Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

PROPUESTA PARA OPTIMIZAR LA RED IEEE 802.11 EN EL ÁREA DE RECREACIÓN DE LA FACULTAD DE INGENIERÍA, USAC

José Angelo Caal Ortíz
Asesorado por el Ing. Carlos Eduardo Guzmán Salazar

Guatemala, mayo de 2017

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

PROPUESTA PARA OPTIMIZAR LA RED IEEE 802.11 EN EL ÁREA DE RECREACIÓN DE LA FACULTAD DE INGENIERÍA, USAC

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

JOSÉ ANGELO CAAL ORTÍZ
ASESORADO POR EL ING. CARLOS EDUARDO GUZMÁN SALAZAR

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, MAYO DE 2017

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Pedro Antonio Aguilar Polanco
VOCAL I	Ing. Angel Roberto Sic García
VOCAL II	Ing. Pablo Christian de León Rodríguez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Jurgen Andoni Ramírez Ramírez
VOCAL V	Br. Oscar Humberto García Nuñez
SECRETARIA	Inga. Lesbia Magalí Herrera López

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Julio Cesar Solares Peñate
EXAMINADOR	Ing. Marvin Marino Hernández Fernández
EXAMINADORA	Inga. María Magdalena Puente Romero
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

PROPUESTA PARA OPTIMIZAR LA RED IEEE 802.11 EN EL ÁREA DE RECREACIÓN DE LA FACULTAD DE INGENIERÍA, USAC

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 21 septiembre de 2015.

José Angelo Caal Ortíz

Guatemala, 19 de enero de 2017

Señor
Coordinador Área de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Estimado Coordinador:

Hago de su conocimiento por este medio que el estudiante JOSÉ ANGELO CAAL ORTÍZ, ha concluido su trabajo de graduación titulado "Propuesta para Optimizar la Red IEEE 802.11 en el Área de Recreación de la Facultad de Ingeniería, USAC". Habiendo cumplido con los objetivos que se plantearon para el mismo.

Por lo que, en mi calidad de ASESOR nombrado por la Escuela de Ingeniería Mecánica Eléctrica, doy mi aval para que se continúe el trámite correspondiente dentro de la Universidad. Así mismo, índico que el estudiante Caal Ortíz y el suscrito somos enteramente responsables por el contenido del trabajo de graduación referido.

Reciba un cordial saludo,

Carlos Guzmán Salazar
ASESOR

CARLOS GUZMAN SALAZAR
Ingeniero Electricista
Col. No. 2762

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 06. 2017.
Guatemala, 20 de ENERO 2017.

Señor Director
Ing. Francisco Javier González López
Director Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: PROPUESTA PARA OPTIMIZAR LA RED IEEE 802.11 EN EL ÁREA DE RECREACIÓN DE LA FACULTAD DE INGENIERÍA, USAC, del estudiante José Angelo Caal Ortíz, que cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,
ID Y ENSEÑAD A TODOS

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

Ing. Carlos Eduardo Guzmán Salazar
Coordinador Área Electrónica

sro

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 06. 2017.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto bueno del Coordinador de Área, al trabajo de Graduación del estudiante JOSÉ ANGELO CAAL ORTÍZ Titulado: PROPUESTA PARA OPTIMIZAR LA RED IEEE 802.11 EN EL ÁREA DE RECREACIÓN DE LA FACULTAD DE INGENIERÍA, USAC, procede a la autorización del mismo.

Ing. Francisco Javier González López

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

GUATEMALA, 24 DE FEBRERO 2017.

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

DTG. 222.2017

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al Trabajo de Graduación titulado: **PROPUESTA PARA OPTIMIZAR LA RED IEEE 802.11 EN EL ÁREA DE RECREACIÓN DE LA FACULTAD DE INGENIERÍA, USAC,** presentado por el estudiante universitario: **José Angelo Caal Ortíz,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

Ing. Pedro Antonio Aguilar Polanco
Decano

Guatemala, mayo de 2017

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

/gdech

ACTO QUE DEDICO A:

Dios	Por ser mi guía y fortaleza en la vida, por todas las bendiciones que me ha dado.
Mis padres	Carlos Manuel Caal y Nancy Asunción Ortíz. Por ser ángeles en mi vida, por su apoyo incondicional, paciencia y amor.
Mi hermana	Helen Elvira Caal Ortíz. Por su apoyo en esos momentos difíciles y por su compañía incomparable.
Mi abuela	Filomena Caal Macz. Por estar cuidándome desde el cielo, por su amor brindado.
Mis amigos	Por su apoyo durante los años universitarios, por haber formado un gran grupo, por haber desarrollado en mi la perseverancia, tolerancia y trabajo en equipo.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por darme la oportunidad de formar un profesional, orgulloso de la institución donde estudió.
EIME USAC	Por ser una importante influencia en mi carrera
Ing. Carlos Guzmán	Por su asesoría del presente trabajo, por ser una persona con valores, por su excelente trabajo como catedrático.
Mi hermana Katherine Rasaná	Por apoyarme a en los momentos cruciales, por su cariño incondicional y acompañarme por el camino de la vida.
Mis amigos de la carrera	Por haber formado un gran equipo de trabajo, por dar la milla extra, por todos esos sacrificios en la universidad.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES VII
LISTA DE SÍMBOLOS XIII
GLOSARIO XV
RESUMEN XXI
OBJETIVOS XXIII
INTRODUCCIÓN XXV

1. CONCEPTOS BÁSICOS DE RADIOFRECUENCIA 1
1.1. Redes inalámbricas 1
1.2. Propiedades de onda 1
1.2.1. Frecuencia 2
1.2.2. Fase 2
1.2.3. Longitud de onda 3
1.3. Decibel 4
1.3.1. dBm 5
1.3.2. dBi 6
1.3.3. dBd 6
1.4. SNR 6
1.5. Potencia de una señal RF 6
1.6. Modulación 8
1.6.1. FHSS 9
1.6.2. DSSS 10
1.6.2.1. 1Mbps DSSS 12
1.6.2.2. 2Mbps DSSS 12
1.6.2.3. 5.5Mbps DSSS 13

1.6.2.4. 11Mbps DSSS 13
1.6.3. OFDM 13
1.7. Interferencia 14
1.7.1. Interferencia Co-Canal 15
1.7.2. Interferencia del canal vecino 16
1.7.3. Interferencia no 802.11 16
1.8. Pérdida en el espacio libre 17
1.9. Propagación de una señal de radio frecuencia 21
1.9.1. Reflexión 21
1.9.2. Absorción 22
1.9.3. Dispersión 22
1.9.4. Refracción 23
1.9.5. Difracción 24
1.10. Zona de Fresnel 25
1.11. Patrones de radiación 26
1.12. Ganancia 27
1.13. Ancho de haz 28
1.14. Polarización 29
1.15. Antena omnidireccional 30

2. ESTÁNDARES INTERNACIONALES PARA TECNOLOGÍA INALÁMBRICA 35
2.1. Organismos regulatorios 35
2.1.1. ITU-R 35
2.1.2. FCC 37
2.1.3. ETSI 38
2.2. Organismo de normalización IEEE 39
2.3. Canales utilizados en 802.11 40
2.3.1. Canales en la banda ISM 2.4GHz 40

2.3.2. Canales en las bandas U-NII 5-GHz 42
2.4. Estándares IEEE 802.11 44
2.4.1. 802.11-1997 45
2.4.2. 802.11b 46
2.4.3. 802.11g 46
2.4.4. 802.11ª 48
2.4.5. 802.11n 49
2.4.5.1. Agregación de canal 50
2.4.5.2. Multiplexación espacial 52
2.4.5.3. Formación del rayo transmitido (TxBF) 53
2.4.6. 802.11ac 54
2.4.7. 802.11ad 54
2.5. Alianza Wi-Fi 54

3. FUNDAMENTOS DE DISPOSITIVOS LAN Y WLAN 57
3.1. Cable par trenzado 57
3.1.1. *Unshielded twisted pair* UTP 57
3.1.2. *Shielded twisted pair* STP 58
3.1.3. *Foiled twisted pair* FTP 58
3.1.4. *Screened fully shielded twisted pair* FSTP 59
3.2. Transceptor SFP 61
3.2.1. Ethernet sobre fibra óptica 61
3.2.2. Ethernet sobre UTP 63
3.3. Punto de acceso inalámbrico 64
3.3.1. Funcionamiento del AP 67
3.3.1.1. Conjunto de servicios básicos (BSS) ... 69
3.3.1.2. Sistema de distribución 71

3.3.1.3. Conjunto de servicios extendidos (ESS) 73
3.4. *Switch* 75
3.4.1. Funcionamiento del *switch* 76
3.4.1.1. Decisión de enviar o filtrar tramas 77
3.4.1.2. Proceso de aprendizaje de direcciones MAC 77
3.4.1.3. Tramas *flood* 78
3.4.1.4. Evitar *loops* utilizando STP 79
3.4.1.5. LANs Virtuales (VLAN) 79
3.5. Controlador inalámbrico LAN 80
3.5.1. *Roaming* 82
3.5.2. Diseño de canales WLAN 83

4. FUNDAMENTOS DE SEGURIDAD EN REDES INALÁMBRICAS 89
4.1. Autenticación 89
4.1.1. Privacidad del mensaje 91
4.1.2. Integridad del mensaje 92
4.1.3. Protección contra intrusos 93
4.2. Métodos de autenticación para clientes inalámbricos 93
4.2.1. Autenticación abierta 93
4.2.2. WEP 95
4.2.3. 802.1x/EAP 95
4.2.4. PEAP 97
4.2.5. EAP-TLS 97
4.3. Privacidad inalámbrica y métodos de integridad 98
4.3.1. TKIP 98
4.3.2. CCMP 99
4.3.3. WPA y WPA2 99

5. DISEÑO DE LA PROPUESTA PARA OPTIMIZAR LA RED 802.11 101
5.1. Estudio del sitio 104
5.1.1. Mapas de calor 107
5.1.1.1. Área 1 – Plaza columnas extensión... 108
5.1.1.2. Área 2 – Plaza columnas..... 110
5.1.1.3. Área 3 - Jardín principal de la Facultad de Ingeniería, USAC 113
5.1.1.4. Área 4 - Los Ranchitos de ingeniería. 115
5.2. Diagrama red inalámbrica HLD (*high level design*) 119
5.3. Diagrama red inalámbrica LLD (*low level design*) 122
5.3.1. Conexiones físicas entre equipos..... 122
5.3.2. *Switch* Cisco Catalyst 2960X-24PS-L..... 124
5.3.2.1. Configuración *switch*Cisco Catalyst 2960X-24PS-L 126
5.3.3. Puntos de acceso Cisco Aironet 3702i 128
5.3.3.1. Instalación física de los *access points* 130
5.3.3.2. Configuración punto de acceso 133
5.3.4. Controlador inalámbrico LAN Cisco 5508..... 133
5.3.4.1. Instalación física del WLC 136
5.3.4.2. Interfaces del wireless LAN *Controller* WLC 137
5.3.4.3. Configuración inicial del WLC..... 139
5.3.4.4. Configuración avanzada del WLC 142
5.3.4.4.1. Interfaz de administración 142
5.3.4.4.2. Puerto de servicio..... 144
5.3.4.4.3. Interfaces dinámicas... 144

5.3.4.4.4. Configuración de redes *wireless* 149
5.3.4.4.5. Generalidades del WLC 154
5.4. Sección económica 156
5.4.1. Fuente de financiamiento 157
5.4.2. Inversión inicial 157
5.4.3. Beneficios 160

CONCLUSIONES 165
RECOMENDACIONES 167
BIBLIOGRAFÍA 169

ÍNDICE DE ILUSTRACIONES

FIGURAS

1. Frecuencia de onda 2
2. Fase de onda 3
3. Longitud de onda 4
4. Potencia de la señal RF sobre el camino 8
5. Canales sin intercepción en DSSS 10
6. Diagrama de bloques transmisión DSSS 11
7. Interferencia Co-Canal 15
8. Interferencia de canal vecino 16
9. Interferencia no 802.11 de un microondas 17
10. Pérdida en el espacio libre por dispersión en la onda 18
11. Rango efectivo para transmisores de 2,4 GHz y 5 GHz 19
12. Cambio dinámico de velocidad en función del rango 20
13. Reflexión de una señal 21
14. Absorción de una señal 22
15. Dispersión de una señal 23
16. Refracción de una señal 24
17. Difracción de una señal 24
18. Zona de Fresnel 25
19. Patrón E y H de una antena isotrópica 27
20. Patrones de radiación para los tres tipos básicos de antena 28
21. Ejemplo de ancho de haz 29
22. Polarización 30
23. Patrón de radiación en 3D de un dipolo 31

24. Patrones de radiación en planos E y H de un dipolo 32
25. Antena monopolo 33
26. Canales en la banda 2,4 GHz 42
27. Canales de las bandas U-NII 5 GHz 43
28. Ejemplos de dispositivos SISO y MIMO 50
29. Comparación entre canales de 20 MHz y 40 MHz 51
30. Multiplexación entre dos dispositivos MIMO 3x3:2 52
31. Formación de rayo dirigido a un dispositivo específico 53
32. Logo certificación WiFi 55
33. Cable UTP 58
34. Cable STP 58
35. Cable FTP 59
36. Cable FSTP 59
37. SFP SX 62
38. SFP LX 62
39. SFP EX 63
40. SFP ZX 63
41. SFP TX 64
42. *Access point* 66
43. Patrones de radiación E y H de una antena omnidireccional 67
44. Comunicación bidireccional 68
45. Interferencia por transmisiones simultáneas 68
46. 802.11 BSS 70
47. Comunicación dentro de un BSS 71
48. Sistema de distribución con BSS 72
49. Múltiples SSIDs en un AP 73
50. 802.11 ESS 74
51. *Switch* 76
52. Dos dominios *broadcast* sin VLAN 80

53. Dos VLANs en un *switch* 80
54. *Roaming* entre dos AP 83
55. Espacio entre celdas alternadas 84
56. Celdas alternadas correctamente 85
57. Celdas de canales en 3D 86
58. Controlador red LAN inalámbrica 88
59. Autenticación de usuario 90
60. Autenticación de AP 91
61. Cifrado de datos en red inalámbrica 92
62. WLAN con autenticación abierta 94
63. Autenticación EAP 96
64. Facultad de Ingeniería, USAC 102
65. Plaza columnas 102
66. Jardín principal de la Facultad de Ingeniería USAC 103
67. Los ranchitos de la Facultad de Ingeniería 103
68. Aplicación de la herramienta Ekahau 106
69. Mapa de calor de la herramienta Ekahau 106
70. Plaza columnas extensión 108
71. SSID FIUSAC en el área 1 109
72. SSID RIUSAC en el área 1 109
73. SSID TESIS en el área 1 110
74. Plaza columnas 110
75. SSID FIUSAC en el área 2 111
76. SSID RIUSAC en el área 2 111
77. SSID TESIS en el área 2 112
78. Jardín principal de la Facultad de Ingeniería, USAC 113
79. SSID FIUSAC en área 3 114
80. SSID RIUSAC en área 3 114
81. SSID TESIS en el área 3 115

82. Los ranchitos de ingeniería 115
83. SSID FIUSAC en el área 4 116
84. SSID RIUSAC en el área 4 116
85. SSID TESIS en el área 4 117
86. Áreas propuestas para el diseño de la red *wireless* 119
87. Diagrama general del diseño *wireless* 120
88. Diagrama de la comunicación capa 1 y capa 2 121
89. Diagrama de la comunicación capa 3 122
90. Diagrama detallado de la red *wireless* 123
91. *Switch* Cisco Catalyst 2960X-24PS-L 126
92. *Access point* serie 3700 130
93. Ubicación de *access point* AP-FIUSAC-01 131
94. Ubicación de *access points* AP-FIUSAC-02 y 03 132
95. Ubicación de *access point* AP-FIUSAC-04 132
96. Cisco WLC 5508 134
97. Configuración interna del WLC 137
98. Interfaces del WLC 5508 139
99. Interfaz de administración del WLC 143
100. Puerto de servicio del WLC 144
101. Interfaces dinámicas del diseño 145
102. Asociación interfaz dinámica – SSID 145
103. Configuración interfaz dinámica paso 1 146
104. Configuración interfaz dinámica paso 2 146
105. Configuración interfaz dinámica paso 3 147
106. Configuración interfaz dinámica paso 4 148
107. Configuración red *wireless* paso 1 149
108. Configuración red *wireless* paso 2 150
109. Configuración red *wireless* paso 3 150
110. Configuración red *wireless* paso 4 151

111. Configuración red *wireless* paso 5 a 152
112. Configuración red *wireless* paso 5 b 153
113. Configuración de red *wireless* paso 6 154
114. SSIDs del diseño propuesto 154
115. Resumen de la información del WLC 155
116. Administración del WLC 156
117. Gráfica relación costo – beneficio 162

TABLAS

I. Técnicas de modulación en LAN inalámbrica 14
II. Requerimientos FCC en la banda U-NII 5 GHz 38
III. IEEE 802.11 Canales en la banda 2,4 GHz 40
IV. IEEE 802.11 canales en la banda 5 GHz 42
V. IEEE 802.11-1997 Tasa de rata 45
VI. IEEE 802.11b Tasa de rata 46
VII. IEEE 802.11g Tasa de rata 47
VIII. IEEE 802.11a Tasa de rata 48
IX. Comparación WPA y WPA2 99
X. Reporte del estudio de sitio 118
XI. Direccionamiento IP de las interfaces WLC 124
XII. Direccionamiento IP para la gestión de los equipos 124
XIII. Direccionamiento IP para *switch* de acceso 125
XIV. Direccionamiento IP para los *access points* 129
XV. Listado de *acccess points* 131
XVI. Datos técnicos del WLC Cisco 5508 135
XVII. Direccionamiento IP para WLC 137
XVIII. Cotización de equipos para la red inalámbrica 157
XIX. Cotización instalación de *access point* 158

XX. Cotización instalación de *switch* 2960 158
XXI. Cotización instalación de WLC 5508 159
XXII. Resumen de cotización de instalación 159
XXIII. Relación costo – beneficio 161

LISTA DE SÍMBOLOS

Símbolo	Significado
AC	Corriente alterna
DC	Corriente directa
$\boldsymbol{d}$	Letra latina d, representa la distancia
$\boldsymbol{f}$	Letra latina f, representa la frecuencia
®	Marca registrada
$\boldsymbol{r_n}$	Radio máximo de elipsoide en ecuación de Fresnel
°	Signo de grado, tipo de medida en ángulo
λ	Símbolo griego lambda, representa la longitud de onda

GLOSARIO

AD HOC	Es una red inalámbrica descentralizada.
Azimut	Es el plural de *samt*, que significa dirección. Se refiere al ángulo de la orientación sobre la superficie de una esfera real o virtual.
BASE-T	Es un subestandar de Ethernet para rede de área local, en donde se ha adoptado los conectores RJ45 y cable UTP.
Bits	Acrónimo de digito binario, es un dígito del sistema de numeración binario.
Bluetooth	Especificación industrial para red inalámbrica personal.
BYOD	Trae tu propio equipo, son los dispositivos que los clientes utilizan en una red, los cuales son propiedad de ellos.
Concéntricas	Que comparten el mismo centro, eje u origen.
Core	Parte principal de una red de telecomunicaciones, aquí se maneja toda la información de los usuarios y donde hay mayor tráfico de paquetes.

Crosstalk	Diafonía, es una perturbación entre señales de diferentes circuitos.
Dipolo	Una antena con alimentación central empleada para transmitir o recibir ondas de radiofrecuencia.
Downlink	Denominación que se le da al enlace de un equipo en donde el tráfico de datos se dirige a los dispositivos finales o cliente.
Echo request	Conocido como ping, es una utilidad diagnóstica en redes que comprueba el estado de la comunicación entre dispositivos.
Ethernet	Es un estándar de redes de área local para dispositivos. Nombre proveniente del concepto físico *ether*.
Ghz	Giga Hertz, unidad de frecuencia equivale a 1 000 000 000 hertz.
Half-duplex	Transmisión en solo una dirección en redes de telecomunicaciones.
Helicoidal	Que tiene forma de hélice.
Hertz	Unidad de frecuencia del sistema internacional de unidades.

Hostname	Nombre que se le da a un equipo dentro de una red para identificarlo.
Isotrópico	Es la característica de algunos cuerpos cuyas propiedades físicas no dependen de la dirección en que son examinadas.
KHz	Kilo Hertz, unidad de frecuencia equivale a 1 000 hertz.
LAN	Red de área local, es una red de dispositivos que abarca un área reducida.
Loop	Es un ciclo infinito en donde la información viaja sin fin dentro de la red.
MAN	Red de área metropolitana, es una red de alta velocidad que da cobertura en un área geográfica extensa.
Mbps	Mega bit por segundo, es una unidad que se usa para cuantificar un caudal de datos equivalente a 1000 kb/s.
MHz	Mega Hertz, unidad de frecuencia equivale a 1 000 000 hertz**.**
Modelo OSI	Modelo de interconexión de sistemas abiertos, es un modelo de referencia para los protocolos de la red de arquitectura en capas.

Monomodo	Es un tipo de fibra óptica utilizada en distancias largas y a velocidades altas. El núcleo es de un diámetro más pequeño en comparación con la fibra multimodo.
Monopolo	Es una partícula que tiene únicamente un polo magnético, norte o sur.
Multimodo	Es un tipo de fibra óptica mayormente utilizada en el ámbito de la comunicación en distancias cortas y velocidad entre 10Mbits/s a 10Gbit/s.
Port-channel	Grupo de interfaces de un equipo para brindar mayor capacidad y redundancia.
QoS	Calidad de servicio, es un requisito básico para poder implantar servicios interactivos como VoIP.
Rack	Es un soporte metálico destinado a alojar equipamiento electrónico, informático o de comunicaciones.
RF	Radiofrecuencia, es un término que se aplica a la porción menos energética del espectro electromagnético.
Subportadora	Es una señal separada analógica o digital, contenida en una transmisión de radio principal, que lleva información como voz o datos.

Uplink	Denominación que se le da al enlace de un equipo en donde el tráfico de datos es hacia el *core* de la red.
VoIP	Voz sobre protocolo de internet, es un conjunto de recursos que hacen posible que la señal de voz viaje a través de internet utilizando el protocolo IP.
WiFi	Es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.
WLAN	Una red de área local inalámbrica, es un Sistema de comunicación inalámbrico para minimizar las conexiones cableadas.

RESUMEN

El presente trabajo pretende mostrar el diseño para mejorar la red inalámbrica y el acceso de los estudiantes en las áreas recreativas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala. El diseño propuesto está basado en la información que se recopilo del Centro de Cálculo y la experiencia de los alumnos.

La administración y el control de los equipos de la red inalámbrica son manejados por personal de Rectoría de la Universidad de San Carlos de Guatemala, personas ajenas a la Facultad de Ingeniería, a causa de esto no se puede realizar los cambios apropiados a la red para mejorarla, que son: cambios de seguridad, potencia, creación de redes y algunas otras que son difíciles de resolver.

La propuesta que se presenta utiliza la implementación de *access points* en puntos específicos, considerados como áreas recreativas y con más demanda. El diseño que se presenta incluye una controladora inalámbrica exclusiva para la Facultad de Ingeniería, complementado el diseño con un *switch* que conecta los equipos. La minuciosa selección del equipo se basó en un estudio de necesidad y demanda de la red, así como la cantidad de usuarios, cantidad de tráfico de datos, entre otros.

Con este diseño lo que se pretende es tener el control completo de la red inalámbrica dentro de la misma Facultad de Ingeniería, específicamente colocando la controladora en el cuarto de comunicaciones del Centro del

Cálculo, para poder modificar y optimizar la señal que se le brinda a los estudiantes.

OBJETIVOS

General

Presentar la propuesta para optimizar la red IEEE 802.11 en el área de recreación de la Facultad de Ingeniería, USAC.

Específicos

1. Dar a conocer los conceptos básicos de radiofrecuencia.

2. Presentar los estándares internacionales para tecnología inalámbrica aplicables en Guatemala.

3. Dar a conocer los fundamentos de seguridad en redes inalámbricas, junto con sus mejores prácticas.

4. Presentar el diseño de la solución propuesta para la red inalámbrica de la Facultad de Ingeniería, USAC.

INTRODUCCIÓN

En la actualidad existen diversos dispositivos que ya no cuentan con puertos RJ45 para poder conectarse a internet o una red LAN, por tanto, para poder acceder es necesaria una red inalámbrica. El WiFi es una de las tecnologías inalámbricas que permite la conexión a una red LAN, resolviendo problemas de acceso a dispositivos móviles: teléfonos inteligentes, tabletas, computadoras portátiles, entre otros.

Uno de los problemas más evidentes en la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala es el servicio WiFi que se brinda a los estudiantes; presenta deficiencias cuando varios dispositivos se conectan o cuando hay gran demanda de ancho de banda, al suceder esto las personas tienen problemas de conexión, pérdida de paquetes, señal débil, porque el *access point* a donde se están conectando no soporta la cantidad de usuarios que se le está demandando o porque se está dando traslape de frecuencias, entre las varias razones varias razones por las que se pueden presentar inconvenientes.

Es importante tener un diseño para la implementación de esta tecnología, ya que al no tener un medio de comunicación para los dispositivos estos quedan aislados sin una forma gratuita de intercambiar datos, siendo una institución de educación superior es importante tener una conexión a internet estable; para tener una buena formación académica en los estudiantes.

1. CONCEPTOS BÁSICOS DE RADIOFRECUENCIA

1.1. Redes inalámbricas

Son redes donde la conexión de dispositivos se da por medio de ondas electromagnéticas, tienen un rango amplio de aplicaciones: bandas para ondas de radio, microondas, bluetooth, señal satelital, televisión satelital, entre otras.

En una red alámbrica dos equipos que necesitan comunicarse tienen que estar conectados por un cable, esto limita la movilidad y distancias ya que el cable tiene que seguir estándares Ethernet IEEE 802.3 para poder transportar los datos. Estas limitaciones son removidas en una red inalámbrica, los datos se transportan en el espacio libre y la restricción de cables ya no existe. Esto disminuye costos de cableado y conexiones físicas entre nodos.

Los datos son transportados por medio de ondas electromagnéticas, estas no viajan en línea recta, estas se expanden en todas las direcciones alejándose de la antena que irradia la señal. Las ondas electromagnéticas en una conexión inalámbrica puede ser medida y descrita por sus propiedades; las propiedades fundamentales de una onda son: frecuencia, amplitud y longitud de onda.

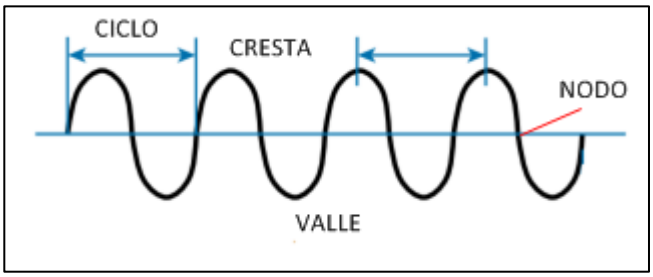
1.2. Propiedades de onda

Las principales propiedades de una onda electromagnética son las siguientes:

1.2.1. Frecuencia

Es el número de veces que la señal da un ciclo completo en un segundo. El ciclo puede empezar en la cima de la cresta, en el valle o nodo de la onda. No importa desde donde se empieza a medir el ciclo, la señal debe realizar una secuencia completa y terminar donde empezó, para empezar el patrón de nuevo.

Figura 1. **Frecuencia de onda**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 10.

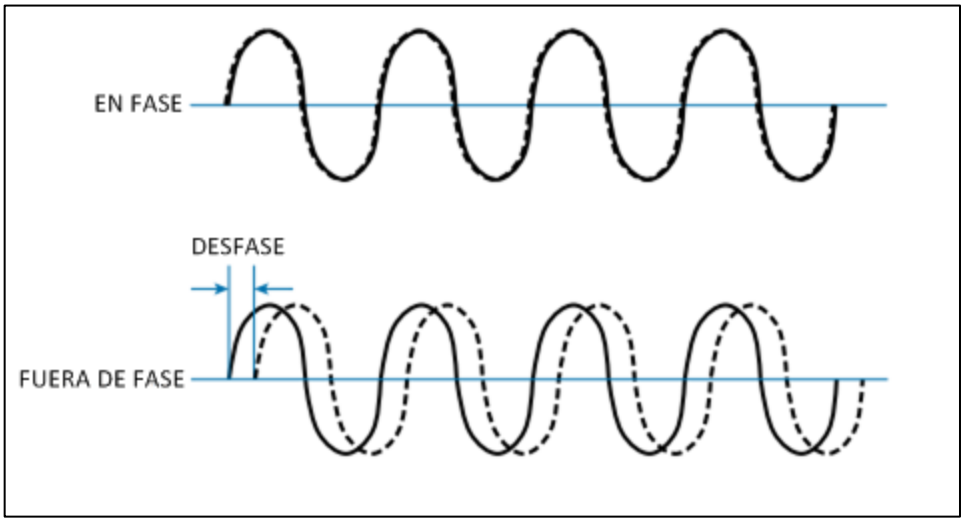
La frecuencia se mide en ciclos por segundo, es igual a un *Hertz*, es la unidad más común utilizada para medir frecuencia.

1.2.2. Fase

La fase de una señal es una medida del cambio en el tiempo; tomando como referencia el inicio de un ciclo. La fase es normalmente medida en grados, donde 0 grados es el inicio de un ciclo y un ciclo completo es igual a 360 grados.

Cuando dos señales idénticas son producidas al mismo tiempo, sus ciclos coinciden y se dice que están en fase una con otra, si una de las señales se retrasa de la otra, se dice que están fuera de fase.

Figura 2. **Fase de onda**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 14.

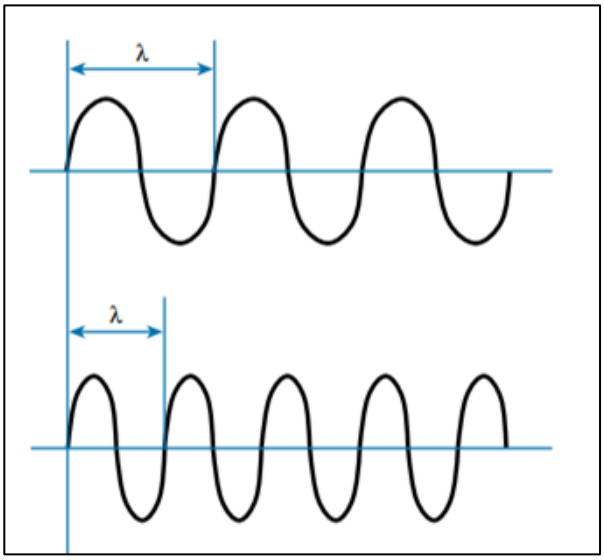
1.2.3. Longitud de onda

La longitud de onda es una medida de la distancia física, cuando la onda completa un ciclo. La longitud de onda es usualmente representada con el símbolo griego lambda (λ).

Independientemente de la frecuencia, las ondas electromagnéticas viajan a una velocidad constante en el vacío a la velocidad de la luz; en el aire, la velocidad es ligeramente menor a la velocidad de la luz. La longitud de onda es inversamente proporcional a la frecuencia, esto significa que mientras la

longitud de onda disminuye la frecuencia aumenta. La longitud de onda se vuelve importante en el diseño y distribución de las antenas.

Figura 3. **Longitud de onda**



Fuente: HUCABY, David. *CCNA Wireless 640-722.* p. 15.

1.3. Decibel

El decibelio (dB) es una función de gran ayuda, utiliza logaritmos para comparar una medida absoluta con otra. Se utilizó inicialmente para comparar niveles de intensidad de sonido, pero luego se utilizó para niveles de potencia. La siguiente ecuación se utiliza para calcular el valor en dB, donde P1 y P2 son las potencias absolutas de dos fuentes:

$$dB = 10(\log_{10} P2 - \log_{10} P1)$$

P2 es la fuente de interés y P1 es el valor de referencia. La diferencia logarítmica también se puede expresar de la siguiente manera, gracias a las propiedades de los logaritmos:

$$dB = 10 \cdot \log_{10}\left(\frac{P2}{P1}\right)$$

Para tener una idea de la escala logarítmica se tienen los siguientes casos:

- Un valor de 0 dB significa que dos valores de potencia absoluta son iguales.
- Un valor de 3 dB significa que el valor de potencia de interés es el doble del valor de referencia.
- Un valor de 10 dB significa que el valor de potencia de interés es diez veces el valor de referencia.

Para poder obtener un valor significativo para una fuente de transmisión o un receptor es importante comparar la señal con una referencia estandarizada, actualmente se utiliza dBm y dBi.

1.3.1. dBm

Se utiliza la fórmula de decibelio para obtener el valor de importancia, se coloca la potencia de interés en la parte superior, y el valor de referencia en la parte superior de la división, el valor de referencia es 1mW, por eso se le designa el nombre a la unidad dB-miliwatt.

1.3.2. dBi

Cuando se necesita conocer la potencia de una antena se utiliza a la antena isotrópica como referencia, esta antena no puede existir en realidad, porque es una antena ideal e irradia la señal en las tres dimensiones formando una esfera perfecta. Se le da el nombre de dB-*isotropic*, y es la unidad que se utiliza para medir potencias en antenas.

1.3.3. dBd

Es una unidad similar al dBi, con la diferencia que se toma un dipolo como referencia, la ganancia de la antena es medida en dB-*dipole*. La ganancia de un dipolo es de 2,14 dBi, si se desea obtener el valor en dBi solo se debe de sumar 2,14 dBi al valor.

1.4. SNR

La relación señal-ruido, se define como la proporción que existe entre la potencia de señal transmitida y la potencia del ruido que causa interferencia. Es medido en decibelios, mientras más alto es el índice de SNR, mejor será la señal recibida y se tendrá mayor posibilidad de reconstruir el mensaje enviado.

1.5. Potencia de una señal RF

En el mundo real nada es perfecto, y siempre se encuentran pérdidas en el camino de la señal hasta el receptor, para poder obtener la potencia final se debe conocer las distintas etapas de amplificación y pérdidas.

EIRP es la potencia isotrópica radiada efectiva, es la suma de la potencia del transmisor, la pérdida del cable y la ganancia de la antena. EIRP es un parámetro importante porque está regulado por agencias gubernamentales en casi todos los países, en tales casos un sistema no puede irradiar una señal que sobrepase el máximo valor EIRP permitido.

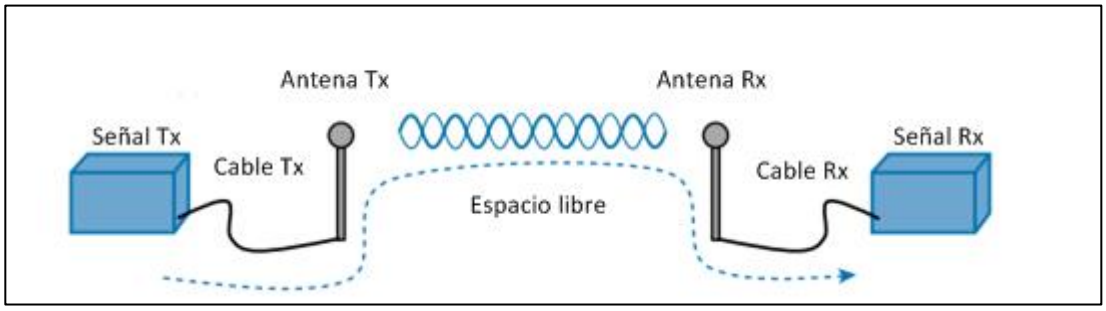
El espacio libre por donde viaja la señal, también agrega perdidas a la señal, por tanto, se debe de tomar en cuenta para obtener el valor de potencia recibido.

RSSI es el indicador de potencia de la señal recibida, utiliza dBm como unidad de medida, y debe de ser lo suficientemente alto para que los datos contenidos en la señal se puedan utilizar.

Se utiliza la siguiente ecuación para relacionar las pérdidas y potencias en un sistema de transmisión:

$$señal\ R_x = señal\ T_x - cable\ R_x + antena\ T_x - espacio\ libre + antena\ R_x - cable\ R_x$$

Figura 4. **Potencia de la señal RF sobre el camino**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 20.

1.6. Modulación

Son técnicas que se utilizan para transportar información sobre una señal portadora, por lo general se utiliza una onda sinusoidal. Se utiliza para un mejor uso de canal, aumentando la tasa de bits que se transmite en forma simultánea, además se le agrega resistencia a ruido e interferencia. El objetivo de la modulación es unir dos señales, la portadora y la señal moduladora, modificando algún parámetro de la señal portadora que varíe con respecto al valor de la señal moduladora.

La modulación se realiza en el transmisor, en el receptor el proceso se invierte, demodulando la señal para interpretar la información recibida.

Debido a las propiedades físicas de una señal RF, la modulación puede alterar los siguientes atributos:

- Frecuencia, solo se permiten variaciones ligeramente por arriba o debajo de la portadora.
- Fase.

- Amplitud.

Las técnicas de modulación requieren un ancho de banda centrada en la frecuencia de la portadora, este ancho de banda sirve en parte para la transmisión de datos y otra parte para los encabezados que se utilizan para codificar los datos y manipular la señal portadora. Si se transmite una tasa de bits baja, el ancho de banda requerido es estrecho, estas señales son llamadas transmisiones de banda estrecha.

Por otro lado, las señales en una red inalámbrica LAN deben de transmitir datos a una alta tasa de bits, requiriendo un ancho de banda más grande para la modulación, esto dio como resultado la utilización de varias frecuencias simultáneamente para transmitir los datos, esto se conoce como espectro ensanchado (*spread spectrum*).

Hay varias técnicas de modulación, entre las más conocidas y empleadas en una red WLAN están:

- Espectro ensanchado por salto de frecuencia (FHSS)
- Espectro ensanchado por secuencia directa (DSSS)
- Multiplexación por división de frecuencias ortogonales (OFDM)

1.6.1. FHSS

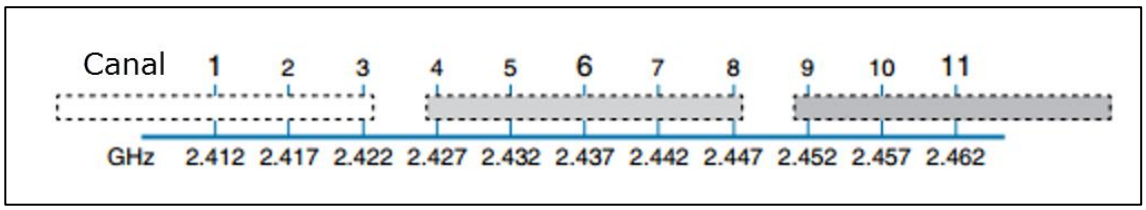
En esta técnica de modulación la señal se transmite sobre una serie de frecuencias aleatorias, cambiando de frecuencia en frecuencia sincrónicamente entre transmisor y receptor. Es una técnica utilizada muy poco actualmente, ya que las ventajas que tenía fueron destituidas por los siguientes puntos:

- Un límite de 1MHz para ancho de banda permitía solo una tasa de transmisión de 1 o 2 Mbps.
- Múltiples transmisores en la misma área podían eventualmente colisionar e interferir entre si al usar el mismo canal.

