

**ANÁLISIS Y DISEÑO DE UNA RED INALÁMBRICA BAJO LAS NORMAS IEEE 802.11(X) PARA
EL CAMPUS DE INGENIERÍAS - SECTOR TULCÁN**



**HERNÁN DARÍO BRAVO GALLEGO
MARTHA CLAUDIA VERA GARCÍA**

**UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
GRUPO DE I+D NUEVAS TECNOLOGÍAS EN TELECOMUNICACIONES
POPAYÁN
2004**

**ANÁLISIS Y DISEÑO DE UNA RED INALÁMBRICA BAJO LAS NORMAS IEEE 802.11(X) PARA
EL CAMPUS DE INGENIERÍAS - SECTOR TULCÁN**



**HERNÁN DARÍO BRAVO GALLEGO
MARTHA CLAUDIA VERA GARCÍA**

**Trabajo de grado presentado como requisito para obtener el título de Ingeniero en
Electrónica y Telecomunicaciones**

**Director
MAG. PEDRO VERA VERA**

**UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
GRUPO DE I+D NUEVAS TECNOLOGÍAS EN TELECOMUNICACIONES
POPAYÁN
2004**

A mis padres Helio Hernán y Melva
por su constante apoyo para alcanzar mis metas.
A mis hermanas Juliana Andrea y Luz Yadira
por el cariño y amor que nos une.
Y a Dios por poder contar con personas tan maravillosas.

Hernán Darío

A Dios por permitirme estar aquí y brindarme las fuerzas
necesarias para derribar todas las barreras
que he encontrado a mi paso.
A mis padres con todo mi amor y admiración,
a quienes debo y agradezco
cada uno de mis logros,
por su grandioso apoyo y amor
incondicional.
A mis hermanos, amigos eternos y con quienes he compartido
momentos maravillosos.

Martha C.

AGRADECIMIENTOS

A la Facultad de Ingeniería Electrónica y Telecomunicaciones y sus profesores por la formación académica.

Por la colaboración que nos brindaron durante el desarrollo del trabajo de grado:

Ing. José Luis Quintero

Ing. Guefry Agredo

Ing. Pedro Vera

Ing. Marian Menke

Ing. Andrés Meneses

Arq. Marcela Rojas

CONTENIDO

	Pág
INTRODUCCION	19
1. NORMAS IEEE 802.11 SUBCAPA MAC	21
1.1 ARQUITECTURA 802.11	22
1.1.1 Componentes básicos	22
1.1.2 Conjunto de servicio	23
1.1.3 Interfaces de servicios	25
1.1.3.1 Servicios de la estación	25
1.1.3.2 Servicios del sistema de distribución	26
1.1.3.3 Relación entre servicios	27
1.2 <i>ROAMING</i>	29
1.3 ACCESO MÚLTIPLE POR DETECCIÓN DE PORTADORA CON EVASIÓN DE COLISIÓN (CSMA/CA)	30
1.4 MODOS DE ACCESO MAC	31
1.5 PROCESO DE COMUNICACIÓN	33
1.5.1 Proceso de comunicación en modo PCF	33
1.5.2 Proceso de comunicación en modo DCF	34
1.6 FRAGMENTACION	34
1.7 CAMBIO DINÁMICO DE VELOCIDAD	35
1.8 BALIZAS	35
1.9 BUSQUEDA	36
1.9.1 Búsqueda pasiva	36
1.9.2 Búsqueda activa	36
1.10 MANEJO DE POTENCIA	37
1.10.1 Modo activo continuo	37
1.10.2 Modo sondeo de ahorro de potencia	37
1.10.2.1 Sondeo de ahorro de potencia en un BSS	38
1.10.2.2 Sondeo de ahorro de potencia en un IBSS	38
1.11 SEGURIDAD	39
1.12 UNIDADES DE DATOS MAC	43
1.12.1 Campo de control de trama	44

1.12.1.1	Subcampo versión del protocolo	44
1.12.1.2	Subcampo tipo y subtipo	45
1.12.1.3	Subcampo Para DS	46
1.12.1.4	Subcampo Desde DS	46
1.12.1.5	Subcampo más fragmentos	46
1.12.1.6	Subcampo reintento	46
1.12.1.7	Subcampo manejo de potencia	46
1.12.1.8	Subcampo más datos	47
1.12.1.9	Subcampo WEP	47
1.12.1.10	Subcampo orden	47
1.12.2	Campo duración ID	47
1.12.2.1	Duración vector de ubicación de la red	47
1.12.2.2	Tramas transmitidas durante el periodo de libre contención	48
1.12.2.3	Tramas PS – Poll	48
1.12.3	Campo de direcciones	48
1.12.3.1	Subcampo dirección 1	49
1.12.3.2	Subcampo dirección 2	49
1.12.3.3	Subcampo dirección 3	49
1.12.3.4	Subcampo dirección 4	49
1.12.4	Campo de secuencia de control	51
1.12.5	Campo de cuerpo de trama	51
1.12.6	Campo FCS	51
2.	NORMAS IEEE 802.11 - CAPA FÍSICA	52
2.1	802.11	52
2.1.1	Infrarrojo	52
2.1.2	Tecnología de espectro ensanchado	53
2.1.2.1	Espectro ensanchado por salto de frecuencia (FHSS)	54
2.1.2.2	Espectro ensanchado por secuencia directa (DSSS)	55
2.2	802.11b	60
2.2.1	PLCP de 802.11b	60
2.2.2	PMD de 802.11b	62
2.3	802.11a	62
2.3.1	Multiplexación por división de frecuencia ortogonal (OFDM)	63
2.3.2	PLCP de 802.11a	64
2.3.2.1	Unidad de protocolo lógico	64

2.3.2.2 Unidad de protocolo físico	66
2.3.3 PMD de 802.11a	66
2.4 802.11g	69
2.4.1 PLCP de 802.11g	69
2.4.2 PMD de 802.11g	69
2.5 PARÁMETROS DE LA CAPA FÍSICA	70
3. INFRAESTRUCTURA Y PROPAGACIÓN EN UNA RED DE AREA LOCAL INALÁMBRICA	71
3.1 PUNTO DE ACCESO	71
3.1.1 Modos de configuración de los APs	72
3.1.1.1 Modo raíz	72
3.1.1.2 Modo repetidor	73
3.2 GATEWAY INALÁMBRICO	74
3.2.1 <i>Gateway</i> inalámbrico residencial	74
3.2.2 <i>Gateway</i> inalámbrico empresarial	75
3.3 PUENTE	76
3.4 DISPOSITIVOS CLIENTE EN UNA WLAN	78
3.4.1 Tarjeta PCMCIA	78
3.4.2 Tarjetas flash compactas	79
3.4.3 Conversor Ethernet y seriales	79
3.4.4 Adaptadores USB	79
3.4.5 Adaptadores PCI e ISA	79
3.4.6 Módulos mini PCI	79
3.5 ANTENAS	79
3.5.1 Tipo de antenas	80
3.5.1.1 Antena omnidireccional	80
3.5.1.2 Antena direccional de baja ganancia	80
3.5.1.3 Antena direccional de alta ganancia	81
3.6 ACCESORIOS WLAN	81
3.6.1 Amplificador RF	81
3.6.2 Atenuador RF	82
3.6.3 Supresor de transientes	82
3.6.4 Divisores RF	83
3.6.5 Conectores RF	83
3.6.6 Cables RF	84
3.6.7 <i>Pigtail</i>	85

3.6.8	Conversor de frecuencia	85
3.6.9	Potencia sobre Ethernet (PoE)	85
3.7	PROPAGACIÓN DE LA SEÑAL	86
3.7.1	Fenómenos físicos	86
3.7.1.1	Reflexión	86
3.7.1.2	Difracción	86
3.7.1.3	Dispersión	87
3.7.1.4	Absorción	87
3.7.1.5	Refracción	87
3.7.2	Pérdidas de espacio libre	87
3.7.3	Pérdidas en el interior de un edificio	87
3.7.3.1	Modelos estadísticos	87
3.7.3.2	Modelos empíricos de trayectoria directa	88
3.7.3.3	Modelos empíricos de multitrayectoria	90
3.7.3.4	Modelos de rayos ópticos	91
4.	MODELO PARA EL DISEÑO DE UNA RED DE AREA LOCAL INALÁMBRICA	92
4.1	ESTUDIO PRELIMINAR	93
4.1.1	Análisis del entorno	93
4.1.2	Redes existentes	93
4.1.3	Análisis de la interferencia	94
4.1.4	Tipo de equipos cliente	94
4.2	CAPACIDAD	94
4.2.1	Tecnología	94
4.2.2	Cambio de velocidades	94
4.2.3	Ancho de banda por usuario	94
4.3	COBERTURA	95
4.3.1	Área de cobertura	95
4.3.2	Patrón de radiación de la antena	95
4.3.3	Montaje de APs y de antenas	96
4.3.4	Frecuencia	96
4.3.5	Ubicación de los APs y sus antenas	96
4.3.6	Potencia de los APs	98
4.4	ASIGNACIÓN DE CANALES	98
4.5	ESTUDIO DEL SITIO	102
4.6	SEGURIDAD	102

4.7 DOCUMENTACION	104
4.8 PROBLEMAS	112
4.8.1 Solución al desvanecimiento por multitrayectoria	112
4.8.2 Solución al problema del nodo oculto	112
4.8.3 Solución de problema cerca/lejos	113
5. DISEÑO DE LA RED DE AREA LOCAL INALÁMBRICA	114
5.1 ESTUDIO PRELIMINAR	114
5.1.1 Análisis del entorno	114
5.1.2 Redes existentes	118
5.1.3 Análisis de la interferencia	120
5.2 CAPACIDAD	121
5.2.1 Tecnología	121
5.2.2 Cambio de velocidades	122
5.2.3 Ancho de banda por usuario	122
5.3 COBERTURA	123
5.3.1 Área de cobertura	123
5.3.2 Patrón de radiación de la antena	124
5.3.3 Montaje de APs y de antenas	124
5.3.4 Frecuencia	124
5.3.5 Ubicación de los APs y sus antenas	124
5.3.6 Potencia de los APs	126
5.4 ASIGNACIÓN DE CANALES	126
5.5 ESTUDIO DEL SITIO	127
5.5.1 Utilización de WinProp	128
5.5.2 Resultados de la simulación	128
5.5.2.1 Resultados según máxima potencia recibida y máxima velocidad de datos.	130
5.5.2.2 Resultados según el mejor AP.	136
5.5.2.3 Resultados según la probabilidad de recepción.	137
5.5.2.4 Resultados según el número de canales.	138
5.6 SEGURIDAD	139
5.7 DOCUMENTACION	140
5.8 CÁLCULO DE LA INVERSIÓN	145
5.8.1 Beneficios directos	146
5.8.2 Beneficios indirectos	146
5.8.3 Costos directos	148

5.8.4 Costos indirectos	148
5.8.5 Costo de la red inalámbrica	149
CONCLUSIONES	151
RECOMENDACIONES	153
BIBLIOGRAFÍA	154
ANEXOS	
ANEXO A. TIPOS DE TRAMAS	
ANEXO B. RESOLUCIÓN NÚMERO 000689 DE 2004	
ANEXO C. PROPIEDADES DE LOS MATERIALES	
ANEXO D. RESULTADOS DE LA SIMULACIÓN	

LISTA DE TABLAS

	Pág.
Tabla 1. Identificadores de tipo y subtipo.	45
Tabla 2. Interpretación de los bits Para DS y Desde DS.	46
Tabla 3. Valores del campo de duración ID.	47
Tabla 4. Uso del campo de direcciones.	49
Tabla 5. Campos de direcciones en la comunicación entre estaciones.	50
Tabla 6. Canales y potencia para DSSS.	58
Tabla 7. Operación punto multipunto en la banda de 2.4 GHz.	59
Tabla 8. Operación punto a punto en la banda de 2.4 GHz.	59
Tabla 9. Valores del campo señal.	61
Tabla 10. Velocidades y modulación de 802.11b.	62
Tabla 11. Bits usados en las velocidades.	65
Tabla 12. Velocidades y modulaciones en 802.11a.	67
Tabla 13. Canales y potencia para OFDM.	68
Tabla 14. Operación punto a punto en la banda superior de 5 GHz.	68
Tabla 15. Parámetros de la capa física 802.11.	70
Tabla 16. Pérdidas cable coaxial a 2.4GHz.	85
Tabla 17. Ubicación de los centros de cableado.	118
Tabla 18. Umbrales de recepción.	122
Tabla 19. Utilización del enlace de bajada.	122
Tabla 20. Utilización del enlace de subida.	123
Tabla 21. Potencia para cada uno de los APs.	126
Tabla 22. Asignación de canales a los APs para los diferentes pisos del Campus.	127
Tabla 23. Costos directos en una WLAN.	148
Tabla 24. Costo de la red inalámbrica.	149

LISTA DE FIGURAS

	Pág.
Figura 1. IEEE 802 y su relación con el modelo OSI.....	21
Figura 2. Componentes básicos de una LAN 802.11.....	23
Figura 3. Conjunto de servicio básico.....	24
Figura 4. Conjunto de servicio básico extendido.....	24
Figura 5. Conjunto de servicio básico independiente.....	25
Figura 6. Servicio de autenticación.....	26
Figura 7. Servicio de asociación.....	27
Figura 8. Relación entre variables de estado y servicios.....	28
Figura 9. Roaming entre ESS.....	30
Figura 10. Funciones de coordinación MAC.....	32
Figura 11. Proceso de comunicación en modo PCF.....	33
Figura 12. Proceso de comunicación en modo DCF.....	34
Figura 13. Fragmentación.....	34
Figura 14. Cambio de velocidad dinámica 802.11b.....	35
Figura 15. Búsqueda pasiva.....	37
Figura 16. Búsqueda activa.....	37
Figura 17. Sondeo de ahorro de potencia en un BSS.....	38
Figura 18. Puerto controlado y no controlado.....	41
Figura 19. Servicio de datos MAC.....	44
Figura 20. Formato general de trama MAC.....	44
Figura 21. Campo de control de trama.....	44
Figura 22. Uso del campo de direcciones en una ESS.....	50
Figura 23. Uso del campo de direcciones en una IBSS.....	50
Figura 24. Secuencia de control.....	51
Figura 25. Espectro ensanchado.....	53
Figura 26. Formato de trama PLCP.....	55
Figura 27. Espectro ensanchado.....	56
Figura 28. Codificación con el código <i>Barker</i>	57
Figura 29. Ensanchamiento de energía en el canal.....	57
Figura 30. Separación entre canales en redes 802.11.....	60

Figura 31. Trama PLCP 802.11b.....	60
Figura 32. Campo de servicio en el encabezado PLCP 802.11b.....	61
Figura 33. Ortogonalidad en el dominio de la frecuencia.....	63
Figura 34. Formato de trama PLCP de 802.11a.....	64
Figura 35. Trama PLCP de 802.11g.....	69
Figura 36. AP en modo raíz.....	73
Figura 37. AP en modo repetidor.....	73
Figura 38. Diagrama físico de un <i>gateway</i> residencial.....	74
Figura 39. Componentes lógicos de un <i>gateway</i> residencial.....	75
Figura 40. Comunicación de puente modo raíz con puente modo no raíz.....	76
Figura 41. Puente en modo repetidor.....	77
Figura 42. Comunicación entre puentes.....	77
Figura 43. Puente de grupo de trabajo instalado en una red.....	78
Figura 44. Patrón de radiación de una antena omnidireccional.....	80
Figura 45. Patrón de radiación de una antena direccional de baja ganancia.....	80
Figura 46. Patrón de radiación de una antena altamente direccional.....	81
Figura 47. Ubicación del amplificador RF en una WLAN.....	81
Figura 48. Ubicación de un atenuador en una WLAN.....	82
Figura 49. Supresor de transientes instalado en una WLAN.....	83
Figura 50. Conector tipo N.....	83
Figura 51. Conector BNC.....	84
Figura 52. Conector SMA.....	84
Figura 53. Conector TNC.....	84
Figura 54. <i>Pigtail</i>	85
Figura 55. Uso de PoE.....	86
Figura 56. Modelo de espacio libre modificado.....	88
Figura 57. Modelo Motley-Keenan.....	89
Figura 58. Modelo multi-paredes.....	90
Figura 59. Modelo de trayectorias dominantes.....	91
Figura 60. Modelo de rayos ópticos.....	91
Figura 61. Arreglo lineal de APs.....	97
Figura 62. Arreglo rectangular de APs.....	98
Figura 63. Arreglo puntual de APs.....	98
Figura 64. Canales no superpuestos en arreglo puntual.....	99
Figura 65. Canales DSSS.....	99
Figura 66. Reuso de canales en la banda de 2.4 GHz.....	100

Figura 67. Reuso de canales en 5 GHz con las bandas más bajas.....	101
Figura 68. Reuso de canales en 5 GHz con las bandas más bajas y medias.	101
Figura 69. Problema del nodo oculto.	112
Figura 70. Problema cerca/lejos.	113
Figura 71. Edificio de Ingenierías - Planta semisótano.	114
Figura 72. Edificio de Ingenierías - Planta primer piso.	115
Figura 73. Edificio de Ingenierías - Planta segundo piso.	115
Figura 74. Edificio de Ingenierías - Planta tercer piso.	115
Figura 75. Edificio de Ingenierías - Planta cuarto piso.	116
Figura 76. Edificio de Postgrados - Planta primer piso.....	116
Figura 77. Parque de Ingenierías.	117
Figura 78. Diagrama topológico red cableada.	119
Figura 79. Interferencia del proyecto EHAS – Tercer piso.	121
Figura 80. Interferencia del proyecto EHAS – Cuarto piso.....	121
Figura 81. Ubicación de los APs y sus antenas para los diferentes pisos del Campus.....	125
Figura 82. Cuarto piso máxima potencia recibida.	130
Figura 83. Cuarto piso máxima velocidad de datos.....	130
Figura 84. Tercer piso máxima potencia recibida.....	131
Figura 85. Tercer piso máxima velocidad de datos.	131
Figura 86. Segundo piso máxima potencia recibida.....	132
Figura 87. Segundo piso máxima velocidad de datos.	132
Figura 88. Primer piso máxima potencia recibida.....	133
Figura 89. Primer piso máxima velocidad de datos.....	133
Figura 90. Sótano máxima potencia recibida.....	134
Figura 91. Sótano máxima velocidad de datos.....	134
Figura 92. Postgrados máxima potencia recibida.....	135
Figura 93. Postgrados máxima velocidad de datos.....	135
Figura 94. Cuarto piso mejor AP para la velocidad de 1 Mbps.	136
Figura 95. Cuarto piso mejor AP para la velocidad de 11 Mbps.	136
Figura 96. Cuarto piso mejor AP para la velocidad de 54 Mbps.	136
Figura 97. Cuarto piso probabilidad de recepción para la velocidad de 1 Mbps.....	137
Figura 98. Cuarto piso probabilidad de recepción para la velocidad de 11 Mbps.....	137
Figura 99. Cuarto piso probabilidad de recepción para la velocidad de 54 Mbps.....	137
Figura 100. Cuarto piso número de canales recibidos para la velocidad de 1 Mbps.....	138
Figura 101. Cuarto piso número de canales recibidos para la velocidad de 11 Mbps.....	138
Figura 102. Cuarto piso número de canales recibidos para la velocidad de 54 Mbps.....	138

ACRONIMOS

ACK	Acknowledgment – Acuse de recibo.
AES	Advanced Encryption Standard – Estándar de encriptación avanzada.
AID	Association Identifier – Identificador de asociación.
AP	Access Point – Punto de acceso.
ARP	Address Resolution Protocol – Protocolo de resolución de direcciones.
ATIM	Announcement Traffic Indication Message - Mensaje de indicación de anuncio de tráfico.
BER	Bit Error Rate – Tasa de bits erróneos.
BPSK	Binary Phase Shift Keying – Modulación de cambio de fase binaria.
BSS	Basic Service Set - Conjunto de servicio básico.
BSSID	Basic Service Set Identifier – Identificador de conjunto de servicio básico.
CAT5	Categoría 5.
CCK	Complementary Code Keying – Modulación de código complementario.
CF	Contention Free – Libre contención.
CFP	Contention Free Period – Periodo de libre contención.
CRC	Cyclic Redundancy Check – Código de redundancia cíclica.
CSMA	Carrier Sense Multiple Access – Acceso múltiple por detección de portadora.
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance - Acceso múltiple por detección de portadora con evasión de colisión.
CW	Cotention Window – Ventana de contención.
CTS	Clear To Send – Listo para enviar.
DA	Destination Address – Dirección destino.
DBPSK	Differential Binary Phase Shift Keying – Modulación de cambio de fase binaria diferencial.
DCF	Distributed Coordination Function – Función de coordinación distribuida.
DHCP	Dynamic Host Configuration Protocol – Protocolo de configuración dinámica de anfitrión.
DIFS	Distributed Inter-Frame Space – Espacio entre trama distribuido.
DQPSK	Differential Quadrature Phase Shift Keying – Modulación de cambio de fase en cuadratura diferencial.
DS	Distribution System – Sistema de distribución.
DSS	Distribution System Service – Servicio del sistema de distribución

DSSS	Direct Sequence Spread Spectrum – Espectro ensanchado por secuencia directa.
EAP	Extensible Authentication Protocol – Protocolo de autenticación extensible.
EIFS	Extended Inter-Frame Space – Espacio entre tramas extendido.
EIRP	Effective Isotropic Radiated Power – Potencia radiada isotrópica efectiva PIRE.
ESS	Extended Service Set – Conjunto de servicio extendido.
FCC	Federal Communications Commission – Comisión federal de comunicaciones.
FCS	Frame Check Sequence – Secuencia de chequeo de trama.
FH	Frequency Hopping – Salto de frecuencia.
FHSS	Frequency Hopping Spread Spectrum – Espectro ensanchado por salto de frecuencia.
GFSK	Gaussian Frequency Shift Keying – Modulación de cambio de frecuencia Gaussiana.
GHz	Gigahertz.
HR/DSSS	High-Rate Direct Sequence Spread Spectrum – Espectro ensanchado por secuencia directa de alta velocidad.
IBSS	Independent Basic Service Set – Conjunto de servicio básico independiente.
ID	Identifier – Identificador.
IEEE	Institute of Electrical and Electronics Engineers – Instituto de ingenieros eléctricos y electrónicos.
IP	Internet Protocol – Protocolo internet.
IR	Infrared – Infrarrojo.
ISA	Industry Standar Architecture – Arquitectura de estándar industrial.
ISM	Industrial, Scientific and Medical – Industrial, científico y médico.
IV	Initialization Vector – Vector de inicialización.
LAN	Local Area Network – Red de área local.
LLC	Logical Link Control – Control de enlace lógico.
MAC	Medium Access Control – Control de acceso al medio.
MHz	Megahertz.
MPDU	MAC Protocol Data Unit – Unidad de datos de protocolo MAC.
MSDU	MAC Service Data Unit – Unidad de datos de servicio MAC.
NAT	Network Address Translation – Traducción de dirección de red.
NAV	Network Allocation Vector – Vector de ubicación de red.
OFDM	Orthogonal Frequency Division Multiplexing – Multiplexación por división de frecuencia ortogonal.
OSI	Open Systems Interconnection – Interconexión de sistemas abiertos.
PC	Personal Computer – Computador personal.

PCF	Point Coordination Function – Función de coordinación puntual.
PCI	Peripheral Component Interconnect – Conexión interna para componente periférico.
PCMCIA	Personal Computer Memory Card International Association – Asociación internacional de tarjetas de memoria para computadora personal.
PDA	Personal Digital Assistant – Asistente digital personal.
PDU	Protocol Data Unit – Unidad de datos de protocolo.
PLCP	Physical Layer Convergence Procedure – Procedimiento de convergencia de la capa física.
PIFS	PCF Inter-Frame space – Espacio entre tramas PCF.
PMD	Physical Medium Dependent – Dependiente del medio físico.
PPDU	PLCP Protocol Data Unit – Unidad de datos de protocolo PLCP.
POP	Post Office Protocol – Protocolo de oficina de correos.
PoE	Power Over Ethernet – Potencia sobre Ethernet.
PRNG	Pseudo Random Number Generator – Generador de números seudo aleatorio.
PS	Power Save – Ahorro de potencia.
PSDU	PLCP Service Data Unit – Unidad de datos de servicio PLCP.
PSK	Phase Shift Keying – Modulación de cambio de fase.
QPSK	Quadrature Phase Shift Keying – Modulación de cambio de fase en cuadratura.
RA	Receiver Address – Dirección de receptor.
RADIUS	Remote Authentication Dial In User Service - Servicio de usuario de acceso telefónico de autenticación remota.
RF	Radio Frequency – Radiofrecuencia.
RTS	Request to Send – Petición para enviar.
SA	Source Address – Dirección fuente.
SDU	Service Data Unit – Unidad de datos de servicio.
SIFS	Short Inter-Frame Space – Espacio entre tramas corto.
Sinc.	Sincronización.
SMTP	Simple Mail Transfer Protocol – Protocolo de transferencia de archivo simple.
SNMP	Simple Network Management Protocol – Protocolo de gestión de red simple.
SS	Station Service – Servicio de la estación.
SSID	Service Set Identity – Identificador de conjunto de servicio.
TA	Transmitter Address – Dirección del transmisor.
TIM	Traffic Indication Map – Mapa de indicación de tráfico.
UNII	Unlicensed National Information Infrastructure - Infraestructura de información nacional sin licencia.

USB	Universal Serial Bus – Bus serial universal.
WEP	Wired Equivalent Privacy – Privacidad equivalente cableada.
WLAN	Wireless Local Area Network – Red de área local inalámbrica.
WM	Wireless médium – Medio inalámbrico.

INTRODUCCION

Sin lugar a dudas uno de los mejores inventos del siglo XX fue la red de redes "internet", a partir del surgimiento de esta red, el mundo cambió y se ha ido metiendo en la cotidianidad de las personas para poder comunicar, estudiar, informar, vender, comprar y hacer muchas otras actividades; hasta hace pocos años, el acceso a internet se podía hacer únicamente por medio de computadores conectados físicamente a una red. Pero en este nuevo siglo, el mundo está viviendo el auge de la tecnología inalámbrica móvil para la comunicación de datos, lo que años atrás se veía como un sueño, ya es una realidad. El avance en cuanto a estandarización, regulación y desarrollo tecnológico han hecho posible este sueño.

El mundo de las redes inalámbricas móviles para comunicaciones de datos se ha visto invadido por diversas tecnologías, pero indudablemente la tecnología que más adeptos ha cautivado últimamente ha sido 802.11, la cual ha sido desarrollada por el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos). 802.11 hace referencia a una familia de normas para redes inalámbricas y es actualmente la tecnología inalámbrica que goza de la mayor aceptación, muestra de ello la gran evolución de la tecnología permitiendo la disponibilidad de variedad y cantidad de equipos en el mercado, así como la implementación masiva de los puntos de conexión públicos, conocidos como *hotspots*.

En razón de los adelantos tecnológicos el Ministerio de Comunicaciones de Colombia, con la aprobación el 21 de abril de la resolución 689 de 2004, dio vía libre al uso de ciertas bandas de frecuencia para el uso de sistemas inalámbricos para la comunicación de datos, esta resolución está conforme con los estándares y las normas técnicas internacionales, permitiendo el buen desarrollo de las redes inalámbricas en nuestro país.

Ya no es raro ver a una persona consultando su correo en una cafetería, hotel, parque y en sitios tan impensables como los aviones, los anteriores son unos pocos ejemplos de lugares donde la tecnología inalámbrica ha incursionado. Las universidades son una muestra de cómo se han involucrado las tecnologías inalámbricas con fines educativos e investigativos para disponer de un acceso a la red a cualquier hora y en cualquier lugar. Con una red inalámbrica se puede extender la funcionalidad de una red a auditorios, salones de clase, salones de reuniones, oficinas, cafeterías, espacios públicos, bibliotecas, parques, etc.; contribuyendo a ofrecer mayor cobertura

de la red para poder suplir la creciente demanda de servicios por parte de una comunidad académica. El concepto de conectividad inalámbrica ha cambiado de ser algo novedoso a algo necesario y el acceso inalámbrico a internet se ha convertido en la herramienta principal para la mayoría de las actividades esenciales de los campus universitarios.

El proceso de enseñanza y aprendizaje en las instituciones educativas ha cambiado gracias a la tecnología inalámbrica y a partir de esta premisa es que nace el proyecto denominado “**Análisis y diseño de una red inalámbrica bajo las normas IEEE 802.11(x).para el Campus de Ingenierías - sector Tulcán**”. El proyecto integra conceptos del área de las telecomunicaciones y busca responder a una necesidad de ampliación de la red de la Universidad del Cauca, que día a día tiene más demanda.

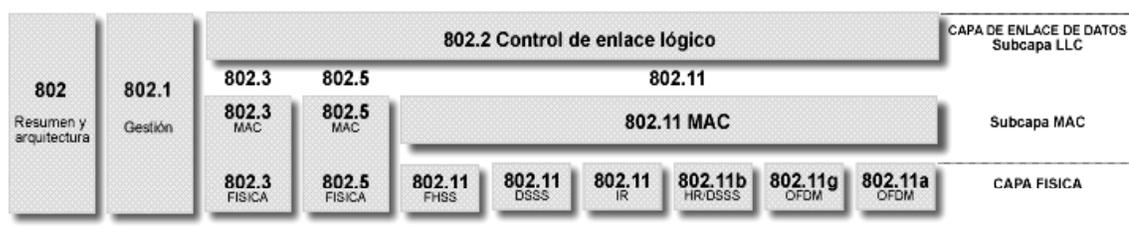
El alcance del proyecto es el análisis y diseño, solamente resta la implementación, que de hacerse puede convertirse en el inicio de una era inalámbrica para la Universidad, beneficiándose la comunidad académica y que muy seguramente se vera reflejado en la proyección que tiene la Universidad a nivel nacional e internacional. Es importante resaltar que el proyecto queda abierto para trabajos posteriores pertenecientes a la temática de las redes inalámbricas, ya que es un tema muy amplio y permite la creación de diversos proyectos.

En este proyecto de grado se hace un estudio de las normas IEEE 802.11 y al final aplicarlas a un caso práctico que es el diseño de una red de área local inalámbrica para el campus de ingenierías. En los dos primeros capítulos se describe detalladamente la tecnología 802.11. En el tercer capítulo se hace referencia a la infraestructura de una red de área local inalámbrica y como ocurre la propagación de la señal en el espacio libre. En el cuarto capítulo se muestra un modelo para el diseño de una red de área local inalámbrica, este modelo se presenta a manera general para ser una guía en el diseño de redes inalámbricas; el modelo presentado puede ser aplicado a las diferentes sedes de la Universidad del Cauca para poder diseñar e implementar una red de este tipo. En el quinto capítulo se localiza y analiza el escenario sobre el cual se orienta el trabajo “Campus de Ingenierías de la Universidad del Cauca” para desembocar en la aplicación del modelo tratado en el capítulo cuatro y finalmente, cumplir con el objetivo cual es el diseño de la red inalámbrica.

1. NORMAS IEEE 802.11 SUBCAPA MAC

Las normas IEEE 802 se enfocan a las dos capas de más bajo nivel del modelo OSI, estas son: la capa de enlace de datos y la capa física, ver figura 1. Las especificaciones individuales se identifican con un segundo número, 802.2 especifica la capa de control de enlace de datos (LLC Logical Link Control), la cual interactúa con las capas más bajas de la tecnología LAN. Las características de gestión para las redes 802 se especifican en 802.1, por ejemplo VLANs (802.1q) y puentes (802.1d). 802.11 es solo otra capa que usa encapsulación capa de control de enlace lógico (802.2). Específicamente las normas IEEE 802.11 se enfocan a la subcapa de control de acceso al medio (MAC Medium Access Control) y a la capa física. La subcapa MAC* es un conjunto de reglas que determinan como se accede al medio y se envían los datos. La capa física** es la encargada de la transmisión y recepción de los datos.

Figura 1. IEEE 802 y su relación con el modelo OSI.



Como se puede apreciar en la figura anterior, 802.11 tiene una especificación MAC común para las diferentes capas físicas 802.11. Las diferentes especificaciones físicas serán tratadas en el capítulo 2.

Este capítulo cubre la subcapa MAC 802.11 incluyendo los conceptos básicos y características principales de la norma IEEE 802.11, fundamentales para el diseño, la administración, la solución de problemas y la implementación de una red de área local inalámbrica. Se analiza la forma como los clientes deben conectarse a un Punto de Acceso (AP Access Point), los términos usados para la configuración de una red de área local inalámbrica (WLAN Wireless Local Area Network), servicios, formato de tramas, seguridad y el modo como se administra la potencia en los clientes.

* Basado en la norma IEEE 802.11-1999, publicación disponible en el Institute of Electrical and Electronics Engineers. <http://standards.ieee.org/getieee802/802.11.html>

** Basado en la norma IEEE 802.11-1999, 802.11a-1999, 802.11b-1999 y 802.11g-2003 publicaciones disponibles en el Institute of Electrical and Electronics Engineers. <http://standards.ieee.org/getieee802/802.11.html>

En el Anexo A se detallan las tramas manejadas en la subcapa MAC.

1.1 ARQUITECTURA 802.11

La arquitectura 802.11 consta de muchos componentes que interactúan para proporcionar una comunicación LAN inalámbrica, que soporta movilidad a las estaciones de una forma transparente para los niveles superiores. La arquitectura 802.11 se describe como una serie de celdas interconectadas y consiste de:

- Componentes básicos: estación o cliente; punto de acceso (AP); medio inalámbrico (WM Wireless Medium) y sistema de distribución (DS Distribution System).
- Conjunto de servicio: conjunto de servicio básico (BSS Basic Service Set), conjunto de servicio extendido (ESS Extended Service Set) y conjunto de servicio básico independiente (IBSS Independent Basic Service Set).
- Interfaces de servicios: servicios de la estación (SS Station Service) y servicios del sistema de distribución (DSS Distribution System Service).

1.1.1 Componentes básicos: son los componentes fundamentales para la creación de una red inalámbrica 802.11. Los componentes básicos son mostrados en la figura 2.

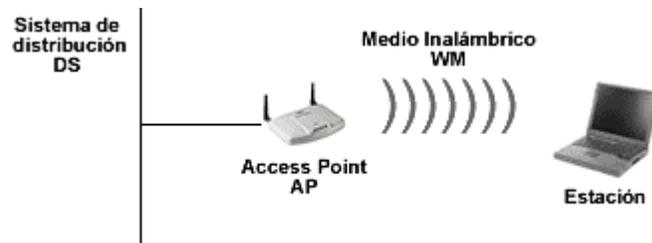
Estaciones o clientes: el propósito principal de una red es la transferencia de datos entre dos o más estaciones. Las estaciones 802.11 son dispositivos que usan interfaces de red inalámbrica llamadas dispositivos inalámbricos. En el caso de redes inalámbricas las estaciones son computadores portátiles, asistentes personales digitales (PDA Personal Digital Assistant), y otros dispositivos que funcionan con batería; sin embargo, estos no son los únicos dispositivos que pueden usar una red inalámbrica, ya que en algunos ambientes son usados computadores de escritorio para la transmisión de tramas mediante redes 802.11.

Punto de acceso (AP): es el dispositivo inalámbrico central de una WLAN que tiene como objeto principal agrupar diferentes estaciones, el AP controla la información que entra a su grupo para enviarla a la estación destino y controla la información que sale de su grupo para entregarla a otro dispositivo de interconexión de red que puede ser un concentrador, un *switch*, un enrutador, u otro AP. Este tipo de dispositivo es una estación que puede hacer las veces de adaptador entre una red cableada y una red inalámbrica, donde convierte tramas de un tipo a otro, por ejemplo, de tramas tipo 802.3 a 802.11 y viceversa.

Medio inalámbrico (WM): para la transmisión de las tramas entre estaciones, las normas 802.11 utilizan el aire. La arquitectura permite que múltiples capas físicas sean soportadas por la capa 802.11 MAC.

Sistema de distribución (DS): el sistema de distribución es el componente lógico de 802.11 usado para la transmisión de las tramas entre APs. Es usado para interconectar un conjunto de servicio básico (BSS) y LANs para crear un conjunto de servicio extendido (ESS), lo que significa que en muchos casos se usa la red Ethernet para transmitir tramas entre APs. Un DS puede ser cableado, inalámbrico, LAN, WAN o cualquier otro método de conectividad de red.

Figura 2. Componentes básicos de una LAN 802.11.



1.1.2 Conjunto de servicio: el término conjunto de servicio se usa para describir la integración de los componentes básicos de una red de área local inalámbrica. Existen tres formas de configurar una WLAN con diferente hardware.

Conjunto de servicio básico (BSS): un BSS consta de un solo AP y uno o más clientes. Como requisito para pertenecer a un BSS la estación debe estar dentro del rango de cobertura del AP. En la figura 3 se muestra un BSS compuesto por un AP y tres clientes que se encuentran dentro de su cobertura.

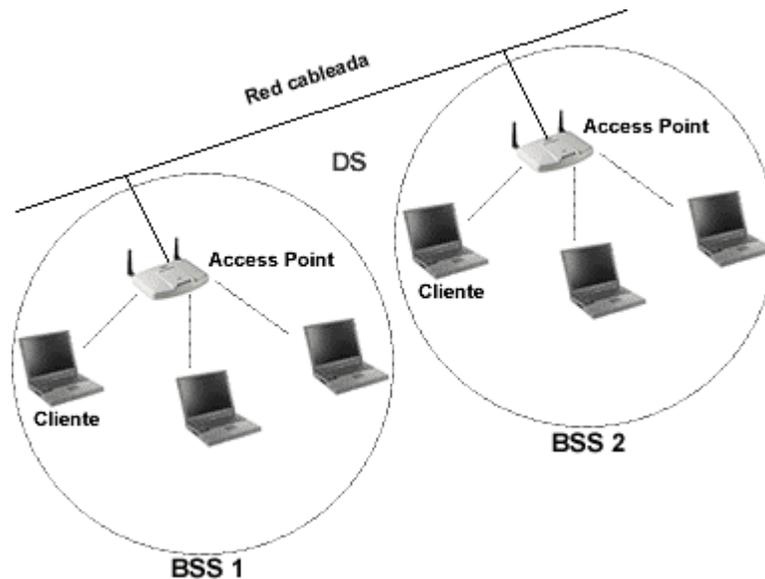
Cuando un BSS se conecta a una red cableada, la configuración de la red es llamada modo infraestructura. No se permite la transmisión cliente-cliente. Cada cliente inalámbrico debe usar el AP para comunicarse con otros clientes inalámbricos o cableados de la red. Las velocidades de datos dentro del círculo dependen de la tecnología usada. Un BSS debe tener un único identificador de conjunto de servicio (SSID Service Set Identifier), que es el nombre que identifica una red 802.11, el SSID diferencia una red inalámbrica de otra red, es un identificador único de 32 caracteres.

Figura 3. Conjunto de servicio básico.



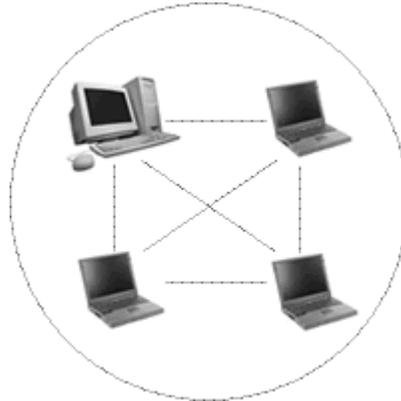
Conjunto de servicio extendido (ESS): el ESS se refiere a dos o más BSS interconectados por un sistema de distribución común (DS) el cual forma la columna de la WLAN. Un ESS cubre múltiples celdas, tiene capacidad de *roaming* y requiere el mismo SSID para todos los BSS. Ver figura 4.

Figura 4. Conjunto de servicio básico extendido.



Conjunto de servicio básico independiente (IBSS): típicamente, un IBSS está compuesto de un número relativamente pequeño de estaciones, aproximadamente 5, configuradas para un corto período de tiempo. Un uso común es el de crear una red que soporte una reunión en un salón; concebida para corta duración, pequeño tamaño y enfocada a un propósito específico, un IBSS es denominado también red *Ad hoc*. Este tipo de red no tiene un AP o cualquier otro acceso a un servicio de distribución, cubre una única celda y tiene un SSID. Ver figura 5.

Figura 5. Conjunto de servicio básico independiente.



1.1.3 Interfaces de servicios: la arquitectura 802.11 permite que el DS pueda ser creado por tecnologías diferentes, por lo tanto no hay restricción en la implementación del DS, mientras que sí específica servicios. Estos servicios son asociados con diferentes componentes de la arquitectura y se encuentran divididos en dos categorías: servicios de la estación (SS) y servicios del sistema de distribución (DSS). Ambas categorías son usadas por la subcapa MAC.

1.1.3.1 Servicios de la estación: los SS están presentes en las estaciones y APs. A este grupo pertenecen 4 servicios: autenticación, des-autenticación, privacidad y entrega de datos.

Autenticación: este servicio verifica la identidad del dispositivo inalámbrico. Si el AP no reconoce la identidad del dispositivo, no le permite el acceso a la WLAN. Es un servicio a través del cual un cliente inalámbrico (tarjeta PC, USB, cliente, AP), verifica su identificación en la red ante un AP. Para este proceso, el cliente envía una trama de petición de autenticación al AP que se encuentra en modo infraestructura, este último debe aceptar o denegar la petición; luego el AP debe notificar su decisión con una trama de respuesta de autenticación. Una estación o cliente puede autenticarse con más de un AP al tiempo, de modo que prepara a otros APs para entrar a su BSS. Ver figura 6.

Des-autenticación: este servicio se usa para destruir la identidad de una estación previamente autenticada, una vez una estación se des-auténtica ya no puede acceder a la WLAN. Este servicio es invocado cuando una estación está bloqueada por un obstáculo o cuando está saliendo del rango del AP, con este servicio se logra liberar recursos para otras estaciones.

Figura 6. Servicio de autenticación.



Privacidad: es usado para proteger los datos cuando pasan por la WLAN, su propósito es proporcionar un nivel de protección equivalente al de la red cableada, por esta razón este servicio es llamado privacidad equivalente cableada (WEP Wired Equivalent Privacy), ya que este proceso no es seguro para la red, existen otros mecanismos para resolver el problema de inseguridad como se explica en el numeral 1.11 referente a seguridad.

Entrega de datos: las redes no son útiles sin el intercambio de datos, este servicio proporciona a una estación transmisora la capacidad de entregar datos a una estación receptora, estos datos son llamados unidad de datos de servicio MAC (MSDU MAC Service Data Unit).

