



UNIVERSIDAD AUTÓNOMA DEL  
ESTADO DE MÉXICO  
CENTRO UNIVERSITARIO UAEM TEXCOCO

“SIMULACIÓN DE DISEÑO DE UNA RED MESH APLICADA AL  
PARQUE TEMÁTICO MUNICIPAL LAS FUENTES”

T E S I S

QUE PARA OBTENER EL TÍTULO DE  
LICENCIADO EN INFORMÁTICA ADMINISTRATIVA

P R E S E N T A N

JORGE GUIDO RAMÍREZ  
RODOLFO GUIDO RAMÍREZ

DIRECTOR

ING. JOSÉ ROBERTO RAMÍREZ CERVANTES

REVISORAS

M en C.A. YEDID ERANDINI NIÑO MEMBRILLO  
M. en C. C. MINERVA REYNA IZAGUIRRE

TEXCOCO, ESTADO DE MÉXICO, JULIO 2015

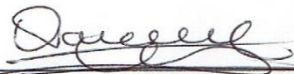
Texcoco, Mex. A 12 de Junio 2015.

M. EN C.E. VIRIDIANA BANDA ARZATE  
SUBDIRECTORA ACADEMICA DEL  
CENTRO UNIVERSITARIO UAEMTEXCOCO.  
PRESENTE:

AT'N LIC. EN I. A. CINTHYA A TERESITA ISLAS RODRIGUEZ  
RESPONSABLE DEL DEPARTAMENTO DE TITULACION

Con base en las revisiones efectuadas al trabajo escrito titulado "Simulación de Diseño de una Red Mesh aplicada al parque temático municipal las Fuentes" que para obtener el título de Licenciado en **Informática Administrativa** presenta el sustentante **Guido Ramírez Jorge y Guido Ramírez Rodolfo**, con número de Cuenta **1024628** y **1024630** respectivamente, se concluye que cumple con los requisitos teorico-metodologicos por lo que se lo otorga el voto aprobatorio para su sustentación, pudiendo **continuar con la etapa de digitalización** del trabajo escrito.

ATENTAMENTE



M en C.A. YEDID ERANDINI NIÑO MEMBRILLO

REVISOR

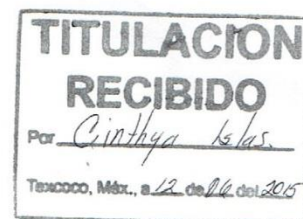


M. en C. C. MINERVA REYNA IZAGUIRRE

REVISOR



ING. JOSÉ ROBERTO RAMÍREZ CERVANTES  
DIRECTOR



## DEDICATORIA

A mis padres

Por su amor, trabajo y sacrificios en todos estos años, gracias a ustedes hemos logrado llegar hasta aquí y convertirnos en lo que somos. Ha sido un privilegio ser sus hijos son los mejores padres.

A mi hermana

Dedico de manera especial a mi hermana Alejandra pues ella fue el principal cimiento de mi vida profesional, sentó las bases de responsabilidad y deseos de superación, en ella tengo el espejo en el cual me quiero reflejar pues sus virtudes infinitas y su gran corazón me llevan a admirarlas cada día más.

## **AGRADECIMIENTOS**

### A nuestras revisoras

Yedid Erandini Niño Membrillo, Por la sabiduría que nos dio y el tiempo que empleo, que sin su ayuda y conocimientos no hubiese sido posible realizar este proyecto.

Minerva Reyna Izaguirre, Por impulsarnos a pensar en grande, ya que con sus acertadas y objetivas observaciones fueron fundamentales para la concreción de este trabajo.

### A nuestro director

José Roberto Ramírez Cervantes, Por su apoyo durante el proyecto, la orientación y el seguimiento de este trabajo, sin el cual no hubiera sido posible esta meta.

### A nuestro profesor

Josué Vicente Cervantes Bazán, Por sus valiosas aportaciones que enriquecieron este trabajo de investigación.

# ÍNDICE GENERAL

Introducción.....	1
Planteamiento del Problema.....	3
Justificación.....	4
Objetivos.....	5
Hipótesis.....	6
<b>Capítulo 1 Introducción.....</b>	<b>7</b>
1.1 Onda de radio .....	8
1.1.1 La señal.....	9
1.1.2 Frecuencia.....	9
1.1.3 Amplitud.....	10
1.2 Polarización.....	10
1.2.1 Polarización lineal.....	11
1.2.2 Polarización circular.....	11
1.2.3 Polarización elíptica.....	11
1.2.4 Polarización por reflexión.....	12
1.2.5 Polarización por refracción.....	13
1.3 Espectro electromagnético.....	13
1.3.1 División del espectro electromagnético.....	14
1.3.2 Frecuencias FR.....	15
1.4 Características físicas de la señal.....	16
1.4.1 Ancho de banda.....	16
1.4.2 Frecuencia.....	18
1.4.3 Potencia de señal.....	19

1.4.4 Ganancia.....	20
1.4.5 Decibelio.....	20
1.4.6 Atenuación.....	21
1.4.7 Perdida de propagación.....	21
1.4.8 Dirección de propagación.....	22
1.5 Medios de transmisión guiados.....	23
1.5.1 Fibra óptica.....	24
1.5.2 Par trenzado.....	25
1.5.3 Cable coaxial.....	27
1.5.4 Redes cableadas.....	29
1.6 Medios de transmisión no guiados.....	30
1.6.1 Microondas.....	30
1.6.2 Ondas.....	32
1.6.3 Redes inalámbricas.....	32
<b>Capítulo 2 Redes inalámbricas.....</b>	<b>34</b>
2.1 Introducción.....	35
2.1.1 Historia y actualidad.....	37
2.1.2 Ventajas de las redes inalámbricas.....	39
2.2 Elementos de las redes inalámbricas.....	40
2.2.1 Dirección Ip.....	41
2.2.2 Mascara de subred.....	42
2.2.3 Puerta de enlace.....	43
2.2.4 Servidores DNS.....	43
2.2.5 SSID ( <i>Service Set Identification</i> ).....	44
2.2.6 DHCP.....	45

2.2.7 Dirección MAC.....	45
2.3 Hardware para redes inalámbricas.....	46
2.3.1 Modem ADSL.....	47
2.3.2 Conmutador ( <i>Switch</i> ).....	48
2.3.3 Encaminador ( <i>Router</i> ).....	49
2.3.4 Puente ( <i>Bridge</i> ).....	50
2.3.5 Pasarela ( <i>Gateway</i> ).....	51
2.3.6 Cortafuegos ( <i>Firewalls</i> ).....	52
2.3.7 Puntos de Acceso ( <i>Access Point</i> ).....	53
2.3.8 Adaptadores de red.....	55
2.3.9 Antena direccional y omnidireccional.....	58
2.4 Clasificación de las redes inalámbricas.....	59
2.4.1 Redes inalámbricas de área personal (WPAN).....	61
2.4.1.1 <i>Bluetooth</i> .....	61
2.4.1.2 DECT.....	63
2.4.1.3 Infrarrojo.....	64
2.4.2 Redes inalámbricas de área local (WLAN).....	64
2.4.2.1 WiFi.....	65
2.4.2.1.1 Redes WiFi de área extensa.....	67
2.4.2.2 HomeRF.....	69
2.4.2.3 HiperLAN.....	70
2.4.3 Redes inalámbricas de área metropolitana (WMAN).....	70
2.4.3.1 LMDS.....	71
2.4.3.2 WiMax.....	72
2.4.4 Redes inalámbricas globales (WWAN).....	73

2.4.4.1 GSM.....	73
2.4.4.2 GPRS.....	74
2.4.4.3 UMTS.....	75
2.4.4.4 HSDPA.....	76
2.5 Tipos de conmutación.....	77
2.5.1 Difusión ( <i>Broadcast</i> ).....	77
2.5.2 Conmutación de circuitos.....	77
2.5.3 Conmutación de paquetes.....	77
2.5.4 <i>Frame Relay</i> (Retransmisión de marcos).....	77
2.6 Protocolos de comunicaciones IEEE 802.11.....	78
2.6.1 IEEE 802.11 <sup>a</sup> .....	78
2.6.2 IEEE 802.11b.....	79
2.6.3 IEEE 802.11g.....	79
2.6.4 IEEE 802.11n.....	80
2.6.5 IEEE 802.11h.....	81
2.7 Métodos de autenticación del estándar 802.11.....	82
2.7.1 Autenticación <i>Open System</i> .....	82
2.7.2 Autenticación <i>Shared Key</i> .....	83
2.8 Seguridad en redes inalámbricas.....	83
2.8.1 Método SSID ( <i>Service Set Identifier</i> ).....	84
2.8.2 Método MAC.....	85
2.8.3 VPN (Red Privada Virtual).....	85
2.8.4 Captive portal.....	85
2.8.5 Método WEP ( <i>Wired Equivalent Privacy</i> ).....	86
2.8.6 Método WPA ( <i>WiFi Protected Access</i> ).....	87



2.8.7 Método WPA-2 y servidor RADIUS.....	87
2.8.8 Proceso de <i>Handoff</i> o <i>Handover</i> .....	89
2.9 Modelo de referencia.....	89
2.9.1 Que es un protocolo.....	90
2.9.2 Modelo OSI.....	90
2.9.3 Modelo TCP/IP.....	92
<b>Capítulo 3 Redes Mesh (Wireless Mesh Network).....</b>	<b>93</b>
3.1 Introducción.....	94
3.1.1 Primera generación.....	95
3.1.2 Segunda generación.....	95
3.1.3 Tercera generación.....	96
3.2 Arquitectura de las Redes Mesh.....	96
3.2.1 Características de las redes Mesh.....	97
3.2.2 Entornos de aplicación.....	98
3.2.3 Técnicas de funcionamiento.....	100
3.2.4 Trafico en la red (balanceo de carga).....	101
3.2.5 Aplicaciones.....	101
3.2.6 Fiabilidad y robustez.....	102
3.2.7 Movilidad (efecto <i>roaming</i> ).....	102
3.2.8 Ataques a las redes Mesh.....	103
3.3 Estándares Mesh.....	103
3.3.1 IEEE 802.11s.....	104
3.3.2 IEEE 802.15.....	104
3.3.3 IEEE 802.16.....	105
3.4 Modos de operación de las redes Mesh.....	106

3.4.1 Red Ad-hoc (IBBS).....	106
3.4.2 Infraestructura (BSS).....	107
3.4.3 Modo hibrido.....	108
3.5 Niveles o capas de las redes Mesh.....	108
3.5.1 Nivel físico.....	108
3.5.2 MAC ( <i>Medium Access Control</i> ).....	109
3.5.3 Nivel de red.....	110
3.5.4 Métrica de los enlaces.....	110
3.5.5 Nivel de transporte.....	111
3.5.6 Calidad de servicio (QoS).....	111
3.6 Redes inalámbrica en malla.....	112
3.6.1 Introducción.....	112
3.6.2 Clasificación de las redes WMN.....	113
3.6.2.1 Redes inalámbricas de clientes en malla.....	113
3.6.2.2 Redes inalámbricas en modo infraestructura.....	114
3.6.2.3 Redes inalámbricas en malla hibrida.....	116
3.7 Algoritmos de enrutamiento en redes inalámbricas.....	117
3.7.1 Elementos de enrutamiento.....	118
3.7.2 Descripción de algoritmos de enrutamiento.....	118
3.7.3 Enrutamiento por la ruta más corta.....	119
3.7.4 Inundación.....	120
3.7.5 Algoritmo Vector-Distancia.....	121
3.7.6 Enrutamiento por estado de alcance.....	123
3.7.7 Enrutamiento jerárquico.....	126
3.7.8 Enrutamiento en redes WMN.....	127

3.7.9 Enrutamiento en red Ad-hoc.....	127
3.8 Clasificación de protocolos de encaminamiento.....	129
3.8.1 Encaminamiento proactivo (Manejo por tablas).....	129
3.8.2 Encaminamiento reactivo (Por demanda).....	129
3.8.3 Encaminamiento híbrido.....	130
3.9 Protocolos de encaminamiento.....	130
3.9.1 OLSR.....	131
3.9.2 BATMAN.....	131
3.9.3 DSDV.....	132
3.9.4 OSPF.....	132
3.9.5 PWRP.....	132
3.9.6 AODV.....	133
3.9.7 BABEL.....	133
3.9.8 DSR.....	133
3.9.9 TORA.....	134
3.9.10 GPSR.....	134
3.9.11 HWMP.....	134
<b>Capítulo 4 Simulación y diseño de la Red Mesh.....</b>	<b>136</b>
4.1 Introducción.....	137
4.1.1 Metodología del proceso de la encuesta.....	137
4.1.2 Criterios para la aplicación de la encuesta.....	138
4.1.3 Determinación del tamaño de la muestra.....	139
4.1.4 Análisis e interpretación de los resultados (Encuesta).....	140
4.2 Características del lugar de estudio.....	144
4.2.1 Introducción.....	144

4.2.2	Ubicación del parque temático las fuentes.....	145
4.2.3	Plano de distribución del parque temático las fuentes.....	146
4.2.4	Areas del parque temático.....	147
4.3	Proveedores de tecnologías Mesh.....	155
4.3.1	BelAir <i>Networks</i> .....	155
4.3.2	Tropos <i>Networks</i> .....	157
4.3.3	Strix <i>Systems</i> .....	159
4.3.4	Cisco <i>Systems</i> .....	162
4.3.5	Aruba <i>Networks</i> .....	164
4.3.6	Elección del proveedor para el desarrollo de la Red Mesh.....	167
4.4	Elementos que integran una red <i>Wireless</i> Mesh.....	168
4.4.1	Servidor DHCP.....	168
4.4.2	Servidor Radius.....	169
4.4.3	Servidor FTP.....	170
4.4.4	Servidor Nos.....	171
4.4.5	Puerta de enlace Gateway.....	172
4.4.6	<i>Access Point</i> .....	172
4.4.7	Router Mesh.....	173
4.5	Estrategias de diseño para las redes en Malla.....	173
4.5.1	Diseño enfocado a la cobertura.....	173
4.5.1.1	Propagación de radio frecuencia.....	174
4.5.1.2	Zonas de cobertura para enlaces de conexión.....	175
4.5.1.3	Posicionamiento adecuado de los <i>Access Point</i> .....	175
4.5.1.4	Factores de una red de infraestructura.....	175
4.5.2	Diseño enfocado a la disponibilidad.....	175

4.5.3 Diseño enfocado al desempeño.....	176
4.5.4 Diseño enfocado a la movilidad.....	177
4.5.5 Diseño enfocado a la seguridad.....	177
4.5.6 Diseño enfocado a la topología.....	177
4.6 Simulación de la Red Mesh.....	178
4.6.1 Ubicación de los <i>Access Point</i> .....	179
4.6.2 Cobertura de los <i>Access Point</i> .....	181
4.6.3 Estado de los enlaces.....	182
4.6.4 Topología Mesh a implementarse en el parque temático.....	183
4.6.5 Herramienta de simulación.....	184
4.6.5.1 Simulador Cisco <i>Packet Tracer</i> .....	184
4.6.5.2 Simulación Cisco <i>Packet Tracer</i> .....	188
4.6.5.3 Configuración del Router Maestro.....	189
4.6.5.4 Configuración del <i>Linksys</i> dependiente (Repetidores)....	193
4.6.6 Direccionamiento IP.....	197
4.6.7 Hardware seleccionado para la Red Mesh en el parque temático.	200
4.6.7.1 Access Point.....	200
4.6.7.2 Controlador de AP.....	202
4.6.7.3 Router <i>AirMesh</i> .....	204
4.6.8 Presupuesto.....	206
<b>Conclusiones y Recomendaciones.....</b>	<b>207</b>
<b>Glosario.....</b>	<b>209</b>
<b>Bibliografía.....</b>	<b>213</b>
<b>Anexos.....</b>	<b>219</b>
<b>Aporte.....</b>	<b>230</b>

## ÍNDICE DE FIGURAS

Figura 0. Colocación de la primera piedra del parque municipal las fuentes.

Figura 1. Distribución de frecuencias.

Figura 2. Polarización electromagnética.

Figura 3. Polarización lineal, circular, elíptica.

Figura 4. Ejemplode polarización por reflexión.

Figura 5. Ejemplo de polarización por refracción.

Figura 6. División del espectro electromagnético.

Figura 7. Canales de frecuencia.

Figura 8. Perdida de propagación de la señal.

Figura 9. Patrones de propagación Omnidireccional y direccional.

Figura 10. Diagrama de clasificación de medios de transmisión.

Figura 11. Estructura de un cable UTP.

Figura 12. Estructura de un cable de fibra óptica.

Figura 13. Cable de par trenzado.

Figura 14. Elementos de un cable tipo par trenzado.

Figura 15. Cable coaxial.

Figura 16. Símbolo de la tecnología *Bluetooth*.

Figura 17. Antenas de conexión vía satélite.

Figura 18. Ondas de trasmisión inalámbricas.

Figura 19. Subcapas de la capa de enlace física.

Figura 20. Símbolo de la alianza de *WiFi*.

Figura 21. Distribución de números IP.

Figura 22. Distribución de un servidor DNS.

Figura 23. *Dynamic Hest Configuration Protocol*.

Figura 24. Ejemplo de una dirección MAC.

Figura 25. Modem ADSL.

Figura 26. Modem y tarjeta de red.

Figura 27. Conmutador (*Switch*).

Figura 28. Diagrama de conexión de red mediante el uso de routers.

Figura 29. Diagrama de uso de un puente.

Figura 30. Esquema de funcionamiento *Gateway*.

Figura 31. Representación simbólica de un *Firewall*.

Figura 32. *Access point Linksys*.

Figura 33. Partes de un *Linksys*.

Figura 34. Interfaz de configuración *Netgear*.

Figura 35. Tarjeta PCMCIA.

Figura 36. Tarjetas de red inalámbricas.

Figura 37. Adaptador de red USB.

Figura 38. Laptop con dispositivo WiFi.

Figura 39. Antena direccional.

Figura 40. Antena omnidireccional.

Figura 41. Esquema de tecnologías.

Figura 42. Dispositivos conectados mediante *Bluetooth*.

Figura 43. Teléfonos celulares con tecnología DECT.

Figura 44. Puntos de acceso y adaptadores inalámbricos.

Figura 45. Esquema representativo de una red de área extensa.

Figura 46. Ventana de configuración.

Figura 47. Interconexión punto a punto.

Figura 48. Símbolo de la tecnología HomeRF.

Figura 49. Símbolo de la tecnología HiperLAN.

Figura 50. Esquema de funcionamiento de la tecnología LMDS.

Figura 51. Símbolo de la tecnología Wimax.

Figura 52. Icono GSM.

Figura 53. Funcionamiento de la tecnología GPRS.

Figura 54. Símbolo de la tecnología UMTS.

Figura 55. Dispositivo USB con funcionamiento HSDPA.

Figura 56. Funcionamiento de la trama MAC.

Figura 57. Estándares y velocidades de la norma 802.11.

Figura 58. Cifrado de datos.

Figura 59. Triangulo de características del método SID.

Figura 60. Proceso de encriptación.

Figura 61. IEEE 802.11.

Figura 62. *Radius Server*.

Figura 63. Modelo de referencia OSI y TCP/IP.

Figura 64. Funcionamiento de una red Mesh.

Figura 65. Esquema de la primera generación de redes Mesh.

Figura 66. Esquema de la segunda generación de redes Mesh.

Figura 67. Esquema de la tercera generación de redes Mesh.

Figura 68. Nodos Mesh.

Figura 69. Red Mesh implementada en un entorno urbano.

Figura 70. Funcionamiento de los nodos de una red Mesh.

Figura 71. Aplicaciones de una red Mesh.

Figura 72. *Wireless Personal Area Network*.

Figura 73. Red en modo Ad-hoc.



Figura 74. Red en modo infraestructura.

Figura 75. Red en modo híbrido.

Figura 76. Icono representativo de QoS.

Figura 77. Topología de una red Mesh

Figura 78. Red Malla en modo cliente.

Figura 79. Nodos que componen la arquitectura Mesh.

Figura 80. Arquitectura de red.

Figura 81. Descubrimiento de rutas.

Figura 82. Ejemplos de métricas.

Figura 83. Teoría de la cuenta hasta el infinito.

Figura 84. Conocimiento de los vecinos.

Figura 85. Ejemplo de medición.

Figura 86. Construcción de la tabla de paquetes.

Figura 87. Clasificación de protocolos de encaminamiento.