1.6.2. DSSS

Utiliza una cantidad pequeña de canales anchos, que soportan esquemas de modulación compleja y una tasa de transmisión escalable. Cada canal tiene un ancho de 22 MHz, un ancho de banda grande en comparación a la velocidad soportada de 11Mbps, pero suficiente para aumentar la tasa de transmisión esparciéndola por las frecuencias y haciendo la señal menos vulnerable a interferencias. En la banda 2,4GHz donde se utiliza DSSS existen 14 canales, pero solo 3 están libres de traslape, dejando utilizables solo 3, los canales 1, 6 y 11.

Figura 5. **Canales sin intercepción en DSSS**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 27.

Para que la señal sea aún menos susceptible al ruido e interferencias se llevan a varias funciones antes de ser modulada:

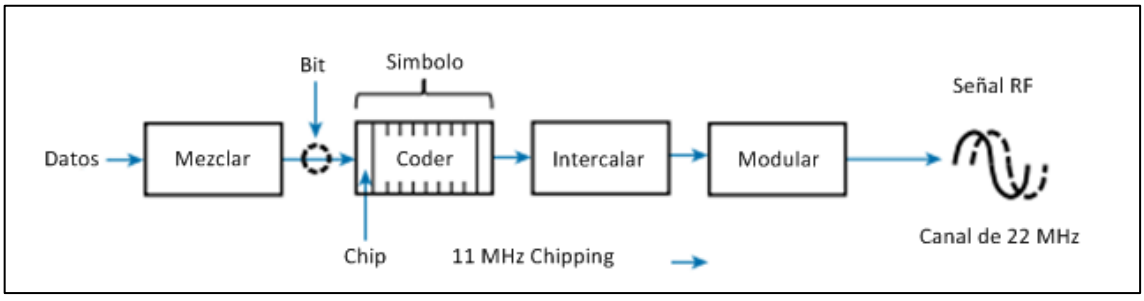
- Mezcla: los datos a enviar son mezclados de forma predeterminada para que el resultado sea una cadena aleatoria de 0 y 1.

- Codificación: cada bit es convertido a múltiples bits de información que contienen patrones, estos suministran protección contra errores por causa de ruido o interferencia. Cada bit codificado es llamado *chip*. Un grupo de *chips* representando un bit de datos es llamado símbolo. DSSS utiliza dos técnicas de codificación: secuencias *Barker* y código complementario de claves (CCK).

- Intercalación: los datos codificados son dispersados entre bloques separados, así la interferencia afecta solo un bloque, pero no todos.

- Modulación: los bits en cada símbolo son utilizados para modular la fase de la señal portadora, con esto se logra transmitir los valores binarios de los datos en la señal RF.

Figura 6. **Diagrama de bloques transmisión DSSS**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 28.

DSSS ha evolucionado y ha incrementado la tasa de transmisión que puede ser modulada, a pesar de la velocidad de transmisión DSSS siempre utiliza una tasa de *chipping* de 11 millones de *chips* por segundo.

1.6.2.1. 1Mbps DSSS

Se utiliza para minimizar los efectos por un índice bajo de SNR y evitar la pérdida de datos en una frecuencia de banda estrecha. Cada bit de los datos es codificado como una secuencia de 11 bits llamada *Barker* 11 *code* (secuencia *Barker* 11). El objetivo es agregar suficiente información adicional a cada bit para que su integridad sea preservada cuando la señal sea transmitida en un ambiente ruidoso.

Cada 11 bits es un *chip* y solo se tiene dos opciones, uno para representar un 1 y otro *chip* para representar un 0. Cada bit en el *chip Barker* se puede transmitir utilizando la modulación DBPSK, modulación diferencial binaria por desplazamiento de fase. La fase de la señal portadora es modificada de la siguiente manera:

- 0: la fase no cambia
- 1: la fase es rotada 180 grados, lo que invierte la señal

1.6.2.2. 2Mbps DSSS

Para duplicar la velocidad de transmisión se toman dos *chips* al mismo tiempo y se modulan la señal portadora utilizando DQPSK, modulación diferencial en cuadratura por desplazamiento de fase. Los dos *chips* se utilizan para modificar la portadora en cuatro formas diferentes:

- 00: la fase no cambia
- 01: la fase rota 90 grados
- 11: la fase rota 180 grados
- 10: la fase rota 270 grados

1.6.2.3. 5.5Mbps DSSS

Para mayor eficiencia se utiliza CCK código de claves complementarias, este reemplaza a la codificación *Barker*. CCK toma 4 bits de datos al mismo tiempo y le agrega información redundante para formar un símbolo de 6-*chip*. A esto se le suma dos bits para indicar la fase de modulación, da como resultado un total de 8 *chips*.

1.6.2.4. 11Mbps DSSS

La velocidad anterior de 5.5 Mbps CCK puede ser doblada ajustando la codificación. En vez de tomar 4 bits para formar un símbolo, se toman 8 bits para crear un símbolo de 8 *chips*.

1.6.3. OFDM

Multiplexación por división de frecuencias ortogonales, envía los datos en paralelo por múltiples frecuencias, todas utilizando un canal de 20 MHz. Cada canal es dividido en 64 subportadoras que están separadas 312,5KHz una de otra. Las 64 subportadoras se clasifican en según su función en:

- Guarda – 12 subportadoras son usadas para separar los canales.
- Piloto – 4 subportadoras tienen una separación igual para que se puedan sintonizar los receptores al canal.

- Datos – 48 subportadoras son utilizadas para transportar datos.

OFDM ofrece varias velocidades de transmisión utilizando varios esquemas de modulación. Como los datos son transmitidos paralelamente, la cantidad de información que es repetida puede variar para alcanzar mayores velocidades. Los nombres dados a OFDM se deben a una fracción que indican que porción son símbolos nuevos y que porción de los datos son repetidos. Utilizando codificación QPSK y QAM se obtienen las siguientes técnicas de modulación: QPSK 1/2, QPSK 3/4, 16-QAM 1/2, 16-QAM 3/4, 64-QAM 2/3, 64-QAM 3/4. En la siguiente tabla se resumen las técnicas de modulación para una red inalámbrica LAN.

Tabla I. **Técnicas de modulación en LAN inalámbrica**

Modulación	DSSS (Mbps)	OFDM (Mbps)
DBPSK	1	
DQPSK	2	
CCK4	5,5	
OFDM BPSK 1/2		6
OFDM BPSK 3/4		9
CCK 8	11	
OFDM QPSK 1/2		12
OFDM QPSK 3/4		18
OFDM 16-QAM 1/2		24
OFDM 16-QAM 3/4		36
OFDM 64-QAM 2/3		48
OFDM 64-QAM 3/4		54

Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 33.

1.7. Interferencia

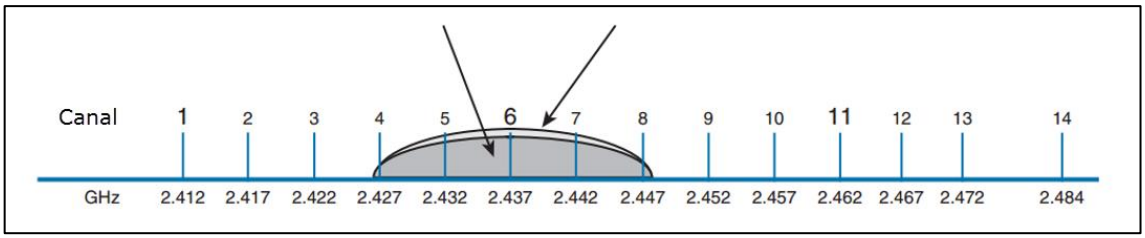
El objetivo detrás de la modulación WLAN es de compactar los datos lo más posible dentro la señal inalámbrica, y minimizar la pérdida de datos debido

a interferencias o ruido. Si se pierden datos se debe de retransmitir la información, utilizando más recursos, por eso es importante y recomendable utilizar un canal abierto y despejado.

1.7.1. Interferencia Co-Canal

Cuando la señal de un transmisor se superpone con otra señal en una frecuencia o canal, la señal interfiere con la otra. La interferencia puede ser descrita como la manera en que las señales se superponen, por ejemplo, una interferencia ocurre cuando dos señales utilizan el mismo canal, en este caso las dos señales utilizan el canal 6.

Figura 7. **Interferencia Co-Canal**



Fuente: HUCABY. David. *CCNA Wireless 640-722*. p. 70.

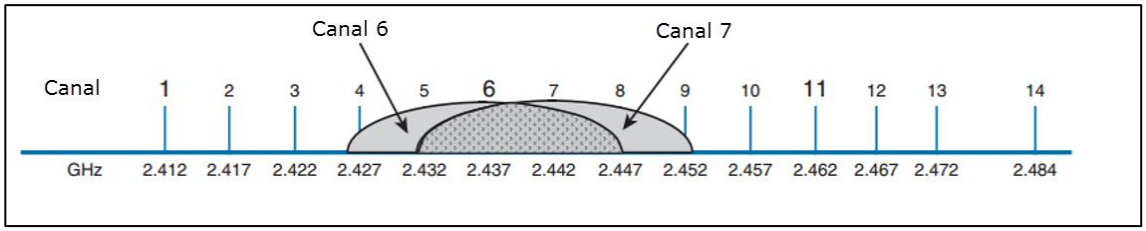
Como las dos señales están utilizando el mismo canal los 22 Mhz de ancho de banda se superpone completamente, puede no ser un problema si solo un transmisor está trabajando a la vez, sin embargo si los dos están transmitiendo el canal se pondrá muy congestionado, esto causa interferencia y pérdida de datos, esto en consecuencia hace que los datos se retransmitan utilizando más recursos y así sucesivamente.

1.7.2. Interferencia del canal vecino

Esta interferencia se da cuando los transmisores son colocados en dos diferentes canales, sin embargo, la separación entre canales no es lo suficientemente grande para evitar la superposición de señales.

Si se utilizan por ejemplo los canales 6 y 7, las señales no estarán completamente superpuestas, pero la interferencia entre las dos es lo suficiente para perjudicarse entre sí.

Figura 8. **Interferencia de canal vecino**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 71.

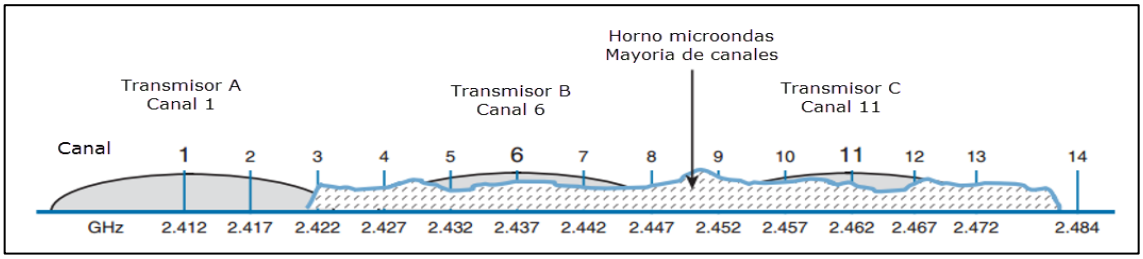
El estándar 802.11 define a los canales adyacentes como los canales que no se superponen, a diferencia de canales vecinos que si se pueden superponer y causar interferencia.

1.7.3. Interferencia no 802.11

En la práctica aparte de las señales de diferentes *Access points* también se presentan interferencias de dispositivos que no son 802.11, tales dispositivos no utilizan un canal especifico, sino que utilizan FHSS para saltar de un canal a

otro aleatoriamente, y aun peor hay dispositivos que no se acoplan a ningún esquema, utilizan todo el rango de frecuencias al mismo tiempo.

Figura 9. **Interferencia no 802.11 de un microondas**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 72.

Por ejemplo, un microonda utiliza la energía de radiofrecuencia en la banda de 2.4 GHz ISM para poder calentar la comida, debido al débil recubrimiento del microondas, las señales RF escapan e interfieren en la mayoría de los canales 802.11b/g. La transmisión del microondas es constante, esto deja inservible todos los canales.

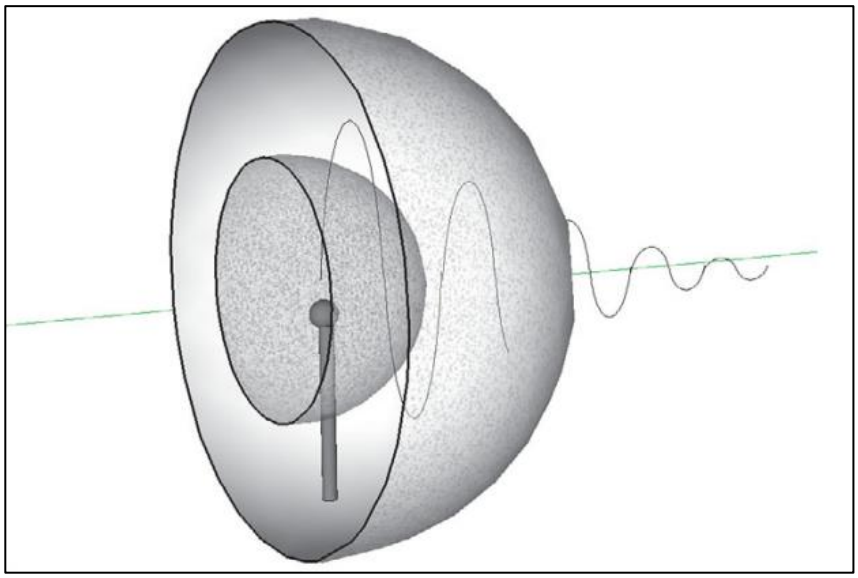
Para mitigar la interferencia de dispositivos que no sean 802.11 se debe de eliminar la fuente, se deben utilizar microondas con mejores recubrimientos, los dispositivos como teléfonos celulares, cámaras de video inalámbricas deben de ser reemplazados por otros que trabajen en bandas diferentes a la 802.11.

1.8. Pérdida en el espacio libre

Cuando una señal RF es transmitida desde una antena, su amplitud disminuye a medida que viaja en el espacio libre. Aun cuando no existen obstáculos en el camino entre en transmisor y el receptor, la señal se debilitará, esto es conocido como pérdida del espacio libre.

El principio de pérdida en el espacio se observa en la siguiente imagen, la energía transmitida por la antes es irradiada en todas las direcciones, la onda toma la forma de una esfera, a medida que la onda viaja, la espera aumenta de tamaño, por tanto, la misma cantidad de energía que sale de la antena es distribuida sobre toda la esfera en el espacio libre, la concentración de la energía se debilita a medida que la distancia hacia la antena aumenta.

Figura 10. **Pérdida en el espacio libre por dispersión en la onda**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 73.

No importa si el rayo transmitido es más direccional, ni el tipo de antena, la pérdida de energía en la señal será consistente.

La pérdida en el espacio libre puede ser calculada con la siguiente ecuación:

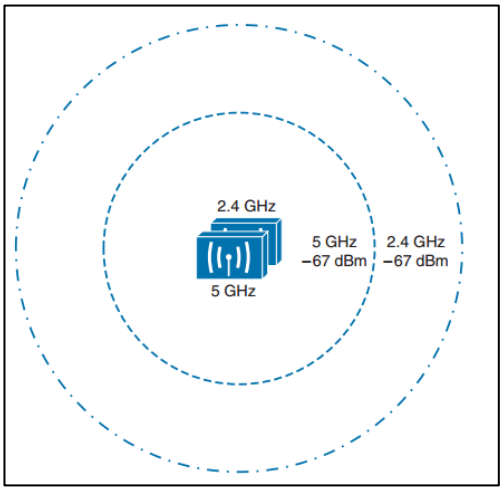
$$FSPL(dB) = 20log10(d) + 20log10(f) + 32{,}44$$

Donde

- d= distancia desde el transmisor en km.
- f= frecuencia en Mhz.
- La pérdida en el espacio libre es una función exponencial, la potencia de la señal cae drásticamente cerca de la antena, pero despacio lejos de la antena.
- La pérdida está en función de la distancia y la frecuencia.

La pérdida en la banda de 5Ghz es mayor que en la banda de 2,4Ghz, esto hace que los dispositivos que utilizan 802.11b/g/n (2,4Ghz) tienen un rango efectivo mayor que los dispositivos que utilizan 802.11a/n (5Ghz); asumiendo que están utilizando la misma potencia. En la siguiente imagen ambas antenas tienen un EIRP de 14dBm y el rango efectivo de cada una termina cuando la potencia de la señal es de -67dBm.

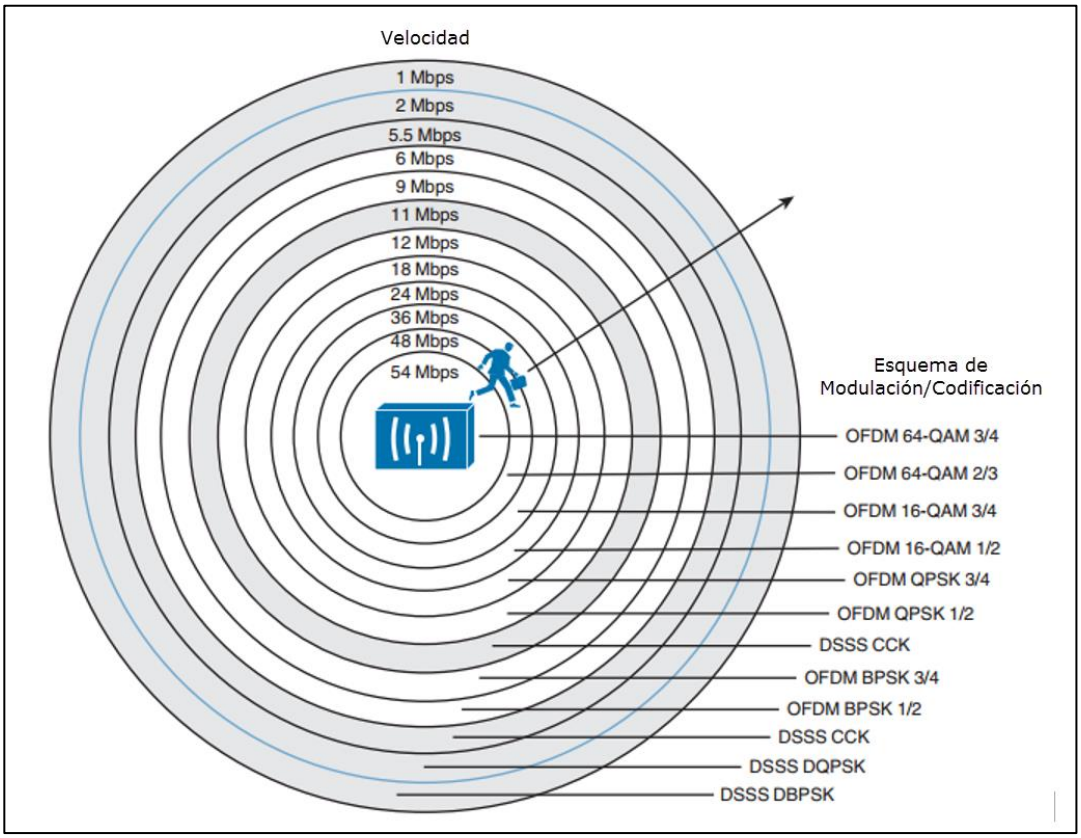
Figura 11. **Rango efectivo para transmisores de 2,4 GHz y 5 GHz**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 74.

Los dispositivos 802.11 tienen la capacidad de ajustar la modulación y esquemas de codificación basados en las condiciones de RSSI y SNR. Si las condiciones son favorables con buena calidad en la señal y alta tasa de rata, se utiliza una modulación y esquema de codificación compleja. Si las condiciones se deterioran, se utilizan esquemas menos complejos resultando en un mayor rango, pero a tasas de rata menores. Esta selección de esquemas es conocido como *dynamic rate shifting* (DSR), cambio de rata dinámico, y como su nombre lo implica, se realiza dinámico sin necesidad de que los cambios se realicen manualmente.

Figura 12. **Cambio dinámico de velocidad en función del rango**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 76.

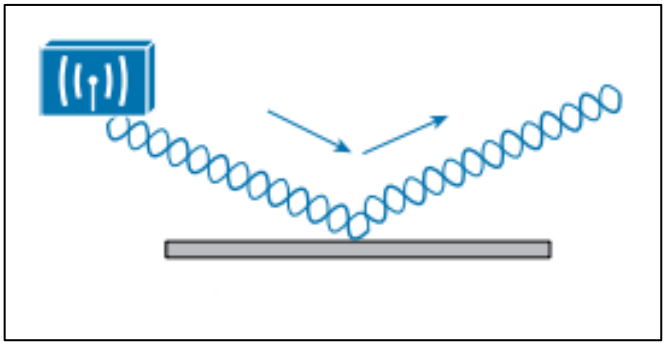
1.9. Propagación de una señal de radio frecuencia

Una señal RF viaja a través del aire como una onda electromagnética. En un mundo perfecto, la señal llegaría al receptor con la misma potencia e idéntica a como el transmisor la envió. En el mundo real esto no sucede, las condiciones y objetos en el camino afectan a la propagación de la señal, a continuación, se cubren los escenarios más comunes.

1.9.1. Reflexión

La reflexión se da cuando una señal rebota sobre un objeto y toma un camino diferente al original; esto desfasa la señal y hace que llegue ligeramente después. Esto se conoce como multi-camino. Cuando el receptor combina las dos señales, el resultado es una representación pobre de la señal original, una señal débil y distorsionada, causando que los datos se corrompan.

Figura 13. **Reflexión de una señal**

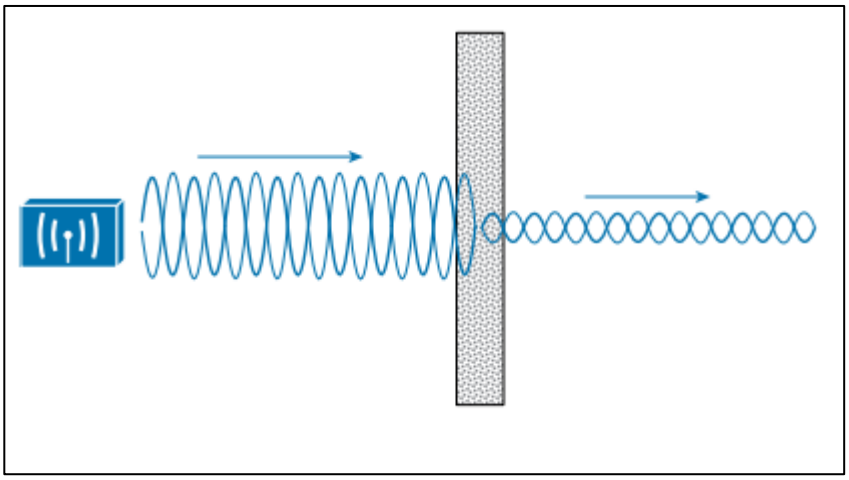


Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 77.

1.9.2. Absorción

Es el proceso en donde la onda es captada por la materia. En general todos los materiales absorben en algún rango de frecuencias, los cuerpos humanos y objetos con agua absorben la señal transmitida.

Figura 14. **Absorción de una señal**

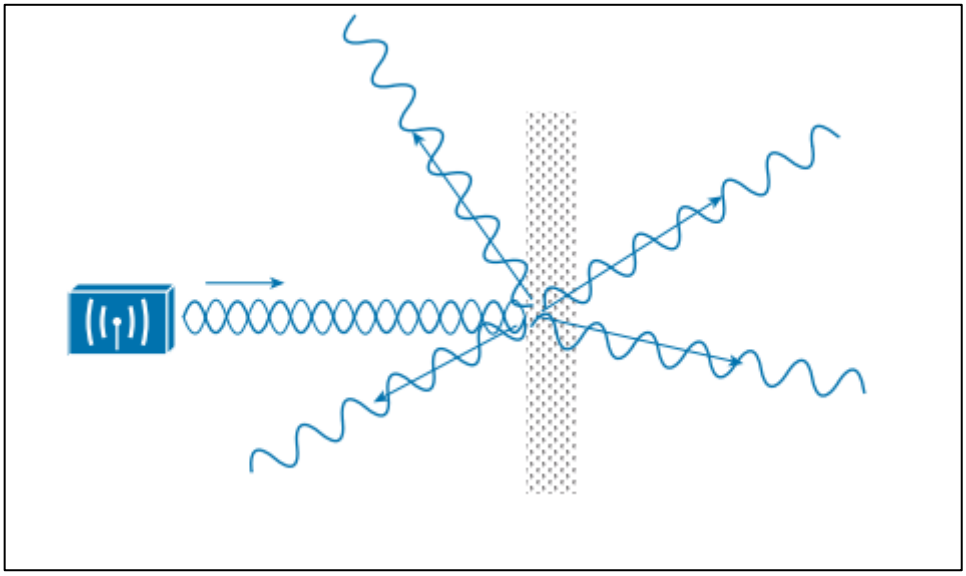


Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 78.

1.9.3. Dispersión

Ocurre cuando una señal inalámbrica pasa a través de polvo, o algún ambiente arenoso. La onda se divide en varias, y cada una toma caminos distintos. La potencia se divide en las ondas dispersadas y parte de la potencia se queda en el objeto causante de la dispersión.

Figura 15. **Dispersión de una señal**

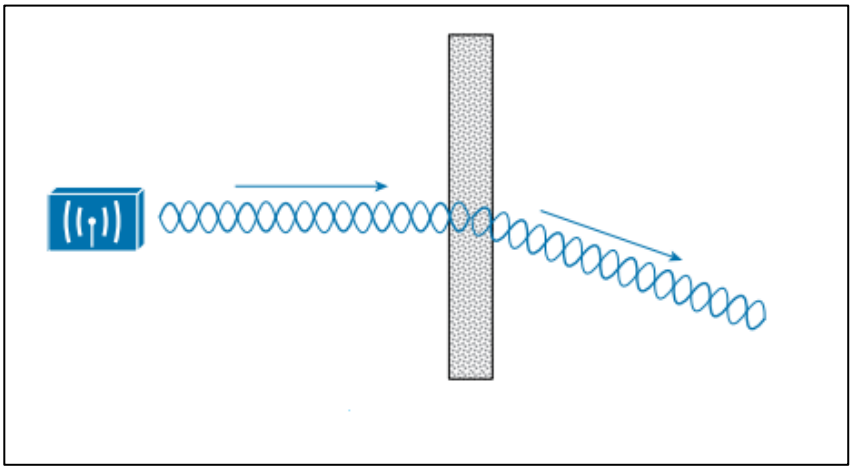


Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 79.

1.9.4. Refracción

Es el cambio de velocidad y dirección, cuando la onda pasa por materiales de índices de refracción distintos.

Figura 16. **Refracción de una señal**

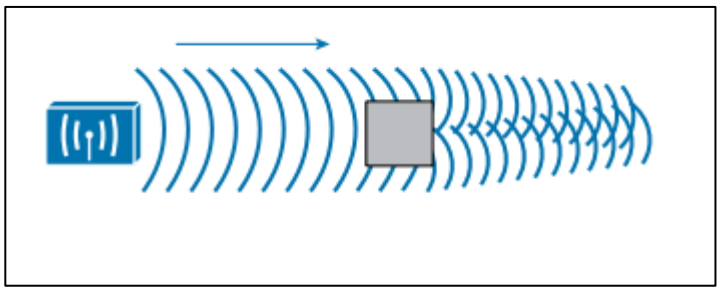


Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 79.

1.9.5. Difracción

La difracción es mejor descrita como ondas concéntricas, en vez de una señal oscilante, así describe mejor el comportamiento en el mundo real. La difracción causa que la señal se auto-regenere por si sola cuando pasa alrededor de un objeto absorbente.

Figura 17. **Difracción de una señal**



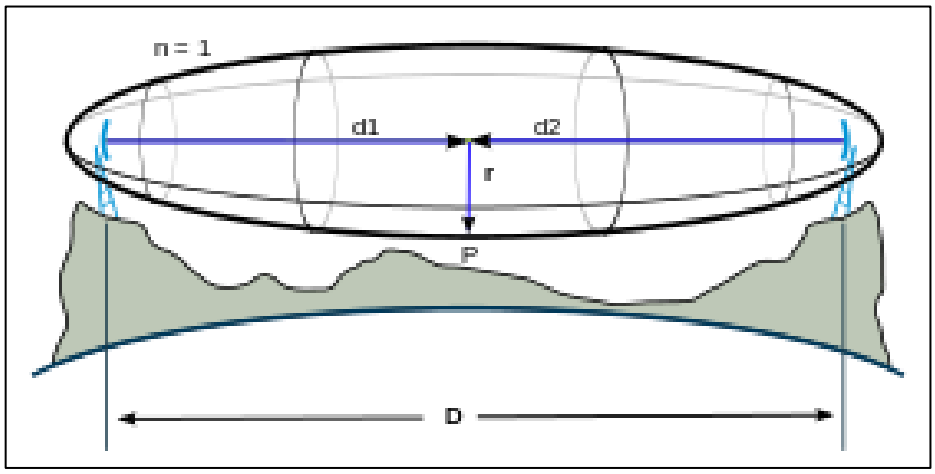
Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 80.

1.10. Zona de Fresnel

Es el volumen entre el emisor de una onda de radiofrecuencia y un receptor, tiene forma elíptica alrededor de la línea de vista entre dispositivos, este volumen tiene que estar libre de obstrucciones en el camino. Si algún objeto se encuentra dentro del volumen elíptico, parte de la señal RF se difractará y cambiara de dirección.

En realidad, existen varias zonas de Fresnel concéntricas alrededor de la línea recta del camino. La primera zona de Fresnel, o el interior, es la que más afecta a la señal si es obstruida. Otro factor interesante es que las zonas de Fresnel impares tiene un efecto destructivo en la señal, mientras que las zonas pares tienen un efecto constructivo para la potencia de la señal.

Figura 18. **Zona de Fresnel**



Fuente: *Zona de Fresnel*. https://es.wikipedia.org/wiki/Zona_de_Fresnel. Consulta: 11 de octubre de 2016.

La fórmula genérica para calcular las zonas de Fresnel es la siguiente:

$$r_n = \sqrt{\frac{n\lambda d_1 d_2}{d_1 + d_2}}$$

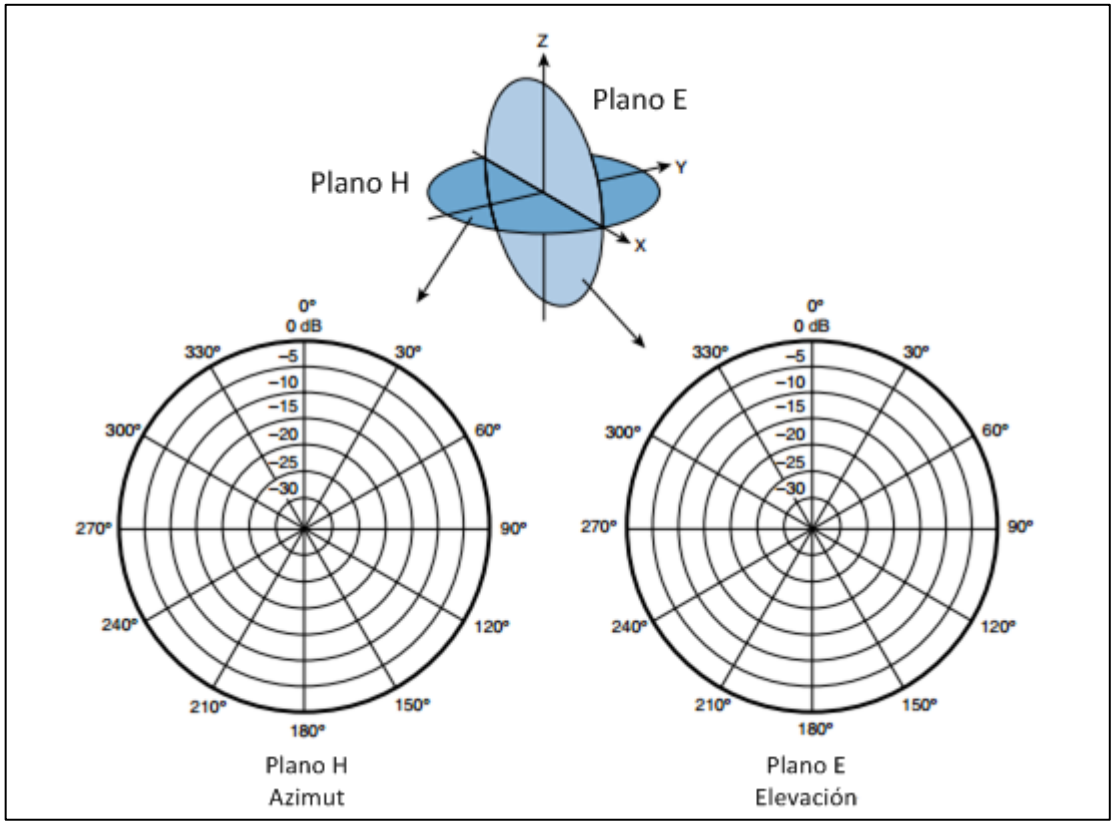
Donde

- rn= radio máximo del elipsoide en metros (n=1, 2,3…)
- d1= distancia desde el transmisor al centro de la elipse en metros
- d2= distancia desde el centro del elipsoide al receptor en metros
- λ= longitud de onda de la señal transmitida en metros

1.11. Patrones de radiación

Es una gráfica que muestra la potencia de una señal alrededor de una antena. Se utilizan dos planos para graficar los patrones de radiación, el plano H conocido como plano azimut o campo magnético, y el plano E conocido como plano de elevación o campo eléctrico. La vista que se tiene desde arriba hacia el centro de la antena es el plano H, y la vista lateral es el plano E.

Figura 19. **Patrón E y H de una antena isotrópica**



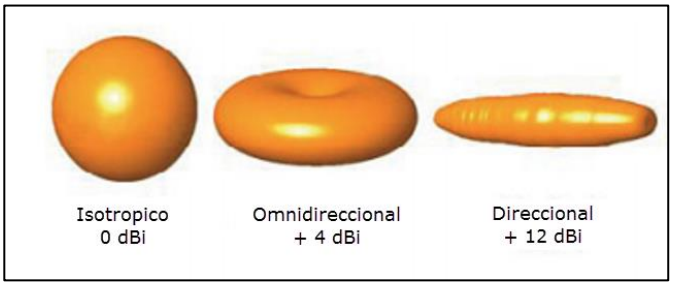
Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 90.

1.12. Ganancia

Las antenas son dispositivos pasivos, ellas no amplifican la señal transmitida si no hay circuitería o una fuente de poder externa, su trabajo se basa en amplificar o sumar ganancia a la señal dándole forma al haz de energía transmitido en el espacio libre. En breves palabras la ganancia de una antena es una medida de que tan efectivamente puede dirigir la energía RF en una determinada dirección.

La ganancia para antenas omnidireccionales es baja, debido a que estas antenas están diseñadas para cubrir un área más amplia, las antenas con ganancia alta están diseñadas para cubrir áreas determinadas.

Figura 20. **Patrones de radiación para los tres tipos básicos de antena**

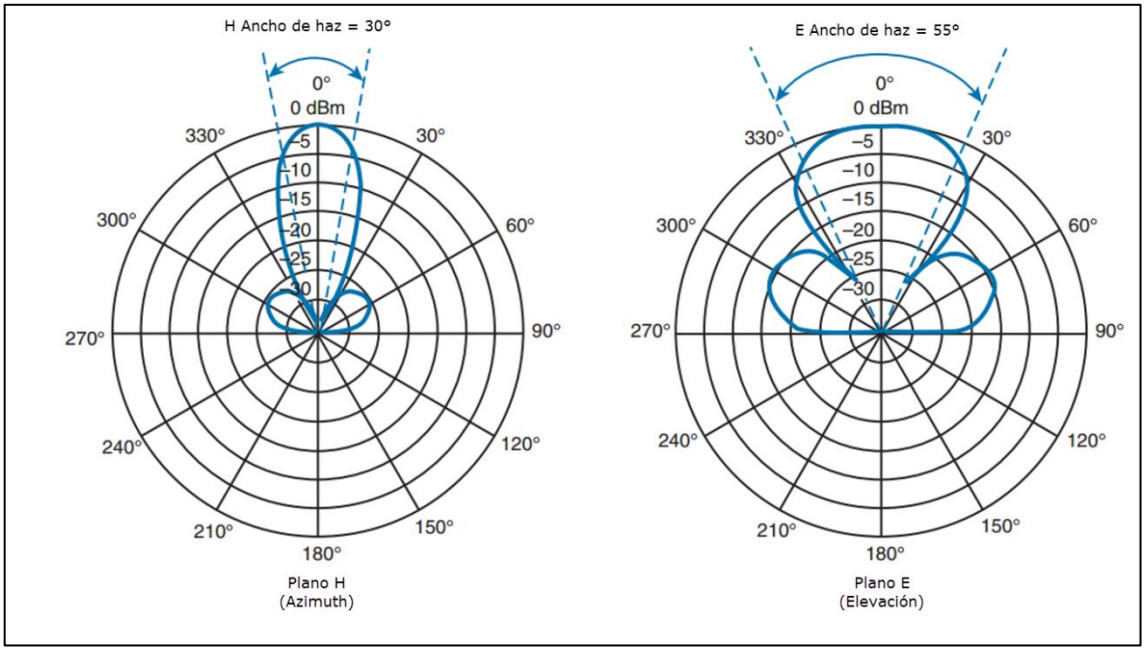


Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 91.

1.13. Ancho de haz

El ancho de haz es normalmente expresado en grados, para ambos planos E y H. El ancho de haz se determina de la siguiente manera: se toma el punto con la potencia más fuerte de la gráfica, generalmente se encuentra en la orilla; luego se sigue la gráfica hasta que la potencia disminuya 3 dB, en donde la señal tiene la mitad de potencia. Finalmente se traza una línea desde el centro de la gráfica hasta las intersecciones de -3dB, y se mide el ángulo entre ambas líneas.

Figura 21. **Ejemplo de ancho de haz**

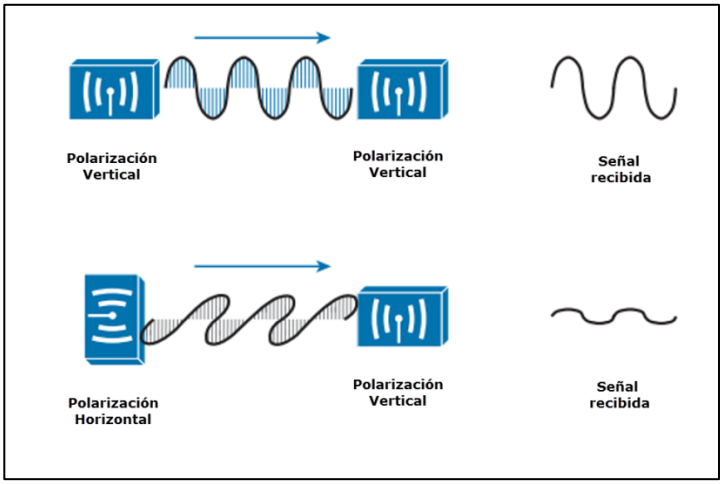


Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 92.

1.14. Polarización

Es la orientación de la onda. Hay diferentes tipos de polarización, por ejemplo: vertical, horizontal, diagonal, circular. Es muy importante utilizar la misma polarización para crear los enlaces de radio, así se asegura transmitir la señal con la mejor calidad, si se utiliza diferente polarización la señal pierde porcentaje de su potencia al ser recibida.