1.1.3.2 Servicios del sistema de distribución: son los servicios proporcionados por el DS, son accedidos y suministrados por los APs, ya que estos son los que se conectan al DS. A este grupo pertenecen 5 servicios: asociación, des-asociación, distribución, integración y re-asociación. Estos servicios toman decisiones respecto a donde las tramas 802.11 deben ser enviadas. Estos servicios se usan para *roaming* cuando un cliente o estación está en movimiento.

Asociación: es el paso siguiente después de la autenticación, este servicio establece una conexión lógica entre una estación y el AP. Determina la trayectoria que el DS necesita para alcanzar el dispositivo. Si la estación no tiene una asociación con un AP, el DS no sabrá donde está ubicada la estación. Una estación se asocia con un único AP. Ver figura 7.

Des-asociación: este servicio es usado para deshacer la asociación entre el AP y la estación. Esto puede ser por ejemplo, cuando la estación sale del área del AP o el AP se apaga.

Distribución: este servicio es usado por el AP cuando envía datos a un destino una vez una trama ha sido aceptada por el AP. Usando distribución se determina si los datos deben ser enviados a

otra estación o a otro AP o si la trama debe ser dirigida fuera de la WLAN dentro de una red cableada.

Figura 7. Servicio de asociación.



Integración: este servicio hace la traducción de datos del formato 802.11 a formato de trama de red cableada y viceversa.

Re-asociación: este servicio se presta cuando una estación se mueve entre áreas de servicio básico dentro de un área de servicio extendido. La re-asociación es iniciada por la estación móvil cuando las condiciones de calidad de señal indican que es mejor asociarse con otro AP o cuando hay *roaming*. Una vez es llevada a cabo la re-asociación, el DS actualiza sus registros de ubicación para notificar el cambio a un nuevo AP.

1.1.3.3 Relación entre servicios: el proceso completo de autenticación y asociación tiene tres estados diferentes:

- Estado 1: no autenticado y no asociado
- Estado 2: autenticado y no asociado
- Estado 3: autenticado y asociado

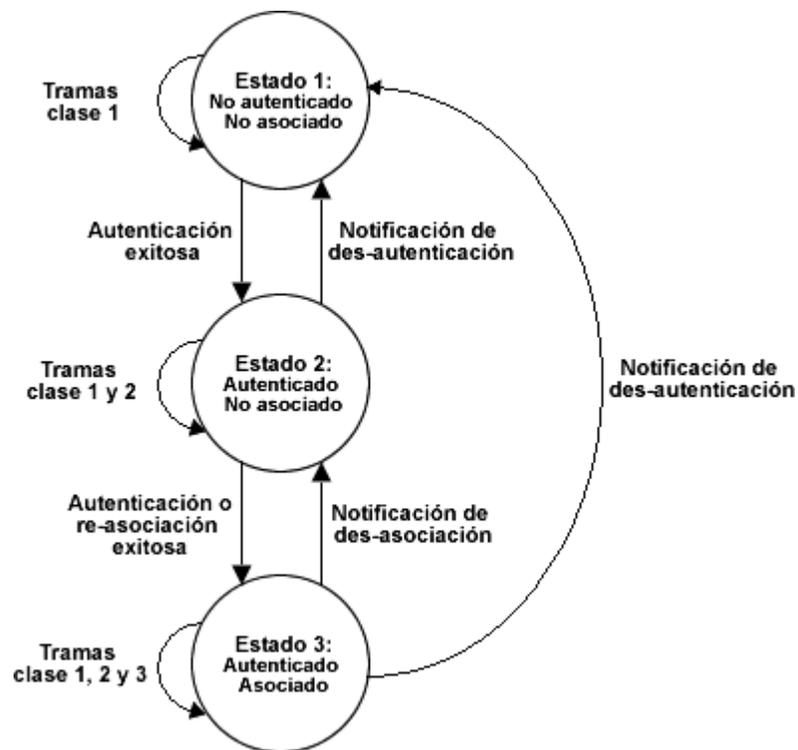
No autenticado y no asociado: en este primer estado la estación está desconectada de la red y es incapaz de pasar tramas a través del AP. Los APs guardan tablas del estado del cliente conocidas como tablas de asociación. No autenticado es cuando la estación no ha completado el proceso de autenticación o ha fallado.

Autenticado y no asociado: en este segundo estado el cliente ha pasado el proceso de autenticación pero aún no se encuentra asociado por lo tanto no se le permite al cliente o a la estación recibir o enviar datos a través del AP. Las tablas de asociación del AP muestran “autenticado” e inmediatamente se inicia el proceso de asociación.

Autenticado y asociado: en esta último estado la estación está completamente conectada a la red y es capaz de enviar y recibir datos a través del AP. En la tabla de asociación aparece “asociado”, indicando que ya se han realizado los procesos anteriores, de modo que ya puede haber intercambio de datos. Con esto, se deduce que las medidas de seguridad deben ser implementadas en el momento en que el cliente hace el proceso de autenticación, esto se verá más adelante en el numeral 1.11 referente a seguridad.

El estado actual entre dos estaciones determina el tipo de trama 802.11 que puede ser intercambiada. Los tipos de trama permitidos se clasifican en clases, las cuales corresponden a los estados de la estación. En el estado 1 se permiten solo tramas clase 1, en el estado 2 son permitidas las tramas clases 1 o 2 y en el estado 3 las clases 1, 2 o 3. Como se observa en la figura 8.

Figura 8. Relación entre variables de estado y servicios.



Las clases de tramas son definidas de la siguiente manera:

Tramas clase 1 (permitidos los estados 1, 2 y 3):

- Tramas de control: petición para enviar (RTS Request To Send), listo para enviar (CTS Clear To Send), acuse de recibo (ACK ACKnowledgment), acuse de recibo del fin de libre contención (CF-End + CF-ACK) y fin de libre contención (CF-End).
- Tramas de gestión: petición y respuesta de prueba, baliza, autenticación, des-autenticación y mensaje de indicación de anuncio de tráfico (ATIM Announcement Traffic Indication Message).
- Tramas de datos: tramas de datos entre las estaciones de un mismo IBSS.

Tramas clase 2 (permitidos los estados 2 y 3):

- Tramas de gestión: petición y respuesta de asociación, petición y respuesta de re-asociación y des-asociación.

Tramas clase 3 (permitido solo el estado 3):

- Tramas de datos: todas las tramas de datos son permitidas.
- Tramas de gestión: des-autenticación.
- Tramas de control: sondeo de ahorro de potencia (PS-Poll Power Save Poll).

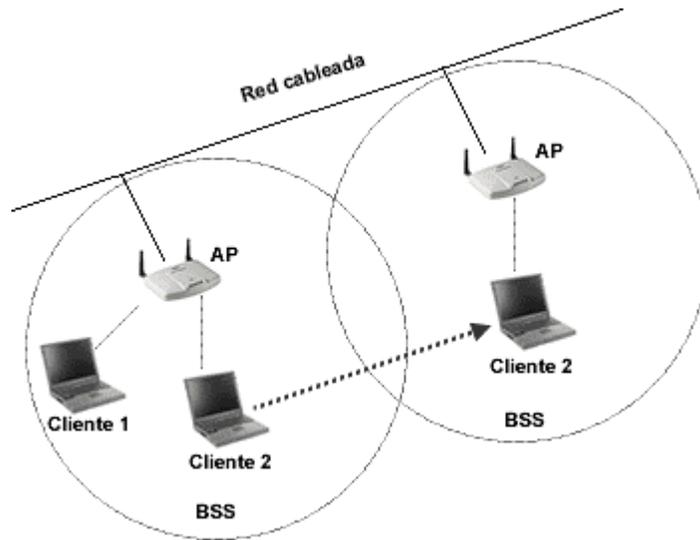
Las tramas anteriores se explican detalladamente en el Anexo A.

1.2 ROAMING

El *roaming* es la capacidad que tiene un cliente inalámbrico para moverse a través de diferentes celdas o BSS sin perder la conectividad a la red, los APs permiten una transferencia entre los clientes de una forma transparente a ellos. *Roaming* es análogo al proceso de *handover* realizado en telefonía celular. En la figura 9 se muestra el proceso de roaming de un cliente entre dos BSS.

El *roaming* se basa en la habilidad que tiene la estación para determinar la calidad de la señal inalámbrica de cualquier AP dentro de su alcance. Para poder tomar la decisión de cambiar la comunicación a un nuevo AP, se basa en las balizas que transmiten los APs, la estación escucha estas balizas y determina cual AP tiene la señal más clara o sea la de mejor relación señal a ruido (S/N). Luego la estación envía la información de autenticación e intenta re-asociarse con el nuevo AP, si la re-asociación es exitosa la estación notifica al anterior AP para que este libere los recursos. El anterior AP y el nuevo AP se comunican para coordinar el proceso de roaming.

Figura 9. Roaming entre ESS.



1.3 ACCESO MÚLTIPLE POR DETECCIÓN DE PORTADORA CON EVASIÓN DE COLISIÓN (CSMA/CA)

CSMA/CA consiste en escuchar el medio y esperar antes de transmitir. Antes de enviar un paquete, la estación escucha si otra estación está transmitiendo (detección de portadora). Si alguna está transmitiendo, evita colisiones (evasión de colisión) esperando un tiempo aleatorio determinado por el algoritmo de retroceso exponencial binario y luego escucha de nuevo. Cuando la estación detecta que el medio está libre comienza a decrementar su contador. Cada estación tiene una ventana de contención (CW Contention Window) para determinar el número de ranuras de tiempo que la estación debe esperar antes de empezar a transmitir. El contador se decrementa después de que el medio ha estado libre por un intervalo de tiempo DIFS, explicado en la sección 1.4.1. Si el contador llega a cero y el medio aún está libre, la estación comienza a transmitir. Si dos estaciones transmiten al mismo tiempo, ocurre una colisión, cada una de ellas aleatoriamente elige un periodo de su CW e intenta ganar control del medio de nuevo.

El mecanismo de acceso básico para 802.11 es CSMA/CA con el algoritmo de retroceso exponencial binario, que sirve para determinar el tiempo de espera, es una progresión exponencial que se consigue multiplicando un número aleatorio con una ranura de tiempo de la capa física. El tiempo de retroceso se calcula como potencias de 2 menos 1, por ejemplo, si el valor aleatorio es 3 y la ranura de tiempo es 10 ms la estación podría esperar $(2^3 - 1) * 10$ ms. Si hay reintentos el exponente aumenta y el tiempo aleatorio sería $2^4 - 1$, luego $2^5 - 1$ y así sucesivamente.

Petición para enviar / listo para enviar (RTS/CTS): RTS/CTS es una extensión del mecanismo CSMA/CA, sirve para reservar el medio durante un determinado tiempo. Cuando existen muchas colisiones este mecanismo es usado para evitarlas o disminuir su probabilidad. Se debe configurar después de un minucioso estudio de las características de las colisiones de la red, rendimiento, retardo, etc. También se usa para solucionar el problema del nodo oculto, el cual hace referencia a que un cliente es incapaz de escuchar las transmisiones de los otros, por lo tanto cree que el medio está libre, esta situación genera muchas colisiones.

Configuración de RTS/CTS: existen tres formas para configurar el AP y las estaciones con RTS/CTS. Estas son encendido, apagado y encendido con nivel.

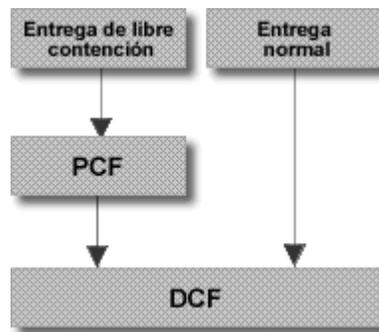
- Encendido: todas las estaciones que desean transmitir una trama por la WLAN previamente deben hacer una petición (RTS) y esperar una trama listo para enviar (CTS) de la estación receptora, con este proceso se genera una cantidad de bits de encabezado y por consiguiente se reduce el rendimiento.
- Encendido con nivel: permite que el administrador de una red inalámbrica fije un nivel de mínimo tamaño de tramas a las cuales se les permite hacer RTS/CTS. Si el paquete que se está transmitiendo es mayor que el nivel, se inicia el mecanismo RTS/CTS. Si el paquete es igual o menor que el nivel, no se inicia el mecanismo RTS/CTS. Con esto se trata de evitar colisiones, ya que estas afectan a las tramas más grandes.

1.4 MODOS DE ACCESO MAC

El acceso al medio es controlado por dos funciones: función de coordinación distribuida (DCF Distributed Coordination Function) y función de coordinación puntual (PCF Point Coordination Function). Estas dos funciones determinan cuando una estación puede enviar o recibir tramas dentro del BSS. Como se muestra en la figura 10, DCF se puede usar sin PCF, pero PCF no se puede usar sin DCF.

Función de coordinación distribuida: la DCF es la base del mecanismo de acceso múltiple por detección de portadora con evasión de colisión (CSMA/CA). DCF permite a todas las estaciones de una WLAN, competir por el acceso al medio. DCF puede ser usado por BSS, ESS e IBSS, ver sección 1.5.2.

Figura 10. Funciones de coordinación MAC.



Función de coordinación puntual: es usada cuando una estación coordina el proceso de comunicación por lo tanto las estaciones no pueden competir por el acceso al medio. La PCF es configurada en los APs y solo puede ser usada en redes modo infraestructura. PCF garantiza una cantidad conocida de latencia, de modo que puede soportar aplicaciones en tiempo real, tales como voz y video.

Sincronización: todas las estaciones en una WLAN deben estar sincronizadas en tiempo, para lograr lo anterior la norma 802.11 define el espacio entre tramas (IFS InterFrame Space). IFS hace referencia a los espacios de tiempo que son usados en una red 802.11. El espacio entre tramas cumple un papel fundamental en la coordinación del acceso al medio. 802.11 usa cuatro espacios entre tramas diferentes, ellos son: EIFS, SIFS, PIFS y DIFS, los cuales dependen del tipo de tecnología.

- *Espacio entre tramas extendido (EIFS Extended InterFrame Space):* espacio de longitud variable usado como un período de espera cuando se recibe mal una trama.
- *Espacio entre tramas corto (SIFS Short InterFrame Space):* es el espacio entre tramas más corto. Va antes y después de que los mensajes son enviados. Tiene el más alto nivel de prioridad, ya que todas las estaciones escuchan el medio esperando que esté libre, cuando el medio está libre, cada estación debe esperar un período de tiempo antes de comenzar a transmitir, este tiempo depende de la función que la estación necesita desempeñar. Las funciones de más alta prioridad son las tramas RTS, CTS y ACK.
- *Espacio entre tramas de función de coordinación puntual (PIFS PCF InterFrame Space):* proporciona el segundo nivel de prioridad, tiene mayor prioridad que DIFS y menor que

SIFS. El AP usa PIFS solo cuando la red está en modo PCF; ya que PIFS tiene menos duración que DIFS, el AP podría ganar el acceso al medio antes que cualquier estación DCF.

- *Espacio entre tramas de función de coordinación distribuida (DIFS DCF InterFrame Space):* usado por defecto por las estaciones que usan DCF. Es el más largo de los espacios entre tramas.

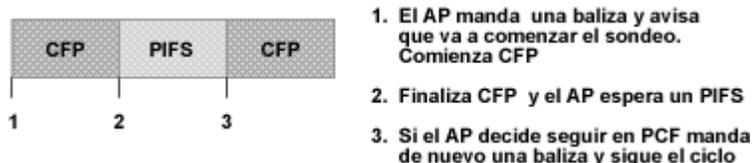
Otro término usado es el de ranura de tiempo, es un periodo estándar usado para temporizar. La ranura de tiempo al igual que el espacio entre tramas depende del tipo de tecnología 802.11.

1.5 PROCESO DE COMUNICACIÓN

Para poder entender mejor el funcionamiento de una red inalámbrica en modo PCF y modo DCF, se describe a continuación el proceso de comunicación de cada uno.

1.5.1 Proceso de comunicación en modo PCF: cuando el AP está en modo PCF, primero manda una baliza indicando que la comunicación se va a realizar en modo de sondeo, por un tiempo denominado periodo de libre contención (CFP Contention Free Period), durante el cual, el AP tiene el control del medio para sondear las estaciones una por una y determinar si alguna necesita enviar datos. Si una estación no necesita enviar datos, envía una trama nula (no hay datos) en respuesta al sondeo, el sondeo continúa alternando los momentos para que una estación transmita datos y finaliza cuando expira el periodo de libre contención. Luego del periodo de libre contención (CFP), las estaciones y el AP esperan un periodo de tiempo para luego competir por el medio, las estaciones esperan un DIFS y el AP espera un PIFS. Ya que el PIFS es menor que el DIFS, parecería que el AP siempre gana el acceso al medio, si el AP quiere continuar en modo PCF gana el acceso al medio y el proceso de comunicación en modo PCF vuelve a comenzar, de lo contrario las estaciones compiten por el medio luego del DIFS y se inicia un proceso de comunicación en modo DCF. Ver figura 11.

Figura 11. Proceso de comunicación en modo PCF.



1.5.2 Proceso de comunicación en modo DCF: en este caso no hay sondeo. Las estaciones esperan que termine el DIFS, para luego competir por el medio, durante un tiempo denominado periodo de contención (CP Contention Period). Durante el periodo de contención, las estaciones calculan su tiempo pseudo aleatorio, el cual depende de un número aleatorio multiplicado por una ranura de tiempo. La estación con el tiempo más corto, gana el acceso al medio y envía sus datos. La estación transmisora espera un SIFS para que llegue un ACK y el proceso comienza de nuevo con un nuevo DIFS. Ver figura 12.

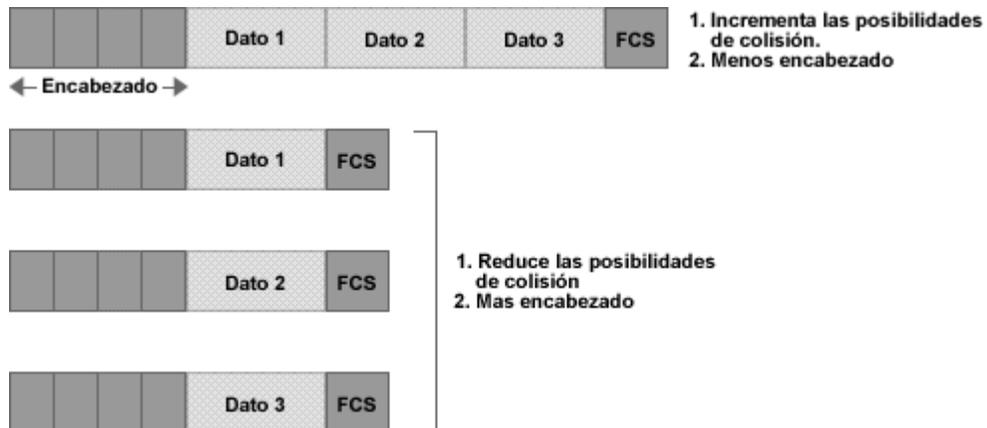
Figura 12. Proceso de comunicación en modo DCF.



1.6 FRAGMENTACION

En un ambiente propenso a la interferencia, existe la posibilidad de que uno o más bits de una trama se alteren durante la transmisión, sin importar el número de bits alterados, la trama necesita ser re-enviada. El administrador puede configurar la característica de fragmentación en una red 802.11 especificando tramas pequeñas en ambientes con mucha interferencia y tramas grandes en ambientes sin interferencia. Cuando se envían fragmentos cortos, se reduce la capacidad de la red ya que cada fragmento debe tener su propio encabezado, pero se reduce el tiempo de retransmisiones cuando hay errores. Es importante encontrar la fragmentación óptima para maximizar el rendimiento de la red. La trama más grande que puede atravesar una WLAN sin fragmentación es 1518 bytes. Lo anterior es mostrado en la figura 13.

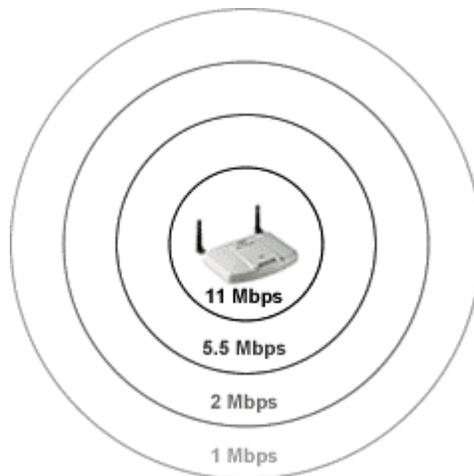
Figura 13. Fragmentación.



1.7 CAMBIO DINÁMICO DE VELOCIDAD

Es un método de ajuste de velocidad automática que ocurre cuando el cliente se aleja o se acerca a un AP o cuando existe un incremento en la interferencia. En las redes 802.11 este ajuste de velocidad hace saltos discretos a velocidades específicas que son determinadas dependiendo del estándar que se ha implementado, de este modo en una red 802.11b estas velocidades son 11 Mbps, 5.5 Mbps, 2 Mbps y 1 Mbps, como se puede ver en la figura 14. Estas velocidades se disminuyen a medida que la estación se aleja del AP.

Figura 14. Cambio de velocidad dinámica 802.11b.



1.8 BALIZAS

Son tramas de gestión que son enviadas desde el AP a una estación en modo infraestructura y de estación a estación en modo *Ad hoc*, sirven como referencia para organizar y sincronizar la comunicación inalámbrica en una WLAN. Entre sus funciones están sincronización, parámetro FH y DS, SSID, mapa de indicación de tráfico (TIM Traffic Indication Map) y las velocidades soportadas.

- Sincronización: esta función se realiza en el cliente en el momento exacto de la transmisión, cuando el cliente recibe la baliza, sincroniza su reloj con respecto al del AP.
- Parámetro FH o DS: informa sobre el tipo de tecnología de espectro ensanchado que va a ser usado.
- SSID: es el nombre de la red, debe ser único, y de 2 a 32 caracteres. Es usado para segmentar las redes como una medida de seguridad rudimentaria. El administrador debe configurar el SSID en cada AP, la estación se configura con el SSID de la red a la cual

quiere acceder. Cuando la estación recibe esta información también recibe la dirección MAC del AP, con esto ya puede autenticarse y asociarse con este AP. La estación se une al AP que tenga la señal más fuerte, en el caso de que existan múltiples APs.

- Mapa de indicación de tráfico: es usado como un indicador de cuales estaciones inactivas tienen paquetes en cola de espera en el AP. Cuando esto sucede los APs mandan balizas a todas las estaciones, de modo que las que se encuentran inactivas se encienden y verifican si tienen información en cola, si es así, ellas continúan activas, en el caso contrario regresan a estado inactivo.
- Velocidades soportadas: en las balizas se envía las velocidades que pueden ser soportadas por el AP.

1.9 BUSQUEDA

Cuando se configura, se instala y finalmente se enciende un cliente 802.11, éste automáticamente detecta si existe una red WLAN dentro de su cobertura. A este proceso de escucha se le conoce como búsqueda y ocurre antes de cualquier otro proceso. Existen dos clases de búsqueda: la pasiva y la activa.

1.9.1 Búsqueda pasiva: es el proceso de escuchar balizas enviadas por el AP (modo infraestructura) o estaciones clientes (modo *Ad hoc*) en cada canal por un periodo de tiempo. La estación que hace la búsqueda, cataloga las características del AP o de la estación que manda las balizas y captura el SSID para intentar unirse a la red. Cuando muchas balizas llegan, el cliente se conecta con el AP que envió la baliza con mayor magnitud y con menor tasa de error (BER Bit Error Rate). La búsqueda continua incluso después que se realiza el proceso de asociación entre la estación y el cliente. Con la búsqueda pasiva la estación ahorra tiempo de reconexión a la red en el caso de des-asociación, ya que la estación mantiene una lista de los APs con sus características (canal, SSID, fuerza de la señal, dirección MAC, etc.). Ver figura 15.

1.9.2 Búsqueda activa: involucra el envío de una trama de petición de prueba por parte del cliente que está buscando una red a la cual unirse. La trama contiene el SSID de la red a la cual desea unirse o un SSID común. Los AP que pertenecen al SSID contestan con una trama de respuesta de prueba, luego la estación determina con cual AP asociarse, basándose en la mayor magnitud de la señal y menor tasa de error (BER). Ver figura 16.

Figura 15. Búsqueda pasiva.

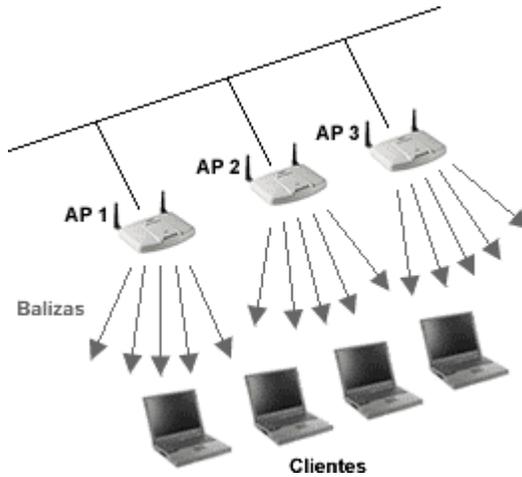
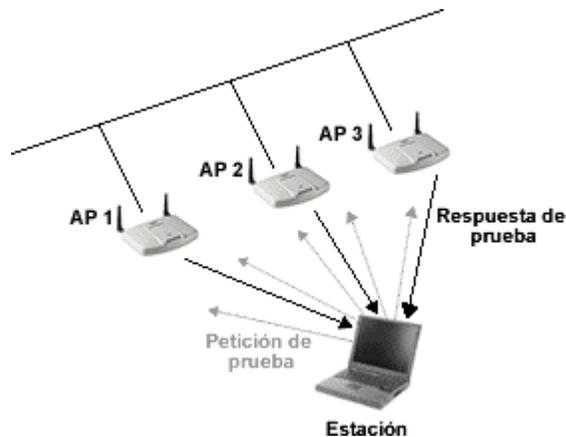


Figura 16. Búsqueda activa.



1.10 MANEJO DE POTENCIA

Las estaciones bajo la norma 802.11 operan en dos modos de potencia, ellos son: modo activo continuo y modo sondeo de ahorro de potencia (PS-Poll).

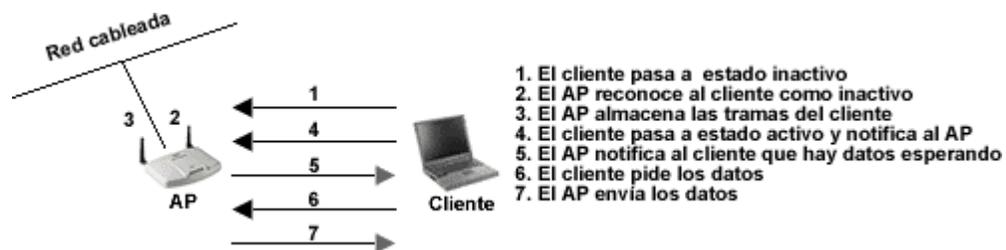
1.10.1 Modo activo continuo: el cliente inalámbrico usa la potencia total y está en constante comunicación con el AP. Cualquier computador conectado a una salida de potencia AC puede permanecer en este modo, ya que no hay razón para que se conserve potencia, por ejemplo, un computador de escritorio o un servidor. El AP funciona en este modo.

1.10.2 Modo sondeo de ahorro de potencia: permite que la estación móvil vaya a modo inactivo para ahorrar potencia sin perder conectividad. La estación envía una trama de sondeo de ahorro

de potencia (PS-Poll) a su AP, para anunciar que va a pasar de un estado activo a uno inactivo, en este último estado el AP debe almacenar las tramas destinadas a la estación. Periódicamente la estación vuelve al estado activo para enterarse si existen tramas para ella almacenadas en el AP, en caso de que no existan envía otra trama PS-Poll y regresa a modo inactivo. El beneficio real es que el usuario móvil es capaz de usar la WLAN por largos periodos de tiempo, sin impactar severamente la vida de la batería.

1.10.2.1 Sondeo de ahorro de potencia en un BSS: el proceso de ahorro de potencia en un BSS ocurre gracias a que las estaciones envían una trama PS-Poll al AP, para informar que van a estar inactivas. El AP registra a la estación como inactiva, de modo que todo el tráfico que es destinado a una estación inactiva, no puede ser enviado a la estación y por lo tanto es almacenado en una memoria del AP. El AP manda constantemente balizas a intervalos regulares de tiempo, el cliente debe estar sincronizado con el AP para saber en que momento escuchar las balizas, la estación escucha la baliza y mira si está listada en el mapa de indicación de tráfico (TIM). Si este es el caso, envía tramas al AP notificándole que está activo y listo para recibir las tramas que tiene almacenadas. Cuando el cliente recibe todas las tramas vuelve al estado inactivo. Lo anterior se aprecia en la siguiente figura 17.

Figura 17. Sondeo de ahorro de potencia en un BSS.



1.10.2.2 Sondeo de ahorro de potencia en un IBSS: este proceso de ahorro de potencia es diferente y no tan eficiente como el usado en un BSS; debido a la inexistencia del AP, por lo tanto cada estación transmisora almacena las tramas destinadas a una estación inactiva y los receptores deben permanecer más tiempo activos. Las estaciones alternan el envío de balizas en una red IBSS, usando métodos que dependen del fabricante.

El manejo de potencia en un IBSS se basa en mensajes de indicación de tráfico, los cuales son conocidos como mensajes de indicación de anuncio de tráfico (ATIM), la trama ATIM es enviada después de la baliza en periodos específicos de tiempo conocido como ventana ATIM, cuando una estación tiene datos almacenados para otra estación, notificando que debe permanecer activa; las

estaciones que no reciben tramas ATIM pueden pasar a estado inactivo. Cuando la ventana ATIM termina, las estaciones comienzan a transmitir los datos. Después de recibir las tramas de datos las estaciones vuelven al estado inactivo esperando la siguiente baliza y el proceso se repite.

1.11 SEGURIDAD

La norma 802.11 proporciona tres formas de seguridad para los datos, usándolos se reduce la probabilidad de exposición a intrusos.

El primer método usa el SSID, para que una estación pueda asociarse con un AP ambos deben tener el mismo SSID; este esquema de seguridad es rudimentario, ya que el SSID es conocido por los usuarios y puede ser compartido fácilmente. Otra desventaja de usar SSID como única forma de autenticación es que si el SSID de la red es cambiado, todas las estaciones deben también cambiarlo. Si se deshabilita la difusión del SSID se crearía una red oculta, con lo que el cliente debería entrar manualmente el SSID. Se podría entonces pensar que si no se conoce el SSID, el cliente no se puede conectar a la red. Esto es falso, ya que existen programas que sirven para explorar redes inalámbricas y fácilmente monitorear el tráfico que pasa por la red supuestamente oculta.

El segundo método se basa en una lista de direcciones MAC de los clientes a los cuales se les permite el acceso a la red. Esta autenticación puede hacerse por medio del AP o por algún otro dispositivo ubicado en la red cableada. Si la dirección MAC no está en la lista, el cliente no se puede asociar, pero como con el método anterior existen programas que pueden monitorear el tráfico que pasa por una red inalámbrica y luego con la técnica conocida como *spoofing* pueden suplantar ilegalmente una dirección MAC.

El tercer método que 802.11 ofrece es mediante el uso de privacidad equivalente cableada (WEP). WEP opera a nivel de la capa MAC. Es un algoritmo de encriptación que usa procesos de autenticación de clave compartida para autenticación de usuarios y para encriptación de datos sobre un segmento WLAN. WEP usa un vector de inicialización (IV Initialization Vector), un generador de número seudo aleatorio (PRNG Pseudo-Random Number Generator) y RC4 (Ron's Cipher 4) que es un código de cifrado. Las claves WEP son asignadas de forma estática o manual para todos los clientes y APs, sin embargo WEP no es muy seguro, ya que, todas las estaciones de la WLAN comparten la misma clave WEP, de modo que cuando se descubre, es necesario cambiar la clave WEP de todos los equipos en forma manual.

Una clave WEP puede ser usada de dos maneras en una WLAN, para autenticación o encriptación de datos. Cuando un cliente con WEP intenta autenticarse y asociarse con un AP, el AP determina si el cliente manda la clave WEP correcta, si la clave es la misma ellos, pueden asociarse. Las claves WEP pueden ser distribuidas manualmente o mediante sistemas de distribución de claves WEP, que van desde claves estáticas hasta el uso de servidores de claves centralizadas.

En redes pequeñas tales como una red casera o una pequeña empresa se pueden usar claves WEP estáticas, siempre y cuando se tenga en cuenta que la clave WEP debe ser cambiada frecuentemente, contener una combinación de caracteres alfanuméricos y no alfanuméricos y tan grande como sea posible dependiendo del tipo de WEP que use el equipo (WEP 64 o WEP 128 o WEP 256) para evitar ataques diccionario o de fuerza bruta.

En redes grandes tales como redes empresariales, redes universitarias se pueden usar sistemas de distribución de claves que se hace por medio de servidores centralizados los cuales generan y distribuyen automáticamente claves, dependiendo del fabricante, esta implementación puede ser por generación de claves por paquete, por sesión u otro método.

Como una mejora a WEP se creó el protocolo de integridad de claves temporales (TKIP Temporal Key Integrity Protocol), para arreglar los problemas de WEP con la implementación del algoritmo RC4, ayudando a determinar la integridad de los mensajes chequeando si usuarios no autorizados han modificado el tráfico de la red.

También fue creado el estándar avanzado de encriptación (AES Advanced Encryption Standar), que reemplaza el algoritmo RC4 con el algoritmo Rijndale. AES está incluido en el estándar 802.11i.

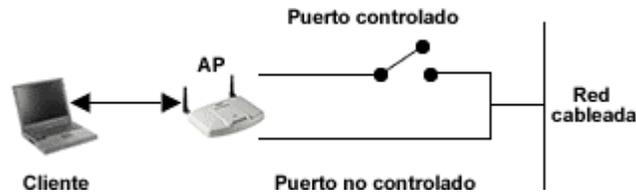
Para mejorar las fallas de WEP para autenticación, la industria está trabajando en muchas soluciones basadas en la especificación 802.1x que proporciona especificaciones de control de acceso a la red basado en puerto, estos puertos hacen referencia a puertos físicos, 802.1x fue inicialmente diseñado para redes cableadas con lo cual se ejerce un control sobre las conexiones RJ-45. En una red inalámbrica el cliente es una conexión virtual RJ-45. 802.1x se encarga de bloquear el tráfico de un puerto, hasta que el cliente sea autenticado por un servidor de autenticación.

802.1x a su vez se basa en el protocolo de autenticación extensible (EAP Extensible Authentication Protocol) definido en el RFC 2284, que es un protocolo flexible usado por muchas redes para la

autenticación usando contraseñas, certificados, claves públicas, tarjetas inteligentes, biometría, etc. La seguridad de una red depende del tipo de este protocolo que sea escogido.

Los elementos básicos de 802.1x son el AP, el cliente 802.1x y el servidor de autenticación. Si un cliente no está autenticado, el AP no le permite pasar tráfico a la red, excepto mensajes 802.1x, después de que el cliente es autenticado se le permite enviar datos. Para este proceso se usan dos puertos virtuales uno controlado y otro no controlado. Figura 18. El puerto no controlado se usa para la comunicación entre el AP y el servidor de autenticación. El puerto controlado permite pasar el tráfico solo cuando el cliente esté autenticado.

Figura 18. Puerto controlado y no controlado.



La forma de autenticación funciona de la siguiente manera:

1. El cliente envía una trama de iniciación EAP.
2. El AP sabe que alguien quiere entrar a la red y contesta con una petición de identidad EAP.
3. El cliente contesta con una respuesta de identidad EAP al AP.
4. El AP transmite esta respuesta al servidor de autenticación.
5. El servidor envía al AP una petición de autorización EAP.
6. El AP se la transmite al cliente.
7. El cliente envía la respuesta al AP.
8. El AP se la envía al servidor de autenticación.
9. El servidor de autenticación evalúa las credenciales y contesta con un mensaje de éxito (o fallo) EAP al AP.
10. El AP transmite el mensaje exitoso al cliente y cambia el estado del puerto controlado a modo de transmisión.

802.1x es efectivo en cuanto a seguridad de redes inalámbricas, ya que soporta generación de clave dinámica, por sesión o por usuario.

La preocupación por el aspecto de la seguridad en las redes inalámbricas llevó a la alianza Wi-Fi (Fidelidad Inalámbrica) ha adoptar una tecnología de seguridad mejorada conocida como acceso Wi-Fi protegido (WPA Wi-Fi Protected Access) como una medida provisional. WPA añade un mayor nivel de seguridad a 802.11.

Las características de WPA son:

- WPA requiere autenticación 802.1x.
- En entornos sin RADIUS, WPA admite el uso de una clave compartida previamente. En entornos con RADIUS, se admite el protocolo de autenticación extensible (EAP).
- WPA requiere el manejo de claves con el protocolo TKIP.
- WPA define el uso del estándar de cifrado avanzado (AES) como sustituto adicional para el cifrado de WEP.

WPA requiere cambios de software en:

- Puntos de acceso inalámbrico
- Adaptadores de red inalámbrica
- Programas cliente inalámbricos

En el estándar 802.11i se menciona las soluciones de seguridad y sistemas criptográficos para las redes inalámbricas, el estándar 802.11i tiene las habilidades de WPA y adiciona el uso de AES para encriptación de datos. El inconveniente de AES es que puede necesitar nuevo hardware para muchas redes inalámbricas existentes.

La alianza Wi-Fi usará WPA2 para referirse a 802.11i, los productos 802.11i/WPA2 tendrán compatibilidad hacia atrás con los productos WPA, siempre y cuando soporten AES.

Cuando se trata de redes que exigen mucha seguridad es necesario implementar soluciones hardware y/o software que involucran seguridad de red cableadas. Entre ellas están:

Firewalls: mediante su uso es posible separar usuarios inalámbricos de los usuarios internos de una red. Un *firewall* puede bloquear peticiones no autorizadas creando una barrera a *crackers* que quieren acceder a la red interna.

VPN: enlaza computadores o redes remotas a un servidor corporativo por medio de un túnel sobre un protocolo como IP. El tráfico dentro del túnel es encriptado y totalmente aislado por lo tanto se protegen los datos en una red inalámbrica insegura.

RADIUS: el servicio de usuario de acceso telefónico de autenticación remota (Remote Authentication Dial-in User Service) es un protocolo que sirve para autenticar conexiones remotas, de modo que proporciona autorización para los recursos de red, es usada en una WLAN para controlar la conexión de los usuarios.

1.12 UNIDADES DE DATOS MAC

La clave de las normas 802.11 es la subcapa MAC, la cual controla la transmisión de datos de usuario. La subcapa MAC proporciona el núcleo de la operación de transmisión de las tramas y la interacción con el *backbone* de la red cableada. Las tramas que tiene que manejar son conocidas como unidades de datos y son las siguientes:

MSDU: unidad de datos de servicio MAC (MAC Service Data Unit), es la unidad de información entre la capa MAC y los puntos de acceso al servicio (SAP's) ubicados en la capa LLC.

MMPDU: unidad de datos del protocolo de gestión MAC (MAC Management Protocol Data Unit), es la unidad de datos intercambiada entre dos pares de entidades MAC que implementan protocolo de gestión MAC.

MPDU: unidad de datos del protocolo MAC (MAC Protocol Data Unit), es la unidad de datos intercambiada entre dos pares de entidades MAC usando los servicios de la capa física.

La forma como se relacionan las unidades de datos con las diferentes capas se muestra en la figura 19.

El formato general de trama MAC se muestra en la figura 20, cada trama MAC consiste de los siguientes componentes básicos:

- Encabezado MAC: comprende el control de trama, duración, dirección e información de control de secuencia.
- Cuerpo de trama de longitud variable: tiene información específica del tipo de trama.

1.12.1.2 Subcampo tipo y subtipo: control, datos y gestión son los tipos de trama que identifican las diferentes funciones de los componentes básicos de la red. Cada tipo de trama tiene varios subtipos. La tabla 1 muestra como son usados los identificadores del tipo y subtipo para la creación de diferentes clases de tramas.

Tabla 1. Identificadores de tipo y subtipo.

Valor del tipo B3 B2	Descripción del tipo	Valor del subtipo B7 B6 B5 B4	Descripción del subtipo
00	Gestión	0000	Petición de asociación
00	Gestión	0001	Respuesta de asociación
00	Gestión	0010	Petición de re-asociación
00	Gestión	0011	Respuesta de re-asociación
00	Gestión	0100	Petición de prueba
00	Gestión	0101	Respuesta de prueba
00	Gestión	0110 – 0111	Reservado
00	Gestión	1000	Baliza
00	Gestión	1001	Mensaje de indicación de anuncio de tráfico (ATIM)
00	Gestión	1010	Des-asociación
00	Gestión	1011	Autenticación
00	Gestión	1100	Des-autenticación
00	Gestión	1101 – 1111	Reservado
01	Control	0000 – 1001	Reservado
01	Control	1010	Sondeo de ahorro de potencia (PS-Poll)
01	Control	1011	Petición de envío (RTS)
01	Control	1100	Listo para enviar (CTS)
01	Control	1101	Acuse de recibo (ACK)
01	Control	1110	Fin de libre contención (CF-end)
01	Control	1111	CF-end + CF-ACK
10	Datos	0000	Datos
10	Datos	0001	Datos + CF-ACK
10	Datos	0010	Datos + CF-Poll
10	Datos	0011	Datos + CF-ACK + CF-Poll
10	Datos	0100	Función nula (no hay dato)
10	Datos	0101	CF-ACK (no hay dato)
10	Datos	0110	CF-Poll (no hay dato)
10	Datos	0111	CF-ACK + CF-Poll
10	Datos	1000 - 1111	Reservado
11	Reservado	0000 - 1111	Reservado

1.12.1.3 Subcampo Para DS: este campo es fijado en 1 cuando la trama es dirigida desde la estación hacia el AP para enviarla al DS, incluyendo el caso donde la estación destino está en el mismo BSS y el AP transmite la trama. El campo DS se fija en 0 cuando tramas son de control y gestión. Ver tabla 2.

1.12.1.4 Subcampo Desde DS: el campo Desde DS es fijado en 1 en las tramas de tipo de datos, cuando las tramas salen del DS hacia una estación. Se fija en 0 para las tramas de control y gestión. Ver tabla 2.

Tabla 2. Interpretación de los bits Para DS y Desde DS.