Figura 88. Gráfica 1

Figura 89. Gráfica 2

Figura 90. Gráfica 3

Figura 91. Gráfica 4

Figura 92. Gráfica 5

Figura 93. Gráfica 6

Figura 94. Gráfica 7

Figura 95. Toma aérea del parque

Figura 96. Ubicación con *Google Maps*

Figura 97. Plano de distribución del parque

Figura 98. Entrada

Figura 99. Canchas

Figura 100. Gym

Figura 101. Palapas

Figura 102. Juegos

Figura 103. Juegos Infantiles

Figura 104. Juego de playa

Figura 105. Fuentes

Figura 106. Lámpara de vela

Figura 107. Baños

Figura 108. Pista

Figura 109. Juego de ciudad

Figura 110. Renta de autos

Figura 111. Modulo

Figura 112. Carritos

Figura 113. Módulo de vigilancia

Figura 114. Logo de BelAir

Figura 115. Arquitectura de red con hardware Bel Air

Figura 116. Hardware BelAir

Figura 117. Logo de Tropos

Figura 118. Arquitectura de una MetroMesh

Figura 119. Hardware Tropos

Figura 120. Logo Strix

Figura 121. Red Mesh tipo Strix

Figura 122. Hardware Strix

Figura 123. Logo de Cisco

Figura 124. *Hardware Cisco*

Figura 125. AP 1520 Cisco

Figura 126. Logo de Aruba *Networks*

Figura 127. Aruba enrutador MSR 4000

Figura 128. Aruba *router* MST 200

Figura 129. Enrutador MST 1200

Figura 130. Aruba AP-60

Figura 131. Aruba AP- 65

Figura 132. Aruba AP 80M

Figura 133. Propagación de señal WiFi

Figura 134. Desempeño de una red Mesh

Figura 135. Ubicación de Access Point

Figura 136. Cobertura de los Access Point

Figura 137. Enlaces de Transito

Figura 138. Diagrama de Red Mesh a implementarse

Figura 139. Simbología del diagrama de la Red Mesh

Figura 140. Ejemplo de una simulación en Cisco

Figura 141. Logo del *software Cisco Packet*

Figura 142. Simulación de una topología de red

Figura 143. Tipos de conexión disponibles en *Packet Tracer*

Figura 144. Ventana del modo de operación de envió de paquetes

Figura 145. Ejecución de Cisco *Packet Tracer*

Figura 146. Hoja de trabajo Cisco *Packet Tracer*

Figura 147. Conexión entre nube y un *router*.

Figura 148. Interfaz GUI

Figura 149. Interfaz de direcciones

Figura 150. Ventana Detalles de la conexión de red

Figura 151. Simulación de conectividad de un usuario

Figura 152. Interfaz de configuración de una laptop en Cisco *Packet*

Figura 153. Ventana de autenticación

Figura 154. Ventana de *setup*

Figura 155. Establecimiento de máscara de red

Figura 156. Desactivación del DHCP

Figura 157. Esquema de conexión entre *Linksys*

Figura 158. Dispositivo con tarjeta Ethernet

Figura 159. Esquema de conexión entre *Linksys*

Figura 160. Simulación de la Red Mesh adecuada para el parque temático

Figura 161. Clasificación de Direcciones IP

Figura 162. *Access Point 80M*

Figura 163. Controlador de Ap Aruba 2400

Figura 164. Router Aruba AirMesh MSR 2000

Figura 165. Logo Aruba *Networks Mesh*

Figura 166. Interfaz del GNS3

Figura 167. Interfaz del *OPNET MODELER*

Figura 168. Modelos del GNS3

Figura 169. Visualización de cobertura WiFi

Figura 170. Topología de una Red Mesh

Figura 171. Guerrero Chimalli

Figura 172. Hospital Dr. Gustavo Baz

Figura 173. C.U UAEM Texcoco

Figura 174. Municipio de Nezahualcóyotl

Figura 175. Logo *WiFi Hotspot*

Figura 176. Logo WiFi Poste Caliente

Figura 177. Lobo súper sayayin

Figura 178. Palacio Municipal Nezahualcóyotl

Figura 179. Esquema general de la red UAEM Texcoco

Figura 180. Mapa de la ubicación de UAEM Texcoco

Figura 181. Distribución de UAEM Texcoco

Figura 182. Red actual de UAEM Texcoco

Figura 183. Red inalámbrica actual de UAEM Texcoco

Figura 184. Distribución de los laboratorios de computo C.U Texcoco

Figura 185. Plano de control escolar y equipos de cómputo

Figura 186. Computadoras Hp

Figura 187. : Recinto de comunicación principal MDF

Figura 188. *Router Watson SHDSL 2 Pair*

Figura 189. Cisco 2900 Series

Figura 190. Recinto de comunicación secundaria IDF

Figura 191. *Patch panel DP5e*

Figura 192. *Switch 2026*

Figura 193. *Switch Cisco Catalyst 2960 Series*

Figura 194. *Patch panel TC-P48C5E 48 puertos*

Figura 195. *Switch Linksys SRW208p*

Figura 196. Dell *PowerEdge R200 Server*

Figura 197. *Switch D-Link DES-1008ª*

Figura 198. AVAYA IP *Office 500 V2*

Figura 199. AVAYA IP 400 *Phone System*

Figura 200. Convertidor de fibra óptica

Figura 201. Conversor de medios *Fast Ethernet*

Figura 202. *Linksys modem ADSL AM300*

Figura 203. *Access Point Aruba 135*

Figura 204. *Rack* Ubicado en la oficina de RTICS

Figura 205. Controlador de AP Aruba 3200

Figura 206. *Switch Cisco Catalyst 2960 Series*

Figura 207. *Switch Linksys SRW208P*

Figura 208. *Patch Panel DP5e*

## ÍNDICE DE TABLAS

Tabla 1. Frecuencia FR.

Tabla 2. Estructura de la trama 802.3 Ethernet.

Tabla 3. Tecnologías usadas en las redes inalámbricas.

Tabla 4. Tabla comparativa de las tecnologías WPAN, WLAN, WMAN.

Tabla 5. Versiones de la normativa IEEE 802.11.

Tabla 6. Grupos de trabajo del IEEE 802.15.

Tabla 7. Tabla de enrutamiento.

Tabla 8. Distribución de paquetes.

Tabla 9. Tabla de rutas.

Tabla 10. Clasificación de paquetes.

Tabla 11. Especificación del *Access Point*

Tabla 12. Condiciones generales de los AP

Tabla 13. Ubicación de los Puntos de acceso

Tabla 14. Tabla de potencia

Tabla 15. Asignación de direcciones IP

Tabla 16. Cotización de hardware

Tabla 17. Cotización de infraestructura

Tabla 18. Total de cotizaciones

Tabla 19: Especificaciones técnicas del *switch*

Tabla 20. Comparativa entre tecnologías

Tabla 21: Rendimiento y capacidad del controlador MMC-3200

Tabla 22: Especificaciones técnicas de Switch Linksys SRW208P

Tabla 23. Cotización de infraestructura de la red de C.U Texcoco

## INTRODUCCIÓN

Día 15 de octubre de 2014 el Gobierno de Nezahualcóyotl inicia obra de parque temático municipal “Las Fuentes”, ubicado en Avenida Bordo de Xochiaca y Avenida Neza en el municipio de Nezahualcóyotl, como parte del rescate del Bordo de Xochiaca: El alcalde Juan Zepeda Hernández recordó que ese espacio, recuperado por el gobierno municipal, era un lugar donde se vendía combustible, lo cual implicaba un riesgo para los ciudadanos, pues incrementaba la posibilidad de que ocurriera una explosión de grandes magnitudes; “no sólo acabamos con un grave peligro, sino que hoy les estamos entregándoles a los vecinos, para que lo disfruten, un parque de primer nivel, a la altura de las mejores ciudades, como debe ser Nezahualcóyotl”.

El presidente municipal Juan Zepeda dio el banderazo para el inicio de la construcción del parque temático “Las Fuentes” el cual contará con 110 fuentes lúdicas, interactivas, con bruma e iluminación donde niños y jóvenes podrán bañarse; además presentará múltiples espacios, actividades recreativas y deportivas; esto, como parte del rescate del Bordo de Xochiaca, cabe mencionar que el acceso será gratuito.

Zepeda Hernández aseguró que además de ello contará con palapas para que los ciudadanos realicen ahí sus fiesta familiares; también dijo que tendrá una ciudad a escala con un circuito vial en el que se le enseñará a conducir a los niños para fomentar la cultura vial, así como juegos infantiles entre los que destacan saltarines, toboganes, columpios y trepaderos; además de colocación de mobiliario urbano como bancas, postes, botes de basura, aparca bicicletas y señalización.

Juan Zepeda mencionó que también contará con áreas verdes, andadores de concreto, espacios recreativos, gimnasio al aire libre, canchas de fútbol y basquetbol, un área donde los ciudadanos puedan acudir a presenciar espectáculos musicales y artísticos, y un módulo de vigilancia; todo ello, completamente gratis; esto con el objetivo de dignificar la vida cotidiana en todo el municipio.

Cabe señalar que esta obra se construye sobre una extensión de 24 mil metros cuadrados y para ello se realizó una inversión inicial de 50 millones de pesos y se estima que para el mes de febrero del 2015 ya esté concluido y con las puertas abiertas para recibir a los ciudadanos en el cruce de la Avenida Bordo de Xochiaca y Avenida Nezahualcóyotl.

El alcalde informó que el parque municipal Las Fuentes forma parte de un proyecto integral para rescatar el Bordo de Xochiaca que incluye instalación de luminarias tipo vela, plantación de palmeras de diferentes tipos, así como la construcción de banquetas y guarniciones.

De igual forma enfatizó que para una segunda etapa se contempla construir otros dos espacios temáticos, uno de playa y otro de ciudad, para que de esta forma los ciudadanos cuenten con áreas dignas y gratuitas donde puedan acudir a divertirse. El munícipe recordó que la zona fue olvidada por muchos años y que ahora con el rescate de espacios públicos, se ha logrado recuperar esta área; tal y como se proyecta rescatar al menos 70 espacios más, en los cuales se fomentará la cultura, el deporte, las artes, la integración familiar y el fortalecimiento del tejido social.

Zepeda Hernández también agradeció a la diputada Federal Juana Bonilla por gestionar recursos en favor de Nezahualcóyotl, pues parte de ellos serán invertidos en este parque, el cual recibirá también inversión municipal. Por su parte el director de Obra Pública y Desarrollo Urbano del municipio de Nezahualcóyotl Valentín Díaz Robles, señaló que esta es una primera etapa de la rehabilitación de todo el Bordo de Xochiaca y específico que la fuente que se construirá será seca, tendrá la figura del coyote y contará con la más alta tecnología.

De acuerdo a los resultados preliminares del censo de población y vivienda 2010, elaborado por el instituto nacional de estadística y geografía, su población es de aproximadamente 1,110,565 habitantes y una densidad de 17,539.6 hab/km<sup>2</sup> siendo así el municipio más poblado del estado de México.

Por su parte la diputada Federal Juana Bonilla se comprometió a seguir gestionando más recursos para el municipio de Nezahualcóyotl y mencionó que ya se discute en la cámara de diputados el presupuesto del 2015 y se dijo comprometida con el rescate de espacios públicos para fomentar la creación de espacios dignos para la ciudadanía. (Nezahualcoyotl, 2015)



Figura 0. Colocación de la primera piedra del parque municipal las fuentes  
<http://www.neza.gob.mx/boletines.php?pagina=96>



## **PLANTEAMIENTO DEL PROBLEMA**

El parque temático municipal “Las fuentes” su afluencia es cada vez mayor y el personal que labora en el parque no es suficiente ya que son solo 12 empleados dificultando las tareas de administración y logística. Inicialmente el parque no cuenta con infraestructura de red para brindar conexión a internet.

En el parque temático municipal “Las fuentes” necesitan canales de comunicación desarrollados mediante las tecnologías de información y comunicación ayudando a mejorar de manera considerable las labores de coordinación y trabajo del personal que labora en dicho parque además de beneficiar a los visitantes con acceso a internet.

El gobierno del municipio de Nezahualcóyotl no quiere invertir en un proyecto de telecomunicaciones dentro del parque sino se demuestra previamente la factibilidad de dicho proyecto.

¿Es necesario contar con una red inalámbrica en el parque municipal las fuentes?

¿En base a la falta de presupuesto por parte del gobierno municipal de Nezahualcóyotl para la implementación de la red inalámbrica la simulación de una Red Mesh será conveniente?

## **JUSTIFICACIÓN**

El parque está ubicado en un municipio con un gran número de población siendo este parque un componente muy necesario para fomentar las actividades recreativas y productivas contribuyendo a disminuir los índices delictivos, fomentando la integración familiar y reforzando el tejido social este parque es visitado mayormente por jóvenes siendo así un beneficio para la comunidad creando pertenencia social.

Con las TICS podemos construir canales de comunicación dentro del parque para apoyar las actividades de logística de esta manera se visualizaran los beneficios y costos de una red Mesh incluyendo este proyecto para llevarse a cabo en la siguiente administración del gobierno de Nezahualcóyotl.

## **OBJETIVOS**

### Objetivo General

- ✚ Diseñar y simular una Red Mesh en el parque temático las Fuentes.

### Objetivos Específicos

- ✚ Investigar los elementos que formulan el marco teórico de una red Mesh.
- ✚ Realizar un análisis del escenario para un correcto diseño de la red Mesh.
- ✚ Diseñar una red Mesh que garantice una completa cobertura en el parque temático las Fuentes.
- ✚ Simular la Red Mesh dando la posibilidad de ver como se comportaría la red en una implementación real.

## **HIPÓTESIS**

La simulación es un procedimiento correcto para demostrar que una red Mesh es fiable en la implementación de la red inalámbrica en el parque temático municipal las fuentes.

# CAPÍTULO I

## INTRODUCCIÓN

## I. INTRODUCCIÓN

Las técnicas más relevantes para la creación y explotación de redes de tecnologías inalámbricas son los infrarrojos, microondas laser y radio. Las tecnologías inalámbricas más comunes para la prestación de servicios de telecomunicaciones son aquellas que se basan en el uso del espectro radio eléctrico (radio), tales como la telefonía móvil LMDS. Las redes *WiFi*, las redes *WiMax*, la tecnología *bluetooth*, las comunicaciones por satélite entre otros.

Estas tecnologías inalámbricas lo son porque las uniones, conexiones o enlaces entre las diferentes terminales no se basan en el contacto físico a través de cables, y los diferentes aparatos se comunican utilizando ondas radio eléctricas mediante elementos de emisión y recepción incorporados. Las principales ventajas de las redes inalámbricas son que permiten una amplia libertad de movimientos, facilidad en la reubicación de las estaciones de trabajo evitando la necesidad de establecer cableado, y una gran rapidez en la instalación.

### 1.1 Onda de radio

Las ondas de radio son un tipo de radiación electromagnética, que tienen una longitud de onda mayor que la luz visible. Estas pueden oscilar en frecuencias que se miden en hertz. Dependiendo de esta medida nos podemos hacer una idea del alcance de la onda. Curiosamente, las microondas que utilizamos para cocinar y para comunicarnos son las mismas, solo que difieren en su longitud. La mayoría de estas ondas, viajan libres por la atmósfera de la tierra. Sólo algunas, son absorbidas por las partículas cargadas de la ionosfera.

Las ondas de radio son omnidireccionales, es decir, se propagan en todas las direcciones. Esto hace que este tipo de ondas no requieran antenas parabólicas para su envío/recepción. El rango de frecuencias comprendido entre 30 MHz y 1 GHz es muy adecuado para la difusión simultánea de información a varios destino (las ondas comprendidas en este rango son denominadas ondas de radio y cubren la banda VHF y parte de UHF).

Las redes LAN inalámbricas están normalizadas en el estándar 802.11 del IEEE, y sus dispositivos son certificados como *WiFi*. Las ondas más extendidas para su empleo como LAN inalámbricas son aquellas que no requieren licencia (ondas de radio: banda de 915 MHz, microondas: bandas de 2.4 GHz y 5 GHz. (Russell, 2005)

### 1.1.1 La señal

Los impulsos eléctricos que se transmiten por radio se llaman señal. Si una cierta estación tiene una buena señal en un territorio determinado, sus programas y comerciales entran con claridad en esa zona. Al hacer una llamada, la señal viaja desde el teléfono del usuario (o emisor) hasta una antena, también conocida como celda. Allí se transmite la señal hasta otras celdas de la misma red, hasta que alcanza el teléfono del receptor. Todo este proceso se lleva a cabo en una fracción de segundo. Si nos encontramos cerca de una celda, tendremos buena señal, pero irá disminuyendo conforme nos alejemos de esa antena, hasta que nos ubiquemos cerca de otra. Es por eso que al viajar en un vehículo podemos notar los diferentes cambios constantes en la señal que llega a nuestro teléfono.

Los teléfonos celulares utilizan ondas electromagnéticas similares a las ondas de radio o de televisión. Sin embargo, cada una tiene una frecuencia diferente, que por el tamaño de la onda y su alcance requiere de diseños específicos para optimizar su cobertura (o alcance). Las montañas y las estructuras metálicas pueden bloquear el paso de la señal y dificultar el acceso en ciertas condiciones. En otros casos, una estructura metálica, puede anular el paso de las ondas electromagnéticas, como lo propone la física con este experimento. (Moya, 2013)

### 1.1.2 Frecuencia

Todas las señales se transmiten mediante ondas electromagnéticas a veces llamadas ondas de radio. Estas ondas tienen diferente frecuencia (la cantidad de ondas que pasan por un punto dado en un periodo determinado de tiempo). Las frecuencias para las estaciones de AM se miden en KHz y las frecuencias de las estaciones de FM se miden en MHz. La FCC les ha asignado las siguientes frecuencias a todas estas estaciones de radio. (Russell J. T., 2005)

AM= 540 a 1700 KHz - FM= 88.1 a 107.9 MHz

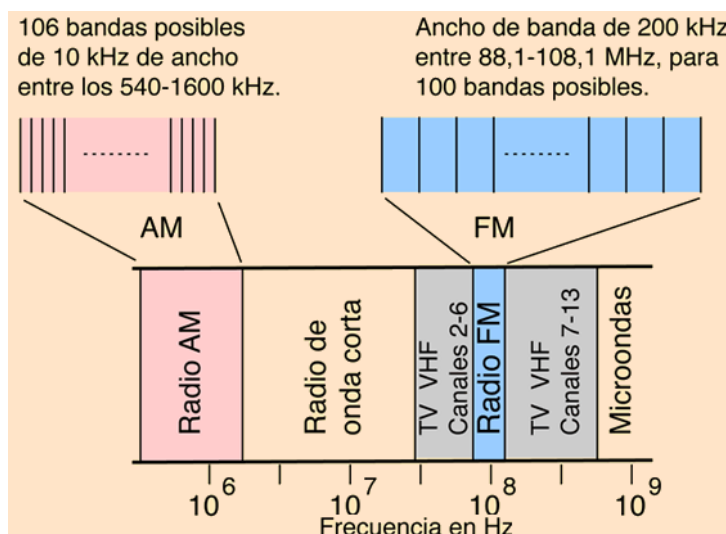


Figura 1. Distribución de onda Frecuencias

### **1.1.3 Amplitud**

Todas las ondas electromagnéticas tienen una altura llamada amplitud cuyo intervalo se asemeja a la diferencia que existe entre una ola del océano y un remolino en un estante, y una velocidad que se mide por la frecuencia con la que una serie de ondas pasan por un punto determinado en un minuto. Por ejemplo, si una estación de radio opera en una frecuencia de 1580KHz está significa que 1.580.000 de sus ondas pasan por un punto dado en un segundo. En base a estas dimensiones amplitud y frecuencia, se han desarrollado dos sistemas separados para transmitir las ondas de radio. El primer sistema transmite las variaciones en una onda sonora mediante variaciones correspondientes en su amplitud; La frecuencia permanece constante este es el principio de amplitud modulada. El segundo sistema transmite la variación en una onda sonora mediante variaciones correspondientes en su frecuencia; La amplitud se mantiene constante este es el principio de la frecuencia modulada FM. La estructura técnica de la radio AM y FM ha creado efectivamente dos medios distintos cada uno ofreciendo distintos valores al escucha y al anunciante. Las señales de AM llegan más lejos pero son susceptibles a la interferencia. La FM tiene una calidad tonal fina, pero las distancias de señal son limitadas. La calidad de recepción de una estación en particular también se determina por las condiciones atmosféricas y por la potencia de la estación (frecuencia de transmisión). (Russell J. T., 2005)

### **1.2 Polarización**

La polarización es una propiedad de las ondas electromagnéticas que describe la dirección de su campo eléctrico. Paso a comentarte algo más de manera introductoria y finalmente te facilitaré algún enlace que te pueda resultar de interés.

La polarización de una onda electromagnética es generalmente elíptica, pudiéndose considerar los casos particulares de polarización lineal, cuando uno de los ejes de la elipse llega a ser nulo, o circular, cuando ambos ejes llegan a tener la misma amplitud.

