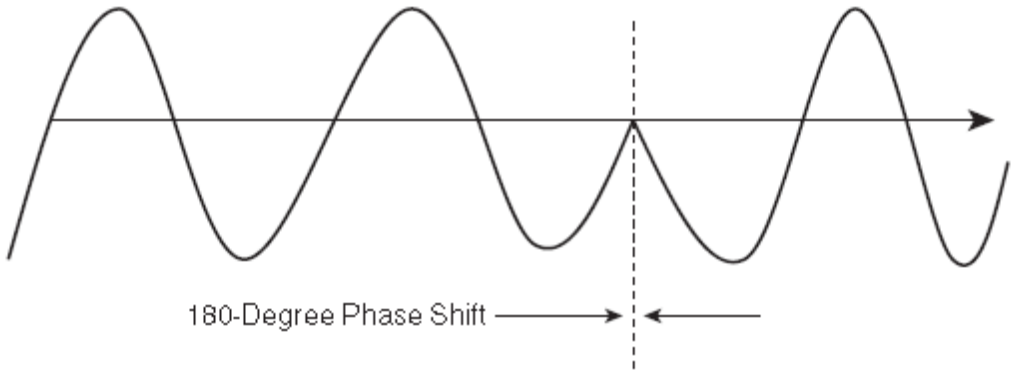


Figura 4: Multiplexor de señal.

Fuente: Carroll, CCNA Wireless Official Guide, 16.

La técnica de modulación Entrada Múltiple/Salida Múltiple (MIMO) es una estrategia empleada por ejemplo en el estándar 802.11n, el mismo que describiremos a detalle en una sección próxima. Consiste en una tecnología que utiliza múltiples antenas para el proceso de envío de datos como también para la recepción de múltiples señales logrando así un alto rango de velocidades en la transmisión de datos que superan los 100 Mbps. La especificación 802.11n a pesar de usar esta técnica de modulación de señal, es aún compatible con otros estándares como 802.11a, 802.11b y 802.11g ofreciendo una mejora en el rendimiento de hasta un 30% en las velocidades de cada una de estas especificaciones (Carroll, 16). La siguiente figura describe el mecanismo usado por MIMO para generar varias transmisiones:

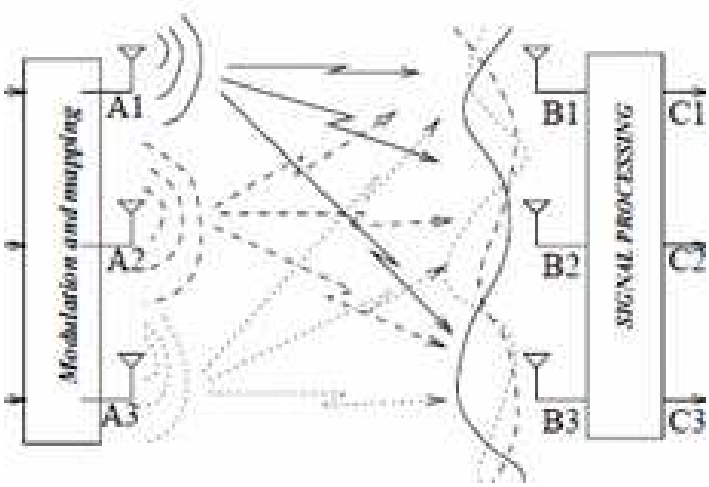


Figura 5: Entrada Múltiple/Salida Múltiple.

Fuente: http://telcoantennas.com.au/site/sites/default/files/images/mimo-technical.jpg

2.1.2 Funciones de Radio Frecuencias

La función de la radio frecuencia en el espectro electromagnético se encuentra en su porción menos energética, es decir, se sitúa en la porción entre 3 kHz y 300 gHz (Boylestad, 525). Las ondas generadas en esta región pueden ser originadas con corriente alterna en un generador hacia una antena que la transmita. En una transmisión de estas características, hay varios factores a tomar en cuenta que influye el comportamiento de las comunicaciones inalámbricas. Es necesario revisar los diferentes componentes que constituyen la comunicación de radio frecuencia para luego poder entender los fenómenos que influyen en su desempeño, a saber, la longitud de onda, las frecuencias y la amplitud.

2.1.2.1 Longitud de onda

La longitud de onda se define como la distancia existente entre los umbrales de una onda. Para poder medir esta distancia, partimos matemáticamente de una representación de onda sinusoide (Carroll, 34) que a su vez, está representada por la función de seno. Dicha onda se describe por las siguientes expresiones matemáticas:

$$y(x) = A\sin(x + \varphi)$$

$$y(x) = A\sin(\omega x + \varphi)$$

$$y(x) = A\sin(\frac{2\pi}{T}x + \varphi)$$

Donde:
- *A* es la amplitud de la oscilación
- ω es la frecuencia
- *T* es el periodo de oscilación y,
- φ es la fase inicial. (Serway y Jewett, 405)

La onda comienza en una señal de corriente alterna generada por un transmisor dentro de un Punto de Acceso (AP), para luego ser enviada hacia la antena, donde finalmente es irradiada como una onda sinusoide. La longitud de onda generada por un transmisor AC puede tener, según su uso, las siguientes características: 400 – 500 metros de largo para ondas de radio AM, 1 milímetro para ondas irradiadas

por satélites y unos pocos centímetros para ondas dentro de una red inalámbrica de área local (Carroll, 34).

2.1.2.2 Frecuencias

El periodo en el cual la señal es detectada y su reiteración es conocida como la frecuencia de la onda. Se determina también por periodos de tiempo o muestreos, en los cuales se observa la reiteración de la transmisión repetida. Para poder medir la frecuencia de una onda, no solo se observa su reiteración sino que, y muy importante, se debe tomar en cuenta el periodo de tiemplo en el cual ocurre. Estos muestreos de tiempo por lo general se miden en segundos.

La unidad de medida de la frecuencia de una onda es el Hertzio. Entre más altas son las frecuencias, menor es la distancia que recorre la onda, por ende una onda vista diez veces en un segundo tiene una frecuencia de 10 Hz mientras que una vista un millón de veces en el mismo lapso correspondería a 1000000 Hz, que comúnmente representaremos como 1 MHz, Mega Hertzio (Carroll, 35).

La frecuencia guarda una relación inversamente proporcional a la longitud de onda, es decir, a mayor frecuencia, menor longitud de onda. La frecuencia está descrita matemáticamente por la siguiente expresión:

$$f = \frac{v}{\lambda}$$

Donde:
- f es la frecuencia en Hz
- v es la velocidad de la onda

- λ es la longitud de onda (Serway y Jewett, 406)

2.1.2.3 Amplitud

A diferencia de la longitud de onda, la amplitud es la distancia vertical del umbral en una onda. En la figura 3 de la sección “Técnicas de modulación” se puede observar gráficamente la descripción de la amplitud. Pueden existir distintas medidas en la amplitud en un escenario de igual longitud de onda o misma frecuencia. La amplitud también está definida como la cantidad de energía que contiene una señal, por ello existen organismos destinados a regular la energía utilizada en cada caso (Carroll, 35). La amplitud se expresa matemáticamente con la siguiente ecuación:

$$x = A\sin(t - K) + b$$

Donde:
- *A* es la amplitud de la onda
- x es la variable de oscilación
- *T* es el tiempo de oscilación y,
- K, b son constantes que representan el tiempo y desplazamiento respectivamente (Serway y Jewett, 405).

Con el conocimiento preliminar de la naturaleza de las ondas de radio frecuencia, sus características y cómo se constituyen, revisaremos ahora las causas más comunes que afectan la transmisión en redes inalámbricas de área local, degradación en la

señal, pérdidas en ambiente de producción para posteriormente ofrecer una respuesta a estos desafíos.

2.1.3 Causas de degradación de la Señal

Aunque existen interferencias que anularían completamente la señal de una transmisión de red inalámbrica, no es el caso de ambientes de producción. En su lugar, los problemas más comunes son aquellos que degradan la señal en una proporción que afecta a los usuarios, no en su totalidad, pero en una mayoría o en una falta de equilibrio en el servicio que cada usuario final obtiene.

Las tres causas principales, aunque no son las únicas, de la degradación de señal que revisaremos son la reflexión, absorción e interferencia de bandas similares.

2.1.3.1 Reflexión

La reflexión consiste en que la señal sufre un desvió en la dirección que se tenía como intencionada para realizar la transmisión y esto se da producto del rebote o “reflejo” en superficies como el metal, vidrio, espejos, etc.

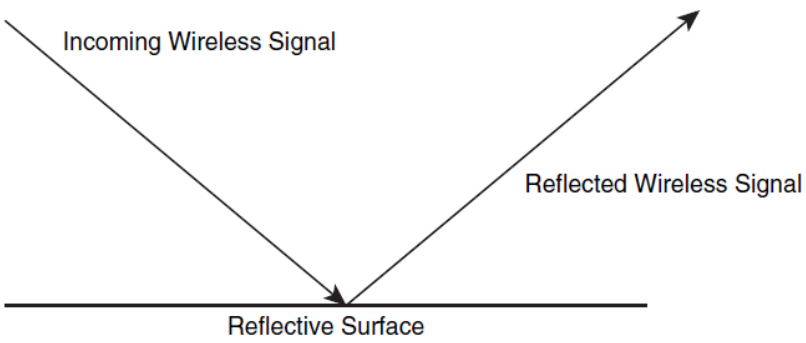


Figura 6: Reflexión.

Fuente: Carroll, CCNA Wireless Official Guide, 39.

La complicación que suele causar este agente de degradación es que la superficie que refleja cierta señal puede variar, es decir que refleja cierta frecuencia mientras no refleja otra mayor o menor (Carroll, 39).

2.1.3.2 Absorción

La absorción es un degradador de la señal ya que reduce la amplitud de la onda, reduciendo así, la distancia que la onda puede viajar. Para ilustrar este fenómeno tomemos el ejemplo del horno microondas. El aparato crea un conjunto de ondas que son absorbidas por el alimento que ingresamos, causando así que se caliente. Por ende la absorción también genera calor al atrapar las ondas.

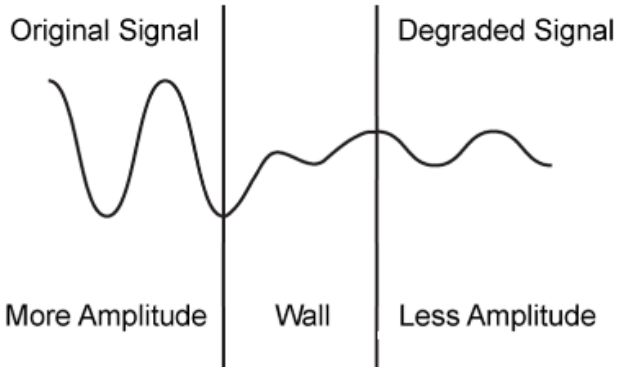


Figura 7: Absorción.

Fuente: http://newhorizons.bg/blog/wp-content/uploads/2010/12/Absorption.png

Paredes, alfombras e incluso el cuerpo humano pueden ser agentes de absorción de la señal de radio frecuencia utilizadas en las redes inalámbricas (Carroll, 38).

2.1.3.3 Interferencia de bandas similares

La interferencia de bandas de frecuencia similares consiste en otros dispositivos transmisores que funcionan en la misma frecuencia que las redes inalámbricas de área local y recordando lo mencionado en el capítulo anterior de “banda de frecuencias no licenciadas”, estos son 900 MHz, 2,4 GHz y 5Ghz (García et al., 1-2). Por lo general los aparatos más comúnmente encontrados como fuentes de interferencia, al compartir ambientes de producción de una red inalámbrica, como oficinas por ejemplo, son los teléfonos inalámbricos, hornos microondas, dispositivos Bluetooth, entre otros que operen en la misma frecuencia.

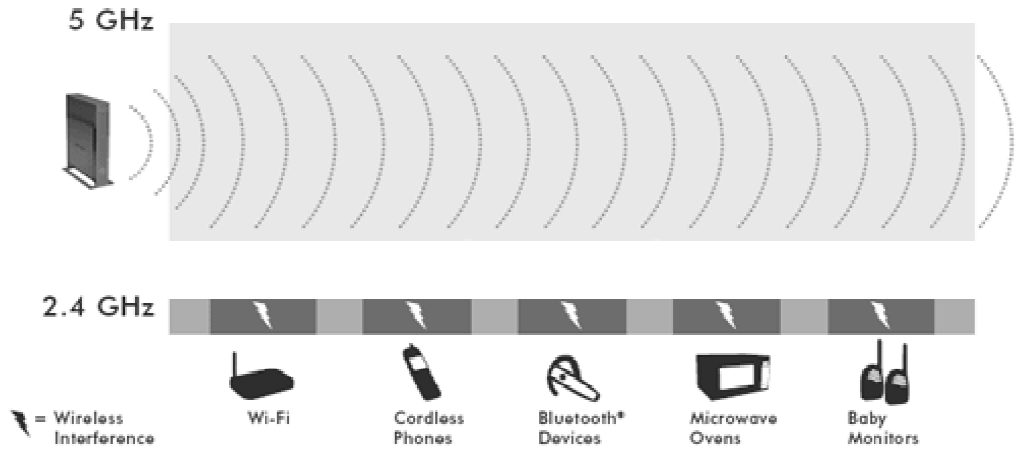


Figura 8: Interferencia de banda.

Fuente: http://www.broadbandbuyer.co.uk/images/products/NETGEAR/wnhde111_avoids-interference.gif

En el diseño y planeación de redes inalámbricas, como mejor práctica de industria, se debe tomar en cuenta los anteriores problemas de radio frecuencia descritos, para obtener un resultado eficiente a la hora de la implementación de la red planeada.

2.1.4 Antenas y su funcionamiento

Observamos anteriormente que un dispositivo de red que irradie señales de radio frecuencia para realizar transmisiones, necesita originar sus ondas con un generador de corriente alterna para luego pasar ésta hacia la antena que es la encargada de generar la transmisión en el medio inalámbrico. Las antenas, por lo tanto, juegan un papel fundamental en las comunicaciones inalámbricas y es necesario explorar su funcionamiento, entender cómo transmiten en el aire y su capacidad de cobertura.

2.1.4.1 Teoría de antenas

El principal objetivo de las antenas en los dispositivos inalámbricos será emitir la onda electromagnética que cumpla los requerimientos de cobertura para una transmisión exitosa según los distintos escenarios que se presenten. Cada onda tiene un comportamiento distinto en cuanto a la orientación de su movimiento y este se conoce como Polarización. Existen tres tipos de polarización de onda:

- Vertical: en el cual la onda oscila linealmente de arriba abajo.
- Horizontal: en el cual oscila linealmente de izquierda a derecha.
- Circular: en el cual la oscilación es circular hacia donde esté orientada la antena (Carroll, 71).

El siguiente gráfico ilustra las distintas oscilaciones y cómo se comportan las ondas según su polarización:

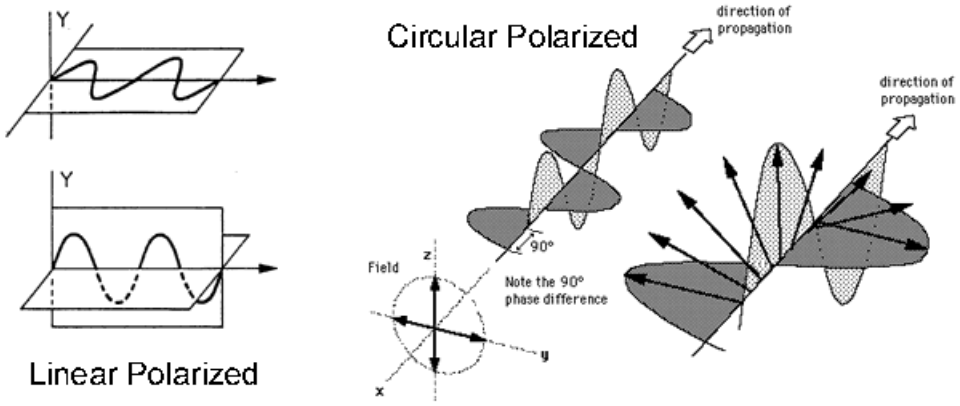


Figura 9: Polarización.

Fuente: http://www.air-stream.org.au/files/polorization.gif

2.1.4.2 Tipos de Antenas

Los dos tipos principales de antenas son las direccionales y omnidireccionales. Aunque ambas usen la misma cantidad de energía al momento de generar la onda, la diferencia radica en cómo cada haz de onda es enfocado. Se puede comparar con una linterna. Para el caso de una direccional, la linterna es apunta en una sola dirección y a pesar de que se usa la misma cantidad de energía, el haz de luz es mucho más potente en esa dirección específica. Por otro lado, con la misma linterna, si encajamos un embudo que proyecte el haz de luz en toda las direcciones (Omnidireccional) se obtiene una área más grande iluminada, pero el haz de luz es menos intenso, a pesar de que es la misma energía en uso (Carroll, 73).

2.1.4.2.1 Direccionales

Las antenas direccionales son aquellas que concentran todo su potencial de irradiación en una o más direcciones dependiendo de cómo estén orientadas. Esta característica les da me mayor desempeño en la transmisión de datos con un menor impacto de interferencia del ambiente. Por esta característica también, las antenas direccionales son mejor aplicables a escenarios de Red en conexión Punto a Punto, conexión entre edificios o diferentes campus de red donde exista línea de vista o para obtener una mejor recepción desde una infraestructura con antenas omnidireccionales (Carroll, 79). Para describir la forma de la onda producida por una antena direccional, usaremos un plano horizontal y vertical angular que está descrito en la siguiente figura:

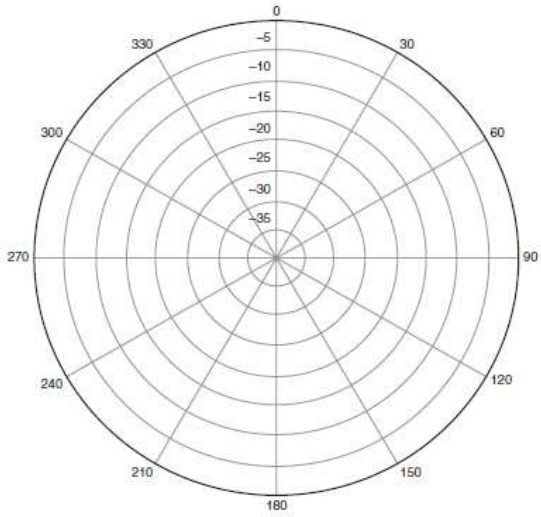


Figura 10: Plano Horizontal y Vertical Angular.

Fuente: Carroll, CCNA Wireless Official Guide, 74.

Las antenas direccionales más comunes, son las antenas Yagi que ofrecen un patrón de de radiación directo a donde estén apuntado. Este tipo de antena direccional tiene un amplio uso: desde televisores en casa hasta antenas para comunicación de redes inalámbricas (Carroll, 82). La onda producida por la antena Yagi direccional, descrita desde el plano de propagación horizontal se muestra en la siguiente figura:

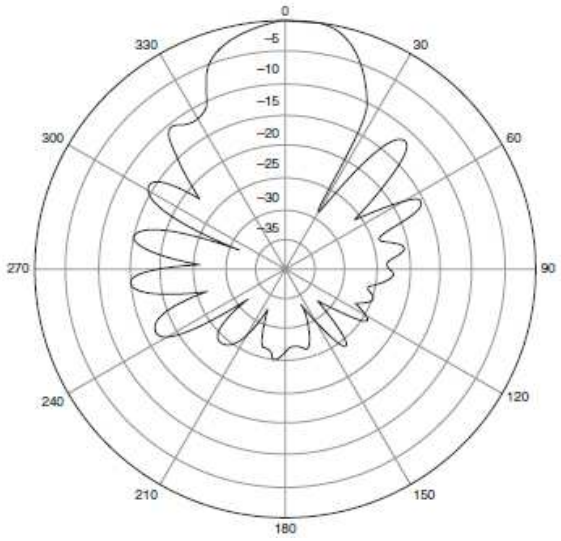


Figura 11: Patrón horizontal direccional Yagi.

Fuente: Carroll, CCNA Wireless Official Guide, 84.

El siguiente gráfico describe la misma onda direccionada producida por la antena Yagi, pero desde una perspectiva de elevación vertical:

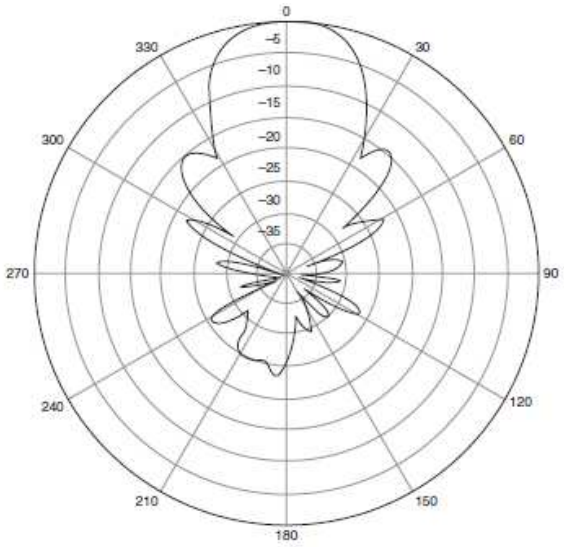


Figura 12: Patrón vertical Yagi.

Fuente: Carroll, CCNA Wireless Official Guide, 85.

Como podemos observar en cada plano, horizontal y de elevación, el comportamiento de la onda producida por una antena direccional, brinda mayor potencia hacia una dirección específica según la orientación de la antena.

2.1.4.2.2 Omnidireccionales

Como está implícito en el nombre, la onda generada por una antena omnidireccional da como resultado cobertura en todas las direcciones. Regresando al plano horizontal, con la antena omnidireccional llegaremos a una cobertura de ondas uniformes que abarca completamente los 360 grados (Carroll, 76). Dentro de plano vertical, se describe la onda como decreciente en potencia cuanto más cerca esté del eje de irradiación de la antena y creciendo a medida que se va alejando del eje que la origina. El patrón final de irradiación, conjugando los dos planos, se asemejará al de un anillo. Gráficamente en el plano horizontal se describe la onda de esta manera:

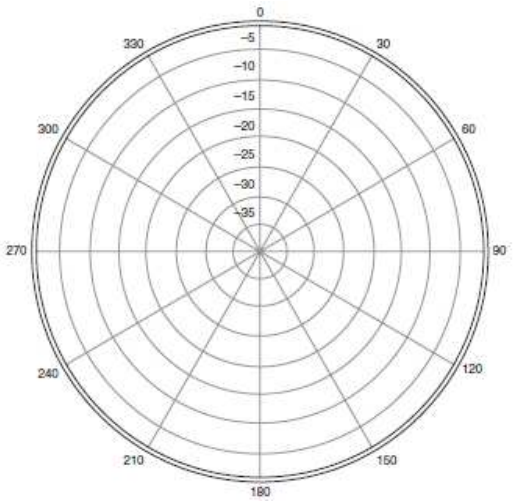


Figura 13: Patrón horizontal omnidireccional.

Fuente: Carroll, CCNA Wireless Official Guide, 73.

El siguiente gráfico describe la misma onda omnidireccional desde una perspectiva de elevación vertical:

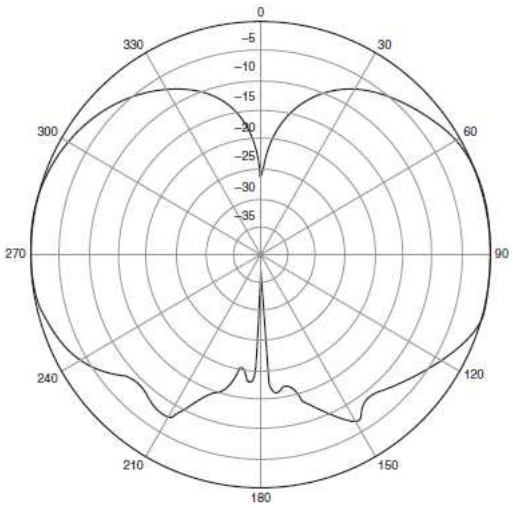


Figura 14: Patrón vertical omnidireccional.

Fuente: Carroll, CCNA Wireless Official Guide, 75

Como resultado de ambos planos, la cobertura tridimensional que ofrece la antena omnidireccional es una onda en forma de anillo y gráficamente se describe de la siguiente manera:

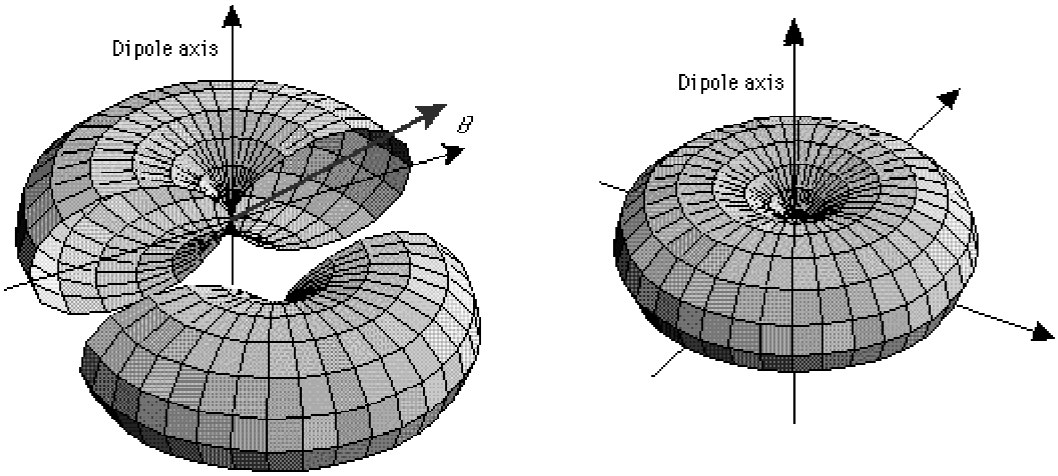


Figura 15: Plano tridimensional omnidireccional.

Fuente: http://people.seas.harvard.edu/~jones/es151/prop_models/dipole.gif

2.1.4.3 Protocolos WLAN (802.11)

El organismo encarga de la estandarización de los protocolos inalámbricos es el Instituto de Ingenieros Electrónicos y Eléctricos (IEEE). El estándar que fue definido para el uso de la mayoría de redes inalámbricas actuales es el protocolo 802.11 desarrollado por la IEEE en 1997 (Carroll, 100), al igual que todos los estándares subordinados que se expondrán más adelante como son 802.11 a/b/g y n.

2.1.4.4 802.11 estándar

El protocolo estándar 802.11 representa el comienzo de las Redes Inalámbricas de Área Local (WLAN). Desarrollado en 1997, solo podía operar a velocidad de 1 a 2 Mbps, lo cual se debía a que utilizaba las técnicas de modulación de Salto de Frecuencia del Espectro (FHSS) y Secuencia Directa del Espectro (DSSS), técnica descrita en una sección anterior. La compatibilidad con los clientes a estas velocidades es mandatoria, es decir, que si un usuario final necesita operar a otras velocidades distintas, no importa si tiene compatibilidad con 1 y 2 Mbps, será considerado como no compatible por los dispositivos que utilizan este estándar. Esta es la característica fundamental para que se haya perdido casi toda la compatibilidad con este estándar en la actualidad. Este protocolo opera tan solo en el rango de frecuencia de 2.4 GHz con once canales permitidos, de los cuales, tres canales no se sobrelapan: 1, 6 y 11. Como resultado de todas estas características, en la actualidad el protocolo 802.11 estándar está casi completamente en desuso (Carroll, 100) y fue reemplazado por los siguientes estándares.

2.1.4.5 802.11b

Este protocolo apareció como suplemento del estándar 802.11 por la necesidad de velocidades mayores que pudieran competir con la velocidad de cable que al momento era de 10 Mbps y lo que ofrecía este protocolo era velocidades de hasta 11 Mbps. El protocolo 802.11b guarda compatibilidad con las velocidades de 1 y 2 Mbps del protocolo anterior usando las mismas técnicas de modulación y codificación. Sin embargo al usar las velocidades de 5.5 y 11 Mbps, se utiliza diferentes técnicas de modulación resultando en una cantidad mayor de datos enviados en el mismo periodo de tiempo. 802.11b fue ratificado por la IEEE en 1999 sin una Solicitud de Comentarios (RFC) ya que se reservó su uso para personas con alto presupuesto (Bidgoli, et al., 198). Un RFC es un documento donde se estandariza los protocolos de internet y se solicita a usuarios de los protocolos, comentar para poder desarrollar actualizaciones o depuraciones de estos estándares. El protocolo contiene once canales con tres canales no sobrelapados: 1, 6 y 11. Este protocolo admite el uso de cambio de rango dinámico (DRS) que consiste en que los clientes de un Punto de Acceso (AP) puedan cambiar dinámicamente las velocidades en las que operan de acuerdo a la distancia que tienen desde el AP. Es así como al alejarse del Punto de Acceso los rangos bajan a 1 o 2 Mbps y suben al acercarse a velocidades de 5,5 y 11 Mbps (Carroll, 101). Aunque este protocolo fue uno de los más utilizados en años pasados gracias a sus características de flexibilidad y compatibilidad, en la actualidad no está entre los más usados en redes inalámbricas de área local ya que se desarrollaron otros protocolos más avanzados.