Para/Desde DS	Significado
Para DS = 0 Desde DS = 0	Tramas de datos entre las estaciones de un mismo IBSS.
Para DS = 1 Desde DS = 0	Tramas de datos dirigida desde una estación a un AP.
Para DS = 0 Desde DS = 1	Tramas de datos saliendo de un AP a una estación.
Para DS = 1 Desde DS = 1	Tramas de datos que son enviadas de un AP a otro.

1.12.1.5 Subcampo más fragmentos: este campo se fija en 1 en todas las tramas tipo gestión o datos, indica que la actual MSDU o la actual MMPDU aun no ha finalizado la comunicación y vienen más tramas. Este campo es 0 en tramas de control.

1.12.1.6 Subcampo reintento: usado cuando las tramas de datos o gestión deben ser retransmitidas. Este bit se fija en 1 para que la estación receptora elimine las tramas duplicadas. Este campo es 0 en tramas de control.

1.12.1.7 Subcampo manejo de potencia: usado para indicar el modo de manejo de potencia de una estación. El valor del campo se mantiene constante en cada trama de una estación particular dentro de una secuencia de intercambio de tramas. El valor indica el modo en el cual la estación estará después de que se complete exitosamente la secuencia de intercambio de trama. 1 indica que la estación está en modo ahorro de potencia, un valor de 0 significa que la estación estará en modo activo. Este campo es siempre fijado en 0 en tramas transmitidas por un AP.

1.12.1.8 Subcampo más datos: es usada para indicar a una estación en modo ahorro de potencia que hay más MSDUs o MMPDUs que van hacia la estación y están siendo almacenadas por el AP, la estación decide si usa esta información para continuar haciendo sondeo o para cambiar a modo activo. Este campo es válido en datos dirigidos o en tramas tipo gestión que son transmitidas por un AP a una estación en modo ahorro de potencia. Es 0 en tramas de control. El valor de 1 indica que al menos existe una MSDU o una MMPDU que va hacia una estación. Este campo es 1 para tramas tipo *multicast* o tipo *broadcast* transmitidas por el AP, es 0 cuando no existen más tramas *multicast* o *broadcast* MSDU o MMPDU para ser transmitidas por el AP durante un intervalo de señal y en todas las tramas *multicast* o *broadcast* transmitidas desde una estación.

1.12.1.9 Subcampo WEP: este campo indica que el cuerpo de trama es encriptado de acuerdo al algoritmo WEP. El campo WEP se fija en 1 en las tramas tipo dato, tipo gestión, subtipo autenticación y se fija en 0 en todas las otras tramas.

1.12.1.10 Subcampo orden: este campo se fija en 1 en cualquier trama de tipo datos que contiene una MSDU, o un fragmento de la misma. Este bit indica que la trama está siendo enviada usando la clase de servicio en estricto orden, este es definido por los usuarios que no aceptan un cambio de orden en tramas *unicast* y *multicast*, el orden de las tramas hacia una dirección específica debe ser siempre mantenido. Es 0 en tramas de control.

1.12.2 Campo duración ID: este campo tiene una longitud de 16 bits, tiene diferentes usos, puede ser un identificador o puede incluir un valor de duración. Puede tomar una de las tres siguientes formas: duración NAV, tramas transmitidas durante el periodo de libre contención y tramas PS – Poll. Los valores de este campo son mostrados en la tabla 3.

Tabla 3. Valores del campo de duración ID.

Bit 15	Bit 14	Bit 13 – 0	Uso
0	0 – 32767		Duración
1	0	0	Valor fijo dentro de las tramas transmitidas durante el CFP
1	0	1 – 16383	Reservado
1	1	0	Reservado
1	1	1 – 2007	AID en tramas de sondeo de ahorro de potencia
1	1	2008 -16383	Reservado

1.12.2.1 Duración vector de ubicación de la red: cuando el bit 15 en duración ID es 0, el campo es usado para el vector de ubicación de la red (NAV Network Allocation Vector). Este valor

representa el número de microsegundos durante el cual el medio va a permanecer ocupado en el transcurso de la transmisión actual. Las estaciones deben supervisar el encabezado de todas las tramas que recibe y actualizar el valor del NAV constantemente.

1.12.2.2 Tramas transmitidas durante el periodo de libre contención: durante este periodo el bit 14 de la trama de Duración ID es 0 y el bit 15 es 1, los otros bits son 0 de manera que el campo toma un valor de 32768. Cuando el contenido del campo de Duración ID es menor a 32768, el valor de la duración se usa para actualizar el NAV.

1.12.2.3 Tramas PS - Poll: las estaciones incluyen el identificador de asociación (AID Association Identifier) para indicar a que AP ellas pertenecen, cuando están en modo ahorro de potencia. Los bits 14 y 15 del campo Duración ID son fijados en 0.

1.12.3 Campo de direcciones: existen 4 campos de direcciones dentro del formato de tramas MAC, cada campo de dirección contiene una dirección de 48 bits. Estos campos son usados para indicar el identificador del conjunto de servicio básico (BSSID Basic Service Set Identification), dirección fuente (SA Source Address), dirección destino (DA Destination Address), dirección de la estación transmisora (TA Transmitter Address) o dirección de la estación receptora (RA Receiver Address), dependiendo del bit Para DS o Desde DS definidos en el campo de control. La función de cierto campo de direcciones es especificado por la posición relativa del campo de dirección (1-4), como se puede ver en la tabla 4.

Campo de dirección fuente (SA): el campo SA contiene una dirección MAC que identifica la entidad MAC desde la cual fue iniciada la transferencia de MSDU (o algún fragmento de ellas) contenidos en el campo de cuerpo de trama.

Campo de dirección receptora (RA): el campo de dirección RA contiene una dirección MAC que identifica las estaciones receptoras inmediatas en el medio inalámbrico, con la información contenida en el campo de cuerpo de trama.

Campo de dirección transmisora (TA): contiene una dirección MAC que identifica la estación que ha transmitido sobre el medio inalámbrico la MPDU contenida en el campo de cuerpo de trama.

Campo de dirección de destino (DA): corresponde a la estación receptora final.

Identificador del conjunto de servicio básico (BSSID): usado para identificar diferentes WLAN en la misma área; en redes tipo infraestructura, el BSSID es la dirección MAC usada por la interfaz en el AP. En redes Ad hoc se genera un BSSID aleatorio con un bit que se fija en 1 para evitar conflicto con la dirección MAC asignada.

1.12.3.1 Subcampo dirección 1: es siempre la dirección de la estación receptora inmediata del paquete, si Para DS está en 0 será entonces la dirección de la estación destino ya que es la receptora inmediata del paquete dentro de un BSS.

1.12.3.2 Subcampo dirección 2: corresponde a la dirección del transmisor, si Desde DS está en 1 significa que esta es la dirección del AP. Cuando está en 0 corresponde a la dirección de la estación que está transmitiendo físicamente el paquete.

1.12.3.3 Subcampo dirección 3: en la mayoría de los casos es la dirección restante, así con una trama con Para DS y Desde DS fijados en 1, este campo de dirección será la dirección destino. Cuando Para DS es 0 la dirección que ocupa este campo es la dirección fuente.

1.12.3.4 Subcampo dirección 4: es un caso especial donde el sistema de distribución es inalámbrico y la trama se transmite de un AP a otro, en este caso los bits Desde DS y Para DS deben permanecer en 1.

Tabla 4. Uso del campo de direcciones.

Para DS	Desde DS	Dirección 1	Dirección 2	Dirección 3	Dirección 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

A continuación se explica como se relaciona la tabla 4 con implementaciones de redes inalámbricas, la figura 22 se muestra un ESS, la figura 23 muestra un IBSS.

Figura 22. Uso del campo de direcciones en una ESS.

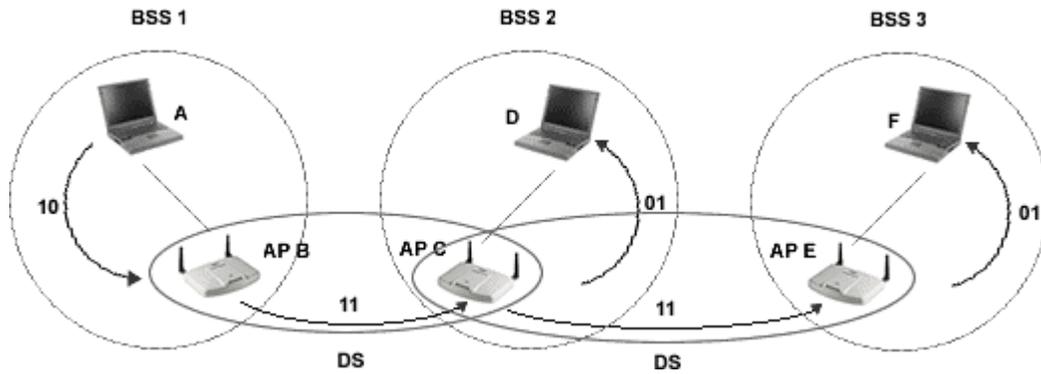
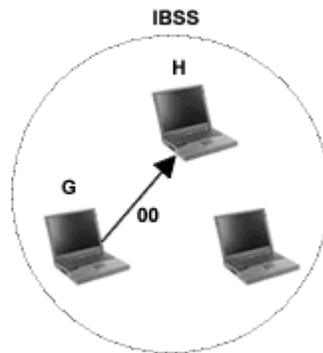


Figura 23. Uso del campo de direcciones en una IBSS.



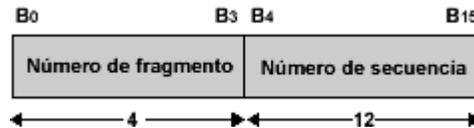
En la figura 22 se realiza una comunicación entre la estación A y D y entre A y F, y en la figura 23 entre G y H, siguiendo el sentido de las flechas. El número junto a la flecha indica el valor del campo Para DS y Desde DS. En la tabla 5 se muestran las direcciones para cada caso.

Tabla 5. Campos de direcciones en la comunicación entre estaciones.

Comunicación		Para DS	Desde DS	Dirección 1	Dirección 2	Dirección 3	Dirección 4
Entre A y D	Entre A y B	1	0	BSSID=B	SA=A	DA=D	N/A
	Entre B y C	1	1	RA=C	TA=B	DA=D	SA=A
	Entre C y D	0	1	DA=D	BSSID=C	SA=A	N/A
Entre A y F	Entre A y B	1	0	BSSID=B	SA=A	DA=F	N/A
	Entre B y C	1	1	RA=C	TA=B	DA=F	SA=A
	Entre C y E	1	1	RA=E	TA=C	DA=F	SA=A
	Entre E y F	0	1	DA=E	BSSID=C	SA=A	N/A
Entre G y H	Entre G y H	0	0	DA=H	SA=G	BSSID	N/A

1.12.4 Campo de secuencia de control: es usado en de-fragmentación y descarte de tramas duplicadas. Tiene 16 bits de longitud y consiste en dos subcampos, el número de secuencia y el número de fragmento. El formato de campo de control de secuencia es el de la figura 24.

Figura 24. Secuencia de control.



Campo número de secuencia: este campo tiene una longitud de 12 bits, indicando el número de secuencia de una MSDU o una MMPDU. Cada trama que es transmitida por una estación se le asigna un número de secuencia. Los números de secuencia son asignados desde un contador modulo 4096, comenzando en 0 e incrementando en 1 por cada MSDU o MMPDU.

Si una MPDU o MMPDU es fragmentada, todos los fragmentos tienen el mismo número de secuencia. Cuando hay retransmisiones, el número secuencia no se cambia.

Campo número de fragmento: es un campo de 4 bits que indica el número de cada fragmento de una MMPU o una MMPDU, este campo es 0 para el primer fragmento y se incrementa en uno por cada fragmento sucesivo. El número de fragmento permanece constante en todas las retransmisiones del fragmento.

1.12.5 Campo de cuerpo de trama: el cuerpo de trama es un campo de longitud variable que contiene información específica para el tipo de trama individual y subtipos. Usado en tramas de datos y de gestión. 802.11 puede transmitir tramas de hasta 2304 bytes sin WEP o 2312 cuando el cuerpo de trama es encriptado usando WEP. 2304 es el resultado de los 2048 bytes de datos más 256 bytes de encabezado de protocolo de nivel superior y *trailers* (información de control de protocolo ubicado al final de una PDU).

1.12.6 Campo FCS: la secuencia de verificación de trama FCS es a menudo conocida como verificación por redundancia cíclica (CRC). Este campo tiene 32 bits de longitud, el FCS es calculado sobre todos los campos del encabezado MAC y sobre el campo de cuerpo de trama. Cuando las tramas son enviadas a la interfaz inalámbrica, el FCS se calcula antes de enviarlas al enlace RF.

2. NORMAS IEEE 802.11 - CAPA FÍSICA

El segundo componente principal de 802.11 es la capa física. 802.11 divide la capa física en dos componentes: procedimiento de convergencia de la capa física (PLCP Physical Layer Convergence Protocol), para tomar las tramas MAC del medio, y el sistema dependiente del medio físico (PMD Physical Medium Dependent) para transmitir estas tramas. El PLCP está en las fronteras de la capa física y la capa MAC. En 802.11, el PLCP adiciona un número de campos a la trama para ser enviada a la subcapa PMD y luego ser transmitida mediante la antena. El nivel físico también incorpora una función de evaluación de canal libre (CCA Clear Channel Assessment), para indicar a la capa MAC cuando el medio está disponible.

El estándar 802.11 en su versión inicial en 1997 definió tres capas físicas: espectro ensanchado por salto de frecuencia (FHSS Frequency Hopping Spread Spectrum), espectro ensanchado por secuencia directa (DSSS Direct Sequence Spread Spectrum) e Infrarrojo (IR InfraRed), luego en 1999, se adicionó multiplexación por división de frecuencia ortogonal (OFDM Orthogonal Frequency Division Multiplexing) en 802.11a y DSSS de alta velocidad (HR/DSSS High Rate Direct Sequence Spread Spectrum) en 802.11b y en el 2003 OFDM en 802.11g.

2.1 802.11

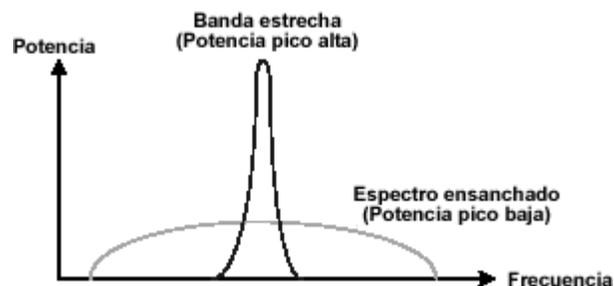
2.1.1 Infrarrojo: 802.11 incluye el uso de infrarrojos, este presenta algunas ventajas sobre las ondas de radio. El puerto infrarrojo es menos costoso que un transmisor o receptor de radio, es tolerante con las ondas de radio debido a que operan a frecuencias diferentes. Las LAN 802.11 basadas en IR pueden ser instaladas en configuración punto a punto requiriendo línea de vista directa y funcionan hasta una distancia de 10 metros permitiendo una movilidad limitada a espacios pequeños como oficinas, salones de conferencia etc., ofreciendo seguridad, ya que la señal está limitada por el bloqueo de obstáculos. El otro tipo es la configuración difusa donde las señales son reflejadas por algún tipo de superficie permitiendo mayores rangos pero menor velocidad y seguridad. Esta configuración permite a los dispositivos tener receptores más sensibles de modo que se puede incrementar el rango hasta los 20 metros.

Esta técnica usa luz infrarroja en el rango de 850 a 950 nanómetros. Este mecanismo opera con un nivel de potencia pico de transmisión de 2 vatios. Esta tecnología no es tan popular ya que no

es adecuada para usuarios móviles. No se entrará en detalle de esta técnica debido a que los productos existentes en el mercado basados en IR, no son fabricados con el estándar 802.11 sino con el estándar de la asociación de comunicación inalámbrica a través de luz infrarroja (IrDA InfraRed Data Association).

2.1.2 Tecnología de espectro ensanchado: el espectro ensanchado es una técnica que se caracteriza por el amplio ancho de banda y la baja potencia pico y posee muchas ventajas sobre una comunicación de banda estrecha que utiliza solo el espectro necesario para enviar la información; la técnica de espectro ensanchado usa un ancho de banda mayor que el requerido para su comunicación. El bloqueo y la interferencia tienen menor efecto sobre una comunicación con esta tecnología.

Figura 25. Espectro ensanchado.



En una comunicación de banda estrecha se puede usar 1 MHz con 10 vatios, mientras que con espectro ensanchado para la misma comunicación es necesario 20 MHz con 100 milivatios. Mediante el empleo de la técnica de espectro ensanchado, se reduce la probabilidad de que los datos sean afectados o bloqueados. Cuando una señal del espectro ensanchado se ve afectada por una señal de banda estrecha, solamente una pequeña porción de la señal se pierde teniéndose que la mayoría de los datos son recibidos sin error.

Existen muchas implementaciones de tecnologías de espectro ensanchado, pero solo dos tipos son especificados por la Comisión Federal de Comunicaciones (FCC Federal Communications Commission) de Estados Unidos, estas son: espectro ensanchado por salto de frecuencia (FHSS) y espectro ensanchado por secuencia directa (DSSS). Las redes 802.11 usan estas dos técnicas en la banda de 2.4 GHz conocida como banda industrial, científica y médica (ISM Industrial Scientific and Medical), la cual va de 2.400 a 2.4835 GHz y está disponible mundialmente para su uso sin licencia.

2.1.2.1 Espectro ensanchado por salto de frecuencia (FHSS): “Técnica de estructuración de la señal que conmuta automáticamente la frecuencia portadora transmitida; proceso que se realiza en forma pseudoaleatoria a partir de un conjunto de frecuencias que ocupa un ancho de banda mucho mayor que el ancho de banda de información. El receptor correspondiente realiza el salto de frecuencia en sincronismo con el código del transmisor para recuperar la información deseada”¹. Esta habilidad para realizar los saltos de frecuencia se conoce como agilidad de frecuencia.

En la técnica de FHSS, la portadora cambia o salta de frecuencia de acuerdo a una secuencia pseudoaleatoria que se repite, esta secuencia es una lista de diferentes frecuencias, valores a los que la portadora salta a determinados intervalos de tiempo. El transmisor usa la secuencia de salto para seleccionar sus frecuencias de transmisión. La portadora permanece en cierta frecuencia un determinado período conocido como tiempo de permanencia; luego salta a otra frecuencia, el tiempo de duración del salto se conoce como tiempo de salto. 802.11 no hace referencia a ninguno de estos tiempos, esta tarea la desempeñan los entes reguladores.

802.11 divide la banda ISM en una serie de canales de 1 MHz de ancho, comenzando con el canal para la portadora de 2.402 GHz, el siguiente para la portadora de 2.403 GHz, sigue la portadora de 2.404 GHz y así sucesivamente hasta la portadora de 2.480 GHz con lo que se obtiene un conjunto de 79 portadoras. Estas 79 portadoras se dividen en tres conjuntos de 26 portadoras cada una, estos conjuntos están diseñados de tal manera que evitan prolongados períodos de colisión entre las diferentes secuencias de salto.

Una estación se une a una red FHSS gracias a que en las balizas se incluye la información necesaria: el parámetro FH y una marca de tiempo. La marca de tiempo permite la sincronización y el parámetro FH incluye el número del patrón de saltos y el índice del salto. De esta manera el receptor recibe la frecuencia correcta en el tiempo correcto.

No se profundiza más sobre esta técnica, ya que no ha sido implementada ampliamente por los fabricantes de equipos debido a que con otras técnicas se logran mayores velocidades. Para una ampliación del tema ver la cláusula 14*.

¹ COLOMBIA. MINISTERIO DE COMUNICACIONES. Resolución número 000689 de 2004. Bogotá, 2004; p.3.

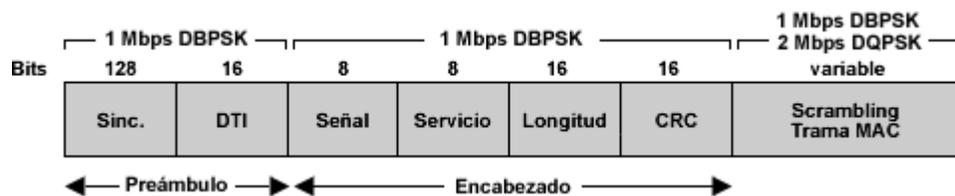
*Cláusula 14 de la norma IEEE 802.11-1999. Frequency-Hopping spread spectrum (FHSS) PHY specification for the 2.4 GHz Industrial, Scientific, and Medical (ISM) band.

2.1.2.2 Espectro ensanchado por secuencia directa (DSSS): “Técnica de estructuración de la señal que utiliza una secuencia pseudoaleatoria digital o código, con una velocidad de transmisión, muy superior a la velocidad de información. Cada bit de información de la señal digital se transmite como una secuencia pseudoaleatoria de datos codificados, que produce un espectro semejante al ruido”².

La capa física de 802.11 recibe las tramas de la capa MAC por medio del procedimiento de convergencia de la capa física (PLCP), el PLCP adiciona un número de campos a la trama para luego ser enviada a la subcapa PMD que se encarga de modularla y transmitirla por el medio.

El PLCP en DSSS adiciona seis campos a las tramas que llegan de la capa MAC. Las tramas que llegan de la capa MAC son las denominadas unidades de datos de servicio PLCP (PSDUs). La trama DSSS PLCP se muestra en la figura 26, haciendo notar que se realiza un proceso de *scrambling* para proteger los datos.

Figura 26. Formato de trama PLCP.



Preámbulo: se encarga de la sincronización entre el transmisor y el receptor antes de efectuar la transmisión. Está compuesto por el campo de sincronización y el campo delimitador de inicio de trama.

- Sincronización (sinc): es un campo de 128 bits compuesto por unos.
- Delimitador de inicio de trama (DTI): este campo permite al receptor encontrar el inicio de la trama, inclusive cuando algunos bits de sincronización hayan desaparecido. Este campo se fija en 0000 0101 1100 1111

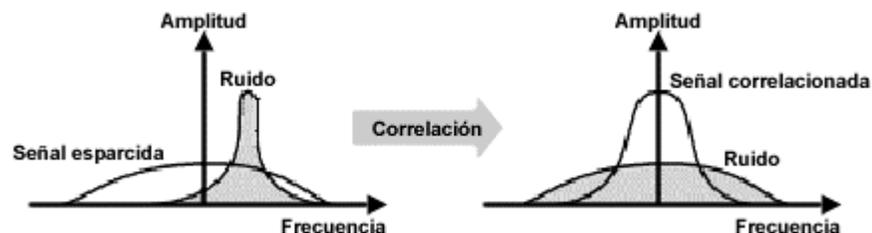
Encabezado: tiene los parámetros específicos de la capa física usados por PLCP, está compuesto por el campo de señal, el campo de identificación de servicio, el campo de longitud, y la secuencia de chequeo de errores.

² COLOMBIA. MINISTERIO DE COMUNICACIONES. Resolución número 000689 de 2004. Bogotá, 2004; p.3.

- Señal: este campo se usa por el receptor para identificar la velocidad de transmisión de la trama MAC. Se fija en 0000 1010 cuando la velocidad es de 1 Mbps y en 0001 0100 para 2 Mbps.
- Servicio: este campo se dejó para uso futuro, se fijan todos sus bits en cero.
- Longitud: este campo de 16 bits se fija dependiendo del número de microsegundos requeridos en la transmisión de la trama.
- Código de redundancia cíclica (CRC): se usa para proteger de los daños, el encabezado de la transmisión en el radio enlace, el transmisor calcula un CRC de 16 bits sobre cada uno de los campos del encabezado y el receptor se encarga de la verificación de CRC antes de procesar las tramas.

La subcapa PMD se encarga del proceso de modulación DSSS, donde a partir de una señal de banda estrecha enviada por el transmisor, la potencia de la señal se ensancha gracias al uso de un código de ensanchamiento con el fin de ampliar el espectro, la ventaja es que ayuda a la recuperación de los datos originales en recepción sin necesidad de retransmisiones, aunque se pierda información en el trayecto. En recepción se aplica un proceso de correlación, inverso al proceso de ensanchamiento realizado en el lado de transmisión para detectar la señal que llega incluyendo el ruido y señales de multitrayectoria. Debido a que el ruido toma forma de pulsos estrechos no produce efectos de importancia en la señal, por lo tanto la señal se puede recuperar libre de ruido y se ensancha luego de la correlación. Ver figura 27.

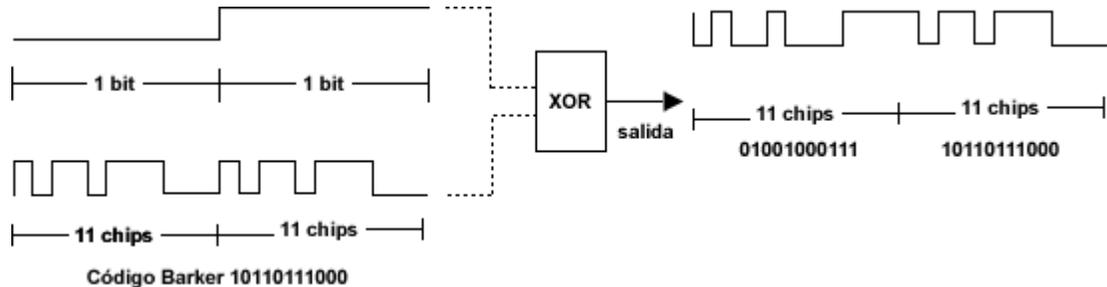
Figura 27. Espectro ensanchado.



El ensanchamiento de la señal en DSSS se forma tomando los bits de información y modulándolos con un patrón llamado secuencia *chipping* que corre a una velocidad más alta que cada bit de información. La secuencia *chipping* usa un código de ensanchamiento de 11 bits (10110111000), esta palabra es llamada código *Barker*, que se aplica a cada bit de información. La cadena de datos hace una XOR con el código *Barker* para generar una serie de datos llamados *chips*, cada bit es codificado por el código *Barker* y cada grupo de 11 *chips* codifica un bit de datos, cuando un 1 es codificado, todos los bits de la secuencia *chipping* cambian y cuando se codifica un 0 la

secuencia permanece igual, como se muestra en la figura 28. Así el receptor analiza el número de 1s y 0s recibidos para deducir el valor del bit enviado.

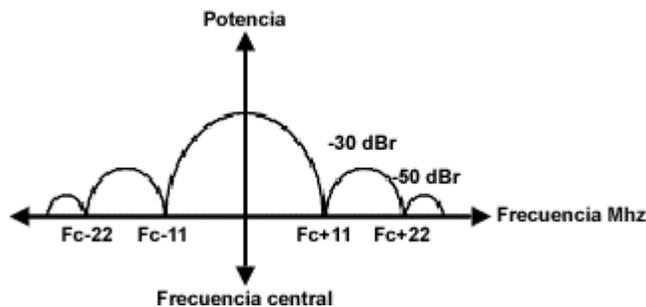
Figura 28. Codificación con el código *Barker*.



La señal generada por la secuencia *Barker* es modulada en fase para ser transmitida por el medio inalámbrico. IEEE 802.11 especifica el uso de modulación por cambio de fase binario diferencial (DBPSK Differential Binary Phase Shift Keying) con lo que se consigue una velocidad de datos de 1 Mbps y el uso de modulación de fase en cuadratura diferencial (DQPSK Differential Quadrature Phase Shift Keying) para una velocidad de 2 Mbps. DQPSK usa las cuatro rotaciones (0, 90, 180 y 270 grados) para codificar 2 bits de información en el mismo espacio donde DBPSK codifica un solo bit.

Luego que la señal es modulada, se envía por el medio inalámbrico a través de los 13 canales disponibles en la banda de 2.4 GHz separados 5 MHz. El primer canal se ubica en 2.412 GHz, el segundo a 2.417 GHz, de manera que el canal 13 se ubica en 2.472 GHz. Dentro de cada canal la energía se distribuye en 22 MHz. La energía se ensancha desde el centro del canal en múltiplos de 11 Mhz, tal como se muestra en la figura 29. Para evitar la interferencia por canal adyacente, el primer lóbulo es filtrado a 30 dBr (razón de potencia) y los lóbulos adicionales son filtrados a 50 dBr por debajo de la potencia del canal central. Esto corresponde a reducir la potencia en un factor de 1.000 y 100.000 respectivamente.

Figura 29. Ensanchamiento de energía en el canal.



La resolución número 000689 de 2004 del Ministerio de Comunicaciones de Colombia, reguló el uso de las bandas y las potencias permitidas para el uso de la banda de 2.4 GHz, que aplican a 802.11, 802.11b y 802.11g. Ver Tabla 6.

Tabla 6. Canales y potencia para DSSS.

Banda	Potencia permitida	Número de canales	Frecuencia central
Banda ISM (2.4000 a 2.4835 GHz)	1 W o 100 mW dependiendo de la antena.	1	2.412 GHZ
		2	2.417 GHZ
		3	2.422 GHZ
		4	2.427 GHZ
		5	2.432 GHZ
		6	2.437 GHZ
		7	2.442 GHZ
		8	2.447 GHZ
		9	2.452 GHZ
		10	2.457 GHZ
		11	2.462 GHZ
		12	2.467 GHZ
		13	2.472 GHz

Según la resolución, en operaciones punto multipunto, las potencias de 1W de transmisión son para antenas direccionales con ganancias de 6 dBi. Si se utilizan antenas con ganancia mayor a 6dBi, la potencia de transmisión pico deberá ser reducida en la cantidad de dB que sobrepase los 6 dBi. Para antenas omnidireccionales el máximo permitido a la entrada de la antena es 100 mW y cuando se excede esta potencia deben ser usadas antenas direccionales con un lóbulo no mayor a 90°. Ver tabla 7.

Para sistemas punto a punto se pueden usar antenas con ganancia mayor a 6 dBi, siempre y cuando se reduzca la potencia del transmisor en 1 dB por cada 3 dB que sobrepase la ganancia de 6 dBi. Ver tabla 8.

Tabla 7. Operación punto multipunto en la banda de 2.4 GHz.

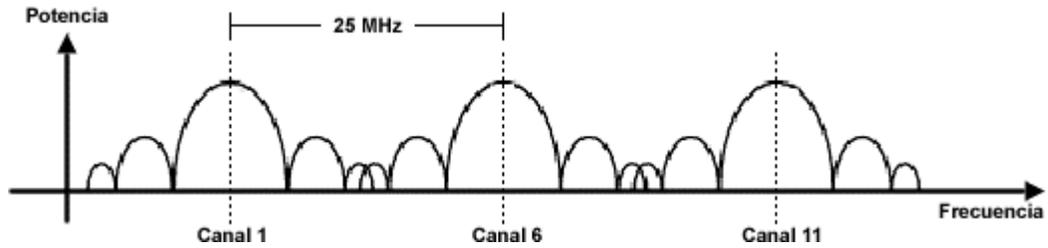
Potencia entregada a la antena (mW)	Potencia entregada a la antena en (dBm)	Máxima ganancia de la antena (dBi)	Potencia isotrópica radiada efectiva PIRE (W)	Potencia isotrópica radiada efectiva PIRE (dBm)
1000	30	6	4	36
500	27	9	4	36
250	24	12	4	36
125	21	15	4	36
63	18	18	4	36
31	15	21	4	36
15	12	24	4	36
8	9	27	4	36
4	6	30	4	36

Tabla 8. Operación punto a punto en la banda de 2.4 GHz.

Potencia entregada a la antena (mW)	Potencia entregada a la antena en (dBm)	Máxima ganancia de la antena (dBi)	Potencia isotrópica radiada efectiva PIRE (W)	Potencia isotrópica radiada efectiva PIRE (dBm)
1000	30	6	4	36
794	29	9	6.3	38
631	28	12	10	40
500	27	15	16	42
398	26	18	25	44
316	25	21	39.8	46
250	24	24	63.1	48
200	23	27	100	50
157	22	30	157	52

Para evitar la interferencia de los canales adyacentes, los equipos que trabajan con DSSS debe tener una separación de por lo menos 25 MHz entre las frecuencias centrales; debido a que la separación entre canales en la técnica DSSS es de 5 MHz, las redes deben estar ubicadas cada 5 canales tal como se muestra en la figura 30.

Figura 30. Separación entre canales en redes 802.11.

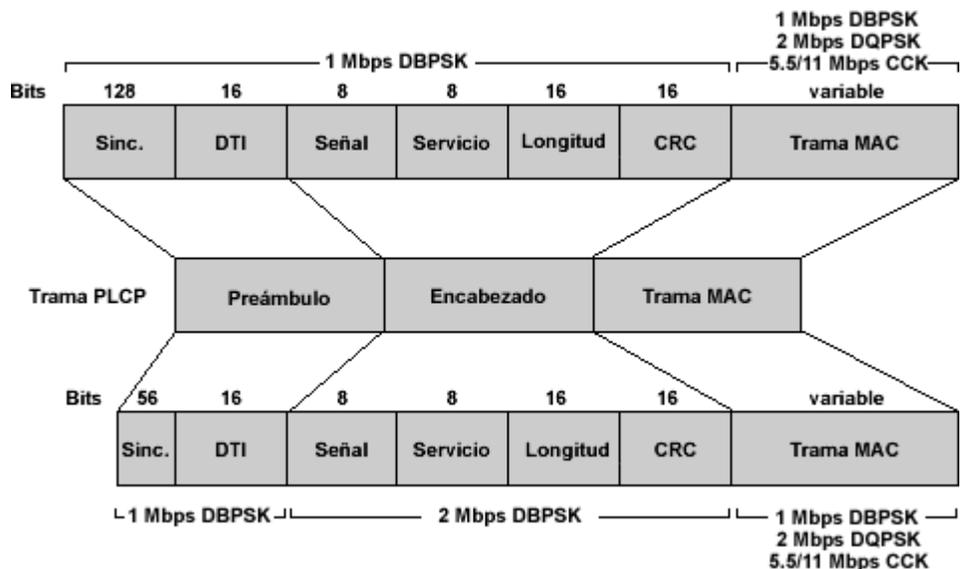


2.2 802.11b

802.11b se basa en la modulación de secuencia directa, sin embargo, permite transmitir a una velocidad hasta de 11 Mbps, por esta razón a esta capa se le denomina DSSS de alta velocidad (HR/DSSS). Aunque se modula de manera diferente a la forma original de secuencia directa, los canales usados son los mismos.

2.2.1 PLCP de 802.11b: para el formato de trama del PLCP se tienen dos opciones. Una opción es la trama larga igual al formato de trama usado en el 802.11. La otra opción es la corta y es mostrada en la figura 31. Sin embargo los equipos manejan el formato más corto por eficiencia y rendimiento, teniendo en cuenta que solo puede utilizarse si las estaciones lo soportan.

Figura 31. Trama PLCP 802.11b.



Preámbulo: es transmitido a 1 Mbps usando DBPSK, está compuesto del campo de sincronización y del campo DTI.

- *Sincronización de la trama PLCP*: en la trama larga este campo esta compuesto de 128 bits 1, la trama corta tiene 56 bits 0, este campo pasa por un proceso de codificación antes de ser transmitido.
- *Delimitador de inicio de trama (DTI)*: indica la finalización del campo de sincronización, en la trama corta el valor del campo es 0000 0101 1100 1111, en la trama larga es 1111 1010 0011 0000.

Encabezado: el preámbulo largo es transmitido a 1 Mbps usando DBPSK, pero como la razón de ser del preámbulo corto es reducir el tiempo de transmisión, el encabezado es transmitido a 2 Mbps usando DQPSK.

- *Señal*: este campo indica la velocidad y el método de transmisión de la trama MAC, los posibles valores de este campo para la trama larga son mostrados en la tabla 9. En la forma corta en el campo señal se definen solo los valores para las velocidades de 2 Mbps, 5.5 Mbps y 11 Mbps.

Tabla 9. Valores del campo señal.

Velocidad	Valores (menos a más significativo)
1 Mbps	0000 1010
2 Mbps	0001 0100
5.5 Mbps	0011 0111
11 Mbps	0110 1110

- *Servicio*: este campo se usa para indicar la cantidad de tiempo en microsegundos que debe ser usado por la trama. Extiende el campo de longitud que tiene la misma función, el tercer bit de este campo indica si en 802.11b el reloj está o no cerrado, esto significa que la frecuencia de transmisión y el reloj del símbolo, usan el mismo oscilador. El cuarto bit indica el tipo de codificación usado. Los bits que se encuentran reservados se fijan en 0. Este campo es el mismo tanto en formatos de tramas cortos como largos. Figura 32.

Figura 32. Campo de servicio en el encabezado PLCP 802.11b.



- *Longitud:* es el número de microsegundos requeridos para la transmisión de la trama MAC. El campo longitud es el mismo tanto en el formato de tramas PLCP corto como en el largo.
- *CRC:* el transmisor se encarga de calcular el CRC usando los campos de señal, servicio y longitud. Los receptores usan este valor para asegurarse de que el encabezado fue recibido sin errores. Este campo es igual tanto en el formato de tramas PLCP corto y largo.

Datos: lleva la trama MAC, es de longitud variable.

2.2.2 PMD de 802.11b: la subcapa PMD de 802.11b usa modulación de código complementario (CCK Complementary Code Keying) para lograr velocidades mayores a 2 Mbps. CCK es una secuencia de códigos usadas para modular la señal, dividiendo la cadena de chips en una serie de símbolos código de 8 bits. CCK permite usar una secuencia de 8 bits para codificar hasta de 6 bits por palabra código. En CCK existen 64 palabras código que pueden utilizarse para codificar la señal, hasta 6 bits pueden ser representados por cualquier palabra código. HR/DSSS permite que el receptor distinga fácilmente entre los diferentes códigos aún en presencia de interferencia o multitrayectoria contrario a DQPSK. En CCK también se ensancha la señal a través de la banda de frecuencias, pero usa ángulos de fase para convertir la palabra código en una palabra de 8 bits. CCK usa un proceso similar al del código Barker pero difiere en que la palabra código CCK es derivada en parte de los datos que se envían; en el código Barker siempre se usa la misma palabra de 11 chips. Ver tabla 10.

Tabla 10. Velocidades y modulación de 802.11b.

Velocidad de datos	Codificación	Modulación	Velocidad de símbolo	Bits/símbolo
1 Mbps	11 bits Barker	DBPSK	1 Msps	1
2 Mbps	11 bits Barker	DBPSK	1 Msps	2
5.5 Mbps	8 bits CCK	DQPSK	1.375 Msps	4
11 Mbps	8 bits CCK	DQPSK	1.375 Msps	8

2.3 802.11a

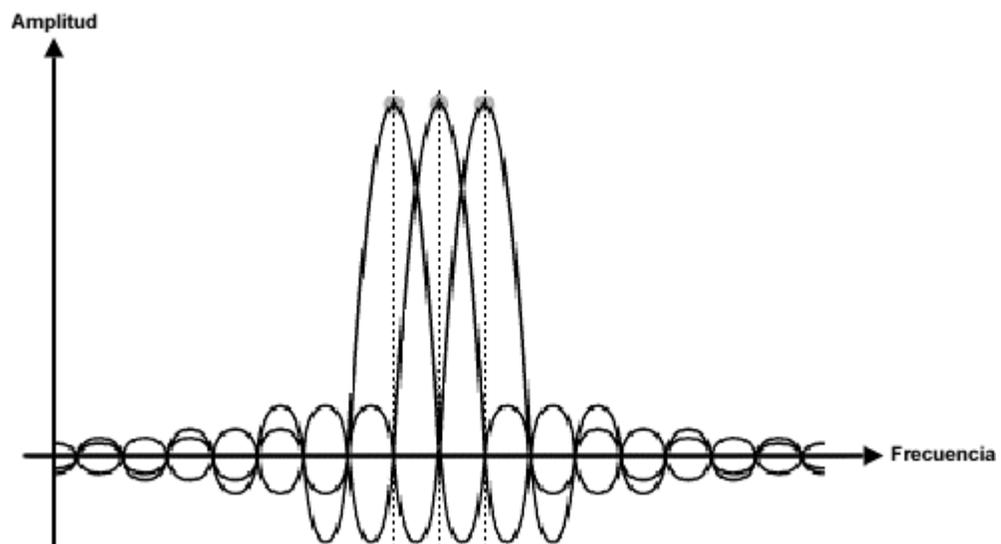
Los equipos 802.11a usan la banda de 5 GHz conocida como infraestructura de información nacional sin licencia (U-NII Unlicensed National Information Infrastructure). Las bandas U-NII proporcionan más espacio en el espectro y tienen menos fuentes de interferencia que la banda de

2.4 GHz, la desventaja es que al usar frecuencias altas se producen mayores pérdidas de propagación. 802.11a se basa en la multiplexación por división de frecuencia ortogonal (OFDM).

2.3.1 Multiplexación por división de frecuencia ortogonal (OFDM): OFDM es similar a la multiplexación por división de frecuencia (FDM Frequency Division Multiplexing). Ambas dividen el ancho de banda disponible en porciones llamadas portadoras y subportadoras, de modo que usa distintos canales para la transmisión de datos. FDM fue usada por teléfonos móviles de primera generación como un método para la ubicación del canal de radio. Cada usuario usa un canal y las bandas de guarda se usaron para asegurar que un usuario de un canal no causará problemas a los usuarios de los canales adyacentes, el problema con FDM es que las bandas de guarda desaprovechan ancho de banda y por lo tanto se reduce la capacidad.

OFDM utiliza las bandas de guarda desaprovechadas por FDM asignando canales que se superponen pero que no se interfieren, ya que se encuentran ortogonalmente separados, la ortogonalidad en frecuencia quiere decir que cuando una frecuencia presenta un máximo todas las demás tienen amplitud cero, por lo tanto se consigue un mayor uso del espectro y por ende un mayor rendimiento en la red. La figura 33, muestra la división de la banda en tres subportadoras, en el pico de cada subportadora, las otras tienen amplitud cero.

Figura 33. Ortogonalidad en el dominio de la frecuencia.



OFDM es un caso especial de transmisión multiportadora, donde una cadena de datos es transmitida sobre un número de subportadoras de baja velocidad, OFDM puede ser visto como una técnica de modulación o una técnica de multiplexación, con su uso se previene el desvanecimiento

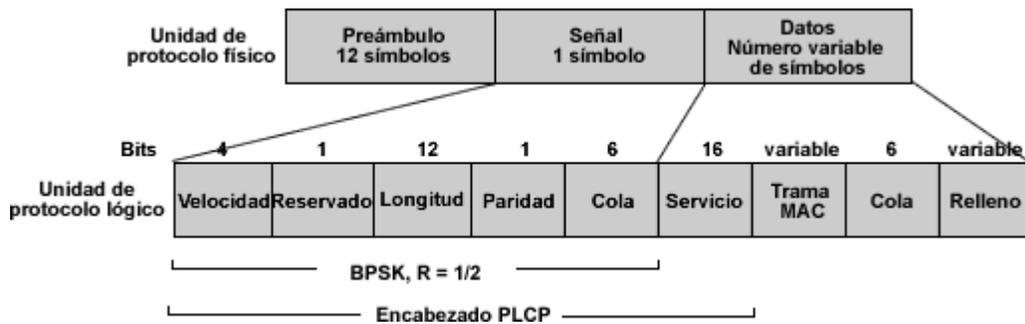
selectivo en frecuencia y la interferencia de banda estrecha, ya que al distribuir la información en subportadoras solo un pequeño porcentaje puede ser afectado por estos problemas, los errores pueden ser corregidos mediante el código convolucional.