Figura 22. **Polarización**

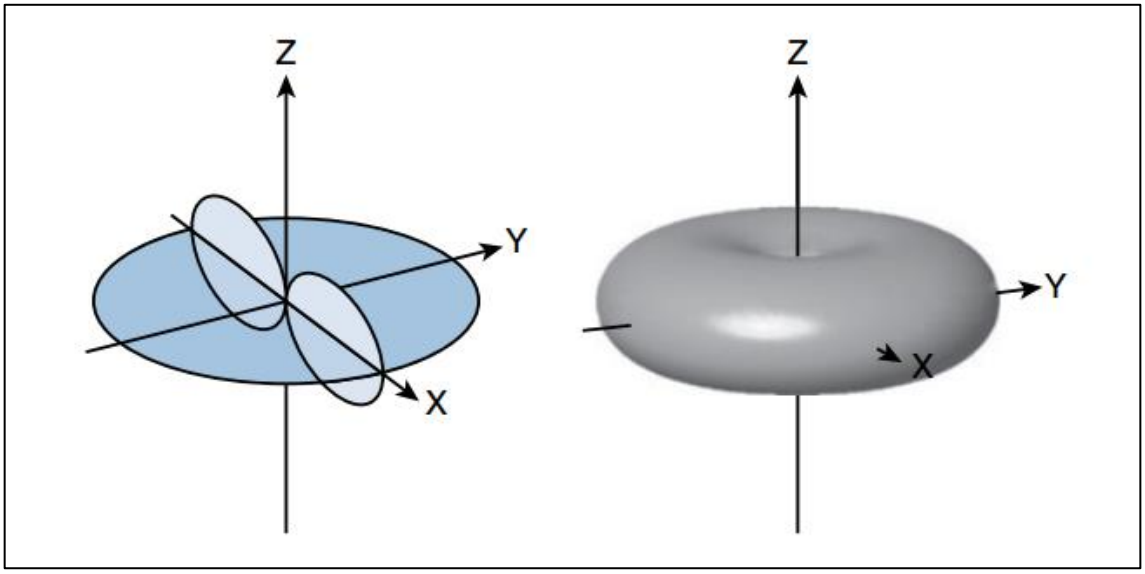


Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 93.

1.15. Antena omnidireccional

Una antena omnidireccional es comúnmente construida en forma de un cilindro delgado. La señal se propaga equitativamente en todas las direcciones desde la antena, pero no a través del eje de la antena. El volumen resultante tiene forma de dona donde que se expande más en el plano H que en el E. Este tipo de antena funciona bien para cubrir áreas amplias o lugares donde la antena se coloca en el centro. Como la antena omnidireccional distribuye la energía RF por toda el área, tiene una ganancia relativamente baja.

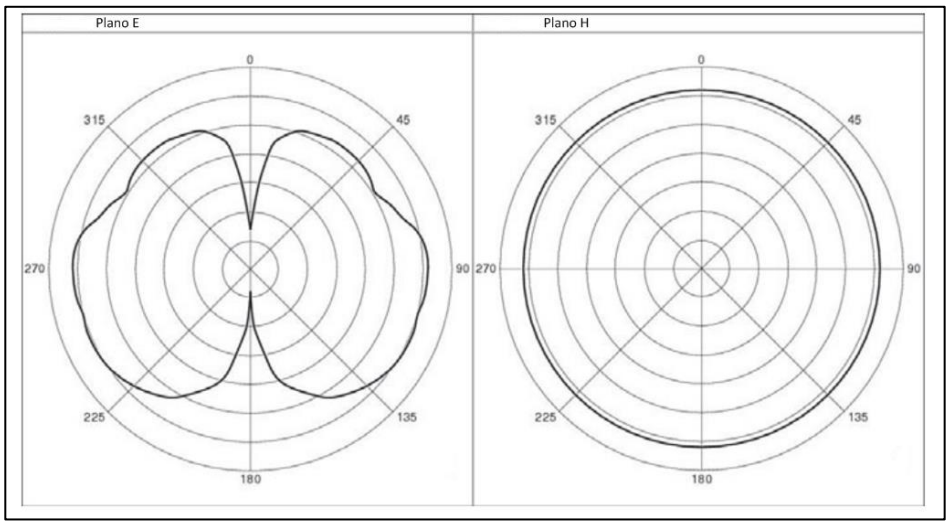
Figura 23. **Patrón de radiación en 3D de un dipolo**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 95.

Una antena omnidireccional común es el dipolo, los dipolos tienen una ganancia alrededor de +2 a +5 dBi. Algunos modelos de dipolo son articulados y se puede doblar para modificar el área que se cubre con la señal. Como su nombre los dice, el dipolo tiene dos alambres separados que irradian la señal RF cuando una corriente alterna es aplicada en ellos.

Figura 24. **Patrones de radiación en planos E y H de un dipolo**

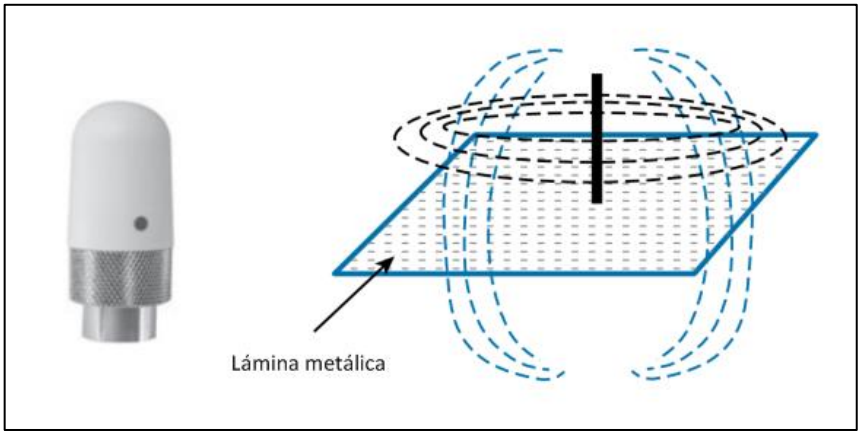


Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 95.

Los dipolos son muy utilizados en dispositivos inalámbricos LAN, se instalan en los techos de casas y pasillos, pero las antenas dipolo tiene una longitud entre 3,5 y 5,5 pulgadas, por lo tanto, no siempre es estético colocarlas. Por esta razón se utilizan antenas monopolo como sustitución.

Las antenas monopolo son bien cortas, miden menos de 2 pulgadas de longitud. Para lograr ese tamaño, solo tienen un alambre corto para irradiar la señal. Lo que se realiza para obtener un dipolo es colocar el monopolo sobre el dispositivo y la otra mitad del dipolo se convierte en la parte metálica del dispositivo. Con esto se logra un patrón de radiación similar, pero no tan simétrico. Las antenas monopolo tienen una ganancia de 2,2 dBi en las bandas de 2,4GHz y 5 GHz.

Figura 25. **Antena monopolo**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 95.

2. ESTÁNDARES INTERNACIONALES PARA TECNOLOGÍA INALÁMBRICA

2.1. Organismos regulatorios

La porción RF del espectro de frecuencias va desde los 3kHz hasta los 300GHz; las frecuencias dentro del espectro RF están disponibles porque existen en cualquier lugar, pero no sería inteligente utilizar cualquier frecuencia. Para que la comunicación inalámbrica sea posible se deben de seguir estándares en donde se establecen frecuencias en el espectro que pueden ser utilizadas: métodos de generación de señales, tipos de modulación y codificación, parámetros y características de comunicación, entre otros factores. Todo esto sin interferir con la operación de dispositivos inalámbricos de alrededor.

2.1.1. ITU-R

Es un organismo de regulación en el área de telecomunicaciones, este decide que parte del espectro de ondas de radio frecuencia es utilizado para determinado propósito, y como se debe de usar. ITU-R, el Sector de Radiocomunicaciones ITU (International Telecommunication Union Radiocommunication Sector), mantiene el espectro y frecuencias asignados a tres regiones:

- Región 1: Europa, África y Norte de Asia
- Región 2: Norte y Sur América
- Región 3: Sur de Asia y Australia

Además de que ITU-R hace disponible el espectro en todos los países, ITU-R también hace todo lo posible para que las señales RF de un país no interfieran con las de otro. Incluso ITU-R monitorea el curso de los satélites de orbitas geoestacionarias y sus frecuencias para que los de un país no interfieran con los de otros.

La mayoría de bandas en el espectro RF son reguladas, necesitando una licencia de un organismo regulatorio para poder utilizarlas. Las bandas licenciadas son restrictivas por una buena razón, mantiene la interferencia a lo mínimo, debido a que mantiene las frecuencias solo para: transmisores aprobados, propósitos y ubicaciones determinadas. Para poder utilizar una banda licenciada, se debe de enviar una solicitud a un organismo regulatorio que administre las frecuencias en ese país, esperando por su aprobación y respetando cualquier restricción que pueda ser aplicada.

Al contrario de las bandas licenciadas, ITU-R tiene rangos de frecuencias libres específicamente para aplicaciones industriales, científicas, y médicas (ISM). Existen otras bandas ISM pero solo dos aplican para LANs inalámbricas:

- 2,400 a 2,500GHz
- 5,725 a 5,825GHz

Los propósitos de estas bandas son libres y accesibles para cualquiera que quiera utilizarlas, en otras palabras, las bandas ISM se pueden utilizar sin licencia y no se necesitan permisos o registros para utilizarlas. La desventaja es que al ser libre hay más interferencia en estas frecuencias.

Todas las bandas de frecuencias utilizadas para LAN inalámbricas son sin licencia. Se puede adquirir un dispositivo LAN inalámbrico y utilizarlo

inmediatamente, siguiendo las reglas de la agencia regulatoria que gobierna RF en el país, estas reglas por lo general son que se debe irradiar la señal dentro de un rango de frecuencias establecido y la limitación de la máxima potencia irradiada.

2.1.2. FCC

En los Estados Unidos y muchos otros países de América, la Comisión Federal de Comunicaciones FCC, regula las frecuencias, canales y potencia permitida. Además de regular las frecuencias permitidas, 2,4GHz y 5 GHz para la LAN inalámbrica, establece los tipos de conectores en antenas y la potencia irradiada máxima (EIRP) para enlaces de punto a punto o de punto a múltiples puntos. La página oficial de FCC es http://www.fcc.gov.

En adición a las bandas ISM de 2,4-2,5GHz establecidas por ITU-R, FCC ha asignado la Unlicensed National Information Infraestructure (U-NII) espacio de frecuencia en la banda de 5 GHz para uso de LAN inalámbrica. U-NII son cuatro sub-bandas separadas:

U-NII-1 (Banda 1)	5,15 a 5,25 GHz
U-NII-2 (Banda 2)	5,25 a 5,35 GHz
U-NII-2 Extendida (Banda 3)	5,47 a 5,725 GHz
U-NII-3 (Banda 4)	5,725 a 5,825 GHz (ISM)

Los transmisores en la banda 2,4 Ghz pueden ser utilizados dentro de instalaciones como fuera. La potencia emitida por el transmisor está limitada a 30dBm y el EIRP a 36dBm. Se asume una antena de +6 dBi. Sin embargo, hay flexibilidad en estos límites siguiendo las siguientes dos reglas:

- Enlaces punto a multipunto: donde la señal transmitida se propaga en todas las direcciones, se pueden hacer ajustes siguiendo la regla 1:1.Por cada dBm que se remueva del transmisor, se puede sumar un dBi a la ganancia de la antena, siempre y cuando el EIRP no sea mayor a 36 dBm.

- Enlaces punto a punto: donde la señal transmitida es propagada en una dirección en general, se pueden hacer ajustes siguiendo la regla *3:1.* Por cada dBm que se remueva del transmisor, se puede sumar 3 dBi a la ganancia de la antena. El EIRP puede exceder los 36 dBm, pero no puede ser mayor que 56 dBm.

Los transmisores en la banda 5 GHz tienen que seguir los límites de FCC de la siguiente tabla. En cada una de las bandas U-NII se pueden hacer ajustes con la regla 1:1.

Tabla II. **Requerimientos FCC en la banda U-NII 5 GHz**

Banda	**Uso permitido**	**Transmisión max.**	**EIRP max.**
U-NII-1	Solo interior	17 dBm (50 mW)	23 dBm
U-NII-2	Interior o exterior	24 dBm (250 mW)	30 dBm
U-NII-2 Extendida	Interior o exterior	24 dBm (250 mW)	30 dBm
U-NII-3	Interior o exterior	30 dBm (1 W)	36 dBm

Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 44.

2.1.3. ETSI

En Europa y otros países, el Instituto Europeo de Estándares de Telecomunicaciones, ETSI; http://www.etsi.org, es el encargado de la regulación de radios en transmisores. Así como FCC, ETSI permite a LAN

inalámbrica la utilización de las bandas ISM 2.4GHz y la mayoría de las bandas U-NII 5Ghz, la excepción es la banda U-NII-3 que es licenciada y no se puede utilizar.

2.2. Organismo de normalización IEEE

Se necesitan parámetros y estándares para poder utilizar un enlace inalámbrico como medio de transmisión, las rede LAN inalámbricas por lo general están formadas por más de un transmisor y un receptor, normalmente varios dispositivos son los que necesitan utilizar el tiempo de aire en una frecuencia. El instituto de Ingenieros eléctricos y electrónicos, IEEE; http://ieee.org, es el encargado de los estándares en la industria utilizados para las rede LAN inalámbricas, entre muchos otros.

Los estándares IEEE 802 se encargan de las reden LAN y MAN, principalmente en la capa física y enlace de datos del modelo OSI, también con el transporte de tamaño variado a través de un medio en la red; en la parte dedicada a las redes LAN inalámbricas, los estándares 802 se concentran en como el medio RF, capa 1 OSI, es compartido por los dispositivos en la red y en cómo se envía y reciben los datos, capa 2 OSI.

Para desarrollar los estándares, la organización IEEE trabaja en grupos, a cada grupo se le asigna un número que está asociado con la familia 802, al grupo encargado de los estándares LAN inalámbricos se les asignó el 802.11. Cada vez que hay una actualización en el estándar se asigna una letra del alfabeto y se coloca como sufijo, así como van introduciendo actualizaciones los nombres de las mismas son 802.11a, 802.11b, 802.11c, y así consecutivamente. Si hay demasiadas actualizaciones hasta alcanzar la letra z, la siguiente actualización se le asignan dos letras como sufijo, comenzando con

la letra a y seguida por la letra a hasta la z. Hasta el momento el grupo 802.11 tiene asignadas las actualizaciones 802.11aa hasta la 802.11aq. Las actualizaciones también se pueden encontrar con la referencia del año en que fueron introducidas, por ejemplo, el estándar original 802.11 fue creado en 1997, y es conocido como 802.11-1997.

Luego de que los estándares son desarrollados pasan por una etapa de aprobación y finalmente son publicados y aplicados a los dispositivos LAN inalámbricos.

2.3. Canales utilizados en 802.11

Los dispositivos inalámbricos, trabajan en base a los estándares 802.11 para poder utilizar el espectro RF, a medida que los dispositivos se mueven deben de ser capaces de detectar y conectarse a las redes inalámbricas a medida que estas estén disponibles, a continuación, se describen los canales 802.11 utilizados en las bandas 2.4 y 5 GHz.

2.3.1. Canales en la banda ISM 2.4GHz

En la banda ISM 2,4 GHz el espacio de frecuencias está dividido en 14 canales, enumerados desde el 1 hasta el 14. A excepción del canal 14, los canales están espaciados 5 MHz:

Tabla III. **IEEE 802.11 Canales en la banda 2,4 GHz**

Canal	Frecuencia (GHz)
1	2.412
2	2.417
3	2.422

Continuación de la tabla III.

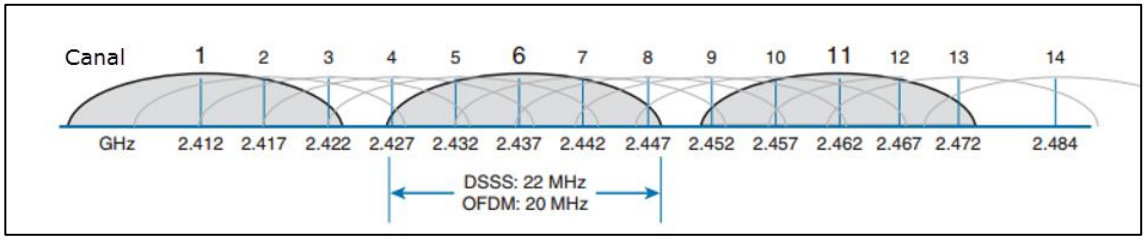
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462
12	2.467
13	2.472
14	2.484

Fuente: elaboración propia.

El estándar 802.11 permite la utilización de DSSS o OFDM en la banda 2,4 GHz, DSSS utiliza 22 MHz de ancho de banda y OFDM utiliza 20 MHz, siendo cualquiera que se utilice, solo hay 5 MHz de ancho de banda entre canales, las transmisiones de los canales vecino se traslapan e interfieren entre si. Aunque la banda este dividida en 14 canales, no todos son utilizables en los países. FCC limita la utilización de los canales 1 hasta el 11.

En la siguiente imagen se observa la superposición de los canales, la única manera de evitar la interferencia es mantener un canal de separación, el arreglo más común es la utilización de los canales 1, 6 y 11, los cuales no se superponen entre sí.

Figura 26. **Canales en la banda 2,4 GHz**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 49.

2.3.2. Canales en las bandas U-NII 5-GHz

Cada subbanda de la frecuencia 5GHz está dividida en canales que tiene una separación de 20MHz.

Tabla IV. **IEEE 802.11 canales en la banda 5 GHz**

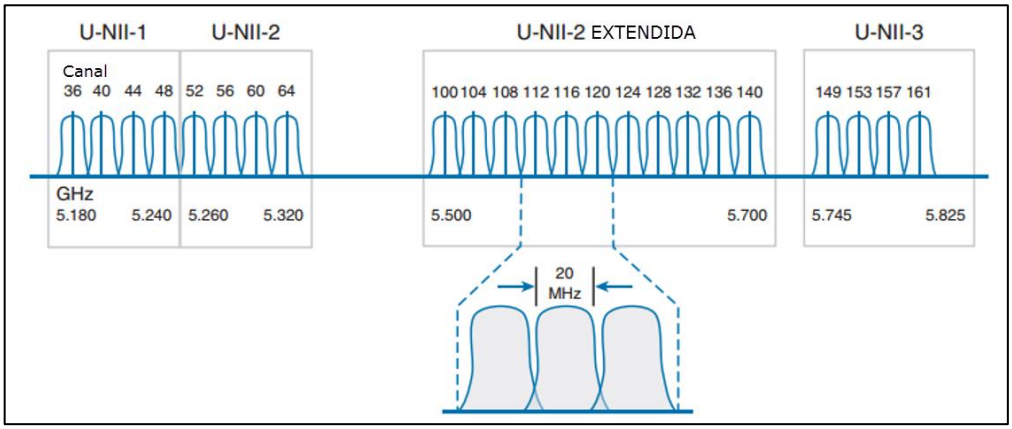
Banda	**Canal**	**Frecuencia (GHz)**
U-NII-1	36	5.180
	40	5.200
	44	5.220
	48	5.240
U-NII-2	52	5.260
	56	5.280
	60	5.300
	64	5.320
U-NII-2 Extendida	100	5.500
	104	5.520
	108	5.540
	112	5.560
	116	5.580
	120	5.600
	124	5.620
	128	5.640
	132	5.660
	136	5.680
	140	5.700

Continuación de la tabla IV.

U-NII-3	149	5.745
	153	5.765
	157	5.785
	161	5.805

Fuente: elaboración propia.

Figura 27. **Canales de las bandas U-NII 5 GHz**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 51.

Los estándares 802.11 permiten la utilización de solo modulación y esquemas de codificación OFDM en las bandas U-NII. OFDM utiliza canales de 20 MHz, lo cual encaja perfectamente con el espacio de 20MHz de las bandas U-NII, lo cual permite la utilización de bandas vecinas sin que se superpongan e interfieran.

Con todas las bandas U-NII, se tiene un total de 23 canales sin superposición disponibles, a diferencia de los 3 canales de la banda 2,4GHz. Con 23 canales disponibles se tiene mayor flexibilidad en un ambiente saturado, y aumenta el desempeño de las redes LAN inalámbricas.

2.4. Estándares IEEE 802.11

Este estándar define el uso de los niveles más bajos de la capa OSI, la capa física y la capa de enlace, especificando normas de funcionamiento para una red inalámbrica LAN. El estándar 802.1 unifica la modulación, codificación, bandas, canales y tasas de rata para brindar un medio de comunicación robusto.

Los conceptos generales que se discuten y estandarizan son los siguientes:

- Estaciones: dispositivos con interfaces de red inalámbricas.
- Medio: Las frecuencias utilizadas para la transmisión de datos.
- *Access point* (punto de acceso, AP): son los dispositivos cuya función es unir la red cableada con la red inalámbrica, intercambiando los paquetes Ethernet a la red inalámbrica y viceversa.
- Sistema de distribución: es la parte de la red cableada a donde se conecta la solución inalámbrica, esta proporciona interconexión entre AP y el *core* del sistema.
- Conjunto de servicio básico (BSS): es el grupo de estaciones que se intercomunican, existen dos tipos:
    - Independientes: las estaciones trabajan por si solas, sin ningún dispositivo que las controle.

- Infraestructura: cuando las estaciones se comunican a través de un dispositivo centralizado, un controlador.

- Conjunto de servicio extendido (ESS): es la expansión de grupo de estaciones, donde se unen varios BSS.

- Área de servicio básico (ABS): es la región que abarca la señal de una red 802.11, indica el espacio que un dispositivo tiene para movilizarse.

- Límites de la red: traslapes de frecuencias, co-canal, canales vecinos.

Existen varias versiones del estándar 802.11, ya que este ha evolucionado y se ha publicado varias modificaciones, ya sea por velocidad, modulación, métodos de seguridad entre otros, a continuación, las versiones del estándar 802.11.

2.4.1. 802.11-1997

El estándar original fue publicado en 1997, utiliza FHSS y DSSS, especifica dos velocidades de transmisión de 1 y 2 Mbps. Se utiliza el protocolo CSMA/CD, múltiple acceso por detección de portadora evitando colisiones, como método de acceso.

Tabla V. **IEEE 802.11-1997 Tasa de rata**

Banda	**Tipo de transmisión**	**Modulación**	**Tasa de rata**
2.4 GHz	FHSS	--	1.2 Mbps
	DHSS	DBPSK	1 Mbps
		DQPSK	2 Mbps

Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 52.

2.4.2. 802.11b

Es una modificación de la norma IEEE 802.11 introducida en 1999 que mejora la tasa de transferencia hasta los 11 Mbps usando codificación CCK en la banda de 2,4 GHz. 802.11b está basado en DSS y se encuentra en la banda 2,4 GHz, es compatible con el estándar original 802.11, los dispositivos pueden seleccionar entre 1, 2, 5,5 y 11 Mbps simplemente cambiando la modulación y esquema de codificación.

Tabla VI. **IEEE 802.11b Tasa de rata**

Banda	**Tipo de transmisión**	**Modulación**	**Tasa de rata**
2.4 GHz	DSSS	CCK	5.5 Mbps
			11 Mbps

Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 52.

2.4.3. 802.11g

Introducido en el 2003, también llamado velocidad extendida PHY (ERP) o ERP-OFDM. Es una corrección del estándar original, donde se obtiene un rendimiento de hasta 54 Mbps, utilizando OFDM en la banda de frecuencias de 2,4 GHz al igual que 802.11b, en donde solo hay 3 canales libres de intercepción. Utiliza modulación OFDM para lograr velocidad de transmisión alta, y la potencia máxima permitida es de 15 dBm, en vez de 20 dBm que es el límite al utilizar DSSS.

Tabla VII. **IEEE 802.11g Tasa de rata**

Banda	**Tipo de transmisión**	**Modulación**	**Tasa de rata**
2.4 GHz	ERP-OFDM	BPSK 1/2	6 Mbps
		BPSK 3/4	9 Mbps
		QPSK 1/2	12 Mbps
		QPSK 3/4	18 Mbps
		16-QAM 1/2	24 Mbps
		16-QAM 3/4	36 Mbps
		64-QAM 2/3	48 Mbps
		64-QAM 3/4	54 Mbps

Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 53.

Seleccionando ocho diferentes tipos de modulación, los dispositivos inalámbricos son capaces de elegir tasas de rata de 6, 9, 12, 18, 24, 36, 48 o 54 Mbps, la tasa más alta se puede utilizar cuando la señal y la relación SNR son óptimas.

802.11g ofrece una tasa de rata mayor a 802.11b, sin embargo, no es posible utilizar solo 802.11g cuando hay dispositivos que solo son capaces de utilizar 802.11b, ya que estos dos estándares utilizan diferente transmisión, OFDM contra DSSS, por lo tanto los dispositivos no son capaces de comunicarse directamente. 802.11g fue diseñado para ser compatible con su predecesor 802.11b, los dispositivos 802.11g son capaces de utilizar DSSS para comunicarse con los demás. Para que esto ocurra 802.11g ofrece un mecanismo de protección, la idea se basa en que cada transmisión 802.11g OFDM sea precedida por una bandera DSSS que los dispositivos 802.11b sean capaces de entender y así saber que un dispositivo 802.11g está a punto de enviar tráfico.

2.4.4. 802.11ª

Revisión publicada en 1999, opera en la banda de 5GHz y utiliza solamente modulación OFDM alcanzando una velocidad de 54 Mbps, fue diseñada para trabajar en las bandas U-NII (Unlicensed National Information Infraestructure), superando la limitación de 802.11b y 802.11g que trabajan en la banda 2.4GHz con solo 3 canales sin interferencia.

Tabla VIII. **IEEE 802.11a Tasa de rata**

Banda	**Tipo de transmisión**	**Modulación**	**Tasa de rata**
5 GHz	OFDM	BPSK 1/2	6 Mbps
		BPSK 3/4	9 Mbps
		QPSK 1/2	12 Mbps
		QPSK 3/4	18 Mbps
		16-QAM 1/2	24 Mbps
		16-QAM 3/4	36 Mbps
		64-QAM 2/3	48 Mbps
		64-QAM 3/4	54 Mbps

Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 55.

802.11a no fue diseñado para ser compatible con nada anterior, por lo tanto, no es necesario soportar velocidades menores a 6Mbps o de soportar DSSS. Los dispositivos inalámbricos pueden seleccionar entre 8 esquemas de modulación para soportar velocidades de 6, 9, 12, 18, 24, 36, 48 o 54 Mbps.

802.11a utiliza solamente OFDM el cual utiliza 20MHz de ancho de banda, lo cual encaja con las bandas U-NII que están espaciadas 20MHz entre canales, sin embargo, aún se superpone una cantidad pequeña de la señal, por tal causa 802.11a recomienda que los transmisores utilicen bandas con un canal de separación.

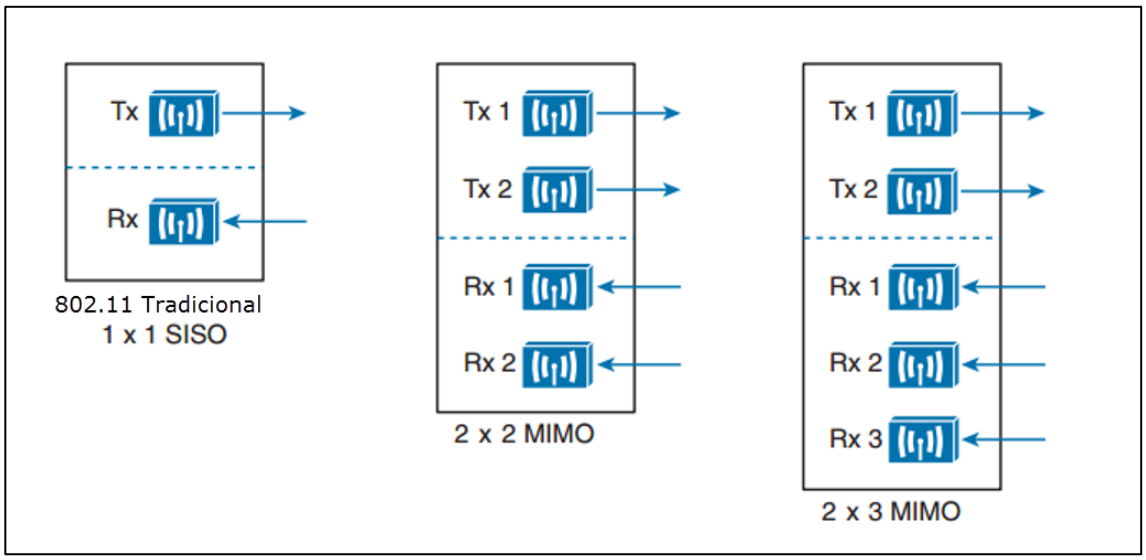
2.4.5. 802.11n

Revisión del año 2009, se caracteriza porque comenzó a utilizar múltiples antenas para incrementar las tasas de transmisión, hasta 600 Mbps utilizando canales de 40 MHz. Entre sus características nuevas están: el uso de arquitectura MIMO (*Multiple Input Multiple Output*), agregación de canales, mejoras de seguridad, formación del rayo transmisor (TxBF), entre otras.

Puede trabajar en las bandas de frecuencia de 2,4 GHz o 5 GHz, y es compatible con las versiones anteriores 802.11b, 802.11g y 802.11a.

Antes de 802.11n, los dispositivos inalámbricos utilizaban un transmisor y un receptor, creando solo un radio enlace o cadena de radio, conocido como un sistema SISO (single-in, single-out). 802.11n crea múltiples cadenas de radio utilizando varios transmisores y receptores, convirtiéndose en un sistema MIMO (multiple-in, multiple-out). Los dispositivos 802.11n se caracterizan por la cantidad de cadenas de radio disponible. Una cadena de radio es la unión de una antena transmisora y una receptora, esto es descrito de la forma TxR, donde T es el número de transmisores y R es el número de receptores. 802.11n requiere por lo menos dos cadenas de radio (2x2) y un máximo de cuatro (4x4).

Figura 28. **Ejemplos de dispositivos SISO y MIMO**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 56.

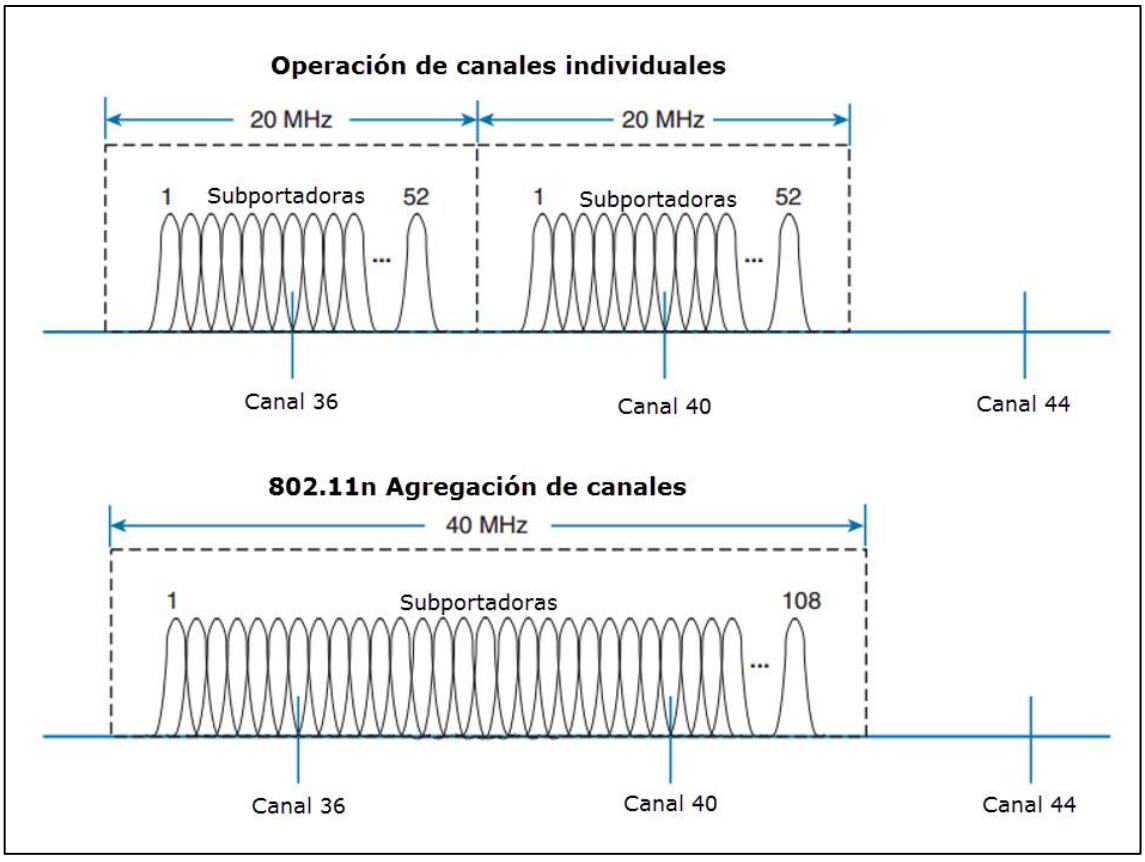
2.4.5.1. Agregación de canal

Normalmente los dispositivos 802.11a o 802.11g; tienen solo un transmisor y un receptor trabajando en un canal de 20MHz, el transmisor y receptor pueden ser configurados para operar en un diferente canal, pero solo uno a la vez. Cada canal OFDM de 20MHz contiene 48 subportadoras que transportan datos paralelamente.

802.11n aumenta la capacidad del canal de 20MHz aumentando el número de subportadoras a 52. Además 802.11n introdujo radios que pueden operar en canales de 20MHz o de 40MHz, aumentando el ancho a 40MHz duplica también la capacidad de transmisión.

Los canales agregados tienen que ser canales adyacentes de 20MHz. Cuando dos canales de 20MHz son unidos, queda un espacio remanente superior e inferior, pero el espacio entre los dos canales de 20MHz se utiliza para subportadoras adicionales, llegando a un total de 108, mientras más subportadoras se utilicen, más datos se pueden transmitir.

Figura 29. **Comparación entre canales de 20 MHz y 40 MHz**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 57.

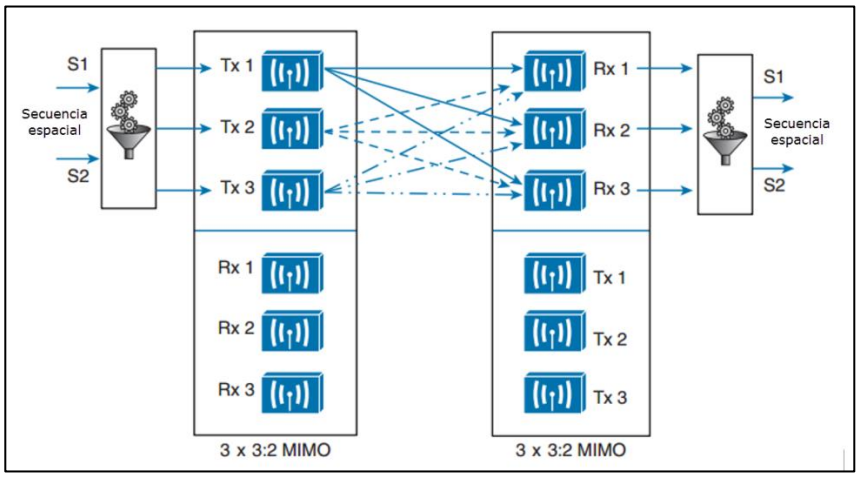
2.4.5.2. Multiplexación espacial

Los dispositivos 802.11n contienen múltiples cadenas de radio para utilizar, para aumentar la velocidad de transmisión, los datos son multiplexados o distribuidos a través de dos o más cadenas de radios, todas operando en el mismo canal, pero separadas por la diversidad de espacio.

La multiplexación espacial necesita un buen procesador de señales digitales en transmisor y receptor, esto compensa el aumento de tráfico a través del canal, mientras más líneas disponibles, más datos que pueden ser enviados en el canal.

El número de líneas multiplexadas que un dispositivo puede soportar; se define añadiendo un punto y coma y un número a la especificación MIMO del radio. Por ejemplo un dispositivo 3x3:2 MIMO tiene 3 transmisores, 3 receptores y soporta dos líneas multiplexadas.

Figura 30. **Multiplexación entre dos dispositivos MIMO 3x3:2**



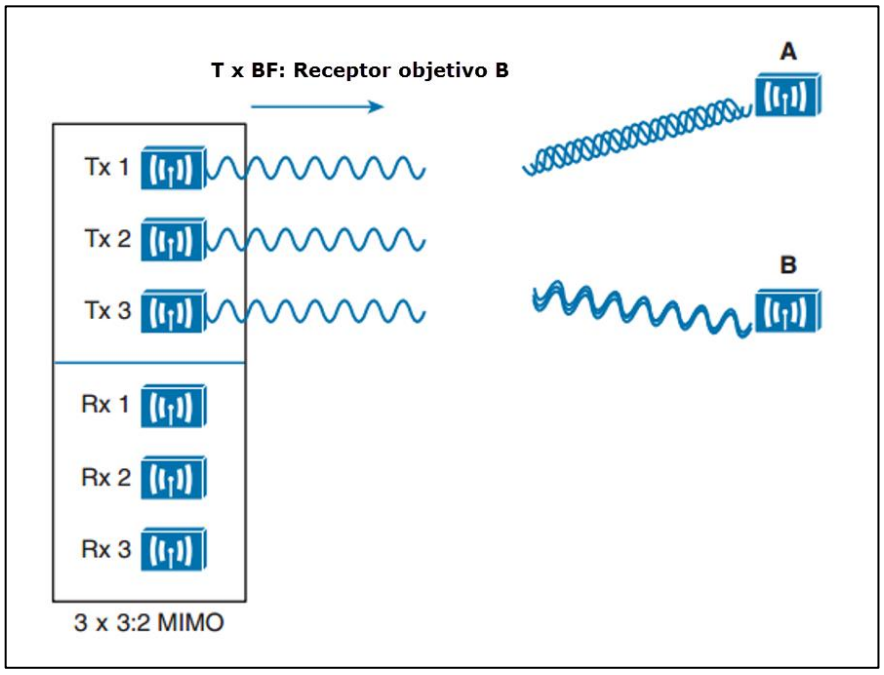
Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 59.

2.4.5.3. Formación del rayo transmitido (TxBF)

802.11n ofrece un método modificado de transmisión en donde se puede preferir un receptor a otro. Utilizando MIMO, la misma señal puede ser transmitida sobre múltiples antenas para alcanzar a un cliente en específico con más eficiencia.

Cuando múltiples señales llegan al mismo receptor con una diferencia de caminos y diferentes tiempos, causa un desfase en la señal total, esto es destructivo y disminuye el SNR generando una señal corrupta. Con la formación del rayo transmitida (TxBF) la fase de la señal es alterada antes de enviarla para que cuando la señal llegue a su destino se mantenga en fase.

Figura 31. **Formación de rayo dirigido a un dispositivo específico**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 60.

2.4.6. 802.11ac

Utiliza una mejor agregación de canal, canales de 40 MHz se unen para formar canales de 80 o 60 MHz de ancho. Utiliza una modulación más densa, utilizando 256-QAM se toman masa datos al mismo tiempo y mejora la tasa de transmisión, hasta 1 Gbps.