2.1.4.6 802.11g

En junio de 2003, la IEEE ratificó el estándar del protocolo 802.11g con rangos de velocidad más altos que los protocolos anteriores, esta vez con velocidades de hasta 54 Mbps. El rango de frecuencia utilizado por este protocolo se sitúa en el de 2,4 GHz lo que le ayuda a mantener la compatibilidad con el protocolo 802.11b en las velocidades de 1, 2, 5.5 y 11 Mbps en tanto se usen las mismas técnicas de modulación y codificación como Secuencia Directa del Espectro (DSSS). Para poder conseguir mayor rango de velocidad 802.11g utiliza la técnica de modulación de Multiplexación por División de Frecuencia Ortogonal (OFDM), descrita en una sección anterior. El rango de velocidades alcanzado por este estándar a través de OFDM es: 6, 9, 12,18, 24,36, 48 y 54 Mbps con los mismos once canales que contienen tres que no se sobrelapan (Carroll, 101-102).

2.1.4.7 802.11a

Al igual que 802.11b, 802.11a fue ratificado por la IEEE en 1999 pero difieren en el uso de la frecuencia que son 2,4 GHz y 5 GHz respectivamente. Por ello 802.11a es incompatible con los protocolos 802.11, b y g, lo que lo convierte en un protocolo menos popular en el uso de redes inalámbricas a pesar de que el uso del rango de frecuencia de 5 GHz, mitiga el problema de interferencia de banda con teléfonos inalámbricos, microondas y dispositivos bluetooth que funcionan en el rango de 2.4 GHz. Otra ventaja mayor en el uso de 802.11a es la disponibilidad de 12 a 23 canales no sobrelapados en contraste con los tres canales de este tipo que se

maneja en los protocolos b/g. Al usar OFDM, la división ortogonal permite que los sub-canales se puedan sobrelapar. Este estándar define velocidades de 6, 12, 24 y 54 Mbps (Carroll, 106). Un inconveniente con el uso de 802.11a radica en que las señales propagadas por los dispositivos que funcionan con este estándar pueden sufrir un fenómeno de frecuencia donde las múltiples señales divididas son desviadas de su posiciones ideales, por mala implementación por ejemplo, causando así degradación, menos eficiencia al transversar paredes u otros cuerpos sólidos que generen absorción y en consecuencia, menor desempeño comparado con los estándares 802.11b/g,

2.1.4.8 802.11n

El protocolo 802.11n se ha ratificado como estándar recientemente y ha abandonado su estatus de “draft” que duró siete años. La IEEE ratificó este estándar en 2009 (McCabe). Este protocolo guarda compatibilidad con los estándares 802.11a/b/g y en teoría alcanzaría velocidades mayores a 300 Mbps en ambientes de 802.11n puros y hasta 100 Mbps en ambientes con clientes de otros estándares. Las capacidades de compatibilidad y velocidad se deben a que utiliza múltiples antenas dentro de la tecnología MIMO (Multiple-in, Multiple-out) descrita en una sección anterior. El mecanismo usado en la tecnología MIMO consiste, a breves rasgos, en que mediante el uso de múltiples antenas, se puede enviar y recibir información simultáneamente resultando en mayor desempeño y velocidad de característica full dúplex (Carroll, 108).

Conociendo los distintos tipos de estándares de protocolos de red inalámbrica (McCann, y Ashley), pasaremos ahora a explorar los distintos tipos de topologías existentes en la actualidad según su magnitud geográfica, interacción con el usuario final y su utilidad.

2.1.5 Topologías Wireless

Al hablar de topologías de redes inalámbricas, hay distintas maneras de abordar el tema. Por área de cobertura puede ser una de las primeras formas de abordar, ya que dentro de esta categoría encontramos las redes de área local (WLAN) o las redes de área amplia (WWAN), que pueden abarcar municipios, ciudades o regiones. Otra categoría para abordar el tema de las redes inalámbricas pueden estar definido por la interacción que presentan con usuarios finales. Una red de área personal (WPAN) como dispositivos bluetooth o Ad hoc puede variar con una red de telefonía celular a pesar de que ambas están enfocadas a brindar un servicio de telecomunicación a usuarios finales (Carroll, 52).

2.1.5.1 WLAN

Las redes inalámbricas de área local (WLAN) están diseñadas para que el servicio de cobertura inalámbrica vaya de 35 a 70 metros aproximadamente desde los dispositivos de infraestructura como Puntos de acceso (AP) hasta los usuarios finales, dependiendo del protocolo en uso. Pueden escalar desde oficinas caseras a

grandes redes empresariales de campus. El hecho de que sean de área local significa que en su mayoría la administración de la infraestructura sea local.

Utilizan el rango de frecuencias entre 2.4 GHz y 5 GHz con usuarios e infraestructura "doble-banda" que significa que pueden operar en cualquiera de las dos frecuencias. Esta característica también puede implicar el uso mixto de los estándares 802.11a/b/g con sus respectivas frecuencias, codificadores y técnicas de modulación. Para el correcto funcionamiento de las redes de área local es necesario irradiar mayor potencia eléctrica para producir las ondas requeridas, sin embargo se debe vigilar el uso de la potencia con referencia a los organismos de control local, como la FCC por ejemplo en Estados Unidos o la CONATEL para nuestro país, para no exceder los límites de radiación en cada caso de las bandas no-licenciadas.

Estas redes de área local están diseñadas para proveer servicios a usuarios móviles además de servidores de impresión, almacenamiento, recursos compartidos, etc. (Carroll, 53), lo cual agrega complejidad a la administración y genera la necesidad de implementar seguridad, autenticación, encriptación entre otros tantos requerimiento en las redes actuales.

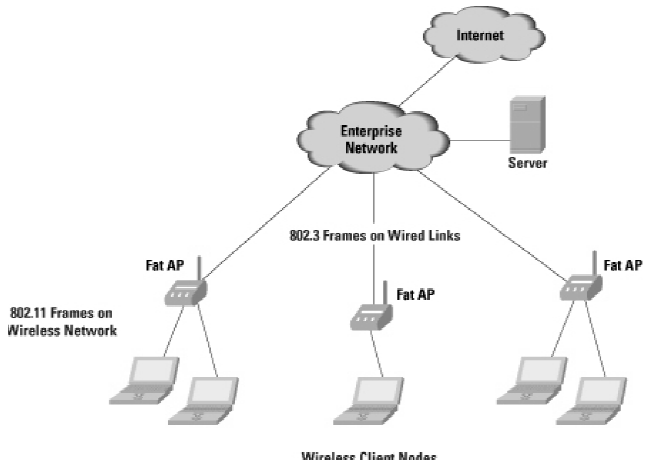


Figura 16: WLANs

Fuente: http://www.cisco.com/web/about/ac123/ac147/images/ipj/ipj_9-3/93_wlan_fig1_lg.jpg

2.1.5.2 WWAN

Una red inalámbrica de Área Amplia (WWAN) es la que cubre un área geográfica extensa. Como características principales tenemos que su ancho de banda para transferir datos es reducido, se paga por su uso como la telefonía celular por ejemplo, y tiene un alto costo de implementación por infraestructura. Las tecnologías de red de área amplia más utilizadas en la actualidad son el Sistema Global para Comunicación Móvil (GSM) y División de Código Multi-Acceso (CDMA). En ambos casos se accede a servicio de datos y voz con un rango de velocidad de hasta 115 Kbps y el pago por el uso de esta infraestructura por lo general es basado en la cantidad de datos transmitidos (Carroll, 55).

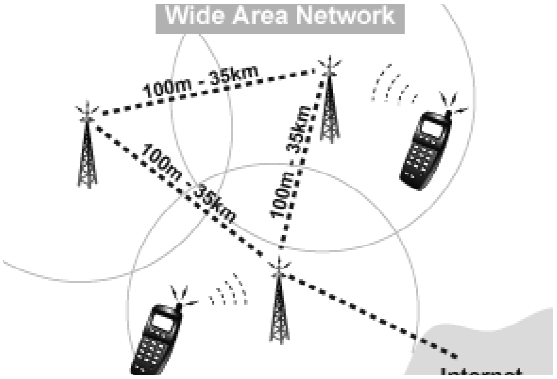


Figura 17: WWAN

Fuente: http://www.e-cartouche.ch/content_reg/cartouche/LBStech/en/image/networks-wwan.png

2.1.5.3 WiMax

Interoperabilidad para Acceso Microonda es un servicio de “última milla” que significa que provee servicios de conexión a suscriptores que desean obtener una alternativa a la red cableada. El objeto es recibir servicios como Televisión por cable o el

servicio de Línea de Suscriptor Digital (DSL). Esta infraestructura es capaz de brindar hasta 40 Mbps por canal fijo sin la necesidad de línea de vista con estaciones base. Está estandarizado dentro del protocolo de la IEEE 802.16. WiMax opera entre el rango de frecuencias de 10 – 66 GHz por lo cual no presenta problemas de interferencia con los rangos utilizados por las WLANs (Carroll, 138 - 139).

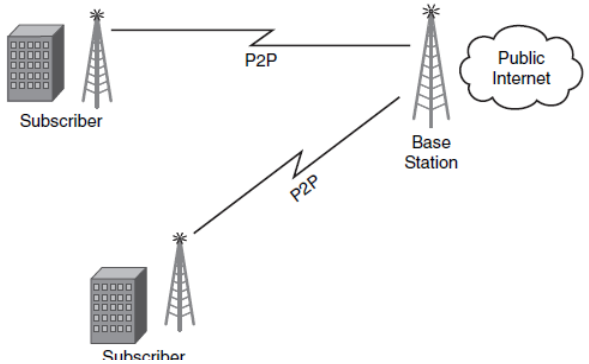


Figura 18: WiMax

Fuente: Carroll, CCNA Wireless Official Guide, 139

Las anteriores fueron descripciones de redes inalámbricas y sus topologías generales. Sin embargo las topologías definidas por el estándar 802.11 son de dos tipos: Ad Hoc o de Infraestructura.

Las redes de infraestructura describen el uso de dispositivos como Puntos de acceso que cumplen con la función de puente o intermediador entre el usuario final y la red. Los dispositivos de infraestructura de red además cumplen con la función de concentrar las comunicaciones de todos los usuarios dentro de la red.

2.1.5.4 Ad Hoc

La red Ad hoc en contraste con las redes de infraestructura, describen la comunicación y transmisión de dos o más equipos finales directamente conectados, sin tener otros dispositivos cumpliendo funciones de puente o concentrador de datos en la comunicación. En una topología de este tipo, es un equipo final el que define un nombre de red y parámetros como contraseñas, seguridad, etc., para que el resto de usuarios se puedan conectar. El equipo final crea un conjunto de Set de Servicio Básico (BSS) que define el área de alcance cobertura para que el resto se conecten. Este Set de Servicio Básico es independiente (IBSS) y no tiene ningún equipo intermediario como en la redes de infraestructura (Carroll, 55).

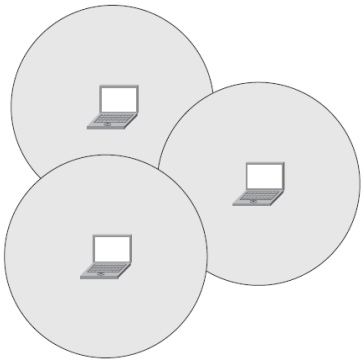


Figura 19: Redes Adhoc

Fuente: Carroll, CCNA Wireless Official Guide, 56.

En este diagrama, cada PC representa un Set de Servicio Independiente (IBSS), en otras palabras, cada usuario final es representa una red y un área de cobertura a la cual otros usuarios finales se pueden asociar. Esta clase de topología trae ciertos problemas a la hora de implementar seguridad ya que el control sobre autenticación o autorización es muy limitado.

2.1.5.5 Bluetooth

Bluetooth es un tipo de tecnología estándar (IEEE 802.15) ejemplo de las topologías de Red Inalámbrica Personal (WPAN). El rango de frecuencia usado por Bluetooth es el de 2.4GHz, por esta razón presenta interferencias con las redes WLANs. Sin embargo al estar diseñado para una cobertura de máximo 10 metros, bajo poder de transmisión y la técnica de modulación que usa es FHSS, su potencial de interferencia es reducido drásticamente. Bluetooth permite una conexión de hasta 8 dispositivos, 1 maestro y 7 esclavos (Carroll, 135).

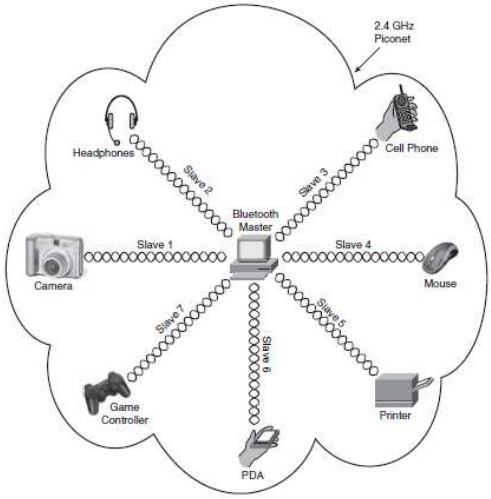


Figura 20: Bluetooth

Fuente: Carroll, CCNA Wireless Official Guide, 136.

Una vez exploradas las topologías más comunes en las redes actuales, trataremos un tema congruente a todas, el identificador o “nombre” con el cual los usuarios finales pueden interactuar y asociarse para obtener los recursos y servicios de red que requieren.

2.1.5.6 Nombre de Red (SSID)

Dentro de un Punto de Acceso, la red difundida está relacionada con su propia dirección de Control de Acceso al Medio (MAC) y a su vez, esta red aparece publicada con un Identificador de Set de Servicios (SSID) a los usuarios. Los nombres de red pueden variar desde uno simple que asocia su dirección MAC con un SSID constituyéndose en un Identificador de Set de Servicios Básico (BSSID) hasta uno de mayor complejidad que genera distintas direcciones MAC para distintos nombres de red que se podrían aplicar a redes que brindan servicio a usuarios invitados, de intranet, o corporativos constituyéndose en un Identificador de Set de Servicios Múltiple (MBSSID), haciendo una analogía, como si se tratase de un Punto de Acceso virtual que genera varias redes con el mismo hardware (Carroll, 58).

Dependiendo de la configuración, los Puntos de acceso envían por un periodo de tiempo regular tramas “Beacon” para difundir la red que contienen a potenciales usuarios finales. Sin embargo es configurable la difusión en el caso de que no se desee enviar estas tramas por medidas de seguridad de red pero esto implica configuraciones extras en los usuarios finales. La siguiente figura muestra la difusión de una red inalámbrica:

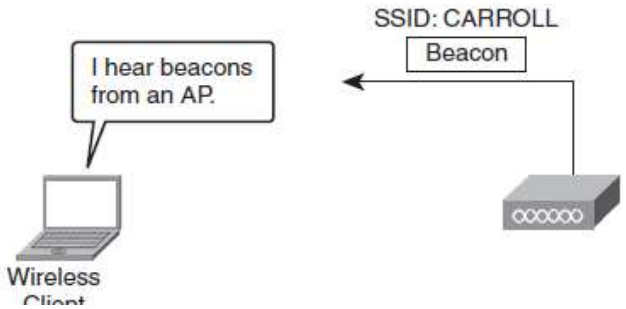


Figura 21: Difusión de red inalámbrica (SSID)

Fuente: Carroll, CCNA Wireless Official Guide, 121.

Una vez revisado los estándares de tecnología inalámbrica 802.11 y sus variantes, pasaremos a explorar la manera como el usuario final interactúa en el proceso de asociación a la red inalámbrica para obtener servicios y recursos.

2.1.6 Proceso de asociación: usuario – infraestructura

En el proceso de asociación usuario - infraestructura inalámbrica, el usuario primero y obligatoriamente debe estar en la zona de cobertura de los Puntos de acceso que, según su configuración, propagan el Identificador de Set de Servicios (Carroll, 147). En el caso de que la difusión de la red esté habilitada, el usuario pasa directamente al siguiente paso de asociación con la red donde se autentica, caso contrario, si no se difunde por medidas de seguridad de red, el usuario final requiere configuración adicional en su equipo donde se defina el nombre de la red SSID y parámetros de protocolo de autenticación, certificados, etc.

2.1.6.1 Transmisión de tramas inalámbricas

En la transmisión de tramas inalámbricas es importante considerar que estas redes funcionan por defecto en modo Half-duplex, es decir, en una transmisión un equipo solo debe enviar o recibir en el mismo periodo de tiempo, sin la capacidad de hacerlo simultáneamente. En el caso de que dos equipos transmitan en el mismo periodo de tiempo, puede ocurrir una colisión y obtendríamos una trama ilegible que necesita ser retransmitida.

La estrategia utilizada por la tecnología de red inalámbrica para tratar de mitigar este problema, en un medio compartido, es la Evasión de Colisión en un Medio de Múltiple Acceso (CSMA/CA), diferente a lo que encontramos en las Redes Cableadas Ethernet, donde la estrategia es la detección de colisiones en el medio, donde se opere en Half-duplex. En la estrategia CSMA/CA, el equipo que centraliza las comunicaciones debe determinar el estatus de las comunicaciones, es decir, si alguien está transmitiendo o el medio se encuentra libre para comenzar una nueva transmisión. Para determinar en qué periodo de tiempo cada equipo está autorizado para transmitir, se define un espacio de tiempo inter-trama (IFS). La IEEE definió los siguientes según su utilidad dentro de las comunicaciones inalámbricas:

- Espacio Inter-trama Corto (SIFS): para tramas con alta prioridad usadas comúnmente para reconocimiento (Acknowledgement) de recepción.
- Espacio Inter-trama de Punto-coordinador (PIFS): para tramas en Puntos de acceso que controlan la red.
- Espacio Inter-trama de Coordinación-distribuida (DIFS): para tramas de datos, que representan el lapso de tiempo estándar que debe esperar cada transmisor (Carroll, 109).

2.1.6.2 Encabezados

Dentro del proceso de transmisión, los encabezados de trama juegan un papel importante ya que aportan en cómo se deben distribuir los lapsos de tiempo cuando

las transmisiones ocurren y cuando el medio está libre para el envío de datos. La siguiente figura muestra una trama 802.11 completa con énfasis en el encabezado:

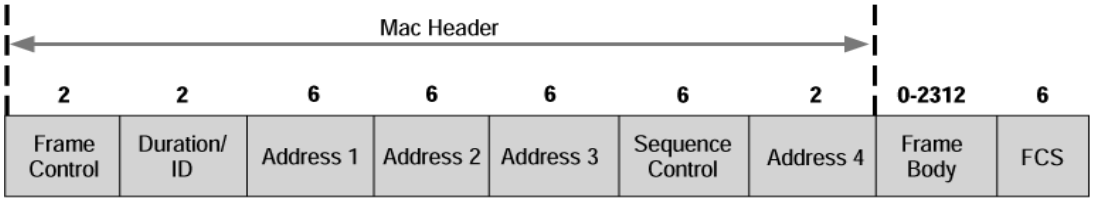


Figura 22: Trama 802.11.

Fuente: http://www.microsoft.com/mspress/books/sampchap/5566/0735614857-02.gif

El encabezado comienza con un Preámbulo donde se encuentra el campo de Tipo/Subtipo y un campo de Control de Trama, que pueden llegar de los 76 a 165 bytes. Continúa con una sección de “Flag” y luego el campo de duración. Este último es de suma importancia para que el medio sepa cuánto tiempo esta trama utilizará para su transmisión y evitar colisiones. Luego continúa con los campos de direcciones MAC que son de destino, Set de Servicios Básicos (BSSID) y dirección MAC de origen. El último es el campo de Control de secuencia que indica si la trama está fragmentada y el número de secuencia (Carroll, 119).

El siguiente gráfico muestra la captura de un encabezado de trama inalámbrica, en el orden respectivo de la descripción anterior:

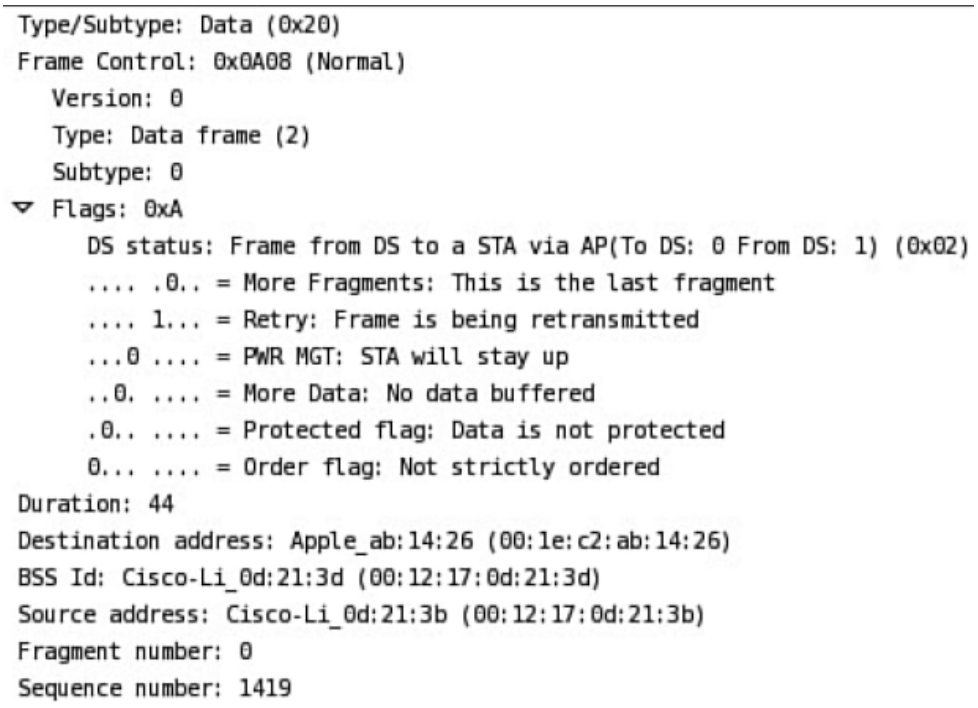


Figura 23: Encabezado de trama 802.11.

Fuente: Carroll, CCNA Wireless Official Guide, 119.

2.1.6.3 Tipos de tramas

Las tramas envueltas en el proceso de asociación, administración, datos y control de las redes Wireless definen las diferencias fundamentales entre las WLANs y las redes cableadas. Entre los principales tipos de tramas para la comunicación de red inalámbrica y que cumplen con las funciones de transmisión tenemos:

- “Beacon”: es un tipo de trama usada para que el usuario final pueda obtener información sobre la celda de red inalámbrica a la que puede acceder como por ejemplo el SSID lo que le permite potencialmente poder asociarse a la red.

- Trama de administración: usadas para asociarse o dejar la red inalámbrica representada por un SSID específico. Incluyen los tipos Solicitud de Asociación, Respuesta de Asociación, Solicitud de Re-asociación, Respuesta de Autenticación entre otros.
- Tramas de control: son tramas utilizadas para hacer reconocimiento (Acknowledgement) de que las porciones de datos enviadas han sido exitosamente receptadas.
- Tramas de Datos: son utilizadas para el envío efectivo de datos (Carroll, 116).

2.1.6.4 Conexión a la Red inalámbrica

Ahora que conocemos las bases más importantes dentro de la transmisión en una red inalámbrica, sus estrategias de evasión de colisiones en el medio de múltiple acceso, el modo en el que a través de temporizadores, definen cuando hay transmisiones y cuando el medio está disponible para posibles envíos y además que papel cumple cada tipo de trama y encabezados, haremos una descripción completa de lo que sucede en una conexión paso a paso.

1. El Punto de Acceso (AP) envía tramas “Beacon” cada 2 segundos para difundir el SSID de la red inalámbrica.

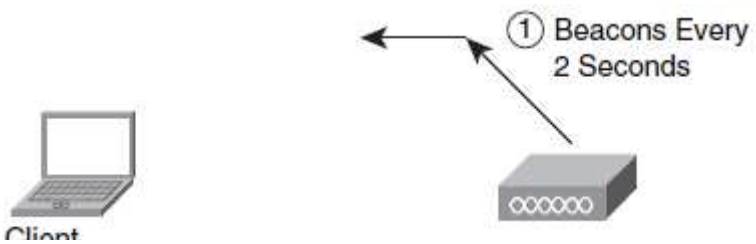


Figura 24: Tramas Beacon.

Fuente: Carroll, CCNA Wireless Official Guide, 125.

2. El Cliente hace un barrido del medio para encontrar las tramas “Beacon” y determinar si puede existir conexión con la red.

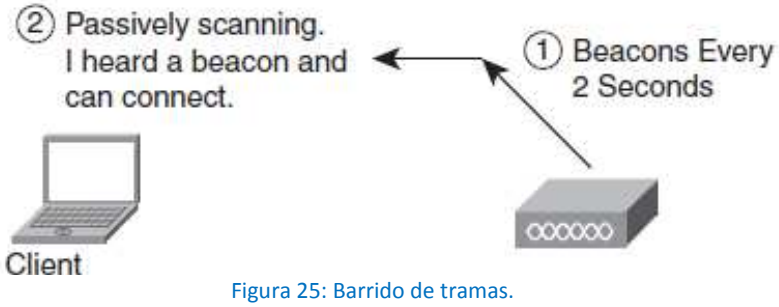


Figura 25: Barrido de tramas.

Fuente: Carroll, CCNA Wireless Official Guide, 125.

3. Si el usuario final decide entablar conexión se envía una trama “Prueba de solicitud” hacia el punto de acceso, caso contrario sigue en el paso anterior.

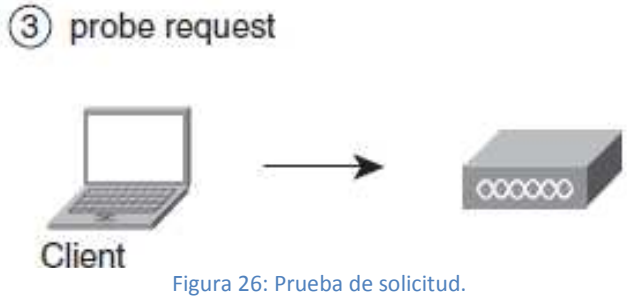


Figura 26: Prueba de solicitud.

Fuente: Carroll, CCNA Wireless Official Guide. 126.

4. El AP envía una trama “Prueba de respuesta” para probar si la conexión es posible.

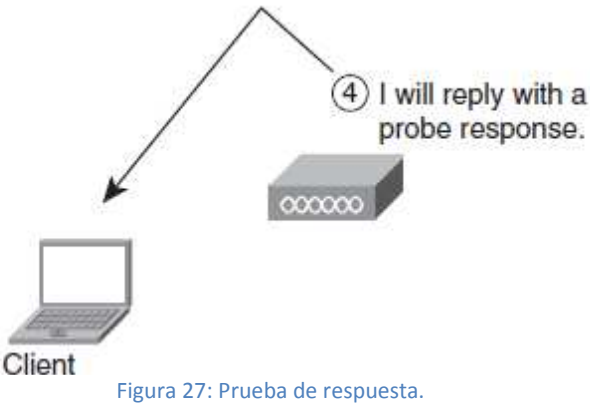


Figura 27: Prueba de respuesta.

Fuente: Carroll, CCNA Wireless Official Guide, 126.

5. El cliente continúa la petición de conexión con una trama “Solicitud de autenticación”, para poder ser autenticado dentro de la red.
6. El AP responde con una trama “Respuesta de Autenticación” y en caso de ser exitosa la autenticación pasarán al siguiente peldaño.

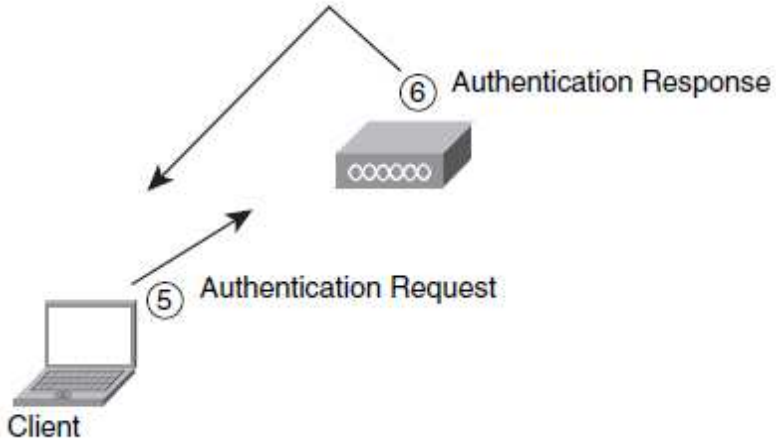


Figura 28: Solicitud y Respuesta de autenticación.

Fuente: Carroll, CCNA Wireless Official Guide, 126.

7. El cliente envía un “Solicitud de asociación”.
8. El AP responde con una trama “Respuesta de asociación” completando el proceso de asociación (Carroll, 125 - 127).