Dentro de la polarización lineal se pueden considerar los casos particulares de polarización horizontal, vertical u oblicua dependiendo de la dirección. Asimismo, la polarización circular, y la polarización elíptica en general, puede ser levógira o dextrógira.

Esta propiedad de las ondas electromagnéticas juega un papel determinante en el modo de operación de muchos sistemas de radiocomunicación, como pueden ser los diferentes sistemas de transmisión de radio, la telefonía móvil o los diferentes sistemas de posicionamiento global.



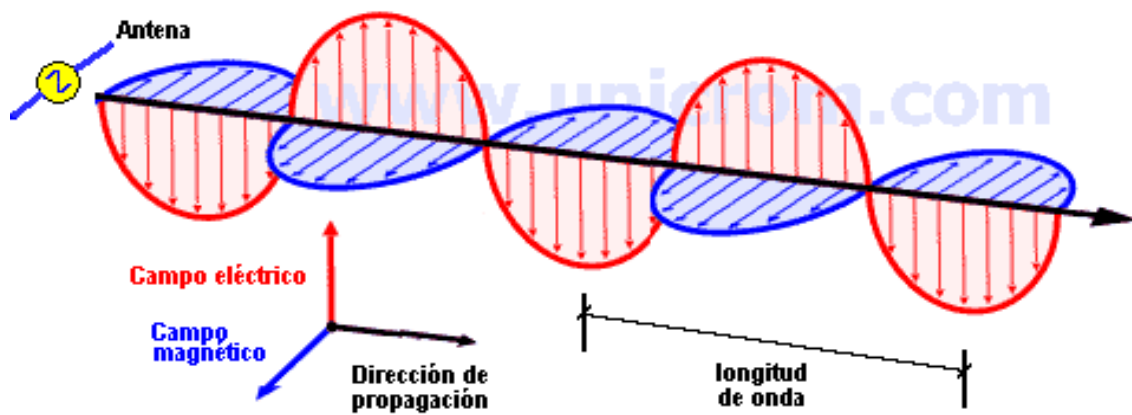


Figura 2. Polarización de una onda electromagnética  
<http://evidenciasoeg.blogspot.mx/>

### 1.2.1 Polarización lineal

Polarización Lineal - Cuando el campo eléctrico oscila en el plano perpendicular a la dirección de propagación de la onda. Normalmente, la polarización es sólo parcial y se define como: La razón entre la radiación polarizada y la no polarizada. La polarización parcial de un láser polarizado es normalmente de 1:500. Grado de polarización - Se define con la máxima intensidad ( $I_{max}$ ) transmitida a través del polarizador y la mínima intensidad ( $I_{min}$ ). (Nave, 2007)

### 1.2.2 Polarización circular

Polarización Circular - Se produce cuando la intensidad del vector de campo eléctrico es constante, pero la dirección de oscilación está rotando a una velocidad constante. No hay preferencia por una dirección específica de oscilación. Tomando en cuenta a la dirección de rotación del vector campo eléctrico desde la dirección en la que el haz se propaga, si esta dirección es en el sentido de las agujas del reloj, se trata de polarización circular derecha. Si esta dirección es en sentido contrario al de las agujas del reloj, se conoce como polarización circular izquierda. (Nave, 2007)

### 1.2.3 Polarización elíptica

En electrodinámica, la polarización elíptica es la polarización de la radiación electromagnética de forma que la punta del vector de campo eléctrico describe una elipse en cualquier plano fijo, interseccionando, o es normal a, la dirección de propagación. Una onda polarizada elípticamente puede ser resuelta en dos ondas polarizadas linealmente en cuadratura de fase, con sus planos de polarización en ángulos rectos entre sí. Dado que el campo eléctrico puede girar en sentido horario o en sentido contrario, ya que se propaga, las ondas polarizadas elípticamente exhiben quiralidad.

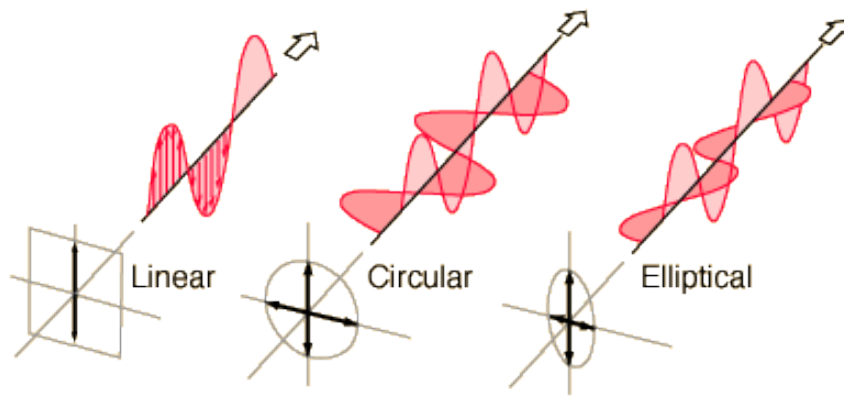


Figura 3. Polarización, Linear. Circular Elíptica  
<http://hyperphysics.phy-astr.gsu.edu/hbasees/phyopt/polclas.html>

### 1.2.4 Polarización por reflexión

Polarización por reflexión – Cuando la luz ordinaria sin polarizar incide a un ángulo de  $57^\circ$  sobre la superficie pulida de una placa de vidrio, la luz reflejada es polarizada plana. Este hecho fue descubierto primero por Etienne Malus, un físico francés, en 1808.

En general, para cada material hay un ángulo especial, llamado ángulo de polarización, donde sólo la luz polarizada en el plano perpendicular al plano del haz tiene componente reflejada. Entonces, en el ángulo de polarización el haz reflejado es 100% linealmente polarizado. La componente transmitida en el otro medio, incluye todas las componentes polarizadas paralelas y algunas perpendiculares al plano del haz. Por lo tanto, el haz transmitido está parcialmente polarizado (Nave, 2007)

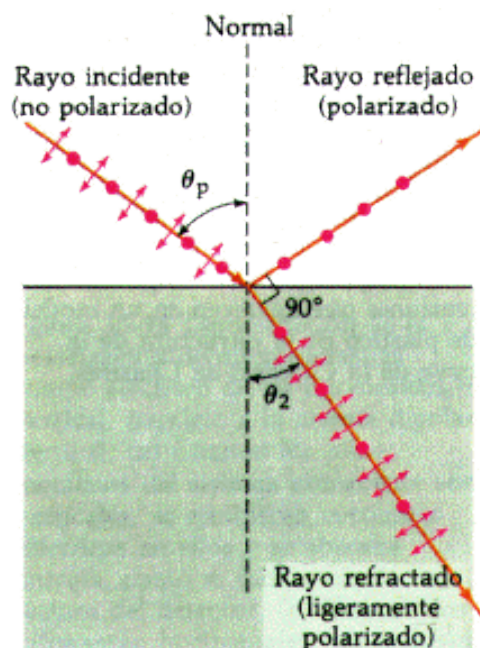


Figura 4. Ejemplo de polarización por reflexión  
[http://rabfis15.uco.es/lvct/tutorial/31/polarizacion\\_por\\_reflexion.htm](http://rabfis15.uco.es/lvct/tutorial/31/polarizacion_por_reflexion.htm)

### 1.2.5 Polarización por refracción

La polarización por reflexión, la radiación transmitida está parcialmente polarizada. La onda reflejada es polarizada paralela a la superficie del material, de modo que la radiación transmitida contiene menos radiación paralela a la superficie. Cuando varias láminas (como diapositivas de microscopio) se disponen como en la figura, la mayor parte de la radiación polarizada paralela a la superficie es reflejada, y la onda transmitida es polarizada. Si el haz incide con el ángulo de Brewster ( $\theta_B$ ), la polarización del haz transmitido es perpendicular al límite de la superficie.

Polarización por doble refracción – Algunos cristales en la naturaleza tienen diferentes índices de refracción en diferentes direcciones, por lo que el índice de refracción depende de la dirección de polarización de la luz que entra en el cristal. (Nave, 2007)

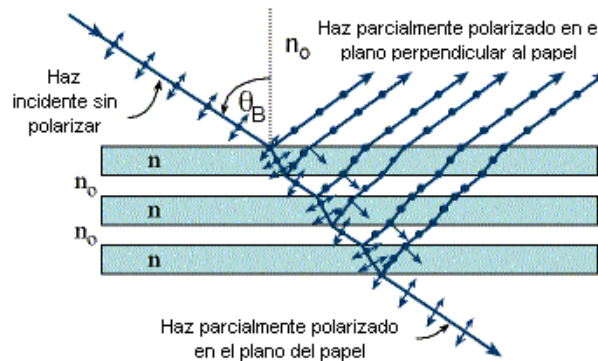


Figura 5. Ejemplo de polarización por refracción 1998  
<http://html.rincondelvago.com/espectro-redes-y-polarizacion.html>

### 1.3 Espectro electromagnético

Al flujo saliente de energía de una fuente en forma de ondas electromagnéticas se le denomina radiación electromagnética. Esta radiación puede ser de origen natural o artificial. El espectro electromagnético es el conjunto de todas las frecuencias (número de ciclos de la onda por unidad de tiempo) posibles a las que se produce radiación electromagnética. Así, el límite teórico inferior del espectro electromagnético es 0 (ya que no existen frecuencias negativas) y el teórico superior es  $\infty$ . Con los medios técnicos actuales, se han detectado frecuencias electromagnéticas inferiores a 30 Hz y superiores a  $2,9 \cdot 10^{27}$  Hz. Aunque formalmente el espectro es infinito y continuo, se cree que la longitud de onda electromagnética (distancia entre dos valores de amplitud máxima de la onda) más pequeña posible es la longitud de Planck ( $l_p \approx 1,616252 \cdot 10^{-35}$  m), distancia o escala de longitud por debajo de la cual se espera que el espacio deje de tener una geometría clásica (medidas inferiores no pueden ser tratadas en los modelos de física actuales debido a la aparición de efectos de gravedad cuántica). Igualmente, se piensa que el límite máximo para la longitud de una onda electromagnética sería el tamaño del universo.

### 1.3.1 División del espectro electromagnético

No todas las ondas electromagnéticas tienen el mismo comportamiento en el medio de propagación, la misma procedencia o la misma forma de interacción con la materia. Por ello, el espectro electromagnético se divide convencionalmente en segmentos o bandas de frecuencia. Esta división se ha realizado en función de diversos criterios, y en todo caso no es exacta, produciéndose en ocasiones solapamientos en las bandas, pudiendo una frecuencia quedar por tanto incluida en dos rangos (por ejemplo, debido a diferentes fenómenos físicos que originan la radiación, o a diferentes aprovechamientos de la energía radiada a una frecuencia concreta). La clasificación más típica del espectro electromagnético establece las siguientes categorías de radiación electromagnética: (Ordoñez, 2011)

- Ondas subradio.
- Ondas radioeléctricas.
- Microondas.
- Rayos T.
- Rayos infrarrojos.
- Luz visible.
- Rayos ultravioleta.
- Rayos X.
- Rayos gamma.
- Rayos cósmicos

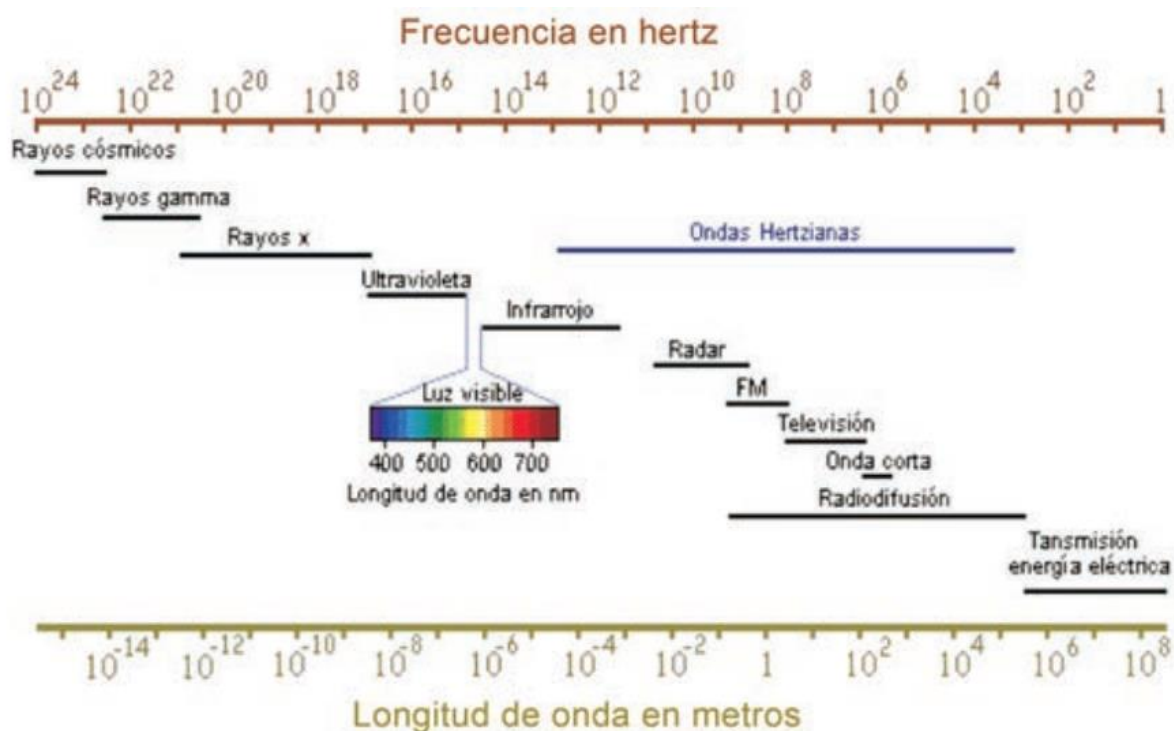


Figura 6. División del espectro electromagnético  
<http://slideplayer.es/slide/1607406/>

### 1.3.2 Frecuencias RF

En función de lo anterior, el espectro radioeléctrico o de Radio Frecuencia (RF) se refiere a la parte de espectro electromagnético en el cual las ondas electromagnéticas pueden generarse alimentando a una antena con corriente alterna. En la siguiente tabla se muestran una de las bandas de RF más importantes:

Abreviatura	Descripción	Banda	Frecuencias	Longitud de onda
			Inferior a 3 Hz	> 100.000 km
ELF	Extremely low frequency	1	3-30 Hz	100.000 km – 10.000 km
SLF	Super low frequency	2	30-300 Hz	10.000 km – 1000 km
ULF	Ultra low frequency	3	300–3000 Hz	1000 km – 100 km
VLF	Very low frequency	4	3–30 kHz	100 km – 10 km
LF	Low frequency	5	30–300 kHz	10 km – 1 km
MF	Medium frequency	6	300–3000 kHz	1 km – 100 m
HF	High frequency	7	3–30 MHz	100 m – 10 m
VHF	Very high frequency	8	30–300 MHz	10 m – 1 m
UHF	Ultra high frequency	9	300–3000 MHz	1 m – 100 mm
SHF	Super high frequency	10	3-30 GHz	100 mm – 10 mm
EHF	Extremely high frequency	11	30-300 GHz	10 mm – 1 mm
			Por encima de los 300 GHz	< 1 mm

Tabla 1. Frecuencias FR

## **1.4 Características físicas de la señal**

A continuación se van a analizar las características físicas de la señal de las redes inalámbricas: La frecuencia y la potencia de la señal.

### **1.4.1 Ancho de banda**

Para señales analógicas, el ancho de banda es la longitud, medida en Hz, del rango de frecuencias en el que se concentra la mayor parte de la potencia de la señal. También son llamadas frecuencias efectivas las pertenecientes a este rango.

El ancho de banda digital es la cantidad de datos que se pueden transmitir en una unidad de tiempo. Por ejemplo, una línea ADSL de 256 Kbps puede, teóricamente, enviar 256000 bits por segundo. Esto es en realidad la tasa de transferencia máxima permitida por el sistema, que depende del ancho de banda analógico, de la potencia de la señal, de la potencia de ruido y de la codificación del canal.

Como ejemplo de banda limitada es la conexión dial up la cual tiene un ancho de banda de apenas 56 Kbps mientras que la conexión de banda ancha es aquella que puede llevar la suficiente información como para mantener la sucesión de imágenes en una presentación de video tienen una mayor tasa de transferencia, este tipo de banda se realiza por medio de una conexión DSL, microondas, cable módem o T110. Cada tipo de conexión tiene su propio ancho de banda analógico y su tasa de transferencia máxima. El ancho de banda y la saturación de red son dos factores que influyen directamente sobre la calidad de los enlaces. La tasa de transferencia es la cantidad de información por segundo que puede ser enviada entre un servidor de acceso o aplicaciones a tu computadora, ésta se ve afectada por las horas pico, tráfico en la red, velocidad de acceso y capacidad de transacciones en los servidores Web y de aplicaciones.

El ancho de banda inalámbrica se refiere a la velocidad de datos transferidos entre dispositivos electrónicos capaces de comunicarse de manera inalámbrica, usando señales de frecuencia de radio. El ancho de banda inalámbrica se mide generalmente en miles de bits (kilobits) o millones de bits (megabits) por segundo (Mbps), pero muchos factores pueden limitar o reducir el ancho de banda y ralentizar las conexiones inalámbricas y volverlas menos confiables de lo que los usuarios esperan.

Un término que vamos a encontrar a menudo en la física de radio es ancho de banda. El ancho de banda es simplemente una medida de rango de frecuencia. Si un rango de 2400 MHz a 2480 MHz es usado por un dispositivo, entonces el ancho de banda sería 0,08 GHz (o más comúnmente 80MHz). Se puede ver fácilmente que el ancho de banda que definimos aquí está muy relacionado con

la cantidad de datos que puedes transmitir dentro de él a más lugar en el espacio de frecuencia, más datos caben en un momento dado. El término ancho de banda es a menudo utilizado por algo que deberíamos denominar tasa de transmisión de datos, como en “mi conexión a Internet tiene 1 Mbps de ancho de banda”, que significa que ésta puede transmitir datos a 1 megabit por segundo.

- **Tecnología:** El ancho de banda inalámbrica está limitado al ancho de banda especificado para cualquier tecnología inalámbrica particular. Los dispositivos que cumplen con la familia de estándares 802.11 del Instituto de Ingenieros Eléctricos y de Electrónicos (IEEE), coloquialmente conocidos como dispositivos "Wi-Fi", ofrecen unos anchos de banda teóricos máximos que van desde 11 Mbps (para dispositivos 802.11b o inalámbricos B) hasta 450 Mbps (para dispositivos 802.11n o inalámbricos-N). La tecnología Bluetooth, por otro lado, ofrece un ancho de banda teórico máximo de 2.1 Mbps (para dispositivos con Bluetooth 2.0).
- **Distancia:** La fuerza de las señales inalámbricas disminuye con la distancia, así que las tecnologías inalámbricas también especifican un rango teórico máximo por fuera del cual los dispositivos pueden sufrir de un ancho de banda reducido o no recibir señal del todo. Los dispositivos inalámbricos-N tienen un rango teórico máximo de 650 pies (200 m) o más, mientras que los dispositivos Bluetooth2.0 tienen un rango teórico máximo de cerca de 300 pies (90 m), pero un dispositivo conocido como repetidor inalámbrico, posicionado entre los dispositivos inalámbricos, puede extender estos rangos máximos.
- **Obstrucciones:** Las señales de redes inalámbricas tienen unas frecuencias relativamente altas y unas longitudes de onda cortas, lo cual significa que son atenuadas o debilitadas por obstrucciones como paredes, techos y objetos metálicos. El debilitamiento de la señal puede limitar el ancho de banda, reduciendo mucho la velocidad de conexión o dificultando que los dispositivos inalámbricos establezcan una conexión en primer lugar. Las obstrucciones grandes y sustanciales cercanas a los dispositivos inalámbricos causan las mayores interferencias en este tipo de señales.
- **Interferencia de radio:** Otros factores, incluyendo la interferencia de radio de los dispositivos comunes del hogar, como teléfonos sin cable, hornos microondas y juguetes a control remoto, o el terreno, la vegetación e incluso las condiciones del clima, como la alta presión del aire, la lluvia y el viento, pueden limitar el ancho de banda. Algunos dispositivos inalámbricos, conocidos como dispositivos de doble banda, pueden operar en la frecuencia de 2.4GHz y la menos llena de 5GHz del

espectro de radio, así que cambiar a la frecuencia más alta puede reducir la interferencia de radio y sus efectos en el ancho de banda. De lo contrario, puedes reducir la interferencia de radio al elegir los dispositivos del hogar que operan en una banda de frecuencia diferente, como la banda de 900 MHz, desde tus dispositivos de red inalámbrica. (Commons, 2015)

### 1.4.2 Frecuencia

El espectro está dividido en partes iguales distribuidas sobre la banda en canales individuales. Los productos WiFi utilizan bandas libres dentro de las cuales encontramos la banda de 2.4. En esta banda de 2.4, se definieron 11 canales utilizables por equipos WIFI, que pueden configurarse de acuerdo a necesidades particulares. Sin embargo, los 11 canales no son completamente independientes (canales contiguos se superponen y se producen interferencias). El ancho de banda de la señal (22MHz), es superior a la separación entre canales consecutivos (5MHz), por eso se hace necesaria una separación de al menos 5 canales con el fin de evitar interferencias entre celdas adyacentes.