OFDM toma la señal codificada para cada subportadora y usa una transformada rápida inversa de Fourier para crear la forma de onda que será transmitida. Los receptores OFDM aplican la transformada rápida de Fourier a la forma de onda recibida para extraer la amplitud de cada componente de la subportadora.

Código convolucional: OFDM usa un código de corrección de errores llamado COFDM (Coded Orthogonal Frequency Division Multiplexing). Una técnica comúnmente aplicada es la de código convolucional, este código es descrito por una relación R que especifica el número de bits de datos transmitidos por los bits totales. A medida que la relación se decrementa, más bits están disponibles para corregir errores y el código se vuelve más robusto, sin embargo entre más robusto menor rendimiento del sistema. 802.11a usa una relación de $\frac{1}{2}$ o en algunos casos usa una relación de $\frac{3}{4}$.

2.3.2 PLCP de 802.11a: el formato de trama PLCP es el mostrado en la figura 34.

Figura 34. Formato de trama PLCP de 802.11a.



2.3.2.1 Unidad de protocolo lógico: está compuesto por el encabezado PLCP, la trama MAC, la cola y el relleno.

Encabezado PLCP: este campo incluye los subcampos de velocidad, de longitud y de cola.

- *Velocidad:* ocupa cuatro bits que codifican la velocidad. En la tabla 11 se muestran los bits usados para codificar cada una de las velocidades.

- *Longitud:* 12 bits codifican el número de bytes que se encuentran en la trama MAC. La longitud es procesada por un código convolucional como protección contra errores.

Tabla 11. Bits usados en las velocidades.

Velocidad de datos Mbps	Bits (orden de transmisión)
6	1101
9	1111
12	0101
18	0111
24	1001
36	1011
48	0001
54	0011

- *Paridad y reservado:* El cuarto bit es reservado para uso futuro, por ahora se fija en 0. El bit número 17 es un bit de paridad para el campo de señal como protección contra errores.
- *Cola:* tiene 6 bits, finaliza el campo de señal con seis ceros. Estos bits son procesados por el código convolucional.
- *Servicio:* tiene 16 bits y finaliza el encabezado PLCP. Se transmite en un campo de datos de la unidad de protocolo de la capa física en la misma velocidad de datos de la trama MAC. Los primeros ocho bits son fijados en cero.

Trama MAC: como en otras capas físicas la trama MAC pasa por un proceso de codificación llamado *scrambling* antes de ser transmitidos, los primeros 6 bits se fijan en cero para iniciar el proceso de *scrambling*. Los bits restantes son para uso futuro y se fijan en cero. El esquema de codificación usado depende de la velocidad de los datos. El campo de servicio del encabezado se incluye en el campo de datos de la unidad de protocolo de la capa física ya que este inicia el proceso de *scrambling*.

Cola: tiene 6 bits, es colocado al final de la trama MAC y termina el código convolucional.

Relleno: este campo es variable, OFDM requiere que los bloques de bits de datos transferidos sean de tamaño fijo, el campo de datos es relleno de modo que la longitud siempre es un

múltiplo entero del tamaño del bloque. El tamaño del bloque depende del tipo de codificación y modulación usado por la velocidad de los datos.

2.3.2.2 Unidad de protocolo físico: esta compuesto por el preámbulo, la señal y los datos.

Preámbulo: el preámbulo está compuesto por 12 símbolos OFDM para la sincronización entre el transmisor y el receptor, para la decodificación de los símbolos, los 10 primeros símbolos representan la secuencia corta, en la cual el receptor detecta la señal más fuerte para seleccionar la antena adecuada (en el caso donde el receptor usa múltiples antenas).

Señal: el campo señal está compuesto por 1 símbolo OFDM y lleva los campos del encabezado PLCP excepto el servicio.

Datos: este campo tiene un número variable de símbolos, está conformado por los campos de servicio, trama MAC, cola y relleno.

2.3.3 PMD de 802.11a: los canales que operan en 802.11a tiene un ancho de 20 Mhz cada uno, OFDM divide cada canal en 52 subportadoras. Cuatro subportadoras se usan como subportadoras piloto, para monitorear los cambios de trayectoria en la interferencia entre portadoras, las otras portadoras se usan para la transmisión de datos. El espaciamiento entre subportadoras es de 0.3125 MHz.

OFDM en 802.11a usa diferentes esquemas de modulación para lograr diferentes velocidades de datos dentro del rango de 6 Mbps a 54 Mbps. Todos los esquemas de modulación usan una velocidad de símbolo de 250.000 símbolos por segundo a través de 48 subportadoras, el número de bits de datos por símbolo varía.

Existen cuatro grupos de velocidades: 6 y 9 Mbps, 12 y 18 Mbps, 24 y 36 Mbps y por último 48 y 54 Mbps. Las velocidades de 6 y 9 Mbps se consiguen con modulación de cambio de fase binaria (BPSK Binary Phase Shift Keying), que codifica un bit por subportadora o 48 bits por símbolo. Debido al código convolucional la mitad o un cuarto de los bits son bits redundantes, usados para la corrección, así solo hay 24 o 36 bits de datos por símbolo. Las velocidades de 12 y 18 Mbps se logran con modulación de cambio de fase en cuadratura (QPSK Quadrature Phase Shift Keying), que codifica dos bits por subportadora, para un total de 96 bits por símbolo; después de sustraer el encabezado del código convolucional, el receptor queda con 48 o 72 bits de datos. Las velocidades de 6 y 9 Mbps se consiguen con modulación de cambio de amplitud en cuadratura 16

QAM (QAM Quadrature Amplitude Modulation) para codificar cuatro bits usando 16 símbolos, para un total de 192 bits por símbolo; después de quitar los bits del código convolucional, el receptor queda con 96 o 144 bits de datos. Por último, 48 Mbps y 54 Mbps, se logran mediante 64 QAM, que codifica 6 bits usando 64 símbolos, sin los bits del código convolucional, los bits de datos son 192 y 216 bits de datos. En la tabla 12 se puede ver algunos detalles de la codificación para las diferentes velocidades en OFDM.

Tabla 12. Velocidades y modulaciones en 802.11a.

Velocidad (Mbps)	Modulación y Relación de código R	Bits codificados por portadora	Bits codificados por símbolo	Bits de datos por símbolo
6	BPSK, R=1/2	1	48	24
9	BPSK, R=3/4	1	48	36
12	QPSK, R=1/2	2	96	48
18	QPSK, R=3/4	2	96	72
24	16-QAM, R=1/2	4	192	96
36	16-QAM, R=3/4	4	192	144
48	64-QAM, R=2/3	6	288	192
54	64-QAM, R=3/4	6	288	216

Los bits codificados por subportadora son una función de la modulación, los bits codificados por símbolo son una función de la velocidad del código convolucional.

Las potencias permitidas para el uso de la banda de 5 GHz en Colombia, fueron reguladas en la resolución número 000689 de 2004 del Ministerio de Comunicaciones de Colombia, una copia de la resolución está en el Anexo B. En la tabla 13, se muestran las potencias permitidas en cada banda.

Las potencias son para antenas con ganancias de 6 dBi. Si se utilizan antenas con ganancia mayor a 6dBi, la potencia pico de transmisión y la densidad espectral de potencia pico deberán ser reducidas en la cantidad de dB que sobrepasen los 6 dBi.

Para antenas omnidireccionales la potencia máximo permitido a la entrada de la antena es 100 mW, para antenas que excedan esta potencia deben usar antenas direccionales con un lóbulo no mayor a 90°.

Tabla 13. Canales y potencia para OFDM.

Banda	Potencia permitida	Número de canales	Frecuencia central
Banda baja U-NII (5.15-5.25 GHz)	El menor valor de: 50 mW o 4dBm +10 log B	36	5.180 GHz
		40	5.200 GHz
		44	5.220 GHz
		48	5.240 GHz
Banda media U-NII (5.25-5.35 GHz)	El menor valor de: 250 mW u 11dBm +10 log B	52	5.260 GHz
		56	5.280 GHz
		60	5.300 GHz
		64	5.320 GHz
Banda superior U-NII (5.725-5.825 GHz)	El menor valor de: 1 W o 17dBm +10 log B	149	5.745 GHz
		153	5.765 GHz
		157	5.785 GHz
		161	5.805 GHz

En la anterior tabla B hace referencia al ancho de banda de emisión a 26 dB*.

En la banda superior se pueden emplear antenas con ganancia hasta de 23 dBi, sin la correspondiente reducción, en los sistemas de operación punto a punto, ver tabla 14. Cuando se emplean antenas que pasan de 23 dBi se debe reducir 1 dB por cada dB que sobrepase la ganancia.

Tabla 14. Operación punto a punto en la banda superior de 5 GHz.

Potencia entregada a la antena (mW)	Potencia entregada a la antena en (dBm)	Máxima ganancia de la antena (dBi)	Potencia isotrópica radiada efectiva PIRE (W)	Potencia isotrópica radiada efectiva PIRE (dBm)
1000	30	6	4	36
1000	30	9	8	39
1000	30	12	16	42
1000	30	15	316	45
1000	30	18	63.1	48
1000	30	21	125	51

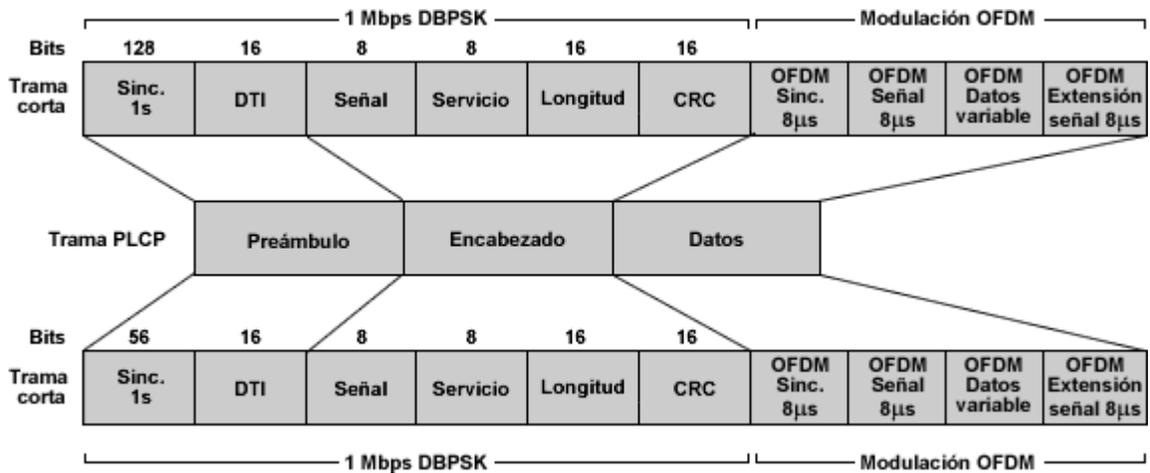
* Ancho de banda de emisión es la medida del ancho de la señal entre dos puntos, uno por debajo de la frecuencia central de la portadora y otro por encima de la frecuencia de la portadora, esta a 26 dB relativo al máximo nivel de la portadora modulada.

2.4 802.11g

La norma 802.11g combina la velocidad de 802.11a con el alcance de los dispositivos 802.11b. 802.11g proporciona la ventaja de la interoperabilidad con 802.11b. 802.11g opera en la banda ISM de 2.4 GHz utilizando los mismos canales y las mismas potencias que 802.11b pero usa diferentes esquemas de modulación. 802.11g es también conocido como capa física con velocidad extendida (ERP Extended Rate Physical), que significa una mejora en velocidad.

2.4.1 PLCP de 802.11g: la capa física PLCP tiene dos tipos de formato, que depende del tipo de preámbulo usado. El preámbulo corto se usa con la intención de mejorar la eficiencia de la red inalámbrica, para permitir aplicaciones en tiempo real como voz y video. Los equipos 802.11g deben ser capaces de transmitir y recibir tramas con preámbulos cortos y largos.

Figura 35. Trama PLCP de 802.11g.



2.4.2 PMD de 802.11g: la norma puede soportar varias velocidades de datos lo que permite que los clientes seleccionen la mejor velocidad posible para su comunicación, adiciona a las velocidades soportadas por 802.11b (1, 2, 5.5 y 11 Mbps) las velocidades de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps, de las anteriores son obligatorias las velocidades de 1, 2, 5.5, 11, 6, 12 y 24 Mbps.

802.11g soporta CCK y código Barker para soportar velocidades hasta de 11 Mbps lo que garantiza la compatibilidad con 802.11b y modulación OFDM para soportar velocidades altas hasta de 54 Mbps.

802.11g proporciona un mecanismo de protección para permitir la comunicación de clientes 802.11g y 802.11b dentro de un mismo ambiente. Un dispositivo 802.11b no escucha cuando el medio inalámbrico está ocupado con una señal 802.11g OFDM, el mecanismo de protección se encarga de avisar a los clientes 802.11b que el medio esta siendo usado por un cliente 802.11g OFDM. El uso de la protección produce mas intercambio de mensajes de control reduciendo el rendimiento de los usuarios. Los mecanismos de protección usados son el RTS/CTS y el CTS.

Cuando el AP y todos los clientes son 802.11g, se consigue el máximo rendimiento, el AP detecta que todos los clientes son 802.11g y la comunicación se hace sin el mecanismo de protección. Cuando el AP es 802.11g y los clientes son 802.11b y 802.11g, el AP detecta ambas tecnologías y activa el mecanismo de protección, haciendo que el rendimiento caiga un 25% del máximo. Cuando el AP es 802.11b y los clientes son 802.11g, el cliente es capaz de asociarse con el AP, la comunicación se hace usando CCK y se alcanza velocidades de 802.11b, el cliente 802.11g puede funcionar como un cliente 802.11b.

2.5 PARÁMETROS DE LA CAPA FÍSICA

En la siguiente tabla se recopilan algunos de los parámetros de las diferentes capas físicas de las normas 802.11, estos parámetros son útiles para la subcapa MAC.

Tabla 15. Parámetros de la capa física 802.11.

Parámetro	802.11	802.11b	802.11a	802.11g
Ranura de tiempo	20 μ s	20 μ s	9 μ s	20 μ s
Tiempo SIFS	10 μ s	10 μ s	16 μ s	10 μ s
Duración del preámbulo	144 μ s	144 μ s	20 μ s	20 μ s
Duración de encabezado PLCP	48 μ s	48 μ s	4 μ s	4 μ s
Trama MAC máxima	4095 bytes	4095 bytes	4095 bytes	4095 bytes

3. INFRAESTRUCTURA Y PROPAGACIÓN EN UNA RED DE AREA LOCAL INALÁMBRICA

Este capítulo cubre las diferentes clases de equipos, los dispositivos cliente, antenas, accesorios y las diferentes topologías que se encuentran en una red inalámbrica, los equipos anteriores constituyen la infraestructura de una red de área local inalámbrica, en una comunicación inalámbrica entre diferentes equipos, la señal puede o no encontrar obstáculos que afectan su propagación, debido a ello en este capítulo también se consideran los diferentes modelos de propagación para redes de este tipo.

Para lograr que una red WLAN sea más eficiente necesita de una estación base, en las normas IEEE 802.11 se hace referencia solamente a los puntos de acceso pero los fabricantes se han encargado de introducir los conceptos de *gateway* inalámbrico y puente.

Las diferencias entre un AP y un *gateway* inalámbrico no son muchas, ya que sus funciones son muy parecidas. Un AP está orientado a grandes empresas, Campus universitarios, etc., que ya tienen una infraestructura de red cableada. Un *gateway* inalámbrico está orientado a ambientes donde no se cuenta con una red cableada.

La norma 802.11 no define específicamente un puente, pero los fabricantes han construido puentes inalámbricos a ser implementados en redes bajo esta norma. Un puente se utiliza para interconectar redes LAN cableadas o para extender el rango de la red inalámbrica existente. Un puente es más fácil de instalar, configurar y menos costoso que un AP.

3.1 PUNTO DE ACCESO

Proporciona a los clientes un punto de acceso a la red. Es un dispositivo *half duplex* inteligente equivalente a un *hub* en Ethernet. Los APs se comunican con sus clientes, con la red cableada y con APs. El AP es considerado un portal, ya que permite conectividad desde una red 802.11 a una red 802.3 o a una red 802.5.

Un AP no proporciona enrutamiento de traducción de dirección de red (NAT Network Address Translation) o protocolo de configuración dinámica de anfitrión (DHCP Dynamic Host Configuration Protocol), ya que los enrutadores y/o servidores de la red cableada hacen estas funciones, por esta

razón son ideales para ambientes con una infraestructura de red ya existente como en el caso de grandes empresas, campus universitarios, etc.. Proporcionan *roaming*, alto nivel de seguridad, alto nivel de gestión y control de red dependiendo de su configuración. Un AP puede tener diferentes opciones hardware y software:

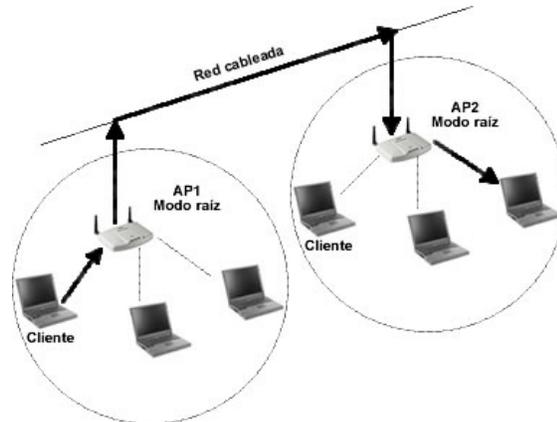
- *Antenas fijas o removibles:* se puede conectar una antena a un AP por medio de un cable dependiendo de las necesidades del cliente. En caso de necesitar cubrimiento externo se puede conectar una antena removible a un AP por medio de un cable, para ubicar una antena externa fuera del edificio y el AP dentro del edificio. Debido al fenómeno de multitrayectoria a un AP le pueden llegar señales por diferentes trayectorias, como una solución a este problema se usa la diversidad de antena con la cual se consigue capturar la mejor señal en recepción. El AP puede o no tener diversidad de espacio con sus antenas fijas.
- *Capacidades de filtrado avanzado:* un AP puede incluir funcionalidad de filtrado de protocolos o direcciones MAC, como mecanismo de seguridad contra intrusos.
- *Tarjetas radio removibles:* algunos APs tienen dos ranuras para tarjetas PCMCIA, permitiendo tener la funcionalidad de tener dos APs en uno, es decir, que un solo AP puede trabajar en diferentes canales evitando la superposición.
- *Potencia de salida variable:* algunos APs permiten controlar la potencia de salida, permitiendo por consiguiente variar el área de cubrimiento. También se puede variar el área de cubrimiento mediante el uso de APs con salida fija, añadiendo accesorios tales como amplificadores, atenuadores, cables, etc..
- *Conexión a red cableada:* las opciones de conectividad de un AP incluyen 10baseTx, 10/100baseTx, 100baseFx, 100baseTx, *token ring* y otros. Cuando se conecta un AP a un armario se debe tener en cuenta las limitantes de distancia, por ejemplo los cables Cat5 están especificados hasta los 100 metros.
- *Configuración:* un AP se puede configurar por consola, telnet, USB, web o software propietario.

3.1.1 Modos de configuración de los APs: los APs pueden configurarse para comunicarse a través del medio inalámbrico o a través de la red cableada con otros APs o con clientes.

3.1.1.1 Modo raíz: es el modo que viene por defecto en un AP, se usa cuando se conecta el AP a la red cableada para proporcionar acceso a diferentes clientes inalámbricos. Cuando varios APs están en modo raíz estos se comunican entre si solo a través de la red cableada, dos APs en modo raíz no se pueden comunicar a través del medio inalámbrico; el AP en este modo se comunica por

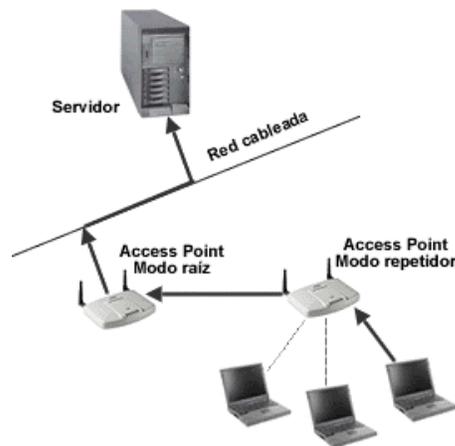
el medio inalámbrico solo con los clientes y con repetidores. Ver figura 36. Para el proceso de *roaming* los APs en modo raíz se comunican entre ellos mediante el protocolo entre APs que se encuentra en la norma 802.11f para compartir información sobre los clientes dentro del ESS, con este proceso, los clientes que cambian a otro AP no deben asociarse de nuevo, simplemente llevan a cabo el proceso de re-asociación.

Figura 36. AP en modo raíz.



3.1.1.2 Modo repetidor: funciona como un intermediario entre un AP en modo raíz y clientes, se usa para extender la cobertura de un AP. El AP en modo repetidor es un cliente del AP en modo raíz. Un AP en modo repetidor se usa solo en caso necesario, ya que no es recomendable debido a que las celdas de los dos APs deben superponerse al menos en un 50%, reduciendo el rendimiento de los clientes conectados al repetidor. El puerto Ethernet del AP en modo repetidor debe ser deshabilitado. Ver figura 37.

Figura 37. AP en modo repetidor.



3.2 GATEWAY INALAMBRICO

Un *gateway* inalámbrico es un dispositivo de interconexión de redes que enruta tramas de una WLAN a otra red, típicamente una red de área amplia (WAN Wide Area Network). Este dispositivo opera en la capa 2 y 3 del modelo OSI. Combina las funciones de un AP, un enrutador y a menudo proporciona funciones de *firewall*.

Frecuentemente incluyen enrutamiento NAT y servicios DHCP, crea y proporciona direcciones IP individuales de modo dinámico por esto es útil en redes pequeñas tales como oficinas y redes caseras, cuando el sistema inalámbrico no está conectado a una LAN. Un *gateway* inalámbrico puede incluir seguridad, encriptación, VPN y VoIP. Los *gateway* inalámbricos se pueden dividir en dos clases: residencial y empresarial.

3.2.1 Gateway inalámbrico residencial: tiene las características básicas para ser implementado en una pequeña oficina y el hogar, las cuales son:

- Incluye servidor de DHCP.
- Usa traducción de direcciones de red (NAT).
- Tiene un puerto para conectarse a la WAN, ya sea a través de cable modem, modem DSL, modem satelital, modem analógico, puerto serial o puerto Ethernet.
- Tienen una antena incorporada.
- Pueden ser configurados con un software propietario o a través de puerto serial o USB.
- Los costos son bajos comparados con los *gateway* empresariales.

Figura 38. Diagrama físico de un *gateway* residencial.

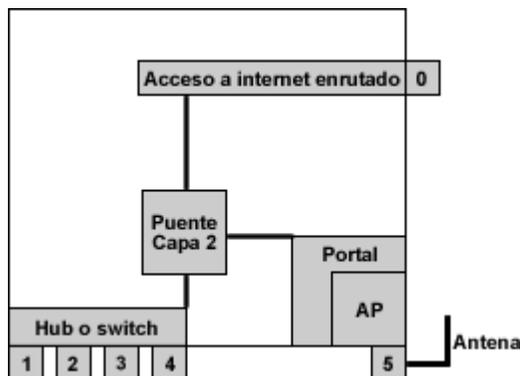
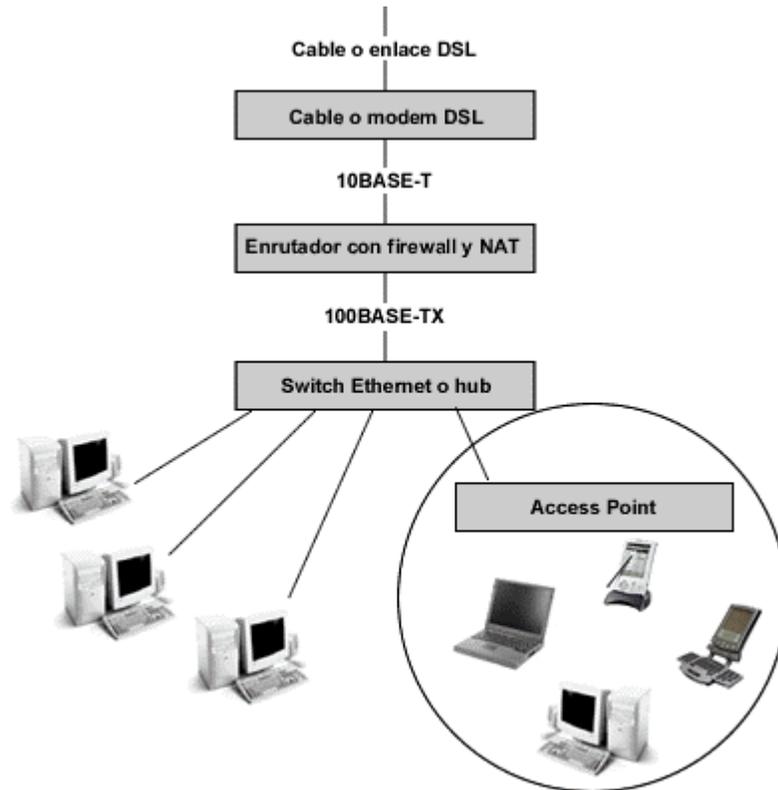


Figura 39. Componentes lógicos de un *gateway* residencial



3.2.2 Gateway inalámbrico empresarial: útil en ambientes más grandes que los residenciales, proporcionan además de las funcionalidades de los *gateway* residenciales las siguientes características:

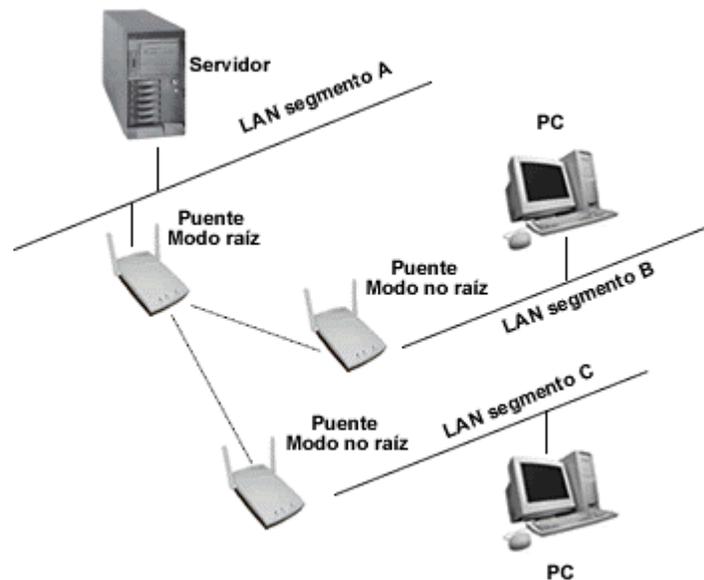
- El área sobre la cual se requiere movilidad puede llegar a ser mucho mayor, y requiere que varias *gateway* trabajen en conjunto, para ello deben soportar el protocolo entre *puntos de acceso* 802.11f.
- Tienen tarjetas PCMCIA removibles que permite una actualización a los *gateway* en el caso que se requiera cambio de tecnología.
- Las interfaces inalámbricas en los *gateway* empresariales permiten la posibilidad de usar antenas externas con el fin de proporcionar cobertura en áreas específicas. La potencia de transmisión puede ser ajustada en varios dispositivos para aumentar o disminuir el área de cobertura.
- Soportan seguridad 802.1x.
- Tiene capacidades de SNMP, monitoreo y gestión mucho más amplia que los *gateway* residenciales.

3.3 PUENTE

El puente sirve para conectar dos redes cableadas separadas entre sí, es un dispositivo *half duplex* que realiza conectividad en la capa 2. A un puente no se le pueden conectar directamente clientes inalámbricos. Los puentes se usan generalmente para conexiones punto a punto. Los puentes inalámbricos pueden comunicarse con otros puentes en uno de los tres modos siguientes:

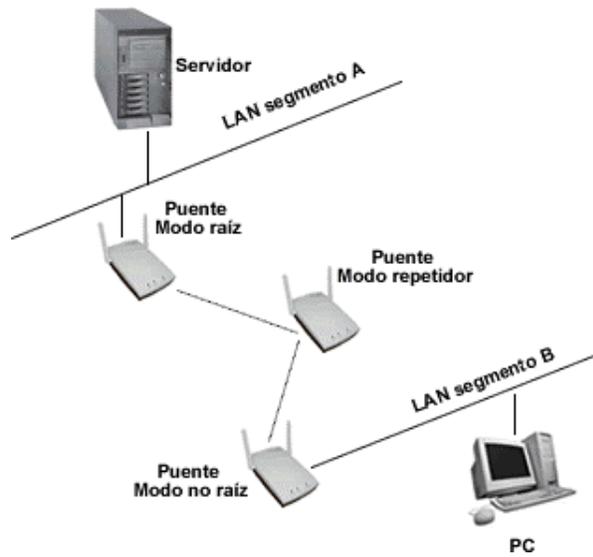
- Modo raíz: un puente en este modo solo se puede comunicar con un puente en modo no-raíz, o un puente en modo repetidor y con la red cableada, pero no puede asociarse con otro puente en modo raíz. Ver figura 40.
- Modo no raíz: un puente inalámbrico en este modo se conecta directamente a un puerto Ethernet para luego conectarse inalámbricamente a un AP o a un puente, ambos en modo raíz. Ver figura 40.

Figura 40. Comunicación de puente modo raíz con puente modo no raíz.



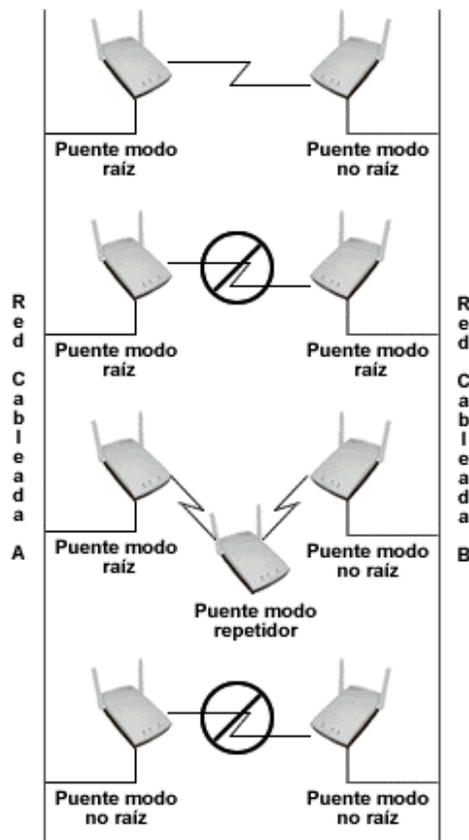
- Modo repetidor: en este modo un puente se conecta entre dos puentes uno de ellos en modo raíz y el otro en modo no raíz, con el propósito de extender la comunicación inalámbrica. Los puentes en modo repetidor son puentes en modo no-raíz a los cuales se les deshabilita la conexión a la red cableada. Un puente en este modo reduce el rendimiento debido a que las tramas deben ser repetidas al llegar al puente en modo repetidor. Ver figura 41.

Figura 41. Puente en modo repetidor.



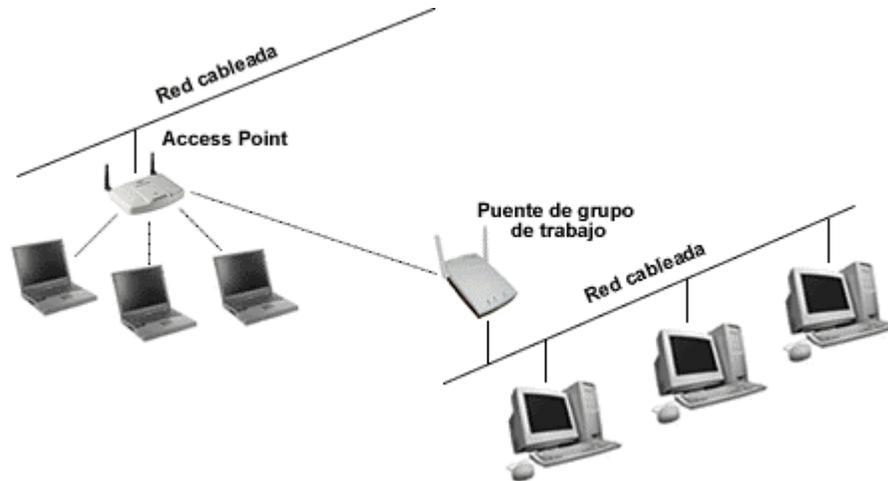
En la figura 42 se muestra los diferentes modos de configuración de los puentes y las conexiones permitidas y no permitidas entre ellos.

Figura 42. Comunicación entre puentes.



Puentes de grupo de trabajo (WGB): un puente de grupo de trabajo (WGB WorkGroup Bridge) conecta redes inalámbricas a redes Ethernet cableadas, actúa como cliente para el AP. Estos puentes son útiles en campus que tiene edificios remotos donde un pequeño grupo de usuarios necesita acceder a la red principal. También un WGB puede hacer filtrado de protocolos o de direcciones MAC, lo que permite controlar el tráfico a través del enlace inalámbrico. Ver figura 43.

Figura 43. Puente de grupo de trabajo instalado en una red.



3.4 DISPOSITIVOS CLIENTE EN UNA WLAN

Para que los APs proporcionen conectividad inalámbrica a clientes como computadores de escritorio, computadores portátiles, Palms, PDAs, periféricos, se necesita de dispositivos adicionales conocidos como dispositivos cliente. Estos dispositivos son los siguientes:

3.4.1 Tarjeta PCMCIA: se conocen también como tarjetas PC, es el dispositivo cliente más común, se usan en computadores portátiles, PDAs, etc., también pueden estar en algunos APs, puentes, puentes de grupo de trabajo, *gateways*, adaptadores USB, adaptadores PCI e ISA. La mayoría de estas tarjetas están listas para conectar y se insertan en las ranuras PC de los equipos clientes.

Las tarjetas PC son dispositivos pequeños y planos que pueden tener antenas fijas en el extremo de la tarjeta que por lo general usan diversidad dual, o pueden tenerlas removibles conectadas a la tarjeta PC mediante un cable, esto permite que pueda usarse una antena de mayor ganancia para aumentar el rango.

3.4.2 Tarjetas flash compactas: también se conocen como tarjetas CF, tienen la misma funcionalidad que las tarjetas PC pero su diferencia radica en que las tarjetas CF tienen menor tamaño y menor potencia de salida, por estas razones son usadas prioritariamente en PDAs.

3.4.3 Conversor Ethernet y seriales: se usan en dispositivos que tienen puertos seriales o Ethernet para convertir estas conexiones de red en conexiones WLAN. Los conversores Ethernet permiten convertir un grupo de nodos cableados a inalámbricos durante un corto período de tiempo. Los conversores seriales son usados en equipos de telemetría e impresoras seriales que usan puerto serial para conectarse a la red.

3.4.4 Adaptadores USB: la mayoría de los equipos cliente no tienen ranuras para tarjetas PC, este problema se resuelve usando un adaptador USB. Este adaptador se conecta al puerto USB del equipo cliente y no requiere más potencia que la que es entregada a través del puerto USB. Los adaptadores USB pueden tener tarjetas PC removibles o fijas.

3.4.5 Adaptadores PCI e ISA: es útil en equipos que no tienen ranuras PC, estos adaptadores se instalan dentro de un computador de escritorio o un servidor por medio del bus ISA o PCI para habilitarlo para que trabaje inalámbricamente. Estos adaptadores pueden venir con la antena incluida, en caso contrario requiere el uso de una tarjeta PC que se inserta dentro del adaptador.

3.4.6 Módulos mini PCI: es un módulo conectado a una extensión del bus PCI llamado mini PCI. Viene embebido en algunos computadores portátiles y de escritorio. Permite conectividad a una WLAN.

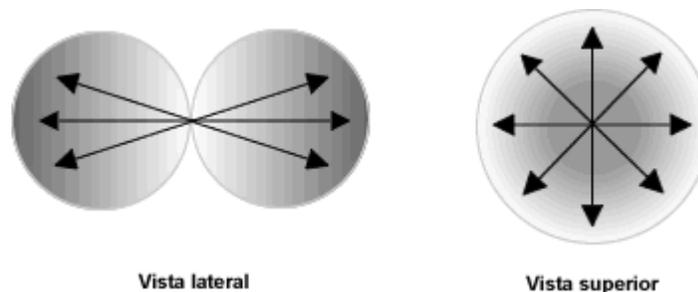
3.5 ANTENAS

Un componente muy importante de los APs, *gateways*, puentes y de los dispositivos cliente son las antenas. Como se señaló anteriormente, las antenas generalmente están incorporadas en estos equipos o pueden ser removibles. Las antenas se usan frecuentemente para incrementar el rango de cobertura en los sistemas WLAN, pero una mala selección y posición de las antenas puede hacer que la señal se propague fuera del área pretendida permitiendo su fácil interceptación. En esta sección se hace referencia a los tipos de antena, sus patrones de radiación, la polarización, y usos de diferentes antenas y la forma como la posición de la antena puede mejorar la señal en recepción.

3.5.1 Tipo de antenas: la antena está determinada por su patrón de radiación, puede ser omnidireccional o direccional. Deben ser ubicadas de acuerdo a su uso, una antena omnidireccional es buena para efectos de gran cubrimiento, una antena direccional de baja ganancia es útil en ambientes como corredores y una antena direccional de alta ganancia es ideal en enlaces punto a punto entre edificios o puntos remotos.

3.5.1.1 Antena omnidireccional: es la antena más común en WLAN, una antena omnidireccional radia su energía alrededor de su eje en todas las direcciones, un ejemplo de una antena omnidireccional es el dipolo. El patrón de radiación del dipolo se muestra en la figura 44, su ganancia puede estar en el rango de 3 dBi a 10 dBi, entre mayor sea la ganancia, el patrón de radiación es más estrecho. El dipolo se ubica en el centro del área que se desea cubrir, si se trata de un edificio, alguna parte de la señal afectará el piso superior e inferior.

Figura 44. Patrón de radiación de una antena omnidireccional.



3.5.1.2 Antena direccional de baja ganancia: una antena direccional de baja ganancia radia su energía en una dirección particular. El patrón típico de este tipo de antena se puede ver en la figura 45. Por sus características, una antena direccional de baja ganancia puede usarse en un rango medio, como el caso de puente entre dos edificios separados por una calle, también puede usarse dentro de edificios para ampliar el cubrimiento dado por una antena omnidireccional, tal es el caso de un corredor largo. Las antenas direccionales de baja ganancia comúnmente usadas en una WLAN son las antenas Patch, Panel y Yagi. El valor de ganancia de una antena Yagi puede estar entre 12 y 18 dBi.

Figura 45. Patrón de radiación de una antena direccional de baja ganancia.



3.5.1.3 Antena direccional de alta ganancia: este tipo de antena emite la mayoría de su señal en un rayo estrecho, como se puede ver en la figura 46, tiene un valor de ganancia más grande comparado con la direccional de baja ganancia y la omnidireccional. Una antena direccional de alta ganancia es útil para enlaces punto a punto de grandes distancias y no puede ser útil para dar servicio a estaciones móviles. Como ejemplo de antena direccional de alta ganancia está la antena parabólica, que típicamente tiene valores de ganancia hasta 24 dBi.

Figura 46. Patrón de radiación de una antena altamente direccional.

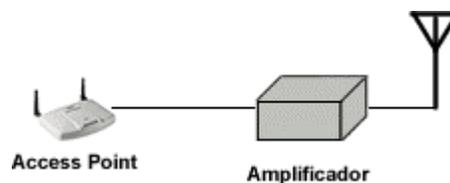


3.6 ACCESORIOS WLAN

Para poder conectar todos los dispositivos inalámbricos en una red es necesario usar accesorios que permitan maximizar el rendimiento, reducir las pérdidas y hacer conexiones correctamente. Entre los diferentes accesorios útiles en una WLAN se encuentran: amplificadores RF, atenuadores RF, supresores de transientes, conectores RF, cables RF, divisores RF y *pigtails*. El uso de estos accesorios puede ser obligatorio en algunos casos.

3.6.1 Amplificador RF: se usa para incrementar la amplitud de una señal de radiofrecuencia (RF Radio Frequency) y se conecta a un AP que tiene la opción de conectar una antena externa. Existen amplificadores unidireccionales usados para transmisión y amplificadores bidireccionales usados para transmisión y recepción. En cualquiera de los casos el amplificador RF se ubica lo más cerca posible a la antena con el objeto de disminuir la intervención del ruido, para poder compensar las pérdidas de la señal transmitida al pasar por el cable que une el AP con la antena o las pérdidas de propagación en el espacio libre y en recepción para ampliar la señal recibida aumentando la sensibilidad. Ver figura 47.

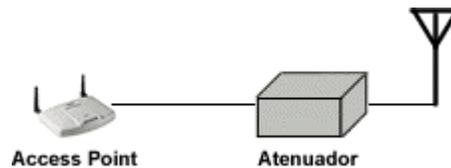
Figura 47. Ubicación del amplificador RF en una WLAN.



En la elección de un amplificador RF se debe tener en cuenta la impedancia (ohmios) generalmente los componentes de una WLAN tienen una impedancia de 50 ohmios; ganancia (dB), se obtiene a partir de los cálculos hechos para la señal RF; respuesta en frecuencia (rango en GHz), indica la banda de frecuencia en que opera la WLAN; voltaje de relación de onda estacionaria (VSWR Voltaje Standing Wave Ratio), especificaciones de entrada (mW o dBm) y de salida (mW o dBm). Como el amplificador RF se conecta a la red, entonces debe ser escogido con el mismo tipo de conectores que use el cable y la antena.