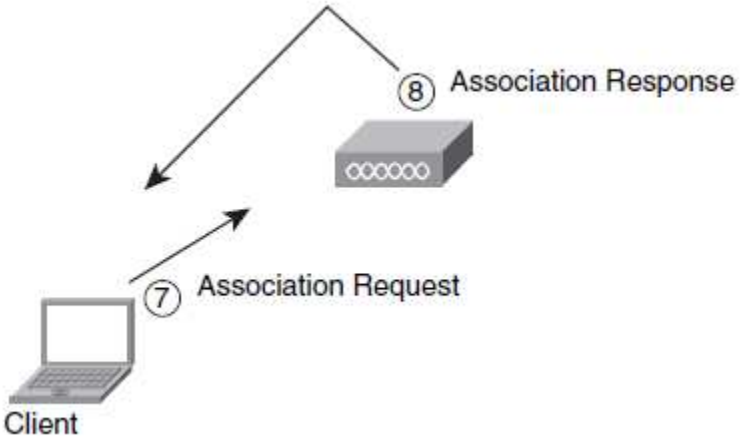


Figura 29: Solicitud y Respuesta de asociación.

Fuente: Carroll, CCNA Wireless Official Guide, 127.

Esta es una descripción general y resumida del proceso total de asociación. La descripción completa tiene dependencia de otras variables como los protocolos en uso 802.11, autenticación local o remota, compatibilidad, velocidades, etc.

2.2 Servicios de la Red inalámbrica

Previamente mostramos el proceso de asociación general que comúnmente los usuarios finales deben pasar para poder acceder a los servicios de la Red inalámbrica. La gama de servicios que ofrecen las redes inalámbricas hoy en día es amplia. Muchas aplicaciones de tiempo real como voz y video, datos, servicios de administración, seguridad de red, intranet, etc., se ofrecen ya sobre la infraestructura inalámbrica. Es por ello que observaremos a mayor detalle que ofrecen estas redes.

2.2.1 Administración centralizada

Uno de los servicios o características más importantes que deben ofrecer las redes de la actualidad es la centralización en la administración de infraestructura. Si bien podemos tener escenarios de oficinas caseras o pequeñas que son abastecidas con uno o dos puntos de acceso, la administración de cada uno de estos puede ser individual sin agregar complejidad a los administradores, sin embargo, los escenarios, en su mayoría ya no son de este tipo, es decir, los nuevos escenarios están en campus de compañías o empresas con una densidad de usuarios que requieren de múltiples puntos de acceso, con necesidades de cobertura ampliada,

ancho de banda suficiente para cubrir sus demandas, aplicaciones crítica en tiempo real, etc., lo que agrega una gran complejidad al labor de administración y hace imperativo que esta sea centralizada con fines de eficacia.

Las estrategias tomadas a nivel de hardware realizada por la industria en diferentes marcas, es la de centralizar la administración y configuración de todos los puntos de acceso de una infraestructura de red inalámbrica mediante Controladores LAN de redes inalámbricas (WLC). Es una práctica muy arraigada en el mercado actual dicha estrategia ya que simplifica la administración de muchos APs, genera configuraciones que son congruentes a lo largo de toda la red, censa el desempeño de la red como un conjunto entre otras ventajas (Carroll, 171).

2.2.1.1 Wireless LAN Controller

La función de un Wireless LAN Controller es la de lograr escalabilidad en una red inalámbrica grande. La controladora inalámbrica se comunica con los puntos de acceso siempre y cuando éstos operen en modo “lightweight” (LWAPP), que significa básicamente que operan enviando toda su información de Radio Frecuencia, estatus, configuraciones, etc., a la controladora y puede operar en capa 2 o capa 3 del modelo OSI.

Dentro de la gama de controladoras inalámbricas encontramos dispositivos o Appliances (hardware y software vendidos como una solución cerrada) independientes e interconectados a la porción cableada (LAN) de la red inalámbrica, así como basados en software dentro de switches o como módulos de routers de

Servicios Integrados (Carroll, 181). La solución depende del número de puntos de acceso existentes en la red. Por cada dispositivo, el número de APs puede llegar hasta las 500 licencias en marcas como Cisco y más allá de ese número, es necesario compartir la carga con otro dispositivo.

2.2.1.1.1 Descubrimiento de APs

Recordemos que los puntos de acceso deben correr el protocolo “lightweight” para funcionar con la controladora inalámbrica. Al encenderse un AP con el protocolo LWAPP en función, depende totalmente del WLC (Wireless LAN Controller) para funcionar. Primeramente el AP envía un mensaje de “LWAPP Solicitud de descubrimiento” que es una trama de inundación (Broadcast) en capa 2 (OSI), sin embargo este intento de contactar a la controladora debe fallar ya que el dispositivo se va a comunicar posteriormente con la misma solicitud a través del DHCP capa 3 (OSI) y en Cisco específicamente es la opción DHCP 43 (esto quiere decir que no es un parámetro estándar, por lo tanto se debe especificar como opción). Al recibir la controladora el “LWAPP Solicitud de descubrimiento” a través de la petición DHCP, esta responde con un mensaje “LWAPP Respuesta de descubrimiento”. Finalmente, si escoge una entre múltiples controladoras encontradas el paso siguiente es enviar un mensaje de “Solicitud de unión” para que la asociación se cumpla (Carroll, 196 - 197). Aunque este es el proceso general para la asociación punto de acceso – controladora, existen pasos adicionales descritos sobre validación de certificados y autenticación descritos en el siguiente gráfico:

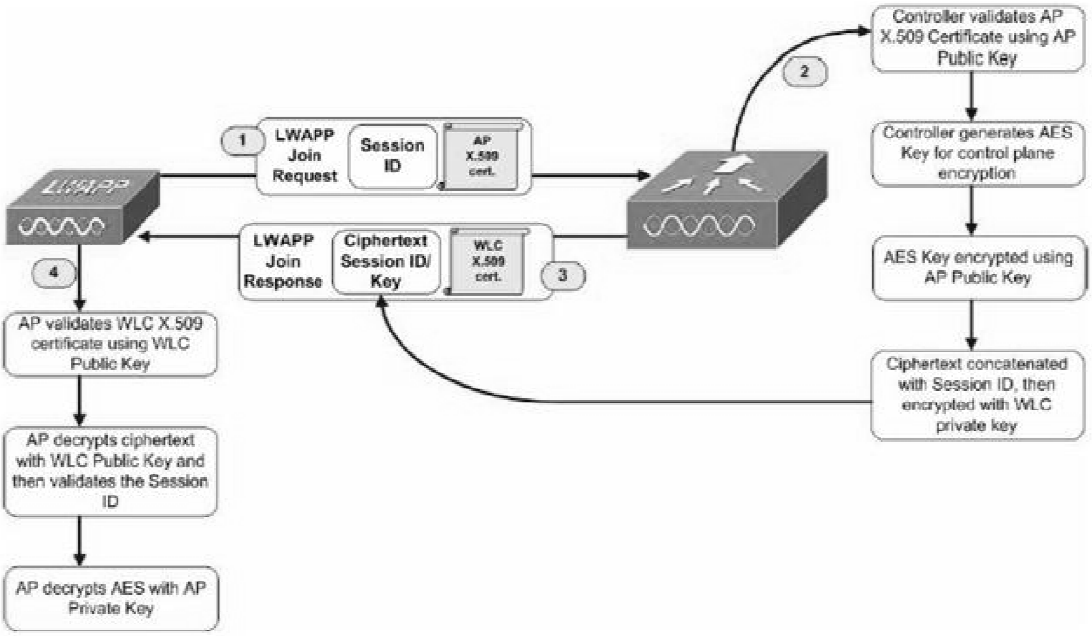


Figura 30. Asociación Punto de acceso – Controladora.

Fuente: http://4.bp.blogspot.com/_F0xKISdTaPM/TPP29o97ufI/AAAAAAAACDU/igQAyI7m-MY/s1600/lwapp_join_process.JPG

Después de que la asociación es exitosa, el Punto de Acceso entra en una fase de sincronizar su imagen de sistema operativo. La controladora sobre-escribe la imagen que contenga el AP a menos de que sea una igual y los mensajes LWAPP son los encargados de cargar el nuevo sistema operativo al punto de Acceso. Luego de cargar la imagen del sistema operativo que contiene, la controladora procede a exportar la configuración hacia todos los APs asociados.

2.2.1.1.2 Modos de Puntos de acceso APs.

En la descripción del proceso anterior hemos dado ya un tipo de punto de acceso: LWAPP. Este se define como "esclavo" o dependiente total de la controladora

inalámbrica para poder desempeñar su función de infraestructura para usuarios finales. Sin embargo, el otro modo principal para los puntos de acceso es independiente (Stand-Alone). En este modo el AP está imposibilitado de conectarse a una controladora y por ello toda la configuración y sistema operativo es de significancia local (Carroll, 204). El uso de este tipo de puntos de acceso se encuentra frecuentemente en ambientes de red con baja densidad de usuarios como oficinas pequeñas, caseras, pequeñas sucursales, etc., donde la administración no es grande y no necesita ser centralizada.

2.2.2 Compatibilidad

Como parte de la gama de servicios que las redes inalámbricas actuales deben ofrecer a los usuarios finales encontramos la capacidad de compatibilidad con los varios estándares de la IEEE 802.11 descritos anteriormente en la sección sobre estos protocolos. A pesar de que existe equipamiento y protocolos de que no necesariamente están dentro de este estándar desarrollado por la IEEE, está fuera de este trabajo la discusión de los mismos. Exploraremos aquí la capacidad de compatibilidad de estos equipos en las bandas 2.4 GHz y 5 GHz IEEE 802.11.

2.2.2.1 Bandas Soportadas

Dentro de la discusión de bandas soportadas actualmente como principales operando a 2.4 y 5 GHz encontramos la distribución de los diferentes estándares

802.11 según lo ratificado por la IEEE como característica propia en cada caso. Es así como tenemos lo siguiente según las bandas soportadas:

- 2.4 GHz: 802.11 histórico (que en casos específicos también operaba a 900 MHz), 802.11b, 802.11g y 802.11n (que específicamente opera a 2.4 y 5 GHz pero no está ratificado como los otros estándares).
- 5 GHz: 802.11a, 802.11n y dos borradores de estándar IEEE que al momento no han sido ratificados pero se encuentran en etapa de desarrollo: 802.11ac y 802.11ad.

2.2.2.2 Protocolos 802.11 soportados

La sección anterior nos da una idea concisa y resumida de cada estándar y la frecuencia en la que opera. Ahora observaremos como cada uno de ellos guarda interoperabilidad con otros estándares que comparte su frecuencia.

Los dispositivos que operan en conformidad con el protocolo 802.11g están en la capacidad de mantener interoperabilidad con los dispositivos que operan en 802.11b aunque esto significa un cambio en la velocidad de transmisión que es menor.

El protocolo 802.11b por su parte, se podría considerar una extensión del protocolo 802.11 original o “legacy”, por lo tanto guarda compatibilidad con el mismo pero en las velocidades específicas, a saber, 1 y 2 GHz. Esta característica ha dejado en desuso al protocolo 802.11 original.

La compatibilidad del protocolo 802.11a es sumamente reducida por operar en la banda de 5GHz. En realidad este estándar no es muy popular ya que es incompatible

con los protocolos 802.11 b/g. Guarda solo interoperabilidad con el protocolo estándar 802.11n cuando este se encuentra en operación de banda en 5 GHz.

Finalmente el protocolo 802.11n opera en ambas bandas 2.4 y 5 GHz haciéndolo el único compatible e interoperable con cada ambiente 802.11 o sea, a/b/g.

2.2.2.3 Velocidad de transmisión

Al momento hemos explorado los fundamentos de compatibilidad con respecto a las bandas de operación en el caso de los distintos tipos de protocolos 802.11 y como resultado en el siguiente gráfico se muestran de forma general las propiedades de cada uno y, muy importante, las velocidades que cada uno ofrecen para la transmisión:

	802.11a	802.11b	802.11g	802.11n
Maximum data rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps
Modulation technologies	OFDM	DSSS, CCK	DSSS, CCK, OFDM	DSSS, CCK, OFDM+
RF band	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz and 5 GHz
Number of spatial streams and antennas	1	1	1	Up to 4
Number of channels	23	3	3	26

Tabla 1: Propiedades de protocolos estándar 802.11

Fuente:http://www.eetkorea.com/ARTICLES/2006NOV/2/xEEKOL_2006NOV_BC.gif.pagespeed.ic.MLuVIMCyeb.png

2.2.3 Seguridad

La seguridad en redes, no solo inalámbricas, sino en redes de todo tipo, es uno de los servicios críticos que se debe ofrecer actualmente. Sin embargo la seguridad de redes no es un producto sino un proceso en constante regeneración. Se ha producido tal fenómeno ya que históricamente, desde el comienzo del mundo de las redes y telecomunicaciones, han venido de la mano ataques de distintos tipos, con objetivos distintos como: apoderamiento de información, denegación de servicio, probar la habilidad de Hackers para ingresar a redes, por nombrar unos pocos. El problema real surge cuando paulatinamente encontramos que si bien los ataques anteriores han requerido de mucho conocimiento para ser generados, con el paso de los años se generan herramientas que pueden ser de fácil uso para cualquier usuario sin conocimiento y sin embargo generar resultados catastróficos en las redes objetivo. Aunque la seguridad de redes depende de varios aspectos, revisaremos dos aspectos de mitigación principales: Autenticación y Encriptación.

2.2.3.1 Autenticación

Uno de los primeros aspectos a explorar en la seguridad de redes son los usuarios que se conectan a la red. ¿Están autorizados para acceder a la red? Esta pregunta se responde desde la perspectiva de la Autenticación. Mediante este mecanismo lo que buscamos es que los usuarios que se asocian a nuestra red estén previamente “seleccionados” para ingresar a recursos y que cumplan con cierto nivel de seguridad para mitigar ataques según el nivel de privilegios que manejen cada uno de ellos. El

sistema de autenticación permitirá que un usuario invitado a la red “Guest” tenga la capacidad de asociarse a una red con un nivel de privilegios básicos como navegación limitada, usuarios corporativos que se asocian a la red interna para acceder a recursos como archivos, impresoras o el sistema interno o, la autenticación también permitiría que un usuario administrador pueda asociarse con los recursos avanzados que requiere para realizar su trabajo de configuración o monitoreo.

Existen varios tipos de autenticación según el nivel de seguridad que cada una adicione a su mecanismo, como por ejemplo la autenticación abierta, la cual es débil o casi nula en materia de seguridad, hasta mecanismos más avanzados como 802.1x o RADIUS los cuales ingresan a su mecanismo servidores dedicados para seguridad con bases de datos de usuarios permitidos en la red con sus privilegios respectivos.

2.2.3.1.1 Abierta (Open)

La autenticación abierta es un mecanismo que no agrega seguridad alguna a la red. En realidad, se podría definir más como un proceso inherente al mecanismo de asociación usuario final – red inalámbrica. En el proceso de asociación descrito en una sección anterior, en la etapa de “Solicitud de autenticación – Respuesta de autenticación”, el punto de acceso autentica al usuario que en este caso, no ha enviado ningún tipo de contraseña o nombre de usuario (Carroll, 334). La autenticación abierta funciona en la capa 2 del modelo OSI y puede estar

configurada para no requerir ninguna información de parte del usuario suplicante, sin embargo es un proceso obligatorio para asociarse a la red y a pesar de no ingresar credenciales, siempre es exitoso. Este tipo de autenticación es usada con frecuencia en “Hot Spots” así los usuarios no tienen complicaciones al momento de asociarse y obtener el servicio de navegación. El siguiente gráfico muestra este sencillo método de autenticación:

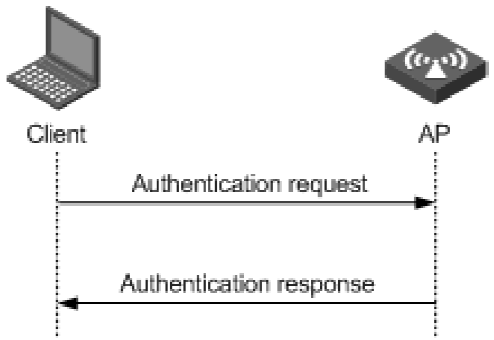


Figura 31: Autenticación Abierta.

Fuente:
http://www.h3c.com/portal/res/200812/26/20081226_709505_image002_624019_57_0.png

2.2.3.1.2 Llave Pre-compartida (PSK)

La autenticación de Llave Pre-Compartido (PSK) cuando funciona con el método de encriptación de Privacidad Equivalente a Red Cableada (WEP) no agrega mucha seguridad, pero funciona mejor que la autenticación abierta ya que en lugar de autenticar al usuario suplicante, lo que hace es verificar tan solo si tiene una llave o contraseña pre-compartida (Bidgoli, et al., 177). Además, las llaves WEP hoy en día son fácilmente descifradas lo que resulta en un mecanismo de seguridad poco robusto y vulnerable. El proceso con la Llave Pre-Compartida es el siguiente:

- El cliente envía una trama de “Solicitud de autenticación”.
- El punto de acceso responde con un mensaje en texto plano que contiene un desafío para el cliente.
- El cliente usa este texto para responder con un paquete encriptado de autenticación. La encriptación es realizada mediante una llave estática WEP que tiene el cliente.
- El Punto de Acceso compara el paquete de autenticación recibido con el resultado propio que obtiene del mensaje que envío previamente y su llave pre-compartida WEP. Si coinciden ambas, pasan al proceso de asociación.

El siguiente gráfico resume el proceso de autenticación mediante el uso de Llave Pre-Compartida (PSK) con encriptación WEP:

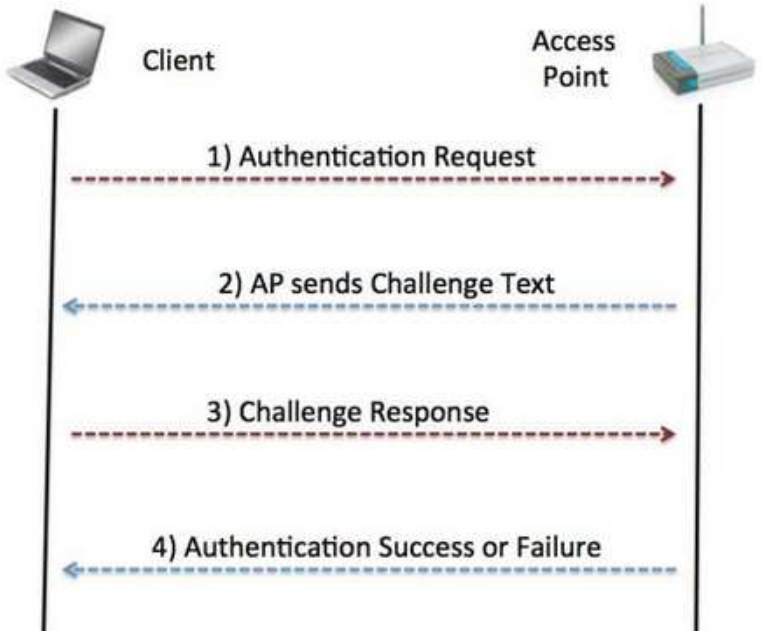


Figura 32: Llave Pre-compartida

Fuente: http://periwalaakar.blogspot.com/2012/04/cracking-wep.html

2.2.3.1.3 Filtrado MAC

El Filtrado basado en la dirección de Control de Acceso al Medio (MAC) es una manera simple de autenticar al usuario utilizando su dirección física. Se debe definir previamente en el punto de acceso o en un servidor de autenticación una lista de direcciones MAC de los equipos autorizados a asociarse a la red. Aunque la autenticación mediante la dirección MAC de un equipo es relativamente sencilla y práctica, no es un método seguro ya que se enfrenta a la posibilidad de que se modifique en un equipo no autorizado una dirección MAC que sí está autorizada lo que resulta en la asociación de un usuario no legítimo (Bidgoli, et al., 86).. El siguiente gráfico resume el mecanismo de autenticación mediante filtrado MAC:

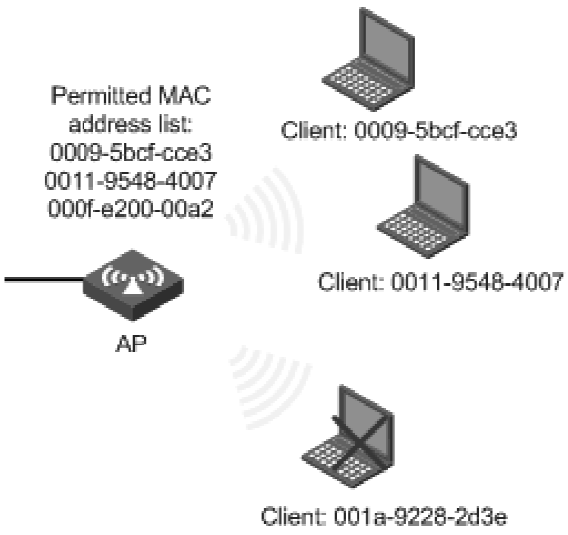


Figura 33: Filtrado MAC.

Fuente: http://www.h3c.com/portal/res/200812/26/20081226_709508_image005_624019_57_0.png

Hemos revisado los métodos más sencillos y comunes en ambientes de hogar y de oficinas pequeñas. Estos mecanismos están clasificados dentro de la autenticación local, es decir, que se valida la autenticidad de los usuarios finales a través de los

recursos o base de datos local del punto de acceso. Sin embargo, en la clasificación de los métodos de autenticación tenemos la autenticación centralizada donde los dispositivos utilizados no son locales sino que están como dispositivos dedicados a este fin.

Los métodos de seguridad centralizada presentan esquemas más robustos de autenticación como el protocolo 802.1x o el uso de servidores como RADIUS que serán descritos a continuación.

2.2.3.1.4 802.1x

802.1x es un estándar ratificado por la IEEE. Por lo general el funcionamiento de este protocolo es basado en “puertos” y depende del modelo de Autenticación, Autorización y Auditoría (AAA). Este modelo básicamente es una gama de mecanismos que permiten al usuario autenticarse para después ser dispensado con los servicios, recursos y privilegios que le corresponden por políticas y finalmente, se contabilizan, registran y auditan todas sus acciones posterior a los dos pasos preliminares. 802.1x usa en sus comunicaciones un Protocolo de Seguridad Extensible (EAP), el cual garantiza un modelo de autenticación más robusto a los previamente revisados de clasificación local (Watkins, y Wallace, 232-233). El mecanismo de 802.1x para autenticar a un usuario suplicante de asociación a la red inalámbrica, se puede describir de la siguiente manera:

- El punto de acceso requiere que cliente “suplicante” envíe sus credenciales.
- El usuario “suplicante” envía sus credenciales al “autenticador”

- El punto de acceso a su vez, envía la información de credenciales al servidor autenticador, que puede ser a través de un paquete RADIUS o TACACS+ en el caso de un ambiente Cisco.
- El servidor RADIUS o TACACS+ devuelve un paquete de desafío al punto de acceso y este de regreso al suplicante. El desafío va de acuerdo al protocolo usado ej.: WEP o EAP.
- El cliente envía un mensaje de respuesta al desafío enviado por el servidor RADIUS.
- El servidor RADIUS envía el mensaje de acceso exitoso si la autenticación es válida y adicionalmente, una llave WEP o EAP de sesión.
- La llave EAP es usada por el punto de acceso para la comunicación entre éste con el servidor autenticador.
- El punto de acceso a su vez, envía esta llave EAP para la comunicación con el cliente y adiciona una llave Broadcast/Multicast EAP para el cliente ya que estas clases de comunicaciones están protegidas por el mecanismo 802.1x, así que el Broadcast o Multicast generado por el cliente puede ser escuchado solo por el punto de acceso.

El siguiente gráfico resume el proceso de asociación a la red inalámbrica mediante el método de autenticación 802.1x:

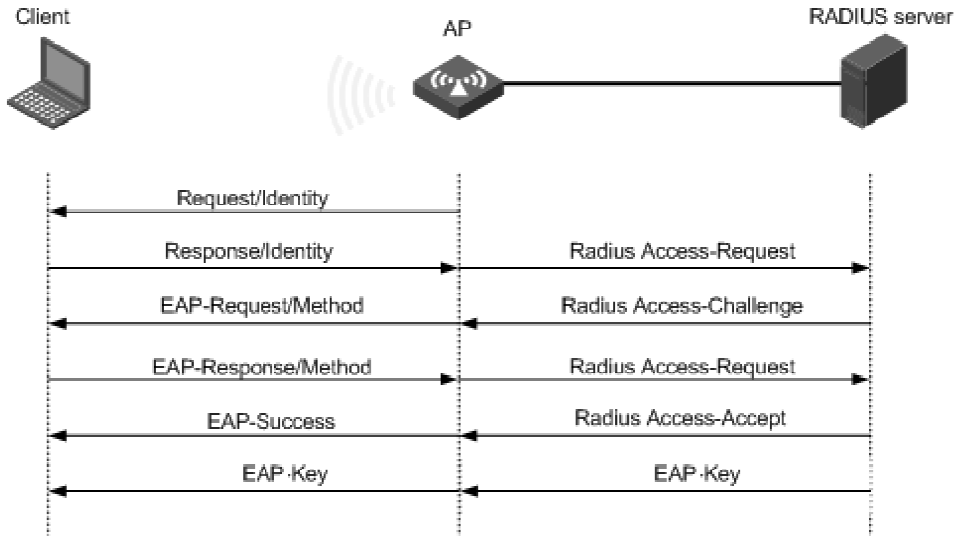


Figura 34: 802.1x

Fuente: http://www.h3c.com/portal/res/200812/26/20081226_709510_image007_624019_57_0.png

2.2.3.1.5 RADIUS

El Servicio de Autenticación Remota Dial-In (RADIUS) es un protocolo que provee centralización para esquemas AAA anteriormente discutidos. Existen varias maneras de implementar un servidor de autenticación RADIUS, es decir, se puede encontrar como servidor dedicado, como parte de un appliance de Cisco conocido como Servidor de Control de Acceso (ACS) o como aplicativo dentro de un dispositivo como un router de Servicios Integrados. Este protocolo funciona a nivel de capa 7 del modelo OSI y se comunica en capa 4 a través del protocolo UDP (Watkins, y Wallace, 142). Las principales funciones del servidor RADIUS en producción y en concordancia con el esquema AAA son:

- Autenticar a los usuarios que poseen credenciales válidas.

- Autorizarlos a que obtengan los recursos, servicios y privilegios que se han dispuesto según las políticas establecidas.
- Finalmente guardar información de auditoría de cómo actúa cada usuario con respecto a sus privilegios dentro de la red.

El siguiente gráfico describe la función de un servidor RADIUS al autenticar a un usuario suplicante en una comunicación donde interviene un Servidor de Acceso a la Red (NAS):

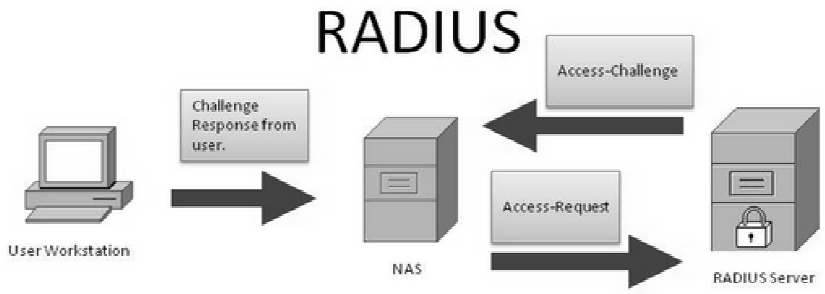


Figura 35: RADIUS.

Fuente: http://russsevinsky.com/wp-content/uploads/2012/03/RADIUS5c.jpg

2.2.3.2 Encriptación

Otro de los pilares fundamentales de la seguridad en redes inalámbricas es la encriptación, esto es porque todos los datos enviados y recibidos están en un medio totalmente compartido donde cualquiera, con el conocimiento para hacerlo, puede capturar comunicaciones. Según la capacidad de cada protocolo para cifrar los datos encontramos métodos menos seguros como la Privacidad Equivalente a Red Cableada (WEP) hasta métodos más seguros como Acceso Inalámbrico Protegido (WPA).

2.2.3.2.1 WEP

Como está implícito en su nombre, la finalidad de este algoritmo es la de brindar confidencialidad equivalente al de una red de cable. Sin embargo la encriptación WEP es muy débil y se ha demostrado actualmente que las sus llaves que consisten ente 10 y 24 caracteres hexadecimales con descifrables fácilmente. El principal motivo para su poca seguridad es que el proceso de autenticación la comunicación entre el cliente y autenticador es en texto plano y el cifrado que usa (RC4) es vulnerable al combinar este desafío en texto plano con la llave WEP (Bidgoli, et al., 77). Actualmente WEP es una solución adecuada para redes inalámbricas de hogar u oficina pequeña, pero no entrega seguridad significativa en ambientes más grandes como campus corporativos, empresas, etc.