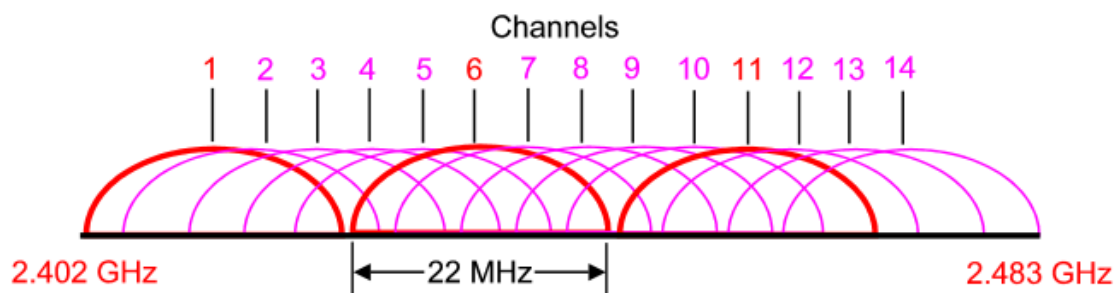


Figura 7. Canales de frecuencia 2011

<http://www.comusoft.com/mi-red-wi-fi-interfiere-con-telefonos-inalambricos-u-otras-redes>

La frecuencia de una onda sonora se define como el número de pulsaciones (ciclos) que tienen por unidad de tiempo (segundo). La unidad correspondiente a un ciclo por segundo es el *herzio* (Hz). Las frecuencias más bajas se corresponden con lo que habitualmente llamamos sonidos graves, son sonidos de liberaciones lentas. Las frecuencias más altas corresponden con lo que llamamos agudos y son vibraciones muy rápidas. El espectro de frecuencia audible varía según cada persona, edad, u otro factor. Sin embargo normalmente se acepta como el intervalos entre 20Hz y 20KHz.

Como se ha visto en el capítulo anterior el estándar 802.11b/g trabaja en la banda de 2.5GHz cada punto de acceso trabaja en un canal determinado. En total hay 11 canales y cada canal se corresponde con una frecuencia determinada los números de canales consecutivos corresponden también ha



frecuencias consecutivas por tanto, mientras más diferencia haya entre los números del canal mayor diferencia habrá entre sus frecuencias.

Bandas de frecuencia usadas en *WLANs* 2.4 GHz La gama de frecuencias de 2.4 GHz es probablemente el más ampliamente utilizado en *WLANs*, se utiliza por los estándares 802.11, 802.11b, 802.11g, y las normas de IEEE 802.11n. El rango de frecuencias de 2.4 GHz puede utilizarse en *WLANs* se subdivide en canales que van desde 2400 a 2,4835 GHz. En estados unidos se tienen 11 canales, cada canal tiene un ancho de 22 MHz. Unos canales se traslapan con los demás y causan interferencias. Por esta razón, los canales 1, 6 y 11 son los más comúnmente utilizados, ya que no se traslapan, de hecho, muchos productos inalámbricos, están sujetos a seleccionar solo uno de los tres canales. A continuación en la figura se muestran los 11 canales, incluyendo los traslapes como se puede observar los canales 1, 6 y 11 no se traslapan. GHz La gama de 5GHz es utilizado por el estándar 802.11a y por la nueva norma 802.11n. En el estándar 802.11a, velocidad de transmisión de datos puede variar desde 6 Mbps a 54 Mbps, dispositivos con 802.11a, aparecieron en el mercado hasta el año 2001, el 5 GHz se subdivide en canales, 20 MHz de ancho cada uno. La gama de 5 GHz cuenta con un total de 23 canales no traslapados. La frecuencia de 5GHz utiliza la multiplexión por división de frecuencia ortogonal (*OFDM* por sus siglas en inglés *Orthogonal Frequency Division Multiplexing*)

En teoría se puede utilizar cualquier canal para nuestro punto de acceso, pero existen países, como es el caso de España, en los que legalmente solo se puede utilizar un conjunto reducido de canales. A continuación se van a ver los canales que se pueden utilizar en cada zona geográfica: (Julio, 2008)

- Europa. Del canal 3 al 13, excepto en Francia que solo se puede utilizar los canales del 10 al 13 y España, que únicamente se pueden utilizar los canales 10 y 11.
- Japón. Todos los canales.
- USA. Del canal 1 al 11.

### **1.4.3 Potencia de señal**

La potencia de una antena inalámbrica se puede entender como el grado de amplificación de la señal. La ganancia se puede medir en decibelios (dB) o en voltaje (mV), tiene el mismo valor en la antena para recibir y enviar información. Cuanta mayor sea la ganancia de una antena, mejor cobertura tendrá la red inalámbrica. Por ejemplo, las antenas de los puntos de acceso poseen, como es lógico, mucha mayor ganancia que las antenas de los adaptadores de red inalámbricos, ya que deben ofrecer cobertura a una amplia zona del espacio. No obstante, las antenas direccionales tienen mayor ganancia que las omnidireccionales, ya que concentran toda la energía en una sola dirección, y por lo tanto tienen mayor alcance.

#### 1.4.4 Ganancia

La ganancia de potencia  $G$  de un amplificador es la relación entre la potencia de salida y la potencia de entrada:

$$G = \frac{P_{out}}{P_{in}}$$

Si la potencia de salida es de 20W y la entrada 10W, la ganancia es:

$$G = \frac{20W}{10W} = 2$$

Lo que significa que la potencia de salida es dos veces mayor que la de entrada. Si la ganancia es menor que 1, se llama atenuación.

#### 1.4.5 Decibelio

El logaritmo decimal de la ganancia expresa su relación en la unidad logarítmica del Belio, denominada así en honor de Graham Bell. Dos potencias diferentes en  $N$  Belios cuando:

$$\frac{P_{out}}{P_{in}} = 10^N$$

Decimos que una señal de potencia  $P_{out}$  tiene un nivel de  $N$  Belios respecto a otra señal de potencia  $P_{in}$ :

$$N = \log \frac{P_{out}}{P_{in}} \text{ Belios}$$

Como el Belio es una unidad muy grande, se utiliza un submúltiplo diez veces menor: El decibelio, cuya notación abreviada es dB.

$$\frac{P_{out}}{P_{in}} = 10^{0,1 \cdot N}$$

$$10 \log \frac{P_{out}}{P_{in}} \text{ deciB(dB)}$$

Por lo tanto las expresiones, en decibelios (dB) son comparaciones logarítmicas (en base 10) entre magnitudes del mismo tipo, por tanto son adimensionales. Se utilizan ampliamente en telecomunicaciones por razones de tipo práctico:

convierte las multiplicaciones y divisiones en sumas y restas respectivamente, simplificando por tanto las expresiones numéricas.

Si expresamos en decibelios el ejemplo anterior:

$$G_{dB} = 10 \log \frac{20W}{10W} = 3dB$$

Si la ganancia es 4 y después 8, entonces:

$$G_{dB} = 10 \log 4 \approx 6dB$$

$$G_{dB} = 10 \log 8 \approx 9dB$$

Luego cada vez que la ganancia en potencia aumenta el doble, la ganancia en dB aumenta 3 dB. Además existe varias formas de denotar la potencia d un dispositivo (en dB o en mW). Las dos medidas están relacionadas y si una tarjeta tiene una potencia de 30mW entonces tiene 14,77 dB.

$$G_{dB} = 10 \log 30mW = 14,77dB$$

#### 1.4.6 Atenuación

Se considera atenuación cuando la ganancia de un sistema es menor que 1. Suponga que la ganancia de potencia es de 10. Expresada en dB:

$$G_{dB} = 10 \log 10 = 10dB$$

Si la ganancia de potencia fuera 100, entonces serian 20dB. Si la ganancia de potencia fuera 1000, entonces la ganancia fuera de 30 dB. El patrón que observamos es que la ganancia en dB aumenta en 10 dB cada vez que la ganancia en potencia se incrementa por un factor 10. Lo mismo ocurrirá con respecto a la atenuación; Para atenuación de 0,1 0,01 y 0,001 tendremos -10 dB, -20 dB y -30 dB respectivamente.

#### 1.4.7 Pérdida de propagación

La pérdida d propagación es la cantidad de señal necesaria para llegar de un punto a otro de la transmisión. Es decir, es la cantidad de señal que se pierde al atravesar un espacio.

Hacer un cálculo teórico del alcance de una señal, considerando todos los posibles obstáculos, resulta algo complicado, por lo que se realizan los cálculos en espacio abierto. En un espacio sin obstáculos, la pérdida de propagación puede calcularse con la siguiente formula:

$$P_p = 20 \log(d) + 20 \log(f) + 32,4$$

Donde  $d$  es la distancia en kilómetros y  $f$  es la frecuencia en MHz. Aunque el valor de la frecuencia depende del canal en el que trabaja el equipo, para simplificar se va considerar la frecuencia de 2,4GHz. En este caso, la formula anterior quedaría resumida de la siguiente forma:

$$P_p = 20 \log(d) + 67.81 + 32.4 = 20 \log(d) + 100$$

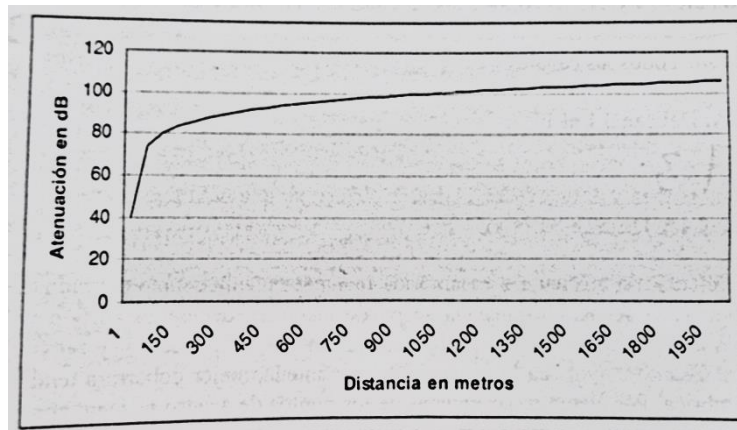


Figura 8. Perdida de propagación de la señal 2008

<http://mx.casadellibro.com/libro-guia-de-campo-de-wifi/9788478978458/1180231>

#### 1.4.8 Dirección de propagación

La dirección de propagación de las antenas se clasifica en dos grandes grupos: Direccionales y Omnidireccionales. Las antes direccionales son aquellas que concentran toda su actividad en una única dirección. Por lo tanto hay que enfocarlas directamente hacia el lugar donde se encuentra el dispositivo con el que se quiere comunicar. Las antenas omnidireccionales reciben y emiten señales en todas direcciones. Estas antenas tienen un menor alcance que las antenas direccionales, debido precisamente a que la señal se propaga en todas direcciones, y por lo tanto la potencia debe repartirse. (Julio, 2008)

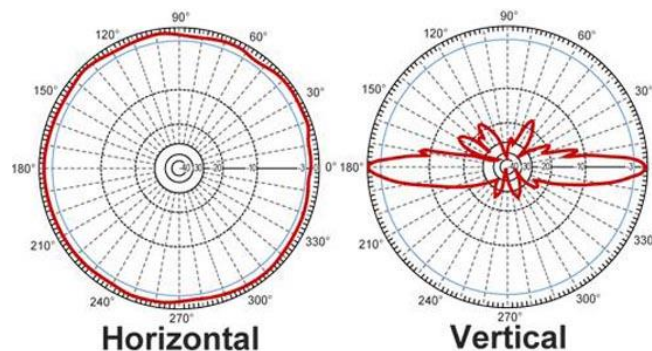


Figura 9. Patrones de propagación omnidireccional y direccional

<http://www.fpvuk.org/equipment/antennas/>

## 1.5 Medios de transmisión guiados

Dentro de los medios de transmisión habrá medios guiados y medios no guiados; la diferencia radica que en los medios guiados el canal por el que se transmite las señales son medios físicos, es decir, por medio de un cable; y en los medios no guiados no son medios físicos.

Medios Guiados: Se conoce como medios guiados a aquellos que utilizan unos componentes físicos y sólidos para la transmisión de datos. También conocidos como medios de transmisión por cable.

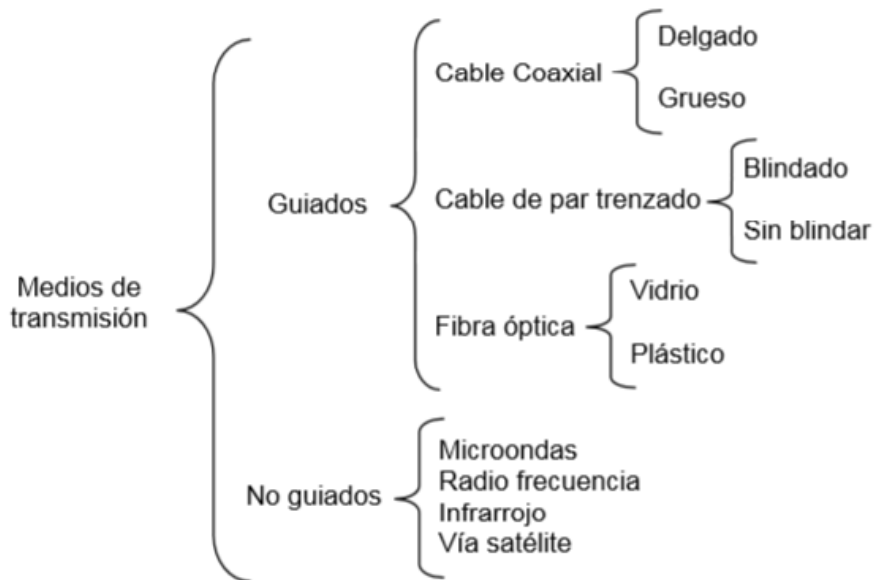


Figura 10. Diagrama de clasificación de medios de transmisión  
<http://genesifermini.blogspot.mx/>

Alambre se usó antes de la aparición de los demás tipos de cables (surgió con el telégrafo), Guía de honda verdaderamente no es un cable y utiliza las microondas como medio de transmisión.

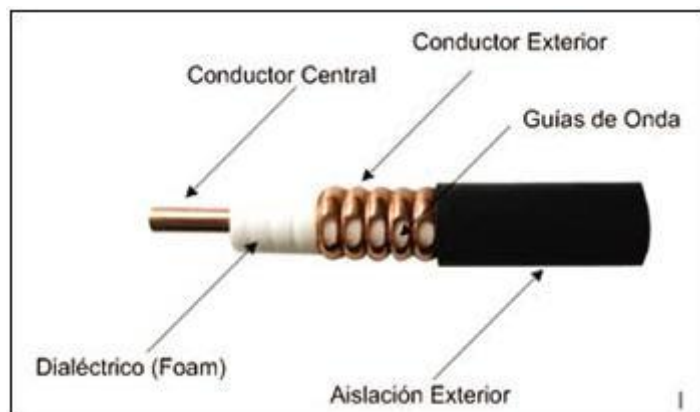


Figura 11. Estructura de un cable UTP  
<http://lumugo.com/?p=113>

## 1.5.1 Fibra Óptica

Fibra óptica: es el mejor medio físico disponible gracias a su velocidad y su ancho de banda, pero su inconveniente es su coste. Es un cilindro de vidrio o plástico sobre el que se aplica otro de menor índice de refracción y un protector opaco.

Este medio es capaz de dirigir la luz emitida por un láser o LED a lo largo de su longitud usando la reflexión interna. Se utiliza para la comunicación a largas distancias, permitiendo enviar gran cantidad de datos a gran velocidad.

Las diferentes trayectorias que puede seguir un haz de luz en el interior de una fibra se denominan modos de propagación. Y según el modo de propagación tendremos dos tipos de fibra óptica:

- *f* Monomodo: Es una fibra óptica en la que sólo se propaga un modo de luz. Se logra reduciendo el diámetro del núcleo de la fibra hasta un tamaño (8,3 a 10 micrones) que sólo permite un modo de propagación. Su distancia máxima es de 3 Km. A diferencia de las fibras multimodo, las fibras mono modo permiten alcanzar grandes distancias y transmitir elevadas tasas de bit.
- *f* Multimodo: Es una fibra que puede propagar más de un modo de luz, puede tener más de 1000 modos de propagación de luz. Se usan comúnmente en aplicaciones de corta distancia, menores a 1 km. Simple de diseñar y económico.

El núcleo de una fibra multimodo tiene un índice de refracción superior, pero del mismo orden de magnitud, que el revestimiento. Debido al gran tamaño del núcleo de una fibra multimodo, es más fácil de conectar y tiene una mayor tolerancia a componentes de menor precisión.

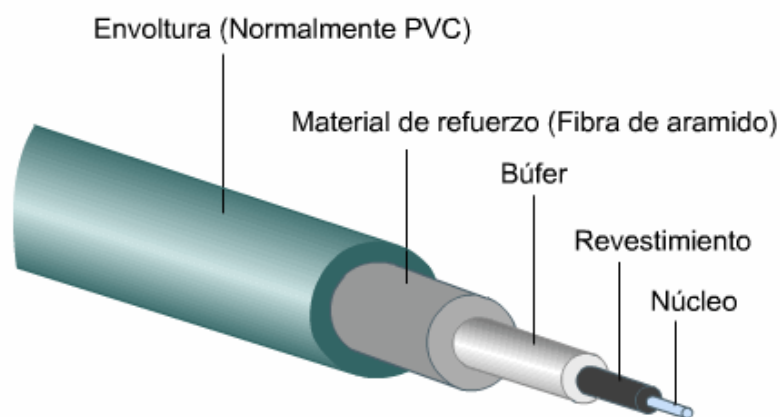


Figura 12. Estructura de un cable de Fibra óptica  
<http://www.monografias.com/trabajos30/cableado/cableado.shtml>

## 1.5.2 Par Trenzado

El cable de par trenzado es un tipo de conexión usado en telecomunicaciones en el que dos conductores eléctricos aislados son entrelazados para anular las interferencias de fuentes externas y diafonía de los cables adyacentes. Fue inventado por Alexander Graham Bell.

Este cable es el medio más usado debido a su comodidad de instalación y a su precio. Está formado por dos alambres de cobre, aislados y entrelazados en forma helicoidal, lo cual permite reducir la interferencia eléctrica entre pares. El cable de par trenzado consiste en ocho hilos de cobre aislados entre sí, trenzados de dos en dos que se entrelazan de forma helicoidal, como una molécula de ADN.

De esta forma el par trenzado constituye un circuito que puede transmitir datos. Esto se hace porque dos alambres paralelos constituyen una antena simple. Cuando se trenzan los alambres, las ondas se cancelan, por lo que la radiación del cable es menos efectiva.

Así la forma trenzada permite reducir la interferencia eléctrica tanto exterior como de pares cercanos. Un cable de par trenzado está formado por un grupo de pares trenzados, normalmente cuatro, recubiertos por un material aislante. Cada uno de estos pares se identifica mediante un color.

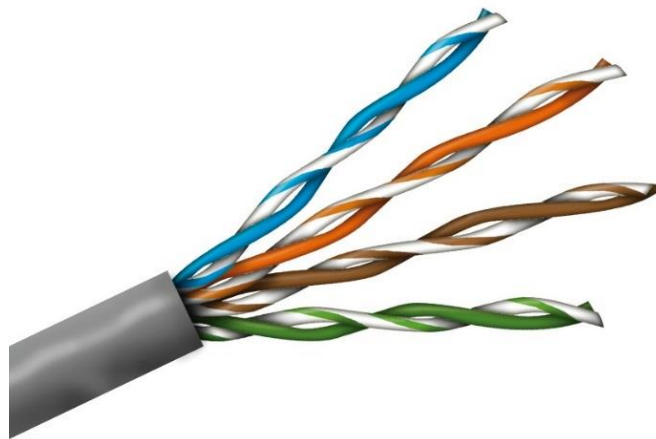


Figura 13. Cable de par Trenzado

<http://articulo.mercadolibre.com.mx/MLM-494160901-cable-de-red-utp-categoria-5-bobina-100-mts-rj45-gris-pc- JM>

Existen tres tipos de cable par trenzado:

- UTP (*Unshielded Twisted Pair*). La distancia máxima sin repetidores es de 100 metros. Consiste en dos pares de alambre de cobre cubierto de plástico.
- FTP (*Foiled Twisted Pair*). Exactamente al UTP, pero los grupos de pares están envueltos en cinta conductora, similar al papel aluminio.
- STP (*Shielded Twisted Pair*). Se encuentra recubierto por una hoja laminada de aluminio. Es altamente inmune al ruido eléctrico, se comporta igual que el UTP pero mejora en distancias de comunicación largas.
- La categoría de un cable par trenzado se obtiene por el número de trenzas que este tiene en 30.48 centímetros.
- *f* Categoría 3. Transmite a 16MHz. Son utilizados en redes Ethernet a 10Mbps.
- *f* Categoría 5. Transmite a 20MHz. Empleados en redes Ethernet a 100Mbps. *f*
- Categoría 6. Transmite a 250MHz. Usados en redes Ethernet a 1Gbps.