3.6.2 Atenuador RF: se utiliza para decrementar la amplitud de la señal RF. Es útil por ejemplo cuando se tiene un AP con una salida fija en mW y se tiene una antena con una ganancia muy grande, debido a que existen reglas en cuanto a la magnitud de potencia de señal de RF a la salida es necesario disminuir esta potencia. Un atenuador es ubicado en cualquier punto entre el AP y la antena, ver figura 48. Al igual que con el amplificador RF se debe tener en cuenta el tipo de conector usado, la impedancia, atenuación, potencia de entrada, respuesta en frecuencia.

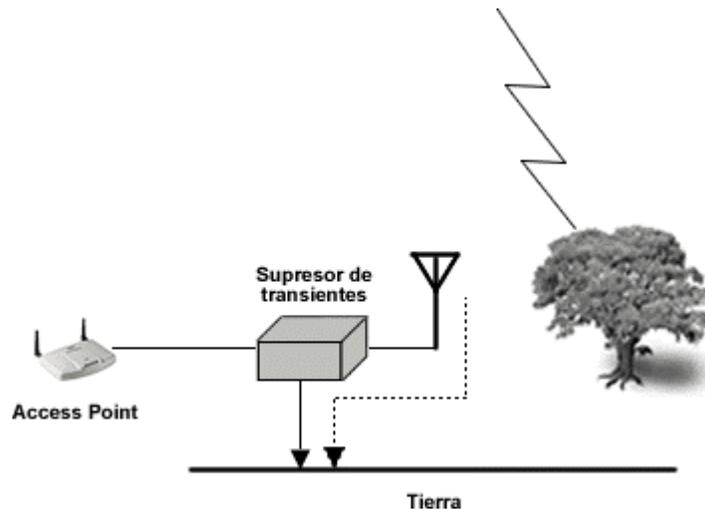
Figura 48. Ubicación de un atenuador en una WLAN.



3.6.3 Supresor de transientes: un supresor de transientes es usado para desviar a tierra la corriente transiente causada por un relámpago. En una WLAN se usan supresores de transientes para proteger el equipo WLAN que está conectado a la antena por medio de un cable, como se muestra en la figura 49. Cuando un rayo cae sobre un objeto, crea un campo eléctrico alrededor por un instante, cuando el rayo termina, el campo colapsa induciendo cantidades altas de corriente a los objetos cercanos, en una WLAN estos objetos cercanos pueden ser el cable o la antena. Lo anterior no quiere decir que un supresor de transientes en una WLAN proteja la red completamente, si el rayo cae directamente a la antena ni el mejor supresor de transientes en el mercado puede proteger de una destrucción de la WLAN.

Algunos supresores de transientes pueden ser reusables y otros no; se debe tener en cuenta el tipo de conector usado; respuesta en frecuencia; impedancia; relación de onda estacionaria; pérdidas de inserción (dB), garantía del producto, deben actuar en menos de 8 μ s acorde con las normas de la IEEE.

Figura 49. Supresor de transientes instalado en una WLAN.



3.6.4 Divisores RF: es un dispositivo que tiene una única entrada y múltiples salidas, el objetivo es dividir la señal RF en múltiples señales RF. Puede ser útil cuando se necesita combinar dos antenas para generar un patrón de radiación específico, por ejemplo dos antenas semidireccionales apuntando a dos direcciones diferentes. Un divisor RF no es muy usado en implementaciones WLAN, pero sirve para tomar muestras de la señal.

3.6.5 Conectores RF: los conectores RF se usan para conectar cables a dispositivos o para conectar dispositivos a dispositivos. En una WLAN es típico encontrar conectores N, SMA, BNC y TNC. Cuando se escoge un conector se debe tener en cuenta la impedancia de los otros componentes de la WLAN, las pérdidas de inserción del conector, la respuesta en frecuencia y el género (femenino o masculino).

N: es un conector con rosca usado para unir cables coaxiales. Este conector es usado en instalaciones profesionales, casi todas las antenas para exteriores usan este tipo. Esta disponible para casi todos los tipos de cables. Su nombre es debido a la inicial del inventor Paul Nelly del laboratorio Bell.

Figura 50. Conector tipo N.



BNC (Bayonet Neill-Concelman): tipo de conector RF más pequeño que el conector tipo N. Usado para terminación de cable coaxial. Raramente es visto en equipos 802.11. Disponible para la mayoría de los cables.

Figura 51. Conector BNC.



SMA (Subminiature A): conector pequeño, fue diseñado por Bendix Scintilla Corporation y es uno de los conectores RF mas usados. Tiene un mecanismo de acoplado tipo rosca y está disponible para el uso con cables RG-316, RG-58 y H-155.

Figura 52. Conector SMA.



TNC (Threaded Neill Concelman): este conector es una versión con rosca del conector BNC, es usado en algunos APs. Esta disponible para cables tipo RG-316, RG-174, RG-58 y H-155.

Figura 53. Conector TNC.



3.6.6 Cables RF: los cables RF sirven para conectar las antenas a los APs o tarjetas PC, entre menor sea la distancia entre ellos, así mismo serán las pérdidas, además al incrementar la frecuencia también incrementan las pérdidas del cable. La tabla 16 muestra algunos de los cables coaxiales más comunes y sus pérdidas para la banda de 2.4 GHz.

Tabla 16. Pérdidas cable coaxial a 2.4GHz.

Tipo de cable	Pérdidas típicas [db/m]
RG 58	1
RG 213	0.6
RG 174	2
Aircom	0.21
Aircell	0.38
LMR-400	0.22

3.6.7 Pigtail: es un cable adaptador usado para conectar cables que tienen conectores estandarizados a equipos propietarios WLAN. Su uso más frecuente es para conectar antenas externas a APs o tarjetas PCMCIA. El *pigtail* se muestra en la figura 54.

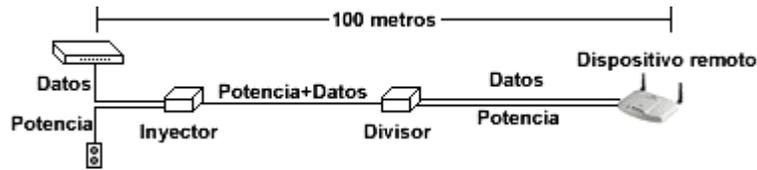
Figura 54. *Pigtail*.



3.6.8 Conversor de frecuencia: se usa para convertir un rango de frecuencia a otro. Es útil cuando se desea cambiar de banda, por ejemplo, pasar de una banda muy congestionada a una que no esté muy congestionada.

3.6.9 Potencia sobre Ethernet (PoE): se usa para entregar alimentación al AP por medio de cable Ethernet, combinando los datos con la alimentación DC, la descripción de PoE se encuentra en el estándar IEEE 802.3af. PoE es útil en áreas donde no se tiene fácil acceso a fuente de potencia, por ejemplo el techo; tiene la ventaja de que el AP se puede colocar cerca de a la antena esto para el caso de uso en exteriores; reduce costos, ya que el cable Ethernet es más barato que el cable coaxial. Para el funcionamiento de PoE primero se usa un módulo para insertar voltaje DC a los cables no usados del cable Ethernet (los pares 4-5 y 7-8), este módulo es conocido como inyector, ya que recibe la señal de datos del concentrador y la señal DC y las combina en el mismo inyector, recibe los datos del *hub* y la potencia DC para combinarlas en el mismo cable; en el otro extremo otro módulo se encarga de dividir los datos para el AP y la alimentación, este módulo es conocido como divisor. El divisor puede estar incorporado en el AP o como un módulo externo. La siguiente figura muestra la conexión de estos módulos, destacando que el divisor es externo.

Figura 55. Uso de PoE.



3.7 PROPAGACIÓN DE LA SEÑAL

Antes de realizar un diseño de una red inalámbrica de área local se necesita entender cómo la señal de radiofrecuencia se propaga por el espacio libre, esto involucra el entendimiento de los fenómenos que afectan la señal entre el transmisor y el receptor. Factores como la reflexión, difracción, dispersión y absorción determinan el rango de operación de una WLAN; estos factores dependen del ambiente circundante: las obstrucciones, el tamaño y forma de estas, las características físicas, etc.. Este ambiente circundante está compuesto de objetos estáticos y objetos móviles que complican aún más la propagación de la señal. En el Anexo C se recopilan algunos resultados de estudios que determinan las propiedades de los materiales más comunes en edificios.

3.7.1 Fenómenos físicos: la propagación de una señal en una WLAN, se ve afectada principalmente por la reflexión, difracción y dispersión. En un ambiente típico de implementación de una WLAN la señal puede recorrer distancias que son relativamente grandes con respecto a la longitud de onda de la señal (12.5 cm para 2.4 GHz y 6 cm para 5 GHz).

3.7.1.1 Reflexión: cuando una señal incide sobre una superficie, puede ser reflejada. La reflexión de una señal depende de las propiedades físicas de la superficie (geometría, grosor, textura y propiedades dieléctricas del material) y de las propiedades de la señal (ángulo de incidencia, amplitud, fase, polarización y frecuencia). La reflexión origina la multitrayectoria, para solucionar este problema se usa la diversidad de espacio. En un ambiente como el interior de un edificio los elementos que contribuyen a la reflexión son las paredes, techos, pisos, muebles y personas.

3.7.1.2 Difracción: la difracción ocurre cuando la señal se encuentra en su recorrido con obstáculos afilados o esquinas. La señal al no poder atravesar este tipo de obstáculos se dobla alrededor del obstáculo, convirtiéndose en un nuevo centro de energía. La difracción también depende de la geometría de la obstrucción y las propiedades de la señal. La difracción en el interior de un edificio puede ocurrir en puertas, esquinas, ventanas, etc..

3.7.1.3 Dispersión: cuando los obstáculos son relativamente pequeños con respecto a la longitud de onda de la señal, la señal experimenta el fenómeno de la dispersión, que consiste en una división de la señal en varias direcciones. Este fenómeno es generalmente producido por superficies rugosas y objetos pequeños. La dispersión puede ocurrir en las ramas de los árboles.

3.7.1.4 Absorción: ocurre cuando la señal RF atraviesa un objeto generándose unas pérdidas que dependen del grosor del objeto y las propiedades del material.

3.7.1.5 Refracción: la refracción ocurre cuando una señal pasa a través de un medio de diferente coeficiente de refracción, este paso hace que la señal se curve en otra dirección. La refracción debe tomarse en consideración para enlaces de larga distancia, a través de la troposfera, sobre todo cuando las condiciones atmosféricas cambian.

3.7.2 Pérdidas de espacio libre: este tipo de pérdidas se obtiene cuando no hay obstáculos entre el transmisor y receptor, las pérdidas de espacio libre están dadas por la siguiente ecuación:

$$L_{FS} = 32.45 + 20 \log f + 20 \log d$$

donde,

f = frecuencia portadora (MHz),

d = distancia entre el receptor y transmisor (Km),

L_{FS} = pérdidas de espacio libre (dB).

3.7.3 Pérdidas en el interior de un edificio: la propagación en el interior de un edificio es difícil de calcular, ya que en pocos casos se tendrán condiciones de línea de vista entre el transmisor y el receptor. La señal en esta clase de ambientes sufre los fenómenos previamente descritos, generando a la propagación una dependencia de los obstáculos y las propiedades que estos tengan. Debido al auge de la telefonía móvil y recientemente de las redes inalámbricas, se han desarrollado modelos para la propagación en el rango de frecuencias de 500 MHz a 5 GHz. Los diferentes modelos se pueden dividir en cuatro grupos: estadísticos, empíricos de trayectoria directa, empíricos de multitrayectoria, rayos ópticos.

3.7.3.1 Modelos estadísticos: estos modelos no necesitan información acerca de las paredes, solo es necesario la información a cerca del tipo de edificio (oficina, hotel, hospital, etc.). El más usado de los modelos de propagación estadísticos es el modelo de espacio libre modificado, el

cual analiza la distancia entre paredes y las pérdidas de penetración de las paredes, pero no se considera la posición de las paredes ni las características de las paredes. Este modelo calcula las pérdidas de propagación de manera similar a las pérdidas de espacio libre con un exponente adaptable y un factor de corrección.

$$l_{MF} = n \cdot 20 \log \frac{4\pi \cdot d}{\lambda} + l_C$$

donde,

l_{MF} = pérdidas del modelo de espacio libre modificado (dB),

n = exponente adaptable,

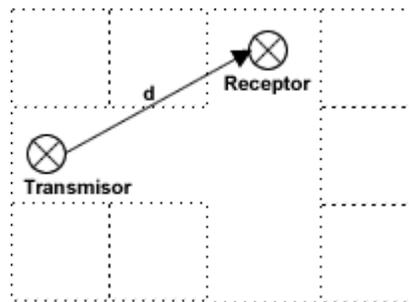
d = distancia entre el receptor y transmisor (m),

λ = longitud de onda (m)

l_C = factor de corrección (dB).

Diferentes tipos de edificios son caracterizados por el parámetro n , para línea de vista su valor va desde 1 a 1.4 y sin línea de vista el valor varía hasta 2.

Figura 56. Modelo de espacio libre modificado.



3.7.3.2 Modelos empíricos de trayectoria directa: estos modelos se basan en la trayectoria directa entre el transmisor y el receptor, no se consideran rayos adicionales. Ejemplos de este tipo de modelo son el modelo de Motley-Keenan y el modelo de multi-paredes.

El modelo de Motley-Keenan usa iguales pérdidas de transmisión para cada pared, las pérdidas de propagación solo se ven influenciadas por el número de paredes y su ubicación exacta. Las pérdidas del modelo se calculan con la siguiente ecuación:

$$l_{MK} = l_{FS} + l_C + k_W l_W$$

donde,

l_{MK} = pérdidas del modelo Motley-Keenan (dB),

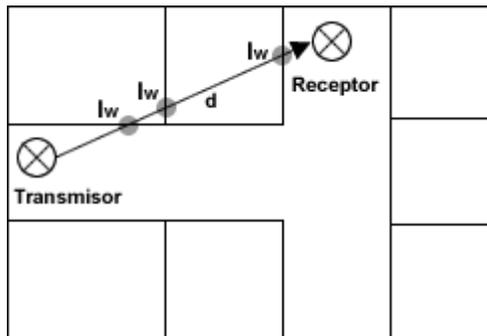
l_{FS} = pérdidas de espacio libre (dB),

l_C = factor de corrección (dB),

k_W = número de paredes cruzadas por el rayo directo entre el transmisor y el receptor,

l_W = pérdidas de penetración, uniforme para todas las paredes (dB).

Figura 57. Modelo Motley-Keenan.



El modelo de multi-paredes considera las pérdidas de cada una de las paredes, ya que tiene en cuenta el material de cada una de las paredes. Ver Anexo C. El modelo multi-paredes adiciona a las pérdidas de espacio libre, las pérdidas introducidas por las paredes atravesadas por el rayo directo entre el transmisor y el receptor, también tiene en cuenta un factor de corrección empírico. La ecuación para calcular las pérdidas de propagación con este modelo es:

$$l_{MW} = l_{FS} + l_C + \sum_{i=1}^N k_{wi} l_{wi} + k_f l_f$$

donde,

l_{MW} = pérdidas del modelo multi-paredes (dB),

l_{FS} = pérdidas de espacio libre (dB),

l_C = factor de corrección (dB),

k_{wi} = número de paredes cruzadas de tipo i ,

k_f = número de pisos cruzados,

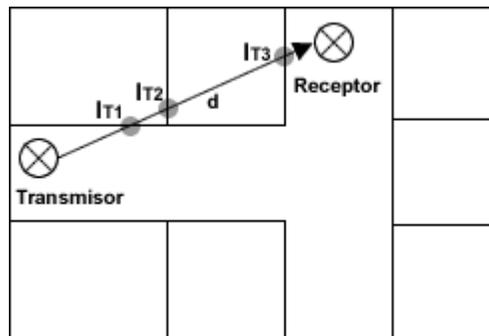
l_{wi} = pérdidas de pared tipo i (dB),

l_f = pérdidas entre pisos adyacentes (dB),

N = número de paredes de diferente tipo.

El factor de corrección normalmente es cercano a cero. La sumatoria representa la suma de las pérdidas totales de las paredes entre el transmisor y el receptor.

Figura 58. Modelo multi-paredes.

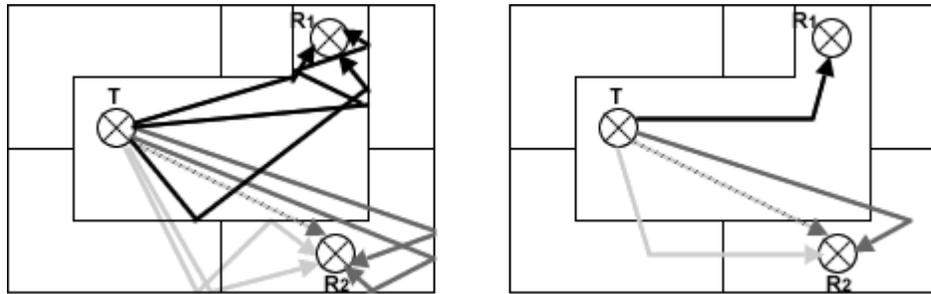


3.7.3.3 Modelos empíricos de multitrectoria: estos modelos se basan en la propagación multitrectoria entre el transmisor y el receptor. Se tienen en cuenta las diferentes trayectorias y sus correspondientes parámetros para el cálculo de la propagación. El más destacado de este tipo de modelos es el modelo de trayectorias dominantes.

El modelo de trayectorias dominantes se basa en las trayectorias entre el transmisor y el receptor, pero no en todas, sino en las más representativas ver figura 59. Solo es necesario conocer cuales habitaciones son atravesadas por los rayos y como estos van pasando de habitación en habitación por trayectorias diferentes, para al final alcanzar el receptor. Con esto se obtiene un árbol de habitaciones.

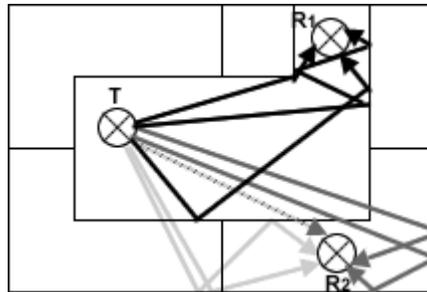
Este modelo no tiene en cuenta la posición exacta de las paredes para el cálculo de la propagación, lo importante para calcular la propagación es la información acerca de la habitación y la influencia de las habitaciones vecinas.

Figura 59. Modelo de trayectorias dominantes.



3.7.3.4 Modelos de rayos ópticos: asumiendo que las longitudes de onda son más pequeñas que los obstáculos, las ondas electromagnéticas pueden ser aproximadas a rayos ópticos, estos modelos consideran reflexiones en las paredes y difracciones en las esquinas. Los modelos de rayos ópticos pueden calcular el retardo y la magnitud de la señal. Su principal desventaja es la dependencia de la exactitud de las propiedades de los materiales y la ubicación de las paredes. Los modelos más representativos son el trazado de rayos y el lanzamiento de rayos.

Figura 60. Modelo de rayos ópticos.



El modelo de trazado de rayos es un algoritmo punto a punto que busca trayectorias de rayos entre el transmisor y receptor. Para el cálculo del cubrimiento se mueve el receptor por el área sobre la que se desea hacer el cálculo.

En el modelo de lanzamiento de rayos es un algoritmo orientado a área, los rayos son transmitidos desde el transmisor en todas las direcciones relevantes y viajan hasta que encuentran un obstáculo, después se reflejan, se difractan o se dispersan. La magnitud de la señal se obtiene de la suma de la contribución de todos los rayos que llegan a un punto.

4. MODELO PARA EL DISEÑO DE UNA RED DE AREA LOCAL INALÁMBRICA

Con el fin de definir el modelo a seguir para llevar a cabo el diseño de una red de área local inalámbrica, se tuvieron en cuenta los pasos que en general se siguen para el diseño de un sistema de comunicaciones, que finalmente después de un análisis concienzudo y teniendo en cuenta las características del sistema a diseñar se creó el modelo para el diseño de una red de área local inalámbrica. Siguiendo los pasos descritos en el modelo se puede realizar el diseño de una red inalámbrica en cualquier tipo de escenario.

El diseño de redes inalámbricas de área local es más complejo que el de redes cableadas, debido a que la propagación y por ende el comportamiento de la señal en el espacio libre se basa en métodos probabilísticos, a diferencia de una red cableada donde la señal solo viaja por el cable. Cada edificación tiene diferentes características y por consiguiente diferentes comportamientos de la señal de radio.

Los siguientes son pasos a tener en cuenta en el diseño de una red inalámbrica:

- Estudio preliminar: consiste en la recopilación de información a cerca de las instalaciones y las redes existentes.
- Capacidad: se debe tener en cuenta para el manejo y administración del ancho de banda, el número de usuarios y las aplicaciones acorde con sus necesidades y requerimientos.
- Cobertura: este paso determina el área de cobertura donde se desea proporcionar conectividad inalámbrica, finalizando con una escogencia de la ubicación de los equipos, la orientación de la antena, la potencia del AP, el patrón de radiación de las antenas, frecuencia.
- Asignación de canales: después de determinar los AP necesarios se procede a la asignación de canales, esto depende de la tecnología 802.11 escogida.
- Estudio de sitio: es uno de los pasos más importantes para la implementación de la red, ya que se verifica en la práctica si lo pasos anteriores están correctos.
- Seguridad: se hace el análisis de requerimientos de seguridad de la red, se crean políticas de seguridad y se decide acerca del mecanismo de seguridad a usar.
- Documentación: es el resultado final del diseño, en la documentación se plasman los resultados de los pasos anteriores.

- Problemas: para el eficiente funcionamiento de una WLAN es necesario configurar los AP teniendo en cuenta el canal de operación, nivel de fragmentación, nivel RTS/CTS, velocidad de datos, etc..

4.1 ESTUDIO PRELIMINAR

En este paso se determinan los requerimientos de la empresa o del cliente. Consiste en recoger información acerca de las instalaciones, las redes existentes, los usuarios, el ancho de banda usado por ellos, aplicaciones, detección de fuentes de interferencia, lo anterior como requisito para el estudio de cobertura, capacidad, seguridad y calidad de servicio.

4.1.1 Análisis del entorno: se considera lo correspondiente al ambiente donde se desea instalar la red inalámbrica (casa, campus, empresa, bodegas, hospital, aeropuerto, etc.); si es para interconexión de usuarios o de edificios; interconexión interna o externa, porque de estos depende el fenómeno de propagación de la señal, tal como se anotó en el capítulo anterior. Si el ambiente es interno, es importante conseguir los planos donde se muestra el tamaño, materiales, habitaciones, corredores, etc., en caso de que los planos no existan es de vital importancia crearlos. Si el ambiente es externo se debe tener en cuenta árboles, montañas, y cualquier otro tipo de obstrucción. En este análisis también se consideran las características meteorológicas como el calor, la lluvia, el frío, el viento, la humedad, la luz del sol, el polvo, los cambios de temperatura, y demás. En caso de que se requieran torres para enlaces punto a punto, se debe verificar la estructura donde se va a ubicar, la cual debe ser resistente.

4.1.2 Redes existentes: se comprueba si existe una red cableada o inalámbrica dentro de la cobertura, en caso donde exista una red cableada se necesita conocer el diagrama topológico de la red, la ubicación de los armarios, la ubicación de los puntos de red, los tomas eléctricos, la tecnología que actualmente esta siendo usada, capacidad, etc.; en caso de que sea una red inalámbrica es necesario obtener la ubicación de los equipos, la tecnología usada, cobertura, capacidad, etc.. En ambos casos se debe verificar si existe alguna convención para nombrar los dispositivos de la infraestructura como enrutadores, *switches*, APs, concentradores, repetidores, puentes inalámbricos, *gateways*, entre otros. Otro punto importante a tener en cuenta, es la existencia de puertos disponibles en los *switches* y concentradores, cuando los APs se conectan a la red cableada. Se debe determinar si la red es privada o pública para la asignación de direcciones IP.

4.1.3 Análisis de la interferencia: las redes inalámbricas trabajan en una banda libre por lo tanto debe compartir el espectro con otras redes, el Ministerio de Comunicaciones da prioridad a las estaciones de servicio primario determinadas en el cuadro nacional de atribución de bandas de frecuencias*. También se hace una consulta acerca de la existencia de redes inalámbricas exteriores cercanas que puedan causar interferencia con la red que se está diseñando, por ejemplo redes bluetooth, redes HomeRF u otras redes 802.11 y la existencia de equipos médicos, teléfonos inalámbricos, hornos microondas, que también trabajan en la banda de 2.4 GHz. HyperLAN que opera en la banda de 5 GHz.

4.1.4 Tipo de equipos cliente: se determina el tipo de equipo que van a usar los clientes de la red inalámbrica, estos pueden ser computadores portátiles, computadores de escritorio, PDA, teléfonos VoIP, servidores de impresión, cámaras, proyectores, etc., ya que el equipo cliente determina el tipo de aplicaciones y por lo tanto el ancho de banda.

4.2 CAPACIDAD

En este paso se determinan los factores que influyen directamente en la capacidad del sistema.

4.2.1 Tecnología: debido a que 802.11a y 802.11g soportan hasta 54 Mbps con un rendimiento efectivo aproximado de 33 Mbps y 802.11b hasta 11 Mbps con un rendimiento efectivo aproximado de 5.5 Mbps, la elección de la tecnología es un factor importante para determinar la capacidad máxima de la red.

4.2.2 Cambio de velocidades: se debe tener en cuenta que las velocidades disminuyen a medida que aumenta la distancia, esto es debido a la relación señal a ruido (S/N Signal Noise), que determina la velocidad a la cual el cliente puede asociarse, por ejemplo los clientes cerca al AP se asocian a velocidades más altas que los clientes más lejanos. Los cambios de velocidad dependen de la sensibilidad de receptor, que consiste en un umbral mínimo de energía recibida para el que la señal alcance una cierta velocidad. Si la energía de la señal es más baja que la velocidad máxima alcanzable será decrementada o se decrementará el desempeño.

4.2.3 Ancho de banda por usuario: un AP puede soportar cierta cantidad de usuarios dependiendo de las características del fabricante y de las aplicaciones que los clientes están usando. El desempeño de la red inalámbrica se degrada a medida que el tráfico aumenta, por lo

* Ministerio de Comunicaciones. Cuadro nacional de atribución de bandas de frecuencia. Bogotá. 2001. Disponible en: <http://www.mincomunicaciones.gov.co/Archivos/Sectorial/CuadroAtribucion.pdf>

tanto se recomienda colocar más APs dentro de la misma área para disminuir la carga. Dependiendo del tipo de usuarios, el requerimiento en capacidad cambia, si se pretende hacer el diseño de una red inalámbrica en un almacén para ser usada por escáneres de código de barra, el ancho de banda por usuario es muy poco y serían suficientes 25 Kbps, por lo que se alcanza 200 usuarios cuando se asocian a 11 Mbps y máximo 20 usuarios cuando la velocidad es de 1 Mbps. Para una red universitaria, donde el protocolo más usado es HTTP, un ancho de banda de 300 Kbps por usuario es aceptable, por lo que se alcanzan 17 usuarios cuando se asocian a 11 Mbps. Si se necesita llegar a más usuarios se debe aumentar el número de APs dentro la misma área. Cuando se trata de usuarios que usan la red para transferencia de archivos grandes o aplicaciones que requieren mucho ancho de banda tales como transferencia de imágenes médicas, archivos CAD, etc., son suficientes 500 Kbps por usuario, con lo cual se pueden tener cerca de 50 usuarios asociados a una velocidad de 54 Mbps. Si el requerimiento de los usuarios es para la visualización de video de alta calidad en tiempo real se puede necesitar hasta 2000 Kbps, con lo que se alcanzaría a tener 3 usuarios simultáneos asociados a 11 Mbps o alrededor de 14 si se asocian a 54 Mbps. Si se necesita que la red soporte aplicaciones de voz sobre WLAN (VoWLAN Voice over WLAN), el número de usuarios simultáneos depende del esquema de codificación y de-codificación usado, si se usa G.711 con una velocidad de 128 Kbps para una comunicación direccional con requerimientos de 200 pps (packets per second), se pueden tener aproximadamente 6 comunicaciones de voz simultáneas asociadas a 11 Mbps y hasta 25 si hay asociación a 54 Mbps.

4.3 COBERTURA

Se determina el área que debe ser cubierta por la red inalámbrica, la ubicación de los equipos, la orientación de la antena, la potencia del AP, el patrón de radiación de las antenas, son factores que inciden en el diseño para lograr el buen cubrimiento, funcionamiento eficiente y ahorro de costos de la red.

4.3.1 Área de cobertura: en este paso se determina cual es el área donde se requiere cobertura inalámbrica, el área está determinada por aquellos lugares donde no existe conectividad a la red o se quiere aumentar conectividad o si es el caso, reemplazar la infraestructura de red actual. El área puede ser todo o una parte del entorno definido en el análisis preliminar.

4.3.2 Patrón de radiación de la antena: la mayoría de los APs tiene una antena omnidireccional, mientras que otros tiene la opción de conectar una antena externa, con lo cual se puede tener el patrón de radiación deseado. Dependiendo de las características del ambiente, algunas antenas pueden ser más útiles que otras, por ejemplo en el caso donde se tiene un corredor se podría

colocar un AP con una antena direccional, para interconexión entre edificios se usan antenas direccionales de alta ganancia y en amplios salones se usan las antenas omnidireccionales.

4.3.3 Montaje de APs y de antenas: lo mejor a la hora de hacer el montaje del AP y su antena es que se ubiquen lo más cerca, con el fin de disminuir pérdidas. Un AP puede ser montado sobre una superficie o colocado en la pared, pero cuando se desea protegerlo del robo, de la manipulación o del clima se debe considerar el uso de carcasas. En el mercado existen varias opciones algunas de ellas hacen menos visible la ubicación de los APs y agradable estéticamente, ya que se ubica en el techo. Otras carcasas están diseñadas para ser resistentes a los cambios climáticos, pueden ser usadas tanto en ambientes internos, como en ambientes externos. El material de la carcasa puede ser aluminio, fibra de vidrio reforzado con poliéster, policarbonato, entre otros. El montaje de la antena también depende de su uso, si está orientado a ambientes externos o a ambientes internos. El montaje de la antena debe ser suficientemente sólido para evitar accidentes y el balanceo de la antena, ya que esto produce el movimiento de la celda. Una antena puede montarse en el techo, en la pared, en las columnas, en el piso o en un mástil.

4.3.4 Frecuencia: ya que las diferentes tecnologías operan en diferentes bandas, 802.11b y 802.11g en 2.4 GHz y 802.11a en 5 GHz; la cobertura está determinada por la tecnología que se elija. A mayor frecuencia mayor atenuación por lo tanto menor cubrimiento, así, el cubrimiento de los equipos que trabajan en la banda de 5 GHz es la mitad del cubrimiento de los equipo que trabajan en la banda de 2.4 GHz.

4.3.5 Ubicación de los APs y sus antenas: es un factor importante para determinar el área de cobertura; si el AP se conecta a la red cableada, se debe tener en cuenta los límites de distancia entre el AP y el armario, el cual depende del tipo de cable usado por sus características de atenuación con respecto a la longitud. También es necesario tener en cuenta que el AP necesita alimentación AC, en caso de no existir una fuente AC cerca, se debe considerar el uso de dispositivos que soporten potencia DC sobre cables Ethernet CAT-5. La ubicación también depende del patrón de radiación de la antena, por ejemplo si se tiene una antena omnidireccional, en auditorios o salones de conferencia se ubica en el centro, mientras sea posible. La ubicación de las antenas debe ser lo más alto posible con el fin de aumentar el área de cubrimiento. Si el requerimiento es interconectar edificios, la ubicación de las antenas debe ser lo suficientemente alta para liberar la zona Fresnel y hacer que los árboles y otros edificios no obstaculicen la señal. Las antenas ubicadas en los exteriores de la edificación deben estar protegidas contra el calor y frío extremo.

Una asignación apropiada para el análisis de cobertura de un AP con una antena omnidireccional es aproximar las áreas de cobertura a circunferencias de radio R las cuales deben ser ubicadas de tal forma que no existan huecos de cubrimiento y evitar al máximo las superposiciones de áreas de cubrimiento, ya que incrementa los costos.

Los APs pueden ser ubicados en un edificio dentro de un arreglo que puede ser lineal (Figura 61) o rectangular (Figura 62) para cada uno de los pisos, estos arreglos se usan en casos donde se tiene baja densidad de usuarios. Un arreglo lineal de AP se usa cuando el ancho del edificio es menor que el radio del área de cobertura y el arreglo rectangular se usa cuando el ancho del edificio es relativamente grande respecto a R .

En áreas con alta densidad de usuarios, se opta por un arreglo puntual donde se colocan varios APs que cubran la misma área, obviamente configurados en diferentes canales, este arreglo es mostrado en la figura 63. Sin embargo, dentro de una edificación no todas las áreas tienen la misma densidad de usuario de modo que se pueden combinar los arreglos para lograr el mejor rendimiento de la red.

Figura 61. Arreglo lineal de APs.

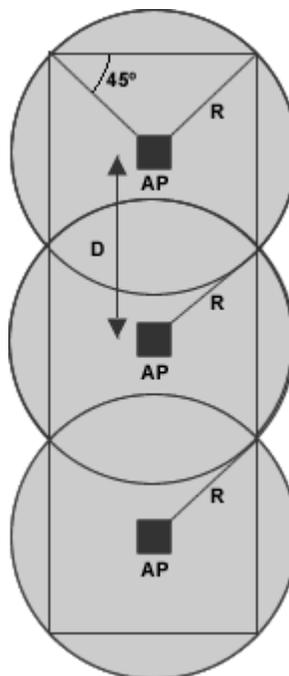


Figura 62. Arreglo rectangular de APs.

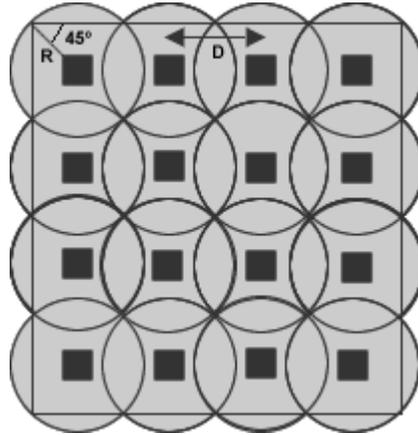
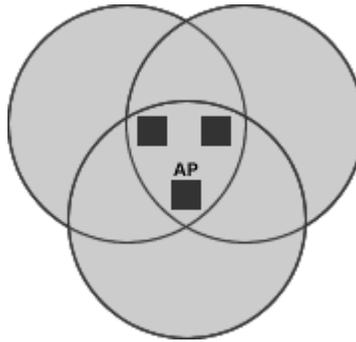


Figura 63. Arreglo puntual de APs.



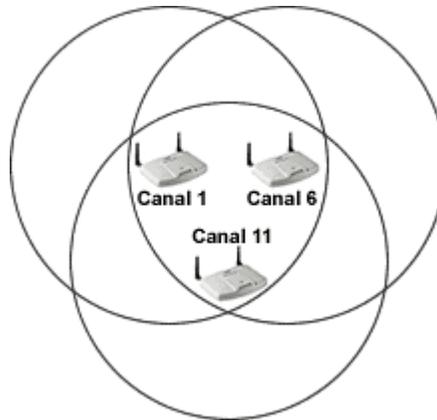
4.3.6 Potencia de los APs: el tamaño de una celda está determinado por la potencia de transmisión y la sensibilidad del receptor, a un nivel de potencia alto se tienen grandes tamaños de celdas y a niveles de potencia bajos se tienen pequeñas celdas. A veces las celdas pequeñas son mejores ya que reducen la interferencia con los APs vecinos, empleando la reutilización de canales y es importante que la cobertura no pase los límites de la instalación. Muchos AP tienen la opción de modificar la potencia y en caso de que no se tenga esta opción es necesario recurrir a atenuadores, amplificadores, cables, etc., referenciados en el capítulo anterior. Las potencias de los APs en mW pueden ser 1, 2, 5, 10, 20, 32, 40, 50, 64, 100, 200, 500, 1000.

4.4 ASIGNACIÓN DE CANALES

La asignación de canales sirve para proporcionar mayor ancho de banda alcanzando un mayor rendimiento de la red en beneficio a los usuarios inalámbricos de un área determinada. En Colombia, en el espectro de frecuencias asignado está entre 2.4000 a 2.4835 GHz, si se usa DSSS, los canales asignados son 13 con un ancho de banda de 22 Mhz de ancho, de acuerdo a la

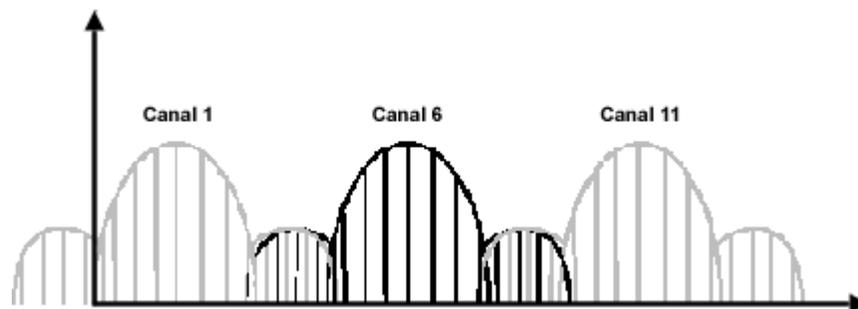
frecuencia central y al ancho por canal solamente tres no se superponen. Para evitar superposición entre canales las frecuencias centrales deben estar separadas mínimo 25 MHz. El mayor número de AP que se pueden ubicar dentro de la misma área física usando equipos bajo las normas 802.11b y 802.11g es de tres, estos son los canales 1, 6 y 11 o los canales 2, 7 y 12 o 3, 8 y 13. Ver figura 64.

Figura 64. Canales no superpuestos en arreglo puntual.



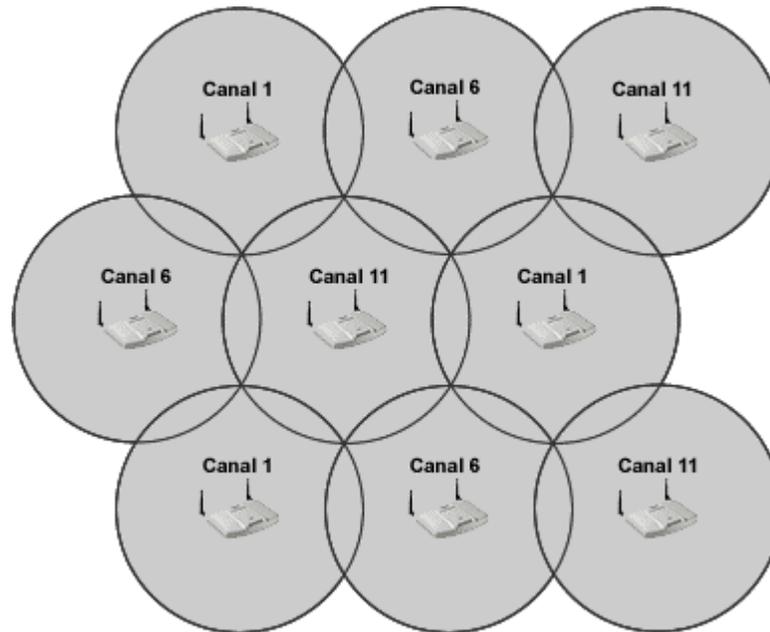
Teóricamente permite la ubicación de tres APs cercanos en los tres canales no superpuestos, experimentando un rendimiento de 4.5 a 5.5 Mbps para 802.11b y de 33 a 36 Mbps en 802.11a y 802.11g, esto es debido a la naturaleza *half duplex* de los radio RF y al encabezado de las normas WLAN. Sin embargo, en los canales que se encuentran separados 25 MHz, en la práctica tienen superposición parcial, debido a que se usan las mismas potencias para transmitir, que aunque es de poca magnitud, no se deben ubicar cercanas. En este caso el rendimiento de los APs puede caer hasta los 4 Mbps o menos en 802.11b y hasta los 30 Mbps en 802.11a y 802.11g. Ver figura 65.

Figura 65. Canales DSSS.



En situaciones donde se necesita *roaming*, se pueden reusar los canales para cubrir toda el área, esta técnica se muestra en la figura 66.

Figura 66. Reuso de canales en la banda de 2.4 GHz.



Las bandas asignadas en Colombia en el espectro de frecuencia de los 5 GHz para 802.11a, son las bandas de 5.150 a 5.250 GHz, de 5.250 a 5.350 GHz y de 5.725 a 5.850. Los números de canales de operación válidos son 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157 y 161. Entre las bandas más bajas y las medias se tienen ocho canales y cuatro en las bandas más altas.

En la figura 67 se muestra el reuso usando las bandas más bajas. En la figura 68 se puede ver el reuso de usando las bandas medias y bajas. La asignación de canales se debe hacer primero para las áreas con mayor densidad de usuarios y luego para las de baja densidad. No se muestra el reuso de canales para las bandas más altas, ya que esta banda se utiliza para enlaces punto a punto.

Figura 67. Reuso de canales en 5 GHz con las bandas más bajas.