2.2.3.2.2 WPA

Como opción al mecanismo tan poco robusto que ofrecía el cifrado WEP, se introdujo en 2003 el protocolo de Acceso Wireless Protegido (WPA) no como un estándar sino como una solución de empresa y proveedores provisional para mitigar de cierta manera el mecanismo tan ineficiente de WEP (Bidgoli, et al., 92). WPA ofrece un mecanismo más robusto de encriptación ya que al usar el protocolo TKIP (Protocolo de Integridad de Llave Temporal) se cambian dinámicamente las llaves que se usan en la comunicación. Adicionalmente al uso del protocolo de TKIP se puede usar el Protocolo Estándar Avanzado de Encriptación (AES) entregando así un esquema de seguridad muy robusto, pero con un costo adicional por mejoras en el equipamiento.

Dentro del esquema de WPA existen dos formas para que el usuario final se autentique:

- **Modo Empresa:** en este modo se requiere un servidor dedicado, por ejemplo un RADIUS para la autenticación y distribución de llaves.
- **Modo Personal:** en este modo se utilizan Llaves Pre-Compartidas (PSK), constituyéndose en un esquema más débil de seguridad (Carroll, 346).

2.2.3.2.3 WPA 2

WPA2 es compatible con el estándar 802.1i desarrollado como mejora de WPA. Esta mejora fue hecha a través del reemplazo de hardware. Como método de encriptación en WPA2 tenemos el uso extensivo del mecanismo AES y en el caso de TKIP, el uso es casi nulo ya que este último no ofrece un mecanismo tan fuerte. Una de las mejoras de este protocolo en comparación con su antecesor es que existe un caché de llaves o contraseñas que está habilitado para así brindar una mayor velocidad de reconexión (Carroll, 347 - 348). Al igual que WPA anterior, el funcionamiento de WPA2 sigue manteniendo los dos modos: Personal y Empresa. La siguiente tabla resume las diferencias más importantes entre WPA y WPA2 en cuanto a sus esquemas de autenticación – encriptación y ambientes de producción más comunes en cada caso:

	WPA	WPA2
Enterprise mode (Business, education, Government)	Authentication: IEEE 802.1X/EAP Encryption: TKIP/MIC	Authentication: IEEE 802.1X/EAP Encryption: AES-CCMP
Personal mode (SOHO, home and personal)	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: AES-CCMP

Tabla 2: Comparación WPA – WPA2.

Fuente: http://new.ciscotests.org/assets/images/icnd1/37-wpa-and-wpa2-modes.jpg

2.2.4 Redundancia

La redundancia en redes de topo tipo es una de las características fundamentales que se debe ofrecer para garantizar alta disponibilidad en el servicio. Los datos críticos que circulan en las redes inalámbricas como: tráfico de voz, video o información transaccional, por nombrar unos cuantos, dependen de un esquema de alta disponibilidad para continuar con un constante funcionamiento sin importar los errores o caídas que pueda sufrir la infraestructura de red. La garantía de esta alta disponibilidad se logra a través de la redundancia. Para el caso de las redes inalámbricas es de alta importancia revisar la redundancia en dispositivos como Puntos de Acceso (APs) y Controladoras LAN de red Inalámbrica (WLC) (Carroll, 201). Haremos de igual manera, una revisión resumida de la redundancia en la porción de red cableada LAN o nivel de switches.

2.2.4.1 Redundancia en Puntos de acceso

La redundancia en puntos de acceso se describe como múltiples APs dentro del mismo dominio de radio frecuencia. Este esquema se usa con el fin de mitigar problemas de un mal desempeño en la cobertura. Estos implica que cuando un AP no brinda la cobertura por caída de hardware, en una celda inalámbrica, los demás APs redundantes incrementan su poder de irradiación subiendo niveles de potencia o incluso cambiando el canal en el que operan con la finalidad de mitigar los problemas de cobertura en determinada área para poder brindar el servicio a los usuarios finales que se encuentren en dicha celda (Carroll, 201).

En el esquema de redundancia de puntos de acceso cabe recalcar la importancia de una controladora de área local de redes inalámbricas (WLC) ya que en este dispositivo se lleva a cabo la automatización de los procesos de auto configuración de potencia para cobertura, detención de la caída en los APs que forman una celda y también de un censo o “survey” que se puede realizar a la red inalámbrica para garantizar la alta disponibilidad.

El siguiente gráfico muestra esta relación de redundancia entre APs y cómo la controladora LAN Wireless aporta en el esquema de redundancia:

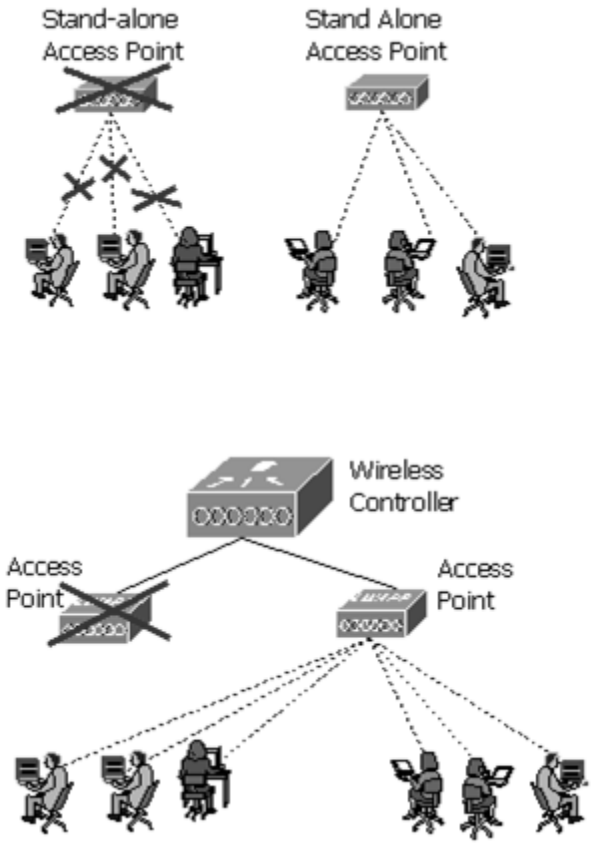


Figura 36: Redundancia en puntos de acceso.

Fuente: http://www.excitingip.com/wp-content/uploads/2010/03/autofailover.bmp

2.2.4.2 Redundancia en Controladores

Ahora bien, el segundo aspecto importante a tratar a la hora de desarrollar una red inalámbrica de alta disponibilidad es la redundancia de WLC, la misma que tiene varios escenarios de implementación según el esquema que se haya escogido para obtener alta disponibilidad. Entre los esquemas de redundancia de WLC tenemos los siguientes:

- El diseño N + 1: En este diseño cada controladora tiene un solo punto de redundancia o “backup”. Si este controlador de backup es compartido por

múltiples WLC, puede ser contraproducente por la carga que cada uno aplica en un solo dispositivo. La siguiente figura muestra este esquema:

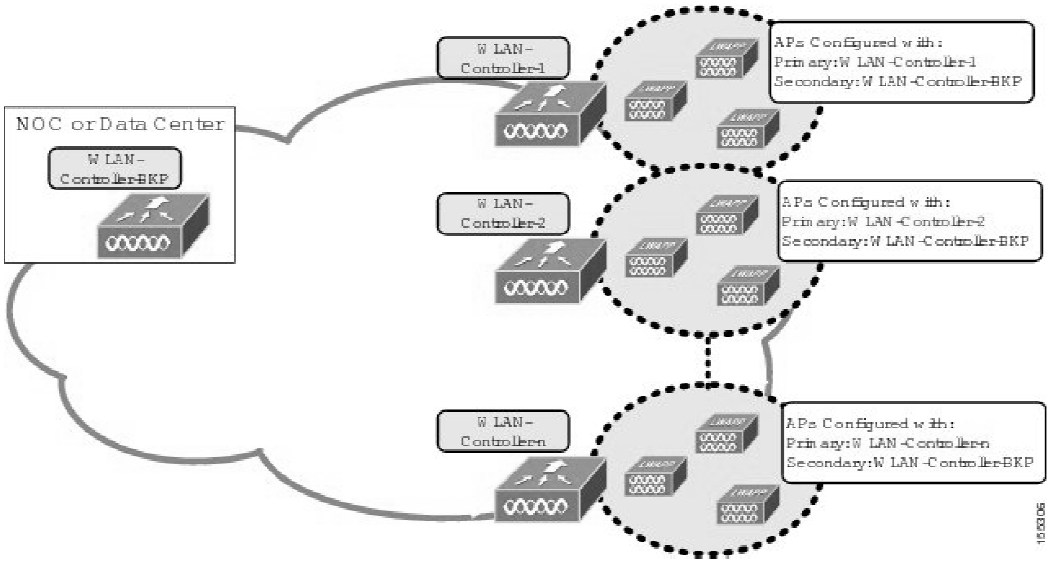


Figura 37: Redundancia WLC N + 1.

Fuente: http://www.cisco.com/en/US/i/100001-200000/150001-160000/155001-156000/155306.jpg

- El diseño N + N: para este caso cada WLC es un backup de todos los participantes en el esquema de redundancia. Es así como cada AP puede asociarse a una controladora primaria y a su vez tener como secundarias a todas las demás como un backup para garantizar la continuidad del servicio. La siguiente figura muestra el esquema N + N:

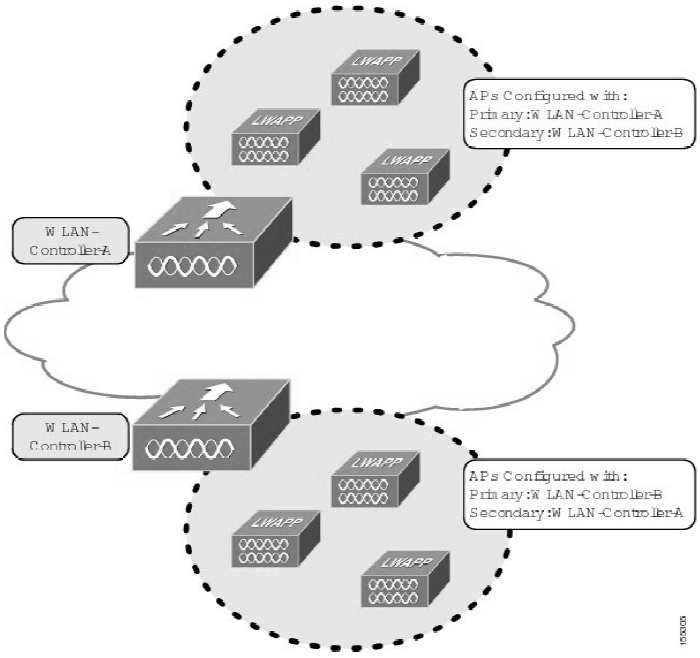


Figura 38: Redundancia WLC N + N.

Fuente: http://www.cisco.com/en/US/i/100001-200000/150001-160000/155001-156000/155305.jpg

- El diseño N + N + 1: Es el diseño de mayor redundancia que se puede implementar. En resumidas cuentas, es una síntesis de los dos diseños anteriores al que agregamos una WLC como backup “ternario” (Carroll, 202).

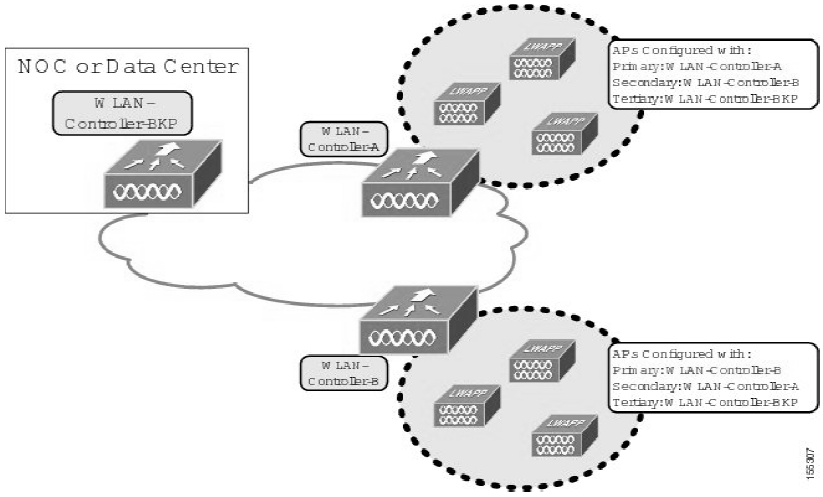


Figura 39: Redundancia WLC N + N + 1.

Fuente: http://www.cisco.com/en/US/i/100001-200000/150001-160000/155001-156000/155307.jpg

La caída de la controladora por distintas razones como falta de energía, sobrecarga de CPU, fallo de sistema operativo, o la pérdida del enlace con la red cableada, puede significar un perjuicio para los usuarios que requieren los recursos de red para poder realizar sus actividades laborales. Los esquemas de redundancia están encaminados a mitigar este impacto. La siguiente figura muestra uno de los escenarios más comunes de red inalámbrica con redundancia en WLC (N + 1):

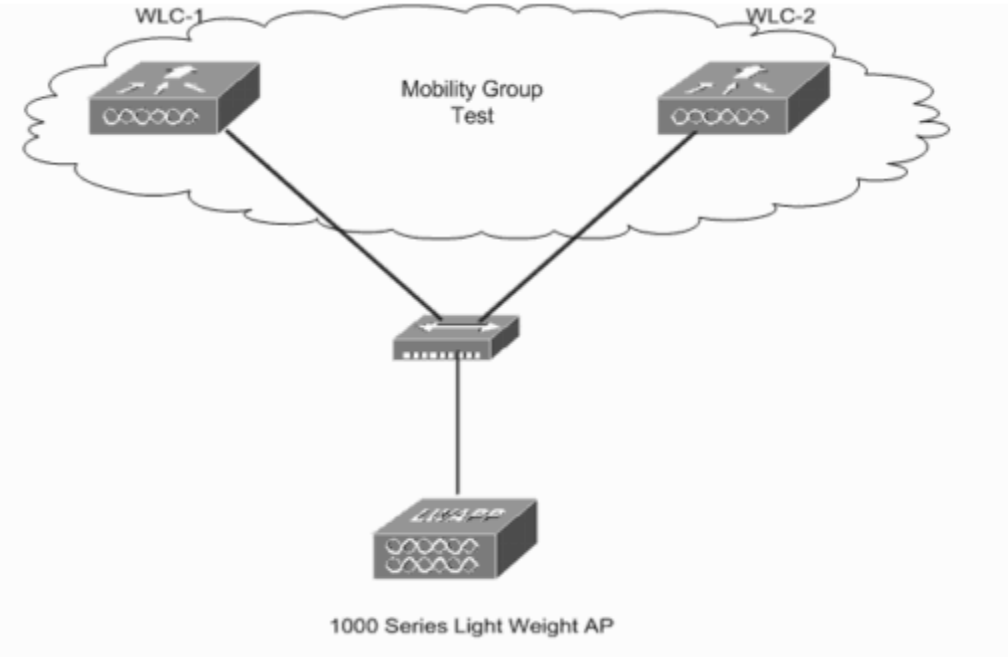


Figura 40: Redundancia de WLC.

Fuente: http://www.cisco.com/image/gif/paws/69639/wlc_failover-1.gif

2.2.4.3 Redundancia de red cableada.

Parte de la discusión de redundancia inalámbrica depende también de la disponibilidad del servicio a través del esquema de alta disponibilidad que tengamos en nuestra porción de red cableada. Como demuestra la figura anterior, la comunicación entre los puntos de acceso y la WLC, está intermediada casi siempre

por uno o más switches que proveen un enlace “Uplink” (enlace a entidad de mayor jerarquía en la red) para que la red inalámbrica se integre con todos los servicios ubicados en las porciones de red con cable: como servidores, impresoras, central telefónica, etc.

Logramos obtener redundancia “switching” mediante la adquisición de otro dispositivo de similares capacidad para eliminar el punto único de falla. Surge un problema en la redundancia de switches ya que, al tener múltiple enlaces en direcciones similares, se pueden formar bucles, ya que los dispositivos funcionan en la capa 2 del modelo OSI. La redundancia switching depende de un protocolo estándar que sirve para mitigar este problema: Spanning Tree Protocol (STP). El algoritmo de STP permite una red de switches libre de bucles ya que bloquea lógicamente los caminos redundantes (Black, 81). El siguiente gráfico describe el funcionamiento de Spanning Tree Protocol en un ambiente switching redundante:

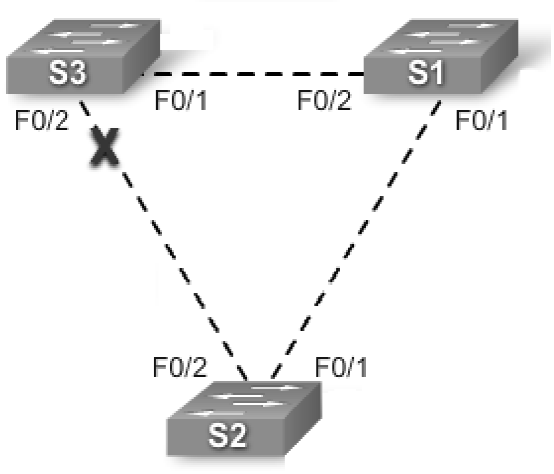


Figura 41: Redundancia de red cableada.

Fuente: https://ls-a.org/lib/exe/fetch.php?media=school:stp-port-decisions.png

Como podemos ver, el puerto F0/2 del Switch 3 fue bloqueado para evitar bucles en esta red. La discusión profunda del funcionamiento del este protocolo está fuera del alcance de este documento ya que se trata principalmente las redes inalámbricas y su funcionamiento, sin embargo existe documentación completa en la web, fuentes como los documentos IEEE o Cisco que ofrecen un detalle completo sobre todo lo referente a Spanning Tree Protocol.

2.2.5 Cobertura a Usuarios Móviles (Roaming)

Uno de los servicios más importantes que las redes inalámbricas hoy en día deben ofrecer a sus usuarios, es la continuidad de cobertura a usuarios móviles. Es aquí cuando los esquemas de Roaming entran en acción. Los usuarios dentro de un campus corporativo no están obligados a estar en un mismo sitio siempre, como por ejemplo sus oficinas, sino que necesitan cambiar su posición ocasional o frecuentemente, así: sala de reuniones, conferencias, cafeterías, etc.; lo que no debe ser un problema ya que en cualquiera de estos distintos lugares deben mantener conexión con la red inalámbrica (Carroll, 210). El esquema de Roaming es posible dentro de una red inalámbrica donde la administración esté centralizada en una WLC.

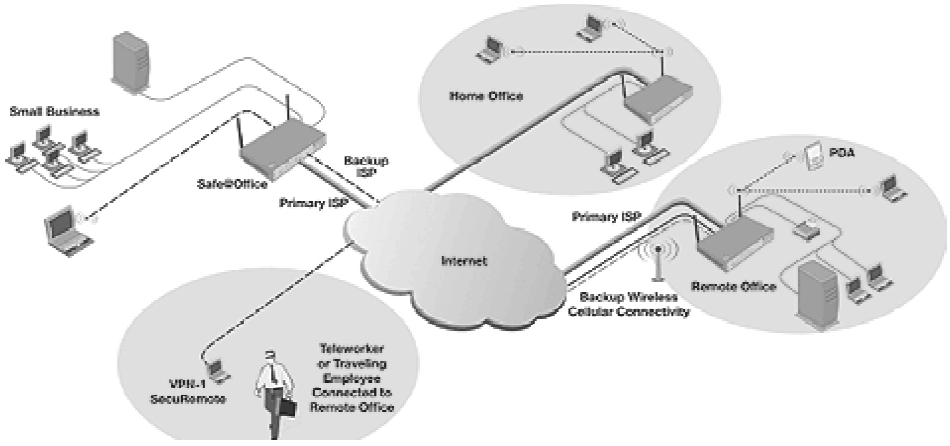


Figura 42: Roaming.

Fuente: http://www.checkfirewalls.com/images/wireless_roaming.gif

2.2.5.1 Teoría de Roaming

Para entender la teoría de Roaming, debemos comenzar revisando los grupos de movilidad (Mobility Groups). Un grupo de movilidad es un ajuste dentro de una WLC donde se define un conjunto al cual pertenecen una o más controladoras. Estos grupos definen que controladoras van a compartir información sobre clientes que están haciendo Roaming (Carroll, 210).

2.2.5.2 Grupos Roaming

Mediante estos grupos de movilidad o Roaming, los clientes son capaces de cambiar su posición física sin preocuparse por la reconexión ya que al definirse los grupos, las controladoras comparten la información de estos usuarios. Además de los grupos móviles, existen los dominios móviles. Estos se usan también para garantizar que los usuarios del Roaming no pierdan continuidad en la conexión y cobertura pero esto implica comunicación a través de la red cableada además de configuraciones extra en las controladoras que forman parte de un mismo dominio (Carroll, 210). Las siguientes figuras ejemplifican a los Grupos móviles y a los Dominios móviles:

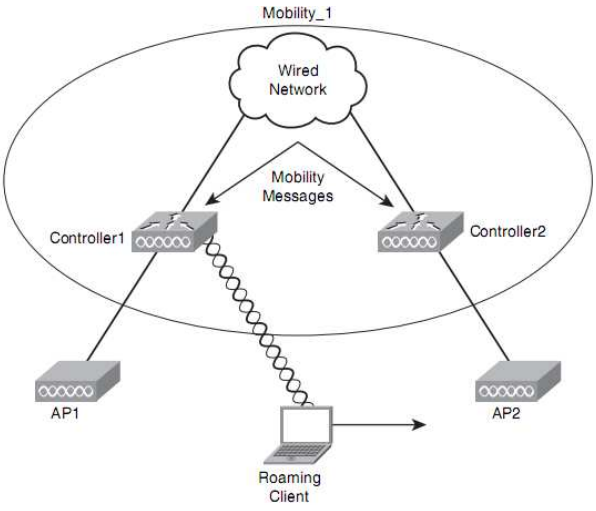


Figura 43: Grupo Móvil.

Fuente: Carroll, CCNA Wireless Official Guide, 211.

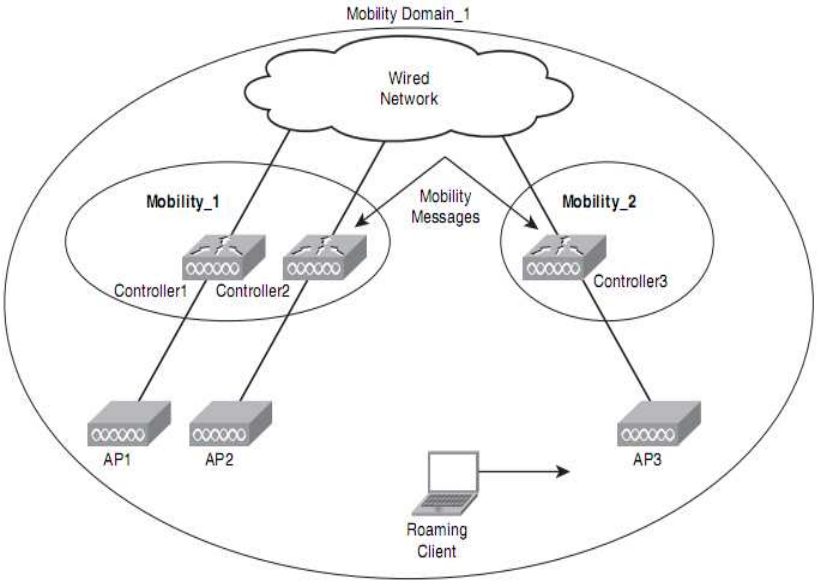


Figura 44: Dominio Móvil.

Fuente: Carroll, CCNA Wireless Official Guide. 211.

2.2.5.3 Tipos de Roaming

Según su configuración, el Roaming puede efectuarse las capas 2 y 3 del modelo OSI. Partiendo de los conceptos anteriores de Grupo móvil y Dominio móvil, los dos tipos de Roaming son:

2.2.5.3.1 Roaming de Capa 2 (OSI)

Para el caso en que el usuario que está haciendo uso de la característica Roaming de su red inalámbrica y no cambia su dirección IP, su subred o su VLAN aunque haya cambiado de punto de acceso, estamos haciendo uso del Roaming en Capa 2. En resumidas cuentas, es totalmente transparente al usuario el hecho de que se ha

enviado una solicitud de autenticación al cambiar de AP y que esta ha sido procesada como un cliente previamente autorizado, continuando así con los servicios y la cobertura. Este mecanismo se conoce como “Roaming Intra-Controladora”. Para el caso en el que el cliente se cambia de grupo de movilidad, es decir, a otra controladora, el proceso de Roaming es Inter-controladora. En este caso la información de clientes que comparten las distintas controladoras de un mismo grupo sirve para garantizar la continuidad de servicios de conexión y cobertura a los usuarios finales. En este caso el cliente sigue con la misma dirección IP, en la misma VLAN y no tiene que realizar una petición DHCP que cortaría la sesión (Carroll, 215). Las siguientes figuras describen el Roaming capa 2 en sus modos Intra e Inter-controladora:

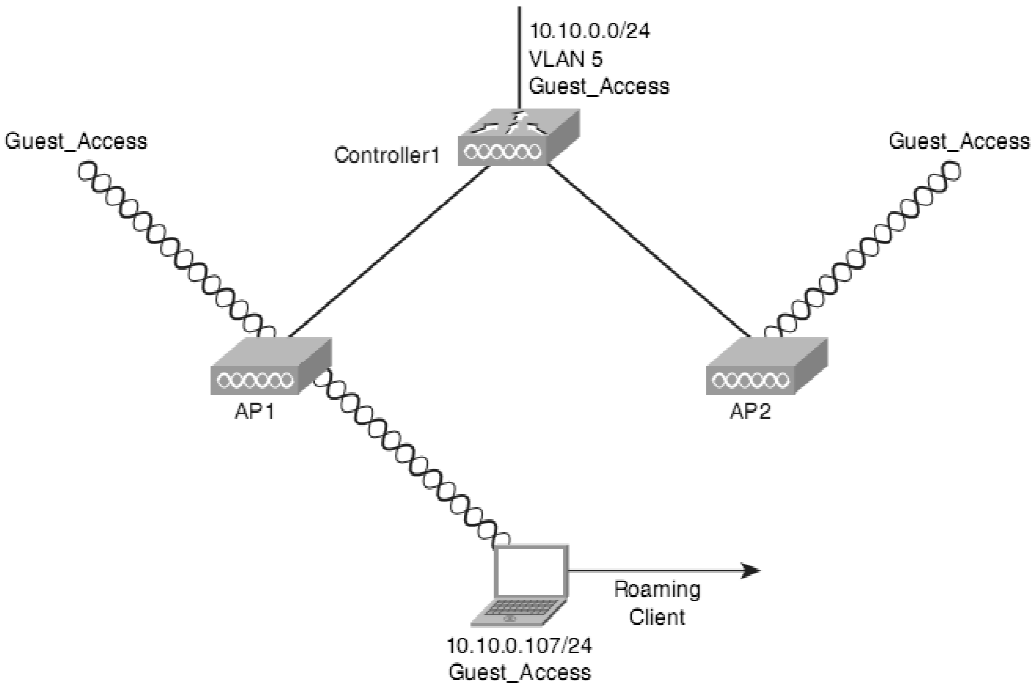


Figura 45: Roaming capa 2 Intra-controladora.

Fuente: Carroll, CCNA Wireless Official Guide, 215

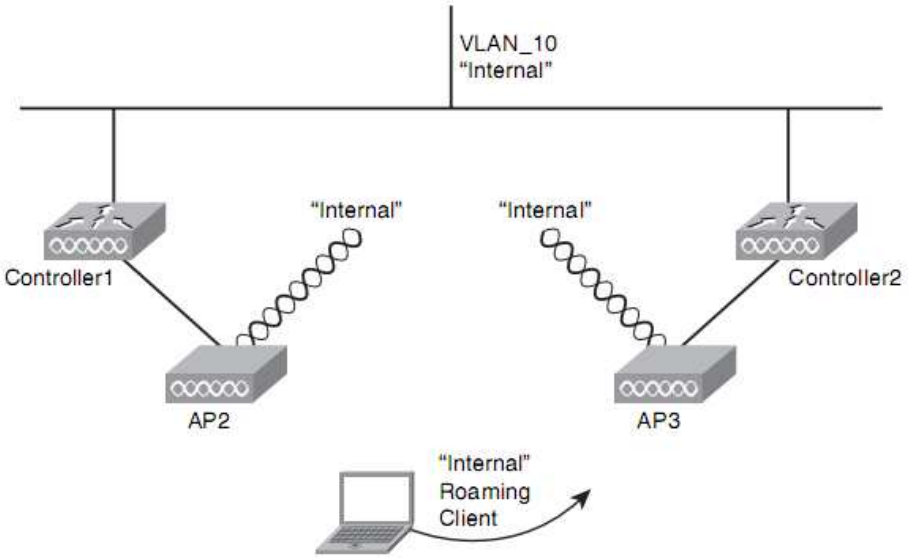


Figura 46: Roaming capa 2 Inter-controladora.

Fuente: Carroll, CCNA Wireless Official Guide, 216.

Resumiendo, podemos decir que el Roaming en capa 2 del modelo OSI es el que permite al cliente continuar con la misma subred y VLAN, convirtiéndose en el más transparente al usuario final.