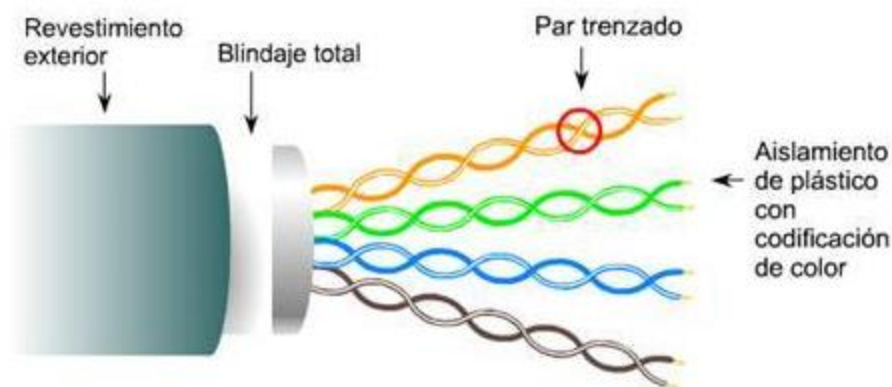


Figura 14. Elementos de un cable tipo par trenzado  
<http://www.monografias.com/trabajos30/cableado/cableado.shtml>



### 1.5.3 Cable coaxial

El cable coaxial está formado por un núcleo de alambre de cobre como conductor central, cubierto por un aislante, mismo que está rodeado por una malla trenzada, empleada como tierra y todos a su vez los envuelve una cubierta aislante resistente a la interferencia electromagnética, como se ilustra en la Figura 2.3.

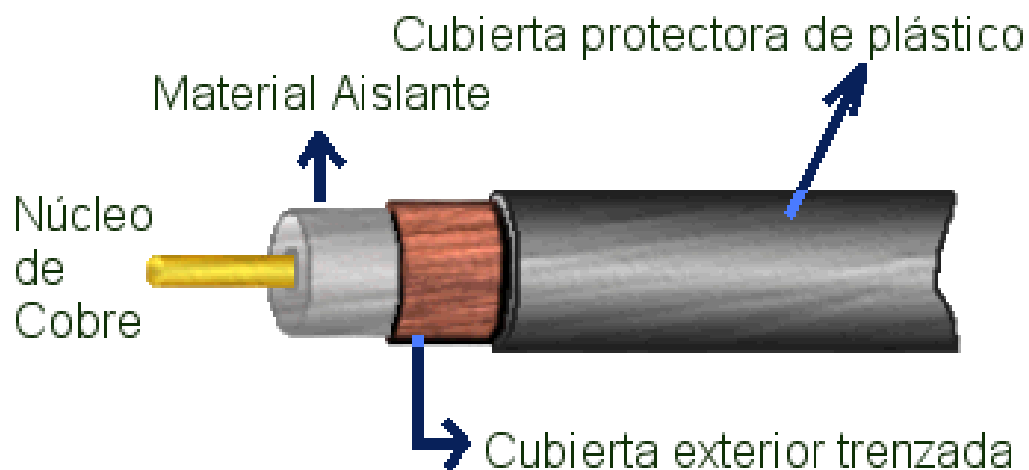


Figura 15. Cable coaxial

<https://ionorue.wordpress.com/2012/12/09/estudio-comparativo-distintos-medios-de-transmision-guiados/>

Existen diversos tipos de cable coaxial, cada uno con un diámetro e impedancias diferentes. Pero la característica que mantienen es que cada extremo del cable debe terminar con una resistencia llamada terminador.

El cable coaxial es capaz de lograr altas velocidades de transmisión en largas distancias. Por esa razón, se utiliza en redes de comunicación de banda ancha (cable de televisión) y cables de banda base (Ethernet). De acuerdo a la transmisión a generarse, el cable se divide en dos tipos según su impedancia:

Cable de 50 ohms para comunicaciones *BaseBand* y transmisiones digitales, empleado en redes LAN. Los cables coaxiales más comunes son el RG-58. Cable de 75 ohms para comunicaciones *BroadBand* y transmisiones analógicas, utilizado en sistemas de televisión por cable. Cable coaxial RG-59. (Ternero, 2006).

Cuando es utilizado en redes puede ser del tipo:

- Cable coaxial delgado.
  - Estándar: IEEE 802.3 10Base2.
  - Diámetro aproximado del cable:  $\frac{1}{4}$  pulgada.
  - Especificaciones técnicas del medio: RG-58.
  - Velocidad de operación: 10Mbps.
  - Distancia máxima del segmento 185 metros.
  - Distancia mínima entre nodos: 0.5 metros.
  - Número máximo de nodos por segmento: 30
- Cable coaxial grueso.
  - Estándar: IEEE 802.3 10Base2.
  - Diámetro aproximado del cable:  $\frac{1}{2}$  pulgada.
  - Especificaciones técnicas del medio: RG-58.
  - Velocidad de operación: 10Mbps.
  - Distancia máxima del segmento 500 metros.
  - Distancia mínima entre nodos: 2.5 metros ó múltiplos.
  - Número máximo de nodos por segmento: 100.

### 1.5.4 Redes cableadas

Una red cableada es una red en la que se conectan diferentes computadoras mediante cable computadoras las cuales a su vez se puede comunicarse entre sí y otros dispositivos periféricos. A través de una red se puede intercambiar archivos y también enviar datos a otros dispositivos de salida como una fax una impresora.

Una red cableada conecta dos o más ordenadores mediante un cable. También es posible agregar a la red impresoras y otros dispositivos. Para la conexión es necesario un conmutador (*switch*), que a menudo viene integrado en el router. Sólo las personas autorizadas tienen acceso a los datos compartidos en la red.

Ethernet es un estándar de redes de área local para computadores con acceso al medio por detección de la onda portadora y con detección de colisiones (CSMA/CD). Su nombre viene del concepto físico de ether. Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI.

Ethernet se tomó como base para la redacción del estándar internacional IEEE 802.3, siendo usualmente tomados como sinónimos. Se diferencian en uno de los campos de la trama de datos. Sin embargo, las tramas Ethernet e IEEE 802.3 pueden coexistir en la misma red.

## Protocolo Ethernet/802.3

Estructura de la trama de 802.3 Ethernet

Preambulo	Delimitador de inicio de trama	MAC de destino	MAC de origen	802.1Q Etiqueta(opcional)	Ethertype (Ethernet II) o longitud (IEEE 802.3)	Payload	Secuencia de comprobación (32-bit CRC)	Gap entre frames
7 Bytes	1 Byte	6 Byte	6 Bytes	(4 Bytes)	2 Bytes	De 46 (o 42) hasta 1500 Bytes	4 Bytes	12 Bytes
64–1522 Bytes								
72–1530 Bytes								
84–1542 Bytes								

PREÁMBULO	DIRECCIÓN DESTINO	DIRECCIÓN FUENTE	TIPO/ LONGITUD	DATOS	FCS
-----------	-------------------	------------------	----------------	-------	-----

Tabla 2. Estructura de la trama 802.3 Ethernet  
[http://es.wikipedia.org/wiki/IEEE\\_802.3](http://es.wikipedia.org/wiki/IEEE_802.3)

## 1.6 Medios de transmisión no guiados.

Medios no Guiados: o sin cable han tenido gran acogida al ser un buen medio de cubrir grandes distancias y hacia cualquier dirección, su mayor logro se dio desde la conquista espacial a través de los satélites y su tecnología no para de cambiar. De manera general podemos definir las siguientes características de este tipo de medios: La transmisión y recepción se realiza por medio de antenas, las cuales deben estar alineadas cuando la transmisión es direccional, o si es omnidireccional la señal se propaga en todas las direcciones.

### 1.6.1 Microondas

Las emisiones pueden ser de forma analógica o digitales pero han de estar en la línea visible, el envío de ondas electromagnéticas se hace en línea recta por lo que es necesario el uso de antenas parabólicas para obtener una relación señal ruido aceptable. Tiene problemas para atravesar edificios e incluso pueden verse refractadas por diferentes capas atmosféricas empleando más tiempo para su transmisión.

- *f* Velocidad de 300 Mb/seg.
- *f* Alcance de 10000 - 80000 m. *f*
- Su uso está extendido en telefonía móvil y televisión.



Figura 16. Símbolo de la tecnología Bluetooth

[http://www.hwupgrade.it/news/periferiche/rilasciate-ufficialmente-le-specifiche-bluetooth-40\\_33167.html](http://www.hwupgrade.it/news/periferiche/rilasciate-ufficialmente-le-specifiche-bluetooth-40_33167.html)

Radio enlaces.

Es la comunicación vía radio, mediante un emisor y receptor sintonizados en la misma frecuencia. Su generación es sencilla y omnidireccional lo que simplifica y facilita la instalación de las interfaces.

- Baja velocidad 4800 Kb/s. *f*
- Confidencialidad de los datos. *f*
- Mantiene un poco de interferencias.

## Rayos infrarrojos.

Para que se dé la comunicación el emisor y el receptor debe estar visibles uno con respecto del otro. Poseen las mismas técnicas que las empleadas por la fibra óptica pero son por el aire. Son una excelente opción para las distancias cortas, hasta los 2km generalmente.

- Velocidad de 10 y 40 m/s. *f*
- Alcance de 10 - 2000 m. *f*
- Confidencialidad de los datos. *f*
- Mantiene una dificultad compleja para atravesar objetos sólidos. *f*
- Se utiliza en mandos a distancia y controles remotos. *f*
- Bajo costo de fabricación e implementación.

## Vía satélite.

Los satélites reciben la señal en una frecuencia y tras amplificarla la devuelven de nuevo a la tierra en otra de distinta frecuencia con el fin de no perturbar la señal de entrada con un retardo de 270 más ventajas tales como son la libertad geográfica, su alta velocidad, pero sus desventajas tiene como gran problema el retardo de las transmisiones debido a tener que viajar grandes distancias.

- Mantiene una fiabilidad excelente y no hay una tasa de error. *f*
- Se comenta que es la mejor.



Figura 17. Antenas de conexión vía satélite  
<http://es.slideshare.net/ErwinPQ/satelites-13447983>

### 1.6.2 Ondas

- Ondas cortas: también llamadas radio de alta frecuencia, su ventaja es que se puede transmitir a grandes distancias con poca potencia y su desventaja es que son menos fiables que otras ondas.
- Ondas de luz: son las ondas que utilizan la fibra óptica para transmitir por el vidrio.

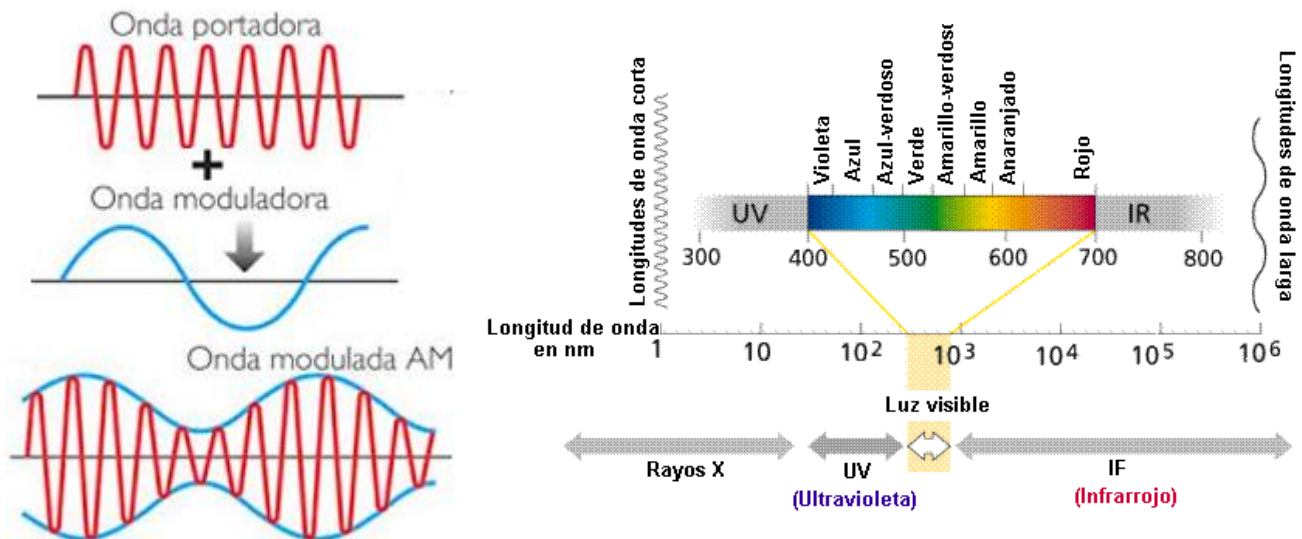


Figura 18. Ondas de transmisión inalámbricas 2004,2012  
<http://www.alquimistadeacuarios.com/foro/viewtopic.php?t=3078>  
<http://mrecursos tecnologicos.blogspot.mx/>

### 1.6.3 Redes Inalámbricas

El funcionamiento de las redes inalámbricas, especificado en el estándar IEEE 802.11, es similar al de las redes Ethernet, especificado en IEEE 802.3, lo único que cambia es la manera que tienen los ordenadores de acceder a la red: en un caso es a través de un cable, y en otro de manera inalámbrica. Por lo tanto, dentro del modelo OSI visto anteriormente, solo cambian las dos primeras capas en el estándar IEEE 802.11, que son las capas física y de enlace, o lo que es equivalente, la primera capa del modelo TCP/IP.

De este modelo, el estándar IEEE 802.11 define una nueva capa física (PHY) y otra de enlace, donde la capa de enlace a su vez se divide en otras dos capas (MAC y LLC). A continuación se describen las características más importantes de cada una de estas capas:

- PHY (*Physical Layer*). La capa física se encarga de establecer todo lo relacionado con la difusión de la señal. A su vez se divide en otras dos subcapas: PLCP (*Physical Layer Convergence Protocol*) y PMD (*Physical Medium Dependet*). La principal función de la subcapa PLCP consiste en realizar conversiones en el formato de datos para lograr la compatibilidad co0n el medio físico. También se encarga de comunicar a la capa Mac si el medio está en ese momento en uso o no. Por otro lado, la sub capa PMD es la encargada de la difusión de la señal a través del medio.
- MAC (*Medium Access Control*). Es la encargada de controlar el acceso al medio físico, detectando el momento en el que se puede transmitir y en el que se debe esperar. Si el medio se encuentra disponible, transmitirá el paquete, y si está ocupado, deberá esperar. Esta capa utiliza una tecnología llamada CA (*Collision Avoidance*), que evita que se produzcan colisiones al intentar acceder dos ordenadores a la vez del medio físico. Además, también se encarga de determinar el origen y el destino de cada paquete que se transmite.
- LLC (*Logical Link Control*) Permite establecer conexiones fiables al medio físico y de mantenerlas para que no existan problemas durante la transmisión de la información. (Julio, 2008)

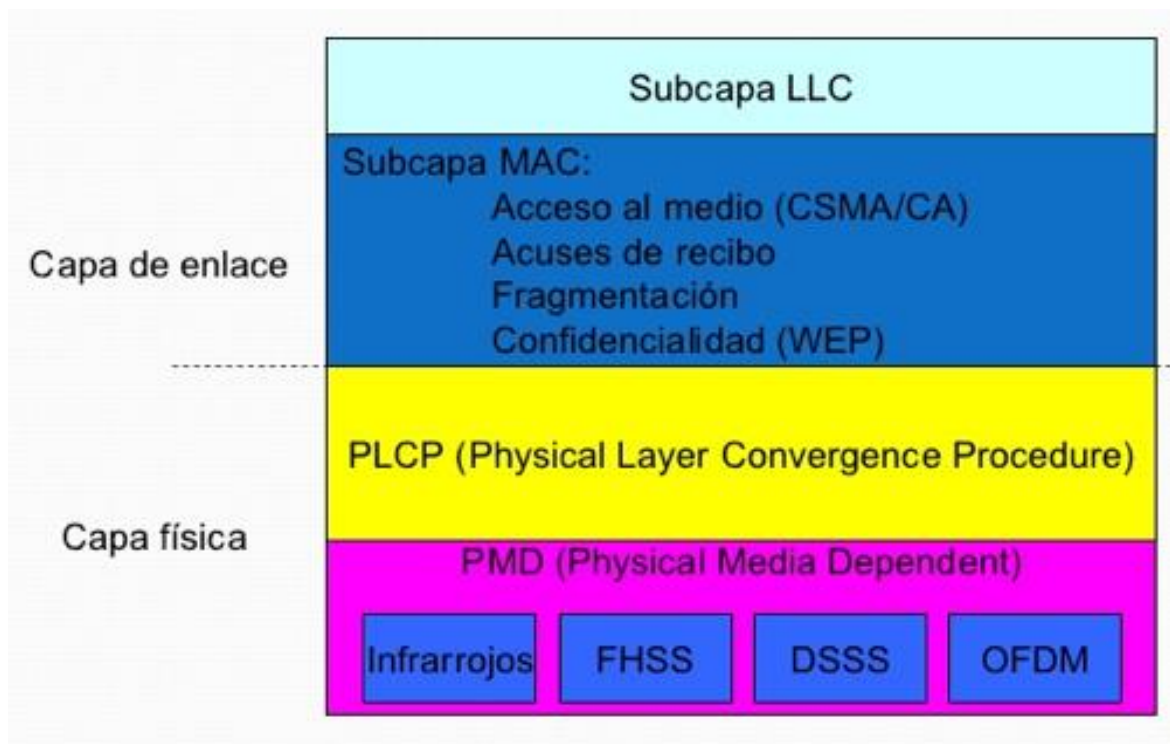


Figura 19. Subcapas de la capa de enlace y física 2012

<http://es.slideshare.net/malepaz14/wlan-wireless>

# CAPÍTULO II

## REDES INALÁMBRICAS



## II. REDES INALÁMBRICAS

Red es un concepto que procede del vocablo latino rete y que hace mención a la estructura que dispone de un patrón característico. El concepto se utiliza para nombrar al conjunto de los equipos informáticos interconectados que comparten servicios, información y recursos.

Inalámbrico, por su parte, es un sistema de comunicación eléctrica que no utiliza alambres conductores. Esto quiere decir que dicha comunicación se establece sin apelar a cables que interconecten físicamente los equipos.

Una red inalámbrica, por lo tanto, es aquella que permite conectar diversos nodos sin utilizar una conexión física, sino estableciendo la comunicación mediante ondas electromagnéticas. La transmisión y la recepción de los datos requieren de dispositivos que actúan como puertos.

Las redes inalámbricas permiten establecer vínculos entre computadoras y otros equipos informáticos sin necesidad de instalar un cableado, lo que supone una mayor comodidad y un ahorro de dinero en infraestructura.

### 2.1 Introducción.

En los últimos años se ha producido un crecimiento espectacular en lo referente al desarrollo y aceptación de las comunicaciones móviles y en concreto de las redes de área local (*Wireless LANs*). La función principal de este tipo de redes es la proporcionar conectividad y acceso a las tradicionales redes cableadas (*Ethernet*, *Token Ring*), como si de una extensión de éstas últimas se tratara, pero con la flexibilidad y movilidad que ofrecen las comunicaciones inalámbricas.

El momento decisivo para la consolidación de estos sistemas fue la conclusión del estándar IEEE802.11 el pasado mes de junio de 1997. En este estándar se encuentran las especificaciones técnicas que se deben tener en cuenta a la hora de implementar una red de área local inalámbrica *WLAN*.

Una red inalámbrica es un sistema de comunicación formado por un conjunto de dos o más dispositivos conectados entre sí, que no utilizan cables para comunicarse. Existe una gran variedad de tecnologías que permiten crear redes inalámbricas; desde los infrarrojos y radiofrecuencias que se utilizan para comunicar dispositivos situados a cortas distancias, hasta las grandes redes globales que transmiten voz y datos a lo largo de las enormes regiones geográficas.