Sigue utilizando tecnología MIMO, hasta 8 tramas espaciadas simultáneamente. Multiusuario MIMO (MU-MIMO), un dispositivo tiene la habilidad de enviar varias tramas a múltiples receptores simultáneamente.

El *hardware* para 802.11n ha ido evolucionando lentamente, en la primera onda se alcanzó una velocidad entre 1 a 2,4 Gbps, en la segunda onda los dispositivos llegan a tener una tasa de transferencia de 6.93 Gbps.

2.4.7. 802.11ad

Es una especificación introducida por la Alianza Gigabit Inalámbrica (WiGig), y en teoría ofrecerá una velocidad de 7 Gbps sobre la frecuencia no licenciada de 60 GHz.

2.5. Alianza Wi-Fi

Todos los productos LAN inalámbricos deben acoplarse a los estándares IEEE 802.11 para ser compatibles. A pesar de que los estándares 802.11 son claros, está la posibilidad que un fabricante construya un producto en base a una interpretación del estándar y otro construya el suyo con otra interpretación diferente, esto ocurre especialmente cuando los estándares aún están en etapa de desarrollo. Adicional los fabricantes no están obligados a implementar cada

función descrita en los estándares, son libres de elegir ciertas partes o en su totalidad, incluso pueden agregar características propietarias.

La alianza Wi-Fi (http://wi-fi.org) es una asociación industrial sin fines de lucro, creada por fabricantes de dispositivos inalámbricos de alrededor del mundo. Para combatir el problema de incompatibilidad en productos inalámbricos, la alianza Wi-Fi introdujo el programa certificado Wi-Fi en el año 2000. Los productos inalámbricos son puestos a prueba y laboratorios autorizados, para poder certificar la correcta implementación del estándar. Si el producto pasa la prueba, entonces es certificado y recibe la estampa de certificación Wi-Fi, la cual utiliza el siguiente logo.

Figura 32. **Logo certificación WiFi**

Fuente: *Wi-Fi Certified*. http://www.wi-fi.org/certification. Consulta: 11 de octubre de 2016.

3. FUNDAMENTOS DE DISPOSITIVOS LAN Y WLAN

El objetivo de una red de área local inalámbrica es minimizar las conexiones cableadas, realizando un cambio de datos a través de un medio físico, por ejemplo, cobre o fibra, hacia ondas de radio, sin embargo, siempre existirá infraestructura cableada y equipos que se interconecten con el *core*, a continuación se presentan los dispositivos principales que se utilizan en una infraestructura WLAN, su descripción y funcionamiento.

3.1. Cable par trenzado

Es un tipo de conexión usado en telecomunicaciones en el que los alambres son entrelazados para anular interferencias de fuentes externas y diafonía de los cables adyacentes. El cable par trenzado consiste de 8 hilos de cobre aislados entre sí, tranzados en pares de forma helicoidal.

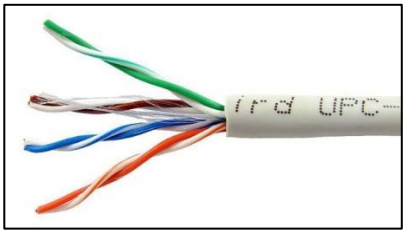
Se trenzan los alambres ya que al aplicar corriente alterna a un alambre se vuelve una antena, al entrelazarlos las ondas se cancelan, disminuyendo la radiación emitida. Así se disminuye interferencia eléctrica para el exterior y también para los pares cercanos.

Entre los tipos de cable par trenzado se encuentran los siguientes:

3.1.1. *Unshielded twisted pair* UTP

Cable par trenzado sin blindaje, es de bajo costo y fácil uso, aunque es susceptible a interferencias electromagnéticas, produciendo más errores.

Figura 33. **Cable UTP**

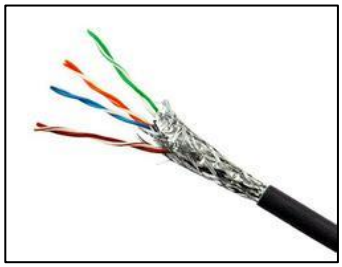


Fuente: *Redes BPS*. http://redesbps.com/. Consulta: 11 de octubre de 2016.

3.1.2. ***Shielded twisted pair*** **STP**

Cable par trenzado blindado, los pares se encuentran dentro de una cubierta protectora, con un número específico de trenzas por pie. Tiene inmunidad al ruido, es más caro que el UTP.

Figura 34. **Cable STP**

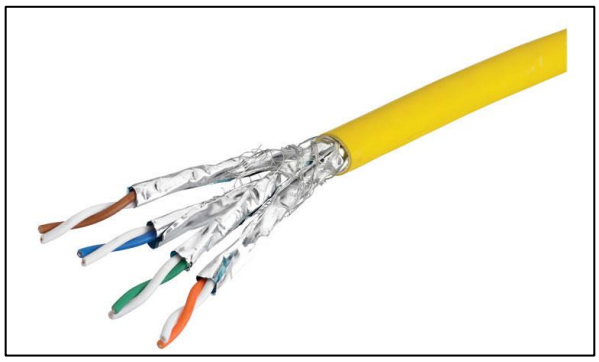


Fuente: *IndiaMART*. http://dir.indiamart.com/. Consulta: 11 de octubre de 2016.

3.1.3. ***Foiled twisted pair*** **FTP**

Cable par trenzado con blindaje global, los pares poseen una pantalla conductora global en forma trenzada, aumentando la protección contra interferencias.

Figura 35. **Cable FTP**

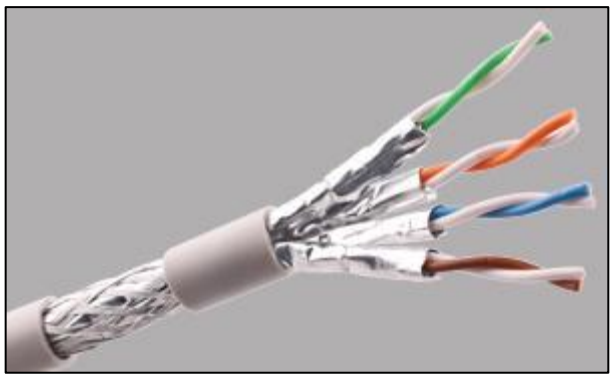


Fuente: *BioNEXTOR Access Control*. http://www.boutique-infocom.fr/. Consulta: 11 de octubre de 2016.

3.1.4. ***Screened fully shielded twisted pair* FSTP**

Cable par trenzado totalmente blindado, es un tipo especial de cable que utiliza múltiples protecciones metálicas.

Figura 36. **Cable FSTP**



Fuente: *Contact Us*. http://www.enpucable.com/. Consulta: 11 de octubre de 2016.

Dependiendo de la velocidad de transmisión, se utiliza un tipo de cable UTP específico para cada situación y construcción, la asociación Industrias Electrónicas e Industrias de las Telecomunicaciones (EIA/TIA) establece categorías, entre las más utilizadas en una red LAN están:

- Categoría 5: se utiliza para 10BASE-T y 100BASE-TX Ethernet.

- Categoría 5e: es una mejora de la CAT 5, fue realizada a base de mejores normas de pruebas, y es adecuado para Gigabit Ethernet, se utiliza en 100BASE-TX y 1000BASE-T Ethernet.

- Categoría 6: es utilizada para 1000BASE-T Ethernet y transmite a una velocidad de 1000Mbps.

- Categoría 6a: utilizada para 10GBASE-T Ethernet, transmite a 10 Gbps.

En redes LAN las velocidades de transmisión soportadas pueden llegar a 10Mbps (Ethernet), 100 Mbps (Fast Ethernet), 1Gbps (Gigabit Ethernet) y 10 Gbps (10 Gigabit Ethernet). Si se utilizados pares para la transmisión se tiene una transmisión half-duplex, un para para trasmitir y otro par para la recepción, de lo contrario, si solo se utiliza un par se tiene una conexión half-duplex.

Como toda tecnología y estándar, el cable par trenzado tiene sus ventajas y desventajas:

- Ventajas
    - Bajo costo de instalación
    - Facilidad para solución de problemas y rendimiento
    - Fácil pre-implementación en lugares industriales

- Desventajas
  - Altas tasas de error a altas velocidades
  - Ancho de banda limitado
  - Baja inmunidad al ruido y efecto crosstalk (diafonía)
  - Distancia limitada, 100 m máximo

3.2. Transceptor SFP

Small form-factor pluggable transceptor, conocido en inglés como SFP, es un dispositivo electrónico compacto y conectable en caliente (*hot-swappable*), utilizado para aplicaciones de telecomunicaciones y redes de datos. Soportan varios estándares de comunicaciones como lo son: Sonet, Fiber-channel, Gigabit Ethernet, entre otros.

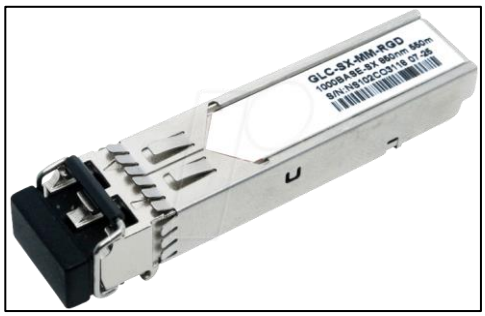
En el estándar Ethernet se tiene dos opciones, Ethernet sobre fibra óptica y sobre UTP.

3.2.1. Ethernet sobre fibra óptica

Los SFP que trabajan con fibra como medio de transmisión pueden ser uno o dos hilos, si el SFP solo tiene un hilo la transmisión y recepción deben de estar en diferente frecuencia para no interferir entre sí. Si es de dos hilos no existe problema en el tema de frecuencias ya que cada hilo es utilizado para transmisión y recepción respectivamente. Además de la cantidad de hilos también hay diferencias de tipo de fibra, monomodo o multimodo, dependiendo de las distancias a las que se desea transmitir, el núcleo será más pequeño para mayores distancias.

- SX, Fibra multimodo, diámetro del *core* 850 nm

Figura 37. **SFP SX**



Fuente: *Elektronik und Technik bei reichelt elektronik günstig bestellen*. http://www.reichelt.de/. Consulta: 11 de octubre de 2016.

- LX, Fibra monomodo, diámetro del *core* 1310 nm, distancia 10 Km

Figura 38. **SFP LX**

Fuente: *Provantage LLC*. http://www.provantage.com/. Consulta: 11 de octubre de 2016.

- EX, Fibra monomodo, diámetro del *core* 1310 nm, distancia 40 Km

Figura 39. **SFP EX**

Fuente: *Champion ONE*. http://www.championone.com/. Consulta: 11 de octubre de 2016.

- ZX, Fibra monomodo, diámetro del *core* 1550 nm, distancia 80 Km

Figura 40. **SFP ZX**

Fuente: *PlanetBarcode*. http://www.planetbarcode.com/. Consulta: 11 de octubre de 2016.

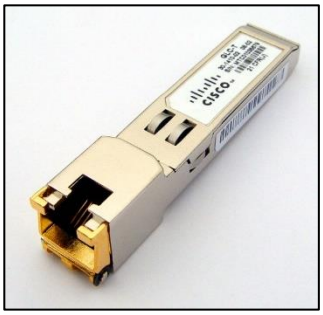
3.2.2. Ethernet sobre UTP

Los SFP que transmiten por cobre como medio, tienen una entrada para conector RJ-45 con sus 8 respectivos pines para la configuración de colores dependiendo de la aplicación.

- TX, velocidad 1Gbps

.

Figura 41. **SFP TX**



Fuente: *COMDIEL*. http://www.comdiel.cl/. Consulta: 11 de octubre de 2016.

Los equipos con puertos, diseñados para colocar SFPs tienen la ventaja de colocar el SFP dependiendo de la velocidad, aplicación y medio de transporte a utilizar. Por ejemplo, en un *switch* de acceso, se utilizan SFP de fibra para el *uplink* en un puerto de gran capacidad, y los *downlinks* utiliza SFP de cobre para cada usuario en donde comúnmente se conectan laptops o desktops y sus puerto Ethernet por lo general no pasan los 100Mbps.

3.3. Punto de acceso inalámbrico

Access point (AP), es un dispositivo de red que conecta la parte cableada con la inalámbrica, relaciona las VLAN de la red cableada con los SSID de una red inalámbrica. Los AP permiten la conexión de dispositivos móviles a una red.

Los puntos de acceso siguen el estándar IEEE 802.11 para determinar frecuencias, velocidad, tipos de modulación, etc. Los AP tienen dos opciones para trabajar:

- Modo LWAPP (*LightweigthAccess point* Protocol), gestionados por un controlador de WLAN, el WLC (*wireless* LAN *Controller*) se encarga de enviar al AP la configuración necesaria, actualizaciones y comandos de modificación, el AP solo sigue las órdenes del WLC, no mantiene mayor configuración en él, simplemente contiene un certificado de autenticación y direccionamiento básico de red para poder comunicarse.

- Modo autónomo, en donde el AP es independiente y se puede configurar SSIDs, IP, servidor DHCP, métodos de autenticación, entre otras opciones, todo en el AP.

Para utilizar el AP ya sea en modo LWAPP o autónomo, es necesario descargar la imagen especial para cada modo e instalársela al AP, la principal diferencia se nota al ingresar por consola al AP, en el modo LWAPP el dispositivo no tendrá la opción de configuración, permitiendo solo determinar direccionamiento IP y la IP del WLC para poder levantar el túnel LWAPP.

Cuando un AP es dirigido por un controlador, la administración y configuración es realizada en este dispositivo centralizado. Se pueden tener múltiples controladores y unirlos para cubrir más espacio y tener una red inalámbrica de mayor rango.

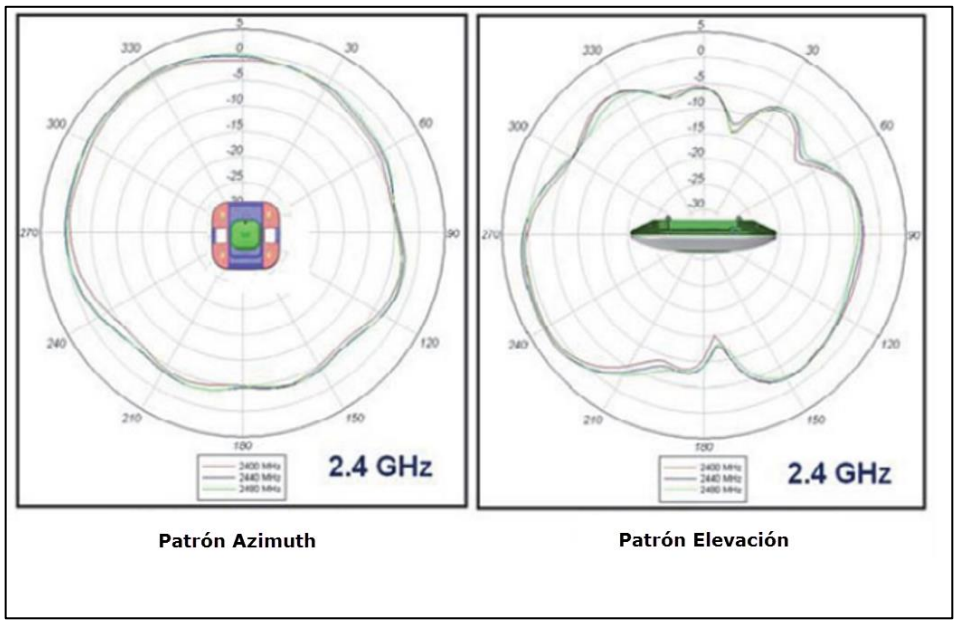
En el modo autónomo el AP tiene la habilidad de trabajar por sí solo, realizando la configuración y administrándolo por una interfaz gráfica, se ingresa a este GUI por medio de HTTP o HTTPS. En este modo no es posible lograr *roaming*, ya que cada AP trabaja por si solo y no hay forma de unirlos, por lo tanto, se utiliza en modo autónomo cuando se necesita cubrir un área pequeña.

Figura 42. ***Access point***

Fuente: *Cisco*. http://www.cisco.com/. Consulta: 11 de octubre de 2016.

Los AP interiores por lo general y convenientemente utilizan antenas monopolo, por el tamaño de las antenas y el patrón de radiación que tiene, tipo omnidireccional, cubren un área más amplia y uniforme, pareciéndose al patrón de una antena isotrópica.

Figura 43. **Patrones de radiación E y H de una antena omnidireccional**

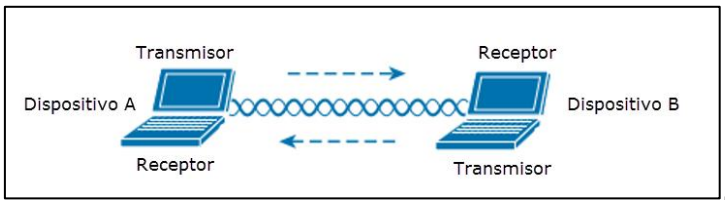


Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 96.

3.3.1. Funcionamiento del AP

Las señales RF viajan desde el transmisor al receptor, estos dos dispositivos pueden contactarse siempre y cuando estén sintonizados en la misma frecuencia o canal, utilicen el mismo esquema de codificación y modulación, esta comunicación debe ser en ambas direcciones.

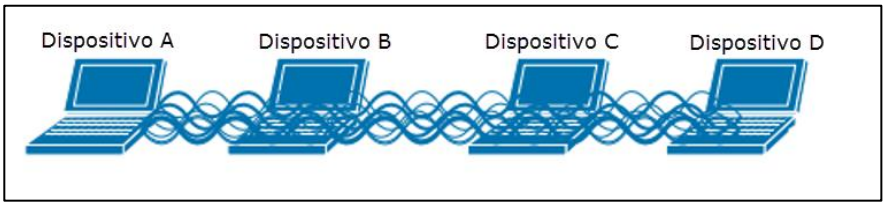
Figura 44. **Comunicación bidireccional**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 109.

Debido a que ambos dispositivos utilizan el mismo canal, es necesario dos fases en la comunicación: esperar turno y enviar en otros momentos. Si múltiples señales son recibidas al mismo tiempo, estas interfieren una con otra. La interferencia aumenta si la cantidad de dispositivos inalámbricos aumenta.

Figura 45. **Interferencia por transmisiones simultáneas**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 109.

Este mecanismo de esperar turnos para evitar interferencias es como el de Ethernet LAN, donde los usuarios comparten un ancho de banda en común y un dominio de colisión.

Los usuarios deben operar en *half-duplex* para evitar colisiones con otros transmisores, la consecuencia es que ningún usuario puede transmitir y recibir al mismo tiempo en la misma frecuencia.

3.3.1.1. Conjunto de servicios básicos (BSS)

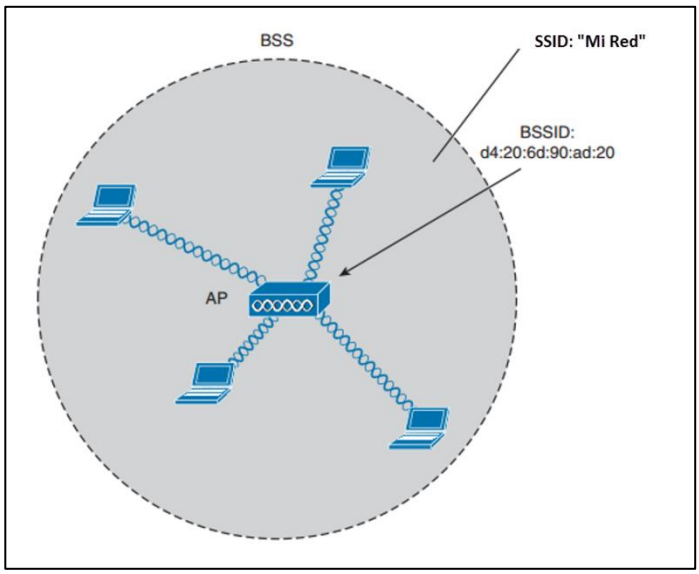
La solución para la interferencia entre usuarios, es hacer cada área de servicio un grupo cerrado, antes de que el cliente se asocie, se debe de advertir las capacidades y luego permitirle la asociación. El estándar 802.11 lo llama *basic serviceset* (BSS). En el centro de cada BSS se encuentra un AP inalámbrico.

Debido a que la operación del BSS recae en el AP, el BSS está limitado por el área donde la señal del AP es utilizable. A esta área se le conoce como *basic servicearea* (BSA) o celda.

El AP trabaja como punto de contacto, para cada dispositivo que quiere utilizar el BSS, el AP anuncia la existencia del BSS para que los dispositivos puedan encontrarlo y asociarse. Para realizar esta acción el AP usa un identificador BSS único (BSSID) que se basa en la dirección MAC del radio AP.

Para finalizar, el AP anuncia la red inalámbrica con un identificador de servicio (SSID), es un texto de caracteres que contiene un nombre lógico. La diferencia entre BSSID y SSID es que el BSSID es un nombre leíble para máquinas, el cual identifica el AP, y el SSID es un nombre leíble para humanos con el cual se identifica un servicio inalámbrico.

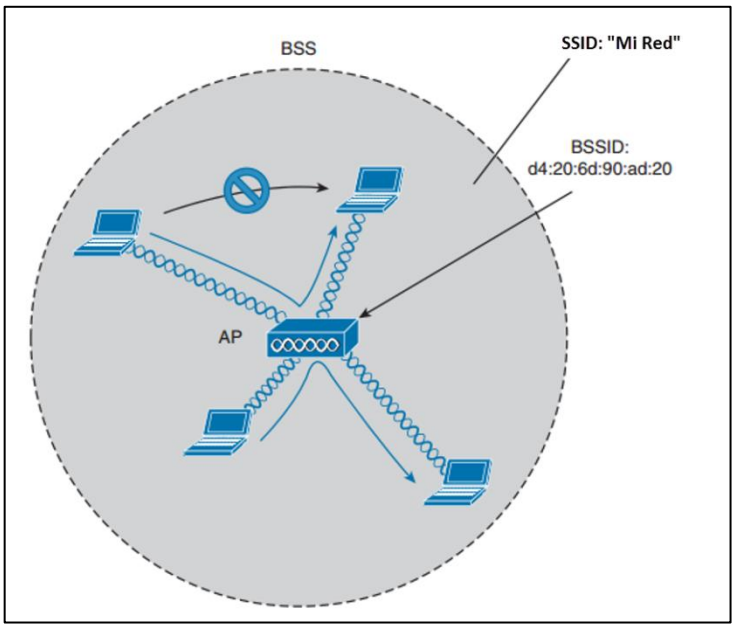
Figura 46. **802.11 BSS**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 111.

Cuando un dispositivo se une a un BSS se llama *asociación*. Un dispositivo debe enviar una solicitud de asociación y el AP le permite o deniega la solicitud. Cuando un dispositivo se asocia y se convierte en cliente, a este se le llama una estación (STA) del BSS. Mientras el cliente este asociado con el BSS, toda la comunicación pasa por el AP, si se desea comunicarse entre usuarios, el tráfico siempre debe pasar por el AP, sino la idea de organización y administración del BSS sería en vano.

Figura 47. **Comunicación dentro de un BSS**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 112.

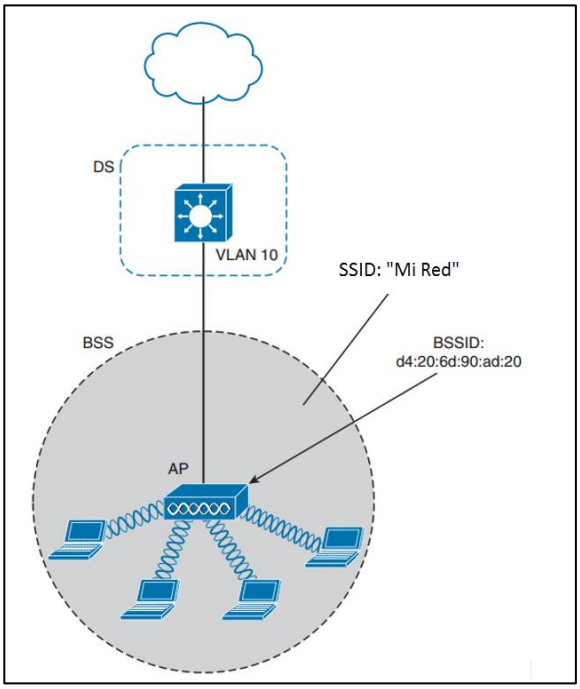
3.3.1.2. Sistema de distribución

EL BSS contiene un AP pero no se tiene conexiones con una red Ethernet regular. En esa configuración, el AP y los clientes asociados hacen una red autónoma. El trabajo del AP, no queda solo en ser el centro del BSS y administrarlo, en algún momento los clientes inalámbricos necesitarán comunicarse con un dispositivo ubicado en otro BSS en el cual no es miembro. El AP tiene habilidades cableadas e inalámbricas, el AP puede conectarse hacia una red Ethernet.

El AP se convierte en un puente entre los datos inalámbricos y cableados a un nivel de capa 2; en otras palabras el AP es el encargado de mapear una VLAN a una SSID. Este concepto puede extenderse a múltiples VLAN

mapeadas a múltiples SSIDs, para hacer eso el AP debe estar conectado a un *switch* por medio de una troncal que permita las VLANs.

Figura 48. **Sistema de distribución con BSS**



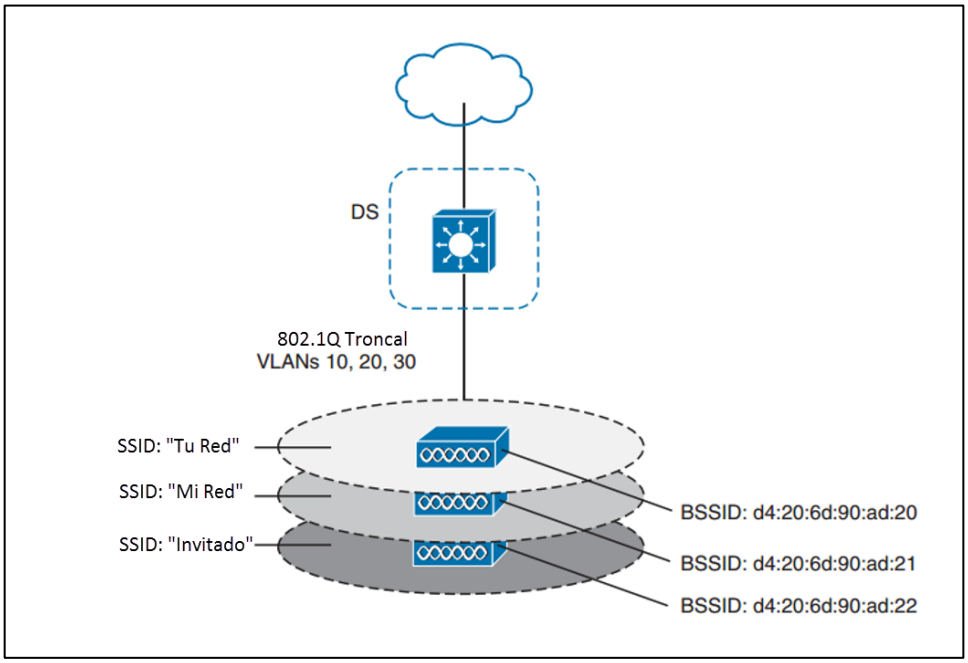
Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 113.

Cuando un AP utiliza múltiples SSIDs, en realidad está utilizando el aire como troncal para todas las VLANs, el cliente debe utilizar el SSID apropiado que esta mapeado a la respectiva VLAN que tiene configurada el AP. El AP se convierte en múltiples AP lógicos, uno por cada BSS, con un único BSSID. Con APs Cisco se aumenta el último digito de la MAC del radio para cada SSID.

Aunque un AP puede anunciar y soportar múltiples redes inalámbricas lógicas, cada SSID cubre la misma área geográfica, esto es porque el PA usa el transmisor, receptor, antenas y canal para cada SSID soportado. Múltiples

SSIDs no significa que se tiene mayor capacidad, los clientes tienen que compartir el *hardware* del mismo AP y compartir el tiempo de aire en el mismo canal.

Figura 49. **Múltiples SSIDs en un AP**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 114.

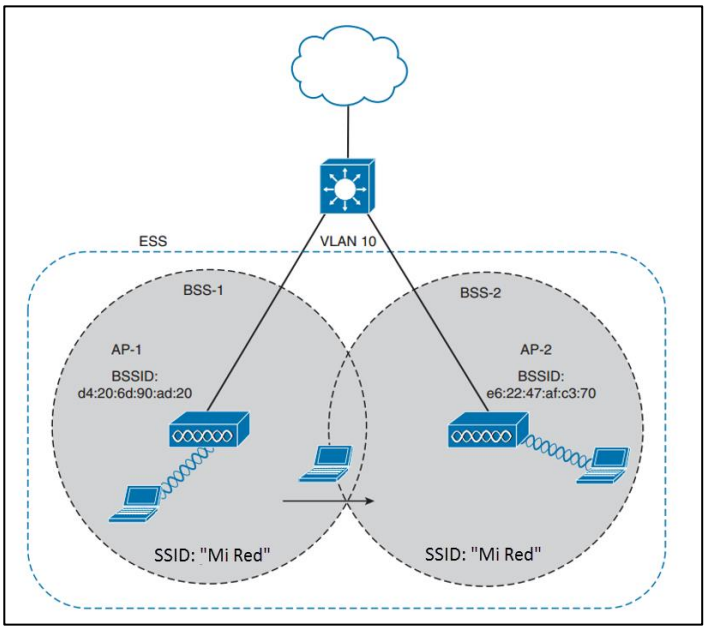
3.3.1.3. Conjunto de servicios extendidos (ESS)

Por lo general un AP no basta para cubrir un área completa, en donde se encuentran los clientes. Para cubrir un área más grande se debe de agregar más APs y ubicarlos en el área geográfica.

Cuando los AP son ubicados en diferentes posiciones, pueden ser interconectados por una infraestructura *switcheada*, el estándar 802.11 lo llama *extended service set* (ESS).

El objetivo es que múltiples AP, cooperen para que el servicio inalámbrico sea consistente sin espacios desde la perspectiva del cliente. Idealmente cada SSID que está definida en un AP debería estar en todos los AP dentro del ESS.

Figura 50. **802.11 ESS**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 115.

En un ESS, el cliente inalámbrico puede asociarse con un AP mientras este cercano a este, si el cliente se mueve a una ubicación diferente puede asociarse a un diferente AP automáticamente, logrando lo que se conoce como *roaming*.

3.4. *Switch*

Conmutador es el dispositivo que interconecta equipos a segundo nivel del modelo OSI, en la capa de enlace de datos. Su función es interconectar dos o más equipos, intercambiando las tramas entre sí por medio de la dirección física de los equipos, la MAC (*media access control*).

La MAC es un identificador de 48 bits, representado en 6 bloques hexadecimales, el cual corresponde de manera única a una tarjeta o dispositivo de red. Conocido también como dirección física. La formación de la MAC está determinada de la siguiente forma:

- Primeros 24 bits – IEEE
- Últimos 24 bits – Fabricante del dispositivo

Un ejemplo de una dirección MAC es 00:50:56:C0:00:08.

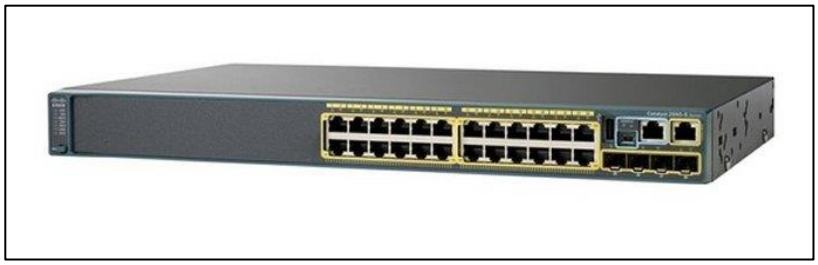
Existen *switch*es de capa 3 que pueden enrutar paquetes a otros segmentos, trabajan en capa 2 y 3 del modelo OSI, en la capa de enlace de datos y la capa de red, estos *switch*es tienen mayor capacidad de procesamiento y por lo general se utilizan en el *core* de una red.

Existe gran variedad de *switch*es, se tiene uno para cada escenario y necesidades, entre las características principales que se comparan en un *switch* para ser elegido son:

- Cantidad de puertos.
- Capacidad de los puertos (100Mbps, 1Gbps, 10Gbps, etc).
- Puertos SFP.

- *Uplinks* SFP.
- PoE en los puertos del *switch*.
- Potencia soportada por el *switch* en cada puerto PoE.
- Tipo de fuente de poder (AC o DC).
- Características de los sistemas operativos, capacidad para VoIP, parámetros de seguridad.
- *Switch* modular, con opción a expansión.
- Unidades de rack, espacio utilizado en el sitio a instalar.

Figura 51. ***Switch***



Fuente: *Cisco*. http://www.cisco.com/. Consulta: 11 de octubre de 2016.

3.4.1. Funcionamiento del *switch*

La función de un *switch* es de enviar tramas Ethernet, para alcanzar su objetivo el *switch* utiliza una lógica basada en la dirección MAC origen y destino en la cabecera de cada trama Ethernet.

El *switch* puede enviar tramas *unicast* o *broadcast*, las tramas *unicast* tienen una dirección destino, la cual representa a un solo dispositivo. Las tramas *broadcast* tienen una MAC destino de FFFF.FFFF.FFFF, esta trama es enviada a todos los dispositivos de la LAN.

Los *switch*es LAN reciben las tramas Ethernet y hacen la decisión a donde enviarlas o ignorarlas, para tomar esta decisión realiza 3 acciones:

- Decidir enviar o filtrar una trama, basado en la dirección MAC destino.
- Aprende direcciones MAC examinando la MAC origen de cada trama recibida.
- Crear un ambiente libre de *loops* con otros *switch*es utilizando *spanning tree protocol* (STP).

3.4.1.1. Decisión de enviar o filtrar tramas

Para decidir cuándo enviar las tramas, un *switch* usa una tabla construida dinámicamente en donde enlista las direcciones MAC y las interfaces asociadas. El *switch* compara la MAC destino con la tabla para decidir por cual interfaz enviar la trama o simplemente ignorar la trama.

La tabla MAC del *switch* enlista la ubicación de cada MAC relativamente con ese *switch*, en una LAN con múltiples *switch*es, cada uno hac una decisión independientemente basado en su propia tabla MAC, juntos envían la trama hasta que llegue a su destino.

3.4.1.2. Proceso de aprendizaje de direcciones MAC

La segunda función importante del *switch* es aprende las direcciones MAC e interfaces para colocarlas en su tabla de direcciones. Con una tabla MAC llena y correcta, el *switch* puede decidir con precisión a donde enviar la trama o filtrarla.

Los *switch*es construyen su tabla MAC oyendo las tramas entrantes y examinando el origen de la dirección MAC en la trama. Si la trama entra al *switch* y la MAC origen no está en la tabla MAC, el *switch* crea una entrada en la tabla. La tabla enlista la interfaz en donde la trama fue recibida, así de simple funciona un *switch*.

Los *switch*es tienen un tiempo para cada entrada en la tabla MAC, se llama *tiempo de inactividad.* El *switch* establece un tiempo de 0 para entradas nuevas. Cada vez que el *switch* recibe otra trama con la misma dirección MAC origen, el tiempo se resetea a 0. El contador aumenta, así el *switch* puede definir que entradas han llegado al tiempo máximo desde que se recibió una trama de ese dispositivo. El *switch* entonces remueve las entradas de la tabla cuando son muy antiguas. Si el *switch* se queda sin espacio para entradas en la tabla MAC, remueve las entradas con los tiempos de inactividad más grandes, o sea las entradas más antiguas.

3.4.1.3. Tramas *flood*

Cuando el *switch* no tiene una entrada en su tabla MAC con una dirección a la cual necesita enviar una trama, envía la trama a todas las interfaces (excepto la interfaz donde se recibió la trama) para averiguar la dirección MAC, a esto se le llama *flooding.*

Los *switch*es lo utilizan cuando tienen tramas *unicast* desconocidas. *Flooding* significa que el *switch* envía copias de la trama por todos los puertos, excepto la interfaz donde se recibió la trama. Si el dispositivo desconocido recibe la trama y envía una respuesta, la dirección MAC origen de la trama de respuesta permitirá al *switch* construir una entrada a la tabla MAC para ese dispositivo.

3.4.1.4. Evitar *loops* utilizando STP

La tercera característica de los *switch*es LAN es evitar *loops*; en la red implementando *Spanning tree protocol (STP).* Sin STP cualquier *flood* ocasionaría un *loop* indefinido en la red Ethernet si se tuviera enlaces físicos redundantes. Para prevenir *loops*, STP bloquea algunos puertos para no enviar tramas y que exista solo un camino activo entre cualquier par de segmentos LAN.

El resultado de STP es que no existan tramas en un *loop* indefinido, lo que hace utilizable la red LAN, sin embargo, STP tiene desventajas, incluyendo que necesita trabajo para balancear tráfico a través de enlaces redundantes.

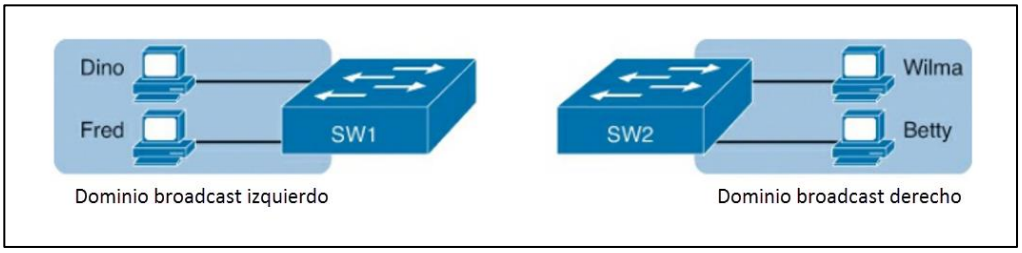
Para evitar *loops*, todos los *switch*es necesitan STP. STP hace que cada interfaz del *switch* se encuentre en un estado de bloqueo o de reenvío. Bloqueo significa que la interfaz no puede enviar o recibir tramas, mientras que reenvío significa que la interfaz puede enviar y recibir tramas, si las interfaces correctas son bloqueadas, solo existirá solo un camino lógico activo entra cada par de LANs.

3.4.1.5. LANs Virtuales (VLAN)

Antes de explicar VLAN se establece la definición de LAN, una LAN consiste en todos los dispositivos en el mismo dominio *broadcast*, sin VLANs, un *switch* considera todas las interfaces del *switch*, y los dispositivos conectados a esos links, en el mismo dominio *broadcast*. En otras palabras, todos los dispositivos conectados en la misma LAN.