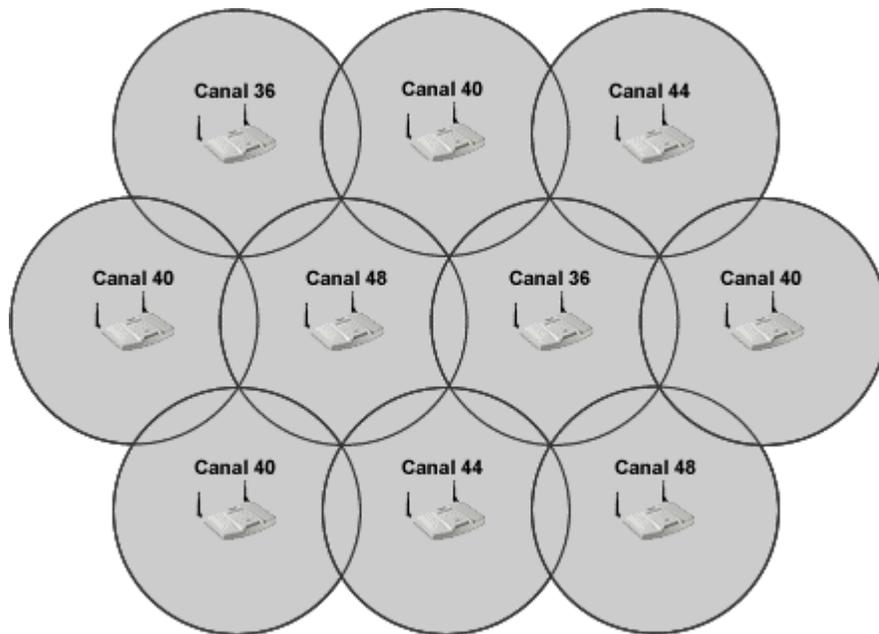
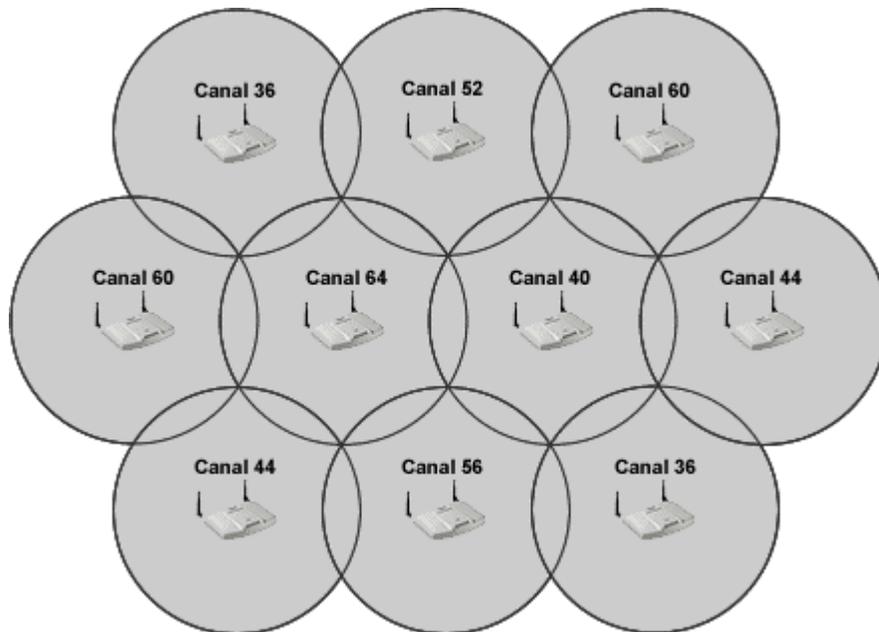


Figura 68. Reuso de canales en 5 GHz con las bandas más bajas y medias.



4.5 ESTUDIO DEL SITIO

Es el estudio teórico de compatibilidad y desempeño electromagnéticos a nivel de RF en el espacio libre, en la práctica se validan los resultados de las medidas con los obtenidos en los pasos anteriores, asegurando de esta manera el cubrimiento a todos los clientes en las áreas necesarias y por consiguiente validando el diseño. Antes de llevar a cabo este paso se requiere la siguiente información:

- Planos del edificio.
- Documentación de estudios del sitio anteriores, si existen.
- Diagrama topológico de la red actual.
- Requisitos de cobertura, capacidad y seguridad.
- Futuros planes de construcción.

Para apoyar el estudio práctico del sitio se requiere de por lo menos un AP, antenas, cables, conectores, un computador portátil o PDA con un dispositivo cliente, baterías, atenuadores y software utilitario. Este estudio consiste en recorrer las instalaciones para verificar la información acerca de los planos, tomacorrientes, puntos de conectividad a la red cableada, obstrucciones RF, fuentes de interferencia, condiciones meteorológicas, distancias de enlaces, etc..

Para medir la cobertura y capacidad de la red inalámbrica diseñada, se ubican los APs en todos los sitios determinados, luego alrededor de los APs se toman medidas como velocidad de datos, magnitud de la señal, relación señal a ruido, frecuencia de operación, posibles interferencias.

En caso de no contar con el equipo para el estudio de sitio se puede recurrir a herramientas de predicción, las cuales usan los modelos de propagación vistos en el capítulo 3. Estas herramientas, se basan en planos hechos en un programa de diseño asistido por computador (CAD), por ejemplo *AutoCAD* y *Visio*®. Las herramientas de predicción de propagación más destacadas son: *WinProp*, *LANPlanner*® y *CINDOOR*®.

4.6 SEGURIDAD

El tema de la seguridad en redes inalámbricas es muy importante para evitar los intrusos, de nada sirve realizar el estudio de cobertura, de capacidad y el uso de tecnología de punta sino se implantan políticas y mecanismos de seguridad a toda la red, ya que una red inalámbrica es tan segura como su enlace más débil. Para saber que nivel de seguridad es necesario consultar al

cliente acerca de los requerimientos, los cuales dependen de la sensibilidad de los datos que pueden ser transmitidos a través de la red inalámbrica. Esto último determina la solución de seguridad que debe ser implementada. A continuación se nombran algunas soluciones de seguridad para las WLAN, desde la que ofrece menos seguridad hasta la que ofrece mayor seguridad:

- WEP.
- Filtrado de direcciones MAC.
- VPN.
- 802.1x con servidor RADIUS.
- WPA.
- 802.11i.
- Combinación entre las anteriores.

No se deben pasar por alto las políticas de seguridad existentes, estas incluyen un conjunto de reglas donde se restringe el uso de la red, en caso de no existir, se crean; las políticas de seguridad son:

- Inhabilitar DHCP para la red inalámbrica, por lo tanto las direcciones IP de los clientes deben ser fijas.
- Mantener actualizado el *firmware* de los APs.
- Los APs deben estar ubicados en sitios seguros para evitar el robo.
- Los APs debe ser desactivados en periodos de inactividad, o deshabilitar aplicaciones cuando sea necesario.
- Cambiar el SSID por defecto de los APs y deshabilitar la difusión del SSID.
- Reducir la propagación de las ondas de radio fuera del campus.
- Ubicar los APs lejos de la frontera del campus.
- Evitar el uso de APs no autorizados.
- Configurar los equipos con la máxima seguridad posible.
- Definir perfiles de usuarios.
- Usar aplicaciones software y hardware para monitorear en tiempo real la red inalámbrica y el uso del espectro evitando las posibles interferencias de modo que se tomen decisiones inmediatas y acordes con el problema.
- Usar aplicaciones de detección de intrusos
- Planear futuras mejoras en cuanto a seguridad.

4.7 DOCUMENTACION

Es importante que todos los pasos anteriores sean bien documentados, desde el estudio preliminar hasta el estudio del sitio. Esta documentación puede variar de acuerdo a las necesidades del cliente. Si la documentación es inexacta, la implementación no trabajará como es debido. Lo importante es adjuntar todos los datos recogidos ya que pueden ser necesarios para futuras referencias.

La documentación debe incluir la información completa del cliente o su representante, sus necesidades, sus requerimientos y como estos son afrontados con el diseño, se presentan mapas, bosquejos, donde se muestran las áreas de cobertura, las velocidades, sitios más densos, los huecos de cobertura, ubicación, frecuencias, potencias, nombres, y canales de los APs, tipos de antenas, montajes, interferencias, equipos utilizados y sus características, problemas, seguridad, comportamiento de la red en las horas pico.

A continuación se presentan un modelo de formato para que el diseñador recolecte toda la información necesaria para el diseño y la implementación de la red inalámbrica.

Datos del cliente

Nombre del cliente: _____

Representante: _____

Dirección: _____

Teléfono: _____

Teléfono celular: _____

Fax: _____

Correo electrónico: _____

Entrevista: En persona Telefónica
 Por correo Mensajería instantánea

Información sobre redes inalámbricas existentes

Existe algún estudio del sitio anterior?

- Si No

Si existe la documentación, está disponible para el diseñador?

- Si No

Existe algún equipo WLAN en el lugar?

- 802.11 802.11b
 802.11a 802.11g
 Otro: _____

Cuántos usuarios tiene la WLAN? _____

Hay horas pico en la WLAN?

- Si No

Horas pico desde _____ hasta _____ . Cuantos usuarios? _____

Hay horas no pico en la WLAN?

- Si No

Horas no pico desde _____ hasta _____ .

Cuántos APs hay en el lugar y que referencias?

Hay convenios con fabricantes?

- Si No

Hay APs desempeñando balance de carga?

- Si No

Qué clase de soluciones de seguridad hay en el sitio?

- Ninguna WEP
 EAP EAP – TLS
 EAP – TTLS PEAP
 VPN RADIUS
 WPA 802.1x
 802.11i Firewall

Otra: _____

Hay otras organizaciones cercanas usando WLAN?

- Si No

Hay fuentes de interferencia?

- Si No

Fuente 1: _____

Fuente 2: _____

Fuente 3: _____

Fuente 4: _____

Hay huecos de cubrimiento?

- Si No

Adjuntar mapas donde se muestre las ubicaciones de los AP, fuentes de interferencia, huecos de cobertura.

Diseño

Tipo de ambiente

- Interior Exterior

Si es interior, que clase es?

- Hospital Almacén Oficina
 Residencial Fábrica Campus Universitario

Otro: _____

Si es exterior, que clase de conexión es? Y cuál es la distancia?

- Punto – punto : _____
 Punto – multipunto: _____

Hay planos de las instalaciones?

- Si No

Hay mapas topológicos de la red actual?

- Si No

Qué tipo de aplicaciones serán usadas en la WLAN?

- Voz Video FTP
 HTTP Telnet SSH
 POP/SMTP Acceso a base de datos Mensajería instantánea
Otros _____

Qué tipo de equipos cliente serán usados?

- Computadores portátiles Computadores de escritorio
 PDAs Otros: _____

Cuántos clientes usarán la red inalámbrica? _____

Tipo de red cableada existente:

- Cable coaxial Thinnet Cable coaxial Thicknet
 Par trenzado sin blindaje (UTP) Par trenzado con blindaje (STP)
 Fibra óptica Otro: _____

Por medio de que dispositivo los APs se conectan?

- Switches Concentradores

Hay suficientes puertos para acomodar los APs?

- Sí No

Qué tipo de fuente de potencia usan los APs?

- AC PoE

Qué subred será asignada a la WLAN?

- Privada Pública

Cómo será gestionada la red?

- SNMP HTTP / HTTPS
 Telnet Consola
 Aplicación propietaria

Otras: _____

Qué tipo de tecnología es la más adecuada para las instalaciones?

- 802.11 802.11b
 802.11a 802.11g

Otra: _____

Qué clase de seguridad es la más adecuada?

- Ninguna WEP
 EAP EAP – TLS
 EAP – TTLS PEAP
 VPN RADIUS
 WPA 802.1x
 TKIP Firewall
 802.11i Otra: _____

Información sobre el AP

Nombre del AP: _____

Referencia: _____

Ubicación del AP: _____

Dirección IP: _____

Canal:

- 1 2 3 4 5 6 7 8 9
 10 11 12 13 36 40 44 48 52
 56 60 64 149 153 157 161

Modo de operación del AP:

- Modo raíz Modo no raíz Modo repetidor

Tipo de AP instalado

- 802.11 802.11b
 802.11a 802.11g

Otra: _____

Tipo de conexión a la red existente

- Concentrador 10baseTx Concentrador 100baseTx
 Switch 10baseTx *Switch* 100baseTx
 Switch 10/100baseTx *Switch* 10/100baseFx
 Switch 10/100/1000baseTx Otro: _____

Información del Switch / concentrador al cual el AP está conectado

Referencia / marca: _____

Dirección IP: _____

Nombre / ubicación: _____

Número de puerto: _____

Velocidad de datos

- | | | | |
|----------------------------------|----------------------------------|-----------------------------------|----------------------------------|
| <input type="checkbox"/> 1 Mbps | <input type="checkbox"/> 2 Mbps | <input type="checkbox"/> 5.5 Mbps | <input type="checkbox"/> 11 Mbps |
| <input type="checkbox"/> 6 Mbps | <input type="checkbox"/> 9 Mbps | <input type="checkbox"/> 12 Mbps | <input type="checkbox"/> 18 Mbps |
| <input type="checkbox"/> 24 Mbps | <input type="checkbox"/> 36 Mbps | <input type="checkbox"/> 48 Mbps | <input type="checkbox"/> 54 Mbps |

Propietaria: _____

Potencia de salida

- | | | | |
|--------------------------------|---------------------------------|---------------------------------|---------------------------------|
| <input type="checkbox"/> 1 mW | <input type="checkbox"/> 2 mW | <input type="checkbox"/> 5 mW | <input type="checkbox"/> 10 mW |
| <input type="checkbox"/> 20 mW | <input type="checkbox"/> 32 mW | <input type="checkbox"/> 40 mW | <input type="checkbox"/> 50 mW |
| <input type="checkbox"/> 64 mW | <input type="checkbox"/> 100 mW | <input type="checkbox"/> 200 mW | <input type="checkbox"/> 500 mW |
| <input type="checkbox"/> 1 W | Otro: _____ | | |

Información adicional

Tipo de antena y ganancia: _____

Cable *pigtail* : _____

Cable de potencia AC: _____

Inyector PoE: _____

Supresor de transientes: _____

Conectores y cable RF: _____

Tipo de montaje: _____

Puntos de medidas

Punto 1: _____

Señal: _____ Ruido: _____ S/N: _____

Notas: _____

Punto 2: _____

Señal: _____ Ruido: _____ S/N: _____

Notas: _____

Punto 3: _____
Señal: _____ Ruido: _____ S/N: _____
Notas: _____

Punto 4: _____
Señal: _____ Ruido: _____ S/N: _____
Notas: _____

Huecos

Punto 1: _____
Causado por: _____
Sugerencias: _____

Punto 2: _____
Causado por: _____
Sugerencias: _____

Punto 3: _____
Causado por: _____
Sugerencias: _____

Punto 4: _____
Causado por: _____
Sugerencias: _____

Qué clase de soluciones de seguridad hay en el sitio?

- | | |
|-------------------------------------|------------------------------------|
| <input type="checkbox"/> Ninguna | <input type="checkbox"/> WEP |
| <input type="checkbox"/> EAP | <input type="checkbox"/> EAP – TLS |
| <input type="checkbox"/> EAP – TTLS | <input type="checkbox"/> PEAP |
| <input type="checkbox"/> VPN | <input type="checkbox"/> RADIUS |
| <input type="checkbox"/> WPA | <input type="checkbox"/> 802.1x |
| <input type="checkbox"/> TKIP | <input type="checkbox"/> Firewall |
| <input type="checkbox"/> 802.11i | Otra: _____ |

El formulario anterior sirve para los puentes o puente de grupo de trabajo, adicionando la siguiente información:

AP al que se conecta: _____

Cuántos clientes cableados se conectan al puente grupo de trabajo: _____

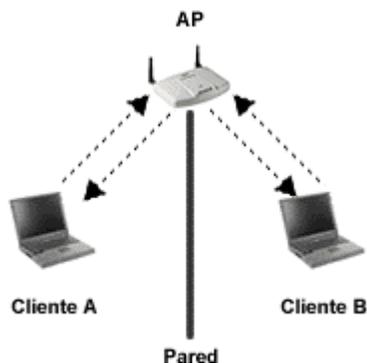
4.8 PROBLEMAS

Existen diferentes problemas presentados en el funcionamiento de las WLAN que reducen el rendimiento de la red, estos problemas son detectados después de la instalación de la red y pueden ser resueltos con una adecuada configuración del AP, para obtener un mejor desempeño.

4.8.1 Solución al desvanecimiento por multitrayectoria: la multitrayectoria puede generar huecos de cubrimiento ya que llegan varias señales en desfase y se cancelan, la solución es la diversidad de espacio, que consiste en el uso de dos o mas antenas conectadas a varias entradas, se selecciona la señal de la antena que fue recibida con mayor magnitud y emplea solamente una antena en cada instante de tiempo, la transmisión se hace por la última antena usada en la recepción, alterna antenas para reintentos y una unidad puede transmitir o recibir pero no realizar las dos al tiempo. La mayoría de los APs usan dos antenas para diversidad de espacio.

4.8.2 Solución al problema del nodo oculto: este problema se presenta cuando un cliente conectado a un AP es incapaz de detectar que otros clientes están transmitiendo, cuando este transmite genera colisiones lo que conlleva a la retransmisión y por lo tanto el rendimiento de la red disminuye. Este problema puede ser generado por un obstáculo o porque la distancia entre los nodos es muy grande. El problema se muestra en la figura 69.

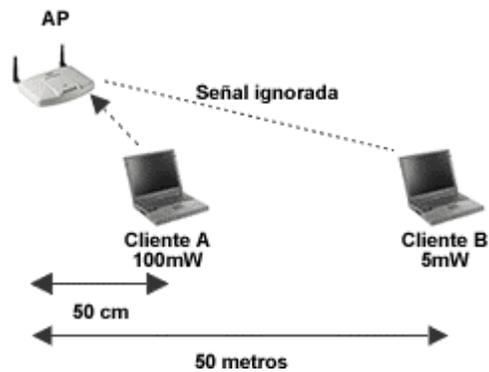
Figura 69. Problema del nodo oculto.



Entre las soluciones a este problema están: el aumento de potencia en los clientes, remover el obstáculo o mover el nodo oculto. El AP al ser configurado para usar RTS/CTS no soluciona totalmente el problema pero reduce el impacto negativo que los nodos ocultos tienen en la red. Ver sección 1.3.1.

4.8.3 Solución de problema cerca/lejos: este problema ocurre cuando varios clientes están asociados a un AP y transmiten con diferentes potencias, se puede dar el caso de que un cliente con baja potencia esté más retirado del AP que uno transmitiendo a alta potencia, por lo que el cliente que se encuentra más retirado no puede ser escuchado por el AP, tal como se muestra en la figura 70.

Figura 70. Problema cerca/lejos.



Para solucionar este problema se debe hacer un buen diseño de la ubicación del AP, aumentar la potencia del cliente lejano o disminuir la potencia de los clientes cercanos.

5. DISEÑO DE LA RED DE AREA LOCAL INALÁMBRICA

En este capítulo se siguen los pasos descritos en el capítulo anterior, para lo cual se ha hecho el correspondiente estudio preliminar y se han tomado en consideración específicamente capacidad, áreas de cobertura, asignación de canales, estudio del sitio, seguridad y documentación, obviando los tipos de equipos cliente ya que esto depende de la Universidad y de la comunidad académica, potenciales usuarios de la Red.

5.1 ESTUDIO PRELIMINAR

5.1.1 Análisis del entorno: el diseño de la red inalámbrica tiene cobertura para el Campus de Ingenierías de la Universidad del Cauca compuesto por el edificio de Ingenierías, el edificio de Postgrados de Ingenierías y el parque de Ingenierías. La red está configurada para la interconexión de usuarios y la ubicación de los usuarios tanto en el interior del edificio como en el exterior del edificio. Los planos de el edificio de Ingenierías y el edificio de Postgrados de Ingenierías estaban hechos a mano en el año de 1984; para pasarlos a una versión digital y actualizada de ellos, se recurrió a la utilización de la herramienta software AutoCAD versión 2002. En las siguientes figuras se muestran los planos de los diferentes pisos con sus respectivas dimensiones y ubicación de los salones, salas, etc., que componen el Campus de Ingenierías.

Figura 71. Edificio de Ingenierías - Planta semisótano.

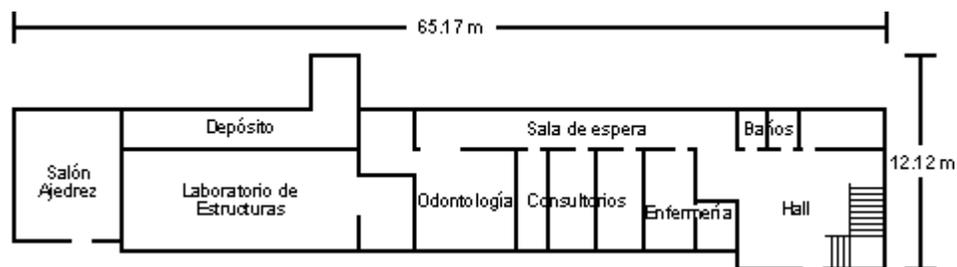


Figura 72. Edificio de Ingenierías - Planta primer piso.

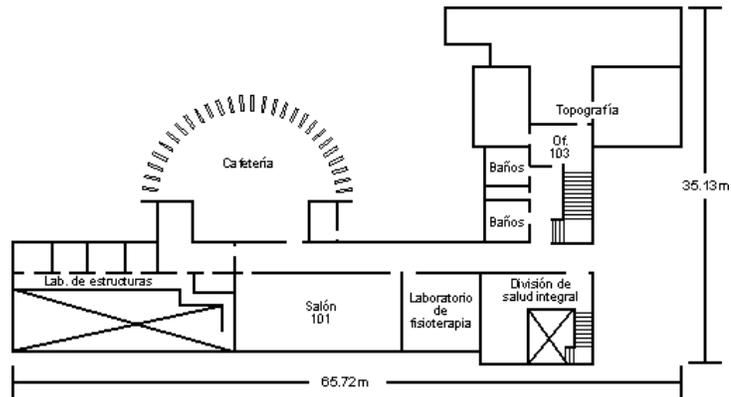


Figura 73. Edificio de Ingenierías - Planta segundo piso.

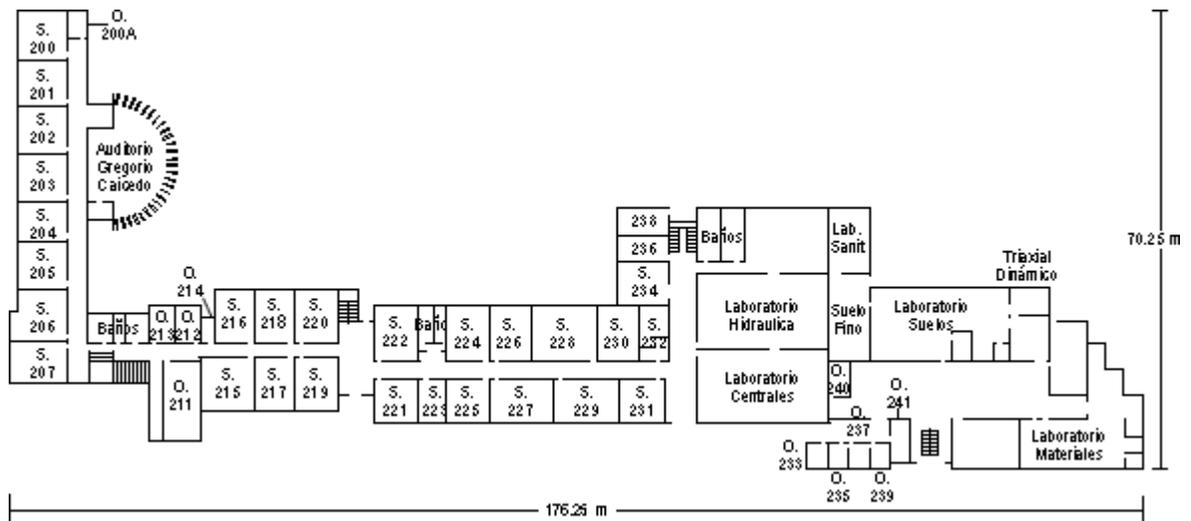


Figura 74. Edificio de Ingenierías - Planta tercer piso.

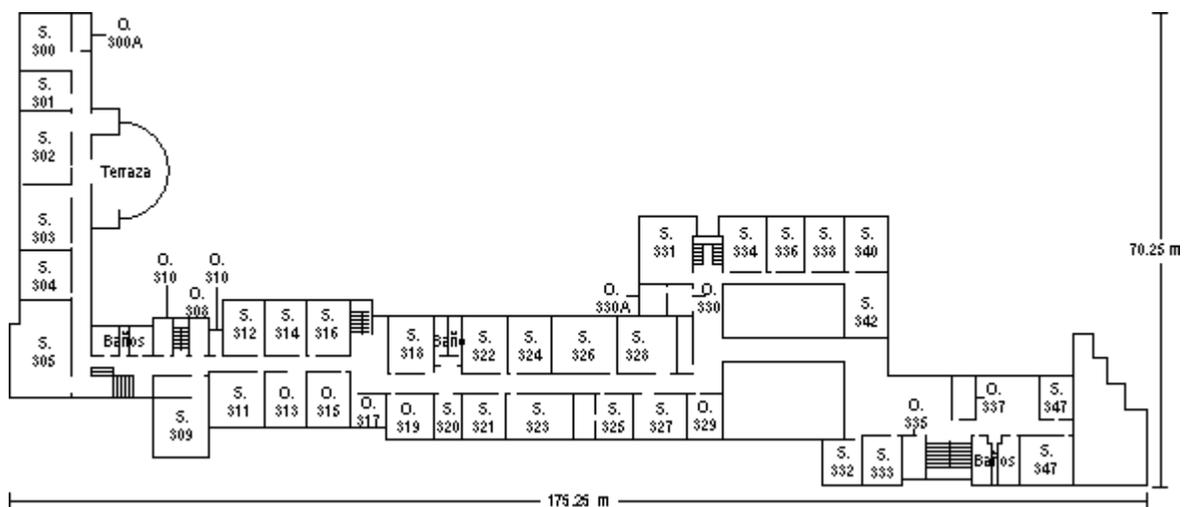


Figura 75. Edificio de Ingenierías - Planta cuarto piso.

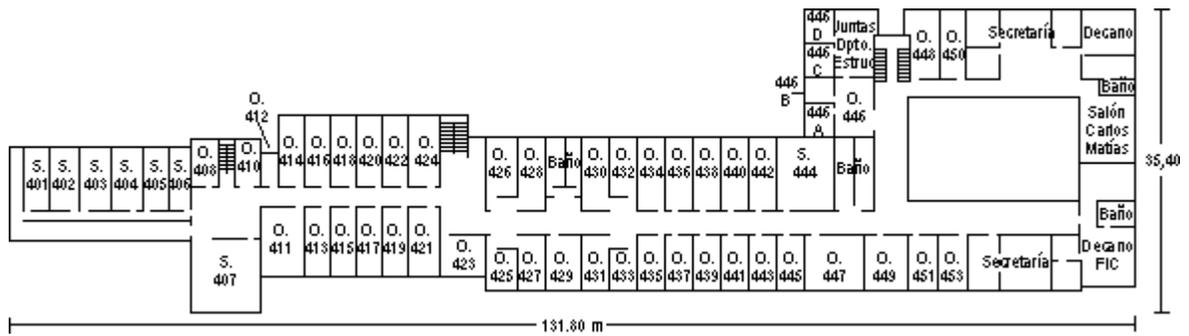
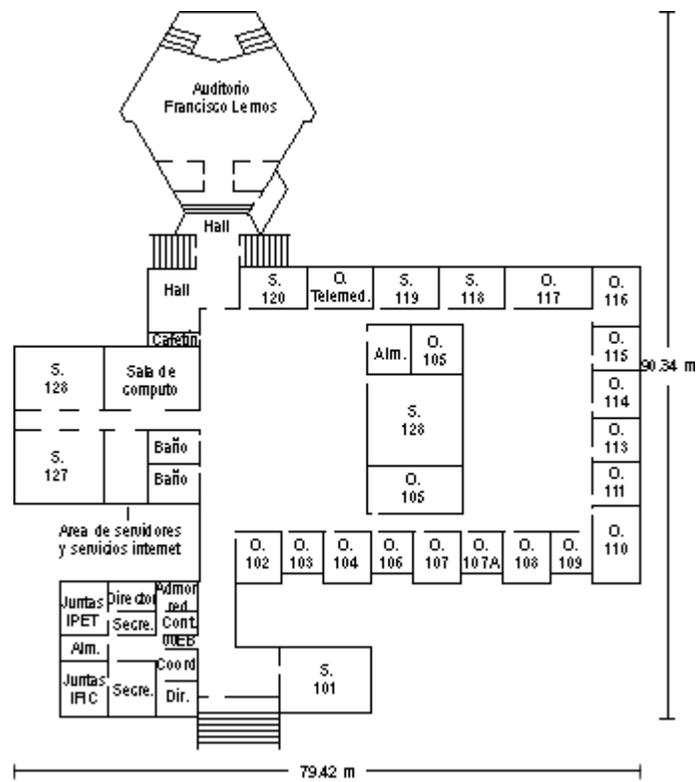


Figura 76. Edificio de Postgrados - Planta primer piso.



Los materiales que constituyen el edificio son:

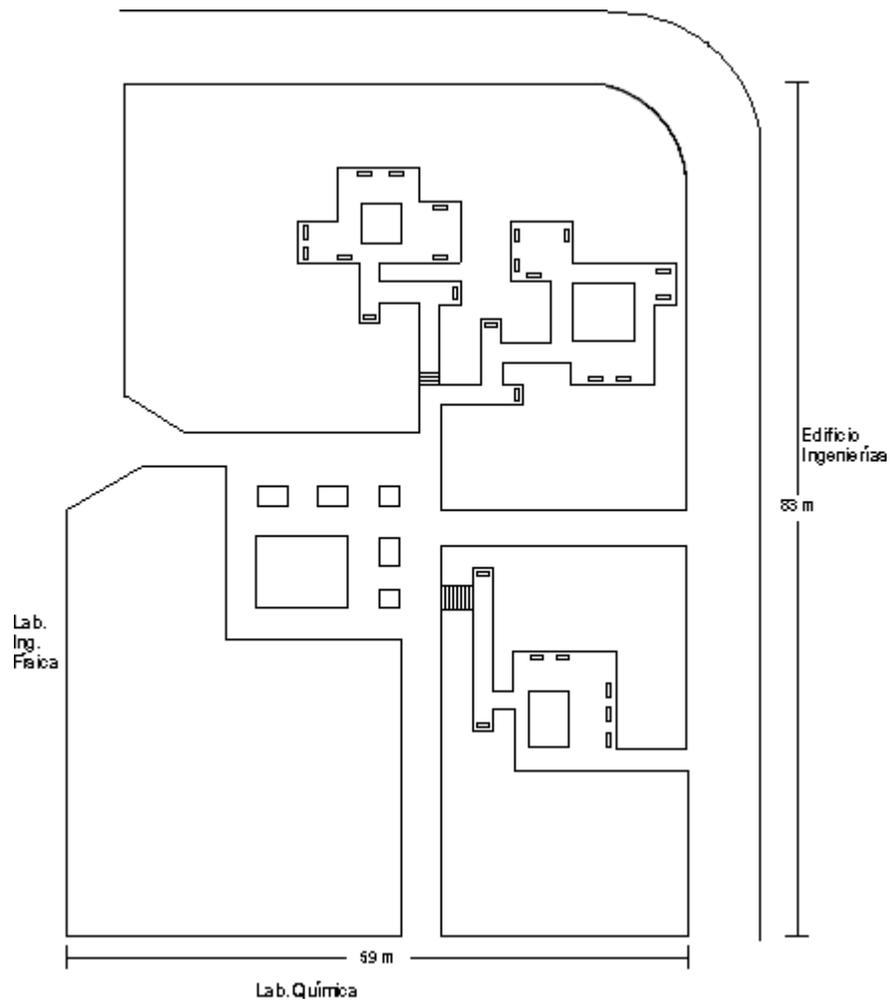
- Concreto
- Ladrillo
- Vidrio
- Madera
- Baldosa

- Cemento
- Aluminio

La altura de cada piso en promedio es de 3.1 m.

El parque se compone de muchos árboles de diferentes tamaños, que seguirán creciendo y que en un momento dado pueden llegar a ser fuentes de bloqueo, afectando la propagación de la señal, sin embargo, se ve menos afectada que en el interior de los edificios, el peor de los casos se presenta cuando las hojas de los árboles están mojadas ya que aumentan la atenuación del enlace inalámbrico. El plano del parque de ingenierías se muestra en la figura 77.

Figura 77. Parque de Ingenierías.



5.1.2 Redes existentes: el edificio de Ingenierías y el edificio de Postgrados cuenta con una infraestructura de red cableada importante distribuida a lo largo de casi cada uno de los edificios.

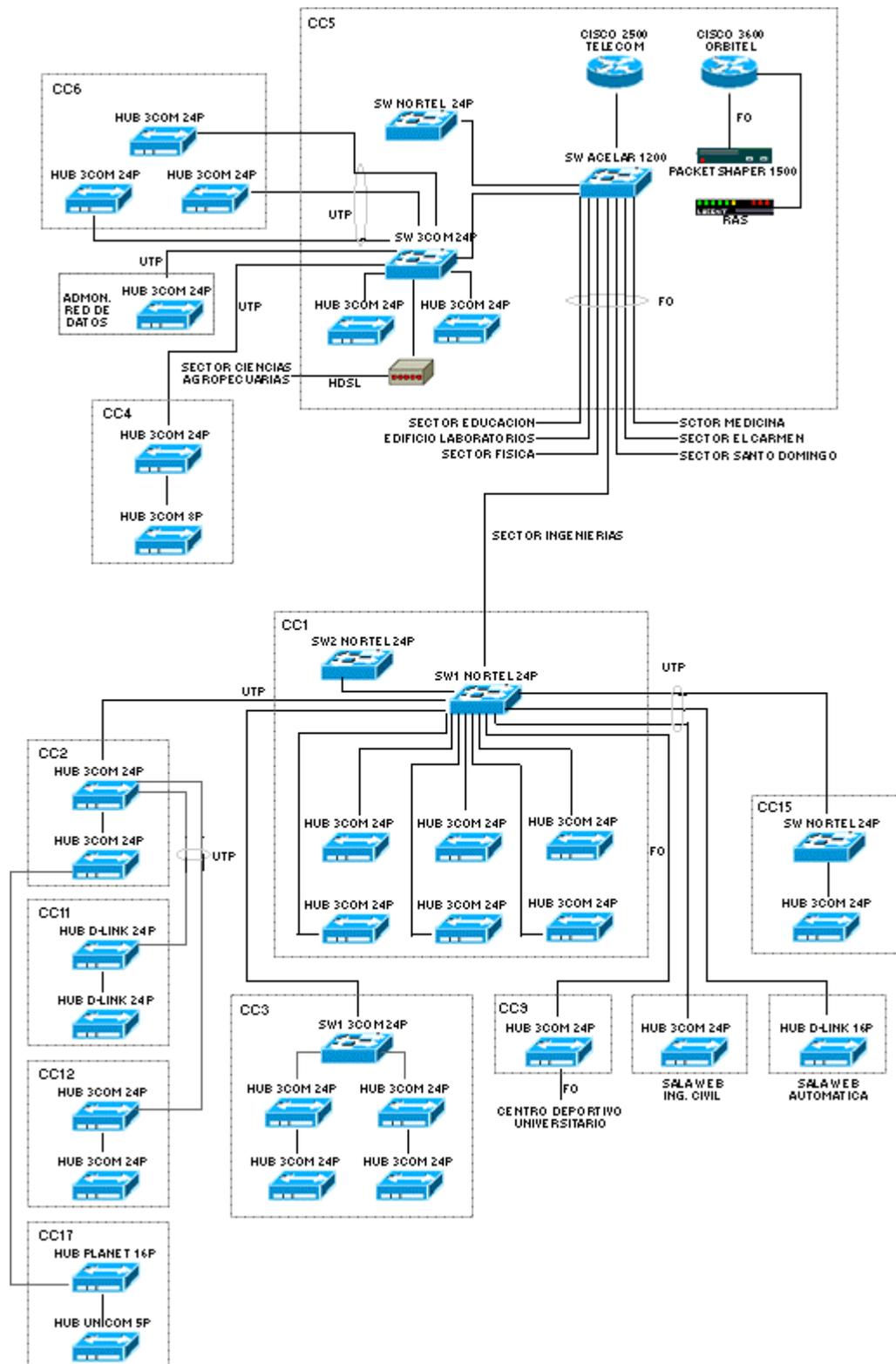
La Red de Datos de la Universidad del Cauca está basada en la tecnología Fast Ethernet y utiliza concentradores para agrupar el flujo de información de clientes por medio de cable UTP categoría 5 y fibra óptica; en la mayoría de las situaciones los concentradores de menor tráfico se encuentran en cascada con otros concentradores por el mismo tipo de cable. Los concentradores de mayor tráfico son conectados a *switches* por medio de fibra óptica.

El diagrama topológico de la red en los sectores de interés se muestra en la figura 78. No existe convención para nombrar los equipos de la red, solo la sigla CC es usada como abreviación para Centro de Cableado. Ver tabla 17.

Tabla 17. Ubicación de los centros de cableado

Centro de cableado	Edificio	Ubicación
CC1	Ingenierías	Oficina 425
CC2	Ingenierías	Salón Carlos Matías
CC3	Ingenierías	Salón 323
CC4	Ingenierías	Oficina 241
CC5	Postgrados	Área de servidores y servicios de internet
CC6	Postgrados	Área de servidores y servicios de internet
CC9	Ingenierías	Enfermería
CC11	Ingenierías	Salón 336
CC12	Ingenierías	Salón 338
CC15	Ingenierías	Oficina 410
CC17	Ingenierías	Salón 342
	Ingenierías	Salón 449
	Ingenierías	Salón 311
	Postgrados	Área de servidores y servicios de internet

Figura 78. Diagrama topológico red cableada.



La red cableada de la Universidad del Cauca en el sector de Ingenierías se encuentra con una demanda de casi el 100 % de los 813 puertos disponibles en *switches* y en concentradores, por lo tanto es difícil encontrar puntos de red libres. Para el diseño de la red se tomarán los que se consideren necesarios, ya que la red inalámbrica contribuirá a aumentar la cantidad de usuarios conectados a la red.

Como la red cableada es Fast Ethernet y debido a que el cable es categoría 5, la máxima velocidad alcanzada es 100 Mbps. Esto es importante ya que se puede soportar perfectamente la conexión de una red inalámbrica a una velocidad máxima de 54 Mbps; sin embargo, este valor está limitado por los concentradores y *switches* a los cuales se conecta el AP, ya que estos algunas veces pueden soportar 10 Mbps.

Todo el edificio de Ingenierías y el edificio de Postgrados cuentan con una infraestructura de red eléctrica en la totalidad de sus salones, por lo tanto no será necesario el uso de dispositivos PoE en el interior de los edificios.

La asignación de direcciones IP se hará de manera estática teniendo en cuenta las direcciones reservadas especialmente para redes privadas dadas en el RFC 1918, que son las siguientes:

- Direcciones Clase A: 10.X.X.X
- Direcciones Clase B: 172.16.X.X
- Direcciones Clase C: 192.168.X.X

Debido a que la Universidad maneja el rango de direcciones clase B que permite la utilización de 65534 *host*, se cuenta con suficientes direcciones libres para la asignación de ellas a los APs y clientes resultantes del diseño de la red inalámbrica.

5.1.3 Análisis de la interferencia: no existen redes inalámbricas exteriores cercanas que puedan causar interferencia, sin embargo, internamente existe interferencia causada por la red 802.11b del proyecto EHAS de la Universidad del Cauca^{*}, que trabaja en el canal 1 con una antena ubicada sobre la oficina 407. Esta interferencia se puede detectar en varios sitios del Campus de Ingenierías como son: el parque, los kioscos de la cafetería y parte de los pisos tercero y cuarto, tal como se indica en

^{*} <http://git.ucauca.edu.co/ehas/>

la figura 79 y 80. Para la medición de la interferencia se hizo uso de la herramienta software para detección de redes inalámbricas NetStumbler** versión 0.3.30.

Figura 79. Interferencia del proyecto EHAS – Tercer piso.

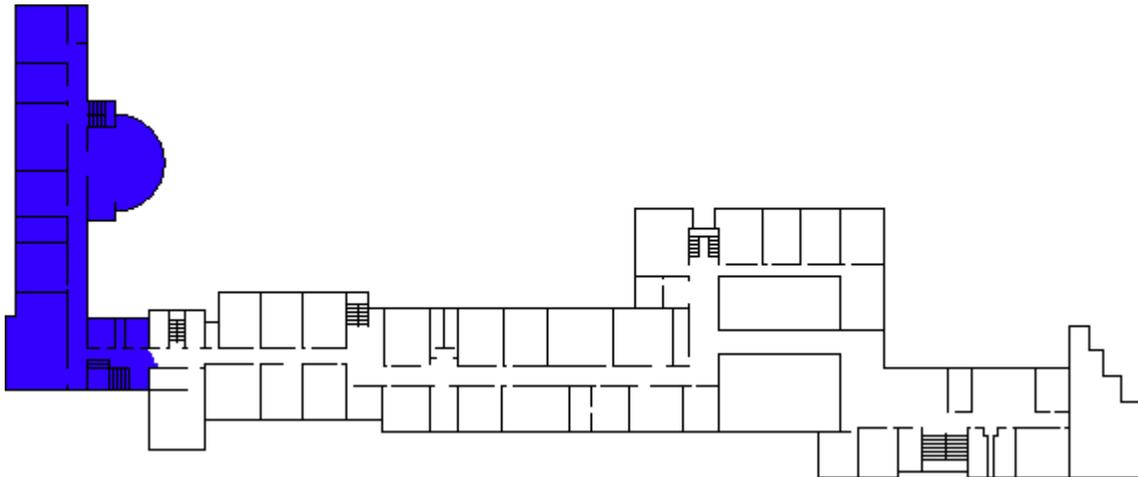
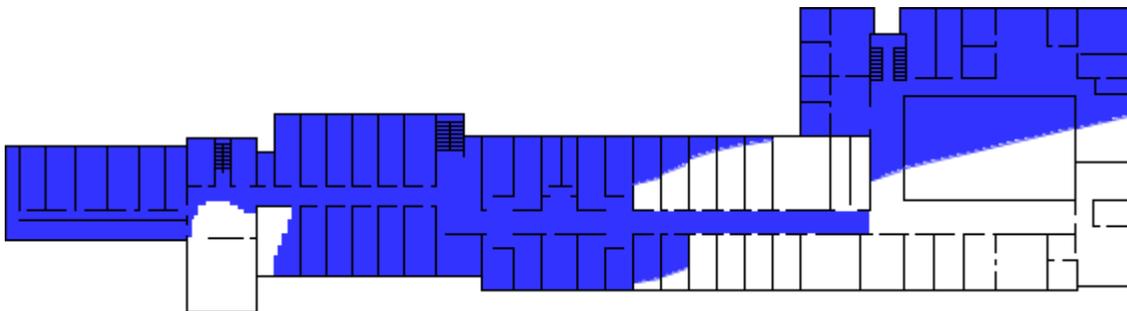


Figura 80. Interferencia del proyecto EHAS – Cuarto piso.



5.2 CAPACIDAD

En este paso se determinan los factores que influyen directamente en la capacidad del sistema.

5.2.1 Tecnología: para el diseño de la red inalámbrica se decidió usar 802.11g, debido a que reúne las ventajas de la norma 802.11a en cuanto a capacidad al soportar hasta 54 Mbps y las ventajas de rango de cobertura de la norma 802.11b. Un aspecto importante es que al seleccionarse 802.11g se garantiza la compatibilidad con 802.11b.