Gracias a su bajo coste, estas redes de última generación han ido incorporándose con gran éxito al uso doméstico, de tal modo que en la actualidad es muy frecuente tener en cualquier hogar o empresa una red inalámbrica, con las mismas prestaciones y funcionalidad que ofrecen las redes cableadas.

Las redes inalámbricas de área local, esto es posible, en gran parte, a que los organismos internacionales que establecen el reparto de las frecuencias han dejado libres varias franjas para uso personal o privado.

Estas frecuencias son usadas, por ejemplo, por teléfonos fijos inalámbricos, *walkie-talkies* etc. Desde hace poco, existe una nueva tecnología que hace uso de las frecuencias libres de licencia: las redes de área local inalámbricas o redes Wireless. Las LAN inalámbricas utilizan básicamente longitudes de onda correspondientes a las microondas (2,4 GHz y 5 GHz) y permiten tener anchos de banda apreciables (desde 1 MB/s en las primeras versiones hasta llegar a los 54 MB/s de los últimos estándares).

También es verdad que aunque la banda alrededor de los 5 GHz es abierta en todo el mundo, el ancho de banda que se puede ocupar depende de la situación particular que haya impuesto cada legislador. Es por ello que en Europa se pueden utilizar hasta 455 MHz, mientras que en Norteamérica el ancho de banda se restringe a 300 MHz y en Japón a 100 MHz. En muchos sitios, las redes Ethernet de cable tradicional han sido ampliadas con la implantación de este tipo de redes inalámbricas.

La interconexión de varias redes locales (como por ejemplo en el caso de redes inalámbricas que se extienden en todo el campus universitario) ha propiciado que algunos visionarios hayan visto la posibilidad de crear una red metropolitana con gran ancho de banda y con la posibilidad de acceso a Internet, de forma que se pudiera acceder a cualquier servicio de los que comúnmente se utilizan en Internet (correo, web, ftp.) desde cualquier lugar dentro del ámbito metropolitano.

### 2.1.1 Historia y actualidad

La tecnología inalámbrica está conviviendo con nosotros desde hace muchos años, nada menos que desde principios de los 90, aunque de manera desordenada, debido a que cada fabricante desarrollaba sus propios modelos, generando por ende dificultades a los otros.

A finales de los años 90, compañías como *Lucent*, *Nokia* o *Symbol Technologies*, se reunieron para crear una asociación conocida como *WECA (Wireless Ethernet Compatibility)*, que en 2003 pasó a llamarse *Wi-Fi Alliance*, cuyo objetivo, era no sólo el fomento de la tecnología Wifi, sino establecer estándares para que los equipos dotados de esta tecnología inalámbrica fueran compatibles entre sí.

En abril de 2000 se establece la primera norma: Wifi 802.11b, que utilizaba la banda de los 2.4Ghz y que alcanzaba una velocidad de 11Mbps. Tras esta especificación llegó 802.11a, que generó algunos problemas entre Estados Unidos y Europa por la banda que se utilizaba (5 Ghz).

Mientras que en Estados Unidos esta banda estaba libre, en Europa estaba reservada para fines militares, situación que paralizó un tanto esta tecnología inalámbrica, sobre todo teniendo en cuenta que la mayoría de los fabricantes de dispositivos (norteamericanos en su mayor parte), tardaron en reaccionar ante la imposibilidad de vender sus productos en el viejo continente. Tras muchos debates se aprobó una nueva especificación, 802.11g, que al igual que la “b” utilizaba la banda de los 2,4GHz pero multiplicaba la velocidad hasta los 54Mbps.

Llegado el momento en que tres especificaciones diferentes conviven en el mercado, se da el caso de que son incompatibles, por lo que el siguiente paso fue crear equipos capaces de trabajar con las tres, saltando “en caliente” de unas a otras, y lanzado soluciones que se etiquetaban como “multipunto” cuando se da este caso la banda de los 5GHz, anteriormente reservada para usos militares, se habilitó para usos civiles, lo que fue un gran adelanto no sólo porque es ese momento ofrecía la mayor velocidad, sino porque no existían otras tecnologías inalámbricas, como *Bluetooth*, *Wireless USB* o *ZigBee* que utilizan la misma frecuencia.

Hoy estamos inmersos en la especificación 802.11n, que trabaja a 2,4GHz a una velocidad de 108 Mbps, una velocidad que gracias a diferentes técnicas de aceleración, es capaz de alcanzar 802.11g. Una de las curiosidades de la especificación 802.11n es que los productos han llegado al mercado antes de aprobarse el estándar, denominándose *Draft-N*, lo que hace referencia a que están sujetos al borrador y no al estándar definitivo. *Wi-Fi* es un sistema de envío de datos sobre redes computacionales, que utiliza ondas de radio en lugar de cables, además es una marca de la Wi-Fi Alliance (anteriormente la WECA: *Wireless Ethernet Compatibility Alliance*), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11

La WECA tiene como misión certificar la interoperabilidad y compatibilidad entre diferentes fabricantes de productos Wireless bajo el estándar IEEE802.11. La WECA fue fundada por 3Com, Cisco, Intersil, Agere, Nokia y Symbol en Agosto de 1999, con el compromiso de impulsar el desarrollo a nivel mundial de la tecnología de LAN inalámbrica bajo el estándar IEEE 802.11.

La lista de miembros se ha incrementado hasta los 170. Desde entonces, Internet, Microsoft e Intel han formado el comité de dirección de WECA. WECA establece un procedimiento de certificación para garantizar la interoperabilidad de los dispositivos entre fabricantes. Aquellos dispositivos con el logo *WiFi* gozan de esa garantía de interoperabilidad. El *Wi-Fi* fue creado para ser utilizado en redes locales inalámbricas.



Figura 20. Símbolo de la alianza de Wi-Fi

<http://www.ubergizmo.com/2012/08/wifi-emergency-mesh-network/>

## 2.1.2 Ventajas de las redes inalámbricas

Las principales ventajas que ofrecen las redes inalámbricas frente a las redes cableadas son las siguientes, movilidad la libertad de movimientos es uno de los beneficios más evidentes las redes inalámbricas. Un ordenador o cualquier otro dispositivo (por ejemplo, una PDA o una webcam) pueden situarse en cualquier punto dentro del área de cobertura de la red sin tener que depender de que si es posible o no hacer llegar un cable hasta este sitio. Ya no es necesario estar atado a un cable para navegar en Internet, imprimir un documento o acceder a los recursos.

Compartidos desde cualquier lugar de ella, hacer presentaciones en la sala de reuniones, acceder a archivos, sin tener que tender cables por mitad de la sala o depender de si el cable de red es o no suficientemente largo.

Desplazamiento. Con una computadora portátil o PDA no solo se puede acceder a Internet o a cualquier otro recurso de la red local desde cualquier parte de la oficina o de la casa, sino que nos podemos desplazar sin perder la comunicación. Esto no solo da cierta comodidad, sino que facilita el trabajo en determinadas tareas, como, por ejemplo, la de aquellos empleados cuyo trabajo les lleva a moverse por todo el edificio.

Flexibilidad. Las redes inalámbricas no solo nos permiten estar conectados mientras nos desplazamos por una computadora portátil, sino que también nos permite colocar una computadora de sobremesa en cualquier lugar sin tener que hacer el más mínimo cambio de configuración de la red. A veces extender una red cableada no es una tarea fácil ni barata. En muchas ocasiones acabamos colocando peligrosos cables por el suelo para evitar tener que hacer la obra de poner enchufes de red más cercanos. Las redes inalámbricas evitan todos estos problemas. Resulta también especialmente indicado para aquellos lugares en los que se necesitan accesos esporádicos. Si en un momento dado existe la necesidad de que varias personas se conecten en la red en la sala de reuniones, la conexión inalámbrica evita llenar el suelo de cables. En sitios donde pueda haber invitados que necesiten conexión a Internet (centros de formación, hoteles, cafés, entornos de negocio o empresariales) las redes inalámbricas suponen una alternativa mucho más viable que las redes cableadas.

Ahorro de costes. Diseñar o instalar una red cableada puede llegar a alcanzar un alto coste, no solamente económico, sino en tiempo y molestias. En entornos domésticos y en determinados entornos empresariales donde no se dispone de una red cableada porque su instalación presenta problemas, la instalación de una red

inalámbrica permite ahorrar costes al permitir compartir recursos: acceso a Internet, impresoras, etc. Escalabilidad. Se le llama escalabilidad a la facilidad de expandir la red después de su instalación inicial. Conectar una nueva computadora cuando se dispone de una red inalámbrica es algo tan sencillo como instalarle una tarjeta y listo. Con las redes cableadas esto mismo requiere instalar un nuevo cableado o lo que es peor, esperar hasta que el nuevo cableado quede instalado. (Falcon, 2004)

## **2.2 Elementos de las redes Inalámbricas**

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está siendo ampliamente investigada. Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos.

También es útil para hacer posibles sistemas basados en plumas. Pero la realidad es que esta tecnología está todavía en pañales y se deben de resolver varios obstáculos técnicos y de regulación antes de que las redes inalámbricas sean utilizadas de una manera general en los sistemas de cómputo de la actualidad.

No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas. Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Mientras que las redes inalámbricas actuales ofrecen velocidades de 2 Mbps, las redes cableadas ofrecen velocidades de 10 Mbps y se espera que alcancen velocidades de hasta 100 Mbps.

Los sistemas de Cable de Fibra Óptica logran velocidades aún mayores, y pensando futuristamente se espera que las redes inalámbricas alcancen velocidades de solo 10 Mbps. Sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una "Red Híbrida" y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina. (A., 2013)

### 2.2.1 Direcciones IP

El lenguaje que utiliza para expresar la dirección de la computadora son los números. Un ejemplo de dirección IP podría ser: 158.42.65.38. Existen algunas reglas en la estructura de estas direcciones. Cuatro números como de un máximo de tres cifras, separados por tres puntos. El valor máximo que puede alcanzar cada número es 255, cuando el número es de dos o una cifra no se incluye ceros a la izquierda.

Toda computadora conectada a internet (o a cualquier red) posee una identificación única, llamada dirección *IP* (en inglés, *Internet Protocol*), compuesta por cuatro combinaciones de números. La dirección IP consiste en un número de 32 bits que en la práctica vemos siempre segmentado en cuatro grupos de 8 bits cada uno (xxx.xxx.xxx.xxx). Cada segmento de 8 bits varía de 0-255 y están separados por un punto. Esta división del número IP en segmentos posibilita la clasificación de las direcciones IPs en 5 clases: A, B, C, D e Y.

El IP estático (o fijo) es un número IP asignado permanentemente a una computadora, o sea, su dirección IP no cambia, excepto si dicha acción se fuera realizada manualmente. Por ejemplo, hay casos de proveedores de acceso a internet por ADSL, que les asignan un IP estático a algunos de sus clientes. Así, siempre que un cliente esté conectado, usará el mismo IP en Internet. Esa práctica es cada vez menos frecuente entre los proveedores de acceso, por una serie de factores, que incluye problemas de seguridad.

El IP dinámico, por su parte, es un número que es asignado a una computadora cuando esta se conecta a la red, pero que cambia cada vez que se establece la conexión. Por ejemplo, supón que te conectaste con tu computadora a internet hoy. Cuando te conectes mañana, te será asignada otra IP. Para entender mejor, imagina la siguiente situación: una empresa tiene 40 computadoras conectadas en red. Usando IPs dinámicos, la empresa pone a disposición 40 direcciones IP para tales computadoras. Como ninguna IP es fija, cuando una computadora "entra" en la red, le es asignada una IP de esas 40 que no esté siendo usada por ninguna otra computadora. Es más o menos así que los proveedores de internet trabajan. Cada vez que te conectas a internet, tu proveedor le da a tu computadora una IP que esté libre. El método más usado para la distribución de IPs dinámicas es el protocolo DHCP (*Dynamic Host Configuration Protocol*). (Staff, 2007)



Figura 21. Distribución de números IP 1992  
<https://tecmoviles1992.wordpress.com/2014/10/24/como-cambiar-tu-direccion-ip/>

### 2.2.2 Mascara de subred

La máscara de subred es un entero de 32 bits exclusivo que define la parte de la red donde se conecta una interfaz. La máscara debe especificarse siempre conjuntamente con una dirección de red (IP). La máscara de subred es una máscara de bits que determina la parte de sistema principal y la parte de red de una dirección IP (Protocolo Internet). La máscara de subred es un entero de 32 bits exclusivo que define la parte de la red donde se conecta una interfaz. La máscara debe especificarse siempre conjuntamente con una dirección de red (IP). La máscara tiene el formato xxx.xxx.xxx.xxx, en el que cada campo es la representación decimal de 1 byte (8 bits) de la máscara.

Por ejemplo, la máscara de subred cuya representación hexadecimal es X'FFFFFF00', en notación decimal es 255.255.255.0. Los bits de la máscara que se establecen en 1 determinan las partes de red y subred de la dirección. Los bits que se establecen en 0 determinan la parte de sistema principal de la dirección. La máscara de subred y la dirección IP permite a IP determinar dónde debe enviar los datos que recibe. IP correlaciona lógicamente la máscara de subred con una dirección IP. Esta acción permite determinar qué bits de la dirección pertenecen a la parte de red y qué bits de la dirección pertenecen a la parte de sistema principal. La máscara de subred permite dividir una red entre varias redes más pequeñas denominadas subredes. Las subredes representan una red dentro de otra red. Todas las direcciones IP que están en la misma subred, o red, tienen la misma máscara de subred. Estas direcciones incluyen el sistema principal y las direcciones de red o subred. (boulder, 2012)



### 2.2.3 Puerta de enlace

Es la dirección IP privada de nuestro router. Puerta de enlace o pasarela (*gateway*) es el dispositivo que permite interconectar redes de computadoras con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red inicial, al protocolo usado en la red de destino. La puerta de enlace es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones de red (*Network Address Translation*, NAT). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada enmascaramiento de IP (*IP Masquerading*), usada muy a menudo para dar acceso a Internet a los equipos de una LAN compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa. (Attribution/Share-Alike, 2013)

### 2.2.4 Servidores DNS

Un servidor DNS proporciona resolución de nombres para redes basadas en TCP/IP. Es decir, hace posible que los usuarios de equipos cliente utilicen nombres en lugar de direcciones IP numéricas para identificar hosts remotos. Un equipo cliente envía el nombre de un host remoto a un servidor DNS, que responde con la dirección IP correspondiente.

El equipo cliente puede entonces enviar mensajes directamente a la dirección IP del host remoto. Si el servidor DNS no tiene ninguna entrada en su base de datos para el host remoto, puede responder al cliente con la dirección de un servidor DNS que pueda tener información acerca de ese host remoto, o bien puede consultar al otro servidor DNS. Este proceso puede tener lugar de forma recursiva hasta que el equipo cliente reciba las direcciones IP o hasta que se establezca que el nombre consultado no pertenece a ningún host del espacio de nombres DNS especificado.

Los servidores DNS son parte de la cadena que queda formada cuando hacemos una petición mediante nuestro navegador de cualquier página web. Estos servidores no son más que computadoras que en sus discos duros almacenan enormes bases de datos. Tienen registrada la relación que existe entre cada nombre de dominio y su dirección IP correspondiente. Los seres humanos identificamos los sitios de internet mediante nombres, como son Google.com, Yahoo.es, Apple.com, etc. lo que los hace más fácil de recordar y de escribir, estos nombres es lo que conocemos como nombres de dominio.

Las computadoras identifican los sitios web y se conectan a ellos utilizando el formato numérico, algo parecido a la numeración telefónica, pero más complejo y con más recursos, es lo que conocemos como las direcciones IP. Ahí es donde entran en acción los servidores DNS, ellos son como enormes y complejas guías telefónicas, que a petición nuestra traducen o convierten los nombres de dominio que le solicitemos, en las direcciones IP que les corresponden. (Server, 2008)

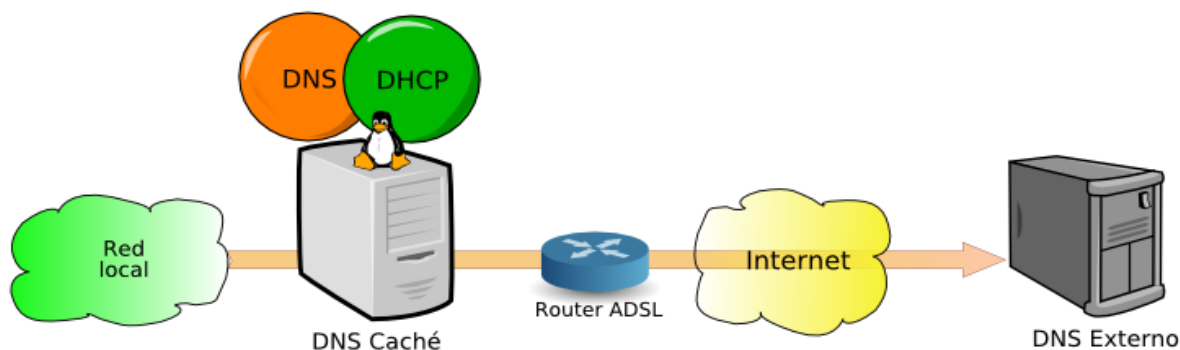


Figura 22. Distribución de un servidor DNS

<http://recursostic.educacion.es/observatorio/web/gl/software/software-general/638-servidor-dns-sencillo-en-linux-con-dnsmasq>

### 2.2.5 SSID (*Service Set Identification*)

Nombre con el que se identifica a una red *Wi-Fi*. Este identificador viene establecido de fábrica pero puede modificarse a través del panel de administración del punto de acceso. El SSID (*Service Set Identifier*) es un nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres, que la mayoría de las veces son alfanuméricos (aunque el estándar no lo especifica, así que puede consistir en cualquier carácter). Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID. Existen algunas variantes principales del SSID. Las redes ad-hoc, que consisten en máquinas cliente sin un punto de acceso, utilizan el BSSID (*Basic Service Set Identifier*); mientras que en las redes en infraestructura que incorporan un punto de acceso se utiliza el ESSID (*Extended Service Set Identifier*). Es posible referirse a cada uno de estos tipos, como SSID en términos generales. A menudo al SSID se le conoce como “nombre de la red”. Uno de los métodos más básicos de proteger una red inalámbrica es desactivar la difusión (*broadcast*) del SSID, ya que para el usuario medio no aparecerá como una red en uso. Sin embargo, no debería ser el único método de defensa para proteger una red inalámbrica. Se deben utilizar también otros sistemas de cifrado y autenticación. (Alfredo, 2008)

## 2.2.6 DHCP

DHCP funciona sobre un servidor central (servidor, estación de trabajo o incluso un PC) el cual asigna direcciones IP a otras máquinas de la red. Este protocolo puede entregar información IP en una LAN o entre varias VLAN. Esta tecnología reduce el trabajo de un administrador, que de otra manera tendría que visitar todos los ordenadores o estaciones de trabajo uno por uno. Para introducir la configuración IP consistente en IP, máscara, *gateway*, DNS. El DHCP (*Dynamic Host Configuration Protocole*) es un mecanismo que permite asignar automáticamente los valores necesarios para la comunicación en la red (dirección IP, mascara de subred, puerto de enlace, DNS). Es práctico pero también para un hacker, que no tendrá que adivinar la configuración de la ya conocida y dependiente de tu subred. Una vez que la red esté instalada y operativa, mejor usar una IP fija (uno decide la IP y la conserva), y además esto permitirá compartir archivos e impresoras. (Portatiles, 2014)



Juan Ríos. Figura 23. Dynamic Host Configuration Protocol 2015  
<http://www.taller-i.net/index.php/redes>

## 2.2.7 Dirección MAC

Es el código único de identificación que tienen todas las tarjetas de red además de nuestro PDA con *WiFi* integrado, al ser un dispositivo de red, también tendrá una dirección MAC única. En las redes de computadoras, la dirección MAC (siglas en inglés de *media access control*; en español "control de acceso al medio") es un identificador de 48bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo.

Está determinada y configurada por el IEEE (los primeros 24 bits) y el fabricante (los últimos 24 bits) utilizando el *organizationally unique identifier*. La mayoría de los protocolos que trabajan en la capa 2 del modelo OSI usan una de las tres numeraciones manejadas por el IEEE: MAC-48, EUI-48, y EUI-64, las cuales han sido diseñadas para ser identificadores globalmente únicos. No todos los protocolos

de comunicación usan direcciones MAC, y no todos los protocolos requieren identificadores globalmente únicos.

Es también: La Dirección del Hardware de Control de acceso a soportes de un distribuidor que identifica los equipos, los servidores, los *routers* u otros dispositivos de red. Al mismo tiempo es un identificador único que está disponible en NIC y otros equipamientos de red. (Commons, 2015)



Figura 24. Ejemplo de una dirección MAC 2001  
<http://www.seguridad.unam.mx/noticia/?noti=672>

### 2.3 Hardware para redes inalámbricas

La clave para el crecimiento del acceso inalámbrico a internet es la tecnología *WiFi*, la cual combina una serie de tecnologías inalámbricas relacionadas entre sí. *WiFi* es un conjunto de estándares para redes inalámbricas. *Wifi* es la marca de la *WiFi* Alliance (anteriormente la *Wireless Ethernet Compatibility Alliance*), la organización comercial que prueba y certifica que los equipos cumplen con los estándares IEEE 802.11X.