2.2.5.3.2 Roaming de Capa 3 (OSI)

A diferencia del esquema de capa 2 donde el usuario se maneja en la misma subred y VLAN, el esquema en capa 3 presenta otro escenario ya que aquí encontramos múltiples WLC operando en diferentes subredes. En el esquema de Roaming capa 3

la meta es que si el usuario se mueve de controladora y esta tiene otra subred, el cliente debe ser asociado con la misma subred mediante túneles que permitan a la controladora comunicar al usuario con la controladora que se asoció en primera instancia. El Roaming en capa 3 del modelo OSI se logra mediante las siguientes clases de túneles:

- **Túnel Asimétrico**: en este modo de túnel, la información del cliente es enviada directamente hacia su destino, sin importar la dirección de origen de los datos. Ahora bien, al regreso de datos de respuesta, la información llega a la controladora donde el cliente se asoció primeramente llamada “ancla” y luego esta reenvía los datos a la controladora donde el cliente se encuentre operando. La palabra asimétrico se refiere a que los caminos que deben tomar los datos al momento del envío y de recibir una respuesta, no son los mismos. El siguiente gráfico describe este esquema de tunelización (Carroll, 216):

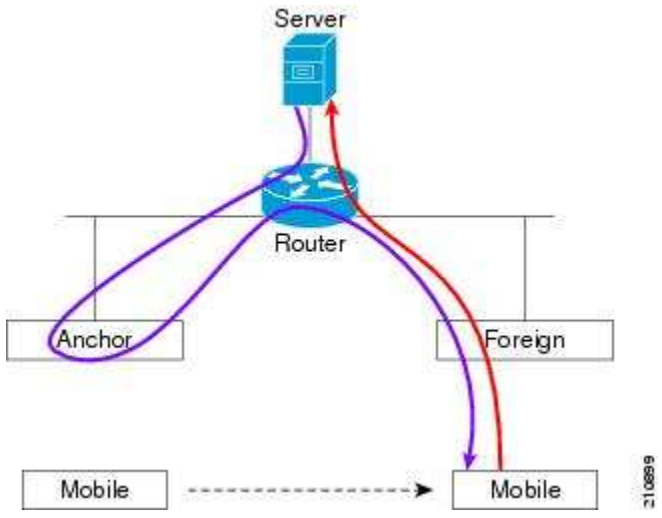


Figura 47: Túnel Asimétrico.

Fuente: http://www.cisco.com/en/US/i/200001-300000/210001-220000/210001-211000/210899.jpg

- **Túnel simétrico**: en este esquema de Roaming capa 3, todos los datos de envío deben ser llevados a través del túnel a la controladora ancla, es decir, donde el usuario final se asoció la primera vez y obtuvo la dirección IP de una subred perteneciente a la misma. La respuesta de datos de igual manera pasa primero por la controladora ancla para luego ser transmitida a la controladora donde se encuentre el cliente. La palabra simétrico aquí hace referencia a que el camino en el que los datos se envían y reciben es el mismo. El siguiente gráfico ejemplifica este proceso (Carroll, 218):

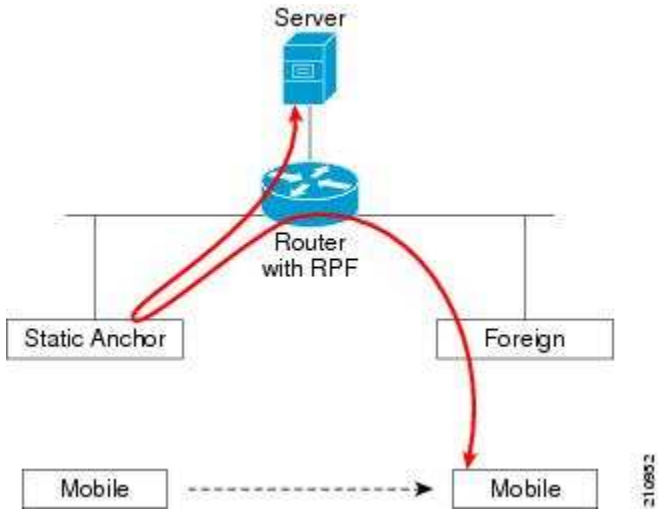


Figura 48: Túnel simétrico.

Fuente: http://www.cisco.com/en/US/i/200001-300000/210001-220000/210001-211000/210952.jpg

CAPITULO III

3 Estudio de las bases de la Red inalámbrica y configuración

Una vez concluida la revisión del marco teórico requerido, conceptos, principios, mecanismos, etc., procederemos a la revisión del requerimiento específico de red inalámbrica que se presentó conceptualmente para proveer al Nuevo Aeropuerto Internacional de Quito de servicios de infraestructura de red inalámbrica y acceso de sus usuarios a Internet. En el estudio de estas bases conceptuales, haremos primeramente una diferenciación entre los aspectos físicos y lógicos de la red inalámbrica.

En el caso de requerimientos físicos nos referimos principalmente al equipamiento, dispositivos, hardware, “appliances”, etc.; es decir, todo lo que sea tangible a la implementación de nuestra red. Por requerimientos lógicos nos referimos a software, licencias, configuraciones, comportamientos de red, etc.; es decir, todo lo intangible que es parte de la red como un conjunto que interactúa con el usuario final.

3.1 Requerimientos físicos de la Red

Dentro de las bases conceptuales, presentaremos todo los puntos que son parte de nuestro estudio para el diseño de la red física, en primera instancia. Luego de analizar el requerimiento en dispositivos a detalle, procederemos a llenar este con un equipamiento específico principalmente justificando cómo los dispositivos cumplen con las bases según mejores prácticas de industria, desempeño en ambientes de

producción y demostrando que se hace uso de las tecnologías más actualizadas. Para el efecto cabe recalcar que todos los dispositivos que harán parte de este estudio y diseño conceptual pertenecen a la marca CISCO, la misma que se encuentra entre las marcas más importantes de equipos de redes de datos, hablando en sentido universal, en la actualidad, y la única que cumple a cabalidad con las bases que están expuestas en este documento.

3.1.1 Equipamiento requerido

Las bases exponen en sus siguientes secciones, los equipos físicos que se requieren en su infraestructura Wireless:

- Equipamiento “Gateway”, el mismo que se utiliza como punto de comunicación entre la red Wireless de área local (WLAN) y la conexión hacia el Internet. Para este caso, este equipamiento incluye los Switches de comunicación para brindar conexión entre los puntos de acceso (APs), y el Datacenter donde se centraliza la administración de estos mediante una Controladora LAN Wireless (WLC). Estos enlaces son conocidos como “Uplinks”, que principalmente cumple la función de comunicar cada punto de acceso con los Switches y finalmente hacia la Controladora inalámbrica.
- 18 Puntos de acceso, que deben soportar un alta capacidad de compatibilidad con todos los protocolos 802.11 estándar revisados en este documentos en secciones anteriores a/n y b/g/n, con funcionamiento en las dos bandas

principales de las redes inalámbricas actuales: 2,4 y 5 GHz y finalmente con una cobertura de un radio de aproximadamente 50 metros con un Sobrelapamiento del 15 al 20% que está contemplado conceptualmente en las bases.

- Equipamiento para “Acceso Seguro y Autorización”. El requerimiento, aunque no se muestra como necesidad de un dispositivo sino de un servicio, se cumple con un servidor RADIUS que estará embebido o incluido en la controladora LAN Wireless conceptualmente. Sin embargo aclaramos que para una implementación en un ambiente de producción con un requerimiento de usuarios de tal densidad es recomendable el uso de servidores dedicados como un Servidor de Acceso a la Red (NAS) o un servidor Cisco ASA.

3.1.1.1 Controladora Inalámbrica (WLC)

Para el dimensionamiento de la Controladora LAN Wireless, se tomó en cuenta varios aspectos con respecto a las bases para verificar su cumplimiento. Entre los principales destacan los siguientes:

- 18 Puntos de acceso.
- Puntos de acceso de gama alta con compatibilidad universal.
- Tecnología que mitigue problemas de radio-frecuencia (Cisco CleanAir).
- Alta densidad de usuarios.
- Capacidad de enlaces de “Uplink” con el Switch de comunicaciones.

Dentro de lo que ofrece CISCO con estos requerimientos, se provee la siguiente controladora inalámbrica (WLC) y con las siguientes opciones de licenciamiento y garantía para satisfacer esta primera necesidad de equipamiento físico:

AIR-CT5508-25-K9	Cisco 5508 Series Wireless Controller for up to 25 APs
CON-SNTP-CT0825	SMARTNET 24X7X4 Cisco 5508 Series
SWC5500K9-60	Cisco Unified Wireless Controller SW Release 7.4
AIR-PWR-CORD-NA	AIR Line Cord North America
LIC-CT5508-25	25 AP Base license
LIC-CT5508-BASE	Base Software License

Tabla 3: Controladora dimensionada.

La siguiente tabla presenta un set de configuraciones de ambiente real que CISCO ofrece a sus socios o “Partners” para realizar dimensionamientos en detalle a clientes potenciales.

En este caso específico, la primera línea se hace referencia al “Número de Parte” que es interno de CISCO para que sus clientes puedan diferenciar con exactitud de que producto se trata, que gama y que licenciamiento posee. En este caso la controladora WLC modelo 5508 Series con licenciamiento para operar un máximo de 25 Puntos de acceso.

La segunda línea pertenece a servicios. En este caso el servicio “SMARTNET” 24x7x4 hace referencia a la garantía del producto que se ofrece por un año en la modalidad de 24 horas al día, 7 días a la semana con un tiempo de respuesta de 4 horas.

La tercera línea de la tabla hace referencia al software que trae instalado el dispositivo WLC. En este caso se trata de la versión o “Release” 7.4 del sistema operativo Cisco Wireless Controladora Unificada que es la más actualizada.

La cuarta y quinta línea hacen referencia al licenciamiento que viene incluido por compra en este controladora LAN Wireless. El número de licencias que ofrece CISCO en sus dispositivos escala por los general entre 5, 25, 50, 100, 250 o 500 Puntos de acceso por controladoras. No se ajusta a la necesidad específica sino que viene en valores predefinidos. Recordando el requerimiento que tenemos en nuestras bases conceptuales, tenemos que cubrir el licenciamiento de 18 Puntos de acceso. Nos vemos en la necesidad de adquirir el licenciamiento para 25 Puntos de acceso, lo que cubre nuestro requerimiento y adicionalmente nos da una capacidad extra de crecimiento de hasta 7 APs adicionales en un futuro. La quinta línea hace referencia a que estas 25 licencias son BASE, dentro de la gama de otras licencias que ofrece Cisco como IP Services, Adv. IP Services, etc.

3.1.1.2 Puntos de acceso (APs)

Según las bases, necesitamos 18 Puntos de acceso que cumplan con los siguientes requerimientos:

- Operar en las bandas más frecuentes en las Redes Inalámbricas funcionan: 2,4 y 5 GHz.
- Ser compatible con todos los protocolos 802.11 existentes en el mercado.

- Soporte de redes de área local virtuales (VLANs) y redes virtuales personales (VPNs) a través de Internet.

- Inyectores de energía para cada Punto de Acceso y la capacidad de energía sobre el cable Ethernet (PoE) es opcional, ya que por las distancias tan grandes del Nuevo Aeropuerto, los enlaces de “Uplink”, es decir, conexión de Puntos de acceso a Switches de comunicación, deben ser de fibra óptica y no de cobre, limitando y anulando en su mayoría la opción de uso de la tecnología PoE.
- Kit de montaje en cielo falso para instalación física.

Para cubrir este requerimiento, elegimos la gama de Punto de Acceso 3600 que es la única que cumple con compatibilidad en todas las tecnologías 802.11 en CISCO operando a 2,4 y 5 GHz. La especificación del producto, en detalle está expuesta en la siguiente tabla:

AIR-CAP3602E-A-K9	802.11n CAP w/CleanAir; 4x4:3SS; Mod; Ext Ant; A Reg Domain
CON-SNTP-C362EA	SMARTNET 24X7X4 802.11n CAP w/CleanAir; 4x4:3SS; Mod; Ex
AIR-AP-BRACKET-1	802.11n AP Low Profile Mounting Bracket (Default)
AIR-AP-T-RAIL-R	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)
S3G2RK9W8-12423JY	Cisco 3600 Series IOS WIRELESS LAN RECOVERY
AIR-ANT2524DW-R	2.4 GHz 2 dBi/5 GHz 4 dBi Dipole Ant. White RP-TNC

Tabla 4: Puntos de Acceso dimensionados.

La primera línea hace referencia al modelo del equipo como un punto de acceso serie 3602 con capacidad de mitigar problema de radio frecuencia mediante la tecnología CISCO propietaria CleanAir, con la capacidad de funcionar con 4 antenas y centralizar su administración hacia la controladora WLC detallada en la sección anterior.

La segunda línea describe la garantía de este producto, que se extiende durante 1 año según lo requerido por estándar en modalidad 24x7x4.

La tercera y cuarta línea hacen referencia al kit de montaje para que el Punto de Acceso pueda ser instalado en el cielo falso siendo así más transparente para usuario final.

La quinta línea hace una descripción del sistema operativo que se viene incluido en este dispositivo, al ser “Wireless LAN Recovery”, implica la necesidad de funcionamiento conjunto con la controladora LAN Wireless.

La última línea de la tabla hace referencia a las antenas que configuramos como parte de la configuración física de este equipo. Para este caso son dos antenas que funcionan a 2.4 GHz y dos que funcionan a 5 GHz y en ambos casos se tratan de antenas dipolo.

3.1.1.3 Switches de comunicación

La finalidad de incluir la parte LAN a nuestra red inalámbrica del Nuevo Aeropuerto es la de brindar la comunicación necesaria entre los Puntos de acceso hacia la controladora WLC y su servidor de autenticación RADIUS embebido. Los requerimientos son los siguientes:

- Capacidad de alta transferencia de datos para los usuarios.
- Ofrecer conexión con la conexión de Internet provista por cable.
- Soportan redes de área local virtuales (VLANs).
- Proveer de conexiones Uplink.

Para cubrir la necesidad expuesta en las bases conceptuales, se tiene provisto como dispositivo de switches CISCO el modelo 3750-X. Dicho switch es uno de los más implementados de la marca y cumple a cabalidad con todos los puntos del requerimiento. Se ha provisto dos switches para redundancia. La siguiente tabla muestra las opciones físicas del equipo:

WS-C3750X-12S-S	12 Gigabit Ethernet SFP IP Base
CON-SNTP-C375012X	SMARTNET 24X7X4 C3750X 12 Gigabit Ethernet
CAB-AC-RA	Power Cord110V Right Angle
PWR-CLIP	Power retainer clip for compact switches

Tabla 5: Switches LAN dimensionados.

El Número de parte de la primera línea hace referencia a nuestro Switch 3750-X con 12 puertos Gigabit Ethernet (GE). La línea también describe el licenciamiento “IP

Base” que está provisto para este caso como un set de comandos y propiedades de su sistema operativo.

La segunda línea describe la garantía que a semejanza de los equipos anteriores es extendida por un año por requerimiento de bases en modalidad 24x7x4.

La tercera línea hace referencia al cable de alimentación de energía que es de 110V para el caso de este switch y la última línea describe un clip que retiene al switch.

3.1.1.4 Enlaces de Uplink

Como parte de los requerimientos en las bases está el proveer de comunicación a los puntos de acceso con la controladora que los administra. Aunque los enlaces de Uplink no estén descritos en las bases de manera explícita, lo están de manera implícita. Los requerimientos de estos enlaces son los siguientes:

- Enlaces de conexión APs – WLC de más de 100 metros.
- Alta velocidad de los enlaces (Gigabit Ethernet).
- Capacidad de conexión con el Switch 3750-X y los puntos de acceso CISCO 3602.

Para estos enlaces, se tiene provisto el dimensionamiento de fibra óptica. Sin embargo la discusión sobre la fibra no está cubierta en el alcance de este documento sino que nuestro interés es mostrar cómo los dispositivos interactúan con la fibra óptica. Para este caso, los puntos de accesos vienen con la capacidad por defecto

de conexión con fibra. Sin embargo los Switches no vienen con esta capacidad por defecto. Para que los switches puedan interactuar con la fibra óptica se debe proveer de una interfaz especial (SFP). Esta interfaz está provista para cada switch en este dimensionamiento de la manera que se describe en esta tabla:

GLC-SX-MM	1000BASE-T SFP

Tabla 6: Interfaz de fibra dimensionada.

Esta línea hace referencia al número de parte y característica Gigabit Ethernet que son los compatibles con las ranuras Gigabit Ethernet que poseen los mismos switches. Tales características en los enlaces de Uplink dan alta velocidad, compatibilidad con los switches - puntos de acceso y la capacidad de conectarse a mayor distancia que por cable de cobre (100 metros).

3.1.1.5 Radius Server

En los requerimientos de las bases en general, no se describe la necesidad específica de un dispositivo o “appliance” dedicado para brindar servicios de Autenticación, Autorización y Auditoría (AAA), aunque se debería en una red de estas características. Sin embargo, en las bases existe efectivamente la necesidad de brindar un esquema de seguridad al usuario final como un servicio y no como un dispositivo dedicado. Para este caso dimensionamos un servidor Radius cuyo funcionamiento fue expuesto en secciones anteriores, pero local a la controladora

dimensionada. Este servidor Radius local logra cumplir con los siguientes requerimientos según las bases conceptuales:

- Estrategias que sirvan para proteger al usuario.
- Un sistema que provee acceso segmentado, autenticación y auditoría.
- Acceso a redes privadas a través de contraseñas.

3.1.1.6 Topología final física

Como resultado de todos los requerimientos físicos en las bases conceptuales para la red inalámbrica del Nuevo Aeropuerto Internacional de Quito tenemos como resultado lo expuesto en el siguiente gráfico:

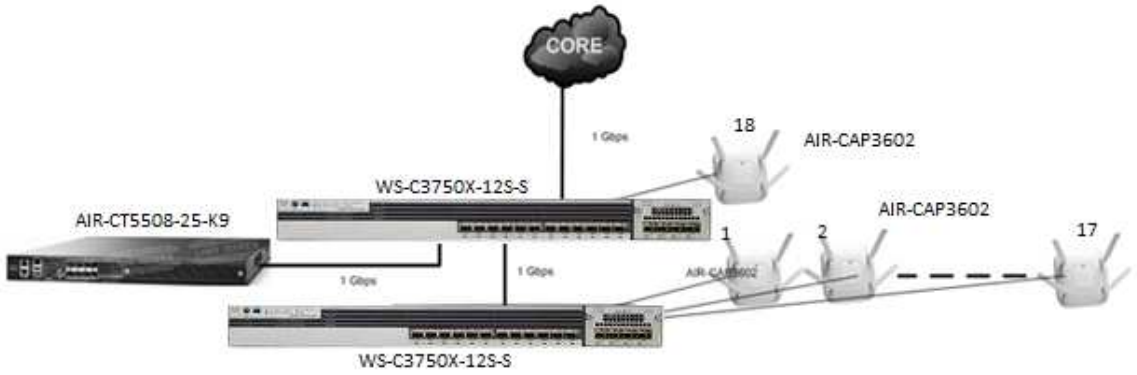


Figura 49: Topología física Wireless.

El presente diagrama representa la porción física de la red. Tenemos como parte LAN 2 switches 3750-X de fibra óptica de 12 ranuras para módulos Gigabit Ethernet,

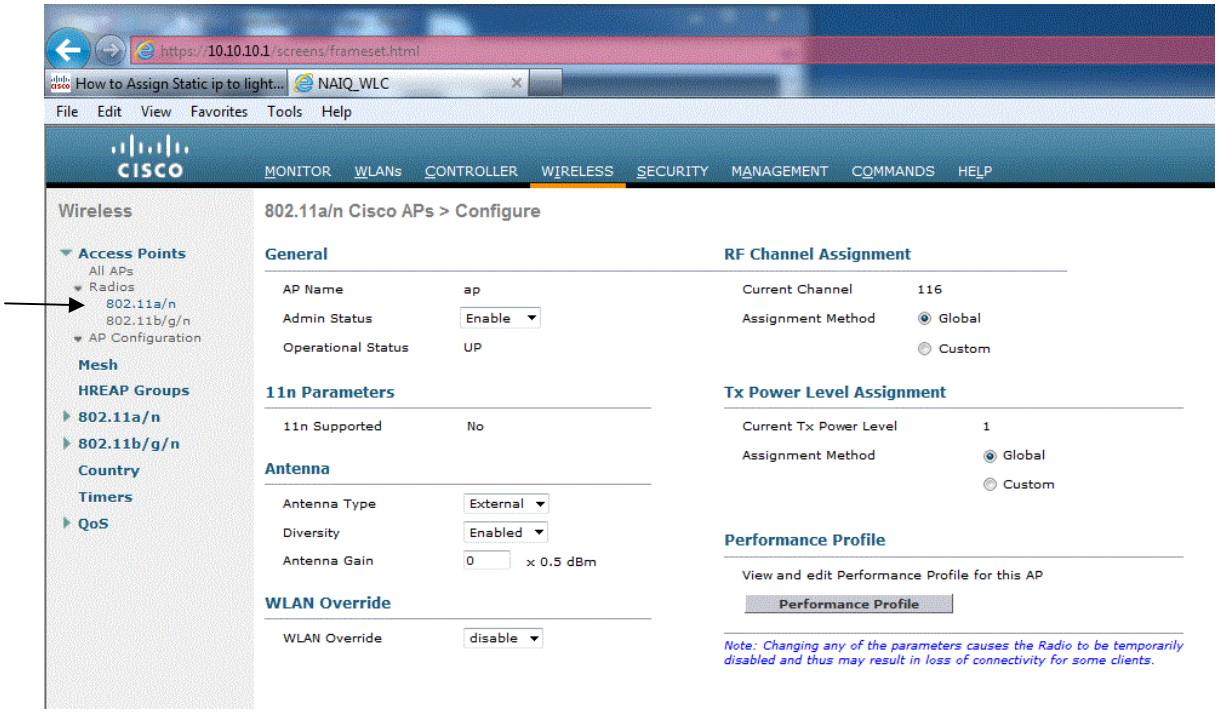
que proveen interconexión a los 18 puntos de acceso Cisco 3602 que están distribuidos 17 en el 2do piso del aeropuerto y el restante en el 3er piso (Sala VIP) hacia una única controladora WLC 5508 para administración de un máximo de 25 puntos de acceso. A través de sus puertos Gigabit Ethernet se provee de una conexión hacia el Núcleo de la Red (Core) donde finalmente nuestra red se conecta contra el Internet en un “backbone” de alta velocidad, porción de la red desconocida en las bases. Tenemos un número de 22 interfaces de fibra para los switches distribuidas de manera que se brinde el Uplink para 18 puntos de acceso y los 4 restantes para conexiones WLC y Core.

3.2 Requerimientos lógicos de la Red

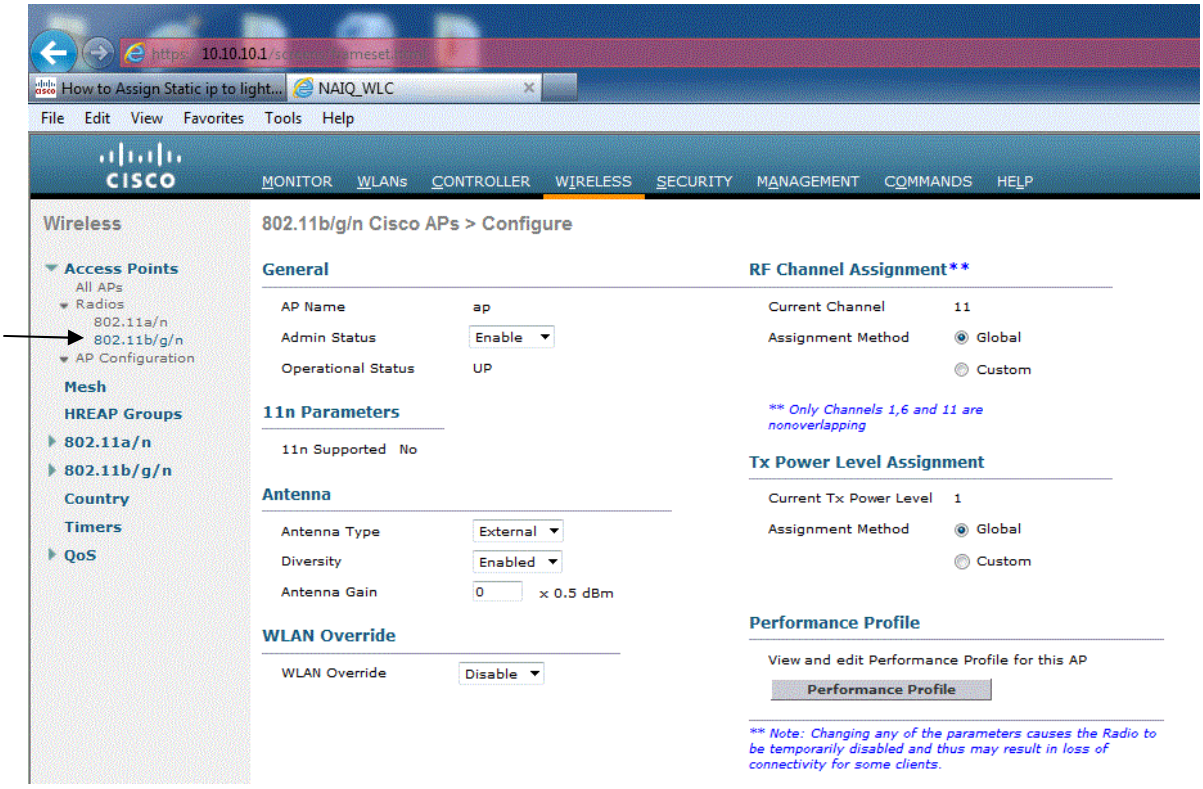
Una vez revisado todo el equipamiento físico de nuestra red, analizaremos todos los requerimientos lógicos, es decir de configuración. Para que nuestro diseño en base a lo requerido funcione de la manera más adecuada, hemos desarrollado un laboratorio con equipamiento que se asemejaría casi perfectamente a cómo funcionaría esta red en un ambiente de producción: WLC 4402 y 2 APs 1400. Las configuraciones se desarrollaron en la controladora WLC donde se definió el uso de bandas 2.4 y 5 GHz, distintas frecuencias, múltiples redes inalámbricas (SSIDs) con servicio DHCP independientes para cada una, la configuración de un servidor RADIUS embebido que brindará servicio sólo a los usuarios de la red administradores y estrategias para mitigar posibles problemas de Radio Frecuencia.

3.2.1 Configuración de Banda

Configuramos las diferentes bandas 2.4 y 5 GHz en la controladora LAN Wireless, en la sección Wireless > Access Points > Radios > 802.11a/n en el caso de 5 GHz. La siguiente captura demuestra los parámetros configurados:



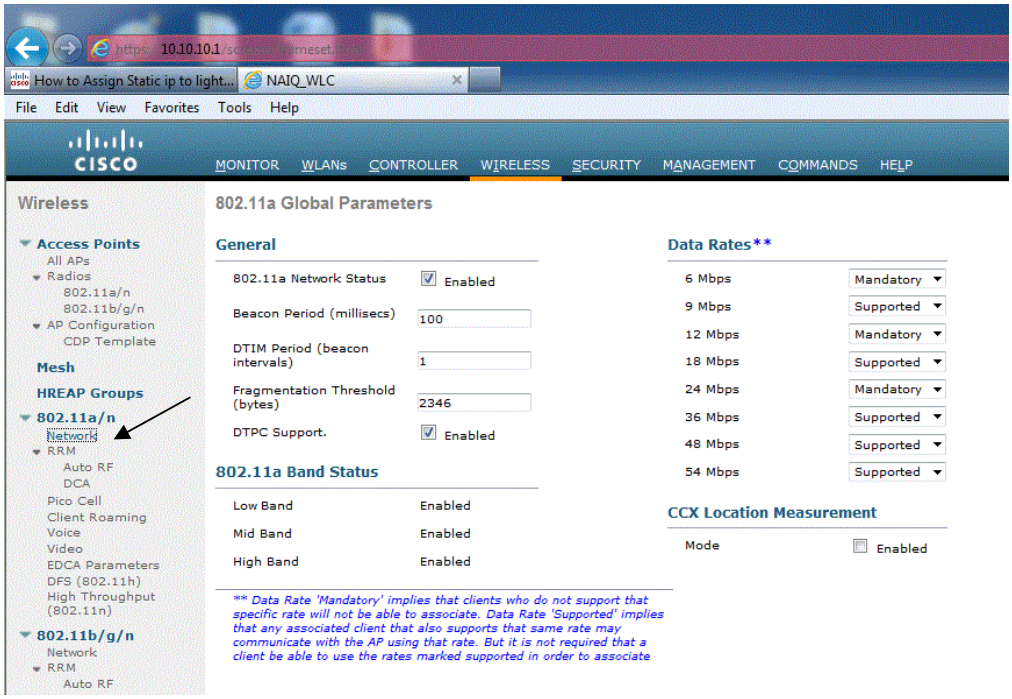
Para la configuración de la banda de 2.4 GHz, debemos dirigirnos a la sección Wireless > Access Points > Radios > 802.11b/g/n. La siguiente captura muestra los parámetros de configuración:



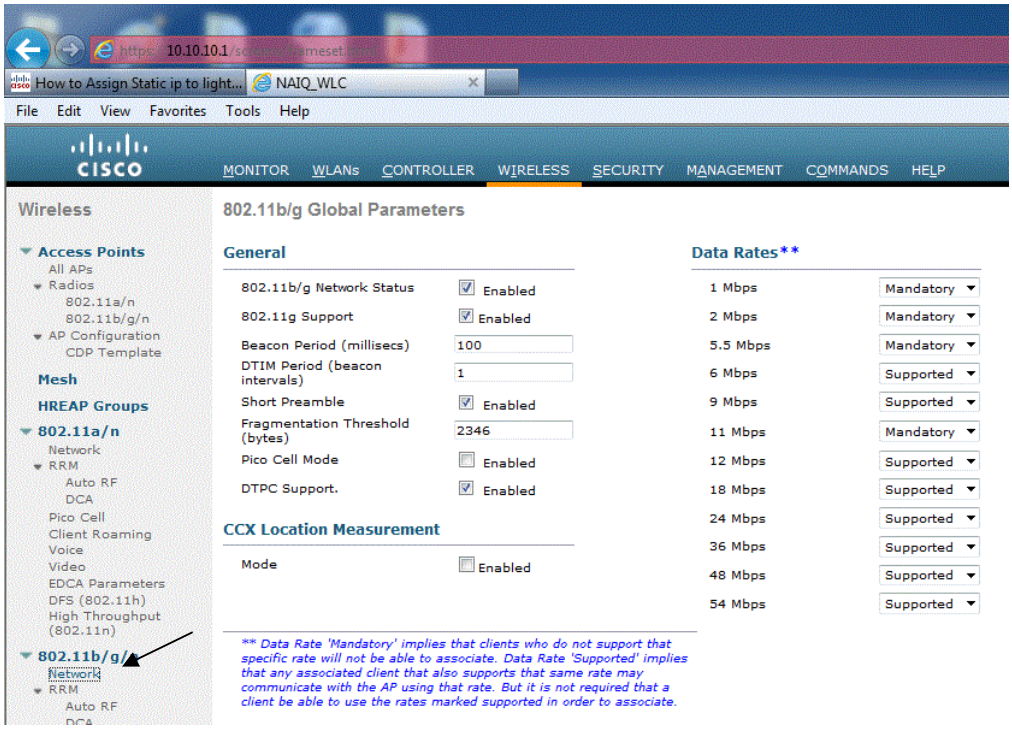
En síntesis, hemos configurado el Punto de Acceso denominado en la controladora como “ap”, operando en las dos bandas 2.4 y 5 GHz. La configuración de antenas es externa en ambos casos y el resto de valores se han mantenido en valores de defecto predefinidos.