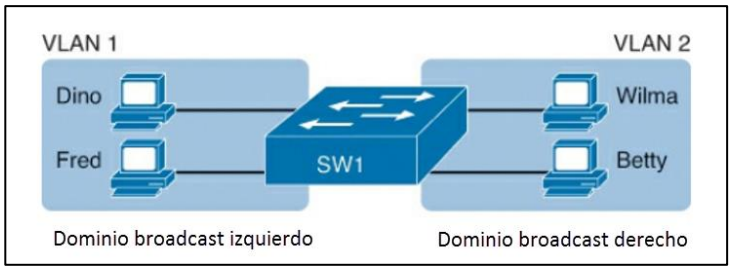
Con VLAN, un grupo de interfaces del *switch* se puede asociar a diferentes VLAN (dominio *broadcast*) para tener diferentes LAN o dominios *broadcast*. En esencia el *switch* crea múltiples dominios y puede asociar dispositivos a LANs separadas sin necesidad de más *hardware*.

Figura 52. **Dos dominios *broadcast* sin VLAN**



Fuente: ODOM, Wendell. *Cisco CCNA Routing and Switching 200-120*. p. 155.

Figura 53. **Dos VLANs en un *switch***



Fuente: ODOM, Wendell. *Cisco CCNA Routing and Switching 200-120*. p. 155.

3.5. Controlador inalámbrico LAN

Es un dispositivo que se utiliza en conjunto con los LWAPP, para administrar los AP en grandes cantidades por el administrador de la red o NOC (*Network Operation Center*). El controlador LAN controla la configuración de todos los AP.

Las redes inalámbricas se han vuelto necesarias en la actualidad, muchos ambientes corporativos e instituciones grandes requieren desplegar redes inalámbricas a gran escala, el controlador ayuda a este manejo, se convierte mucho más fácil, el WLC es el dispositivo que asume el rol central. El trabajo realizado por los Aps como asociación o autenticación de clientes se realiza en el WLC.

Como se había mencionado en la sección de Puntos de acceso AP, los LWAPP se registran con el WLC y crean un túnel en donde se transporta toda la gestión y datos, y luego intercambian los paquetes entre los clientes inalámbricos y la parte cableada de la red.

El túnel que el AP levanta contra el WLC se llama CAPWAP (*control and provisioning of wireless access points* protocol), luego de establecer comunicación el AP descargar el *firmware* y la configuración, cabe mencionar que el túnel CAPWAP es capa 3. Para que el túnel pueda funcionar correctamente los puertos UDP 5246 y 5247 deben estar desbloqueados en la red.

El WLC es el encargado de intercambiar paquetes entre usuarios inalámbricos, sin embargo, no es el único que interviene en el proceso de comunicación, todos los paquetes de los clientes 802.11 son encapsulados por el AP y enviados al WLC. El WLC desencapsula los paquetes y actúa basándose en la IP de destino, si el destino es uno de los clientes inalámbricos asociados al WLC, el paquete es enviado de vuelta en el túnel y el AP desencapsula el paquete y se lo envía al cliente inalámbrico. Si el destino está en la parte cableada de la red, el WLC quita la cabecera 802.11, le agrega la cabecera Ethernet y lo envía al *switch* conectado, de ahí es enviado al cliente en la red cableada. Cuando el paquete viene de la red cableada, el WLC

remueve la cabecera Ethernet y le agrega la cabecera 802.11, encapsula el paquete y lo envía al AP, donde es desencapsulado y entregado al cliente inalámbrico.

Para la configuración del WLC se tiene la siguiente lista de opciones:

- Acceso GUI por medio de HTTP o HTTPS
- Acceso CLI por medio de Telnet, SSH o consola
- Acceso por medio del puerto de servicio (OOB)

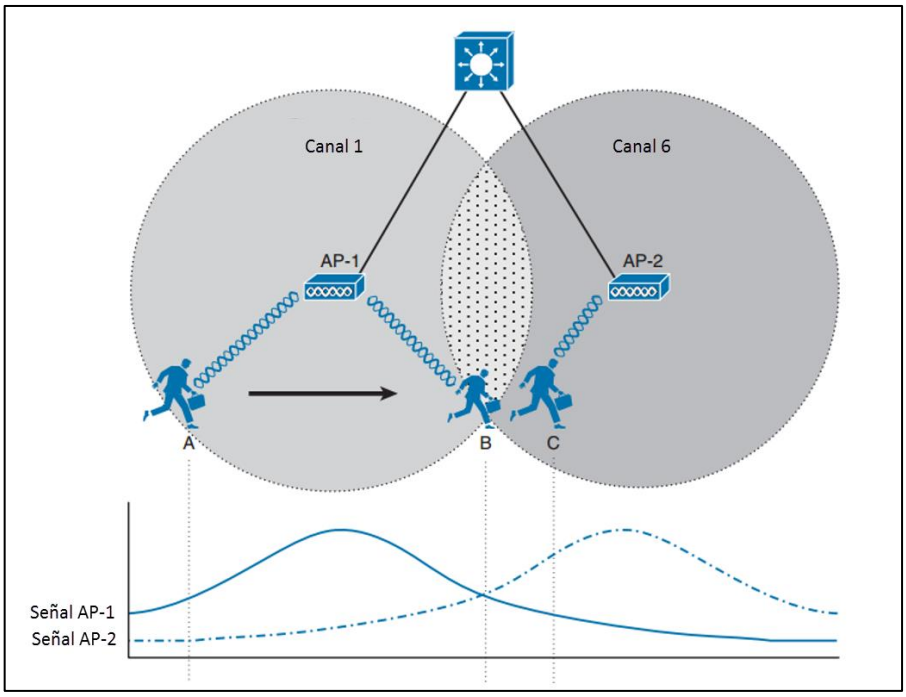
EL WLC guarda la configuración en formato XML en su memoria flash, y lo convierte para que pueda ser leída en formato CLI, la configuración se puede modificar cargando un archivo desde un servidor TFTP o FTP, el WLC se encarga de la conversión de XML a CLI, luego de cargar la configuración se puede modificar por línea de consola, luego de finalizar el WLC se encarga nuevamente de convertir la configuración a formato XML para guardarlo en su memoria flash.

3.5.1. *Roaming*

Entre las mayores ventajas y características más importantes al utilizar el WLC en una red inalámbrica es el *roaming*. El *roaming* es un proceso donde el cliente puede mantener aplicación ininterrumpidamente mientras está en movimiento. Cuando un cliente inalámbrico se asocia y autentica al WLC, este coloca un registro en la base de datos para clientes, este registro incluye dirección MAC y dirección IP del cliente, contexto de seguridad y asociaciones, contexto de QoS, el WLAN y la asociación con el AP. Cuando el cliente se mueve, hacia otro AP asociado al mismo WLC, el registro solamente se actualiza con la información del nuevo AP, así los datos son enviados

apropiadamente al cliente. Cuando el cliente se mueve hacia un AP asociado a diferente WLC, sin importar si se encuentra en la misma red o no, el WLC envía el registro del cliente en la base de datos hacia el nuevo WLC. Esto ayuda a que el cliente mantenga su dirección IP al realizar *roaming* y mantener las sesiones TCP ininterrumpidas.

Figura 54. ***Roaming* entre dos AP**



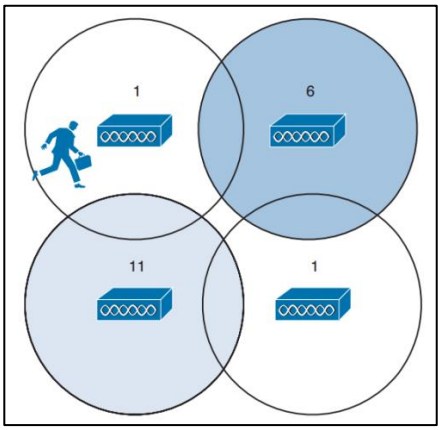
Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 156.

3.5.2. Diseño de canales WLAN

La parte anterior se describió el movimiento entre dos Ap, la mayoría de escenarios requieren más de dos Ap para cubrir apropiadamente el área. Por ello es necesario el diseño y la configuración de cada vez más Ap para escalar el diseño que encaja en el entorno inalámbrico.

Para minimizar la superposición de canales y la interferencia, las celdas de los Ap tienen que estar diseñadas de tal manera que los Ap vecinos utilicen diferentes canales. En el caso de la banda 2,4GHz se tiene la siguiente imagen donde no se tiene interferencia entre canales vecinos.

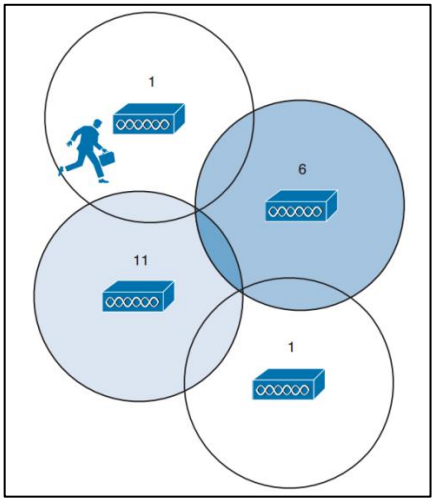
Figura 55. **Espacio entre celdas alternadas**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 158.

Se puede observar que en el centro de las celdas se encuentra un espacio sin cobertura, si un usuario inalámbrico pasa por ese lugar su señal caerá completamente, pero si se unen más las celdas se sobrepondrán las dos que utilizan el canal 1.

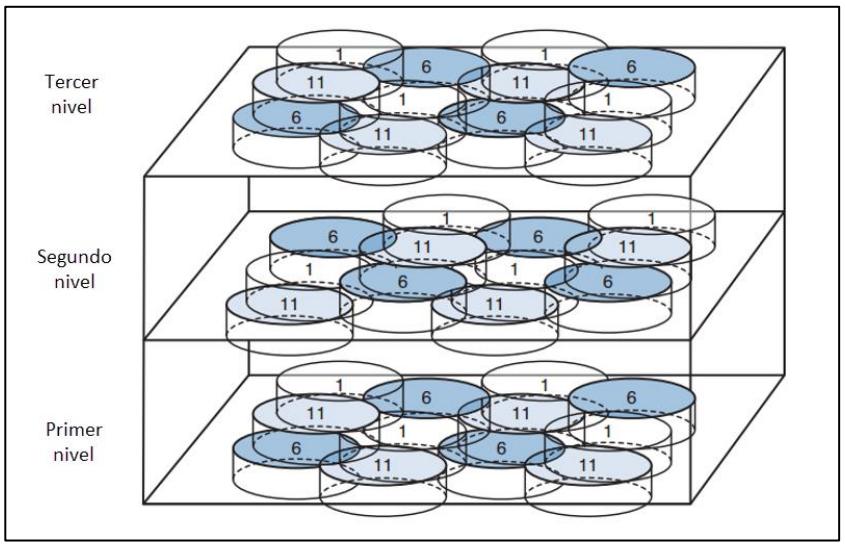
Figura 56. **Celdas alternadas correctamente**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 159.

Para solucionar este inconveniente se utiliza un diseño de panal, en donde no se dejan espacios sin cobertura. Alternar los canales para evitar la superposición se llama comúnmente reutilización de canales. Para dificultar más la situación, las señales propagadas por el AP son tridimensionales, por tal razón en un edificio con más de 1 nivel se tendrán señales arriba que pueden interferir.

Figura 57. **Celdas de canales en 3D**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 160.

Cuando se consideran todas estas posibilidades para poder diseñar y mantener una red LAN inalámbrica, se vuelve un rompecabezas para resolver, se debe de modificar el tamaño de cada celda, potencia transmitida y el canal asignado, todo debe ser coordinado y asignado a cada AP, para solventar este inconveniente existe el WLC, el cual se encarga de todo este proceso y modifica cada una de las características de cada AP para que no existan celdas con canales vecinos que puedan interferir entre, una gran ventaja que proporciona el controlador *wireless*. Esta función del WLC se llama *radio resource management* (RRM).

Características principales del controlador WLAN:

- Detección y prevención de interferencia, la potencia y canales de los AP son ajustados a conveniencia.

- Balanceo de carga, se tiene la opción de balancear la carga de un cliente con múltiples AP para mejorar cobertura y velocidad.
- Detección y corrección de áreas sin cobertura, la potencia de los AP puede ser cambiada, se puede aumentar para cubrir áreas sin señal o disminuirla para evitar superposición de celdas.

Además, un controlador WLAN provee visibilidad, escalabilidad y confiabilidad que se necesita para una segura, escalable red inalámbrica.

Para elegir un WLC acorde a la situación, se debe de estudiar las características y obtener un buen equipo que cubra las demandas del proyecto sin sobrepasar el presupuesto. Entre las características principales que se verifican para seleccionar un WLC son:

- Cantidad de AP soportados
- Cantidad de usuarios soportados
- Estándares de 802.11 soportados
- QoS
- Métodos de autenticación, seguridad de las redes inalámbricas
- Puertos LAN, velocidades y SFPs soportados
- Dimensiones físicas
- Tipo de fuente de poder (AC o DC)

Figura 58. **Controlador red LAN inalámbrica**

Fuente: *Cisco 5508 WirelessController*. http://www.cisco.com/c/en/us/products/*wireless*/5508-*wireless-Controller*/index.html. Consulta: 11 de octubre de 2016.

4. FUNDAMENTOS DE SEGURIDAD EN REDES INALÁMBRICAS

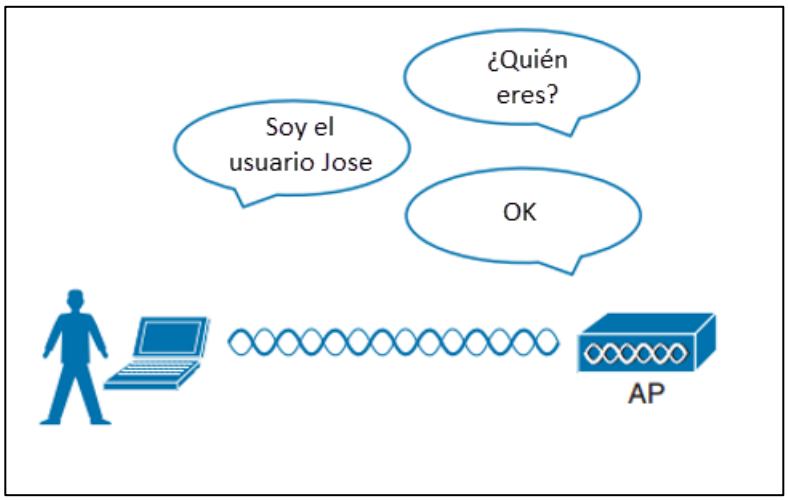
Las redes inalámbricas son complejas, muchas tecnologías y protocolos trabajan en conjunto para dar a los usuarios estabilidad, movilidad y conexión a una infraestructura cableada. Desde la perspectiva del usuario, una conexión inalámbrica no debería de ser diferente a una cableada. Una conexión cableada le da al cliente una sensación de seguridad, los datos que pasan por un cable probablemente no serán captados por alguien más. Una conexión inalámbrica es inherentemente diferente, los datos son transportados por el aire y pueden ser captados por cualquiera dentro el rango.

Por esa razón, asegurar una red inalámbrica se convierte tan importante como cualquier otro aspecto. El proceso de identificación es desarrollado por varios esquemas de autenticación. Proteger los datos inalámbricos involucra funciones de seguridad como encriptación y autenticación.

4.1. Autenticación

Para controlar el acceso a las redes inalámbricas, se puede autenticar al dispositivo del cliente antes de que se le permita asociarse. Los posibles usuarios deben de identificarse a sí mismos presentando algún tipo de credencial a los AP.

Figura 59. **Autenticación de usuario**

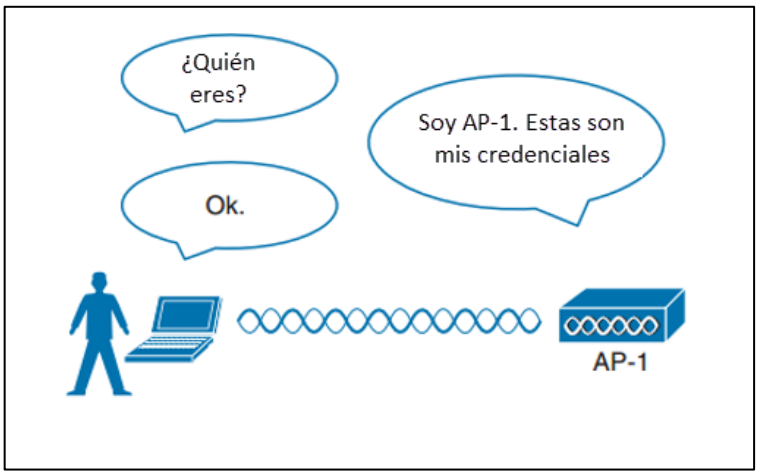


Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 286.

La autenticación puede tomar muchas formas. Algunos métodos solicitan solo un texto estático el cual es el mismo para todos los clientes permitidos y los APs. El texto es almacenado en el dispositivo del cliente y lo enseña al AP cuando es necesario. Otro método más complejo se realiza por medio de la interacción con la base de datos corporativa. En esos casos, el usuario debe ingresar un usuario y contraseña válidos.

No solo los clientes deben de autenticarse, los APs también deben de ser legítimos, ya que cualquier equipo malicioso puede hacerse pasar por un AP irradiando, una SSID con el mismo nombre de una red confiable, esta autenticación se logra legitimando cada trama enviada entre cliente y AP.

Figura 60. **Autenticación de AP**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 287.

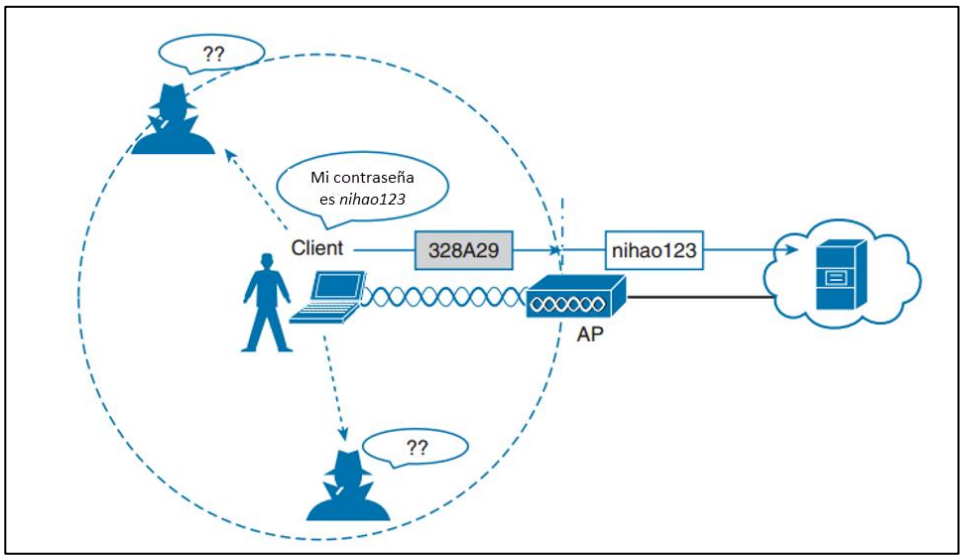
4.1.1. Privacidad del mensaje

Luego de la autenticación entre usuario y AP la conexión entre ambos se vuelve confiable, sin embargo, los datos que pasan entre ellos aún están disponibles para cualquier persona en el mismo canal.

Para proteger la privacidad de los datos en una red inalámbricas, los datos deben ser encriptados, se descifran los datos en cada trama y luego se descifran al llegar a su destino. La idea es utilizar un método de cifrado para que el transmisor y el receptor lo compartan y puedan comunicarse.

En las redes inalámbricas, cada WLAN soporta solo un método de autenticación y cifrado, por tanto, todos los clientes deben de utilizar el mismo método de cifrado para asociarse. El AP negocia con cada cliente una llave de cifrado para que cada vinculación sea diferente y no se pueda ver los datos de otros usuarios.

Figura 61. **Cifrado de datos en red inalámbrica**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 288.

4.1.2. Integridad del mensaje

Al cifrar los datos se evita que sean visibles mientras viajan en una red pública y no confiable. El destinatario debe ser capaz de descifrar el mensaje y recuperar el contenido original, pero cabe la posibilidad que el mensaje no llegase como se fue enviado.

El MIC (*message integrity check*), chequeo de la integridad del mensaje es una herramienta de seguridad que protege ante la manipulación de los datos. El MIC es un tipo de estampa secreta que se agrega a la trama cifrada que se envía. MIC está basado en el contenido de los bits de datos, cuando el receptor descifra la trama, se compara la estampa secreta, creando una a base de los datos que se recibieron, si las dos son idénticas, el receptor puede asumir que los datos no fueron manipulados.

4.1.3. Protección contra intrusos

Muchas herramientas de seguridad trabajan coordinadamente con la comunicación entre el cliente y el AP, ambos dispositivos son participantes activos en la conexión. Las herramientas de seguridad se concentran en evitar que los atacantes se conecten a la red inalámbrica y que estos manipulen las asociaciones existentes.

Las amenazas de seguridad inalámbrica se pueden agrupar en las siguientes categorías.

- Dispositivos intrusos
- Redes AD HOC
- Problemas de asociación cliente
- Ataques pasivos o activos

4.2. Métodos de autenticación para clientes inalámbricos

Se pueden utilizar diferentes métodos para autenticar a los clientes, mientras se asocien a la red. Los métodos han ido aumentando y evolucionando para resolver las debilidades de seguridad. Esta sección describe los métodos de autenticación más comunes.

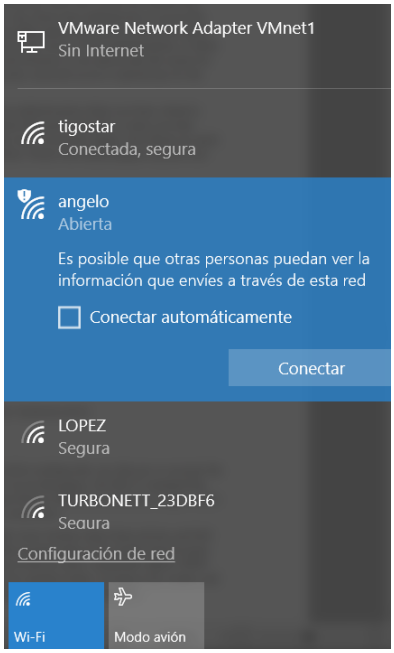
4.2.1. Autenticación abierta

El estándar original 802.11 ofrecía solo dos opciones de autenticación: autenticación abierta y WEP.

Como lo dice su nombre, la autenticación abierta da acceso libre a la WLAN, el único requerimiento es que el cliente utilice autenticación 802.11 antes que se asocie con el AP.

Se utiliza este tipo de autenticación en lugares públicos que ofrecen *hot spots,* para que los clientes consuman en el sitio y se puedan conectar. Por lo general se necesita abrir el explorador web para poder ver y aceptar los términos e ingresar credenciales básicas, como *email*. Las redes con autenticación abierta aparecen por lo general con un icono de advertencia indicando que no es segura si se asocia a la red.

Figura 62. **WLAN con autenticación abierta**



Fuente: elaboración propia.

4.2.2. WEP

Wireless equivalent privacy, es un método para hacer las redes inalámbricas más equivalentes a las conexiones cableadas, WEP brinda privacidad a los datos enviado entre AP y cliente. Se utiliza una cadena de caracteres como llave, llamada comúnmente como llave WEP, mientras el transmisor como el receptor tengan una llave idéntica, podrán cifrar y descifrar los datos enviados.

WEP es conocido como un método de seguridad *shared-key*, de llave compartida, eso quiere decir que la llave debe ser compartida entre el que envía y el que recibe en todo momento. La llave WEP puede ser de 40 o 104 bits de largo, representada como una cadena de 10 o 26 dígitos hexadecimales. Regla de oro, llaves más largas ofrecen más bits para el algoritmo, como resultado se tiene un cifrado más robusto. Pero esto no aplica a WEP, ya que es considerado un método muy débil para asegurar la LAN inalámbrica, por lo que está oficialmente obsoleto.

4.2.3. 802.1x/EAP

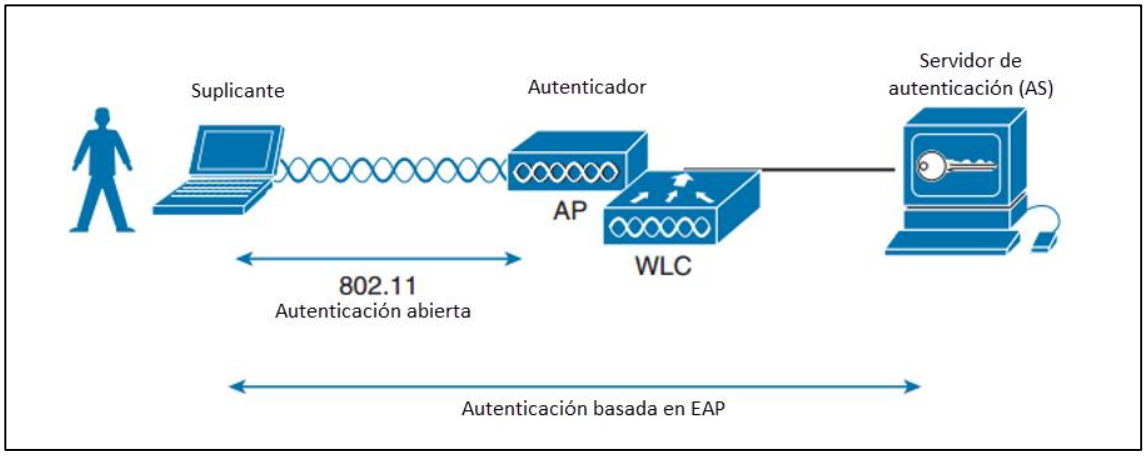
Es un método de autenticación más seguro a comparación de WEP, es un método flexible y escalable, *extensible authentication protocol*. EAP en si no consiste en un método de autenticación, sino que define un grupo de funciones que utilizan métodos de autenticación para permitir conectar clientes. EAP tiene otra cualidad interesante, se puede integrar con el estándar IEEE 802.1x basado en control de acceso para puertos. Cuando 802.1x está habilitado, se limita el acceso a la red hasta que el cliente se autentique por medio de un método EAP, esto significa que un usuario inalámbrico puede asociarse contra

un AP, pero no será capaz de pasar tráfico a otra parte de la red hasta que se autentique correctamente.

Con la autenticación abierta y WEP, los usuarios inalámbricos son autenticados localmente por el AP sin otra intervención, el escenario cambia con 802.11x, el cliente usa autenticación abierta para asociarse al AP y después el verdadero proceso de autenticación ocurre en un servidor dedicado. Las partes de este proceso son:

- Suplicante: el dispositivo del usuario que está solicitando acceso.
- Autenticador: el dispositivo de la red que provee el acceso a la red (WLC).
- Servidor de autenticación (AS): el dispositivo que toma las credenciales del usuario y decide si permitir o denegar el acceso a la red basándose en la base de datos y políticas (servidor RADIUS).

Figura 63. **Autenticación EAP**



Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 293.

4.2.4. PEAP

El método EAP protegido utiliza autenticación interior y exterior, significa que el usuario se autentica dos veces, una con el AP y otra con el AS, el AS presenta un certificado digital para autenticarse a sí mismo con el suplicante en la autenticación exterior. Si el suplicante está conforme con la identidad del AS, ambos levantan un túnel TLS utilizado para el intercambio de llaves para la autenticación y cifrado.

Solo el AS tiene un certificado para PEAP, eso significa que el suplicante se encuentra listo para autenticar el AS. El cliente no tiene un certificado propio, por lo tanto, se debe autenticar dentro el túnel TLS usando uno de los siguientes métodos:

- MSCHAPv2: *Microsoft challenge authentication protocol*
- GTC: *generic token card*

4.2.5. EAP-TLS

PEAP utiliza un certificado digital en el AS, lo cual es un método de autenticación robusto, se puede descargar e instalar el certificado en un servidor, pero el cliente debe utilizar otros medios para identificarse a sí mismo. EAP *transport layer security* va un paso adelante solicitando certificados en el AS y en cada dispositivo de los usuarios.

Con EAP-TLS, el suplicante y el AS intercambian certificados y pueden autenticarse entre sí. EAP-TLS es considerado el método de autenticación inalámbrico más seguro disponible, aunque complejo para implementarlo.

4.3. Privacidad inalámbrica y métodos de integridad

El estándar original 802.11 soportaba solo un método para asegurar los datos en la red inalámbrica, WEP. Como se mencionó, WEP no es seguro ni recomendado, obsoleto en la actualidad. Se han desarrollado más opciones para cifrar los datos y proteger su integridad mientras viaja por el espacio.

4.3.1. TKIP

Desarrollado por el grupo de trabajo 802.11i y la alianza Wi-Fi. TKIP agrega las siguientes características de seguridad; utilizando el *hardware* predecesor y los fundamentos del cifrado WEP:

- MIC: un algoritmo que agrega una etiqueta a cada trama como una medida de seguridad contra manipulación.
- Estampa de tiempo: una estampa se agrega dentro del MIC para prevenir el reenvío de las tramas.
- Dirección MAC del transmisor: el MIC contiene la MAC del transmisor como evidencia de la fuente.
- TKIP contador secuencial: brinda un registro de las tramas enviadas por una MAC única.
- Algoritmo de mezcla de llaves: computa una única llave WEP de 128 bits para cada trama.
- IV Vector de inicialización: el tamaño IV es el doble desde 24 a 48 bits.

TKIP se convirtió en un método razonable para solucionar todas las puertas de inseguridad. Existen ataques con TKIP por lo que se recomienda utilizar un mejor método si hay posibilidad, en efecto TKIP se volvió obsoleto en el estándar 802.11-2012.

4.3.2. CCMP

El protocolo Counter/CBC-MAC es un mejor método de cifrado, consiste de dos algoritmos:

- AES modo cifrado contador
- CBC-MAC, utilizado como un mensaje de chequeo para integridad

AES (*advanced encryption standard*) es un algoritmo libre, accesible al público y representa el método de cifrado más seguro hasta la fecha.

4.3.3. WPA y WPA2

El estándar IEEE 802.11i establece las mejores prácticas en método de seguridad inalámbrica. Mientras el estándar se desarrollaba, la alianza Wi-Fi introdujo a la industria el estándar *Wi-Fi protected access* (WPA).

Cuando el estándar 802.11i fue terminado y publicado, la alianza Wi-Fi agrego las partes nuevas a su versión WPA versión 2 (WPA2). WPA2 ofrece las capacidades de WPA para ser compatible, y agrega el algoritmo CCMP.

Tabla IX. **Comparación WPA y WPA2**

	WPA	**WPA2**
Autenticación	Llave compartida o 802.1x	Llave compartida o 802.1x
Cifrado y MIC	TKIP	TKIP o CCMP
Llave de administración	Llave dinámica	Llave dinámica

Fuente: HUCABY, David. *CCNA Wireless 640-722*. p. 297.

Los estándares WPA y WPA2 también soportan dos modos de autenticación, basados en la escala del aprovisionamiento:

- Modo personal: una llave compartida es utilizada para autenticar a los clientes a la WLAN.
- Modo empresarial: un método de autenticación basado en 802.1x EAP.

El modo personal es más fácil de usar en ambientes pequeños, cada dispositivo debe de tener configurada la misma llave compartida. Si se cambia la contraseña es necesario actualizarla en cada dispositivo en la red WLAN.

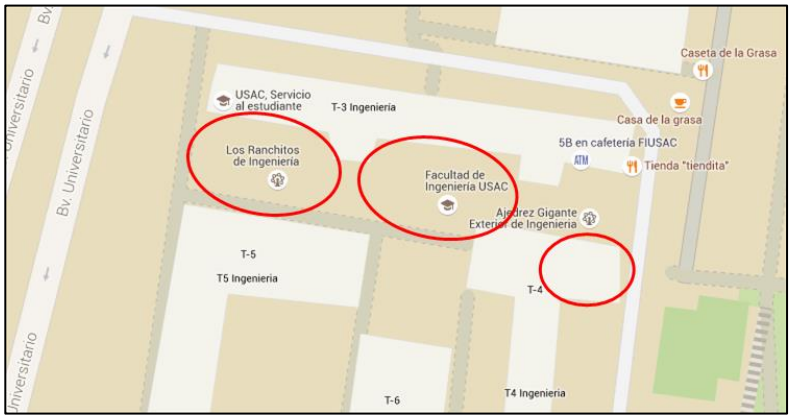
5. DISEÑO DE LA PROPUESTA PARA OPTIMIZAR LA RED 802.11

La propuesta del diseño para la red inalámbrica del área de recreación en la Facultad de Ingeniería, Universidad de San Carlos de Guatemala, está basado en las mejores prácticas por parte del fabricante de los equipos a utilizar, normas RFC internacionales, aplicables a Guatemala y un estudio realizado en el área descrita utilizando equipos reales y en un ambiente cotidiano.

El diseño está compuesto por un controlador Cisco 5508 el cual es el equipo central de la solución, la señal inalámbrica se tendrá gracias a los AP Cisco 3705i los cuales son equipos de gama alta y diseñados para soportar la gran demanda de usuarios y tráfico simultáneo, en la parte de distribución se tienen *switch*es Cisco 2960, equipos versátiles y confiables que también proveerán de alimentación eléctrica a los AP Cisco 3705i.

El lugar donde se llevará a cabo el trabajo será en el área de recreación de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, esto contempla el área de columnas, jardín principal y el área de ranchos. En la siguiente imagen se muestran los lugares:

Figura 64. **Facultad de Ingeniería, USAC**



Fuente: elaboración propia.

Figura 65. **Plaza columnas**

Fuente: elaboración propia.

Figura 66. **Jardín principal de la Facultad de Ingeniería USAC**

Fuente: elaboración propia.

Figura 67. **Los ranchitos de la Facultad de Ingeniería**

Fuente: elaboración propia.

El controlador inalámbrico administra los puntos de acceso distribuidos por toda el área a cubrir, evitando el traslape de bandas de frecuencia. El controlador centralizado y los puntos de acceso estarán conectados por medio de conexiones de cobre (UTP) hacia un *switch* de acceso a una velocidad de 1 Gbps en cada conexión. Para implementar este diseño se debe interconectar el *switch* con el *core* de la Facultad de Ingeniería de la USAC. Las conexiones entre WLC a *switch*, y *switch* a *Core* están hechas por medio de *port-channels,* que son agrupaciones de conexiones, que aumentan velocidad y disponibilidad en las transmisiones.

Se deberá de realizar configuraciones en la parte del *Core* de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, y de la solución *wireless* para poder unificar las dos partes. Al lograr unir la solución a la red de la Facultad de Ingeniería, en el controlador se aplicarán tecnologías desarrolladas para disipar interferencias y mejorar la experiencia del usuario, con una mayor seguridad y con una administración más fácil de usuarios y dispositivos.

5.1. Estudio del sitio

Para poder realizar parte del diseño es necesario realizar un estudio físico del sitio (*site survey*), en este estudio se obtiene datos importantes para la implementación de la solución *wireless* en la Facultad de Ingeniería de la USAC: cantidad de usuarios en hora pico, aplicaciones utilizadas por las personas en el área, saturación de personas en cierta área, dispositivos utilizados, entre otros.

Se utilizan herramientas para realizar mapas de calor, con esto se logra determinar los lugares en donde hay una señal débil, lugares donde la señal no

está disponible, obstáculos que se puedan presentar a la señal y por ello los AP no logran dar cobertura a todo el sitio. También con este estudio se logra observar las señales que existen actualmente, las posibles interferencias por otras fuentes en el sitio, y la contaminación del espectro que pueda existir.

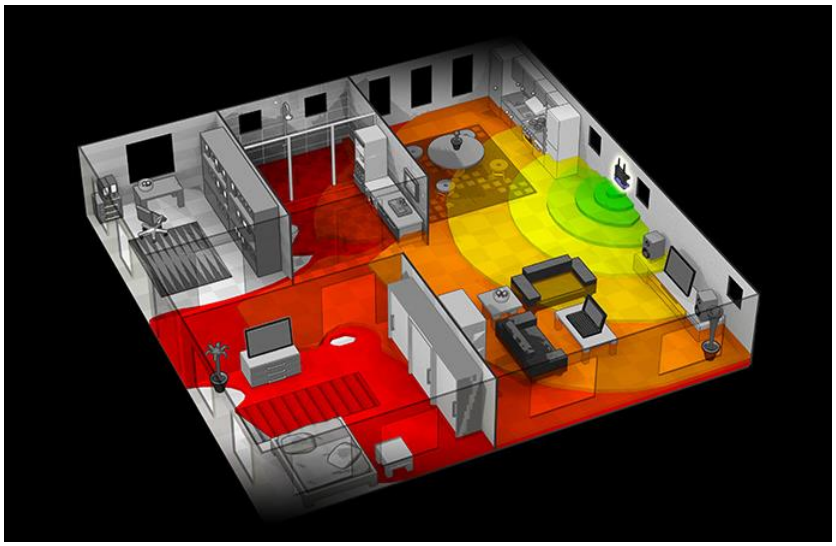
Con el estudio del sitio se determina la cantidad de *Access points* que se deben instalar en el área y la distribución de los mismos para lograr la mejor cobertura posible. Además de determinar la cantidad se obtiene información para elegir el tipo de AP a instalar.

El software utilizado para el estudio del sitio es Ekahau, con este software se crea un mapa ilustrando los diferentes niveles de potencia que se encuentra en el espectro, los niveles de potencia están expresados en la unidad logarítmica decibelio.

Las características principales del *software* Ekahau Heatmapper son:

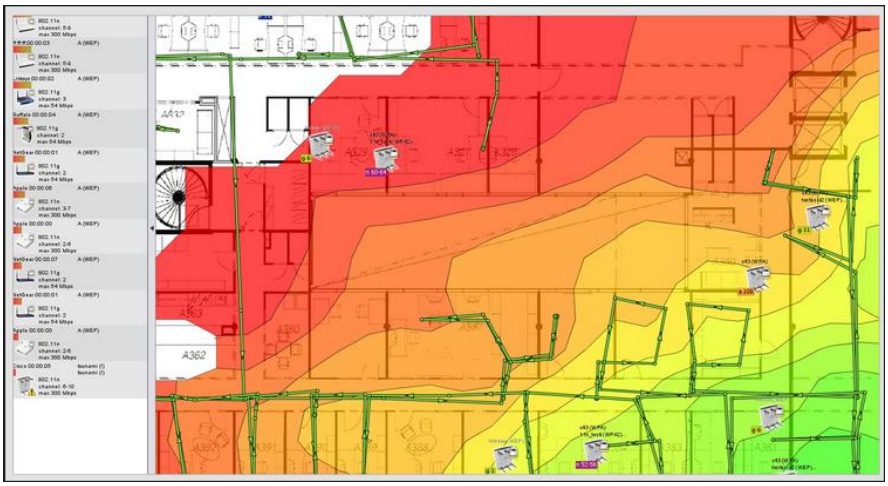
- Se observa la cobertura Wi-Fi en el mapa creado
- Se establece una posición aproximada de los AP existentes
- Encuentra SSID ocultos, y enlista las redes *wireless* disponibles
- Detecta parámetros de seguridad en las SSID encontradas
- Soporta el estándar 802.11n, y sus predecesores a/b/g

Figura 68. **Aplicación de la herramienta Ekahau**



Fuente: *Ekahau Site survey*. http://www.ekahau.com/wifidesign/ekahau-heatmapper. Consulta: 11 de octubre de 2016.

Figura 69. **Mapa de calor de la herramienta Ekahau**



Fuente: *Ekahau Site survey*. http://www.ekahau.com/wifidesign/ekahau-heatmapper. Consulta: 11 de octubre de 2016.