Se trata de un estándar emergente que hace posible que las empresas de hardware fabriquen productos inalámbricos que puedan comunicarse unos con otros. Envía las páginas web y las llamadas telefónicas a través de ondas de radio, haciendo innecesario el uso de costosos cables y ofreciendo un servicio de internet de alta velocidad. La utilidad de *WiFi* es tanto doméstica como empresarial.

### 2.3.1 Modem ADSL

Es un equipo que convierte las señales digitales del ordenador a las analógicas de la línea telefónica (modulación), las envía a otro ordenador y cuando las recibe este las vuelve a convertir de analógicas a digitales (demodulación). Permite conectar equipos que están muy separados físicamente o para acceder a internet, a través de la red telefónica conmutada. Actualmente está en desuso.

En las décadas de los años 80 y 90, los módems fueron los dispositivos de transmisión de datos más extendidos. Antes de que las operadoras de telecomunicaciones construyeran las grandes redes digitales, la única forma de transmitir datos a la larga distancia era utilizando la red telefónica conmutada y en este escenario los módems eran fundamentales.

Actualmente, el desarrollo de las redes digitales así como el uso de nuevas tecnologías como ADSL y cable han propiciado que muchos casos los módems tradicionales hayan dejado de utilizarse. Además la velocidad de transmisión de dato utilizando dichos módems había alcanzado su límite. La tecnología ADSL se utiliza para aprovechar todo el ancho de banda que ofrece el bucle local de abonado y multiplexar las señales de voz y datos (se verá más profundidad en un capítulo posterior). Ofrece lo que se conoce comúnmente como acceso de banda ancha a las redes de datos, especialmente internet.

Su inconveniente es que requiere la adaptación de las infraestructuras de comunicaciones de los operadores, además su uso depende de un factor importante que es la longitud del bucle de abonado, siendo imposible su uso para distancias mayores a 5km. Lógicamente para hacer uso de la tecnología ADSL es necesario utilizar un modem o un router diseñado a tal efecto. Los módems ADSL al igual que los módems de banda vocal, pueden ser internos o externos aunque la mayor parte de los que han comercializado son externos. A diferencia de los módems de banda vocal, los módems ADSL externos utilizan el interface USB para su conexión con el ordenador debido sobre todo a las velocidades más altas que se alcanzan con este interfaz.



Figura 25. Modem ADSL

<http://www.sysnetcenter.com/121-dlink-dsl2640t-54mbps-wireless-adsl2-router-modem-4port-100mbps->



Figura 26. Modem y tarjeta de red 2015

<http://computacion.mercadolibre.com.mx/modem-usb-externo-56k-v.92-fax-modem-externo>

### 2.3.2 Conmutador (Switch)

Un conmutador se utiliza igual que un concentrador pero se caracteriza por no enviar los paquetes a todos los puertos, si no únicamente por el puerto correspondiente al destinatario de los datos. Su función consiste en tomar la dirección MAC destino de una trama de datos (es la dirección que identifica a la tarjeta de red) y, en función d ella, enviar la información por el puerto correspondiente. En comparación con el concentrador, actúa más inteligentemente ya que filtra el tráfico y tiene capacidad de reconocimiento. Los datos pueden conducirse por rutas separadas, mientras que en el concentrador, las tramas son conducidas por todos los puertos. Los conmutadores son capaces de realizar esto utilizando una mejor electrónica que la empleada por los concentradores, troceando el ancho de banda en franjas, llamadas canales, lo suficientemente grandes para dar servicio a cada puerto de conmutación.

De esta manera, utilizando un conmutador se puede dividir una red en varios segmentos y limitar el tráfico al segmento o segmentos a los que pertenece el paquete. Su utilización permite que cada usuario o grupo de usuario tenga su propio segmento dedicado con ancho de banda dedicado, con una mucha menor tasa de colisiones y un mejor tiempo de respuesta en lugar de lo que ocurren en una red Ethernet tradicional en la que muchos usuarios comparten el mismos ancho de banda.



Figura 27. Conmutador (Switch)

[http://www.ipexpress.cl/pyme/product\\_info.php/switch-cisco-ws-c2960x-48fps-p-713](http://www.ipexpress.cl/pyme/product_info.php/switch-cisco-ws-c2960x-48fps-p-713)

### 2.3.3 Encaminador (Router)

Un encaminador no solo incorpora la función de filtrado característico de los puentes, sino que, además, determina la rutina hacia su destino. Se utiliza tanto en redes de área local como en redes de área extensa. Permite la comunicación entre un equipo individual e internet, entre una red e internet o entre dos redes.

Las funciones de un router son:

- Interconectar redes (físicas y lógicas).
- Recibir los paquetes de datos y almacenarlos para distribuirlos progresivamente en función de la situación de la red.
- Averiguar las direcciones IP de las redes y equipos que están conectados a sus puertos para realizar un envío óptimo de los paquetes.
- Evitar la congestión de las redes.

Un router posee dos direcciones IP, una publica para acceder a internet y otra privada para la red interna.

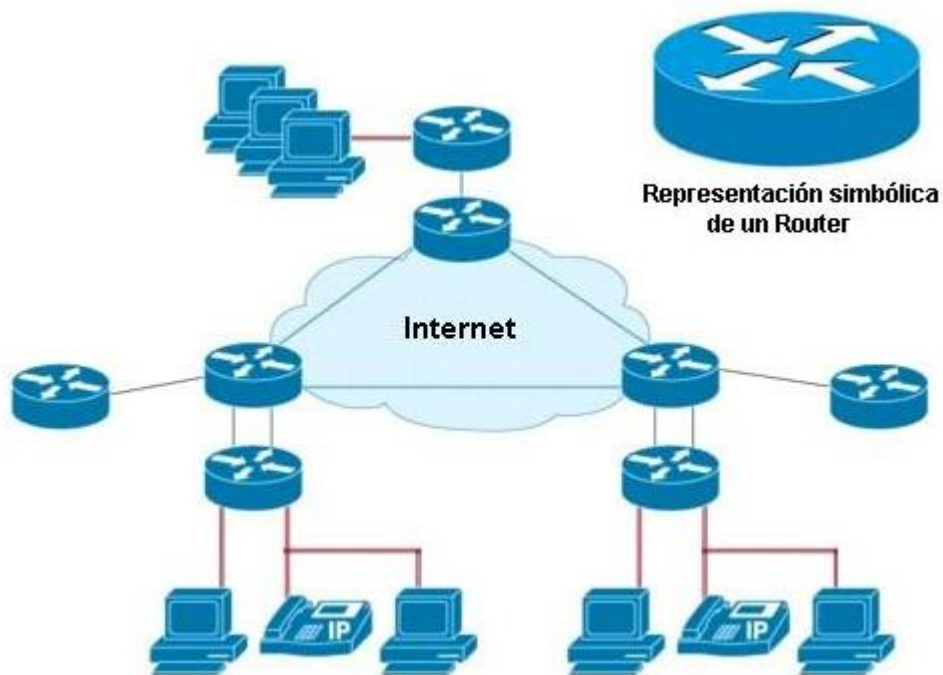


Figura 28. Diagrama de conexión de red mediante *routers*

<http://sincables.com.ve/v3/content/64-routers>

### 2.3.4 Puente (Bridge)

Es un sistema formado por hardware y software que permite conectar dos redes locales entre sí. Se pueden colocar en el servidor de archivo o, mejor, en el servidor de comunicaciones.

Cuando dos redes locales necesitan comunicarse entre sí, necesitan contar con un puente, en cada una de ellas para poder conectarse. Ambas redes han de usar el mismo protocolo de comunicaciones.

Sus funciones básicas son las de auto aprendizaje, filtrado y reenvío. Es decir, si necesita reenviar un paquete de datos a una dirección de red que no está incluida en su tabal de destinos, examina los campos de dirección del paquete (filtrado) y las dirige alas dirección que ha localizado (reenvió). A continuación la añade a su tabla de destino (autoaprendizaje).

La utilización de puentes para unir dos redes es una idea mejor que la configuración de una red grande que englobe a amabas. La razón está en que las redes van perdiendo rendimiento a aumentar el tráfico y se va perdiendo tiempo de respuesta, de este modo mal estar dividida la red se reduce el tráfico y el tiempo de respuesta.

Otra razón es el imite de expansión de la red grande. Todas las redes cuentan con un número máximo de estaciones que pueden soportar, si se desea sobrepasar ese número la única alternativa es crear otra red conectada por un puente.

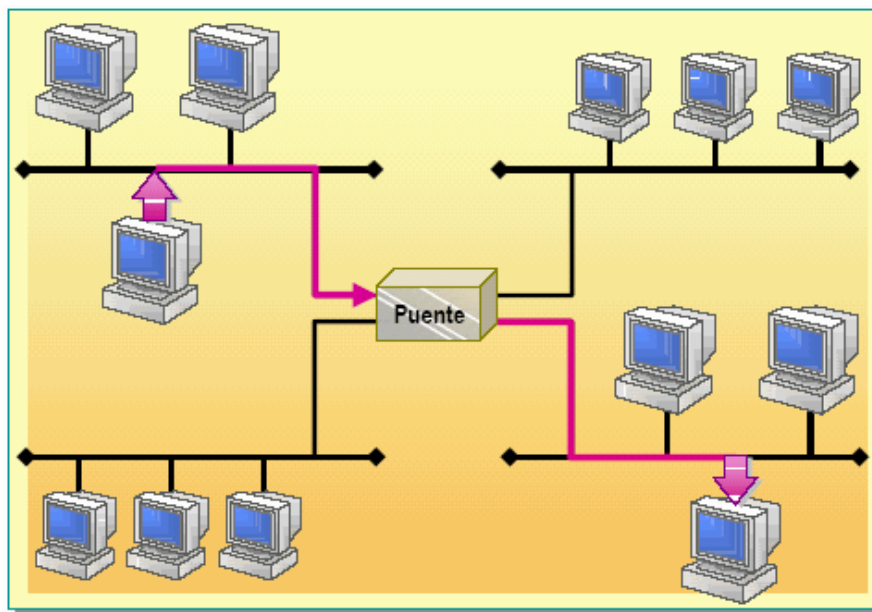


Figura 29. Diagrama de uso de un puente 2012  
<http://www.taringa.net/posts/info/14318822/Otros-dispositivos-de-networking-redes-interconexion.html>



### 2.3.5 Pasarela (Gateway)

Es un sistema formado por hardware y software que permite las comunicaciones entre una red local y un gran ordenador (mainframe) o un mini ordenador (por que utilizan protocolos de nivel de transporte, sesión, presentación y aplicación distintos). Se suelen colocar en el servidor de comunicaciones.

De este modo podrá obtener datos del mini o del mainframe o bien enviarles datos para su almacenamiento. La pasarela realiza la traducción completa entre las familias de protocolos, proporcionando una conectividad completa entre redes de distinta naturaleza.

El enlace entre ambos protocolos necesitara algún tipo de emulación que haga que la estación de trabajo imite le funcionamiento de un terminal y ceda el control al mini o al mainframe. Esta emulación se puede conseguir por medio de software (con un programa), de hardware (con una tarjeta) o de ambos.

Al igual que los encaminadores, están definidos par a un determinado escenario de comunicaciones. Pero a cambio de sus ventajas, el retraso de propagación de un paquete que atraviesa una pasarela es mucho mayor que el experimentado en los otros dispositivos.

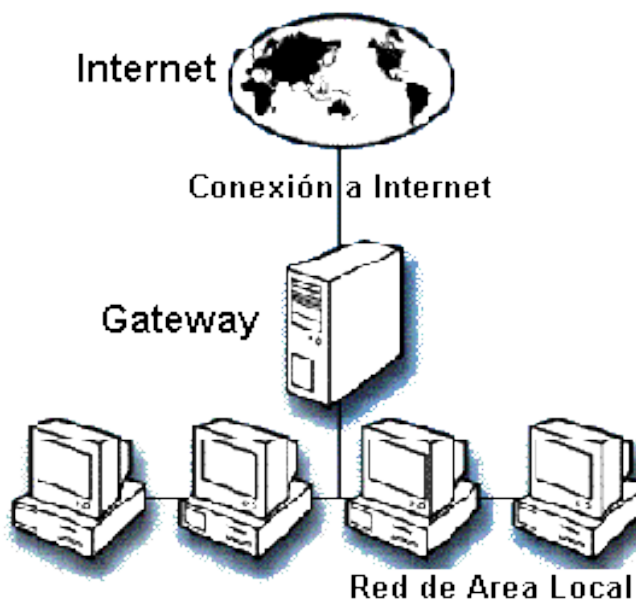


Figura 30. Esquema de funcionamiento Gateway  
<http://www.abcnet.es/gateways-o-puertas-de-enlace/>

### 2.3.6 Cortafuegos (Firewalls)

La función de uno cortafuegos (firewall) es filtrar los intentos de establecimiento de conexión de forma que se pueda detectar e impedir el acceso al sistema a posibles intrusos sin que ni siquiera se halla llegado a establecer un enlace directo entre ellos. El cortafuego puede ser configurado para permitir que solo determinadas dirección, origen y destino, puedan acceder a su red (o desde ella).

Las funciones de cortafuegos se pueden realizar por:

- Ordenadores dedicados exclusivamente al filtrado de paquetes (servidor proxy).
- Encaminadores de red (*routers*) configurados para esta tarea.
- Programas de software para distintos sistemas operativos.
- Cualquier otro dispositivo intercalado entre la red y el exterior que soporte el filtrado de paquetes según unos parámetros previamente definidos.

Entre los posibles beneficio de utilizar cortafuegos se encuentran:

- Acceso controlado a la red.
- Protección para servicios de internet que sean vulnerables.
- Administración de seguridad centralizada.
- Estadísticas de las conexiones a la red.
- Filtrado sofisticado de paquetes. Los filtros de paquetes controlan que tipos de paquetes IP pueden acceder a los servicios de la red interna. Así, pueden denegar paquetes, bloquear paquetes de un ordenador determinado de internet, rechazar direcciones fantasmas.

Entre las posibles razones para no utilizar un cortafuegos se encuentran:

- El acceso a los servicios deseados puede llegar a ser más complejo así como su configuración de lo normal, aunado a esto el coste es mayor.
- El peligro de acceso por una puerta trasera a la red se incrementa sino se tiene previsto su inutilización, necesaria administración de la red.

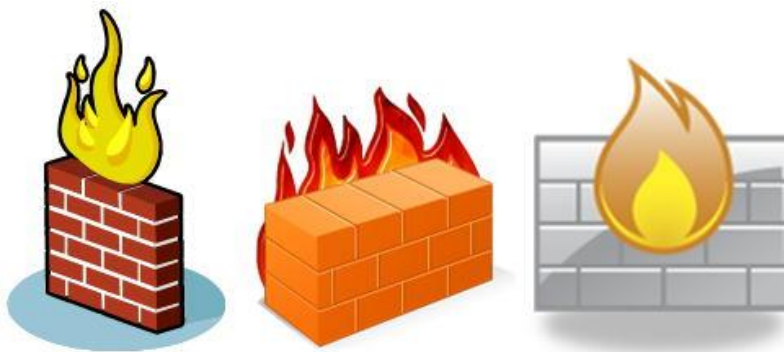


Figura 31. Representación simbólica de un Firewall  
<http://tecnologyc.com/para-que-sirve-el-firewall/>

### 2.3.7 Punto de acceso (*Access Point*)

Un punto de acceso es el dispositivo que se utiliza para conectar los diferentes equipos con las redes inalámbricas que poseen una arquitectura en modo infraestructura. El punto de acceso es el componente que ofrece cobertura inalámbrica a todos los equipos conectados a la red. Por lo tanto el punto de acceso es el elemento fundamental que debe existir en una red inalámbrica, y su objetivo básico consiste en gestionar de manera centralizada la comunicación entre los dispositivos de la red.



Figura 32. Access Point (Linksys) 2011  
<http://www.adslzone.net/postt175513.html>

Un punto de acceso consiste en un equipo de radio que dispone de uno o varias antenas que se usan para transmitir y recibir información, con varios conectores RJ-45 que sirven de enlace físico a la red cableada. Los puertos RJ-45 se pueden usar para conectar la red inalámbrica a una red cableada o a internet. Los puntos de acceso incorporan en su interior un *switch*, y a veces incluso incorporan puertos paralelos o USB para poder compartir impresoras sin necesidad de conectarlas a un ordenador. Un punto de acceso, al igual que un *switch*, incorpora una serie de led que indican en cada momento la actividad del enlace.

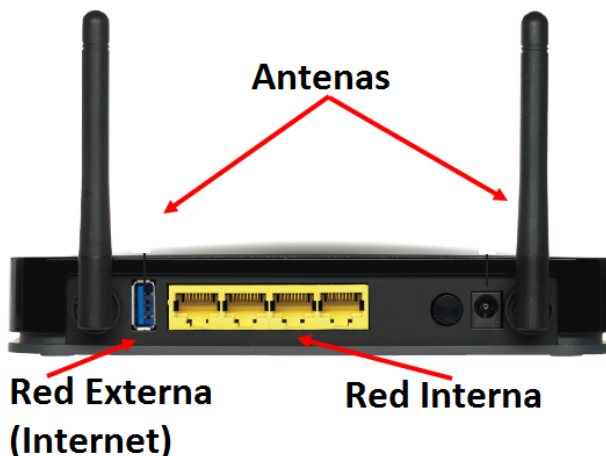


Figura 33. Partes de un Linksys  
<http://www.linksys.com/ar/support-article?articleNum=136692>

Los puntos de acceso hardware suelen ofrecer múltiples servicios como servidor DHCP, filtrado de direcciones MAC, cifrado WEP, cifrado WPA2, etc. Actualmente casi todos los puntos de acceso del mercado suelen incorporar un servidor web que permite configurar el punto de acceso de una forma fácil y cómoda. Para configurar un punto de acceso debe abrir el navegador y escribir la dirección IP que tiene por defecto.



Figura 34. Interfaz de configuración Netgear  
<http://tech.ifelix.net/5501.html>

Los parámetros de configuración más importantes de un punto de acceso son:

- Nombre de la red (SSID). Es el nombre que identifica la red inalámbrica.
- Canal de trabajo. Existen hasta 11 canales de funcionamiento y puede configurar el punto de acceso para que trabaje en un canal determinado o que lo selecciones de forma automática.
- Protocolo de cifrado. Existen protocolos de cifrado: el WEP y el WPA. Por su seguridad se aconseja utilizar el protocolo WPA ya que el protocolo WEP se puede “romper” en pocos minutos. (Cabrera, 2008)

### 2.3.8 Adaptadores de red

Un adaptador de red inalámbrico es un componente hardware que permite a un ordenador conectarse a una red inalámbrica. Se trata por lo tanto de un tipo especial de tarjeta de red o NIC (*Network interface controller*) que permite al usuario conectarse a una red sin necesidad de usar cable. Existen en el mercado numerosos modelos de adaptadores de red inalámbricos que se diferencian dependiendo del bus de expansión que utilizan (PCMCIA, PCI, USB...) y la normativa 802.11 que utilizan (802.11b, 802.11g o 802.11n).

El precio de los adaptadores depende de la normativa que utilizan y del bus de conexión. Los adaptadores más baratos son aquellos que utilizan bus USB y PCI, y los más caros son aquellos que utilizan bus PCMCIA o SD. Respecto a la normativa, lógicamente los adaptadores más caros son aquellos que utilizan una normativa más rápida. Por ejemplo los adaptadores 802.11g son más caros que los 802.11b.

A continuación se van a analizar los diferentes adaptadores dependiendo del bus de expansión que utilizan:

- Adaptadores PCMCIA. Suelen utilizarse sobre todo en los ordenadores portátiles, para expandir su funcionalidad en aspectos muy variados, como puede ser por ejemplo añadirles una tarjeta de red, un nuevo disco duro o memoria. La conexión PCMCIA se ha aplicado todo tipo de componentes del mercado que por supuesto existen numerosos modelos de adaptadores de red inalámbricos disponibles en este formato.