3.2.2 Configuración de Frecuencia

Posterior a la configuración de las bandas y de los Puntos de acceso que operan en estas, configuramos las frecuencias para ajustar las velocidades de transmisión en cada banda y habilitar el estatus del protocolo. Para el caso de 802.11a/n nos dirigimos a la opción Wireless > 802.11a/n > Network como se muestra aquí:



Para configurar las opciones dentro de los protocolos 802.11 b/g/n entramos a la pestaña Wireless > 802.11b/g/n > Network:



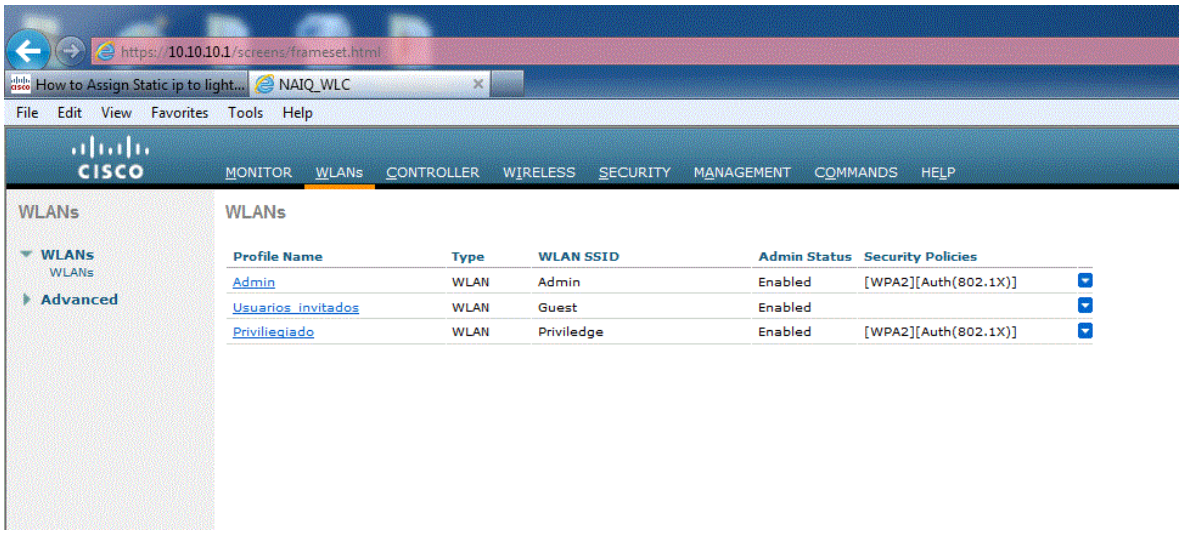
Se configuró el estatus de las redes a y b/g como habilitado poniendo un visto en el checkbox “enable” en cada caso. Las velocidades se ajustaron por defecto recordando de secciones anteriores que el protocolo 802.11a funciona mandatoriamente a 6, 12 y 24 Mbps mientras que b/g a 1, 2, 5.5 y 11 Mbps.

3.2.3 Configuración de SSIDs múltiples

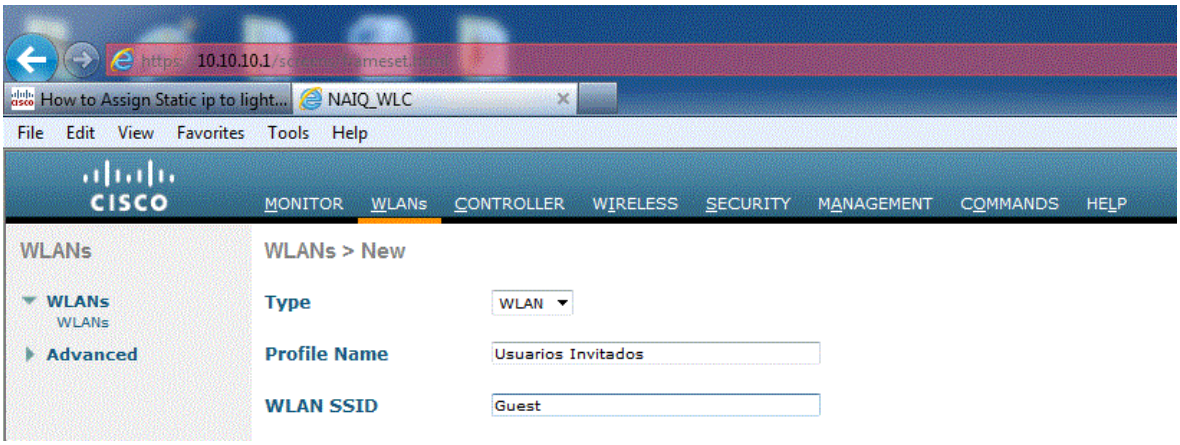
Para el desarrollo en un ambiente de laboratorio que se asemeje a un ambiente de producción común hemos decidido crear tres redes inalámbricas (SSIDs) encontradas con frecuencia:

- Administradores
- Usuarios Invitados
- Usuarios Privilegiados

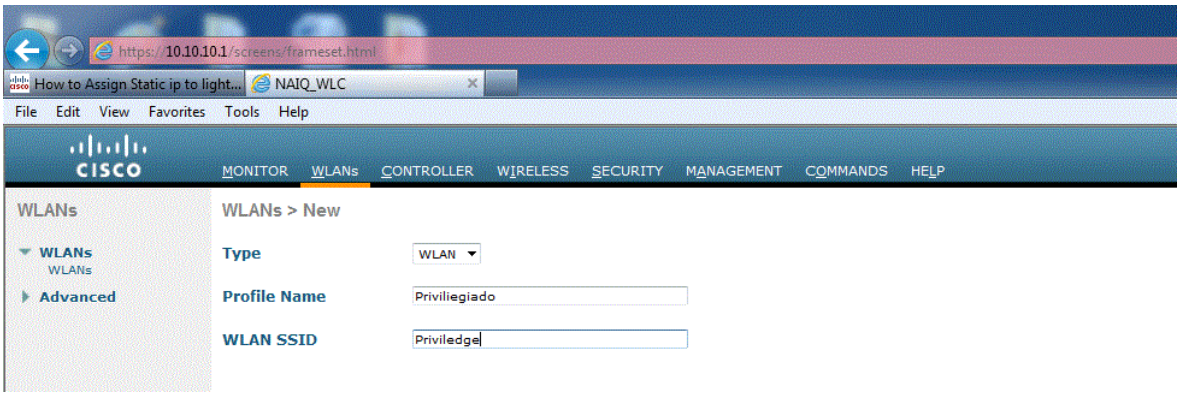
La siguiente captura demuestra la configuración de estas distintas redes en nuestra controladora (WLC):



Para la realizar la configuración de cada una de las redes, procederemos a la pestaña WLANs > New. Para demostrar la configuración del perfil de “Usuarios invitados” tenemos la siguiente captura:



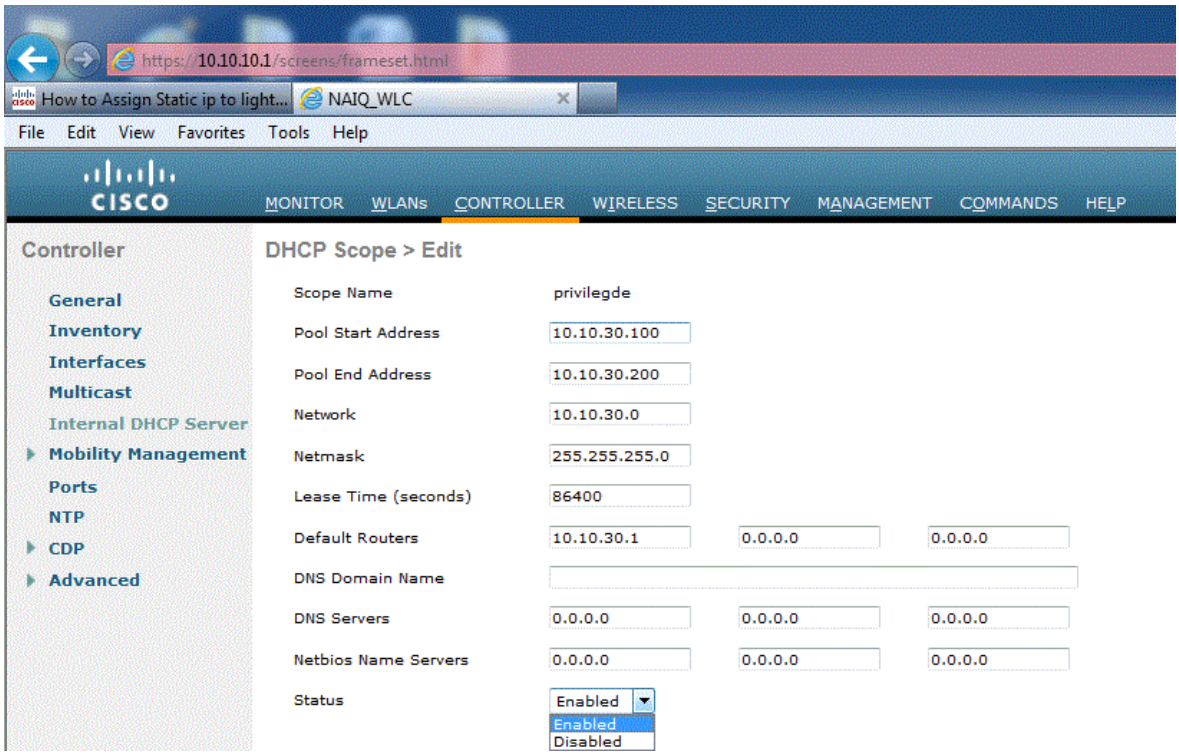
Definimos el nombre del perfil como Usuarios invitados y en la caja de “WLAN SSID” definimos el nombre de red que se mostrará a los usuarios finales al momento de asociarse con la esta red en particular. La siguiente captura muestra la configuración de estos mismos valores para la red de privilegiados:



El definir el nombre de la red (SSID) es apenas uno de los pasos para que estos distintos perfiles funcionen y los usuarios puedan acceder a los diferentes recursos o servicios que cada uno de ellos puedan brindar. Los siguientes pasos serán crear un “pool” de direcciones IP para DHCP, la creación de una “interfaz” y el método de seguridad para ingresar a cada perfil.

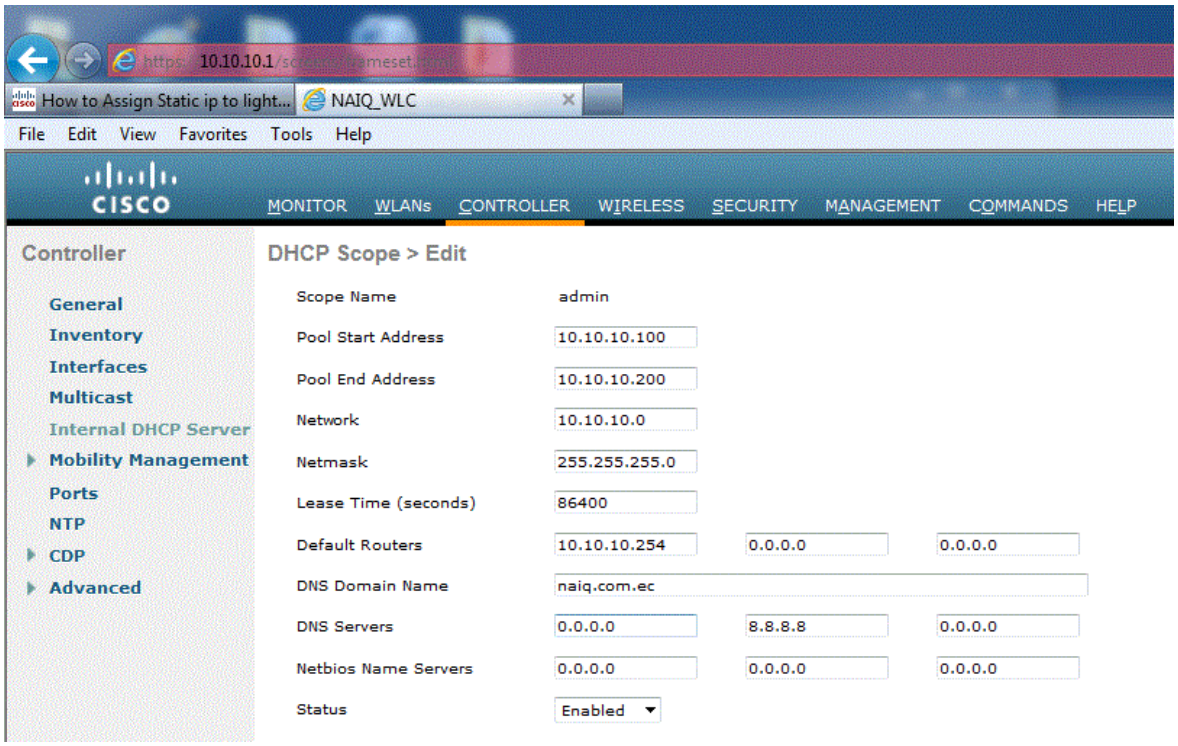
3.2.4 Configuración DHCP local

En la creación de múltiples redes inalámbricas “virtuales” dentro de la misma infraestructura, el siguiente paso será definir un pool de direcciones IP para DHCP con el fin de que los usuarios puedan obtener una dirección que los asocie con su respectiva red. Hemos configurado un pool distinto por cada perfil como muestran las siguientes capturas:



Para la configuración del pool debemos dirigirnos a la pestaña Controller > Internal DHCP Server > New. La captura anterior pertenece al pool asignado a la red de usuarios privilegiados. La red es la 10.10.30.0/24. Sus usuarios asignados podrán obtener una dirección entre la 10.10.30.100 y la 10.10.30.200 con una ruta por defecto en la dirección 10.10.30.1 y el resto de direcciones están reservadas. Finalmente para que este conjunto de direcciones funcione, elegimos la opción “Enabled” en la lista final.

La siguiente captura muestra la configuración del conjunto de direcciones destinado a la red de administradores:

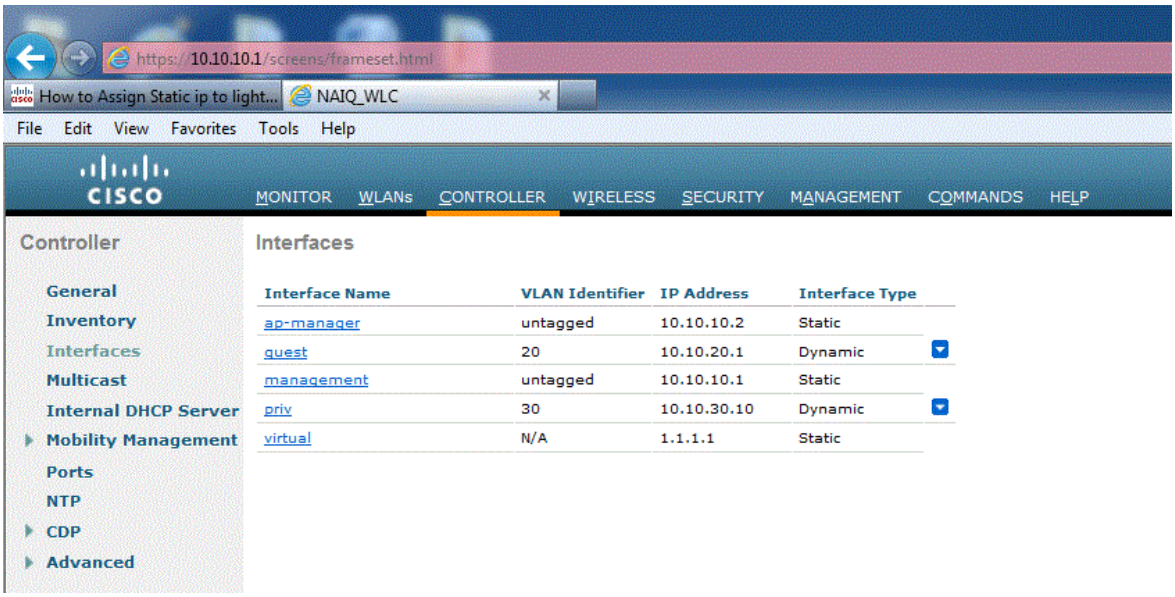


La red destinada a este perfil de administradores es la 10.10.10.0/24. El estatus está habilitado y definimos un nombre para el dominio en naiq.com.ec.

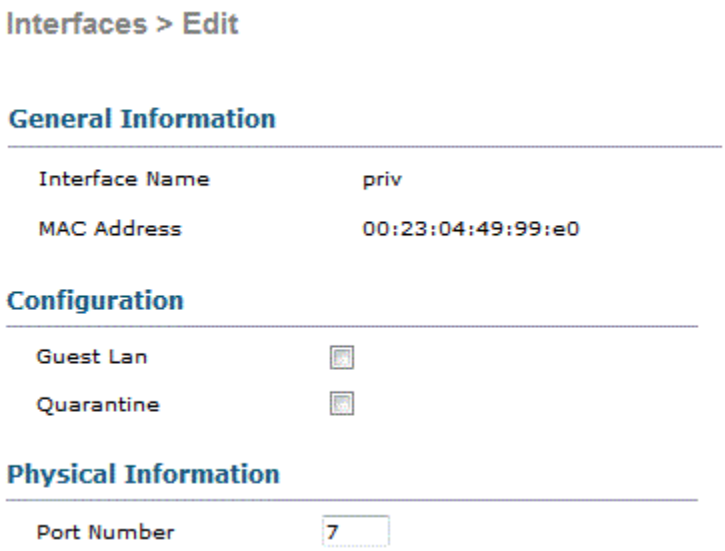
3.2.5 Interfaces WLAN

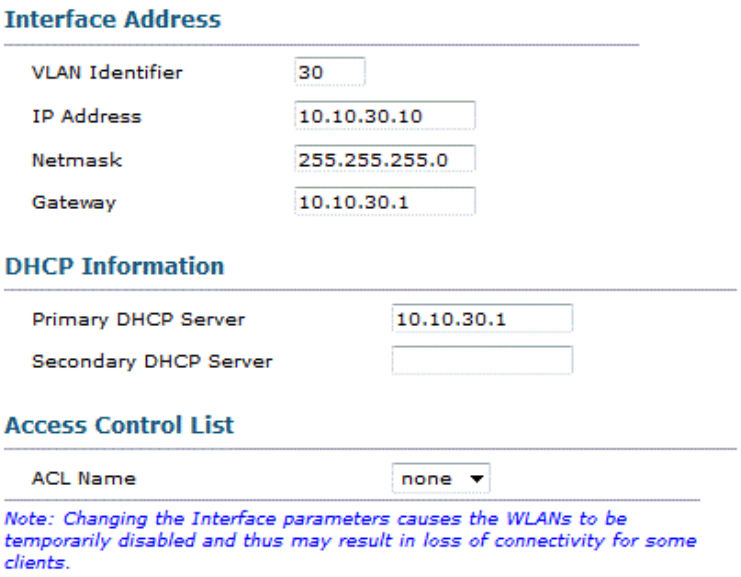
Posterior a la creación del SSID y el pool de direcciones IP designadas por DHCP, el siguiente paso mandatorio para que la configuración de múltiples redes inalámbricas funcionen en la controladora es la creación de “Interfaces”. De esta manera se pueden asociar los distintos nombres a sus direcciones IP dentro de la controladora.

Para configurar las interfaces debemos ir a la opción Controller > Interfaces. La siguiente figura muestra esta opción con nuestras tres redes creadas:



Al poner el puntero sobre la flecha azul que está al lado de las interfaces dinámicas, tenemos la opción de editar la interfaz. La siguiente figura muestra la edición en la interfaz de usuarios privilegiados (priv):

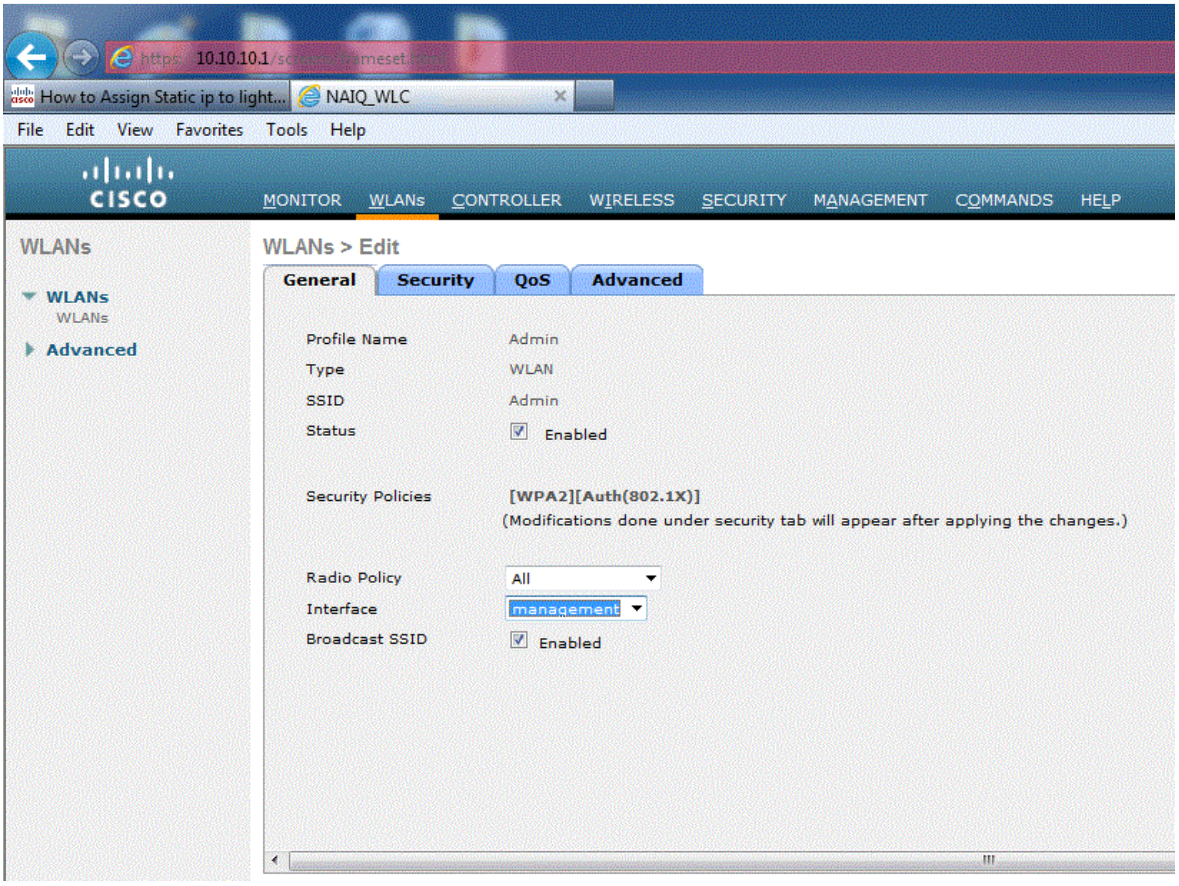




Como información general en esta sección tenemos el nombre de la VLAN “priv” y su dirección MAC (00:23:04:49:99:E0). El puerto físico de comunicación es el número 7 de la controladora Wireless. El identificador de VLAN es VLAN 30 y el Gateway que también está definido como servidor DHCP es la dirección 10.10.30.1. Para este perfil no se ha definido Lista de Control de Acceso (ACL) alguna (none).