5.1.1. Mapas de calor

Los colores en el mapa de calor indican la potencia de la señal. La potencia de la señal es la medida más básica que afecta a la calidad de la conectividad Wi-Fi. Mientras mayor sea la potencia de la señal (lo que significa un número negativo más bajo) es mejor. Los rangos generales son:

- -0dBm a -60dBm: se tiene una buena cobertura de la señal.
- -60dBm a -80dBm: los usuarios se conectarán, pero no necesariamente a las velocidades más altas disponibles.
- -80dBm a -100dBm: conectividad débil, se esperan desconexiones a la red, velocidades bajas y problemas de rendimiento al utilizar video y audio.
- Señales arriba de 0dBm y debajo de -100dBm son raras de verse en una red WLAN.

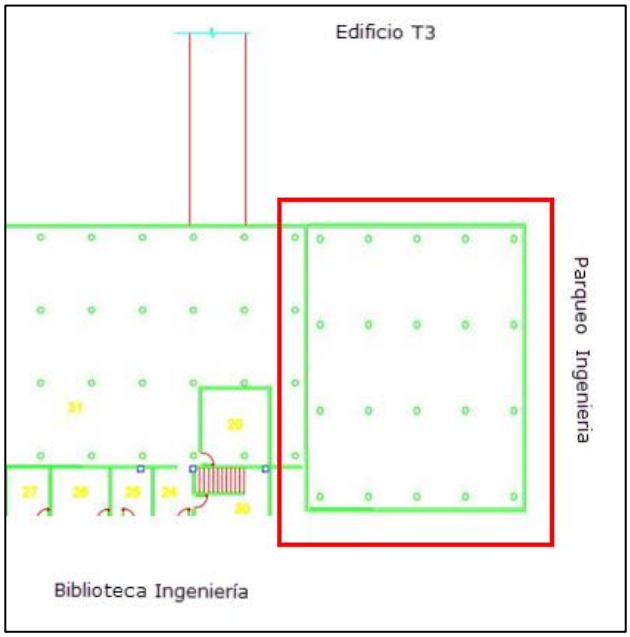
En el estudio del sitio se registraron dos SSID, que se encuentran en gran parte de las áreas analizadas, una es la SSID FIUSAC, la otra es la SSID RIUSAC, además de estas dos redes inalámbricas se detectaron varios dispositivos (AP, *routers*) que irradiaban diferentes SSIDs, esta saturación del espectro es una de las causas de que el servicio de WiFi no sea óptimo en la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, en vez de tener mayor cobertura se logra un traslape de bandas y esto causa choques de ondas lo cual hace que los datos transmitidos sean corrompidos y sea necesario retransmitir hasta que lleguen sin errores a su destino.

A continuación, se presentan los mapas de calor obtenidos de las dos redes inalámbricas más fuertes existentes en el área (FIUSAC y RIUSAC), y de

la SSID “Tesis” la cual es la red inalámbrica irradiada por el AP Cisco 3702, que se colocó de prueba en el estudio de sitio.

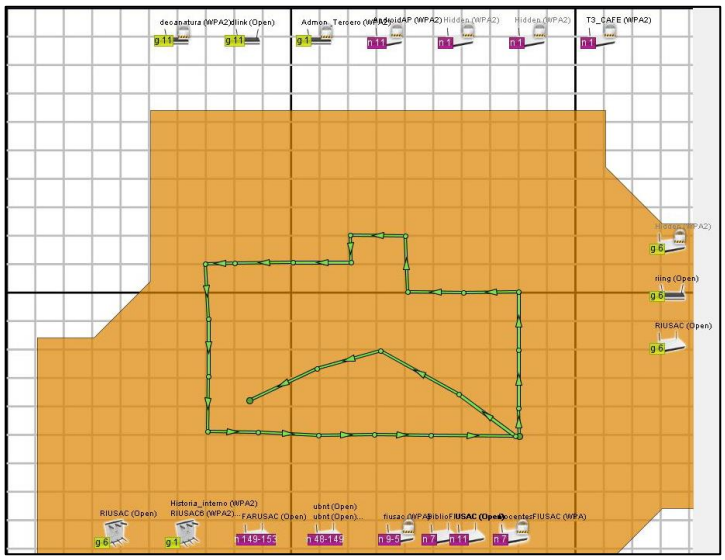
5.1.1.1. Área 1 – Plaza columnas extensión

Figura 70. **Plaza columnas extensión**



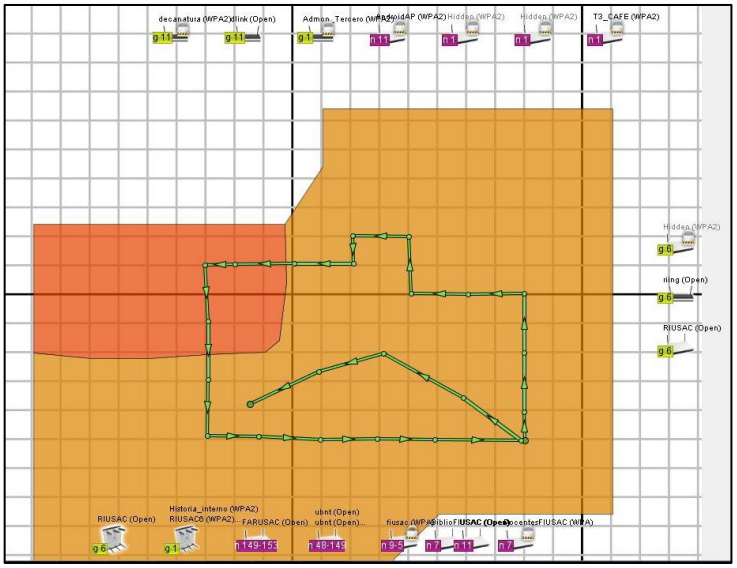
Fuente: FERNÁNDEZ, Jennyfer. *Unidad de Planificación e Infraestructura, Facultad de Ingeniería, USAC. Plano*.

Figura 71. **SSID FIUSAC en el área 1**



Fuente: elaboración propia.

Figura 72. **SSID RIUSAC en el área 1**



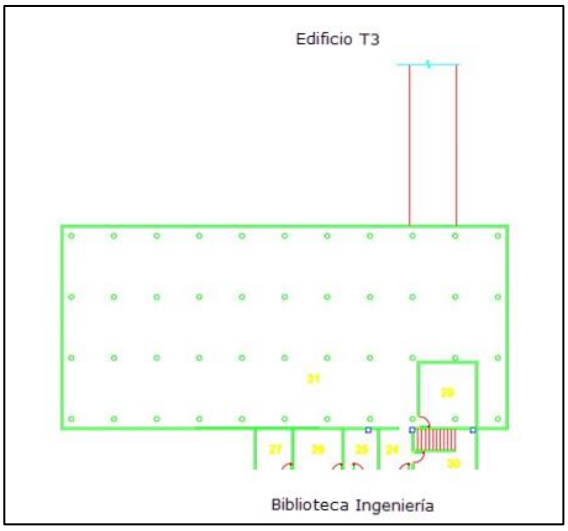
Fuente: elaboración propia.

Figura 73. **SSID TESIS en el área 1**

Fuente: elaboración propia.

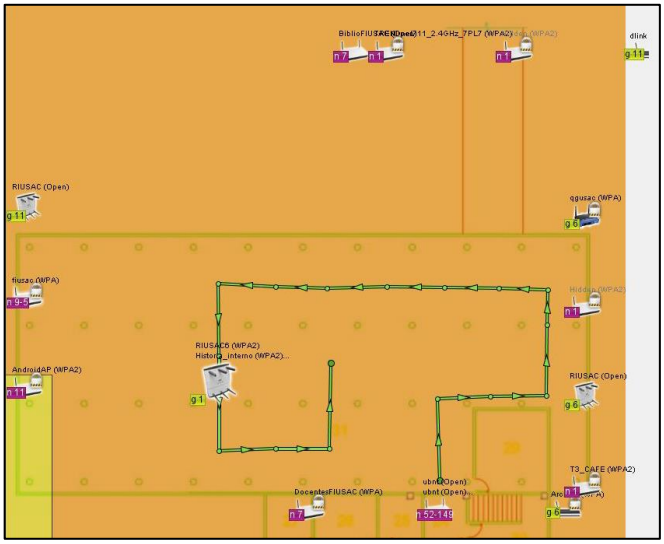
5.1.1.2. Área 2 – Plaza columnas

Figura 74. **Plaza columnas**



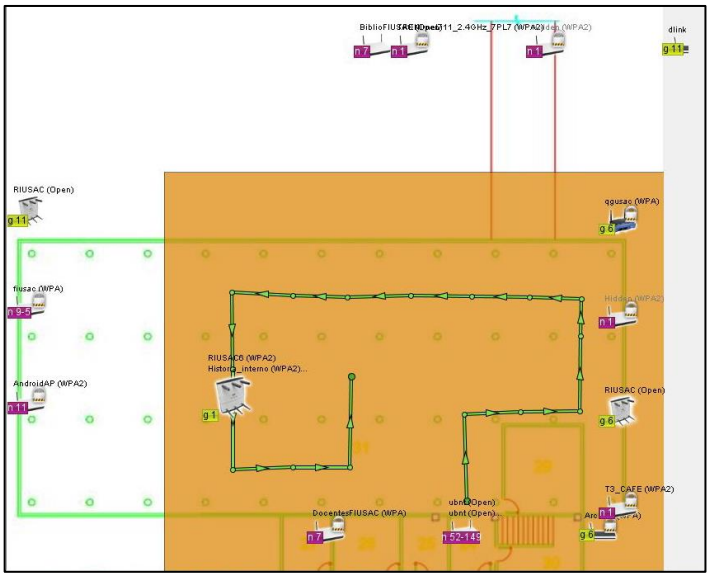
Fuente: FERNÁNDEZ, Jennyfer. *Unidad de Planificación e Infraestructura Facultad de Ingeniería, USAC.* Plano

Figura 75. **SSID FIUSAC en el área 2**



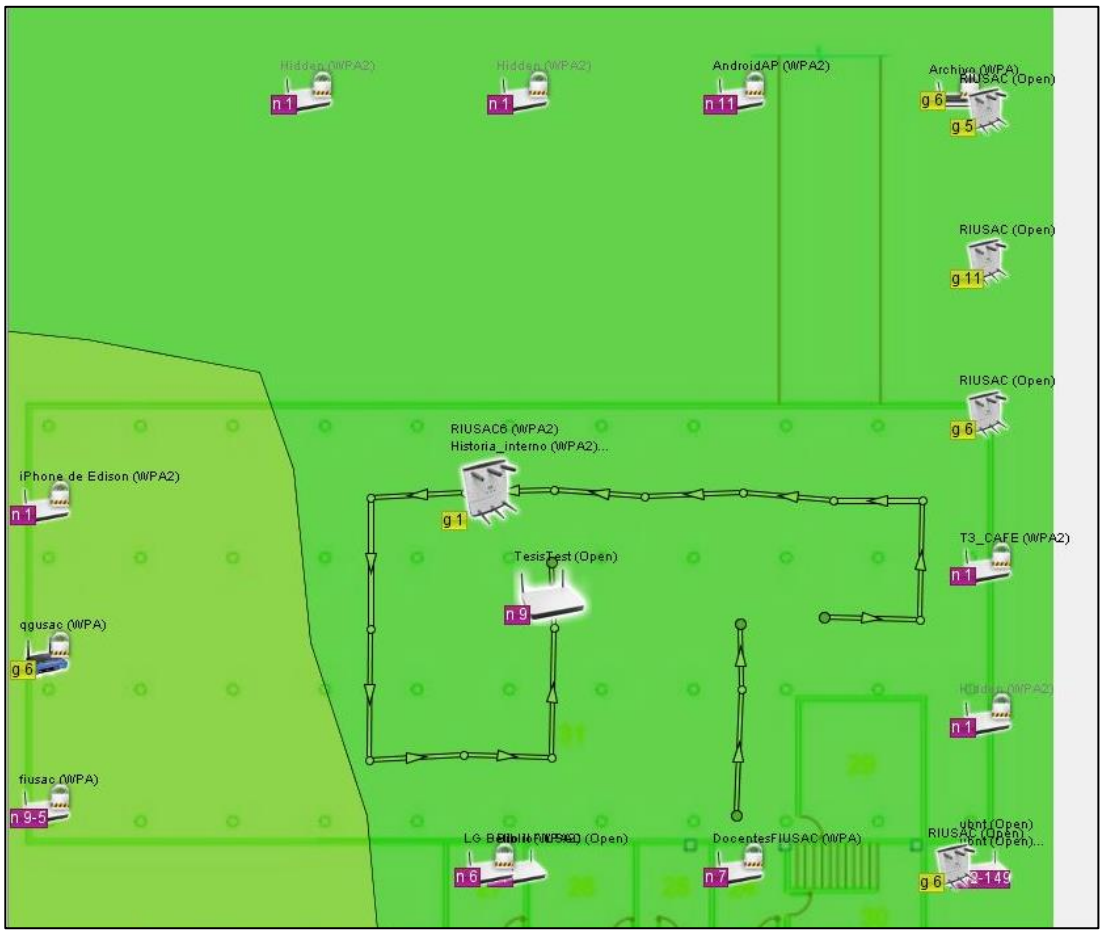
Fuente: elaboración propia.

Figura 76. **SSID RIUSAC en el área 2**



Fuente: elaboración propia.

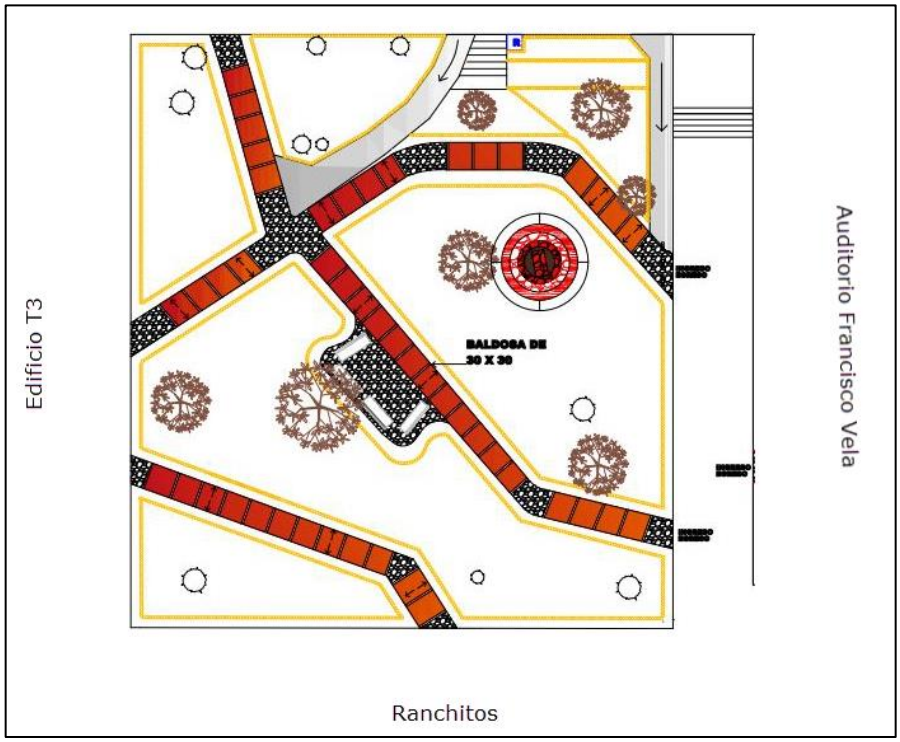
Figura 77. **SSID TESIS en el área 2**



Fuente: elaboración propia.

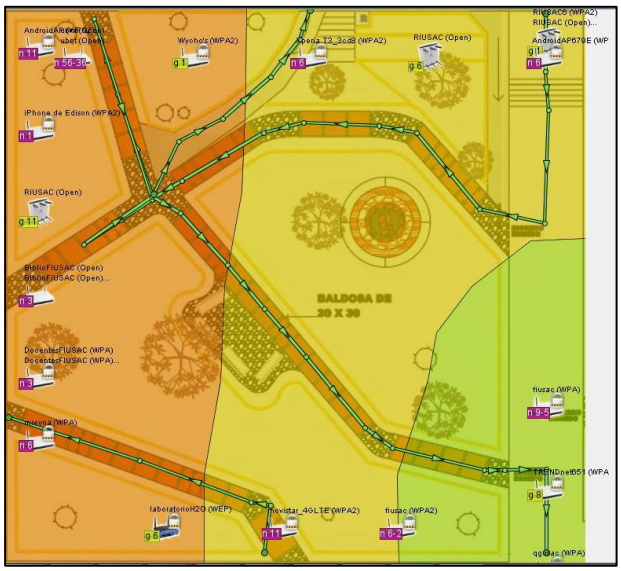
5.1.1.3. Área 3 - Jardín principal de la Facultad de Ingeniería, USAC

Figura 78. **Jardín principal de la Facultad de Ingeniería, USAC**



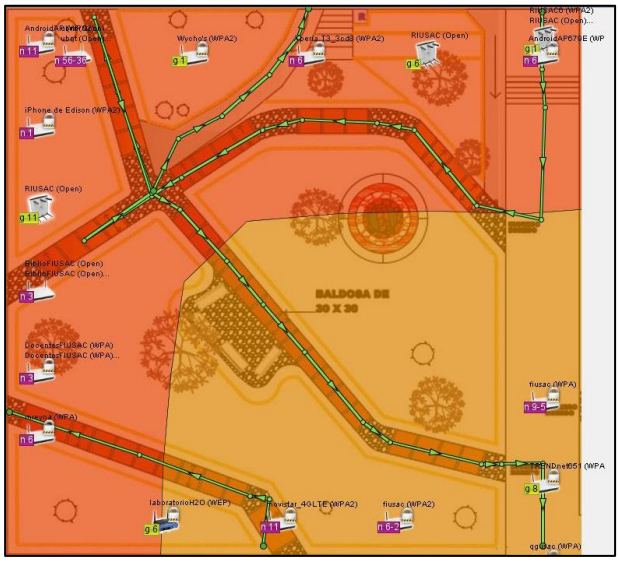
Fuente: FERNÁNDEZ, Jennyfer. *Unidad de Planificación e Infraestructura Facultad de Ingeniería, USAC.* Plano

Figura 79. **SSID FIUSAC en área 3**



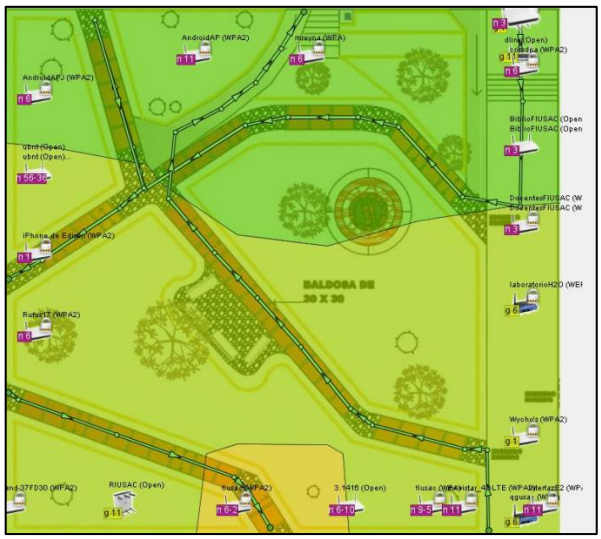
Fuente: elaboración propia.

Figura 80. **SSID RIUSAC en área 3**



Fuente: elaboración propia.

Figura 81. **SSID TESIS en el área 3**



Fuente: elaboración propia.

5.1.1.4. Área 4 - Los Ranchitos de ingeniería

Figura 82. **Los ranchitos de ingeniería**

Fuente: FERNÁNDEZ, Jennyfer. *Unidad de Planificación e Infraestructura Facultad de Ingeniería, USAC*. Plano

Figura 83. **SSID FIUSAC en el área 4**

Fuente: elaboración propia.

Figura 84. **SSID RIUSAC en el área 4**

Fuente: elaboración propia.

Figura 85. **SSID TESIS en el área 4**

Fuente: elaboración propia.

En los mapas de calor obtenidos; se observa que la señal de los SSIDs principales no tiene la potencia necesaria para que los usuarios tengan una buena experiencia. En los mapas de calor con la SSID de Tesis se observa que la señal se propaga adecuadamente en el área con solo un AP irradiando.

Se determina la utilización de 4 *access points* para cubrir completamente el área propuesta, también se toma en cuenta la cantidad de estudiantes promedio en días cotidianos para determinar la cantidad de APs a utilizar. La ubicación de cada AP se establecerá en el diseño propuesto expuesto más adelante.

Según la investigación de observación llevada a cabo en el área propuesta se obtiene la siguiente tabla, en donde se establece la cantidad de usuarios aproximados en las distintas sub-áreas.

Tabla X. **Reporte del estudio de sitio**

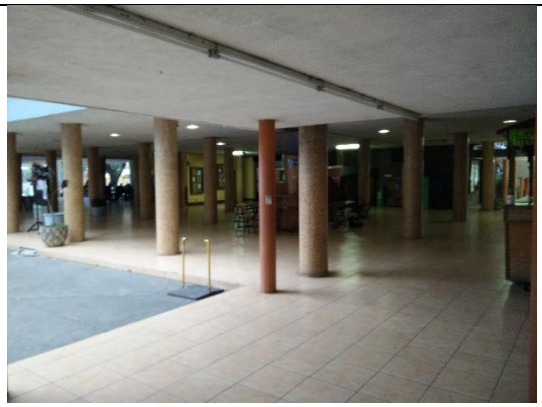
IMPLEMENTACION RED *WIRELESS* **PROPUESTA PARA OPTIMIZAR LA RED IEEE 802.11 EN EL ÁREA DE RECREACIÓN DE LA FACULTAD DE INGENIERÍA, USAC**

FECHA OBSERVACIÓN:	Noviembre 2015 - Septiembre 2016	**HORA SS:**	2:00 PM
LUGAR:	Facultad de ingeniería - Universidad San Carlos de Guatemala	**ELABORADO POR:**	Angelo Caal
# NIVELES	1		
# AREAS DE ESTAR:	4		
# PATIO DE COMIDAS:	0		
TOTAL DE AREAS A CUBRIR:	4		

NIVEL#	AREA#	DESCRIPCIÓN DE AREA	CANTIDAD DE USUARIOS	AREA A CUBRIR
1	1	Área de estar, área de columnas extensión, Rectangular/ Interior	100	12.7m x 19.5m
1	2	Área de estar, área de columnas, Rectangular/ Interior	100	27.5m x 8m
1	3	Área de estar, jardín principal de la Facultad de Ingeniería USAC, Rectangular/ Exterior	25	31.9m x 16.8m
1	4	Área de estar, los ranchitos de Ingeniería, Rectangular/ Exterior	80	37.6m x 21.36m

Fuente: elaboración propia.

Figura 86. **Áreas propuestas para el diseño de la red *wireless***

Área #1 –Plaza columnas extensión	**Área #2 –Plaza columnas**
	
Área #3 - Jardín principal de la Facultad de Ingeniería USAC	**Área #4 - Los ranchitos de Ingeniería**
	

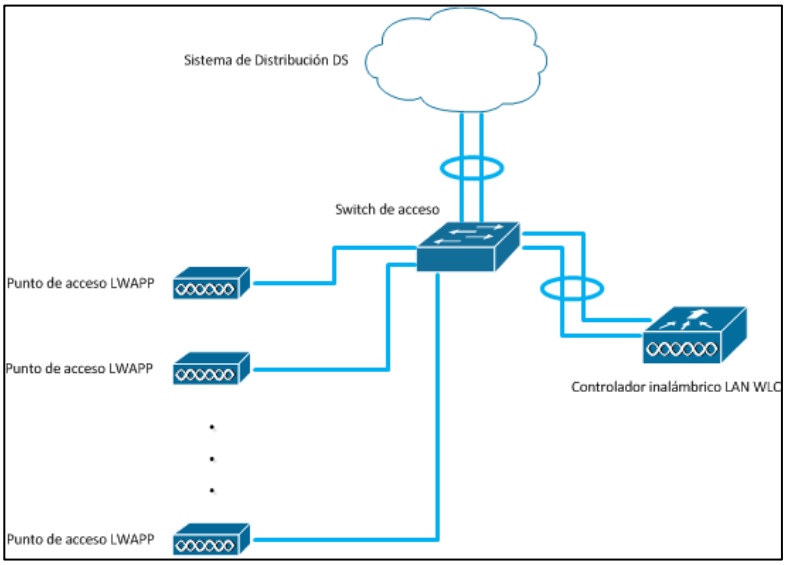
Fuente: elaboración propia.

5.2. Diagrama red inalámbrica HLD (*high level design*)

El diseño general de la propuesta para la red inalámbrica se presenta en el siguiente diagrama, se exponen las conexiones entre dispositivos para implementar la solución y lograr la comunicación con el *Core* de la Facultad de Ingeniería USAC. Un *switch* de acceso con tecnología PoE suministra la energía por el mismo cable que se envían los datos a los LWAPP, la cantidad

de LWAPP depende del área a cubrir y el estudio de sitio que se realiza. Se configura dos *port-channel* en el *switch*, uno hacia el sistema de distribución o *Core*, el otro es la conexión hacia el controlador de *wireless*.

Figura 87. **Diagrama general del diseño *wireless***



Fuente: elaboración propia, utilizando Microsoft Visio.

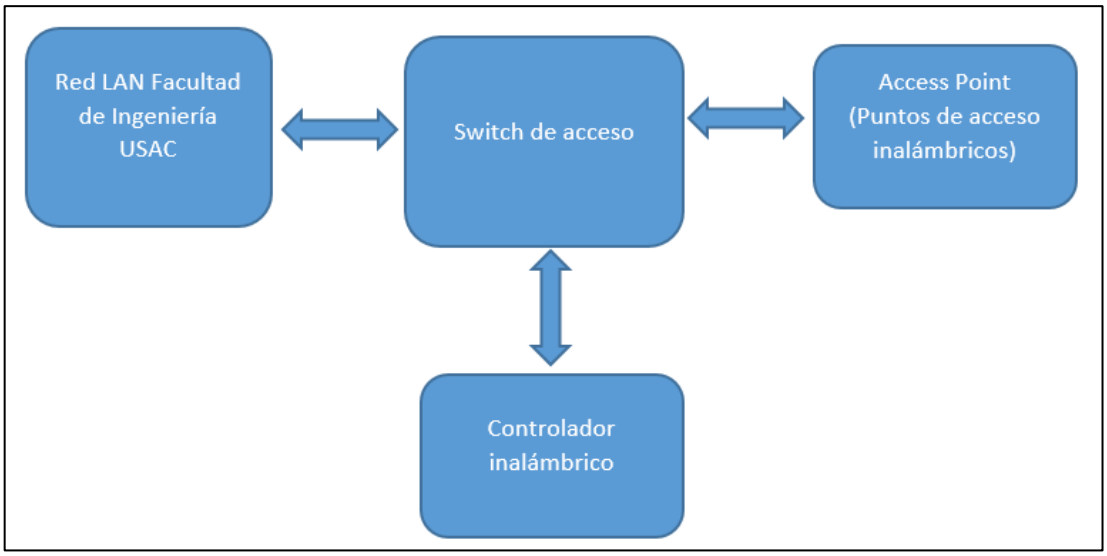
Las partes principales que componen el diseño propuesto son:

- La red LAN o cableada de la Facultad de Ingeniería, USAC
- *Switch*es de acceso
- *Access points*
- Controlador WLA

La comunicación entre las partes del diseño se presenta en el siguiente diagrama, en donde el punto en común donde el tráfico de datos debe pasar en el *switch* de acceso, este comunica y une la red LAN ya existente de la Facultad

de Ingeniería USAC, los *Access points* instalados a través del área a cubrir y el controlador inalámbrico. Esta comunicación se da a nivel de capa 1 y capa 2, la capa uno son los bits enviados por cada equipo por medio de señales eléctricas o potencias dentro de una fibra, la capa 2 es donde la comunicación se da por direcciones MAC y en donde se deben comunicar primero con los equipos conectados directamente a ellos antes de llegar a su destino.

Figura 88. **Diagrama de la comunicación capa 1 y capa 2**



Fuente: elaboración propia.

A nivel de capa 3 se tiene otro diagrama, tiene las mismas partes principales (a excepción del *switch* de acceso), sin embargo, la comunicación entre estas partes es distinta y más directa entre tecnologías para evitar mayor trabajo y dar mayor seguridad en la transmisión de datos, logrando una mejor eficiencia en todo el diseño. Se observa que el *switch* ya no interviene en la comunicación a nivel de capa 3, aquí se utiliza direccionamiento IP, el papel del *switch* de acceso lo toma el controlador inalámbrico, es el encargado de

intercambiar los datos entre la red LAN y los *access point* en caso sea necesario, de lo contrario la comunicación queda entre controlador inalámbrico y *access point*. El controlador levanta un túnel directamente con los AP, así el tráfico solo puede ser descifrado entre los dos, el controlador también se comunica con la red cableada de la facultad para poder tener datos de los servidores y enrutamiento entre segmentos de red.

Figura 89. **Diagrama de la comunicación capa 3**

Fuente: elaboración propia.

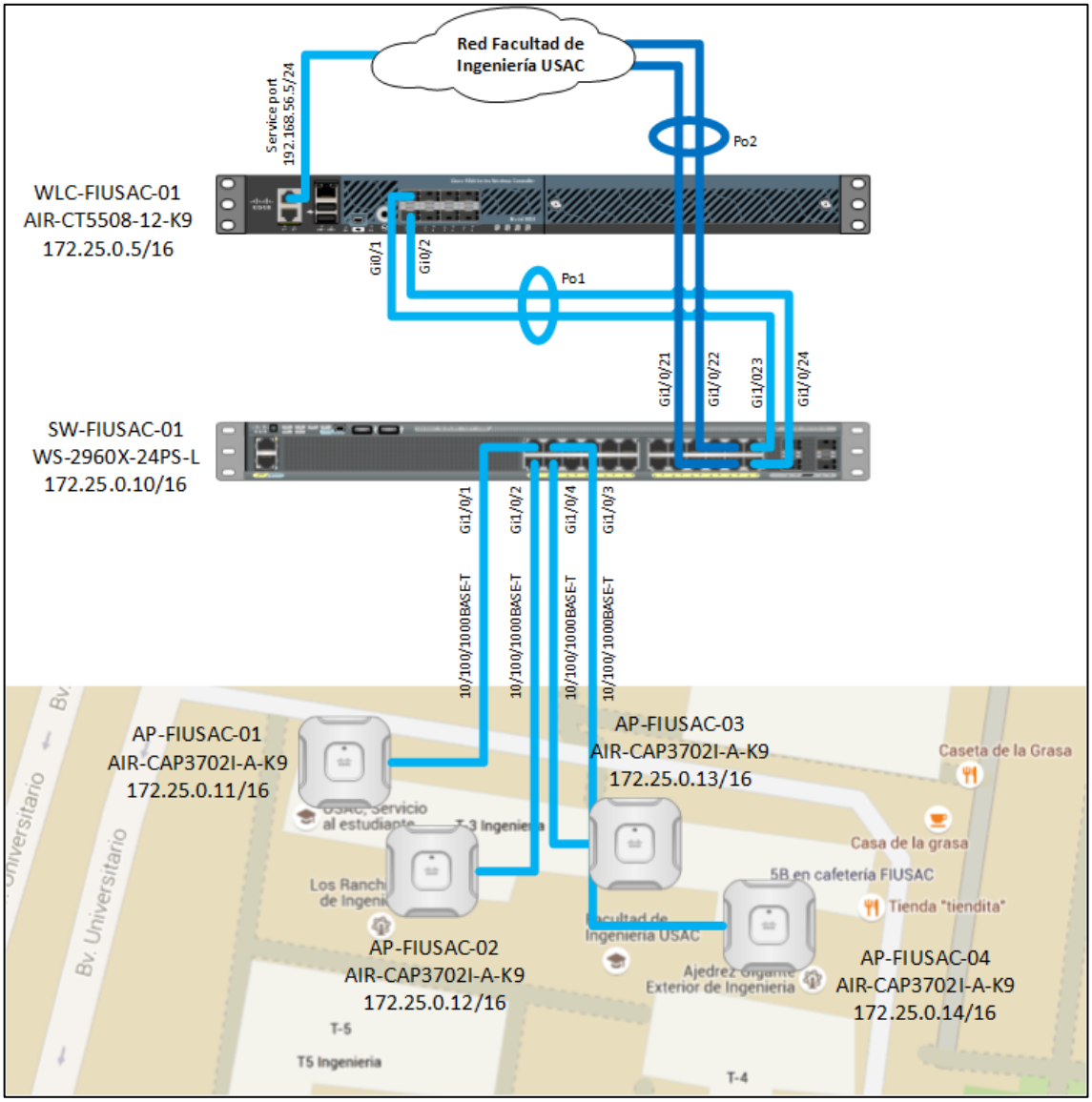
5.3. Diagrama red inalámbrica LLD (*low level design*)

La siguiente sección del diseño se compone por la descripción funcional y física de los equipos específicos a utilizar, el diagrama a detalle de la solución, la configuración de los equipos para que el sistema propuesto funcione adecuadamente y acorde lo diseñado.

5.3.1. Conexiones físicas entre equipos

El diseño propuesto se observa en la siguiente imagen, se presentan las conexiones entre equipos: controlador, *switch*, AP's y red de la facultad de ingeniería USAC. Así también los puertos, direcciones, *hostnames* y equipos Cisco a utilizar.

Figura 90. **Diagrama detallado de la red *wireless***



Fuente: elaboración propia, utilizando Microsoft Visio.

En la siguiente tabla se presentan los segmentos, VLAN y direcciones IP a utilizar para las interfaces del controlador.

Tabla XI. **Direccionamiento IP de las interfaces WLC**

Interfaz	VLAN	Segmento de red	Dirección IP	Default gateway
Wireless admin	360	172.26.0.0/16	172.26.0.5/16	172.26.0.1/16
Wireless estudiantes	361	172.27.0.0/16	172.27.0.5/16	172.27.0.1/16
Interfaz virtual	N/A	N/A	1.1.1.1/32	N/A
Interfaz de administración	561	172.25.0.0/16	172.25.0.5/16	172.25.0.1/16
Puerto de servicio	9	192.168.56.0/24	192.168.56.5/24	192.168.56.1/24

Fuente: elaboración propia.

En la siguiente tabla se especifican los *hostnames*, direcciones IP de administración (VLAN 561) y modelos de equipos.

Tabla XII. **Direccionamiento IP para la gestión de los equipos**

Hostname	Equipo/Modelo	Direccionamiento IP
WLC-FIUSAC-01	AIR-CT5508-12-K9	172.25.0.5/16
SW-FIUSAC-01	WS-2960X-24PS-L	172.25.0.10/16
AP-FIUSAC-01	AIR-CAP3702I-A-K9	172.25.0.11/16
AP-FIUSAC-02	AIR-CAP3702I-A-K9	172.25.0.12/16
AP-FIUSAC-03	AIR-CAP3702I-A-K9	172.25.0.13/16
AP-FIUSAC-04	AIR-CAP3702I-A-K9	172.25.0.14/16

Fuente: elaboración propia.

5.3.2. *Switch* Cisco Catalyst 2960X-24PS-L

Se propone utilizar un *switch* Cisco Catalyst 2960X-24PS-L para interconectar los LWAPP, WLC y la red de Ingeniería USAC. El *switch* tiene la opción de conectarse con otros *switch*es para tener la opción de aumentar los puertos y administrar todos los *switch*es por medio de una sola dirección IP. Está diseñado para simplificar la operación, disminuir costos, ser escalable, seguro y eficiente a la hora de consumir energía.

Es un *switch* de 24 puertos 10/100/1000 Ethernet, con 4 interfaces *uplinks* que soportan SFP, velocidades de hasta 4.7 Gbps, en el diseño propuesto se utilizaran SFP 1000BASE-T para las conexiones necesarias. Soporta el estándar de energía 802.3af por lo tanto es un *switch* PoE y puede suministrar energía eléctrica a los LWAPP conectados a sus puertos, tiene una capacidad PoE de 370W para dividirla en sus 24 puertos.

En sus 24 puertos se utilizará cable UTP CAT6a para conectar los LWAPP y WLC, en los puertos *uplink* se colocaran SFP de cobre 1000BASE-T para utilizar cable UTP CAT6a y realizar la conexión con la red de la Facultad de Ingeniería USAC.

Para administrar y configurar el *switch* se cuenta con los puertos de consola USB y RJ45, además cuando el equipo se encuentra en la red se puede administrar por medio de conexiones SSH o TELNET.

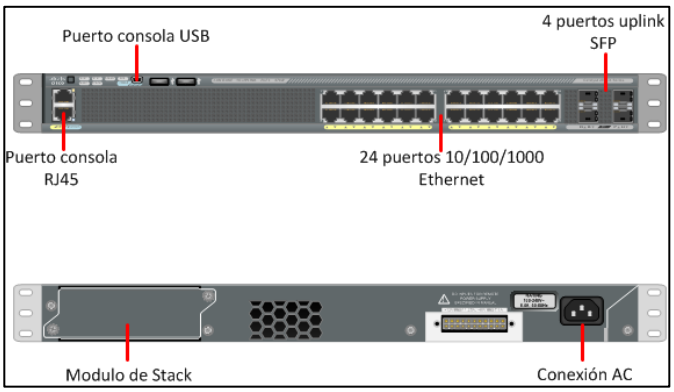
La IP de administración del *switch* debe estar en el mismo segmento de administración del WLC, se utilizará el siguiente direccionamiento:

Tabla XIII. **Direccionamiento IP para *switch* de acceso**

Interfaz	***Vlan***	***Segmento***	***Dirección IP***	***Default gateway***
Vty	561	172.25.0.0/16	172.26.0.10/16	172.26.0.1/16

Fuente: elaboración propia.

Figura 91. ***Switch* Cisco Catalyst 2960X-24PS-L**



Fuente: elaboración propia, utilizando Microsoft Visio.

5.3.2.1. Configuración *switch*Cisco Catalyst 2960X-24PS-L

Se aplica la configuración para comunicación con LWAPP, WLC y red de Ingeniería USAC, se configura dos *port-channel*s para comunicación con la red y configuración básica para gestión del equipo.

Configuración general:

SW1#configure terminal	entra en modo de configuración por consola
Enter configuration commands, one per line.SW1(config)#hostname SW-FIUSAC-01	End with CNTL/Z. se configura el nombre del equipo
SW-FIUSAC-01(config)#line vty 0-15	se ingresa en modo configuración línea virtual

SW-FIUSAC-01(config-line)#login local	se indica que el usuario debe ser local
SW-FIUSAC-01(config)#username admin privilege 15 password contrasena	se configura el usuario y contraseña para ingresar al equipo
Puertos del *switch* hacia LWAPP	
Interface range GigabitEthernet 1/0/1-4	rango de interfases a configurar
description "Link To LWAPP"	descripción de las interfases
*switch*port access vlan 561	interfaces modo acceso en VLAN 561
*switch*port mode access	
spanning-tree portfast	interfaces levantan instantáneamente al conectar el cable en los puertos
Puertos del *switch* hacia WLC	
Interface*port-channel* 1	grupo de interfases etherchannel
description "Link To WLC"	descripción del portchannel
*switch*port mode trunk	portchannel modo troncal
Interface range GigabitEthernet 1/0/23-24	rango de interfases a configurar
description "Link To WLC"	descripción de las interfaces
*switch*port mode trunk	interfaces modo troncal
channel-group 1	interfaces son parte del portchannel #1

Hacia Red de la Facultad de Ingeniería USAC	
Interface*port-channel* 2	grupo de interfases etherchannel
description "Link USAC Engineer Network"	descripción del portchannel
*switch*port mode trunk	portchannel modo troncal
Interfase range GigabitEthernet 1/0/21-22	rango de interfaces a configurar
description "Link USAC Engineer Network"	descripción de las interfases
*switch*port mode trunk	interfaces modo troncal
channel-group 2	interfaces son parte del portchannel #2

5.3.3. Puntos de acceso Cisco Aironet 3702i

Se propone utilizar *access points* Aironet de la serie 3700, el modelo 3702i. Los AP soportan alta densidad de datos, mejora la forma del rayo que irradia para mejorar la experiencia del usuario.