** <http://www.netstumbler.com/>

5.2.2 Cambio de velocidades: mediante el uso de un AP D-link 2000AP, un computador portátil con una tarjeta Broadcom 54g se hicieron mediciones para determinar los umbrales en los cuales habían cambios de velocidad.

Tabla 18. Umbrales de recepción.

Velocidad [Mbps]	Sensitividad [dBm]
54	-40
36	-55
24	-60
18	-65
11	-70
5.5	-75
2	-81
1	-85

5.2.3 Ancho de banda por usuario: para la determinación de las aplicaciones usadas por los usuarios de la red inalámbrica, se tuvo en cuenta las estadísticas de uso de la red de datos de la Universidad del Cauca, gracias al Packetshaper el cual sondea la utilización del enlace de 2 Mbps de Orbitel. Las estadísticas de utilización de la red cableada durante el mes de mayo de 2004, se pueden observar en las tablas 19 y 20.

Tabla 19. Utilización del enlace de bajada.

Aplicaciones	Velocidad promedio [kbps]	Porcentaje [%]
HTTP	492	72
FTP	66.3	10
SMTP	25.1	4
WinMedia	24.2	4
HTTP Interno	18.5	3
MPEG – video	13.2	2
SSL	10	1
Real	4.9	1
DNS	4.8	1
SMB (Bloque de mensajes de servidor)	4.3	1
Otras aplicaciones	16.6	2

Tabla 20. Utilización del enlace de subida.

Aplicaciones	Velocidad promedio [kbps]	Porcentaje [%]
HTTP	272	51
Auto descubierto por defecto	135	25
FTP	56.4	11
SSL	18.8	4
SMTP	13.5	3
Por defecto	11.3	2
SMB (Bloque de mensajes de servidor)	7.7	1
DNS	2.9	1
SSH	2.8	1
NetBios IP	2.6	0
Otras aplicaciones	11.8	2

Por lo tanto se puede concluir que la red de datos es usada principalmente para la navegación en internet y para la descarga de archivos usando HTTP y FTP. Lo anterior, determina que un usuario típico de la red inalámbrica podría usar entre 300 y 500 kbps de la capacidad de un AP.

5.3 COBERTURA

5.3.1 Área de cobertura: el Campus de Ingenierías tiene varias áreas en donde se puede implantar las tecnologías inalámbricas, los lugares de mayor interés están determinados por aquellos sitios donde se encuentra una mayor concentración de usuario o no se cuenta con acceso a la red. El área de cobertura incluye los auditorios, salas de reuniones, salas de audiovisuales, salones de proyectos, Decanaturas, parques, cafetería, terrazas y Bienestar Universitario. Una relación más detallada de los sitios es la siguiente:

- Auditorios: Gregorio Caicedo (FIC) y Francisco Lemos Arboleda (FIET).
- Salas de reuniones: oficina 411 (departamento de hidráulica), oficina 414 (jefatura departamento de telemática), oficina 419 (departamento de ingeniería ambiental y sanitaria), oficina 420 (jefatura departamento de electrónica, instrumentación y control), oficina 424 (jefatura departamento de sistemas), oficina 437 (departamento de vías y transporte), oficina 442 (jefatura departamento de telecomunicaciones), oficina 446 (departamento de estructuras), oficina 451 (educación continuada), oficina 453 (comités FIC), salón Carlos Matías, oficina 329 (departamento de sistemas), oficina 335 (geotecnia), sala de juntas IPET, sala de juntas IPIC, salón 116 (ASPU).

- Salas de audiovisuales: salón 327 (departamento de telecomunicaciones), salón 328 (departamento de telemática), salón 347 (geotecnia), salón 126 (salón de postgrados FIC), salón 127 (salón de postgrados FIET), salón 128 (salón de proyectos FIC)
- Salones de proyectos: oficina 448 (proyecto sociedad de la información), oficina 319 (grupo nuevas tecnologías en telecomunicaciones), oficina 322 (grupo I+D en ingeniería telemática), salón 105 (postgrados), oficina 106 (proyecto ARIADNA), oficina 110 (ambientes de desarrollo), oficina 117 (proyecto telemedicina).
- Cafetería y kioscos externos.
- Terrazas segundo y tercer piso.
- Parque de Ingenierías.
- Sala de espera (Bienestar Universitario).
- Decanaturas FIET y FIC.

5.3.2 Patrón de radiación de la antena: generalmente los APs que se encuentran en el mercado vienen con antenas omnidireccionales tipo dipolo, la ganancia típica de estas antenas es de 2.2 dBi. Para el diseño en el interior del edificio, se tendrán en cuenta las antenas omnidireccionales que vienen con el AP. Para el diseño en el exterior del edificio se considerará el uso de antenas direccionales tipo panel con una ganancia de 9dBi y un lóbulo de radiación horizontal entre 65° y 90°.

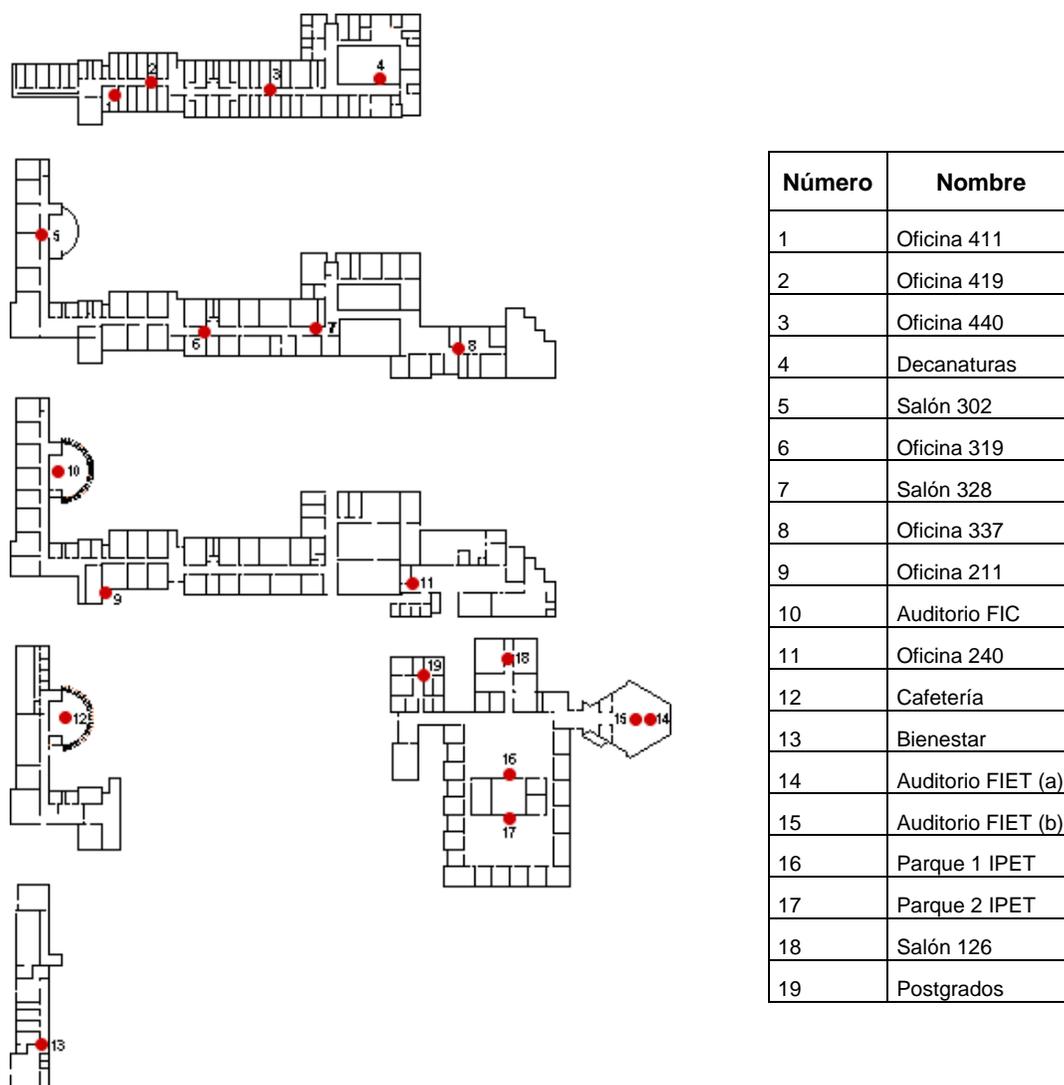
5.3.3 Montaje de APs y de antenas: cuando se trate de un AP ubicado en el interior del edificio se puede montar en una carcasa para el techo, esto también evita un montaje especial para la antena. Cuando se trate de un AP que se encuentre fuera del edificio se puede usar carcasas a prueba de condiciones atmosféricas adversas y la antena se puede ubicar en la pared o en un mástil. Hay que recordar que cuando la antena sea usada en un ambiente externo, se deberá tener en cuenta que sea también a prueba de condiciones atmosféricas adversas.

5.3.4 Frecuencia: ya que el diseño de la red inalámbrica se hará con 802.11g, será usada por lo tanto la banda de 2.4 GHz, que va desde 2.4000 hasta 2.4835 GHz.

5.3.5 Ubicación de los APs y sus antenas: debido a la infraestructura de red cableada con la que cuenta el sector de Ingenierías y por la ubicación estratégica de los centros de cableado, los APs se conectarán a la red cableada a los puntos de red cercanos a las zonas de cobertura y en los casos donde no existan se puede extender cable desde el centro de cableado más cercano ubicado a menos de 100 m. Entre más alto se ubiquen las antenas mejor, ya que se reduce el riesgo de contacto humano con ellas, por lo tanto la altura escogida para las antenas es de 2.5m.

La ubicación de las antenas se hizo mediante un proceso de ensayo, usando un software de simulación llamado ProMan, que se explica en el numeral 5.5.1. El análisis de la simulación determinó la ubicación más adecuada de los APs para cada uno de los pisos que componen el Campus de Ingenierías y el resultado estaba condicionado al menor uso posible de APs y el cubrimiento del área bajo las condiciones adecuadas para el desempeño de la Red. Para cada uno de los pisos del edificio de Ingenierías se optó por un arreglo lineal de APs, para el edificio de Postgrados se optó por un arreglo rectangular de APs y finalmente para el auditorio Gregorio Caicedo se hizo uso de un arreglo puntual de APs. Los resultados acerca de la mejor ubicación para los APs y sus antenas se muestran en la figura 81.

Figura 81. Ubicación de los APs y sus antenas para los diferentes pisos del Campus.



5.3.6 Potencia de los APs: los fabricantes disponen de varios valores de potencia para los APs permitiendo en algunos casos variar la potencia dentro de un determinado rango, pero la mayoría disponen de los siguientes niveles de potencia: 13dbm, 15dBm, 18dBm o 23dBm. Para nuestro caso, el diseño se realizó eligiéndose APs de potencia de 15dBm. Sin embargo, cuando se necesitó limitar su alcance se escogió el AP de menor potencia (13 dBm). En la tabla 21 se resume la asignación de potencia para cada uno de los APs.

Tabla 21. Potencia para cada uno de los APs.

Número	Nombre	Potencia [dBm]
1	Oficina 411	15
2	Oficina 419	15
3	Oficina 440	15
4	Decanaturas	15
5	Salón 302	15
6	Oficina 319	15
7	Salón 328	15
8	Oficina 337	15
9	Oficina 211	15
10	Auditorio FIC	13
11	Oficina 240	15
12	Cafetería	15
13	Bienestar	13
14	Auditorio FIET (a)	13
15	Auditorio FIET (b)	13
16	Parque 1 IPET	13
17	Parque 2 IPET	13
18	Salón 126	13
19	Postgrados	15

5.4 ASIGNACIÓN DE CANALES

Luego de determinar la mejor ubicación de los APs se procedió a asignarles frecuencias a cada uno de ellos, como se escogió 802.11g, se pueden usar hasta 3 canales en una misma área física sin que ocurra interferencia, por lo tanto se hizo escogencia de los canales 1, 6 y 11 que equivalen a las frecuencias de 2.412 GHz, 2.437 GHz y 2.462 GHz.

Teniendo en cuenta que la red 802.11b del proyecto EHAS causa interferencia en parte del parque, de los kioscos de la cafetería, del piso tercero y casi la totalidad del piso cuarto, como se indicó en el numeral 5.1.3; en estas áreas no se podrá usar el canal 1. Por lo tanto la asignación de canales empieza en las áreas donde se presenta interferencia y después en las demás. El resultado de la asignación de canales se muestra en la tabla 22 con la ubicación de la figura 81.

Tabla 22. Asignación de canales a los APs para los diferentes pisos del Campus.

Número	Nombre	Canal	Punto de red más cercano	Distancia [m]
1	Oficina 411	6	Oficina 410	13.87
2	Oficina 419	11	Oficina 425	17.85
3	Oficina 440	6	Oficina 323	8.06
4	Decanaturas	11	Salón Carlos Matías	15.03
5	Salón 302	6	Salón 312	51.43
6	Oficina 319	11	Salón 323	20.67
7	Salón 328	1	Salón 323	22.15
8	Oficina 337	6	Oficina 241	8.26
9	Oficina 211	6	Oficina 319	53.68
10	Auditorio FIC	11	Salón 305	43.5
11	Oficina 240	11	Oficina 241	14.34
12	Cafetería	6	Salón 305	43.5
13	Bienestar	1	Bienestar	9
14	Auditorio FIET (a)	6	Auditorio FIET	10.37
15	Auditorio FIET (b)	11	Auditorio FIET	11.37
16	Parque 1 IPET	11	Almacén IPIC	12.48
17	Parque 2 IPET	1	Oficina 116	43.01
18	Salón 126	1	Área de servidores	28.31
19	Postgrados	6	Área de servidores	5.93

5.5 ESTUDIO DEL SITIO

Para el estudio de cada una de las áreas a cubrir, se recurrió al uso de una herramienta de predicción. Luego de un estudio de las diferentes opciones: WinProp, LANPlanner y CINDOOR. Se decidió utilizar WinProp perteneciente a la compañía alemana AWE Communications GmbH*, ya que ofrecía licencia de uso gratis durante un periodo de evaluación menor a 10 semanas, las otras herramientas software solamente permitían el uso de una versión limitada únicamente al funcionamiento con sus ejemplos (versión DEMO). A continuación se indica cual fue el proceso

* <http://www.awe-communications.com/>

para la utilización de la herramienta y los resultados para el Campus de Ingenierías de la Universidad del Cauca.

5.5.1 Utilización de WinProp: WinProp es una herramienta software para la planeación de redes de comunicaciones móviles como GSM, UMTS, IS-95, IS-54, PDC, DECT, TPMR, NMT, AMPS, TACS, WLAN, entre otras. La planeación puede ser para áreas rurales, urbanas y para interiores de edificios. WinProp es un paquete compuesto por diferentes módulos software que se relacionan para obtener el máximo desempeño, los diferentes módulos son:

- ProMan: módulo para las predicciones.
- WallMan: módulo para la generación de bases de datos de edificios.
- Aman: módulo para la generación de patrones de antena.

WallMan permite importar archivos DXF (Drawing Exchange Format) de AutoCAD versión 13 o anterior. La limitante fue que se tenía una versión más reciente por lo tanto se debió realizar la incorporación de los planos manualmente. Debido a que el uso de WinProp fue para un periodo de evaluación, solamente se permitió la consideración de una única base de datos.

ProMan permite usar la base de datos generada en WallMan, escoger la ubicación de los APs, escoger el tipo de antena, asignar frecuencias y asignar potencias para permitir el cálculo de propagación de la señal. El cálculo de la propagación depende del modelo de propagación, para nuestro caso y según la confrontación entre las medidas prácticas con las arrojadas por los diferentes modelos, se concluyó que el modelo más cercano a los resultados obtenidos en las pruebas realizadas era el modelo Motley – Keenan, el valor de las pérdidas de las paredes escogido fue 13.5 dB.

5.5.2 Resultados de la simulación: la simulación con ProMan permite determinar que los resultados de los pasos anteriores aseguran el cubrimiento en las áreas asignadas. Los resultados que entrega ProMan para cada uno de los pisos son los siguientes.

Máxima potencia recibida: este resultado considera a cada uno de los APs y determina cual es la máxima potencia recibida en cada uno de los lugares de cada piso. Puede que en algún lugar se reciba la señal de más de un AP, el programa de simulación escoge la mayor potencia recibida por uno de ellos y muestra el resultado, este proceso se realiza para cada uno de los lugares del piso. Este resultado no muestra a que AP hace referencia cada potencia. Los valores oscilan entre -28 dBm y -102 dBm.

Máxima velocidad de datos: dependiendo del nivel de señal recibido en cada uno de los sitios de cada piso se puede obtener la máxima velocidad de datos alcanzada. Para los umbrales se tomaron los resultados del numeral 5.2.2. Este resultado muestra las velocidades más representativas, que son: 1, 2, 5.5, 11, 18, 24, 36 y 54 Mbps. Aquellos sitios en blanco representan los huecos de cubrimiento. El resultado no muestra con que AP se asocia para alcanzar cada una de las velocidades.

En las figuras desde 82 a 93 se muestran detalladamente los resultados de potencia recibida y las velocidades alcanzadas para cada uno de los puntos de los edificios de Ingenierías y Postgrados. Cada una de las figuras muestra exactamente como los valores de potencia recibida y velocidad alcanzada cambian a medida que la señal va pasando a través de paredes y propagándose en salones y corredores.

Para cada una de las velocidades de asociación y para cada uno de los pisos se pueden obtener cualquiera de los siguientes resultados.

Mejor AP: para cada uno de los lugares de cada piso se determina cual es el mejor AP en un área determinada. Este resultado se puede ver también como el tamaño de la celda para cada uno de los APs.

Probabilidad de recepción: este resultado muestra cual es la probabilidad de que se tenga señal en un determinado punto del piso, si el resultado cae dentro de una celda la probabilidad será del 100% y si es 0% indica que se trata de un hueco de cubrimiento.

Número de canales recibidos: para cada uno de los lugares del piso se puede mostrar el número de canales recibidos, en la áreas de cobertura. El valor de cero es para los huecos, el valor de uno indica que solamente un AP puede alcanzar el lugar y garantizar determinada velocidad y un valor mayor a uno indica cuantos APs alcanzan el lugar para garantizar determinada velocidad. Este resultado puede servir para derivar el resultado del *handover*, restando en uno el número de canales recibidos, el resultado del *handover* sirve para indicar cuantas alternativas se tienen en determinado punto para alcanzar determinada velocidad.

Para no hacer extenso el número de resultados, se tomaron los resultados solo para las velocidades de 1, 11 y 54 Mbps. En las figura desde 94 hasta 102 se muestran únicamente los resultados para el cuarto piso y se realiza una explicación resumida. En el anexo D se incluyen los resultados para los demás pisos.

5.5.2.1 Resultados según máxima potencia recibida y máxima velocidad de datos.

Figura 82. Cuarto piso máxima potencia recibida.

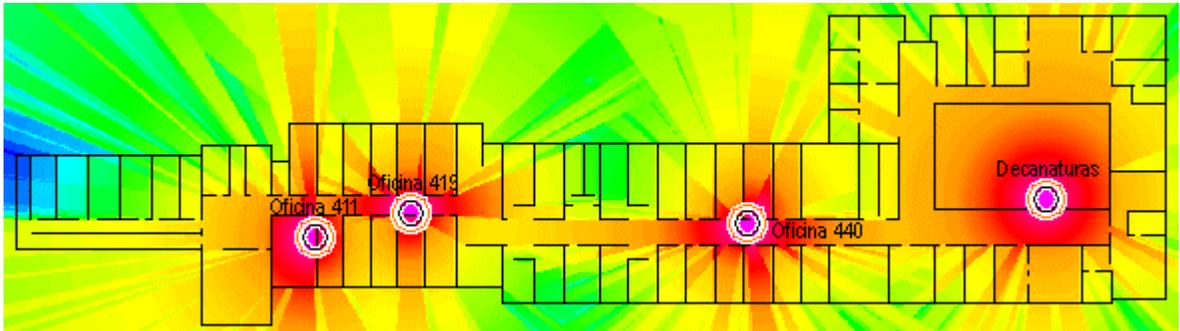


Figura 83. Cuarto piso máxima velocidad de datos.

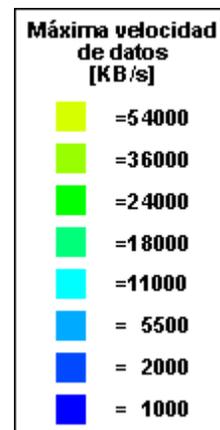
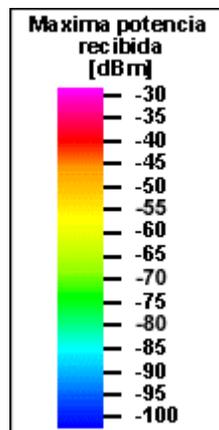
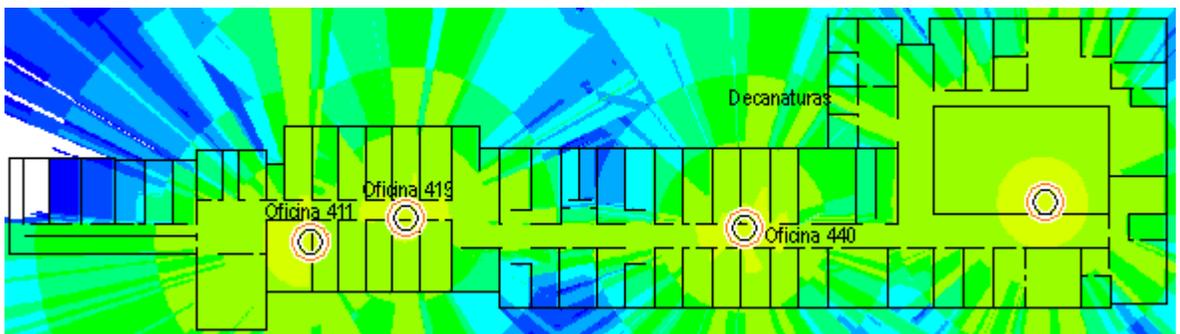


Figura 84. Tercer piso máxima potencia recibida.

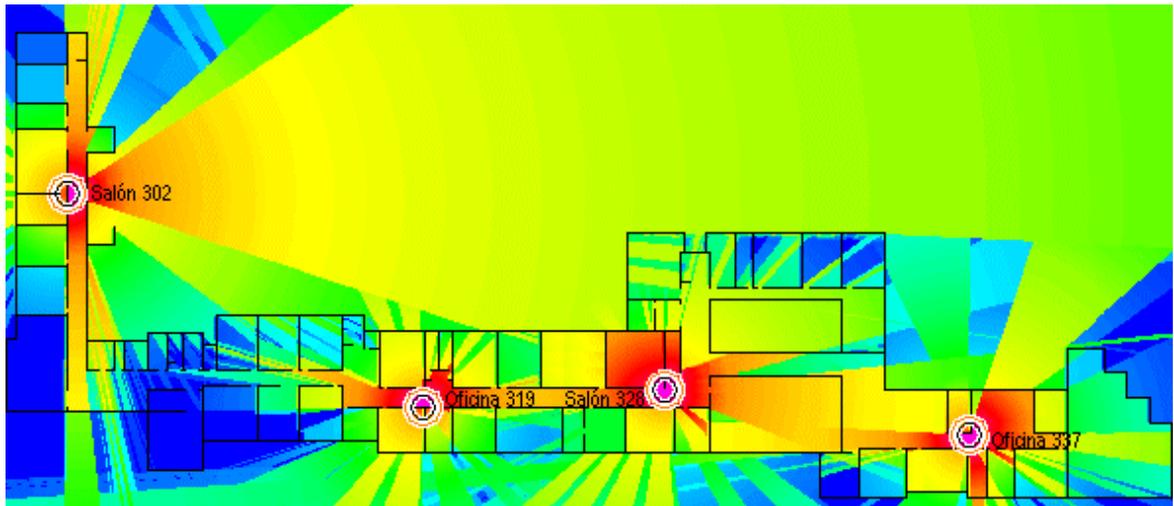


Figura 85. Tercer piso máxima velocidad de datos.

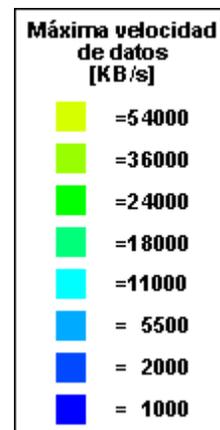
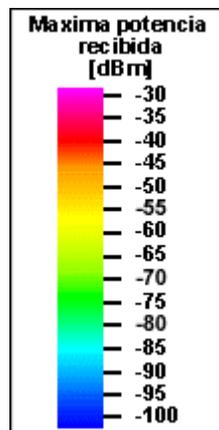
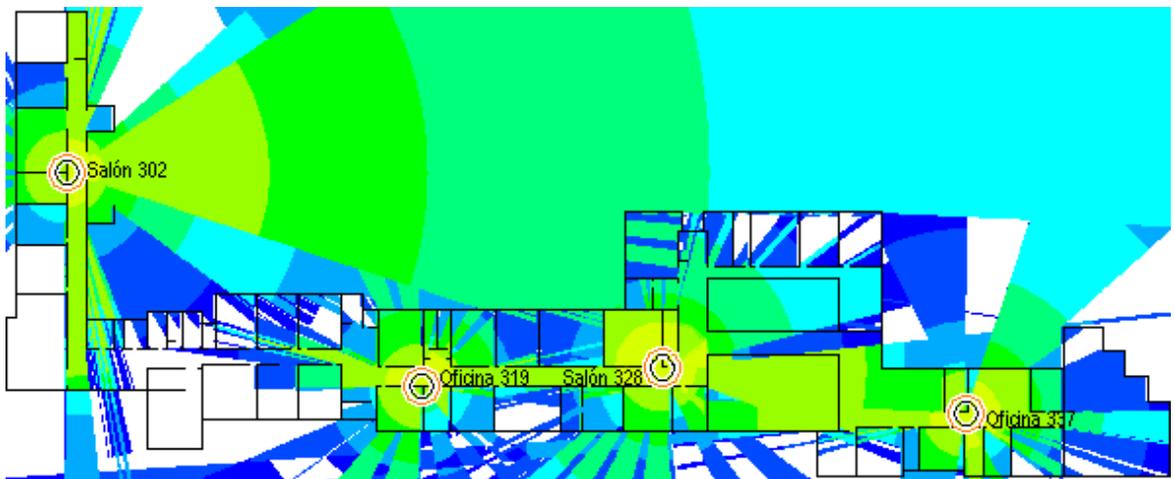


Figura 86. Segundo piso máxima potencia recibida.

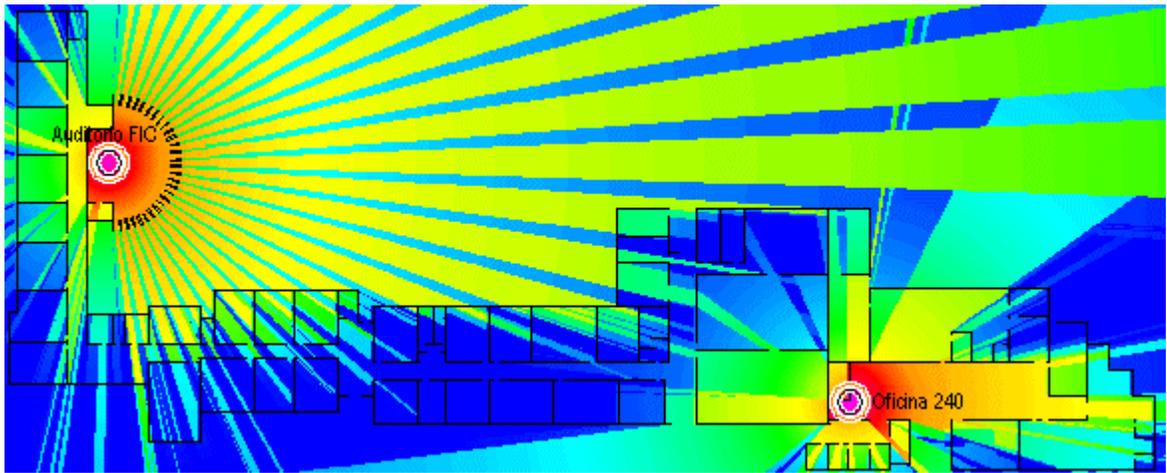


Figura 87. Segundo piso máxima velocidad de datos.

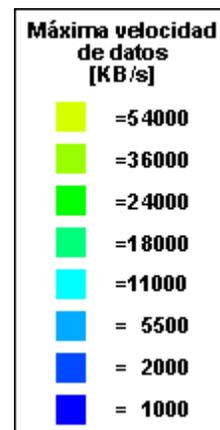
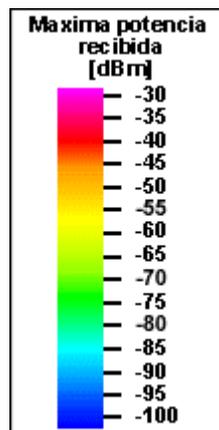
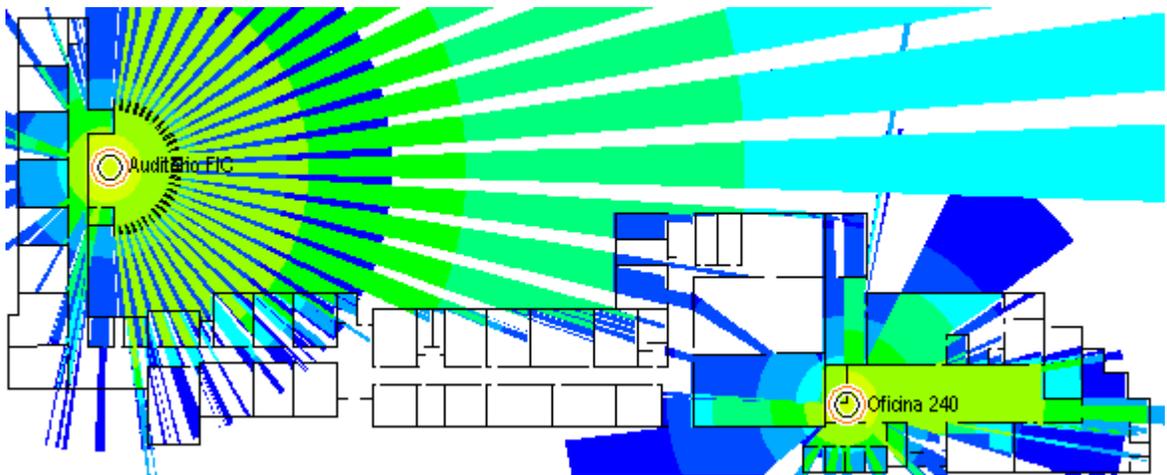


Figura 88. Primer piso máxima potencia recibida.

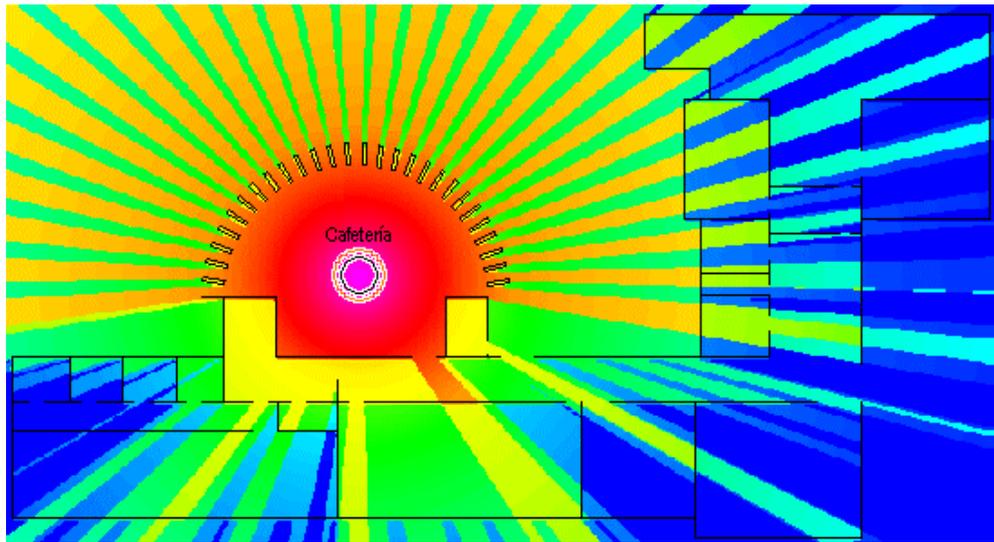


Figura 89. Primer piso máxima velocidad de datos.

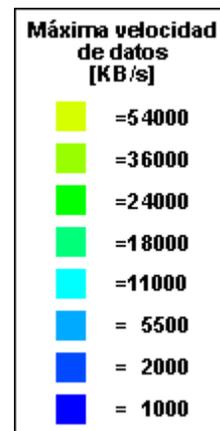
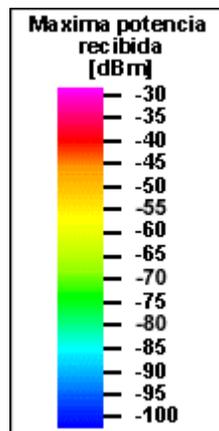
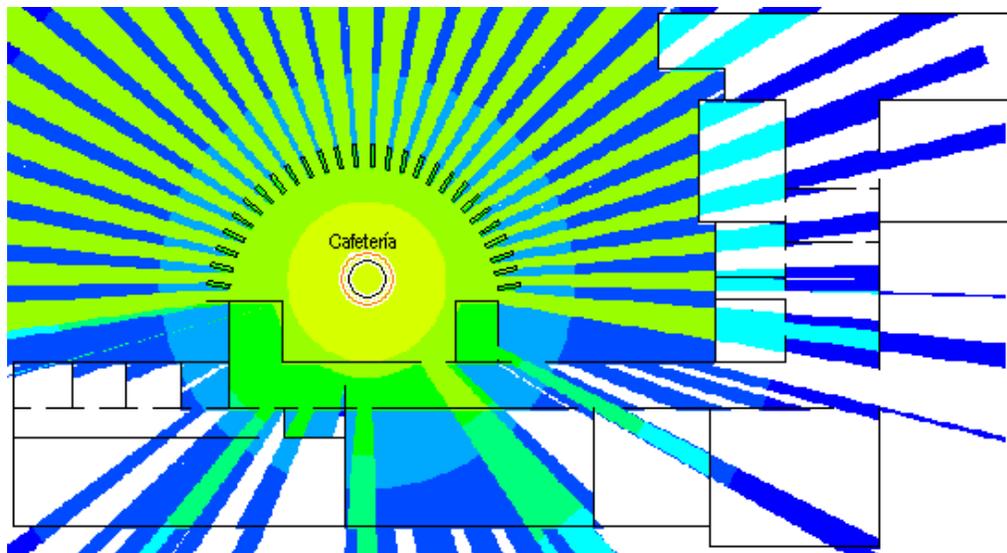


Figura 90. Sótano máxima potencia recibida.

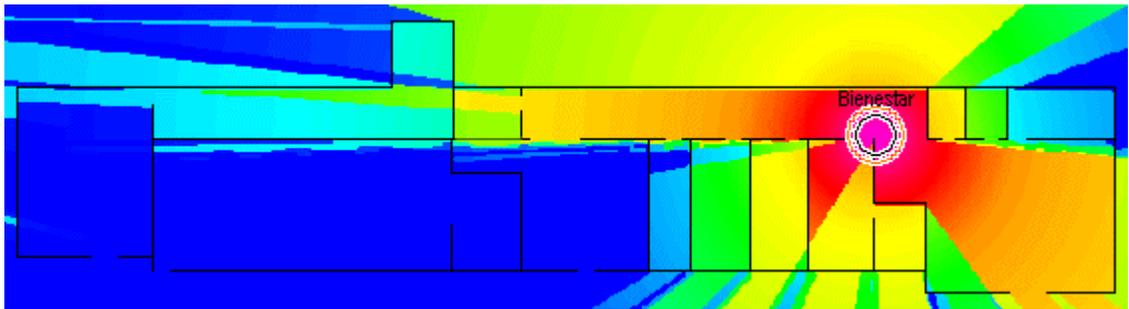


Figura 91. Sótano máxima velocidad de datos.

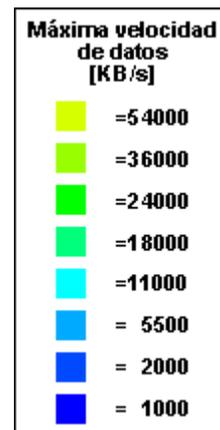
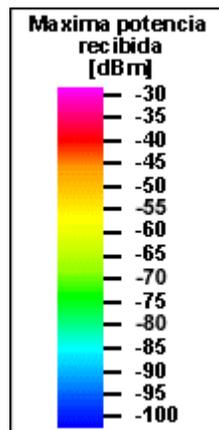
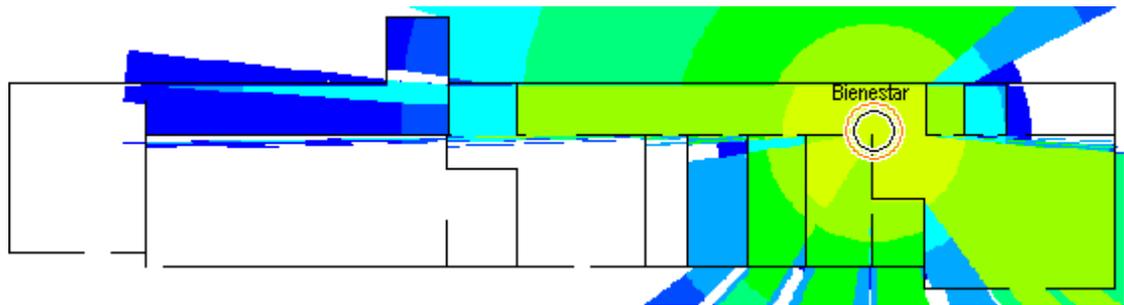


Figura 92. Postgrados máxima potencia recibida.

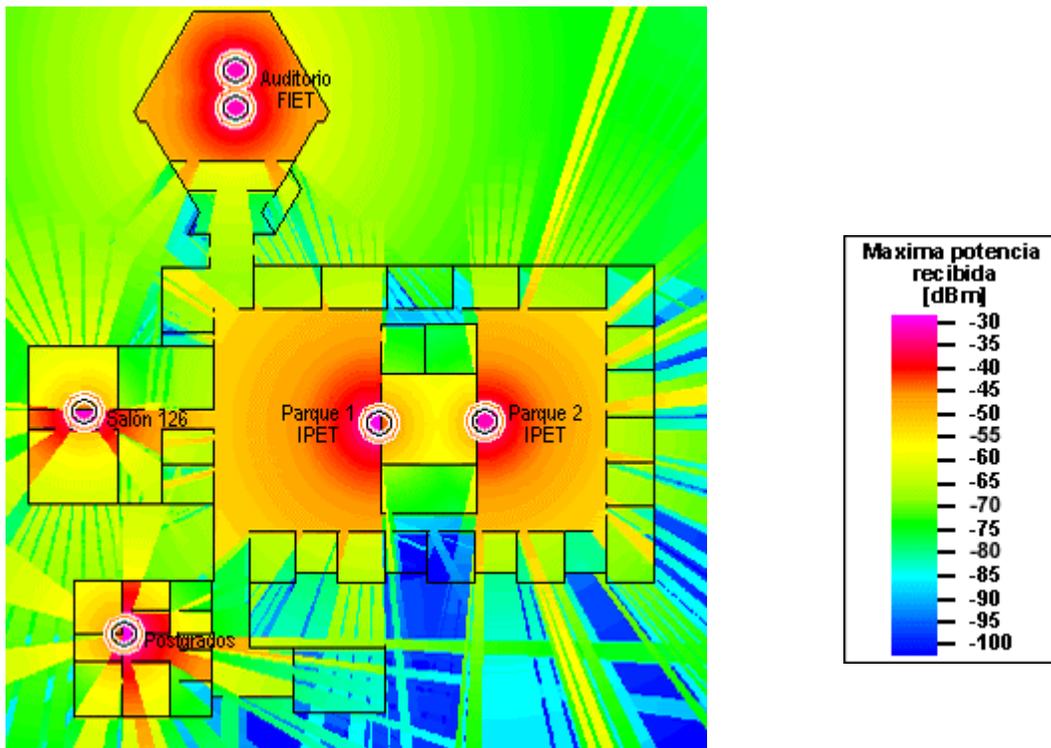
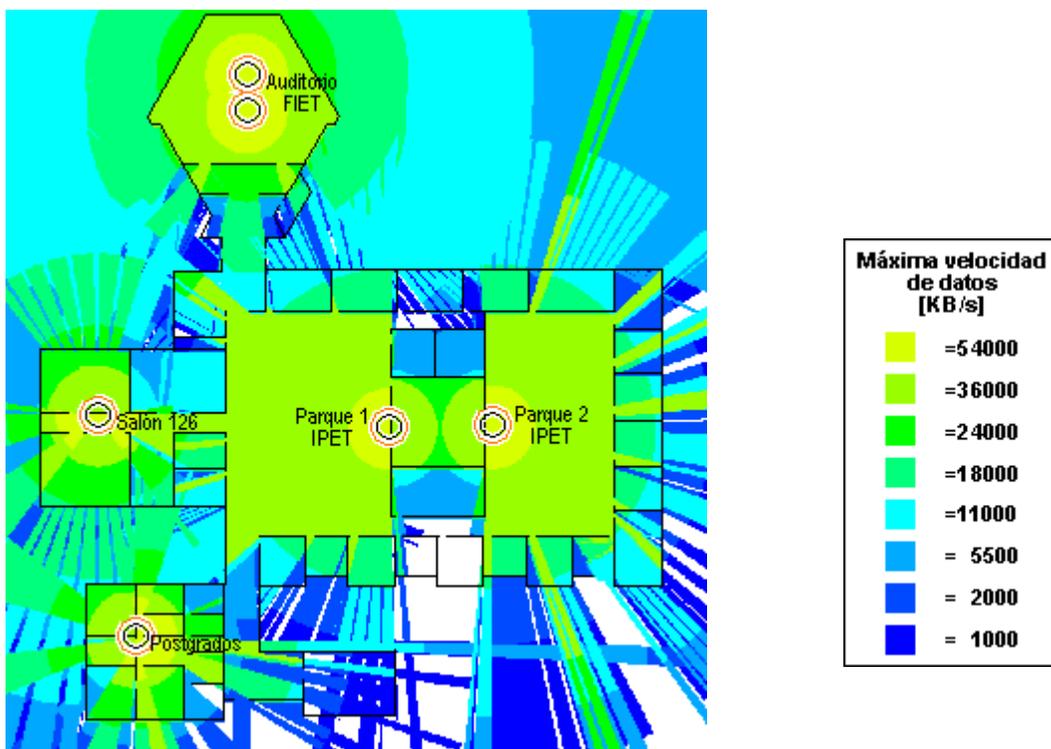


Figura 93. Postgrados máxima velocidad de datos.