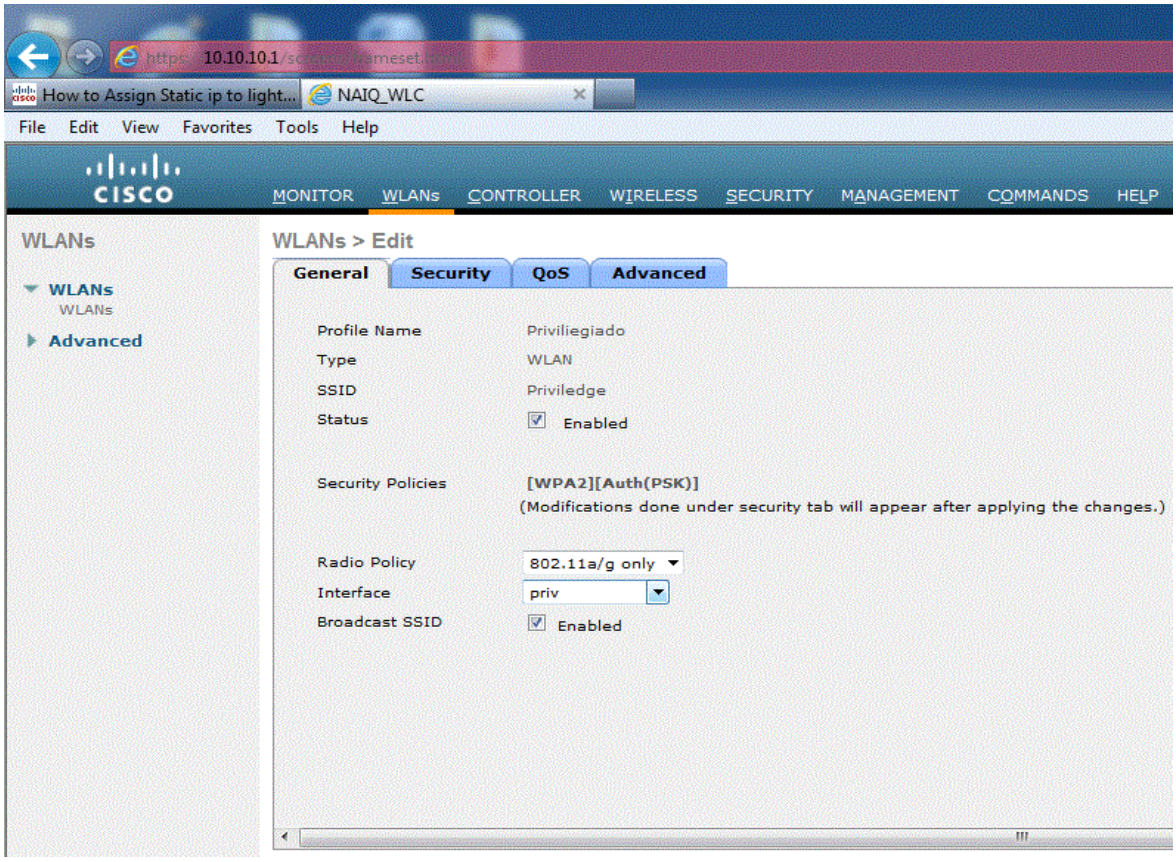
3.2.6 WLANs

Con los pasos previos definidos, la configuración de las redes inalámbricas de área local se completa de la siguiente manera. Nos dirigimos a la sección WLANs > Edit > General como muestra la siguiente captura:



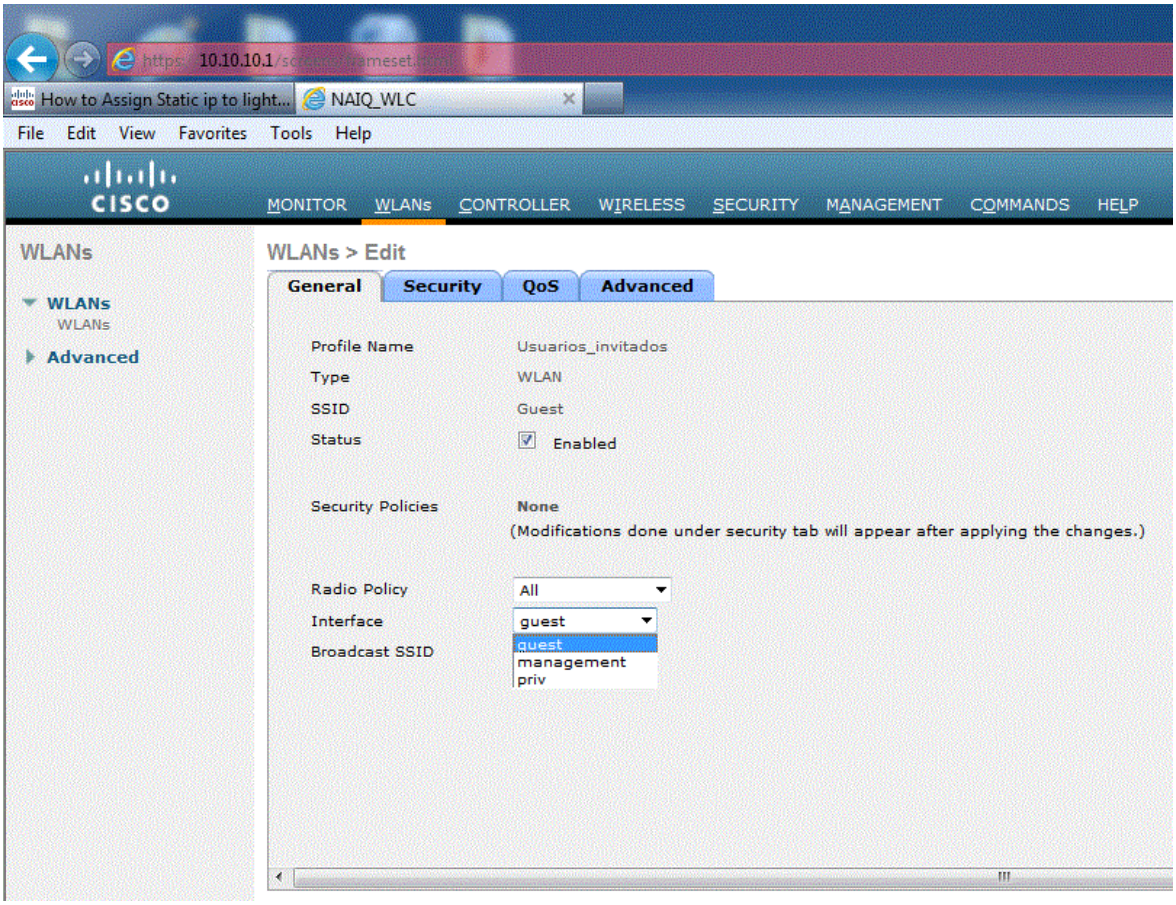
Esta captura muestra la configuración de la red inalámbrica de administradores. El estatus está habilitado, la política de radio opera en las dos bandas: 2.4 y 5 GHz, la interfaz Wireless que definimos previamente se asocia a esta WLAN “managemet” y la difusión de esta red en el medio compartido (Broadcast SSID) está habilitada.

Para el caso de la red inalámbrica de los usuarios privilegiados, definimos los siguientes parámetros en la misma sección:



El estatus de esta red está habilitado, las políticas de seguridad son de llave pre-compartida con WPA2 cuya configuración se discutirá en la siguiente sección, la política de radio está definida en 5 GHz con los protocolos 802.11a/g, la interfaz definida en un paso preliminar se asocia con esta WLAN “priv” y finalmente, la difusión de esta red está habilitada.

La siguiente captura muestra la misma configuración para la red de usuarios invitados en la misma pestaña de configuración con los siguientes parámetros: estatus de red habitada, seguridad abierta, todos los radios de operación, interfaz “guest” y difusión de la red habilitada:



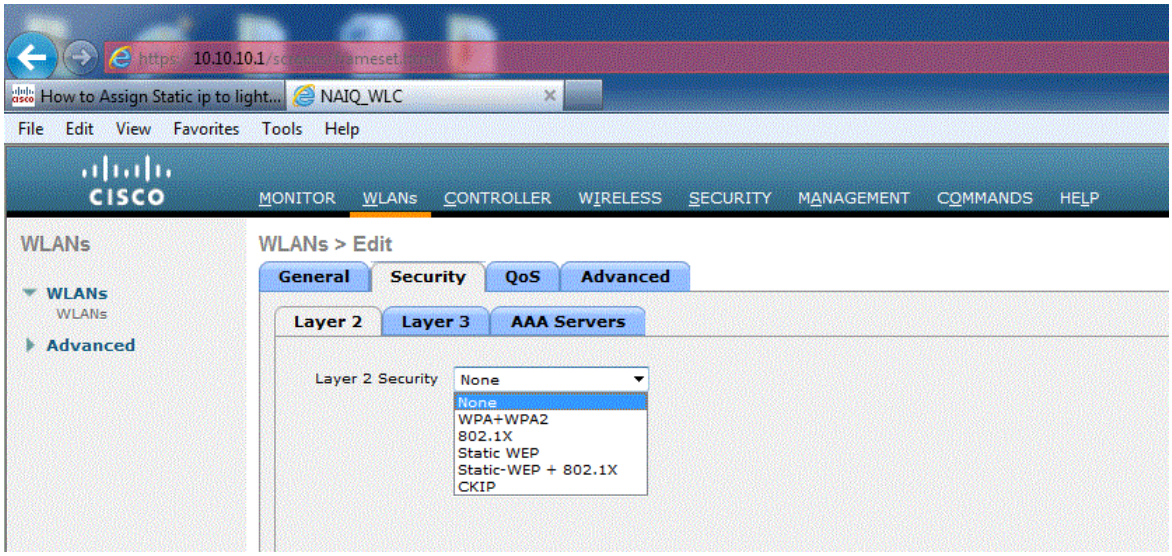
3.2.7 Métodos de seguridad

Con los pasos anteriores realizados, se cumple la configuración de las múltiples redes inalámbricas dentro de la controladora. El siguiente paso a seguir es opcional pero muy importante a su vez, la configuración de la seguridad. Hemos definido distintos métodos de seguridad según el nivel que cada red de nuestro laboratorio requiere:

- Red de invitados: Abierta.
- Red de usuarios privilegiados: WPA2-PSK.
- Administradores: servidor RADIUS local.

3.2.7.1 Abierta (Open)

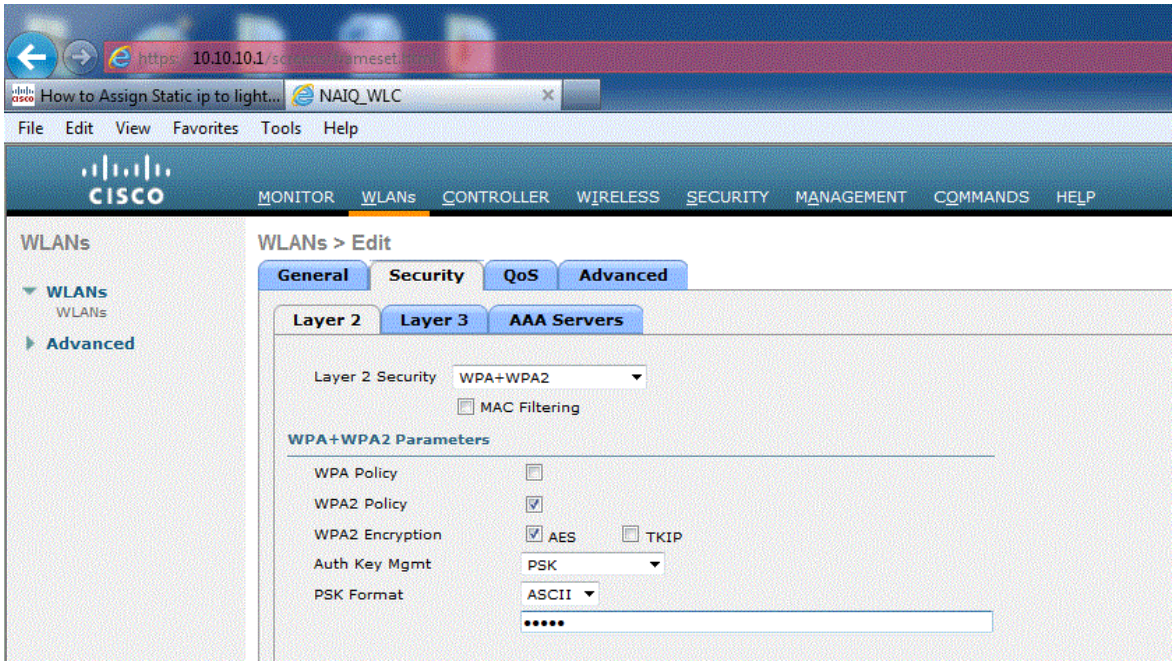
El motivo para elegir el método de autenticación abierta para la red de invitados yace en que es una red que brinda recursos muy limitados para usuarios que no tienen ninguna labor administrativa o que demande mayores privilegios dentro de la red del Nuevo Aeropuerto. Simplemente se limitan a una navegación web con velocidades bajas. La siguiente captura de pantalla muestra la configuración de este método de seguridad en el perfil de usuario invitado ingresando a WLANs > Edit > Security > Layer 2 > None:



Los usuarios de esta red de Invitados no necesitarán ni usuario ni contraseña para poder asociarse con esta red WLAN.

3.2.7.2 WPA2-PSK

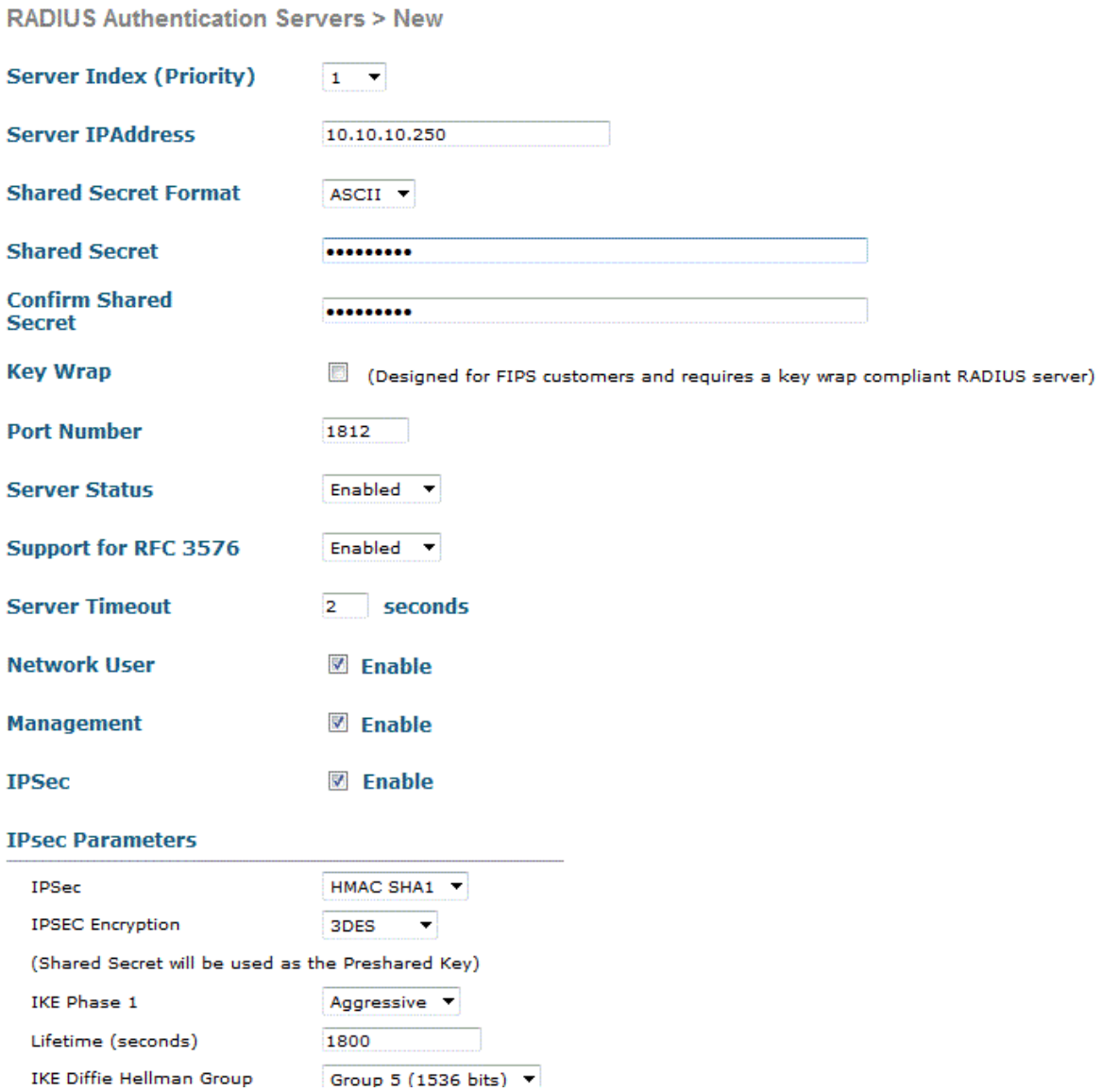
Para que los usuarios privilegiados se puedan asociar con la red inalámbrica que tiene provista sus respectivos recursos y servicios, el método de autenticación elegido es una llave pre-compartida (PSK) con Acceso Protegido Wireless (WPA) versión 2. Para configurar este método nos dirigimos a la sección WLANs > Edit > Security > Layer 2 > WPA + WPA2, como se muestra en la siguiente captura:



En la ficha de WPA + WPA2 encontramos parámetros adicionales para configurar nuestra llave pre-compartida. Elegimos AES como método de encriptación de datos, en la lista de “Auth Key Mgmt” definimos el método de PSK y en la última caja de texto escribimos la llave que en este caso es cisco. Los usuarios que deseen conectarse a esta red encontrarán la red Privilegiada con difusión (Brocadas SSID) habilitada y cuando procedan a conectarse tendrán que ingresar la contraseña cisco.

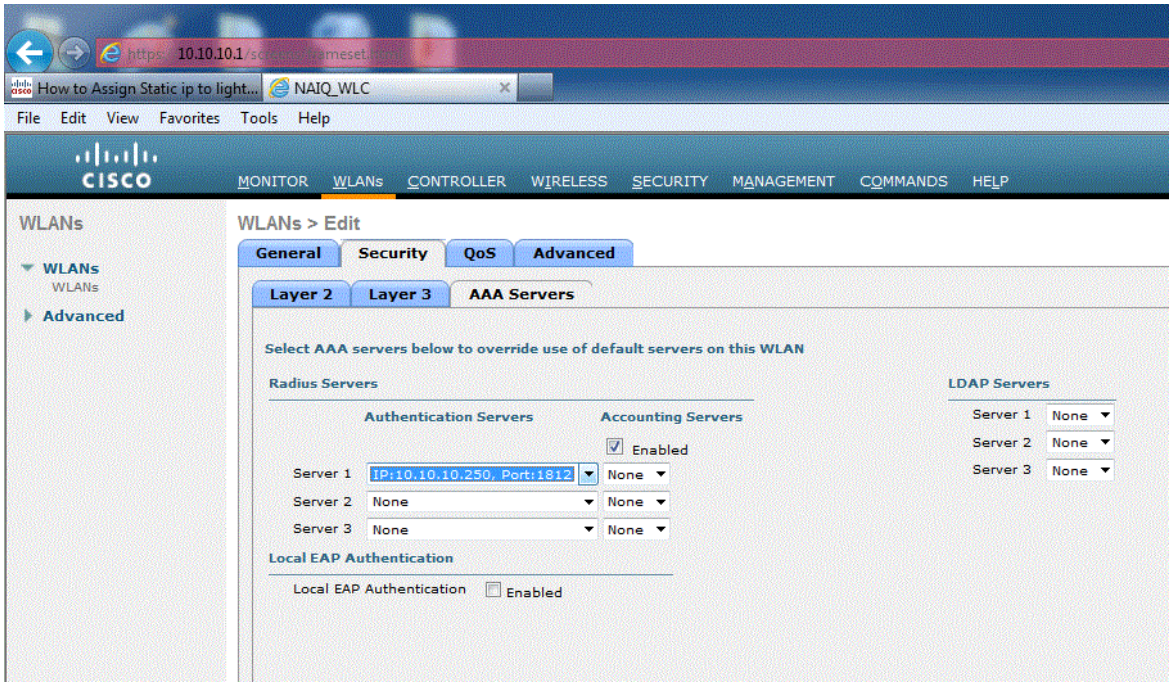
3.2.7.3 RADIUS Local

Por la importancia en la seguridad de los usuarios administradores, el método utilizado para brindar autenticación, por los servicios críticos que utilizan, es la autenticación en un servidor RADIUS local en la controladora LAN Wireless. La primera captura de pantalla muestra como se configura el servidor dentro de las opciones de la controladora. Nos dirigimos a la sección: Security > AAA > RADIUS > Authentication > New:



Definimos en esta pestaña la dirección IP a 10.10.10.250, dirección dentro del rango de administradores, la contraseña compartida que este caso es “naiqcisco”, el puerto por defecto para la comunicación RADIUS 1812, el estatus del servidor como habilitado y los parámetros IPSec en valores por defecto.

Una vez configurado nuestro servidor interno, podemos asociarlo a nuestra red inalámbrica. Nos dirigimos a la sección: WLANs > Edit > Security > AAA Servers.



Dentro de esta sección definimos la dirección IP y puerto de nuestro servidor 10.10.10.250:1812 como habilitada para que este método sirva a los usuarios que deseen asociarse con el perfil de administradores.

CAPITULO IV

4 Prueba del Diseño conceptual para Red inalámbrica

Posteriormente a la puesta en marcha de nuestro diseño de red inalámbrica, ejecutamos pruebas para conocer el funcionamiento de la misma. Las pruebas comprenden verificación de conectividad desde los puntos de acceso, pasando por la red cableada hasta la controladora LAN Wireless, pruebas de conectividad y velocidad hacia el Internet, compatibilidad de equipos móviles con los diferentes protocolos a/n y b/g/n, verificación de los métodos de seguridad provistos a cada red, prueba del direccionamiento IP en cada caso y finalmente las pruebas de redundancia en los dispositivos LAN, Switches de capa 2 del modelo OSI.

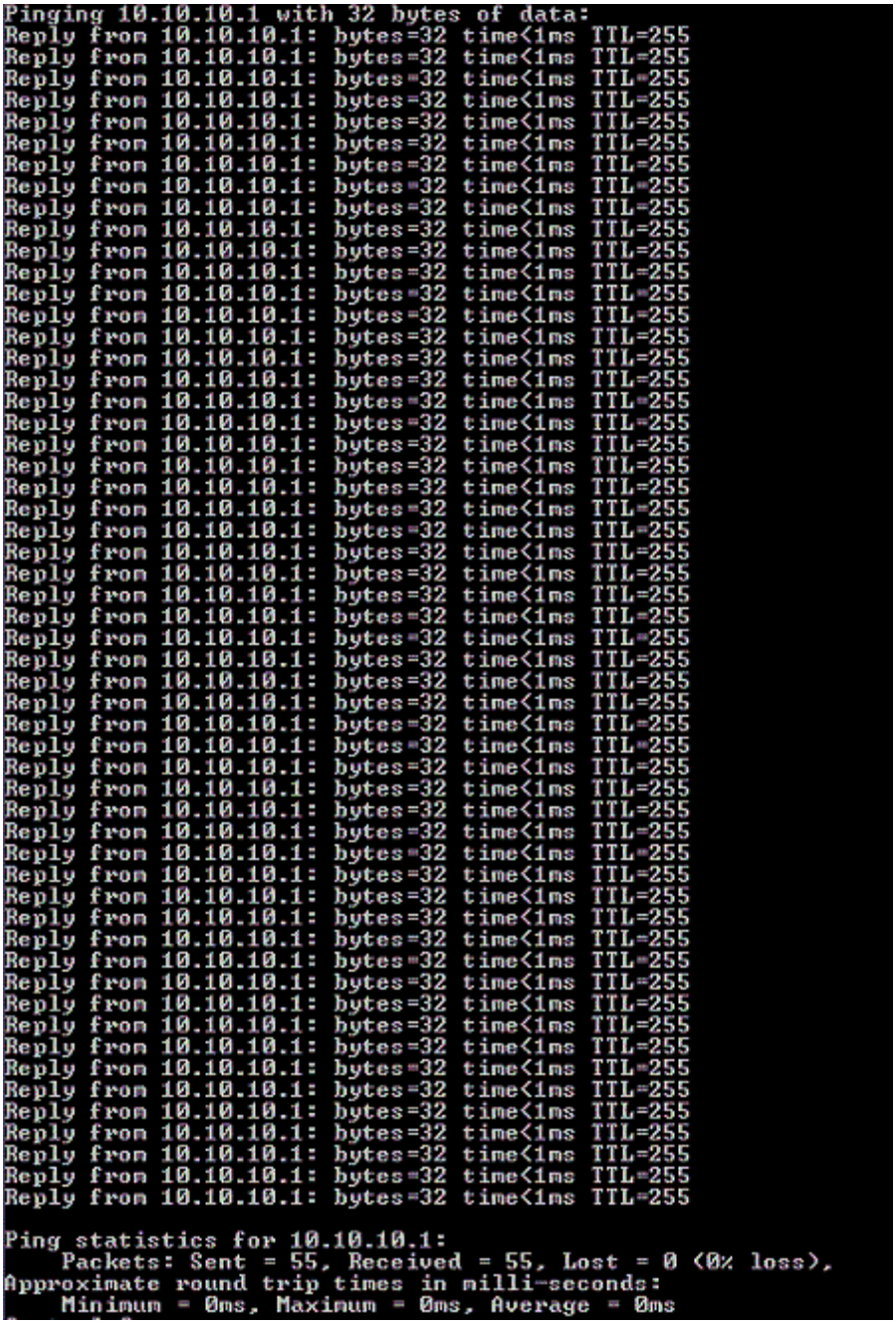
4.1 Pruebas de conectividad

En las pruebas de conectividad usamos el protocolo de Control de Mensaje de Internet (ICMP). Ingresamos a uno de los equipos destinados a la administración de nuestra controladora WLC y que se encuentra en la porción de la red donde están los puntos de acceso para constatar la conexión con la controladora pero sobretodo, la velocidad del enlace.

4.1.1 Velocidad de enlaces

En un promedio, se enviaron 55 paquetes ICMP tanto desde el punto de acceso hacia la controladora como del punto de acceso hacia el Internet. La velocidad dentro de nuestra red como era predecible, se encuentra dentro de lo que llamamos “velocidad de cable”, menor a un milisegundo ya que las conexiones de Uplink son Gigabit Ethernet y el tráfico de datos de usuarios finales no tiene una densidad significativa en un ambiente de laboratorio como se espera en un ambiente de producción. Las siguientes capturas muestran el resultado de las pruebas de conectividad en ambos casos y muestran la velocidad promedio de cada uno:

4.1.1.1 Ping Sistema de administración – WLC

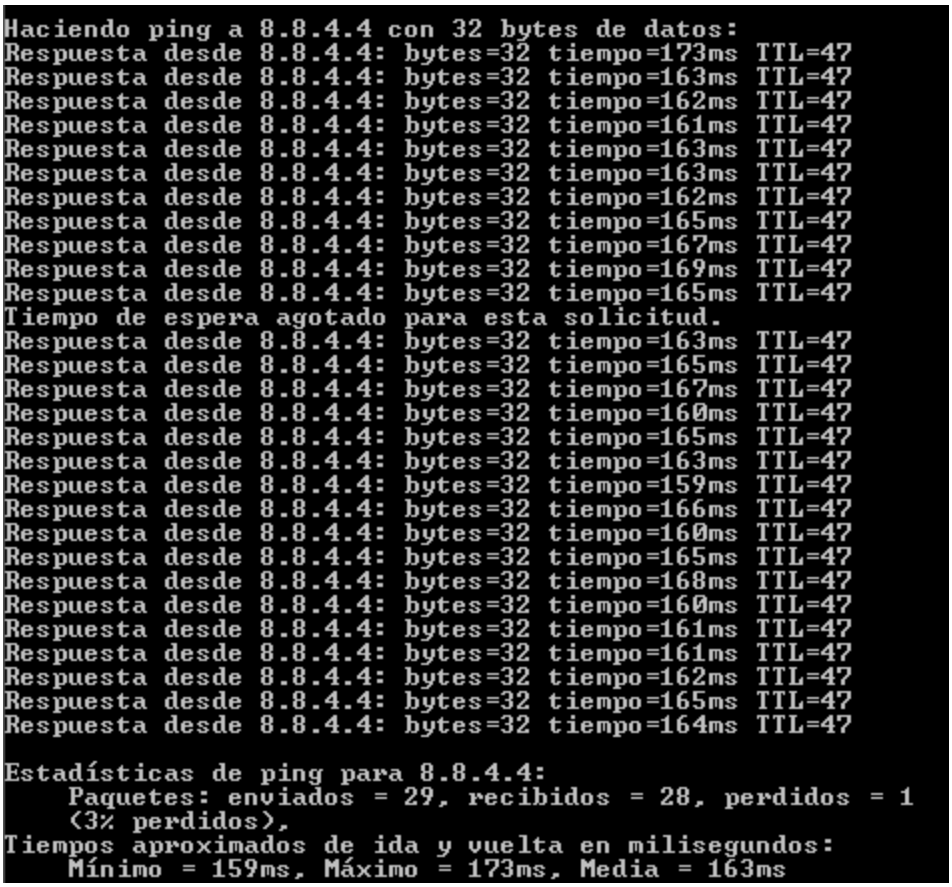


De esta salida podemos observar lo siguiente: se enviaron 55 paquetes y fueron reenviados de regreso 55 de igual manera, la pérdida de paquetes en este caso fue de un 0%. La velocidad de puesta en cable y respuesta de paquete fue menor a 1 milisegundo en el caso de todos los paquetes lo que significa que funciona a

velocidad de cable y la latencia que es el tiempo extra que cada equipo ingresa a las comunicaciones de datos, es nula para este caso.

4.1.1.2 Pruebas de Usuarios finales y salida al Internet

La siguiente prueba de conectividad ICMP que se realizó fue la de los usuarios finales contra el Internet pasando por nuestra infraestructura de red. La siguiente captura muestra los mensajes ICMP:



En esta captura observamos un comportamiento distinto ya que dependemos de otras variables cuando nos conectamos y probamos la conexión a Internet.

Primeramente en los paquetes de control ICMP observamos que existe un mínimo de pérdida de paquetes, obteniendo así un % de pérdida. La velocidad de transmisión de cada paquete fluctúa ya que no depende de nuestra infraestructura de red sino de la conexión de nuestro proveedor de servicios de Internet (ISP), lo que naturalmente agrega latencia y por ende baja la velocidad de transferencia de datos.

En definitiva, las dos capturas de pantalla muestran que existe conectividad y estabilidad en la velocidad de conexión dentro y hacia fuera en nuestra infraestructura de red. El ambiente de red es propicio para que la transmisión de datos se maneje sin ningún problema y los usuarios puedan obtener los recursos y servicios que necesitan.