Características y capacidades

- Velocidad de datos máxima de 1,3 Gbps.
- Tiene capacidad de 200 clientes por radio.
- Soporta 802.11ac de la primera versión, soporta antenas 4x4 MIMO.
- Utiliza tecnología CleanAir para evitar interferencias, soporta canales de 80MHz.
- Utiliza dos radios para las bandas de 2,4 y 5 GHz, y soporta el crecimiento de BYOD (*Bring your own device*) y la demanda en ancho de banda.
- Opción para habilitar módulo de la versión 2 de 802.11ac.

Los AP traen precargado el IOS (*Internetwork operating system*) de LWAPP, el cual al conectarse a la red busca un controlador a cuál vincularse y descargar toda la información necesaria: actualizaciones, *update* del sistema, configuración, certificados, entre otros.

Posee un puerto serial para configuración inicial y acceso a la consola del AP, un puerto Ethernet que es conectado al *switch* de acceso, por donde se transmitirán los datos hacia el *core* y también se suministrara la energía al AP. También tiene una conexión de 48V DC como opción alternativa de suministro de energía. La configuración inicial se realiza por el puerto de consola, al vincularse con el controlador, toda la configuración y administración se realiza desde el controlador *wireless* en una interfaz gráfica, si es necesario se puede habilitar SSH o Telnet en los AP.

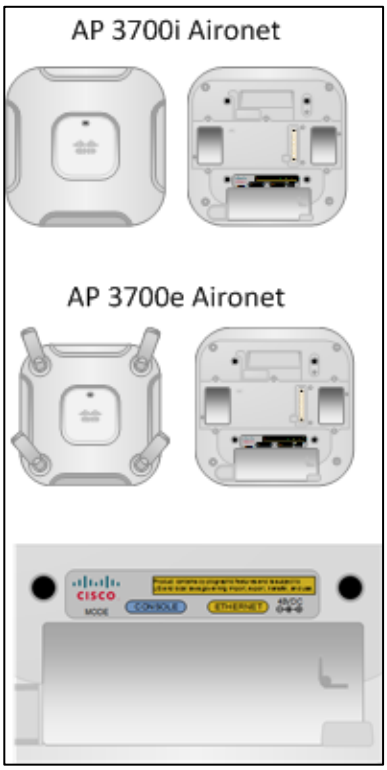
Los detalles del *access points* se establecen en la siguiente tabla:

Tabla XIV. **Direccionamiento IP para los *access points***

Hostname	Interfaz	Vlan	Segmento	Dirección IP	Default gateway
AP-FIUSAC-01	BVI1	561	172.25.0.0/16	172.26.0.11/16	172.26.0.1/16
AP-FIUSAC-02	BVI1	561	172.25.0.0/16	172.26.0.12/16	172.26.0.1/16
AP-FIUSAC-03	BVI1	561	172.25.0.0/16	172.26.0.13/16	172.26.0.1/16
AP-FIUSAC-04	BVI1	561	172.25.0.0/16	172.26.0.14/16	172.26.0.1/16

Fuente: elaboración propia.

Figura 92. ***Access point* serie 3700**



Fuente: elaboración propia, utilizando Microsoft Visio

5.3.3.1. Instalación física de los *access points*

La ubicación física de la instalación de los *access points* está basado en el *site survey* realizado en el área que se necesita cobertura de la red inalámbrica, se necesitarán cuatro (4) *access points* para lograr cubrir las diferentes sub-áreas involucradas en el diseño de la red.

La implementación física de los *access points* y conexiones de las interfaces del *switch* de distribución consisten en la siguiente lista e imágenes:

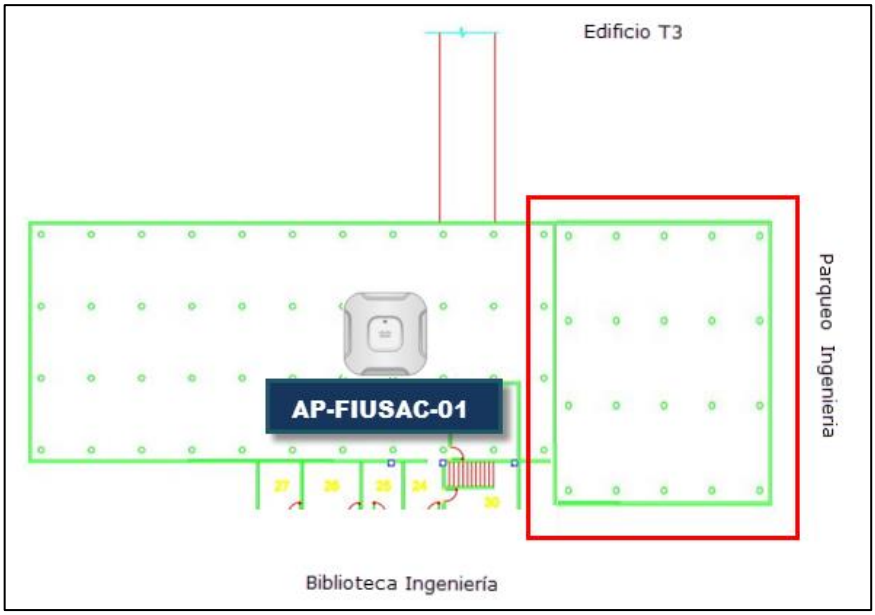
Tabla XV. **Listado de *acccess points***

Hostname	Dirección IP	Modelo AP	VLAN	*Switch* acceso	Puerto
AP-FIUSAC-01	172.25.0.11	AIR-CAP3502I-A-K9	140	SW-FIUSAC-01	Gi1/0/1
AP-FIUSAC-02	172.25.0.12	AIR-CAP3502I-A-K9	140	SW-FIUSAC-01	Gi1/0/2
AP-FIUSAC-03	172.25.0.13	AIR-CAP3502I-A-K9	140	SW-FIUSAC-01	Gi1/0/3
AP-FIUSAC-04	172.25.0.14	AIR-CAP3502I-A-K9	140	SW-FIUSAC-01	Gi1/0/4

Fuente: elaboración propia.

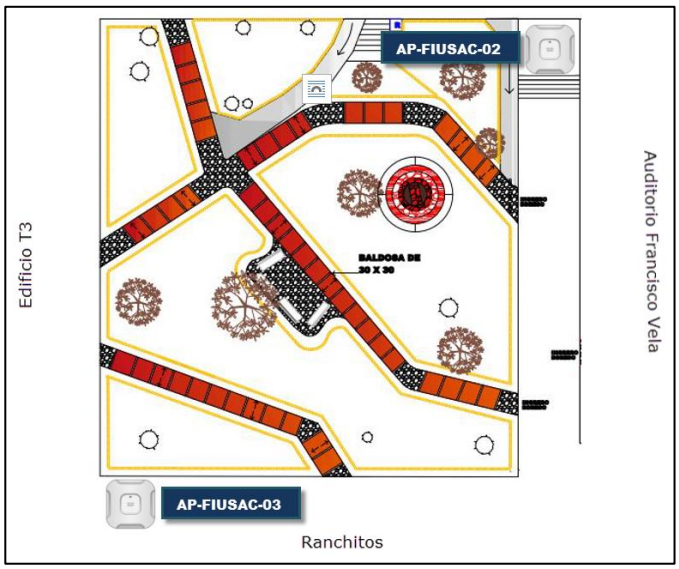
A continuación, se establece la ubicación física de los AP en el área de recreación, se utilizan los planos obtenidos del área Unidad de Planificación e Infraestructura Facultad de Ingeniería/USAC. Con la ubicación propuesta se obtiene una cobertura optimizada, logrando tener las celdas intercaladas de la mejor forma para evitar interferencias.

Figura 93. **Ubicación de *access point* AP-FIUSAC-01**



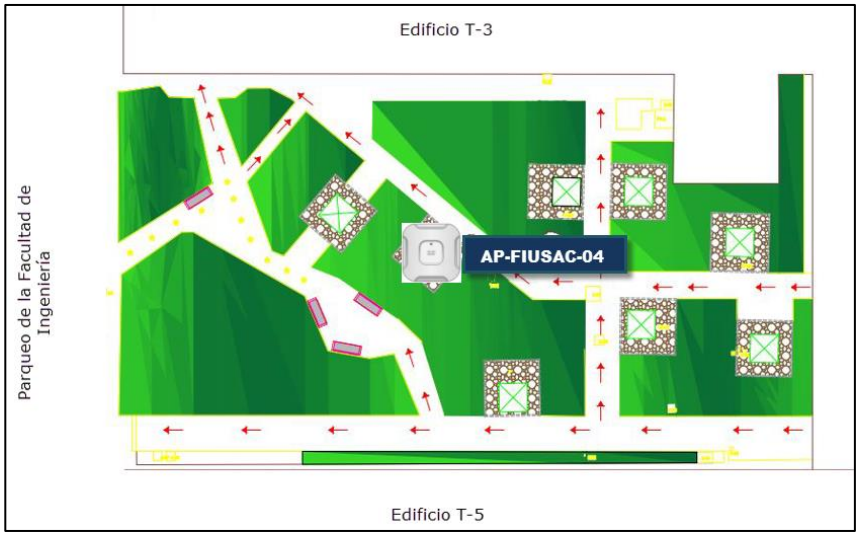
Fuente: elaboración propia.

Figura 94. **Ubicación de *access points* AP-FIUSAC-02 y 03**



Fuente: elaboración propia.

Figura 95. **Ubicación de *access point* AP-FIUSAC-04**



Fuente: elaboración propia.

5.3.3.2. Configuración punto de acceso

A continuación, la configuración básica para que el AP pueda autenticarse con el WLC y descargar la actualización de imagen, también obtener la información necesaria para su funcionamiento en la red inalámbrica.

capwap ap *Controller* ip address 172.25.0.5	IP del WLC
capwap ap ip address <ip_address><255.255.0.0>	IP del AP
capwap ap ip default-gateway 172.25.0.1	Gateway para el AP
capwap ap hostname <hostname>	Nombre del AP

5.3.4. Controlador inalámbrico LAN Cisco 5508

Se propone la utilización de un Cisco 5508 *WirelessController*, es un dispositivo con un rendimiento confiable, flexiblidad mejorada, y sin tiempos muertos en el servicio, ideal para una red *wireless* crítica. Se puede aplicar politicas QoS (*quality of service*) para darle prioridad a las aplicaciones interactivas y de multimedia, voz y video. Los clientes pueden hacer *roaming* sin interrupción del servicio.

Máximo rendimiento y escalabilidad

- Soporta hasta 500 *access points* y 7000 clientes
- Soporta redes 802.11n y 802.11ac
- Capacidad de administrar 500 AP simultáneamente

Mejoras en la movilidad y servicio

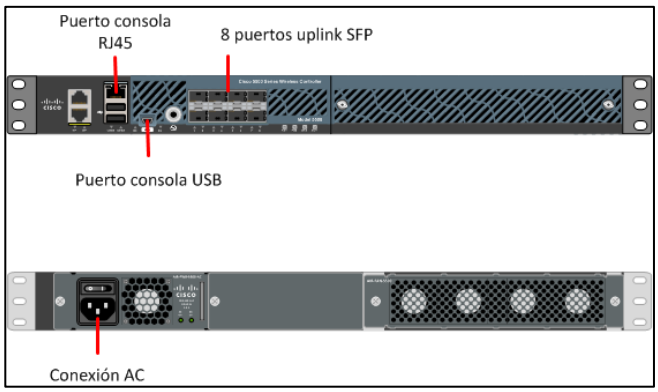
- Conexiones confiables en los ambientes más demandantes

- Áreas de cobertura mayores para aumentar conexiones a clientes simultáneamente
- *Roaming* sin interrupciones

Se administra y configura por medio de una interfaz gráfica para mayor comodidad y facilidad. Además, se tiene la típica consola por medio de los puertos USB y RJ45, y conexiones SSH y Telnet.

Posee 8 puertos *uplink* SFP, se utilizarán 2 módulos SFP GLC-T 1000BaseT para realizar la conexión con el *switch*2960X-24PS-L, en la configuración se tendrá un *port-channel* aumentando el ancho de banda y disponibilidad. La configuración de las interfaces ya se estableció anteriormente.

Figura 96. **Cisco WLC 5508**



Fuente: elaboración propia, utilizando Microsoft Visio.

Tabla XVI. **Datos técnicos del WLC Cisco 5508**

Datos técnicos Cisco WLC 5508	
Máximo de clientes soportados	7000
Máximo de *access points* soportados	500
Bandas *Wireless* soportadas	IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11k, 802.11n, 802.11r, 802.11u, 802.11w, 802.11ac.
Cifrado de seguridad	• WEP y TKIP-MIC: RC4 40, 104 and 128 bits • AES: CBC, CCM, CCMP • DES: DES-CBC, 3DES • SSL y TLS: RC4 128-bit y RSA 1024- y 2048-bit • DTLS: AES-CBC • IPSec: DES-CBC, 3DES, AES-CBC
Medios de administración	• Por página web: HTTP/HTTPS • Interfaz línea de comando CLI: Telnet, Secure Shell (SSH), Puerto serial. • Cisco *Wireless* Control System (WCS)
Interfaces e indicadores	• Puertos: 8 puertos con opción de utilizar transceivers de cobre 1000BaseT o fibra 1000Base-SX y 1000Base-LH • Service Port (Puerto de servicio): 10/100/1000 Mbps Ethernet (RJ45). • Puerto de consola: RS232 (DB-9 macho / conector RJ-45), mini-USB • Indicadores LED: Sys, ACT, Fuente de poder 1, Fuente de poder 2
Físico y ambiental	• Dimensiones (AnchoxProfundidadxAlto): 17.30 x 21.20 x 1.75 in. (440 x 539 x 44.5 mm) • Peso: 20 lbs (9.1 kg) con 2 fuentes de poder • Temperatura: Temperatura de funcionamiento: 32 a 104°F (0 a 40°C); Temperatura de almacenaje: -13 to 158°F (-25 to 70°C) • Alimentación: 100 a 240 VAC; 50/60 Hz; 1.05 A a 110 VAC, 115W Máximo; 0.523 A a 220 VAC, 115W Máximo

Fuente: *Data sheet Cisco 5500 Series WirelessControllers*.http://www.cisco.com/c/en/us/products/collateral/*wireless*/5500-series-*wireless-Controller*s/data_sheet_c78-521631.html. Consulta: 11 de octubre de 2016.

5.3.4.1. Instalación física del WLC

En la implementación del WLC (*Wireless* LAN *Controller*) se diseña la instalación en el cuarto de comunicaciones IT de la Facultad de Ingeniería USAC ubicado en el edificio T4 en el departamento de Centro de Cálculo.

Para lograr la administración de la red independientemente de las redes para maestros y estudiantes de la Facultad de Ingeniería USAC y de la red de visitantes se definieron diferentes VLAN para servicios y administración en los puertos del *switch* de acceso, WLC y *Access points*, a continuación, se explica:

El Cisco WLC 5508 se conectará al *switch* de distribución 2960 por un *port-channel* compuesto por dos interfaces Gigabit, y el *switch* se conectará al *Core* de la red de la Facultad de Ingeniería, también se conectará mediante un *port-channel* compuesto por dos interfaces Gigabit cada uno.

Las conexiones troncales del *Core* hacia el *switch* de distribución, y del *switch* de distribución al WLC son las siguientes:

Se conectarán los puertos Gi1/0/21 y Gi1/0/22 del *switch* de distribución Cisco2960 al *Core* de la Facultad de Ingeniería y los puertos Gi1/0/23 y Gi1/0/24 del *switch* de distribución Cisco 2960 se conectarán al WLC 5508 en las interfaces Gi0/1 y Gi0/2.

En el *Core* y equipos de la red *wireless* se deberá configurar la VLAN de administración 140, la VLAN para maestros y estudiantes de la Facultad de Ingeniería 156 y la VLAN para visitantes 157.

Tabla XVII. **Direccionamiento IP para WLC**

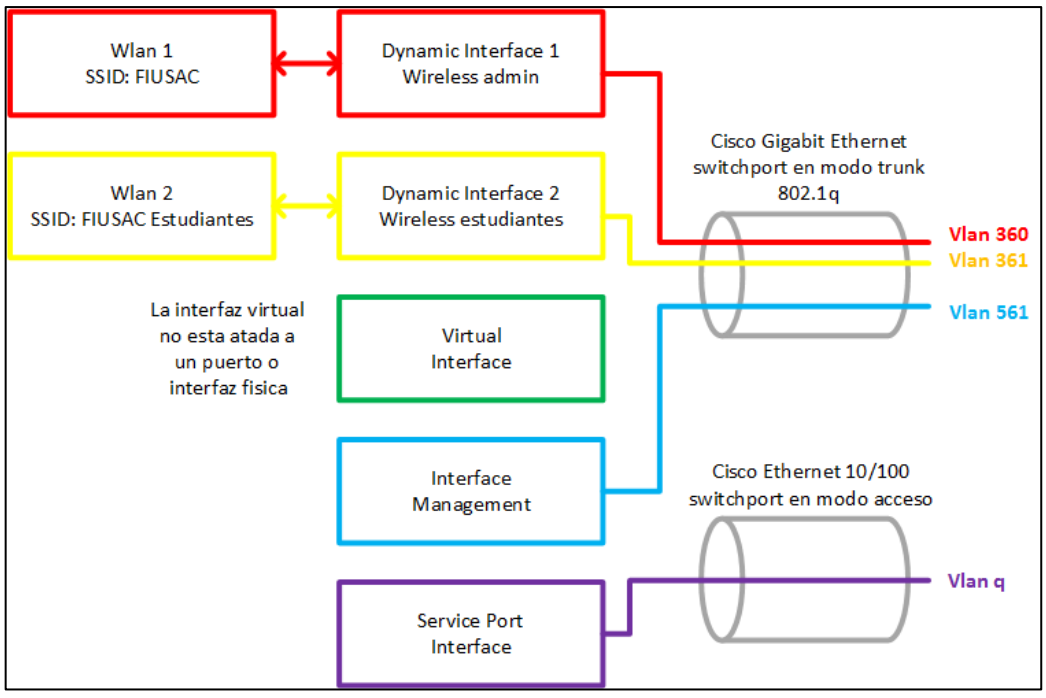
Modelo	Hostname	Dirección IP	Ubicación
WLC-CISCO 5508	WLC-FIUSAC-01	172.25.0.10/16	Centro de Cálculo. IT Room

Fuente: elaboración propia.

5.3.4.2. Interfaces del wireless LAN *Controller* WLC

El siguiente diagrama interno del controlador de red inalámbrica indica las interfaces lógicas y físicas del controlador, como van agrupadas y en que segmento ira el tráfico, identificado con un número de Vlan.

Figura 97. **Configuración interna del WLC**



Fuente: elaboración propia.

La SSID FIUSAC será una de las redes *wireless* que se implementará a la facultad de Ingeniería USAC, en esta red se conectará el personal administrativo y personas con mayor prioridad, ya que esta red estaría configurada con QoS, se le daría prioridad al tráfico de datos, evitando así retrasos y restricción en ancho de banda. La SSID se vincula a la interfaz dinámica con nombre *Wireless* admin, la cual sale por la Vlan 360 hacia la red de la Facultad de Ingeniería.

La otra SSID, FIUSAC Estudiantes, es la otra red *wireless* que se utilizará para los estudiantes, y personal en general, incluyendo visitantes de la facultad de ingeniería USAC. La SSID de estudiantes se vincula con la interfaz dinámica wireless estudiantes, la cual tiene encapsulamiento de Vlan 361.

La interfaz virtual, como su nombre lo dice, es virtual, no se asocia a ningún puerto físico del controlador, y se utiliza para opciones de movilidad cuando se tiene en la red más controladores *wireless*.

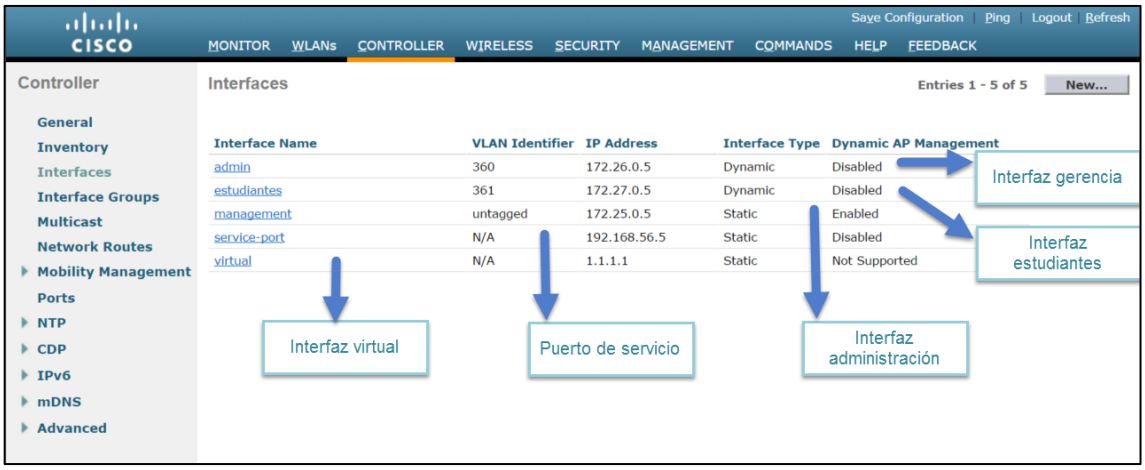
La interfaz de administración es la encargada de recibir los paquetes provenientes de los AP y clientes de la red *wireless*, tiene la única ip del controlador a la cual se le puede hacer ping. Los datos salen etiquetados con la Vlan 561 por los puertos del controlador.

El puerto de servicio se utiliza para la administración y configuración fuera de banda OOB (*out of band*), se conecta a una red utilizada para alcanzar al equipo en caso de que la red principal no funcione correctamente. La Vlan de estos paquetes dependerá de la red existente en la Facultad de Ingeniería, por lo tanto asumiremos la VLAN 9.

Los datos de las dos redes inalámbricas y de la interfaz de administración se encapsulan (802.1q), y se envían a través de los puertos Ethernet que tiene el controlador, estos puertos están configurados en modo trunk, con la capacidad de separar tráfico de datos por VLAN.

Para dispositivos *wireless*, la controladora es un puente 802.1q que toma el tráfico del aire y lo asigna a una VLAN. Desde la perspectiva de un AP, la controladora es un túnel CAPWAP desde el AP hasta la IP del WLC. Desde la perspectiva de la red, la controladora es un dispositivo de capa 2 conectado por uno o más troncales 802.1q.

Figura 98. **Interfaces del WLC 5508**



Fuente: elaboración propia.

5.3.4.3. Configuración inicial del WLC

La configuración inicial en el controlador es básica, direccionamiento IP, direcciones de servidores NTP, RADIUS, posteriormente se configura por medio

de GUI. A continuación, la información necesaria para poner en funcionamiento el WLC.

Username : root
Password : Fiusac2015
Service Port : static
None para deshabilitar el Puerto de servicio, *static* para establecer una IP estática al Puerto de servicio. Escribimos *static.*

Service IP : 192.168.56.5
Mask : 255.255.255.0

El Puerto de servicio en un Puerto *Out of Band*, esto quiere decir que no entra a la red de producción, su función es ofrecer una interfaz para poder acceder al equipo por medio de otra red de mantenimiento.

Management IP : 172.25.0.5
Mask : 255.255.0.0
Default Router : 172.25.0.1

La IP de administración es la única IP a la que se le puede hacer PING, es la única que el WLC utiliza para poder comunicarse en la red y la única IP con la que se puede administrar y configurar el controlador.

DHCP Server IP : <IP del servidor DHCP en la red>

Virtual IP : 1.1.1.1
Esta dirección se utiliza para movilidad en ambientes más grandes, en donde se tiene varios WLC. Generalmente se coloca una IP no común.

VLAN ID : 561

Se determina la vlan de administración para la controladora

DHCP Bridging : No

Opción para el servidor DHCP, se deshabilita.

LAG : Yes

LAG es el protocolo para tener *port-channel* en las interfaces del controlador, Link *Aggregation Protocol*. Se habilita ya que se tendrá dos *uplinks* hacia el *Core*.

RF : FIUSAC

Mobility : No

SSID : FIUSAC

Ntp Server : <IP del servidor NTP>

Set TIME Now : hh:mm:ss

Set Date Now : dd/mm/yy

Se establece la hora y fecha en caso de no tener un servidor NTP en la red.

Restart and Save : Yes

Se reinicia el controlador para aplicar los cambios. Luego se podrá acceder vía HTTPS a la IP de administración para la configuración avanzada de la red *wireless*.

5.3.4.4. Configuración avanzada del WLC

Se definen interfases de administración para asegurar la gestión por medio de la página web (HTTP o HTTPS) del WLC, así mismo se utilizan para la comunicación con los *Access points*.

La definición y configuración de las interfases del WLC se determina acorde el direccionamiento de la red, donde la VLAN 360 está diseñada para los usuarios administrativos, la VLAN 361 para estudiantes y la VLAN 561 para administración.

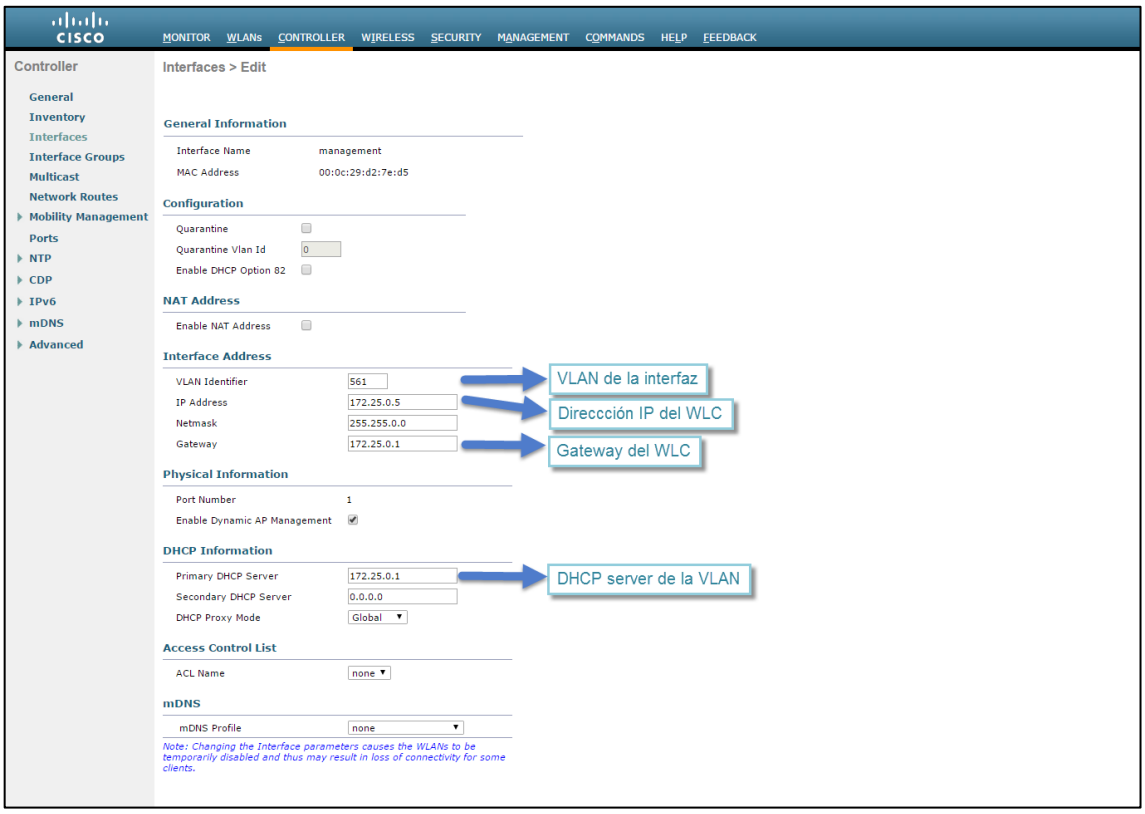
5.3.4.4.1. Interfaz de administración

La interfaz de administración es la predeterminada para ser la interfaz "*in-band*", dentro de la banda, esto significa que opera en la red de producción. Esta interfaz se utiliza para administrar el WLC y comunicarse con servidores empresariales como un servidor AAA. También es utilizada para la comunicación entre el WLC y los APs.

La interfaz de administración es la única *in-band* con IP a la que se le puede hacer "ping" o enviarle *echo request*. Se puede acceder a la GUI del controlador colocando la IP de la interfaz de administración en un explorador web, como Google Chrome o Firefox.

Para los túneles CAPWAP, la controladora necesita de una interfaz de administración para controlar toda comunicación con los dispositivos de la red y en especial con los *access points*.

Figura 99. **Interfaz de administración del WLC**



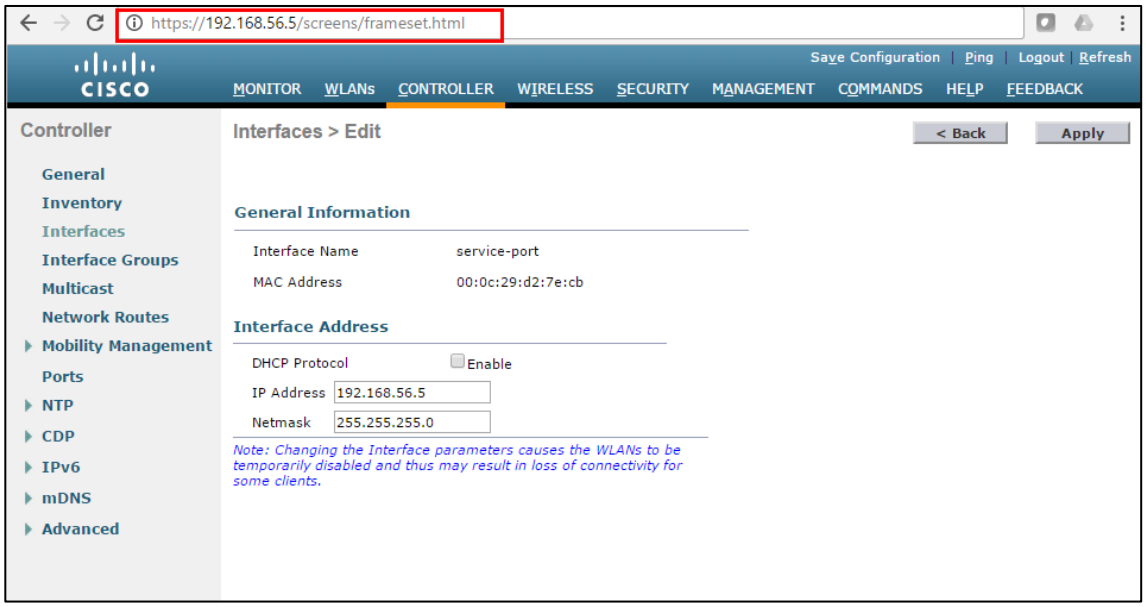
Fuente: elaboración propia.

La VLAN asignada para la interfaz de administración es la 561, el segmento es el 172.25.0.0. La configuración de la interfaz tiene la opción de habilitar una IP para redireccionar las consultas hacia un servidor DHCP y poder asignar direcciones a los usuarios. El WLC tiene la capacidad se ser un servidor DHCP, para tenerlo en uso es necesario colocar la dirección de administración como IP del servidor, sin embargo, no es recomendable utilizar el servidor DHCP del WLC como servidor principal para una red grande, puede utilizarse provisionalmente y en una red simple.

5.3.4.4.2. Puerto de servicio

Esta interfaz OOB que se utiliza para la configuración inicial del WLC y en caso se pierda comunicación con el WLC por la red *in-band* es posible ingresar por medio de la IP configurada en esta interfaz.

Figura 100. **Puerto de servicio del WLC**



Fuente: elaboración propia.

5.3.4.4.3. Interfaces dinámicas

Las interfaces dinámicas son las que se asocian con cada SSID configurada, la mejor práctica de configuración es establecer una interfaz dinámica por cada SSID, cada SSID en una VLAN diferente para apartar segmentos de red y tráfico y así mejorar la experiencia del usuario.

En el diseño de la solución propuesta se configuran dos interfases dinámicas, una para cada SSID, para la administración y otra para los estudiantes.

Figura 101. **Interfaces dinámicas del diseño**

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
admin	360	172.26.0.5	Dynamic	Disabled
estudiantes	361	172.27.0.5	Dynamic	Disabled

Fuente: elaboración propia.

Cada interfaz dinámica creada se asocia con una SSID, se realiza el cambio entre VLAN y red *wireless*.

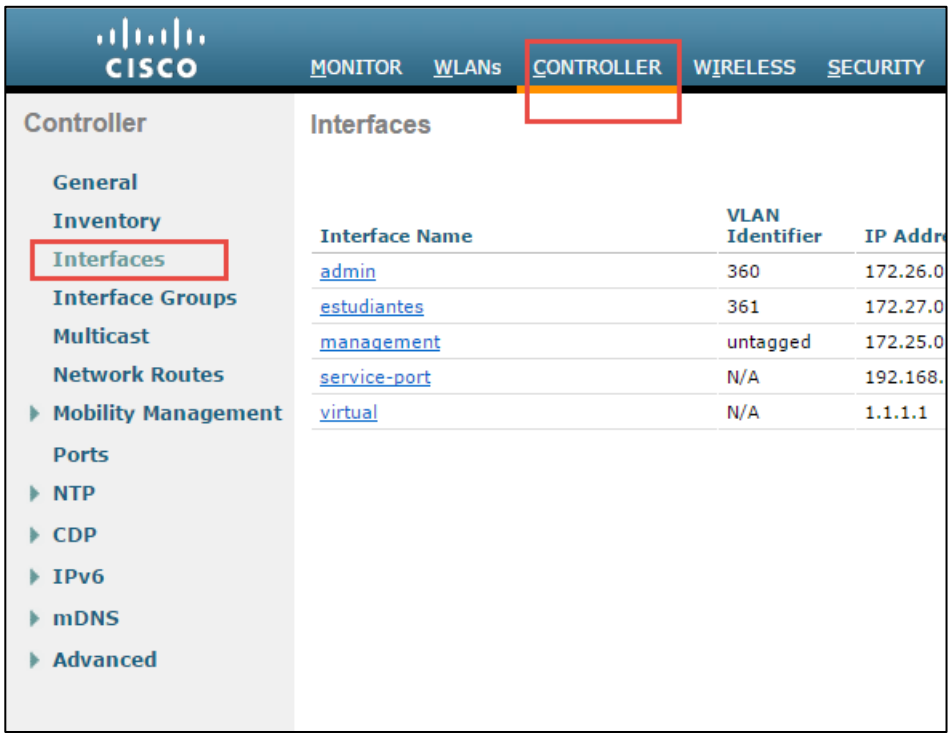
Figura 102. **Asociación interfaz dinámica – SSID**

Fuente: elaboración propia.

A continuación, se explica el procedimiento para la creación de interfaz dinámica.

- Paso 1. Se debe ingresar al área de interfaces, en la pestaña de *CONTROLLER*.

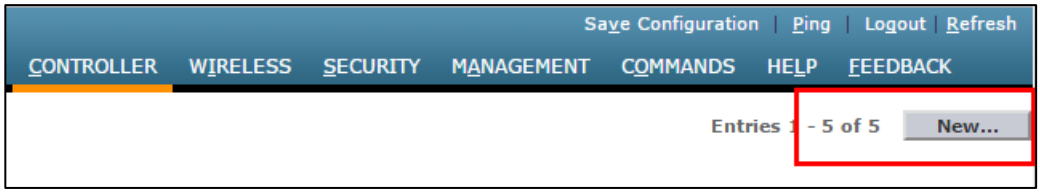
Figura 103. **Configuración interfaz dinámica paso 1**



Fuente: elaboración propia.

- Paso 2. El siguiente paso es presionar el botón de New para crear una interfaz.

Figura 104. **Configuración interfaz dinámica paso 2**



Fuente: elaboración propia.

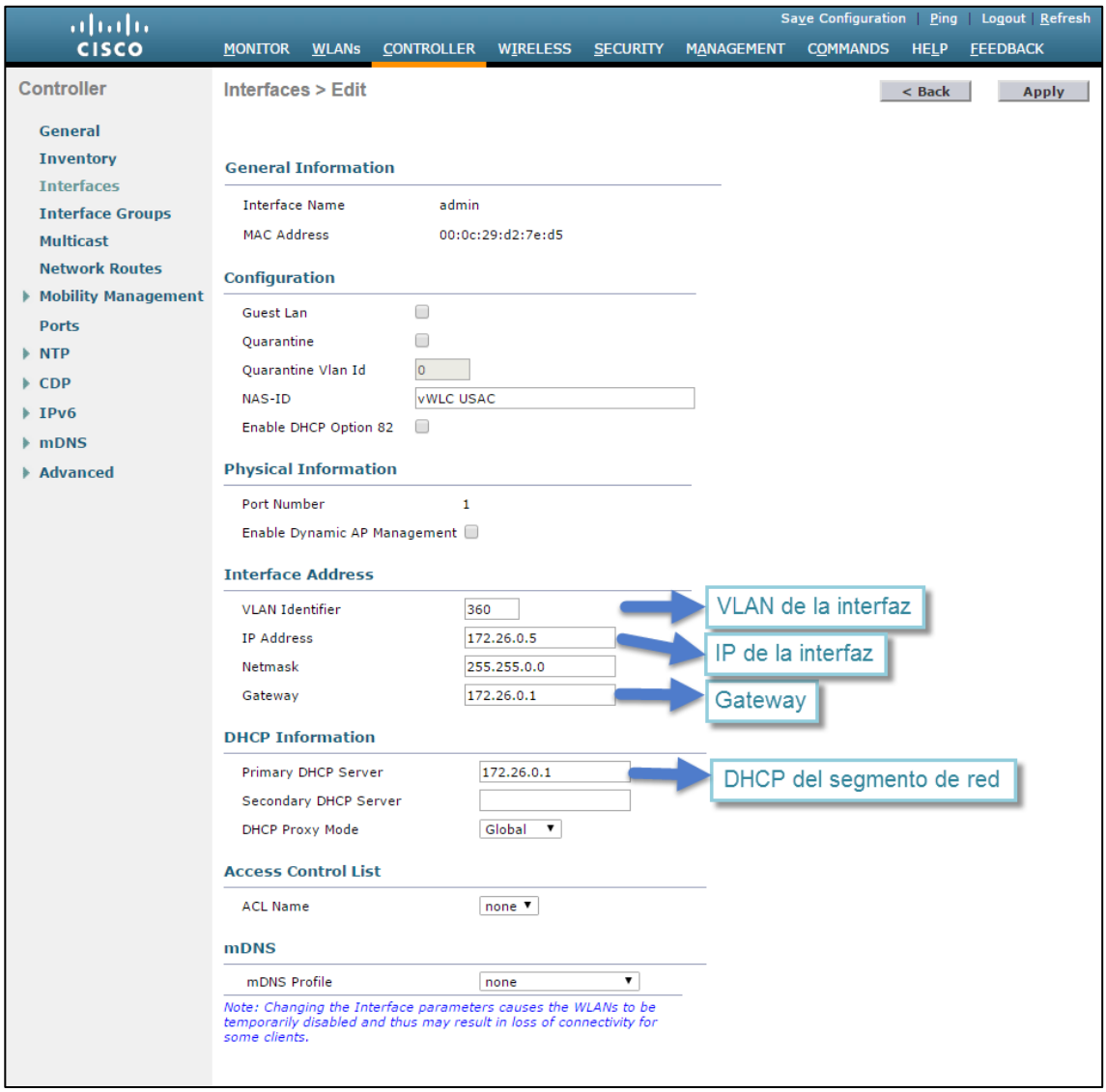
- Paso 3. Se deberá ingresar el nombre de la interfaz y la VLAN, en este procedimiento crearemos la interfaz de administración de la red FIUSAC.