5.5.2.2 Resultados según el mejor AP.

Figura 94. Cuarto piso mejor AP para la velocidad de 1 Mbps.

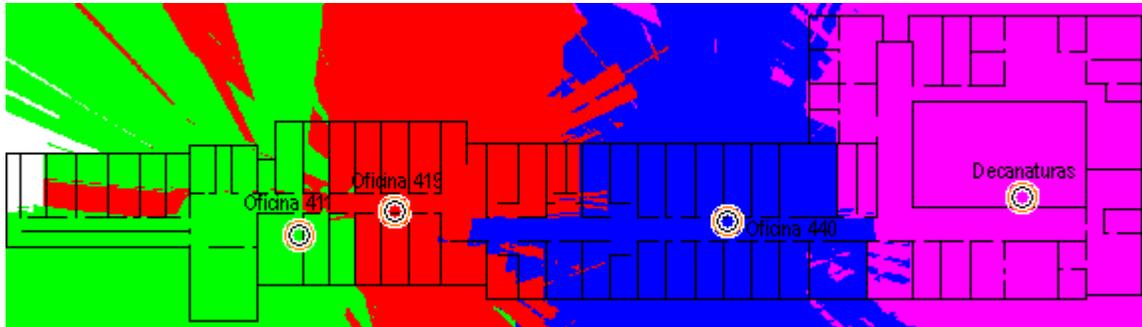


Figura 95. Cuarto piso mejor AP para la velocidad de 11 Mbps.

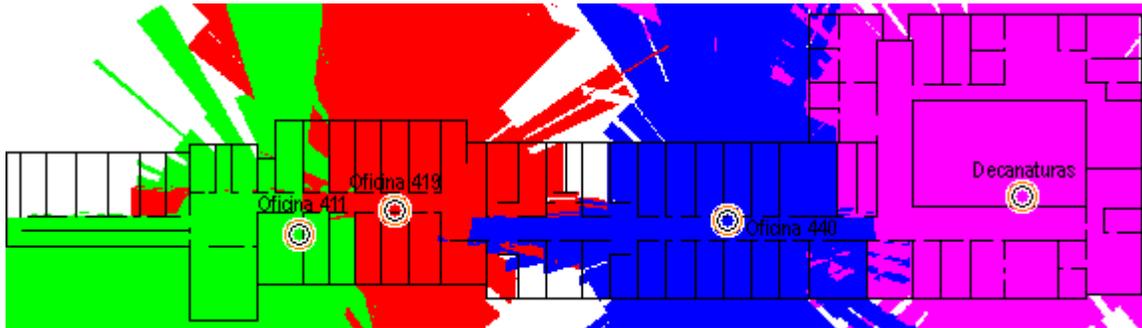
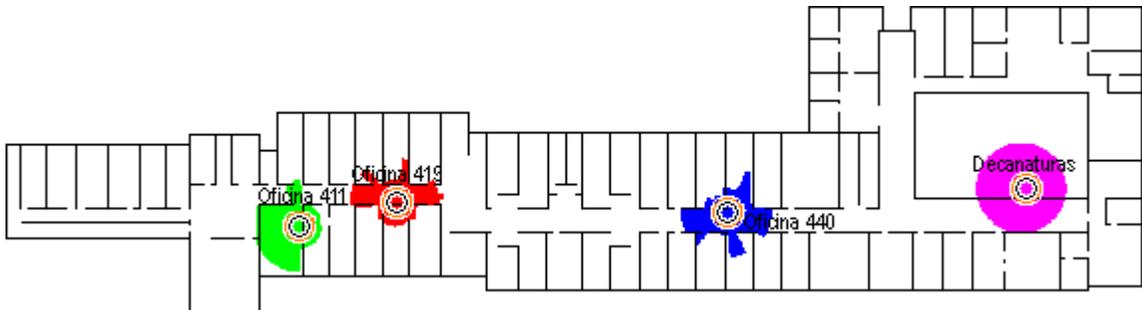


Figura 96. Cuarto piso mejor AP para la velocidad de 54 Mbps.



Cada uno de los colores corresponden al área de dominio de un AP particular. Se puede deducir de los resultados anteriores, que el área de la celda para cada velocidad depende de la potencia de recepción en cada punto. Para la velocidad de 1 Mbps se consiguen las celdas más grandes, mientras que para la velocidad de 54 Mbps se consiguen las celdas más pequeñas debido a que el nivel umbral aumenta a medida que aumenta la velocidad. Se puede concluir que a medida que va aumentando la velocidad de asociación el tamaño de las celdas va disminuyendo.

5.5.2.3 Resultados según la probabilidad de recepción.

Figura 97. Cuarto piso probabilidad de recepción para la velocidad de 1 Mbps.

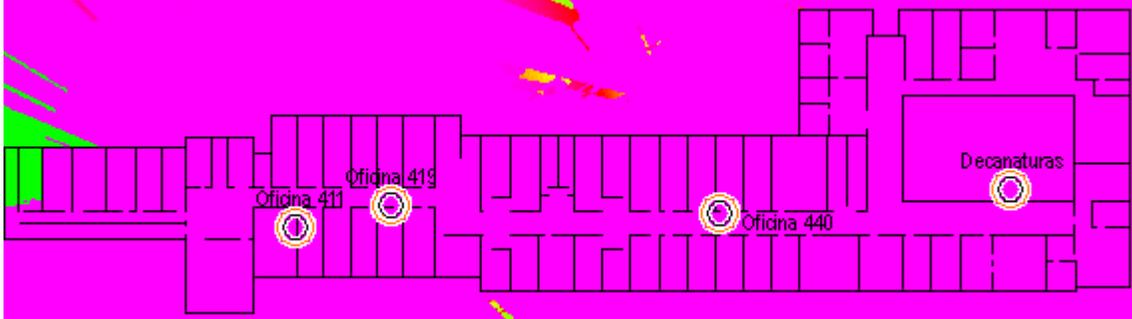


Figura 98. Cuarto piso probabilidad de recepción para la velocidad de 11 Mbps.

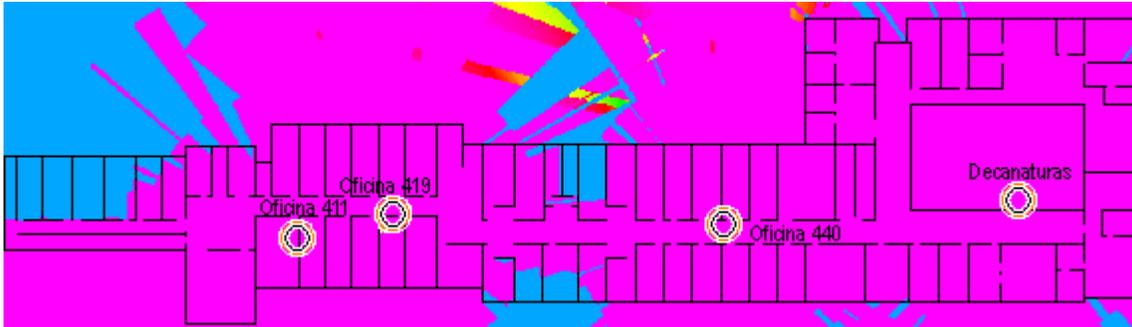
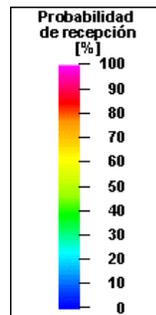
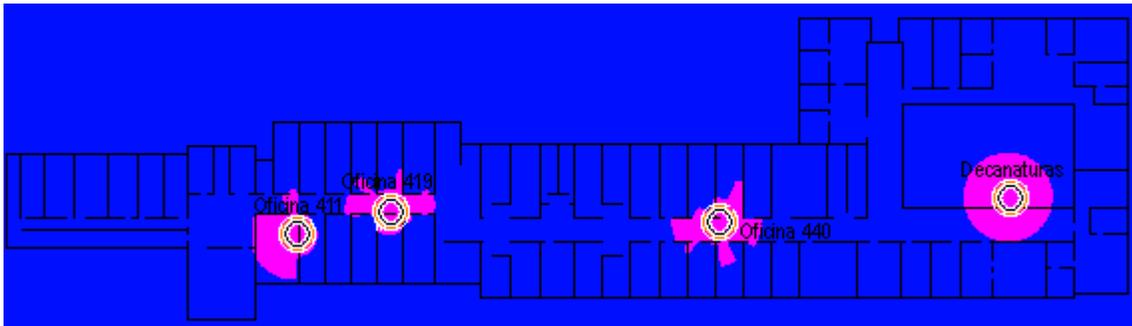


Figura 99. Cuarto piso probabilidad de recepción para la velocidad de 54 Mbps.



Los resultados anteriores muestran la probabilidad de recepción para el cuarto piso, la probabilidad de recepción del 100% va disminuyendo a medida que aumenta la velocidad de asociación. Un

valor diferente al 100% de probabilidad de recepción, indica que aleatoriamente puede llegar a presentarse asociación a determinada velocidad, esto se consigue excepto en el caso de 0%.

5.5.2.4 Resultados según el número de canales.

Figura 100. Cuarto piso número de canales recibidos para la velocidad de 1 Mbps.



Figura 101. Cuarto piso número de canales recibidos para la velocidad de 11 Mbps.

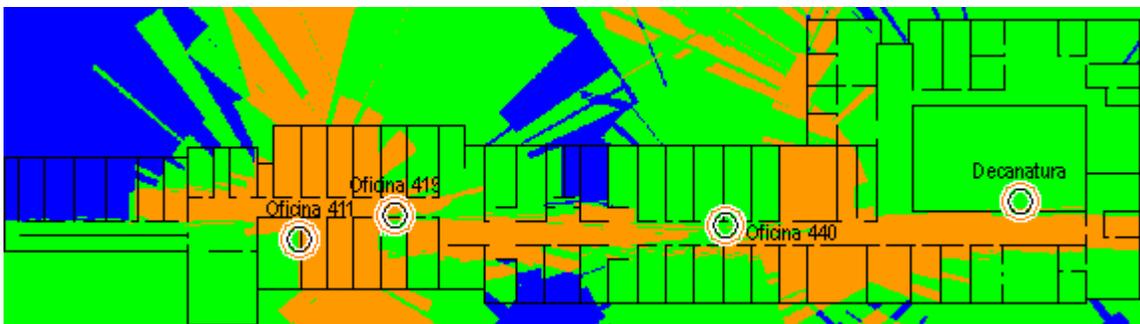
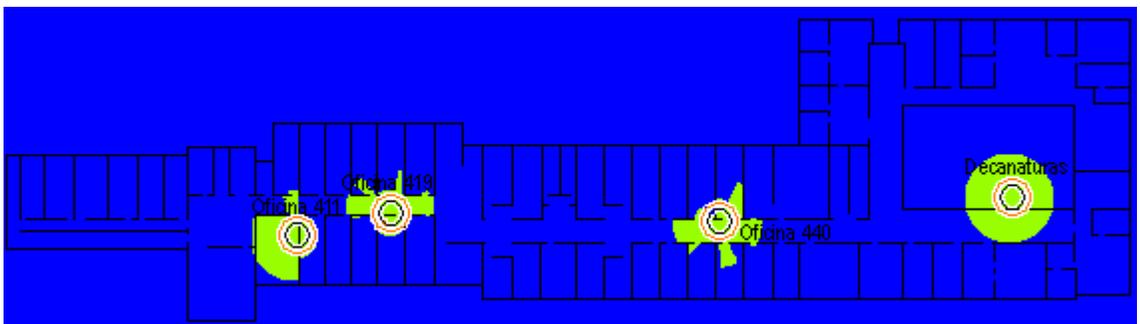


Figura 102. Cuarto piso número de canales recibidos para la velocidad de 54 Mbps.



Los resultados anteriores correspondientes al número de canales recibidos en cada uno de los puntos del cuarto piso, muestran exactamente como ocurre la superposición de celdas. El caso en que existe menor superposición de celdas ocurre a la velocidad de asociación de 54 Mbps, ya que la separación entre la ubicación de los APs y demás características de los APs hace que se presenten las condiciones para recibir máximo un canal. El caso en que ocurre mayor superposición de celdas es para la velocidad de asociación de 1 Mbps, donde se logran hasta 2 canales, este resultado es importante ya que solamente se usan dos canales en el cuarto piso, en caso de haberse recibido más de dos canales, sería un indicio importante de la existencia de interferencia.

A pesar de que no se muestre la influencia de un AP sobre los pisos superiores e inferiores, en pruebas realizadas con el AP D-link 2000AP el cual transmitía a una potencia de 15 dBm, se determinó que únicamente influía en los salones que coincidían exactamente arriba y exactamente abajo, ya que la señal no alcanzaba a pasar más allá de una pared y el techo o suelo entre pisos. A la hora del diseño se tuvo en cuenta ubicar los diferentes APs que operaran en el mismo canal uno exactamente encima o debajo del otro.

5.6 SEGURIDAD

Debido a que recientemente el IEEE aprobó la norma 802.11i, se recomienda el uso de equipos que soporten esta tecnología, los cuales empezarán a ser probados por la Alianza Wi-Fi en septiembre de 2004, que además usará la abreviación WPA2 para referirse a 802.11i. Cabe resaltar que 802.11i será compatible con productos WPA, siempre y cuando soporten AES.

También vale la pena definir las políticas de seguridad para el uso de la red:

- Mantener actualizado el *firmware* de los APs.
- Los APs deben ser constantemente vigilados, con el fin de evitar su robo.
- Los APs debe ser desactivados en periodos de inactividad, o deshabilitar aplicaciones cuando sea necesario.
- Cambiar el SSID por defecto de los APs.
- Inhabilitar la difusión del SSID.
- Evitar el uso de APs no autorizados.
- Configurar los equipos con la máxima seguridad posible.
- Usar aplicaciones software y hardware para monitorear en tiempo real la red inalámbrica y el uso del espectro evitando las posibles interferencias de modo que se tomen decisiones inmediatas y acordes con el problema.

- Usar aplicaciones de detección de intrusos.
- Planear futuras mejoras en cuanto a seguridad.

5.7 DOCUMENTACION

Consiste en los planos, figuras, áreas de cobertura, huecos de cobertura, velocidades alcanzadas; así como la información de los APs: ubicación, potencias, nombres, y canales, tipos de antenas, montajes, interferencias.

A continuación se llena el formato que resume la información adicional y que será necesaria para la implementación de la red inalámbrica.

Datos del cliente

Nombre del cliente: Universidad del Cauca

El diseño de la red inalámbrica es para el Campus de Ingenierías compuesto por la FIET y la FIC.

Información sobre redes inalámbricas existentes

Existe algún estudio del sitio anterior?

- Si No

Existe algún equipo WLAN en el lugar?

- 802.11 802.11b
 802.11a 802.11g
 Otro

Cuántos APs hay en el lugar y que referencias?

1 AP Marca Z-Com del proyecto EHAS

Hay convenios con fabricantes?

- Si No

Hay APs desempeñando balance de carga?

- Si No

Qué clase de soluciones de seguridad hay en el sitio?

- | | |
|-------------------------------------|------------------------------------|
| <input type="checkbox"/> Ninguna | <input type="checkbox"/> WEP |
| <input type="checkbox"/> EAP | <input type="checkbox"/> EAP – TLS |
| <input type="checkbox"/> EAP – TTLS | <input type="checkbox"/> PEAP |
| <input type="checkbox"/> VPN | <input type="checkbox"/> RADIUS |
| <input type="checkbox"/> WPA | <input type="checkbox"/> 802.1x |
| <input type="checkbox"/> 802.11i | <input type="checkbox"/> Firewall |

Otra: Filtrado MAC

Hay otras organizaciones cercanas usando WLAN?

- Si No

Hay fuentes de interferencia?

- Si No

Fuente 1: Red 802.11b del proyecto EHAS

Diseño

Información sobre la red inalámbrica a instalar.

Tipo de ambiente

- Interior Exterior

Si es interior, que clase es?

- | | | |
|--------------------------------------|----------------------------------|--|
| <input type="checkbox"/> Hospital | <input type="checkbox"/> Almacén | <input type="checkbox"/> Oficina |
| <input type="checkbox"/> Residencial | <input type="checkbox"/> Fábrica | <input checked="" type="checkbox"/> Campus Universitario |

Otro: _____

Si es exterior, que clase de conexión es? Y cuál es la distancia?

- Punto – punto : _____
- Punto – multipunto: hasta 100 metros

Hay planos de las instalaciones?

- Si No

Existían planos de las instalaciones (desactualizados) pero no en versión digital, no existía un plano del parque de Ingenierías.

Hay mapas topológicos de la red actual?

- Si No

Qué tipo de aplicaciones serán usadas en la WLAN?

- Voz Video FTP
 HTTP Telnet SSH
 POP/SMTP Acceso a base de datos Mensajería instantánea
Otros _____

Qué tipo de equipos cliente serán usados?

- Computadores portátiles Computadores de escritorio
 PDAs Otros: _____

Cuántos clientes usarán la red inalámbrica? Hasta 1140 usuarios

El número de clientes se obtiene de el máximo número de usuarios por AP (60) multiplicado por el número de APs (19).

Tipo de red cableada existente:

- Cable coaxial Thinnet Cable coaxial Thicknet
 Par trenzado sin blindaje (UTP) Par trenzado sin blindaje (UTP)
 Fibra óptica Otro: _____

Por medio de que dispositivo los APs se conectan?

- Switches Concentradores

Hay suficientes puertos para acomodar los APs?

- Si No

Existen 813 puertos en switches y en concentradores, de este número solamente se usarán 19 para la conexión de los APs.

Qué tipo de fuente de potencia usan los APs?

- AC PoE

Qué subred será asignada a la WLAN?

- Privada Pública

Debido a que la red de la universidad es una red pública y utiliza el rango de direcciones 172.16.X.X se utilizará este. Se necesitan direccional máximo 1140 clientes y 19 APs lo que da un total de 1159 direcciones IP, estas se pueden conseguir con 5 rangos de direcciones. Para efectos de diseño se recomiendan usar las direcciones 172.16.100.X, 172.16.101.X, 172.16.102.X, 172.16.103.X y 172.16.104.X.

Cómo será gestionada la red?

- SNMP HTTP / HTTPS
 Telnet Consola
 Aplicación propietaria

Otras: _____

Qué tipo de tecnología es la más adecuada para las instalaciones?

- 802.11 802.11b
 802.11a 802.11g

Otra: _____

Que clase de seguridad es la más adecuada?

- Ninguna WEP
 EAP EAP – TLS
 EAP – TTLS PEAP
 VPN RADIUS
 WPA 802.1x
 TKIP Firewall
 802.11i Otra: _____

Información sobre el AP

Las características del AP deberán ser tomadas para cada uno de los APs resultantes del diseño, como ejercicio solo se hará para un solo AP. No se hará énfasis en marcas de equipos, solamente en sus características funcionales.

Nombre del AP: Bienestar

Ubicación del AP: División de salud integral

Dirección IP: 172.16.101.60

Canal:

- 1 2 3 4 5 6 7 8 9
 10 11 12 13 36 40 44 48 52
 56 60 64 149 153 157 161

Modo de operación del AP:

- Modo raíz Modo no raíz Modo repetidor

Tipo de AP instalado

- 802.11 802.11b
 802.11a 802.11g

Otra: _____

Tipo de conexión a la red existente

- Concentrador 10baseTx Concentrador 100baseTx
 Switch 10baseTx Switch 100baseTx
 Switch 10/100baseTx Switch 10/100baseFx
 Switch 10/100/1000baseTx Otro: _____

Información del Switch / concentrador al cual el AP está conectado

Referencia / marca: Concentrador 3COM

Nombre / ubicación: Centro de cableado 9

Número de puerto: 3

Velocidad de datos

- 1 Mbps 2 Mbps 5.5 Mbps 11 Mbps
 6 Mbps 9 Mbps 12 Mbps 18 Mbps
 24 Mbps 36 Mbps 48 Mbps 54 Mbps

Propietaria: _____

Potencia de salida

- | | | | |
|---|---------------------------------|---------------------------------|---------------------------------|
| <input type="checkbox"/> 1 mW | <input type="checkbox"/> 2 mW | <input type="checkbox"/> 5 mW | <input type="checkbox"/> 10 mW |
| <input checked="" type="checkbox"/> 20 mW | <input type="checkbox"/> 32 mW | <input type="checkbox"/> 40 mW | <input type="checkbox"/> 50 mW |
| <input type="checkbox"/> 64 mW | <input type="checkbox"/> 100 mW | <input type="checkbox"/> 200 mW | <input type="checkbox"/> 500 mW |
| <input type="checkbox"/> 1 W | Otro: _____ | | |

Información adicional

Tipo de antena y ganancia: antena tipo dipolo ganancia 2.2 dBi

Cable *pigtail* : no

Cable de potencia AC: si

Inyector PoE: no

Supresor de transientes: no

Conectores y cable RF: no

Tipo de montaje: techo

5.8 CÁLCULO DE LA INVERSIÓN

Siempre que se hable de alguna tecnología se debe tener en cuenta el presupuesto. El desarrollo de las tecnologías de la información y comunicaciones está determinado por el impacto que estas puedan tener en el mercado. Al aumentar el consumo, se aumentará la calidad de los productos, acelerando el desarrollo de aplicaciones y por ende el desarrollo económico. Las redes inalámbricas no son ajenas a esta situación. En los últimos años se ha visto como la venta de equipos 802.11 ha aumentado año tras año, beneficiando la adopción de esta tecnología en ambientes corporativos, públicos y caseros; lo anterior gracias al desarrollo tecnológico y a la fuerte competencia en el mercado.

5.8.1 Beneficios directos: son aquellos beneficios que son fácilmente cuantificables y medibles en términos monetarios, tales como ahorros y ganancias. Los beneficios directos en una WLAN son:

Ahorro de tiempo: los empleados disfrutan de un tiempo de respuesta más rápido. Por ejemplo, son capaces de responder un correo electrónico más rápido, o colaborar para una información en un servidor centralizado. Adicionalmente, mientras los trabajadores se movilizan de lugar en lugar, no tienen que desconectar o reiniciar sus PCs lo cual se traduce en ahorro de tiempo.

Incremento en la productividad: gracias a la conexión en cualquier lugar los usuarios realizan más trabajo, generando un aumento en la productividad y en el aprendizaje.

5.8.2 Beneficios indirectos: pueden ser los más importantes y son los más difíciles de cuantificar, son aquellos beneficios que resultan de la aplicación de la tecnología y que se traducen en un aumento en la productividad de los usuarios finales y finalmente en dinero. Los beneficios más importantes del uso de una red inalámbrica son:

Aumento de la capacidad de usuarios: la implementación de una red inalámbrica permite que un mayor número de personas accedan a la red, pueden conectarse cientos de estudiantes a la vez de forma rápida y eficiente. Se aumenta la capacidad de la red, ya que los estudiantes y profesores pueden traer sus equipos y utilizarlos en la Universidad.

Facilidad de instalación: la instalación de una red inalámbrica es mucho más rápida comparada con la instalación de una red cableada, por lo tanto se reduce el esfuerzo de instalación.

Flexibilidad: cuando se crea una red cableada, la ubicación de los puntos de red son ubicados de acuerdo al número de computadores que posiblemente se ubiquen en cada uno de las habitaciones, lo anterior limita automáticamente la ubicación de los escritorios. En caso de necesitar nuevos puntos de red se incrementa el costo de la red, esto es una situación muy común ya que cambia la forma como el espacio es usado. En una red inalámbrica esta situación es diferente, la ubicación de los escritorios es más flexible, con lo cual se consigue un uso más eficiente del espacio, en caso de necesitar mayor capacidad de usuarios en cierta habitación, la instalación es rápida y menos costosa.

Extender cubrimiento a nuevas ubicaciones: un usuario puede estar en cualquier lugar y estos lugares pueden no haber sido cableados, por ejemplo corredores, cafeterías y exteriores. Con una

WLAN se aumenta la cobertura de la red, a aquellos sitios donde la red cableada no llega. El usuario puede conectarse desde cualquier punto a internet o a la intranet de la Universidad y trabajar en red. Una red inalámbrica también es ideal para redes dentro de edificios históricos, ya que no se requiere perforar paredes, colocar canales a lo largo de las paredes, etc.; conservando la arquitectura del edificio intacta.

Incremento de la colaboración: los usuarios no tienen que reunirse cerca de un punto de red o competir por los dos que normalmente están disponibles en los salones de reunión, con una red inalámbrica pueden trabajar en cualquier área e inclusive, en la cafetería. Además, se pueden compartir archivos en el momento que se requiera.

Incremento en la conectividad: al contar con una WLAN los usuarios finales se conectan más minutos por día comparado a tener solo una red cableada. Ya no se está supeditado a los horarios de las salas de cómputo.

Facilidad de acceso: ya que se elimina la utilización de cables, no se requiere buscar un punto de conexión a la red cableada.

Portabilidad: WLAN también hace que las adiciones, mudanzas y cambios sean implementados de una manera mucho más simple. Permitiendo fácilmente crear oficinas y redes temporales, por ejemplo en caso de necesitarse una red de manera temporal en un auditorio se puede trasladar un AP hasta el sitio de manera rápida. Cuando se hacen cambios en el edificio, como es el caso de una construcción, se puede mover la red fácilmente.

Movilidad y libertad: los usuarios son libres de trabajar a cualquier hora y desde cualquier lugar de la universidad, el acceso a la red se consigue desde sitios diferentes a las salas de cómputo y oficinas. También existen muchas actividades humanas que requieren movilidad, por ejemplo el personal de un hospital o un almacén; en estas actividades el acceso a la información al instante, minimizando los errores y sacando el mejor beneficio de la red inalámbrica.

Alta satisfacción del empleado: gracias a los anteriores beneficios los trabajadores se vuelven más productivos y se motivan mucho más.

Mejor imagen corporativa: aumenta la ventaja competitiva debido a que la organización aumenta el nivel de conectividad y participación en la nueva economía. Para una Universidad, permite incrementar su calidad, lo cual atraerá nuevos integrantes.

5.8.3 Costos directos: los costos directos son aquellos normalmente conocidos y que implican un gasto económico. Los elementos que inciden en los costos directos son: software, hardware, soporte y administración.

Costos de software: incluye el precio de compra de licencias, así como las actualizaciones sucesivas.

Costos de hardware: incluye los costos de compra de los equipos y los costos de las actualizaciones que se le haga al mismo.

Costos de soporte: incluye los costos por instalación, mantenimiento, solución de problemas. Estos costos pueden ser internos (realizados por personal de la organización) o externos (contratados a una empresa exterior).

Costos de administración: incluye los costos por gestión del proyecto, desarrollo del sistema, administración del sistema, etc..

Tabla 23. Costos directos en una WLAN.

Costo	Ejemplos
Hardware	APs. Tarjetas de interfaz de red inalámbrica.
Software	SW de seguridad, SW para VPN. Planeación de red.
Soporte	Instalación y configuración de APs. Habilitar seguridad.
Administración	Políticas de mantenimiento para una WLAN

5.8.4 Costos indirectos: son aquellos costos que no están relacionados con la implantación de la tecnología, sino con la aplicación de esta. Los costos indirectos son difíciles de cuantificar en términos monetarios, pueden aparecer en mayor o menor medida a lo largo de la vida de la tecnología, siendo por lo general bastante difíciles de identificar y calificar. Algunos ejemplos de costos indirectos son el tiempo fuera de servicio y el factor *Futz*.

El tiempo fuera de servicio es el tiempo en que una tecnología deja de funcionar, lo cual es muy difícil de predecir. El factor *Futz* indica el tiempo de pérdida en un puesto de trabajo por el uso de las nuevas tecnologías en beneficio propio, uso del correo electrónico, internet, etc..

Debido a que la Universidad del Cauca fue creada sin ánimo de lucro para favorecer a la sociedad y no para generar ganancia, parte de los beneficios que se obtengan del desarrollo de las actividades de la Universidad deben ser destinadas a ella para que pueda seguir desarrollando sus actividades a favor de la sociedad, por lo tanto para el análisis financiero del diseño de la red inalámbrica se tendrá en cuenta únicamente la contribución de los costos.

El costo de los equipos depende de las características de ellos, entre más funcionalidades, respaldo, calidad, etc., los costos se irán incrementando.

5.8.5 Costo de la red inalámbrica: en la siguiente tabla se resumen los costos de la red inalámbrica, solamente se tendrá en cuenta la inversión en hardware como APs, antenas, carcasas y cables. Dependiendo de los fabricantes se tienen unos rangos de precios para cada uno de los elementos necesarios para implementar la red inalámbrica para el Campus de Ingenierías de la Universidad del Cauca.

Tabla 24. Costo de la red inalámbrica.

Elemento	Cantidad	Rango de precios (Pesos)	Rango total (Pesos)
Access Point 802.11g	19	100.000 – 1'600.000	1'900.000 – 30'400.000
Antena direccional	1	75.000 – 350.000	75.000 – 350.000
Carcasas para el techo	19	330.000 – 1'000.000	6'270000 – 19'000000
Cable adaptador	1	60.000 – 90.000	60.000 – 90.000
Extensiones eléctricas 5 metros	19	5.000	95.000
Cable Ethernet 5 metros	1	8.000	8.000
Cable Ethernet 10 metros	4	13.000	52.000
Cable Ethernet 15 metros	5	20.000	100.000
Cable Ethernet 20 metros	2	23.000	46.000
Cable Ethernet 30 metros	2	27.000	54.000
Cable Ethernet 50 metros	5	35.000	175.000
TOTAL			8'835.000 – 50'370.000

A la hora de comprar los APs se debe tener en cuenta lo siguiente:

- *Tecnología:* la oferta de APs varía según la tecnología, sin embargo en el mercado existe gran cantidad de equipos. En el diseño se escogió la tecnología 802.11g.
- *Posibilidad de mejora:* como los estándares para redes inalámbricas evolucionan rápidamente, es importante que los APs incluyan la posibilidad de mejora por medio de *firmware*, por tal motivo es importante buscar un proveedor que respalde la compra.
- *Garantía:* es una característica que indica el respaldo que tiene la compra.
- *Seguridad:* es importante que el AP soporte los últimos adelantos en cuanto seguridad y en caso de que no los tenga, que ofrezca la capacidad de implementarse mediante *firmware*, esta característica puede ser útil por ejemplo para los APs que desean actualizarse a 802.11i.
- *Interoperabilidad:* para garantizar interoperabilidad se recomienda escoger productos con certificación Wi-Fi, lo cual permite la interoperabilidad entre fabricantes.
- *Funcionalidad:* es necesario comprar APs con las funciones necesarias, muchos APs incluyen funcionalidad de enrutamiento, *firewall*, etc.. En el caso del diseño, no se hace necesario la implementación de APs con funcionalidades de enrutamiento ya que otros elementos en la red ya cumplen esta función, tampoco es necesario el uso de DHCP ya que cada cliente contará con una dirección IP única dentro de la red.
- *Precio:* es muchas veces el factor que incide más en la escogencia de equipos, el costo del AP varía a medida que este incluya mayores funcionalidades y mayor respaldo.
- *Disponibilidad:* se debe chequear la disponibilidad del equipo escogido, ya que a veces están descontinuados o en el caso de los modelos recientes son más difíciles de conseguir.
- *Herramientas de configuración:* se debe buscar un AP que proporcione varias alternativas de configuración, entre las que se encuentran Telnet, HTTP o una aplicación propietaria.
- *Potencia de transmisión:* elegir APs con las potencias determinadas en el diseño, o sea 13 dBm (20mw) y 15 dBm (32mw).
- *Antenas:* buscar APs con antenas omnidireccionales tipo dipolo ya que este tipo de antena fue la base para el diseño. Una característica importante es que además permitan ser desmontables, esto último proporciona flexibilidad. Para el caso del AP que proporciona servicio al parque, se sugiere una antena tipo panel cuyo lóbulo de radiación horizontal esté entre 65° y 85°.
- *Regulación:* comprar equipos que no violen las regulaciones del país.

CONCLUSIONES

El desarrollo del proyecto nos permitió la integración de diferentes conocimientos adquiridos en las asignaturas cursadas a lo largo de la carrera, conceptos de propagación, antenas, modulación, multiplexación, redes de computadores, seguridad en redes, gestión de proyectos, etc..

Se realizó un trabajo interdisciplinario ya que nos permitió integrar y conocer conceptos ajenos al programa de Ingeniería Electrónica y Telecomunicaciones, interactuando con profesionales de diferentes áreas del conocimiento tales como arquitectos, ingenieros civiles, contadores públicos, administradores de empresas, ingenieros de sistemas, comerciantes internacionales; la interrelación con todos y cada uno de ellos aportó al buen desarrollo del proyecto.

El éxito del resultado fue debido a la labor conjunta del equipo de trabajo, ya que se adquirió una disciplina para cumplir con las expectativas de los objetivos planteados.

Se profundizó en el estudio de las normas IEEE 802.11a, 802.11b y 802.11g, lo que permitió analizar las características de cada una de ellas, para finalmente escoger la más adecuada a los requerimientos establecidos.

Gracias a la motivación se logró obtener el estado del arte sobre redes inalámbricas, así como tecnologías de punta en software y hardware de aplicación para el diseño de este tipo de redes.

El presente trabajo sirvió para tener una visión sobre el rumbo de la tecnología inalámbrica, lo que nos permite predecir un futuro con gran demanda de soluciones inalámbricas. Lo anterior se soporta en la madurez tecnológica alcanzada y la cantidad de ofertas en el mercado, producto de una demanda de movilidad por parte del público, característica que no es ofrecida por las redes cableadas, por lo tanto las redes inalámbricas en el futuro tendrán mayor acogida que las redes cableadas.

El estudio de las redes de área local inalámbrica nos permitió conocer sus ventajas tales como: ahorro de tiempo, incremento de la productividad, facilidad de instalación, flexibilidad, posibilidad de extender el cubrimiento, facilidad de acceso, portabilidad, movilidad, bajos costos de implementación y mantenimiento.

Se hizo confrontación entre la teoría y la práctica, al hacerse primero un estudio de los modelos de propagación y su simulación con herramientas software, y posteriormente haciendo un ejercicio práctico para finalmente concluir cual era el modelo más acertado para el Campus de Ingenierías, sin embargo, esto no implica que este modelo sea el más adecuado para todos los ambientes ya que sus características difieren de un sitio a otro, lo que implica que cada diseño varía dependiendo de estas, convirtiéndose en un reto para el diseñador.

En las redes cableadas los datos viajan a través del cable, mientras que en las redes inalámbricas estos se esparcen a través de un medio tan variable como lo es el espacio libre, debido a que las ondas se pueden encontrar con obstáculos tanto fijos como móviles, lo que conlleva a cambios de trayectoria, atenuaciones, de modo que el diseño es complejo y es muy difícil determinar con precisión el comportamiento de una red inalámbrica y aún mas en el caso donde se presentan interferencias, ya que se está usando el fenómeno de radiación y además otras tecnologías están utilizando la misma frecuencia.

Se creó un modelo para el diseño de redes inalámbricas consistente en una serie de pasos que puede ser adaptado en cualquier tipo de ambiente. Este modelo dio respuesta efectiva al diseño de la red inalámbrica para el Campus de Ingenierías de modo que sirve como orientación para ser usado en otros edificios de la Universidad.

Gracias al uso de la herramienta de simulación, se pudo analizar la propagación de la señal en el Campus para poder escoger la mejor ubicación de los equipos y a partir de su análisis llegar a conclusiones determinantes a la hora de la implementación de la red inalámbrica.

El diseño de la red inalámbrica para el Campus de Ingenierías permitió sentar las bases para su implementación ya que según lo arrojado por el estudio financiero es viable, si se tiene en cuenta que la inversión es mínima frente a los grandes beneficios de los que puede gozar la comunidad académica mediante su implementación.

RECOMENDACIONES

La gran debilidad de una red inalámbrica 802.11 es su seguridad debido a la accesibilidad al medio inalámbrico, se recomienda que se haga un estudio detallado de la norma 802.11i y de las soluciones propietarias que resuelven estas falencias.

Continuar con el estudio de los próximos normas IEEE de la familia 802.11, tales como: 802.11e, 802.11n, 802.11r, 802.11s. 802.11e que permitirá calidad de servicio para las transmisiones de audio y video. 802.11n que permitirá a las redes manejar velocidades superiores a 100 Mbps. 802.11r cuya idea principal es manejar un “traspaso rápido” cuando un cliente inalámbrico realiza *roaming* entre varios APs de la misma WLAN. 802.11s que permitirá la configuración de las redes en malla, en estas redes los dispositivos inalámbricos tienen capacidades de enrutamiento, en pocas palabras son redes Ad hoc. También el grupo de trabajo 802.11 está buscando futuras normas para usar en vehículos en movimiento, probablemente será la norma 802.11p y para la predicción de desempeño inalámbrico la norma 802.11t.

Las investigaciones en esta área deben estar dirigidas fundamentalmente al logro de una mayor eficiencia de los métodos de acceso contribuyendo al aumento de la capacidad en cuanto al número de usuario, y al aumento de la velocidad mediante aumento en la potencia de los equipos, sensibilidad en los receptores y códigos correctores de error.

BIBLIOGRAFÍA

IEEE Std. 802.11, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. IEEE, 1999. Available from Internet: <URL: <http://standards.ieee.org/getieee802/download/802.11-1999.pdf>>

IEEE Std. 802.11a, Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band. IEEE, 1999. Available from Internet: <URL: <http://standards.ieee.org/getieee802/download/802.11a-1999.pdf>>

IEEE Std. 802.11b, Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-speed Physical Layer Extension in the 2.4 GHz Band. IEEE, 1999. Available from Internet: <URL: <http://standards.ieee.org/getieee802/download/802.11b-1999.pdf>>

IEEE Std. 802.11g, Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Further Higher Data Rate Extension in the 2.4 GHz Band. IEEE, 2003. Available from Internet: <URL: <http://standards.ieee.org/getieee802/download/802.11g-2003.pdf>>

COST 231. Digital mobile radio towards Future generation systems. COST 231 Final Report. 1999. Available from Internet: <URL: <http://www.lx.it.pt/cost231/>>

AFIFI, Hossam and ZEGHLACHE, Djamel. Applications & Services in Wireless Networks. Kogan Page, 2003. ISBN: 1903996309.

ARNESEN, Stig and HÅLAND, Kjell. Modelling of coverage in WLAN. Noruega, 2001. Tesis de postgrado (Information and Communication Technology). Agder University College.

AKIN, Devin et al. CWNA Certified Wireless Network Administrator Official Study Guide (Exam PW0-100). McGraw-Hill, 2002. ISBN: 0971605726

BARKEN, Lee. How Secure Is Your Wireless Network? Safeguarding Your Wi-Fi LAN. Prentice Hall PTR, 1ed, 2003. ISBN: 0131402064

DUMBILL, Edd; JEPSON, Brian and WEEKS, Roger. Linux Unwired. O'Reilly, 2004. ISBN : 0596005830.

ESMAILZADEH, Riaz and NAKAGAWA, Masao. TDD-CDMA for Wireless Communications. Artech House, 2002. ISBN: 158053371X.

FLICKENGER, Rob. Building Wireless Community Networks. O'Reilly, 2ed, 2003. ISBN : 0596005024.

FULLER, Ron and BLANKENSHIP, Tim. Building a Cisco Wireless LAN. Syngress, 1ed, 2002. ISBN: 192899458X.

GAST, Matthew. 802.11 Wireless Networks: The Definitive Guide. O'Reilly, 1ed, 2002. ISBN: 0596001835.

HURLEY, Chris et al. WarDriving: Drive, Detect, Defend: A Guide to Wireless Security. Syngress, 2004. ISBN: 1931836035.

JANEVSKI, Toni. Traffic Analysis and Design of Wireless IP Networks. Artech House, 2003. ISBN: 1580533310.

MAUFER, Thomas. A Field Guide to Wireless LANs for Administrators and Power Users. Prentice Hall PTR, 2003. ISBN : 0131014064.

MULLER, Nathan. LANs to WANs: The Complete Management Guide. Artech House, 2003. ISBN: 1580535720.

MUKHERJEE, Amitava et al. Location Management and Routing in Mobile Wireless Networks. Artech House, 2003. ISBN: 1580533558.

NICHOLS, Randall and LEKKAS, Panos. Wireless Security: Models, Threats, and Solutions. McGraw-Hill; 1ed, 2002. ISBN: 0071380388.

OHRTMAN, Frank and ROEDER, Konrad. Wi-Fi Handbook: Building 802.11b Wireless Networks. McGraw-Hill, 2003. ISBN: 0071412514.

PATIL, Basavaraj et al. IP in Wireless Networks. Prentice Hall PTR, 2003. ISBN : 0130666483.

PEIKARI, Cyrus and FOGIE, Seth. Maximum Wireless Security. Sams Publishing, 2002. ISBN : 0672324881.

PRASAD, Ramjee and MUÑOZ, Luis. WLANs and WPANs towards 4G Wireless. Artech House, 2003. ISBN: 1580530907.

_____ and RUGGIERI, Marina. Technology Trends in Wireless Communications. Artech House, 2003. ISBN: 1580533523.

RAISANEN, Antti and LEHTO, Arto. Radio Engineering for Wireless Communication and Sensor Applications. Artech House, 2003. ISBN: 1580535429.

SHEMA, Mike and JONSON Bradley. Anti-Hacker Tool Kit. McGraw-Hill, 2ed, 2004. ISBN: 0072230207.

STAVROULAKIS, Peter. Interference Analysis and Reduction for Wireless Systems. Artech House, 2003. ISBN: 1580533167.

WHEAT, Jeffrey et al. Designing a Wireless Network. Syngress, 1ed, 2001. ISBN: 1928994458.

<http://www.ieee.org>

<http://www.wi-fi.org>

<http://www.wlana.org>

<http://www.mincomunicaciones.gov.co>

<http://www.itu.int>

<http://www.awe-communications.com>

<http://www.gsr.unican.es>

<http://www.wirelessvalley.com>

<http://www.cisco.com>

<http://www.intel.com>

<http://www.trapezenetworks.com>

<http://www.computerworld.com>

<http://www.nwc.com>

<http://www.nwfusion.com>

<http://www.pcmag.com>

<http://www.wirelessweek.com>

<http://www.bitpipe.com>

<http://www.wi-fiplanet.com>

<http://www.swisswireless.org>

<http://www.sss-mag.com>