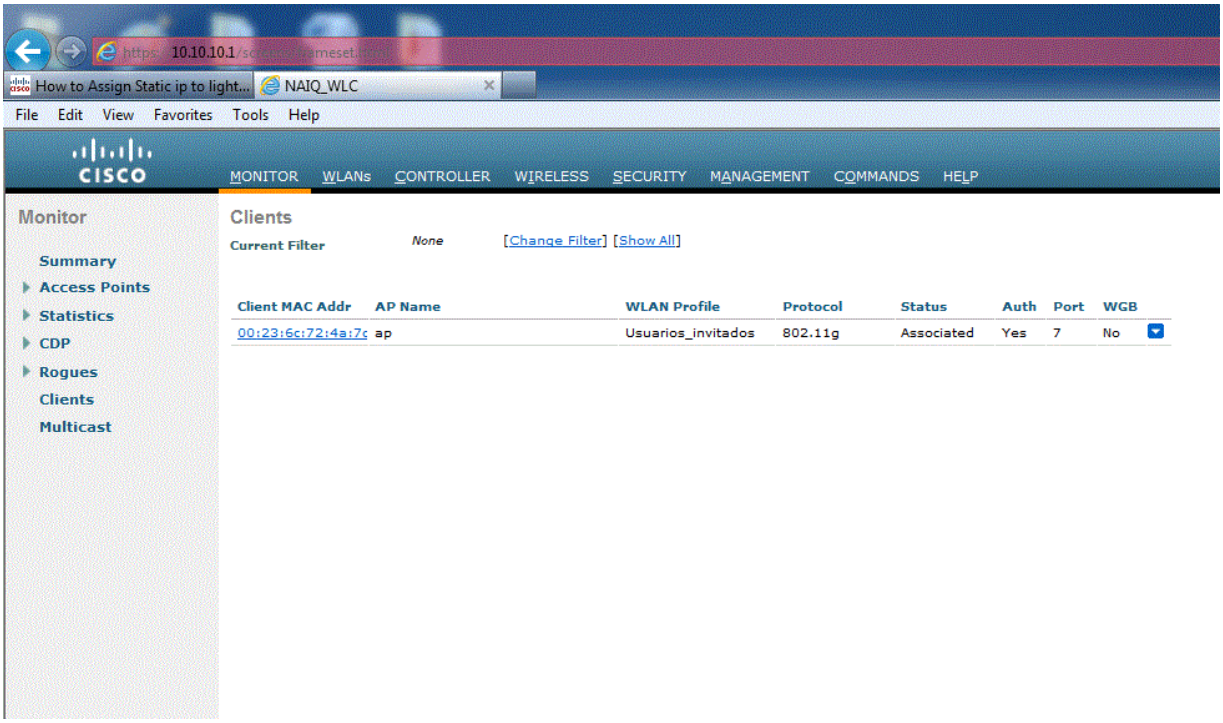
4.2 Pruebas de compatibilidad

Recordando los pasos de configuración de nuestra red, observamos que en las políticas de radio, hemos agregado distintas frecuencia a cada red. Específicamente tenemos que la red inalámbrica de usuarios privilegiados opera a 5 GHz en los protocolos 802.11a/n mientras que los usuarios invitados y administrativos operan en modos mixto a 2.4 y 5 GHz en los protocolos 802.11a/n y 802.11b/g/n. Como usuario final en este ambiente de laboratorio hemos decidido usar un dispositivo Apple Iphone ya que se encuentra entre uno de los dispositivos más usados para la navegación de usuarios en el Nuevo Aeropuerto Internacional de Quito. Las siguientes capturas muestran la compatibilidad del teléfono inteligente y la

infraestructura de nuestra red además del identificador de set de servicios (SSID) que cada red inalámbrica muestra a sus usuarios finales.

4.2.1 Equipos finales b/g/n

La siguiente captura muestra al cliente después de una asociación exitosa con el perfil de red inalámbrica Usuarios invitados. El protocolo de asociación escogido fue 802.11g gracias a sus velocidades superiores. Para desplegar esta información nos dirigimos a la pestaña Monitor > Clients. En este punto demostramos la compatibilidad con el usuario.



La siguiente captura muestra un detalle sobre el cliente asociado en qué perfil, la banda en la que se está operando, la autenticación utilizada, entre otros.

Clients > Detail

Client Properties

MAC Address	00:23:6c:72:4a:7c
IP Address	10.10.20.100
Client Type	Regular
User Name	
Port Number	7
Interface	guest
VLAN ID	20
CCX Version	Not Supported
E2E Version	Not Supported
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No

Security Information

Security Policy Completed	Yes
Policy Type	N/A
Encryption Cipher	None
EAP Type	N/A

AP Properties

AP Address	00:23:ea:02:c4:70
AP Name	ap
AP Type	802.11g
WLAN Profile	Usuarios_invitados
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implementec
CF Poll Request	Not Implementec
Short Preamble	Implemented
PBCC	Not Implementec
Channel Agility	Not Implementec
Timeout	1800
WEP State	WEP Disable

Para ingresar esta pestaña nos dirigimos a la sección Monitor > Clients > Detail. La siguiente salida de pantalla muestra exitosamente la compatibilidad del usuario mediante una prueba de conectividad final del protocolo ICMP.

Clients > Detail

Client Properties

MAC Address	00:23:6c:72:4a:7c
IP Address	10.10.20.100
Client Type	Regular
User Name	
Port Number	7
Interface	guest
VLAN ID	20
CCX Version	Not Supported
E2E Version	Not Supported
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No

Security Information

Security Policy Completed	Yes
Policy Type	N/A
Encryption Cipher	None
EAP Type	N/A

AP Properties

AP Address	00:23:ea:02:c4:70
AP Name	ap
AP Type	802.11g
WLAN Profile	Usuarios_invitados
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implementec

Ping Test Results

Client MAC Address	00:23:6c:72:4a:7c
Packets Length	500
Packets Sent	20
Packets Received	19
Local Signal Strength (dBm)	-67
Local Signal to Noise Ratio (dB)	30

4.2.2 Equipos finales a/n

La siguiente captura muestra el detalle del usuario asociado a la red de Usuarios Privilegiados que operan en los protocolos 802.11a/n a 5 GHz.

Clients > Detail

Client Properties

MAC Address	00:23:6c:72:4a:7c
IP Address	10.10.30.100
Client Type	Regular
User Name	
Port Number	7
Interface	priv
VLAN ID	30
CCX Version	Not Supported
E2E Version	Not Supported
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No

Security Information

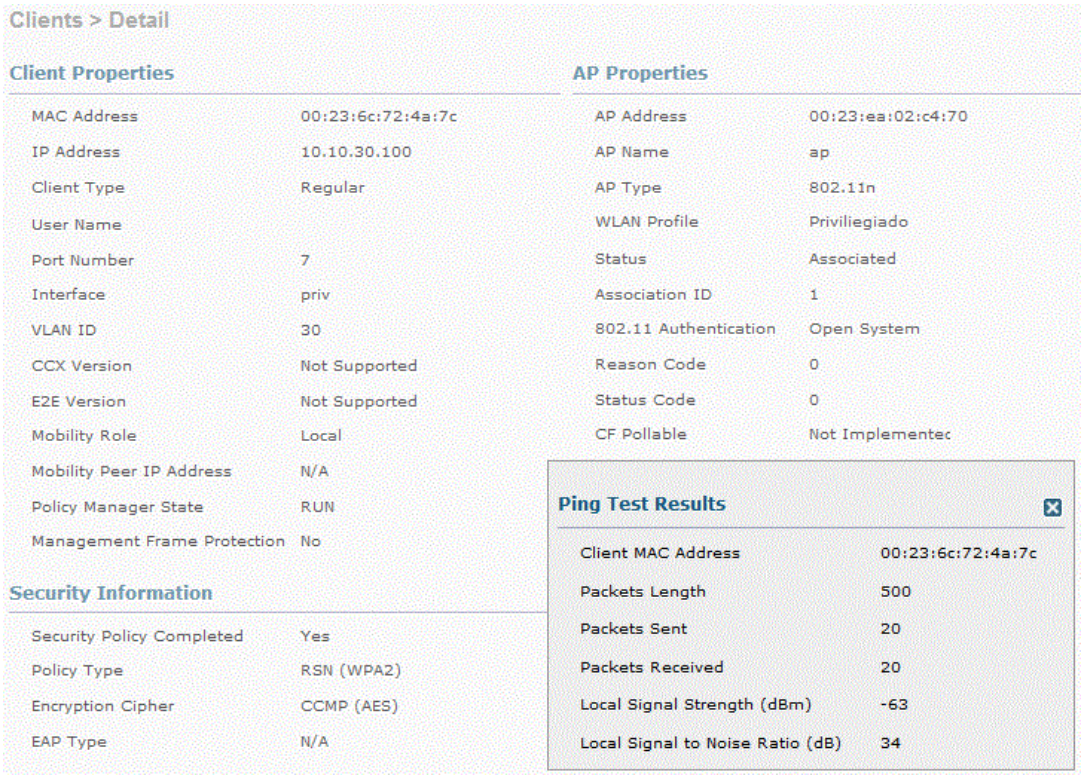
Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	N/A

AP Properties

AP Address	00:23:ea:02:c4:70
AP Name	ap
AP Type	802.11n
WLAN Profile	Priviliegiado
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	1800
WEP State	WEP Enable

Como muestra la captura, el usuario está asociado operando con el protocolo 802.11n, la autenticación en uso es Acceso Protegido Wireless versión 2 (WPA2) con cifrado de Encriptación Avanzada (AES) y se encuentra en la interfaz de red virtual VLAN 30.

La siguiente captura muestra las pruebas de conectividad de la controladora vs el usuario final, demostrando el éxito de conexión con la banda a 5 GHz:



Clients > Detail

Client Properties

MAC Address	00:23:6c:72:4a:7c
IP Address	10.10.30.100
Client Type	Regular
User Name	
Port Number	7
Interface	priv
VLAN ID	30
CCX Version	Not Supported
E2E Version	Not Supported
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No

Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	N/A

AP Properties

AP Address	00:23:ea:02:c4:70
AP Name	ap
AP Type	802.11n
WLAN Profile	Priviliegiado
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implementec

Ping Test Results

Client MAC Address	00:23:6c:72:4a:7c
Packets Length	500
Packets Sent	20
Packets Received	20
Local Signal Strength (dBm)	-63
Local Signal to Noise Ratio (dB)	34

Los procesos de asociación de usuarios en las distintas bandas han sido exitosos, demostrando que nuestro diseño es compatible con todos los protocolos estándar 802.11 disponibles en el mercado y por lo tanto este diseño es aplicable al aeropuerto y sus miles de usuarios.

4.3 Autenticación de usuarios según múltiples SSIDs

En la presente sección se mostrará como los usuarios finales se autentican para acceder a las distintas redes inalámbricas (SSIDs) para obtener sus recursos y servicios correspondientes en cada caso. Recordemos que la red de usuarios

invitados tenía seguridad abierta, la red de usuarios privilegiados tenía una llave pre-compartido (PSK) con WPA2 y la red de administradores funcionaba con RADIUS.

4.3.1 Guest

Recordando la sección de seguridad abierta, definimos este método como el más simple y casi, inexistente. La razón para mantener esta red casi insegura es para brindar a los usuarios del aeropuerto con un servicio que sea transparente y con una navegación de baja velocidad. La siguiente salida de pantalla muestra el proceso de autenticación del usuario móvil a este perfil de red:

Simplemente haciendo clic en la red “Guest” el usuario se asocia sin ninguna configuración extra. La siguiente captura muestra cómo la red dispensa de una dirección IP del “pool” DHCP correspondiente a la red de invitados:

4.3.2 Privilegiados

La red de usuarios privilegiados agrega un avance considerable a su método de seguridad pero no agrega complejidad para la configuración en los dispositivos de usuarios finales, es decir, simplemente se escribe la contraseña. La contraseña se trata de una llave pre-compartida (PSK) que está cifrada con el método de Acceso

Protegido Wireless en su segunda versión (WPA2). La descripción más detallada de este protocolo está en la sección de seguridad en este documento.

Dentro de las opciones de redes inalámbricas hacemos clic en “priviledge” como muestra la figura anterior e inmediatamente nos aparece la petición de contraseña:

Cuando la contraseña es ingresada correctamente, el proceso de asociación a la red continúa con la asignación de una dirección IP del “pool” de direcciones de esta red:

4.3.3 Administrativos

Para el perfil de red inalámbrica de los usuarios administrativos hemos escogido uno de los métodos más robustos de seguridad que se puede observar en la sección de configuración de seguridades. Configuramos una autenticación con servidor RADIUS embebido en la controladora LAN Wireless.

La base de datos del servidor RADIUS contiene las credenciales de nombre de usuario y contraseña para los usuarios administradores, constituyéndose así en uno de los esquemas de seguridad más fuertes. Hemos definido estos valores a: nombre de usuario: admin y contraseña: cisco. Cuando el usuario hace clic en la red “Admin” entre las opciones de redes disponibles en la captura anterior, inmediatamente se requerirá sus credenciales para la autenticación RADIUS como muestra la siguiente captura:

Al introducir correctamente las credenciales, el proceso de asociación puede realizarse con éxito y los usuarios administradores pueden acceder a los privilegios correspondientes.

CONCLUSIONES

5 Conclusiones y Recomendaciones

Después de las pruebas realizadas a nuestro diseño conceptual, concluimos con éxito el proceso de diseño. Teóricamente la red se ajusta a todos los requerimientos del nuevo aeropuerto en cuanto a compatibilidad, confiabilidad, seguridad, velocidad de enlaces y conexión a Internet.

5.1 Análisis de Resultados

Para el análisis de resultados, haremos un recuento de lo solicitado en el nuevo aeropuerto en cuanto a las bases conceptuales y lo que ofrecimos para cumplir con el mismo, en base a las mejores prácticas y estándares de industria.

5.2 Cumplimiento de Bases

- Bases: Equipamiento “Gateway”, el mismo que se utiliza como punto de comunicación entre la red Wireless de área local (WLAN) y la conexión hacia el Internet. Para este caso, el equipamiento incluye los Switches de comunicación para brindar conexión entre los Puntos de acceso (APs), y el Datacenter donde se centraliza la administración de estos mediante una Controladora LAN Wireless (WLC).

Solución ofertada: Porción LAN y de administración de equipamiento “Gateway” que están compuestas por una controladora CISCO 5508 de alta gama para centralización de administración de Puntos de acceso y switches 2960 que ofrecen conectividad entre APs y WLC con redundancia mediante puertos para conexiones Uplink de alta velocidad.

- Bases: 18 Puntos de acceso, que deben soportar un alta capacidad de compatibilidad con todos los protocolos 802.11 estándar revisados en este documentos en secciones anteriores a/n y b/g/n, con funcionamiento en las dos bandas principales de las redes inalámbricas actuales: 2,4 y 5 GHz y finalmente con una cobertura de un radio de 30 metros con un Sobrelapamiento del 15 al 20% que está contemplado conceptualmente en las bases.

Solución ofertada: 18 Puntos de acceso CISCO 3602 que están entre los más avanzados en cuanto a compatibilidad, cobertura y velocidad en el mercado actual. El posicionamiento de cada uno está definido en las bases conceptualmente por lo que este campo de ingeniería de celdas no es parte de la oferta.

- Bases: Equipamiento para “Acceso Seguro y Autorización”. Servidor RADIUS que estará embebido o incluido en la controladora LAN Wireless.

Solución ofertada: servidor RADIUS embebido en la misma controladora WLC para brindar, mediante una base de datos local, autenticación avanzada a cada usuario de la red de administración con un esquema más robusto.

Cabe destacar que la solución ofertada en este trabajo se llevó a cabo tras un proceso de múltiples auditorías al diseño desde julio de 2012 para garantizar que se brinde la tecnología más avanzada en el caso de marca CISCO por ende es de suma importancia recalcar que por marca no existió una mejor posibilidad.

Como parte de las conclusiones es importante hacer referencia al proceso de mejoramiento de las bases ya que como se puede observar en el anexo, las mismas tienen un carácter general y poco específico por lo cual se agregó desarrollaron tareas adicionales al proceso de dimensionamiento.

5.3 Recomendaciones

Para la provisión de una red para el Nuevo Aeropuerto se deben tomar en cuenta aspectos cómo la muy alta densidad de usuarios, por ende esto significa en equipamiento lo siguiente:

- Controladoras LAN Wireless redundantes.
- Servidores ASA y/o ACS dedicados para brindar seguridad.
- Tarifadores o “Traffic Shapers” para una mejor distribución del ancho de banda.
- Una conexión de Internet de alta velocidad con la menor compartición posible.

Dicho equipamiento no ha sido parte de la discusión de este documento por tratarse de un diseño conceptual, pero queremos enfatizar la alta importancia de estos

dispositivos como parte de una solución funcional que brinde el mejor servicio para los futuros usuarios de uno de los Aeropuertos más grandes de Latinoamérica.

BIBLIOGRAFÍA

Carroll, Brandon. *CCNA Wireless Official Guide*. 2da Edición. Indianapolis: Cisco Press, 2009.

"Graham Bell invents the Photophone." *Scientific American* [New York] 02 10 1880, Pág. 3. Web. 7 enero, 2013. <http://www.rarenewspapers.com/view/554832>.

Beals, Gerald. *Major Inventions of Thomas Alba Edison*. Gerald Beals June. Web. 7 enero, 2013. <http://www.thomasedison.com/Inventions.htm>.

Carrión, Hugo. *Internet en el Ecuador*. Hugo Carrión. Web. 7 enero, 2013. <http://www.hugocarrion.com/index_archivos/Docs/E_topcomm_internet.pdf>.

Prasad, Ramjee. *Universal Wireless Personal Communication*. Artech House, 1998.

Boylestad, Robert. *Introducción al análisis de circuitos*. 10ma Edición. México: Pearson, 2004.

Serway, Raymond, and John Jewett. *Principles of physics*. 4ta Edición. Cengage Learning, 2005.

Bidgoli, Hossein; et al. *Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management*. New Jersey: John Wiley & Sons, 2006.

McCabe, Karen. "IEEE Ratifies 802.11n, Wireless LAN Specification to Provide Significantly Improved Data Throughput and Range." Business Wire, 11 2009.

Web. 8 enero, 2013. <http://www.reuters.com/article/2009/09/11/idUS183099 11-Sep-2009 BW20090911>.

McCann, Stephen, and Alex Ashley. "OFFICIAL IEEE 802.11 WORKING GROUP PROJECT TIMELINES." IEEE, 16 2012. Web. 8 enero, 2013. <http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm>.

Watkins, Michael, and Kevin Wallace. *CCNA Security Official Guide*. 2da Edición. Indianapolis: Cisco Press, 2008.

García, Eduardo; et al. "Effect of adjacent-channel interference in IEEE 802.11 WLANs." CrownCom, Web. 8 enero, 2013. <https://upcommons.upc.edu/e-prints/bitstream/2117/1234/1/CrownCom07_CReady.pdf>.

Black, Uyless. *Ip Routing Protocols*. 1era Edición. New Jersey: Prentice-Hall, Inc., 2000.

GLOSARIO

802.11

Conjunto de estándares para la comunicación con los equipos que forman parte de una red local inalámbrica.

802.11a

Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 54 Mbps y una frecuencia de funcionamiento de 5 GHz.

802.11b

Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 11 Mbps y una frecuencia de funcionamiento de 2,4 GHz.

802.11g

Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 54 Mbps, una frecuencia de funcionamiento de 2,4 GHz y con compatibilidad con versiones anteriores con dispositivos 802.11b.

802.11n

Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 600 Mbps en ambientes n puros, una frecuencia de funcionamiento de mixta y con compatibilidad con versiones anteriores con dispositivos 802.11 a/b/g.

Ad-hoc

Grupo de dispositivos inalámbricos que se comunican directamente entre ellos (punto a punto) sin la utilización de un punto de acceso.

AES (Estándar Avanzado de Encriptación)

Técnica de cifrado de datos simétrica de bloque de 256 bits.

Ancho de banda

Capacidad de transmisión de un dispositivo o red determinado.

Base de datos

Recopilación de datos que puede organizarse de forma que sus contenidos puedan accederse, gestionarse y actualizarse fácilmente.

Bit (dígito binario)

La unidad más pequeña de información de una máquina.

Broadcast

Sistema de envío de mensajes, en donde se envía el mensaje a todos los ordenadores participantes y conectados a una red.

Byte

Una unidad de datos que se compone de ocho bits.

CDMA (Code Division Multiple Access)

La Multiplexación por división de código, acceso múltiple por división de código o CDMA es un término genérico para varios métodos de Multiplexación o control de acceso al medio basado en la tecnología de espectro expandido. Habitualmente se emplea en comunicaciones inalámbricas (por radiofrecuencia), aunque también puede usarse en sistemas de fibra óptica o de cable.

DHCP (Protocolo de configuración dinámica de host)

Protocolo que permite a un dispositivo de una red, conocido como servidor DHCP, asignar direcciones IP dinámicas y temporales a otros dispositivos de red, normalmente equipos.

Cifrado

Es la manipulación de datos para evitar que cualquiera de los usuarios a los que no están dirigidos los datos pueda realizar una interpretación precisa.

CSMA/CA (Acceso múltiple de detección de portadora)

Un método de transferencia de datos que se utiliza para prevenir una posible colisión de datos.

Dirección IP

Dirección que se utiliza para identificar un equipo o dispositivo en una red.

Dirección IP dinámica

Dirección IP temporal que asigna un servidor DHCP.

Dirección IP estática

Dirección fija asignada mediante configuración manual a un equipo o dispositivo conectado a una red.

DSL (Línea de suscriptor digital)

Conexión de banda ancha permanente a través de las líneas de teléfono tradicionales.

DSSS (Espectro de dispersión de secuencia directa)

Transmisión de la frecuencia con un patrón de bit redundante que se traduce en una menor probabilidad de que la información se pierda durante dicha transmisión.

EAP (Protocolo de autenticación extensible)

Protocolo general de autenticación que se utiliza para controlar el acceso a redes. Muchos métodos de autenticación específicos trabajan dentro de este marco.

Espectro de Radio Frecuencia

Rango continuo de frecuencias en el que las ondas de una cierta naturaleza tienen alguna propiedad común.

Ethernet

Protocolo de red estándar de IEEE que especifica la forma en que se colocan los datos y se recuperan de un medio de transmisión común.

Fibra óptica

Medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

Full - Duplex

La disponibilidad de un dispositivo de red para recibir y transmitir datos de forma simultánea.

Gateway (Puerta de enlace)

Un dispositivo que interconecta redes con protocolos de comunicaciones diferentes e incompatibles.

GHz

Equivale a 109 hercios (1 millón). Se utiliza muy frecuentemente como unidad de medida de la frecuencia de trabajo de un dispositivo de hardware.

GSM (Global System for Mobile Communications)

Sistema estándar, para la comunicación mediante teléfonos móviles que incorporan tecnología digital.

Half - Duplex

Transmisión de datos que puede producirse en dos direcciones a través de una única línea, pero sólo en una dirección cada vez.

Hardware

El aspecto físico de equipos, telecomunicaciones y otros dispositivos de tecnologías de la información.

Hz (Hercio)

El hertz o hertzio es la unidad de frecuencia del Sistema Internacional de Unidades. Existe la división de este término en submúltiplos y múltiplos documentados en un Sistema Internacional de Unidades.

IEEE (The Institute of Electrical and Electronics Engineers)

Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas.

Infraestructura

Equipo de red e informático actualmente instalado.

IP (Internet Protocol)

Protocolo utilizado para enviar datos a través de una red.

ISP (Internet Service Provider)

Compañía que proporciona acceso a Internet.

MAC (Media Access Control)

Una dirección MAC es la dirección de hardware de un dispositivo conectado a un medio de red compartido.

Máscara de subred

Código de dirección que determina el tamaño de la red.

Mbps (Megabits por segundo)

Un millón de bits por segundo, unidad de medida de transmisión de datos.

MHz

Equivale a 106 hercios (1 millón). Se utiliza muy frecuentemente como unidad de medida de la frecuencia de trabajo de un dispositivo de hardware.

MIMO

(Multiple Input Multiple Output) - nomenclatura para la tecnología de antenas múltiples utilizado para transmitir datos en paralelo.

Modo infraestructura

Configuración en la que se realiza un puente entre una red inalámbrica y una red con cable a través de un punto de acceso.

Multicast

Envío de datos a un grupo de destinos a la vez.

Multiplexación

La Multiplexación es el método que consiste en compartir un mismo medio de transmisión entre varias comunicaciones.

OFDM (Orthogonal Frequency Division Multiplexing)

La transmisión de frecuencia que separa la corriente de datos en un número de corrientes de datos de velocidad inferior que se transmiten en paralelo para prevenir que se pierda información durante la transmisión.

PoE (Alimentación eléctrica a través de Ethernet)

Tecnología que permite a un cable de red Ethernet transmitir tanto datos como corriente.

Preámbulo

Parte de la señal inalámbrica que sincroniza el tráfico de red.

Puente

Dispositivo que conecta dos tipos diferentes de redes locales, como por ejemplo una red inalámbrica a una red Ethernet con cable.

Puerto

Punto de conexión en un equipo o dispositivo de red utilizado para conectar un cable o adaptador.

Punto de acceso

Dispositivo que permite a los equipos y a otros dispositivos equipados con función inalámbrica comunicarse con una red con cable. También se utiliza para ampliar el alcance de una red inalámbrica.

RADIUS (Remote Authentication Dial-In User Service)

Servicio de Autenticación Remota de Usuarios Entrantes. Protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1813 UDP para establecer sus conexiones.

RC4

Es un algoritmo de cifrado de flujo. Los algoritmos de cifrado de flujo, funcionan expandiendo una clave secreta. En el caso de WEP, un vector de inicialización público (IV) y una clave secreta en una clave arbitrariamente larga de bits pseudo-aleatorios.

Red

Serie de equipos o dispositivos conectados con el fin de compartir datos, almacenamiento y la transmisión entre usuarios.

Red LAN (Local Area Network)

Es la interconexión de varios servidores y periféricos. Su extensión está limitada físicamente a un entorno de 100 metros.

Red Punto a Punto

Aquellas que responden a un tipo de arquitectura de red en las que cada canal de datos se usa para comunicar únicamente dos nodos.

Red WAN (Wide Area Network)

Es un tipo de red de computadoras capaz de cubrir distancias desde unos 100km hasta unos 1000 km, dando el servicio a un país o un continente.

RFC

(Request For Comments) RFC son documentos elaborados por el IETF con el objetivo de documentar protocolos, procedimientos operativos y tecnologías de internet.

Roaming

Capacidad de utilizar un dispositivo de comunicación móvil y poder moverse de una célula o punto de acceso a otro sin perder la conexión.

Router

Enrutador, es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Este dispositivo permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

Servidor

Cualquier equipo cuya función en una red sea proporcionar acceso al usuario a archivos, impresión, comunicaciones y otros servicios.

Servidor dedicado de seguridad

Un servidor de seguridad es cualquiera de los esquemas de seguridad que evitan a los usuarios no autorizados obtener acceso a una red de equipos o que supervisa la transferencia de información hacia y desde la red.

Software

Instrucciones para el equipo. Se denomina “programa” al conjunto de instrucciones que realizan una tarea determinada.

SOHO (Oficina pequeña/oficina doméstica)

El segmento de mercado de profesionales que trabajan en casa o en pequeñas oficinas.

Spanning Tree

Protocolo especificado en IEEE 802.1D que permite a una red que tiene una topología que contiene lazos físicos, eliminarlos lógicamente. Spanning Tree opera en Puentes y Switches.

SSID (Service Set IDentifier)

Nombre de su red inalámbrica. Tasa TX Tasa de transferencia.

Switch

Dispositivo que es el punto central de conexión de equipos y otros dispositivos de una red, de forma que los datos puedan transmitirse a velocidad de transmisión completa.

TKIP (Temporal Key Integrity Protocol)

Protocolo de cifrado inalámbrico que cambia periódicamente la clave de cifrado, haciendo más difícil su decodificación.

Topología

Distribución física de una red.

UDP (User Datagram Protocol)

Protocolo de red para la transmisión de datos que no requieren la confirmación del destinatario de los datos enviados.

Up-time

Tiempo de actividad, periodo de la producción activa de una red sin contar cortes en el servicio, periodo operacional.

VLAN (Virtual LAN)

Una red que lógicamente agrupa a un grupo de dispositivos como si estuvieran conectados al mismo cable, cuando en realidad están conectados en diferentes segmentos de una LAN.

VPN (Red privada virtual)

Medida de seguridad para proteger los datos a medida que abandona una red y pasa otra a través de Internet.

WEP (Wired Equivalent Privacy)

Protocolo de seguridad para redes inalámbricas. El objetivo de WEP es proporcionar seguridad mediante el cifrado de datos a través de ondas de radio, de forma que estén protegidos a medida que se transmiten de un punto a otro. Para permitir la comunicación entre los equipos y el enrutador se utiliza una clave compartida (similar a una contraseña).

Wireless

Tipo de comunicación en la que no se utiliza un medio de propagación físico alguno esto quiere decir que se utiliza la modulación de ondas electromagnéticas.

WLAN (Wireless Local Area Network)

Grupo de equipos y dispositivos asociados que se comunican entre sí de forma inalámbrica.

WPA (WiFi Protected Access)

Protocolo de seguridad para redes inalámbricas que se fundamenta en los cimientos básicos de WEP. La robustez añadida de WPA es que la clave cambia de forma dinámica. La clave, en continuo cambio, dificulta que un pirata informático pueda conocer la clave y obtener acceso a la red.

WPA2 (WiFi Protected Access 2)

WPA2 es la segunda generación de WPA y proporciona un mecanismo de cifrado más fuerte a través del Estándar de cifrado avanzado (AES), requisito para algunos usuarios del gobierno.

WPA-Enterprise

Versión de WPA que utiliza las mismas claves dinámicas que WPA-Personal y también requiere que todo dispositivo inalámbrico esté autorizado según lista maestra, albergada en un servidor de autenticación especial.

WPA-Personal

Versión de WPA que utiliza claves de cifrado en constante cambio y de mayor longitud para complicar el proceso de su decodificación.

ANEXOS

Anexo 1 – Bases

Anexo 2 - Ficha técnica WLC 5508

Anexo 3 - Ficha técnica AP 3600