Figura 105. **Configuración interfaz dinámica paso 3**

Fuente: elaboración propia.

- Paso 4. Luego se deberá de configurar IP de la interfaz, máscara de red y default Gateway, también el servidor DHCP para este segmento de red.

Figura 106. **Configuración interfaz dinámica paso 4**



Fuente: elaboración propia.

Se realiza el mismo procedimiento para crear la interfaz dinámica de estudiantes.

5.3.4.4.4. Configuración de redes *wireless*

En el diseño propuesto se tienen dos redes inalámbricas o SSIDs, una para alumnos y otra para la administración, en esta última se encuentran los maestros, personal administrativo de la Facultad y gerencial.

A continuación, se establecen los pasos a seguir para crear una red *wireless*.

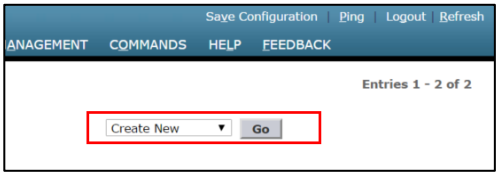
- Paso 1. Se debe de ingresar en la pestaña de WLANs en la opción WLANs.

Figura 107. **Configuración red *wireless* paso 1**

Fuente: elaboración propia.

- Paso 2. Luego se debe de elegir la opción de *Create New* para crear una nueva red *wireless*, se da click en el botón Go para continuar la configuración.

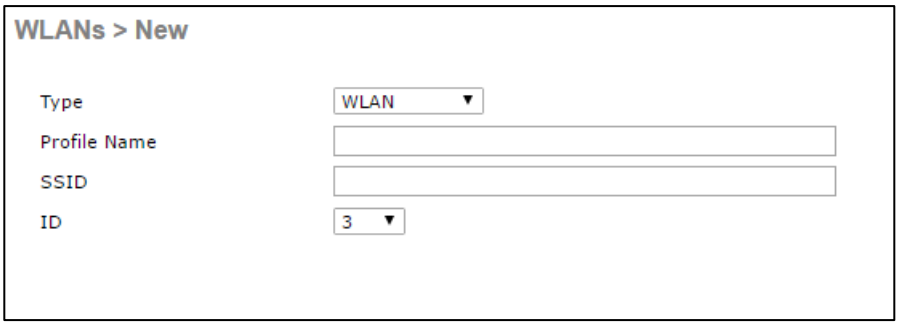
Figura 108. **Configuración red *wireless* paso 2**



Fuente: elaboración propia.

- Paso 3. Aparece el siguiente formulario, se debe de seleccionar el tipo WLAN, en *Profile Name* se coloca un nombre con el cual se identificar la red *wireless*, en SSID se coloca el nombre de la red con el cual se irradiará a los usuarios, y finalmente el ID es solamente un identificador de la red dentro del WLC.

Figura 109. **Configuración red *wireless* paso 3**

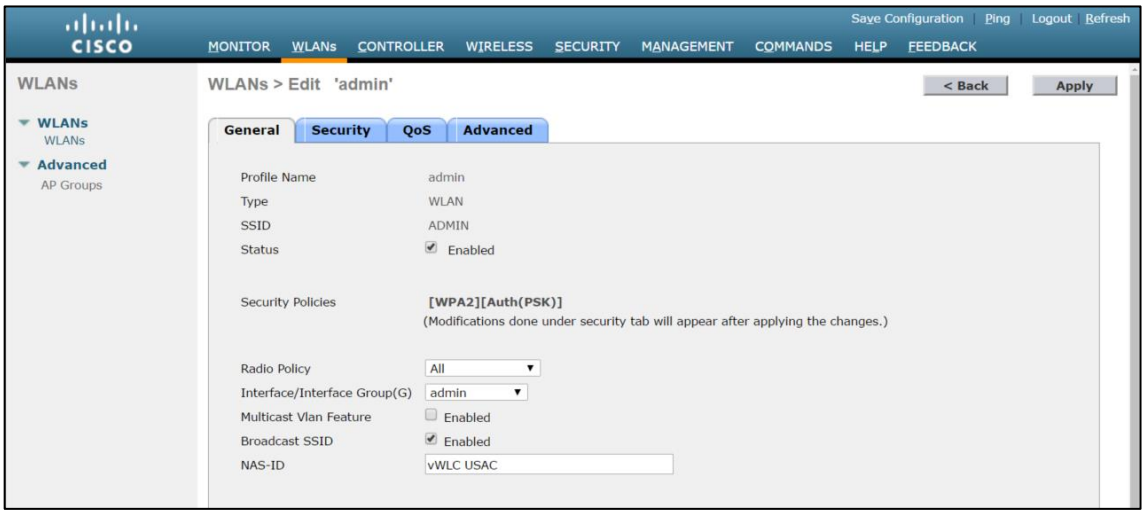


Fuente: elaboración propia.

- Paso 4. En este proceso se creó la red “admin”, para tenerla activa se deben de tener habilitadas las casillas de Status y *Broadcast* SSID, esta segunda opción se habilita para que la red inalámbrica pueda ser observada por los usuarios en sus dispositivos, de lo contrario la red

estará disponible pero solo los dispositivos con una configuración previa podrán utilizarla.

Figura 110. **Configuración red *wireless* paso 4**



Fuente: elaboración propia.

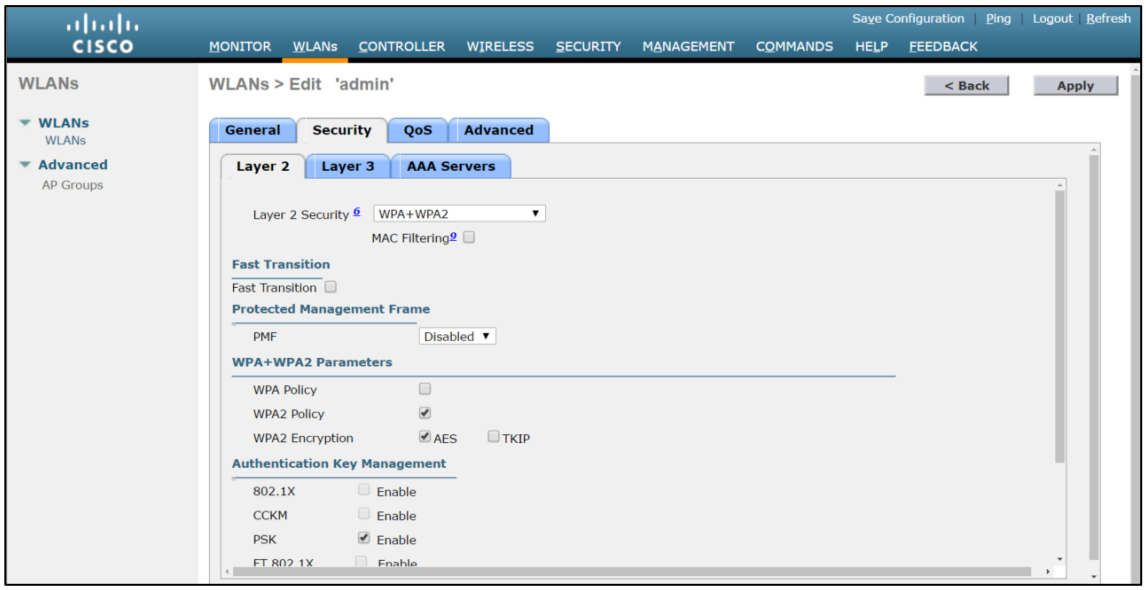
Adicional en esta parte se configuran las siguientes opciones:

Radio Policy, se elige All para que la red *wireless* se irradie en todos los espectros disponibles (802.11 a/b/g).

Interface/Interface Group(G), se elige la interfaz dinámica a la cual se asociará la red *wireless*, en una sección anterior se demostró el proceso de crear una interfaz dinámica para poder utilizarla en esta configuración, para llevar un orden se configuró la interfaz dinámica y la red *wireless* con el mismo nombre “admin”.

- Paso 5. La configuración de la red *wireless* continúa seleccionando la pestaña Security. El diseño propuesto utiliza seguridad WPA, este tipo de seguridad es la más robusta y recomendada por lo que se elige la opción WPA+WPA2, y habilitando las casillas WPA2 Policy, WPA2 Encryption AES.

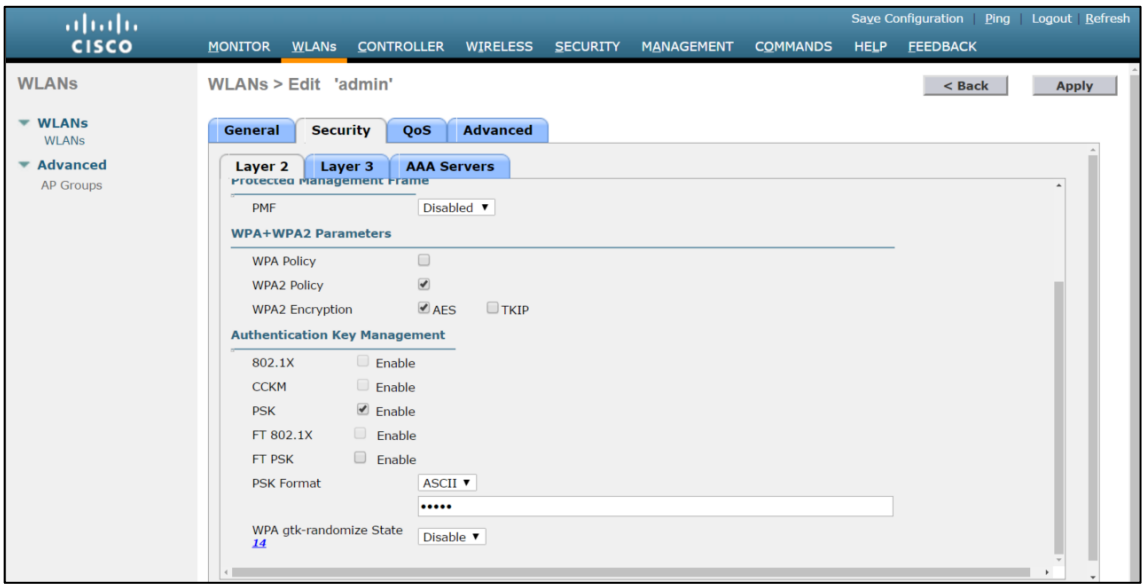
Figura 111. **Configuración red *wireless* paso 5 a**



Fuente: elaboración propia.

En la parte inferior se selecciona la casilla de PSK y formato ASCII, en el cuadro debajo se establece la contraseña para poder unirse a la red *wireless*.

Figura 112. **Configuración red *wireless* paso 5 b**

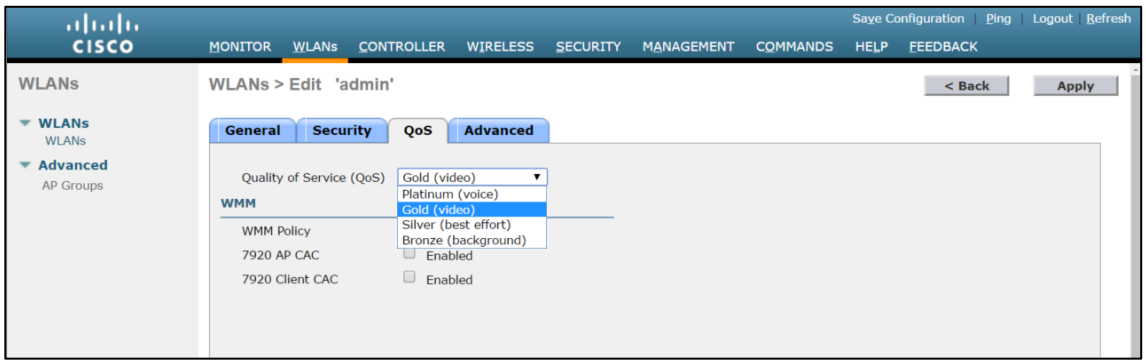


Fuente: elaboración propia.

- Paso 6. En la pestaña de Qos se elige el tipo de calidad de servicio que tendrá la red inalámbrica, en este caso se está creando la red “admin” por lo que tiene que tener una prioridad mayor a la red de “estudiantes”, se selecciona el Qos “Gold”.

La red de estudiantes posteriormente se configura con Qos “Silver”.

Figura 113. **Configuración de red *wireless* paso 6**



Fuente: elaboración propia.

Finalmente se tienen configuradas las dos SSIDs según el diseño propuesto.

Figura 114. **SSIDs del diseño propuesto**

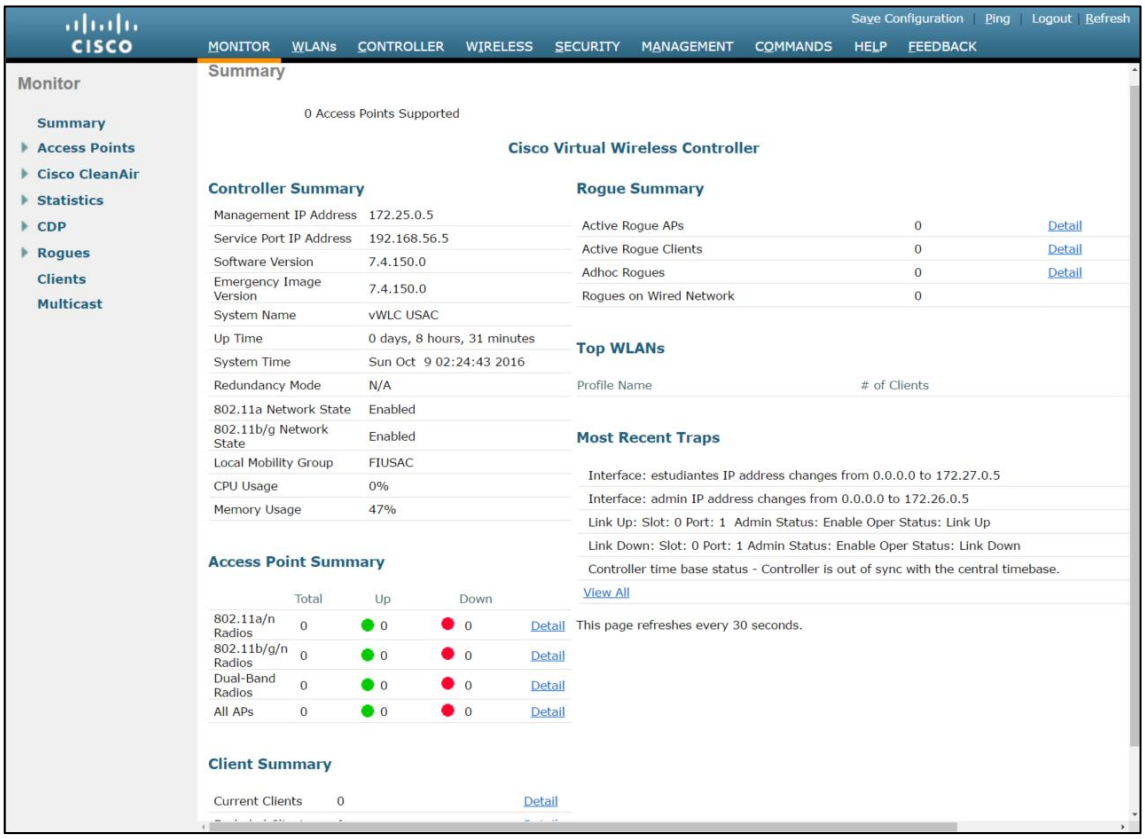
Fuente: elaboración propia.

5.3.4.4.5. Generalidades del WLC

En la pantalla inicial del WLC en la parte de MONITOR > Summary, se observa un resumen de la información importante del WLC, se puede observar la IP de administración, la versión con la cual el equipo está trabajando, los AP asociados al WLC y en que radio está irradiando la SSID, también la cantidad

de cliente por AP, y un pequeño registro de logs con la actividades más recientes en el equipo.

Figura 115. **Resumen de la información del WLC**

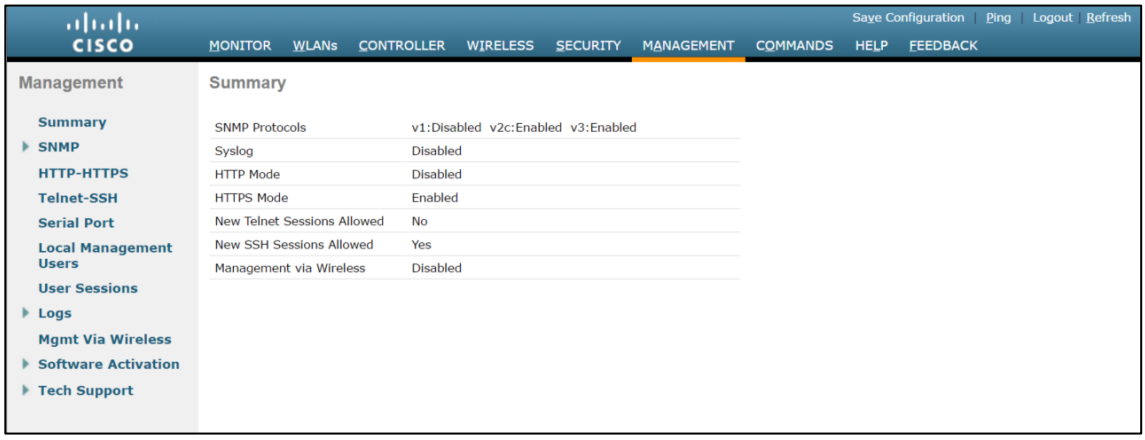


Fuente: elaboración propia.

En la pestaña de MANAGEMENT se puede observar y configurar que tipo de gestión se tiene sobre el WLC, por *default* se deshabilita el modo de gestión por HTTP y Telnet, ya que estos protocolos tienen vulnerabilidades y puede poner en riesgo la información manejada por el controlador inalámbrico. Se encuentra habilitada la gestión por HTTPS y SSH, adicional por default la administración por medio de conexión *wireless* se encuentra deshabilitada, se

debe de conectar a la red LAN donde está conectado el WLC o directamente por consola o el *Service Port*, esto quita el riesgo de que personas ajenas al área de IT puedan realizar cambios de configuración en el equipo.

Figura 116. **Administración del WLC**



Fuente: elaboración propia.

5.4. Sección económica

Cualquier proyecto lleva involucrado costo de inversión y algún tipo de retorno de la inversión a corto, medio y largo plazo.

Para el diseño propuesto se han determinado los recursos, costo de equipos y beneficios del diseño.

En esta fase se contemplarán tres aspectos de importancia:

- Fuentes de financiamiento
- Inversión inicial

- Beneficios

5.4.1. Fuente de financiamiento

El dinero para la inversión inicial sería responsabilidad del área económica de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala.

5.4.2. Inversión inicial

En cuanto a la inversión inicial se realizó la cotización de los equipos que se necesitan para montar la red inalámbrica, también la parte lógica de los equipos, lo que conlleva las licencias para funcionamiento y las imágenes o IOS de los equipos.

Detalle de inversión Inicial:

Tabla XVIII. **Cotización de equipos para la red inalámbrica**

Descripción	Proveedor	Cantidad	Costo Unitario ($.)	Costo total ($.)
Compra de Equipos Electrónico				
AIR-CT5508-12-K9 *WirelessController*	CISCO	1	$ 10 995,00	$ 10 995,00
WS-C2960X-24PS-L *Switch* PoE	CISCO	1	$ 3 195,00	$ 3 195,00
AIR-CAP3702I-A-K9 *Access points*	CISCO	4	$ 1 495,00	$ 5 980,00
SFP-GE-T= SFPs de cobre	CISCO	2	$ 440,00	$ 880,00
Servicios de Software				
CONT-SNT-WSC224SL IOS para *switch* Cayalyst 2960	CISCO	1	$ 276,38	$ 276,38
CONT-SNT-CT0812 IOS para Cisco 5508 WLC	CISCO	1	$ 1 964,88	$ 1 964,88
CONT-SNT-3702IA IOS para *Access point*	CISCO	4	$ 82,50	$ 330,00
Total de Inversión				**$ 23 621,26**
Total de Inversión en Q. (Cambio de dólar 7.58)				**Q 179 049,15**

Fuente: elaboración propia.

Tabla XIX. **Cotización instalación de *access point***

Access point					
No	**Descripción**	**Unidad**	**Cantidad**	**Precio Unitario**	**Precio Total**
Enlace eléctricos					
1	Patchcord Eléctrico Cat. 6 para exterior 50 Mts (EST)	unidad	1	$ 148,19	$ 148,19
2	Etiqueta Brady Continua	unidad	2	$ 1,38	$ 2,76
3	Escalerilla	metro	3	$ 181,80	$ 545,40
4	Tarugo tipo Fisher No. 8	unidad	5	$ 3,22	$ 16,10
5	Tornillo para Tarugo No. 8	unidad	5	$ 3,22	$ 16,10
6	Cinta de aislar	unidad	0,4	$ 5,69	$ 2,28
7	Cincho plástico	bolsa	0,6	$ 14,40	$ 8,64
				Total Materiales	**$ 739,47**
Servicios					
8	Servicios de Logistica: Traslado de equipos, almacenamiento y seguro				$ 29,56
9	Servicios de RS&P				$ 305,20
				Total servicios	**$ 334,76**
				Total instalación *Access point* individual	**$ 1 074,23**
				Total instalación *access points* (4 Aps)	**$ 4 296,90**

Fuente: elaboración propia.

Tabla XX. **Cotización instalación de *switch* 2960**

***Switch* 2960**					
No	**Descripción**	**Unidad**	**Cantidad**	**Precio Unitario**	**Precio Total**
Energía					
1	Cable THHN No.2 Color Verde	metros	15	$ 4,59	$ 68,85
2	Cable TSJ 3x12	metros	25	$ 2,40	$ 60,00
3	PDU 10 puertos AC APC	unidad	1	$ 271,72	$ 271,72
4	Breaker ABB 30 AMP	unidad	1	$ 43,84	$ 43,84
5	Terminal de un ojo 2	unidad	2	$ 10,12	$ 20,24
6	Forro Termocontractil 2	unidad	2	$ 2,58	$ 5,16
7	Terminal de un ojo 12	unidad	3	$ 0,84	$ 2,52
8	Cinta de aislar	unidad	0,2	$ 5,70	$ 1,14
9	Etiqueta Brady Continua	unidad	5	$ 1,38	$ 6,90
				Total Materiales	**$ 480,37**
Servicios					
8	Servicios de Logistica: Traslado de equipos, almacenamiento y seguro				$ 86,46
9	Servicios de RS&P				$ 697,28
				Total servicios	**$ 783,74**
				Total instalación *switch* individual	**$ 1 264,11**
				Total instalación *switch* (1)	**$ 1 264,11**

Fuente: elaboración propia.

Tabla XXI. **Cotización instalación de WLC 5508**

WLC 5508					
No	**Descripción**	**Unidad**	**Cantidad**	**Precio Unitario**	**Precio Total**
Energía					
1	Cable THHN No.2 Color Verde	metros	15	$ 4,59	$ 68,85
2	Cable TSJ 3x12	metros	25	$ 2,40	$ 60,00
3	PDU 10 puertos AC APC	unidad	1	$ 271,72	$ 271,72
4	Terminal de un ojo 2	unidad	4	$ 10,12	$ 40,48
5	Forro Termocontractil 2	unidad	4	$ 2,58	$ 10,32
6	Terminal de un ojo 12	unidad	6	$ 0,84	$ 5,04
7	Cinta de aislar	unidad	0,2	$ 5,70	$ 1,14
8	Etiqueta Brady Continua	unidad	10	$ 1,38	$ 13,80
9	Cincho plástico negro 11"	bolsa	1	$ 14,41	$ 14,41
				Sub-Total energía	**$ 485,76**
Accesorios					
10	Organizador Horizontal de doble cara	unidad	2	$ 64,86	$ 129,72
				Sub-Total Accesorios	**$ 129,72**
Enlaces ópticos (troncales)					
11	Flexitubo amarillo de 1/2"	unidad	0,5	$ 74,42	$ 37,21
12	Patchcord de fibra óptica monomodo duplex de hasta 30m	unidad	4	$ 70,12	$ 280,48
13	Velcro	unidad	0,5	$ 14,43	$ 7,22
14	Etiqueta Brady de bandera	unidad	8	$ 0,58	$ 4,64
				Sub-Total enlaces ópticos	**$ 329,55**
				Total materiales	**$ 945,03**
Servicios					
15	Servicios de Logistica: Traslado de equipos, almacenamiento y seguro				$ 646,14
16	Servicios de RS&P				$ 3 245,25
				Total servicios	**$ 3 891,39**
				Total instalación *switch* individual	**$ 4 836,42**
				Total instalación WLC (1)	**$ 4 836,42**

Fuente: elaboración propia.

Tabla XXII. **Resumen de cotización de instalación**

Resumen cotización de instalación	
Materiales 4 Aps	$ 2.957,86
Servicios 4 Aps	$ 1.339,04
Materiales 1 *switch*	$ 480,37
Servicios 1 *switch*	$ 783,74
Materiales 1 WLC	$ 945,03
Servicios 1 WLC	$ 3 891,39
Total	**$ 10 397,43**

Fuente: elaboración propia.

El resumen del costo total de la inversión en software, *hardware* e instalación para el diseño propuesto se valora en $34 018,69.

5.4.3. Beneficios

El diseño propuesto tiene beneficios económicos y no cuantificables, a través del ahorro de energía y actualización de equipo a un largo plazo, también los beneficios hacia las personas que utilizarían el servicio que la red inalámbrica brinda.

Con el estudio de sitio realizado se tiene el conocimiento de 18 *access points* que cubren el área propuesta, entre las señales del*Access points* están las siguientes:

- Decanatura
- Cafetería del T3
- FIUSAC
- RIUSAC
- FARUSAC
- RIING

Se detectan otras señales propagadas por *access points* instalados por la Facultad de Ingeniería, sin conocer su origen. Todas estas señales consumen tiempo de aire compartido, lo que interfiere y hace que las ondas choquen entre canales sin control alguno. Se tiene conocimiento que cada *access point* consume un promedio de 15.4W por hora.

Según la tarifa de energía eléctrica tomada de la página oficial de ENERGUATE (http://www.energuate.com/tarifas-vigentes) se tiene una tarifa de Q.0,56 con IVA, este es el valor para consumo de energía entre 0 a 60 KWh.

Suponiendo que cada *access point* trabaja las 24 horas al día, se tiene un consumo de 369,6Wh, lo que equivale a Q.0,21 por día. Si multiplicamos el costo de utilización de un AP por los 18 AP que se tienen en el área, da un resultado de Q.3,73 por día, y Q.115,49 al mes.

Con el nuevo diseño se deben retirar todos los AP que trabajan en el área, los AP propiedad de la Facultad de Ingeniería USAC, pueden ser vendidos a una cantidad módica, y los APs propiedad de terceros solamente serán retirados diplomáticamente, con esto se logra tener una pequeña entrada económica y la limpieza del espectro.

Siguiendo el diseño se debería de instalar 4 AP, con solo 4 AP trabajando se tendría un gasto de Q 0,83 por día utilizando los 4 AP, y Q 25,67 al mes, se tiene un ahorro del 77,77 %, una ganancia bruta de Q 89,82 al mes.

Relación costo - beneficio

Tabla XXIII. **Relación costo – beneficio**

Periodo	Costo mensual	Costo Acumulado	Beneficio mensual	Beneficio Acumulado	Costo Beneficio
Mes 1	Q 25,67	Q 25,67	Q 89,82	Q 89,82	Q 64,15
Mes 2	Q 25,67	Q 51,34	Q 89,82	Q 179,64	Q 128,30
Mes 3	Q 25,67	Q 77,01	Q 89,82	Q 269,46	Q 192,45
Mes 4	Q 25,67	Q 102,68	Q 89,82	Q 359,28	Q 256,60
Mes 5	Q 25,67	Q 128,35	Q 89,82	Q 449,10	Q 320,75
Mes 6	Q 25,67	Q 154,02	Q 89,82	Q 538,92	Q 384,90
Mes 7	Q 25,67	Q 179,69	Q 89,82	Q 628,74	Q 449,05
Mes 8	Q 25,67	Q 205,36	Q 89,82	Q 718,56	Q 513,20
Mes 9	Q 25,67	Q 231,03	Q 89,82	Q 808,38	Q 577,35

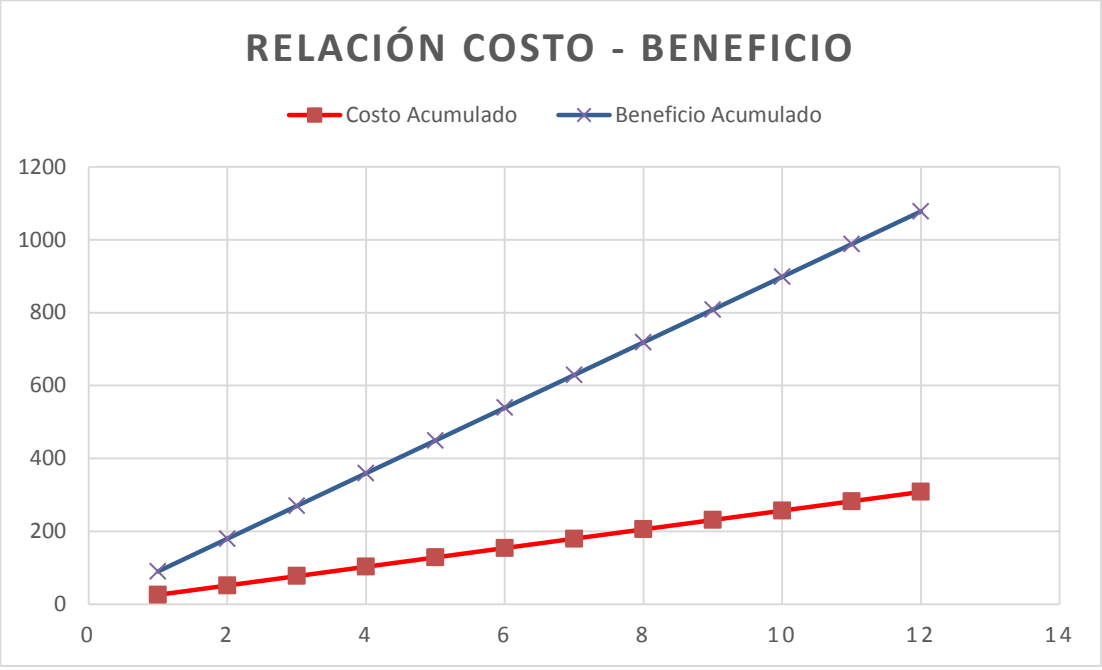
Continuación de la tabla XXIII.

Mes 10	Q 25,67	Q 256,70	Q 89,82	Q 898,20	Q 641,50
Mes 11	Q 25,67	Q 282,37	Q 89,82	Q 988,02	Q 705,65
Mes 12	Q 25,67	Q 308,04	Q 89,82	Q 1077,84	Q 769,80
Totales	**Q 308,04**	**Q 2 002,26**	**Q 1 077,84**	**Q 7 005,96**	**Q 5 003,70**

Fuente: elaboración propia.

Con base en la relación de los costos y beneficios en el consumo eléctrico del *access points*, se observa que se tiene un beneficio económico instantáneo, desde el primer mes que se utiliza el diseño propuesto, desde ahí los beneficios acumulado comienzan a incrementarse.

Figura 117. **Gráfica relación costo – beneficio**



Fuente: elaboración propia.

Entre otros beneficios del diseño propuesto están:

- Los estudiantes de la facultad podrán utilizar una red gratuita y estable, la cual estará disponible las 24 horas del día.

- Los estudiantes con plan de datos podrán elegir utilizar la red inalámbrica al ser capaz de satisfacer el ancho de banda y estabilidad del servicio.

- El café internet de la Facultad de Ingeniería tendrá que ofrecer valores más competitivos para poder ser rentable, beneficiando siempre al estudiante.

- Una red administrada por Centro de Cálculo de la Facultad de Ingeniería USAC, permitiendo adaptarse y actualizarse dependiendo de las demandas de los usuarios.

- Al utilizar equipos de alto rendimiento los mejores de su clase, se tiene una inversión a largo plazo, permitiendo la utilización de los equipos por más tiempo.

- Los *acccess points* desinstalados pueden revenderse para obtener un ingreso adicional para la compra del nuevo equipo.

CONCLUSIONES

1. La radiofrecuencia, es el rango de frecuencias que se utilizan en este trabajo para entablar comunicación por ondas, estas se rigen por las leyes de la teoría electromagnética con las que es posible determinar su comportamiento y naturaleza.

2. La comisión federal de comunicaciones FCC, es el organismo responsable de establecer las frecuencias, canales y potencias en toda Guatemala y el organismo IEEE es el encargado de normalizar estándares 802. 11, igualmente aplicables en el país. Por ello para estar conforme a los estándares internacionales, la alianza Wi-Fi debe certificar todos los equipos utilizados con el fin de facilitar la compatibilidad de distintos dispositivos, de diferentes marcas.

3. La seguridad que se necesita en una red inalámbrica es de total importancia, debido a la naturaleza que tiene este medio de comunicación. Se necesita de un completo cuidado con el cifrado de datos, manteniendo los parámetros de autenticación, para evitar el robo de información. Por tal se utiliza la encriptación WPA2 con TKIP por la actualización, calidad y poca vulnerabilidad.

4. A causa de la deficiencia con la red inalámbrica que se presenta en la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, surge la necesidad de buscar herramientas que ayuden a mejorar la calidad y eficacia de la misma. En base a esta carencia se propone un diseño fundado en un equipo central para la red inalámbrica, en la que se

realiza cambio de VLAN a SSID para poder conectar a la red de la facultad, misma que se encarga de configurar y administrar los equipos periféricos delegados de propagar la señal.

RECOMENDACIONES

1. Ejecutar el diseño en un área pequeña de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, con la finalidad de poner a prueba la propuesta y poder mejorarla, cobrando con datos reales.

2. Dar a conocer la propuesta a las autoridades de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, mostrando los pros que conlleva el diseño, al igual que los valores de inversión, para determinar si se ejecuta o se adapta a un diseño propio.

3. Crear un modelo escala del diseño, centralizada en el área propuesta de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, para buscar patrocinios y poder lograr la implementación del sistema disminuyendo costos.

4. Capacitar al personal educativo, compuesto por los ingenieros, sobre la configuración y mantenimiento de los equipos para realizar cambios en el sistema a favor de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala.

BIBLIOGRAFÍA

1. Cisco Systems. *Catalyst 2960-X Switch Hardware Installation Guide*. San José, CA USA: cisco.com, 2013.

2. Cisco Systems. *Data sheet Cisco 5500 Series Wireless Controllers*. San Jose, CA USA: cisco.com, 2016.

3. *Conmutador*. [en línea]. <https://es.wikipedia.org/wiki/ Conmutador_ (dispositivo_de_red)>. [Consulta: 29 de noviembre de 2016].

4. Decibelio. [en línea]. <https://es.wikipedia.org/wiki/Decibelio>. [Consulta: 29 de noviembre de 2016].

5. HUCABY, D. *CCNA wireless 640-722 official cert guide*. Indianapolis: Cisco Press, 2010.

6. ODOM, Wendell. *CCNA Routing and Switching 200-120 official cert guide.* Indianapolis:Cisco Press, 2013.

7. *Par Trenzado*. [en línea]. <http://informatica.iescuravalera.es/iflica/ gtfinal/libro/c44.html>. [Consulta: 11de octubrede 2016].

8. *PoE Power Draw at PSE for Cisco AP 3702*. [en línea]. <https://suppor tforums.cisco.com / discussion / 12089071 / poe-power-draw-pse-cis co-ap-3702>. [Consulta: 11 de octubre de 2016].

9. *Red inalámbrica*. [en línea]. <https://es.wikipedia.org/ wiki/Red_ inal%C3%A1mbrica>. [Consulta: 29 de noviembre de 2016].

10. Relación señal/ruido. [en línea]. <https://es.wikipedia.org/wiki/Relaci% C3%B3n_se%C3%B1al/ruido>. [Consulta: 29 de noviembre de 2016].

11. *Services, P., Points, A., Series, C., Literature, D., & Sheets, D. Cisco Aironet 3700 Series Access points Data Sheet. Cisco*. [en línea]. <http://www.cisco.com/c/en/us/products/collateral/*wireless*/3700-series-access-point/data_sheet_c78-729421.html>. [Consulta: 11 de octubre de 2016].

12. Support, P., Series, C., Guides, R., & References, T. Cisco Aironet Series 1700/2700/3700 *Access points* Deployment Guide. Cisco. [en línea]. <http://www.cisco.com/c/en/us/td/docs/*wireless*/ technology/ apdeploy/8-0/Cisco_Aironet_3700AP.html>. [Consulta: 11 de octubre de 2016].

13. *Transceptor SFP*. [en línea]. <https://es.wikipedia.org/wiki/Transceptor_ SFP>. [Consulta: 29 de noviembre de 2016].

14. *Tarifas vigentes de ENERGUATE*. [en línea]. <http://www.energuate. com/tarifas-vigentes>. [Consulta: 11 de octubre de 2016].

15. *Unshielded twisted pair.* [en línea]. <https://es.wikipedia.org/ wiki/Unshielded_twisted_pair>. [Consulta: 11 de octubre de 2016].

16. *Wi-Fi Design, WLAN Planning and Site survey Tools, Wi-Fi Spectrum Analysis | Ekahau*. [en línea]. <http://www.ekahau.com/>. [Consulta: 11 de octubre de 2016].

17. *Wireless Access points*. *Cisco*. [en línea]. <http://www.cisco.com/c/en/us/products/*wireless*/access-points/index.html>. [Consulta: 29 de noviembre de 2016].

18. *Zona de Fresnel*. [en línea]. <https://es.wikipedia.org/wiki/Zona_de_Fresnel>. [Consulta: 29 de noviembre de 2016].