Figura 35. Tarjeta PCMCIA

[http://conmutelgdl.mex.tl/102232\\_Equipos-Para-Telefonia-y-Redes.html](http://conmutelgdl.mex.tl/102232_Equipos-Para-Telefonia-y-Redes.html)

- Adaptadores PCI e ISA. Los dispositivos PCI (*Peripheral Component InterConnect*) son componentes hardware que se conectan directamente a la placa base del ordenador, por lo tanto es necesario abrir el equipo para instalar un adaptador inalámbrico PCI en el sistema. También hay tarjetas de red inalámbricas ISA, sin embargo este tipo de conector no es tan eficiente como el PCI, ya que los dispositivos PCI se configuran automáticamente al arrancar el sistema y en los adaptadores ISA hay que configurar algunos parámetros como los IRQ, utilizando para ello *jumpers* externo. Además, actualmente el bus ISA se está quedando obsoleto ya que no suelen incorporarse en las nuevas placas base.



Figura 36. Tarjetas de red inalámbricas  
<http://tarjetasdered-tiposycaracteristicas.blogspot.mx/>

- Adaptadores USB. El conector USB (Universal Serial Bus) se aplica actualmente a casi todos los dispositivos que pueden comunicarse con un ordenador, ya que se trata de un estándar que se ha extendido por todo el mundo y garantiza la compatibilidad entre dispositivos que usan este tipo de conector.



Figura 37. Adaptador de red USB

[http://www.9channel.com/taobao/product-1113324371773-Netcore-\(Netcore\)-54M-Wireless-USB-adapter-NW330.html](http://www.9channel.com/taobao/product-1113324371773-Netcore-(Netcore)-54M-Wireless-USB-adapter-NW330.html)

- Portátiles con WIFI. Actualmente casi todos los ordenadores portátiles que se venden en el mercado incorporan de serie un adaptador de red inalámbrico para poder conectarse a una red WIFI sin necesidad de añadir ningún dispositivo adicional. La incorporación de dichos adaptadores a los portátiles ha surgido como consecuencia de la enorme repercusión social y tecnológica que ha apostado la posibilidad de formar redes de ordenadores sin necesidad de crear para ello una instalación cableada.



Figura 38. Laptop con dispositivo Wi-Fi

<http://www.supportmycomputer.co.uk/product/hp-655-dual-core-laptop-14072.html>

### 2.3.9 Antenas direccional y omnidireccional

#### La antena direccional

Es una antena capaz de concentrar la mayor parte de la energía radiada de manera localizada, aumentando así la potencia emitida hacia el receptor o desde la fuente deseada y evitando interferencias introducidas por fuentes no deseadas. Orientan la señal en una dirección muy determinada con un haz estrecho pero de largo alcance, actúa de forma parecida a un foco de luz que emite un haz concreto y estrecho pero de forma intensa (más alcance). Generalmente el haz o apertura y el alcance son inversamente proporcionales, esto es a mayor apertura menos alcance y a menor apertura más alcance. El alcance de una antena direccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor. Parabólicas (disco o rejilla), con estas se consigue el mayor alcance, pueden llegar a los 5 Km. de distancia.



Figura 39. Antena direccional

[http://www.entrale.com/product\\_info.php?products\\_id=11408902](http://www.entrale.com/product_info.php?products_id=11408902)

#### Antena omnidireccional

Este tipo de antenas presenta menor ganancia, pero también posibilidad de recibir señales desde varias direcciones; por tanto, no se precisa conocer exactamente donde está situada la estación base, permitiéndose la recepción de radiación procedente de reflexiones. Esta última característica resulta ventajosa cuando se produce una pérdida de visibilidad directa ya que en ese caso es posible seguir recibiendo las señales a través de las reflexiones. (Gomez, 2008)



Figura 40. Antena omnidireccional

<http://www.empretel.com.mx/o/745-antena-omnidireccional-24-ghz-8-dbi-apertura-360-para-access-point-ap4000-mr-lr.html>



## 2.4 Clasificación de las redes inalámbricas

Podemos dividir las redes inalámbricas en cuatro grandes categorías, tomando como criterio de clasificación la cobertura que pueden alcanzar:

- Redes inalámbricas de área personal o WPAN (*Wireless Personal Area Network*). Son aquellas que cubren distancias cortas. Debido a su poca cobertura, estas redes se utilizan para interconectar dispositivos que se encuentran muy próximos entre sí, como por ejemplo impresoras y teclados inalámbricos a un ordenador. También se emplean con mucha frecuencia en las PDA. Su objetivo principal es eliminar el cableado en los dispositivos personales de uso más común ofreciendo así una mayor versatilidad. Estas redes se emplean dentro de lo que se ha denominado "espacio operativo personal", es decir, el espacio que rodea una persona. Algunas tecnologías que se utilizan en este tipo de redes son *bluetooth*, DECT y los infrarrojos.
- Redes inalámbricas de área local o WLAN (*Wireless Local Area Network*). Pueden tener un alcance de varios centenares de metros. Durante muchos años, este tipo de redes inalámbricas se crearon empleando tecnologías procedentes de diferentes fabricantes propietarios, y por lo tanto las redes eran incompatibles entre sí. Sin embargo con el paso del tiempo se ha impuesto el sistema WiFi, hasta hace poco desconocida, tiene en la actualidad una gran cantidad de aplicaciones: desde formar grandes redes inalámbricas de acceso a internet en bibliotecas públicas, hasta compartir recursos entre varios ordenadores conectados a la red inalámbrica doméstica. No obstante, aunque WiFi es la tecnología más utilizada en la segunda categoría de redes inalámbricas, no se pueden olvidar otras que también pueden ser de gran utilidad: *homeRF* e *HiperLan*.
- Redes inalámbricas de área metropolitana o WMAN (*Wireless Metropolitan Area Network*). Se utilizan para establecer comunicación entre diferentes ubicaciones dentro de una región metropolitana, aunque también se puede utilizar para conectar un campus universitario o varios edificios. Las tecnologías más usadas dentro de este tipo de redes son LMDS y WiMAX.
- Redes inalámbricas globales o WWAN (*Wireless Wide Area Network*). Son los sistemas basados en telefonía móvil y pueden cubrir todo un país o incluso varios países. Aunque los primeros sistemas fueron analógicos, más tarde aparecieron los sistemas digitales para transmisión de datos, como es el caso de la tecnología europea GSM (*Global System for Mobile Communications*) o la norteamericana CDMA (*Code Division Multiple Acces*). Las tecnologías WWAN se conocen también como sistemas de

segunda generación (2G), o los actuales sistemas de tercera generación (3G). (Hoy, 2007)

En la tabla 1-1 puede observar un resumen de las tecnologías más importantes que se usan en cada categoría de redes inalámbricas.

Tabla 3. Tecnologías usadas en las redes inalámbricas

<b>Categoría de red inalámbrica</b>	<b>Tecnologías utilizadas</b>
Redes inalámbricas de área personal (WPAN)	Bluetooth Infrarrojo DECT
Redes inalámbricas de área local (WLAN)	Wifi HomeRF HiperLAN
Redes inalámbricas de área metropolitana (WMAN)	LMDS WiMax
Redes inalámbricas globales (WWAN)	GSM GPRS UMTS HSDPA

A continuación en la tabla 1-2 puede ver una comparativa de las principales características de las tecnologías WPAN, WLAN, WMAN.

Tabla 4. Tabla comparativa de las tecnologías WPAN, WLAN y WMAN

	Tecnología	Frecuencia	Distancia	Velocidad	Inmune a los obstáculos
WPAN	Bluetooth	2,4 GHz	10 m	3 Mbps	No
	DECT	1,9 GHz	200 m	2 Mbps	Si
	Infrarrojo	3 a 6 Hz	2 m	16 Mbps	No
WLAN	WiFi	2,4 Y 5 GHz	300 m	500 Mbps	Si
	HomeRF	2,4 GHz	50 m	100 Mbps	Si
	HiperLAN	5 GHz	50 m	10 Mbps	Si
WMAN	LMDS	28 GHz	35 Km	8 Mbps	No
	WiMAX	2-11 GHz	50 Km	70 Mbps	Si

Grafico en el que se muestran la cobertura y ancho de banda de las diferentes tecnologías inalámbricas.

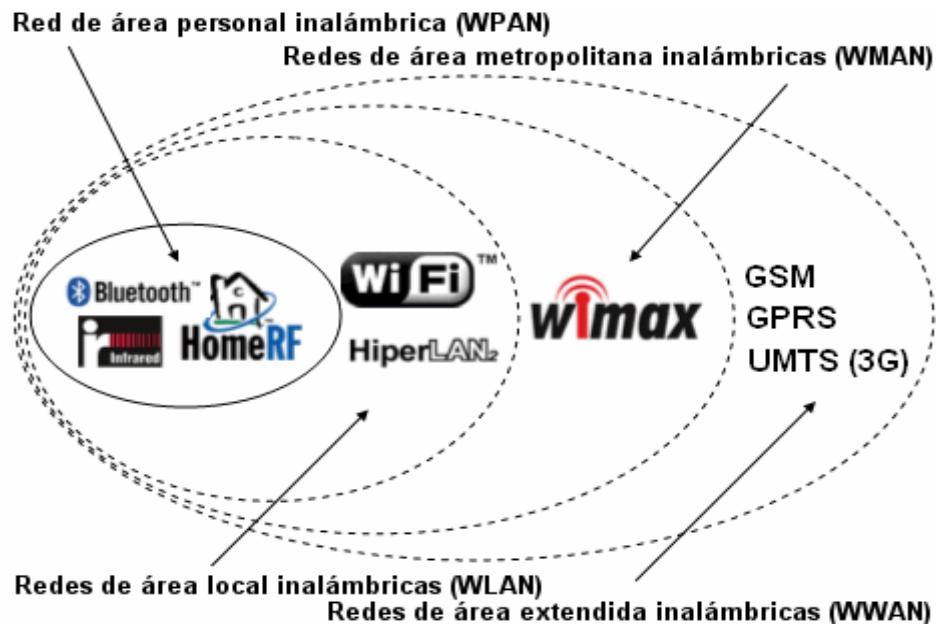


Figura 41. Esquema de tecnologías  
<https://infora.wikispaces.com/Dispositivos+de+comunicaci%C3%B3n.+Redes>

## 2.4.1 Redes inalámbricas de área personal (WPAN)

Las redes inalámbricas de área personal o WPAN (*Wireless Personal Area Network*) son las redes sin cables que ofrecen menor cobertura, pudiendo alcanzar desde los 10 metros máximos de alcance que ofrece *bluetooth*, hasta los casi 200 metros de DECT. Su principal objetivo es mejorar la comodidad del usuario eliminando el cableado de los dispositivos más comunes: teclado, impresora, teléfono, etc. Las principales tecnologías que se pueden utilizar para crear una WPAN son: *bluetooth*, DECT o infrarrojos. (Gomez J. , 2008)

### 2.4.1.1 Bluetooth

Bluetooth es una de las tecnologías más utilizadas, y surgió a partir de la necesidad de unir diferentes dispositivos entre sí, como pueden ser los teléfonos móviles, ordenadores, etc. En 1994 Ericsson desarrollo un estudio para intentar establecer comunicación a través de ondas de radio entre dispositivos, con el principal requisito de que la tecnología resultante tendría que ser económica.

En 1999 se fundó el consorcio SIG (*Special Interest Group*) de *bluetooth*, compuesto por grandes empresas que participan en proyectos comunes para desarrollar y publicar las especificaciones de esta tecnología. En un principio SIG estaba formado por multinacionales de la talla de Ericsson, Nokia, IBM, Intel, y posteriormente se agregaron otros gigantes como Microsoft.



Figura 42. Dispositivos conectados mediante bluetooth  
<http://principiosbasicosnetworking.wikispaces.com/>

Desde un punto de vista técnico, *bluetooth* transmite en la banda de frecuencia de 2,4 GHz. Esto se debe a que uno de los requisitos que se establecieron a priori para el desarrollo de *bluetooth* consistía en que tenía que ser operativo en cualquier lugar del planeta, y solo la banda ISM (Medico-científica internacional) cumple este requisito.

Bluetooth está basado en un sistema de saltos de frecuencia y división de tiempo dúplex, donde el canal queda dividido en slots de 625µs. El canal de comunicación tiene una capacidad de 1Mbps. El alcance de su cobertura de transmisión llega a los 10 metros de radio, aunque este valor puede aumentarse hasta los 100 metros con el uso de repetidores.

Existen varias versiones implementadas de *bluetooth*:

- Bluetooth v1.1: presenta problemas de incompatibilidad con *Wifi*, ya que ambos trabajan a 2,4 GHz.
- Bluetooth v1.2: representa un cambio muy significativo respecto a la versión 1.1, ya se solucionan los problemas de compatibilidad con *Wifi*. Además se mejora notablemente la eficiencia de la transmisión gracias a una técnica llamada *Adaptive Frequency Hopping (AFH)*, y se aumenta la factibilidad de configuración de la comunicación entre dispositivos bluetooth.
- Bluetooth v2.0: incorpora una técnica denominada *Enhanced Data Rate (EDR)* que aumenta la velocidad de transmisión hasta 3 Mbps.
- Bluetooth v2.1: disminuye el consumo de potencia y mejora la comunicación entre los dispositivos.

### 2.4.1.2 DECT

Ante la necesidad de normalizar las comunicaciones inalámbricas que se establecen entre dispositivos telefónicos, el instituto Europeo de Normas de Telecomunicaciones creó el estándar DECT (*Digital Enhanced Cordless Telecommunications*), que permite la transmisión de datos a distancias de hasta 200 metros. La comunicación con la tecnología DECT está orientada por lo tanto a la transmisión de voz y a la mejora de la calidad de transmisión. El uso de esta tecnología en teléfonos se ha extendido a lo largo de todo el planeta excepto en Norteamérica, donde se ha encontrado algunas barreras tecnológicas.



Figura 43. Teléfonos celulares con tecnología DECT  
<http://best2linecordlessphones.cheapwirelessmicrophones1.com/>

Los teléfonos que utilizan DECT se comunican con una base que a su vez está conectada a la roseta telefónica. Normalmente las bases son capaces de gestionar unos cinco teléfonos. Para establecer una comunicación interna entre dos teléfonos, la base solo tiene que crear una conexión inalámbrica entre ambos. Este tipo de llamadas son gratuitas y fáciles de gestionar por parte de la base.

A diferencia del *bluetooth*, que trabaja en una banda de frecuencia de 2,4 GHz, la frecuencia de radio DECT es de 1,9 GHz, con lo cual no se pueden producir interferencias entre ambas tecnologías. Su velocidad de transmisión es de 2 Mbps.

Como método de multiplexación, DECT utiliza la tecnología TDMA (*Time Division Multiple Access*) para transmitir información, que consiste en distribuir los datos en diferentes slots de tiempo proporcionando además acceso múltiple a varias frecuencias. Gracias a esta técnica varios usuarios pueden compartir un mismo canal, de tal modo que las conversaciones no interfieren entre sí.

### **2.4.1.3 Infrarrojo**

La comunicación por infrarrojo se creó para poder transmitir información entre dispositivos que se encuentran muy corta distancia. Consiste en una radiación electromagnética cuya longitud de onda se encuentra entre la luz visible y las microondas de (3 a 6Hz). Una de sus aplicaciones más inmediatas son los mandos de control remoto de las televisiones, aunque en la actualidad se utiliza en muchos otros dispositivos, como por ejemplo en los teléfonos móviles y las PDA. El uso de esta tecnología es muy amplio dado su reducido coste y que no ofrece interferencias con otras tecnologías. Se puede establecer dos categorías dentro de las comunicaciones por infrarrojo, dependiendo de si la visibilidad entre el emisor y el receptor tiene que ser directa (infrarrojo de haz directo) o en cambio puede haber obstáculos entre ellos (infrarrojo de haz difuso). La diferencia básica consiste en la potencia del haz infrarrojo, que en el caso del infrarrojo de haz difuso es mayor, para permitir múltiples reflexiones de luz que permitan evitar los obstáculos entre el emisor y el receptor.

Con el objetivo de difundir el uso de tecnología infrarroja se creó en 1993 IrDA (*Infrared Data Association*), que se encarga de crear las especificaciones para el desarrollo de sistemas de comunicación a través de rayos infrarrojos. Los estándares que ha creado IrDA hasta la fecha son los siguientes:

- IrDA Data: permite realizar transferencias bidireccionales, y las tasas de transmisión pueden llegar hasta los 16 Mbps. Sin embargo la distancia que alcanza no es muy elevada, unos 2 metros como máximo.
- IrDA Control: se utiliza para las comunicaciones de control remoto, como los mandos a distancia, o incluso los dispositivos periféricos de los ordenadores, como pueden ser los teclados o los ratones. La transmisión puede llegar a alcanzar unos 5 metros de distancia, y su tasa de transmisión máxima es de 75 Kbps.

### **2.4.2 Redes inalámbricas de área local (WLAN)**

Las redes inalámbricas de área local o WLAN (*Wireless Local Area Network*) ofrecen una mayor cobertura que las WPAN, pudiendo alcanzar unos pocos cientos de metros de distancia. La tecnología más utilizada dentro de las WLAN es la que sigue la norma IEEE 802.11, conocida como Wifi, que surgió como solución al problema de la incompatibilidad entre redes que no seguían ningún estándar. En la actualidad podemos encontrar que en muchos hogares se utilizan redes inalámbricas con tecnología Wifi. No obstante, para crear este tipo de redes también podemos utilizar otras tecnologías que existen en el mercado, como por ejemplo homeRF e hiperLAN.

### 2.4.2.1 WiFi

En la actualidad, la tecnología inalámbrica más utilizada para crear redes de área local es el sistema *Wifi (Wireless Fidelity)*. Wifi surgió con el objetivo de normalizar el mercado de las comunicaciones inalámbricas, ya que durante muchos años existieron en el mercado dispositivos inalámbricos de diferentes propietarios que eran incompatibles entre sí. Para normalizar la situación, en 1999 se creó una asociación llamada WECA (*Wireless Ethernet Compability Alliance*), de la que formaban parte los principales vendedores de tecnología inalámbrica (Nokia, 3COM, etc.). WECA estableció la normativa IEEE 802.11, que suprimía el problema de la incompatibilidad entre los dispositivos de diferentes fabricantes.

Algunas versiones de la norma IEEE 802.11 utilizan la frecuencia 2,4 GHz también utilizada por la tecnología Bluetooth para la transferencia de información. Para evitar cualquier tipo de interferencia entre ambas tecnologías se optó por crear la versión 1.2 de *bluetooth*, que eliminaba este problema.

Las versiones 802.11b y 802.11g son las más utilizadas y trabajan en la frecuencia de 2,4 GHz. La versión 802.11b tiene una velocidad de transmisión de hasta 11 Mbps, y la 802.11g una velocidad de hasta 54 Mbps. Como puede ver en la tabla, existe varias versiones de la normativa IEEE 802.11

Tabla 5. Versiones de la normativa IEEE 802.11

Versión	Características
802.11 a	54 Mbps WLAN en banda de 5 GHz
802.11 b	11 Mbps WLAN en banda de 2,4 GHz
802.11 c	Cruce sin cables
802.11 d	"Modo Mundial" adaptación de los requerimientos regionales
802.11 e	QoS y extensiones que fluyen a través de 802.11 a/g/h
802.11 f	Tránsito para 802.11 a/g/h
802.11 g	54 Mbps WLAN en banda de 2,4 GHz
802.11 h	802.11a con DFS y TCP (Europa)
802.11 i	Autenticación y cifrado AES
802.11 j	802.11a con canales adicionales por encima de 4-9 GHz (Japón)
802.11 k	Intercambio de información de capacidad entre clientes y puentes de acceso
802.11 m	Mantenimiento, publicación de actualizaciones estándar
802.11 n	Nueva generación WLAN en banda 2,4 GHz que permite velocidades superiores a 500 Mbps

La versión 802.11a utiliza la frecuencia de 5 GHz. Como no existen otras tecnologías que funcionen a esta banda, se suprime completamente el problema de las interferencias.

En lo que respecta a la compatibilidad de Wifi con las redes locales de cable (Ethernet) especificadas en la norma IEEE 802.3, no existe ningún tipo de problema entre ambos tipos de redes, ya que el funcionamiento de ambas es idéntico, lo único que varía es la manera en la que los ordenadores acceden a la red.

Para crear una red inalámbrica Wifi debe disponer de una serie de dispositivos hardware compatibles con la norma IEEE 802.11. El primer componente necesario es el punto de acceso, que es elemento que da cobertura a la red inalámbrica, y consiste básicamente en un aparato de radio con una o varias antenas que ofrece cobertura a nuestra red, y que actúa como controlador central de la comunicación. A ese punto de acceso podrían conectarse numerosos ordenadores u otros dispositivos a través de adaptadores de red inalámbricos.

También pueden utilizarse antenas en una red Wifi con el objetivo de aumentar la cobertura inalámbrica a varios kilómetros de distancia. En el mercado puede encontrar muchos tipos de antenas según el usuario requiera.

Sin embargo, la comunicación Wifi presenta un problema: la seguridad. Si una red inalámbrica no se encuentra debidamente protegida, cualquier persona puede conectarse y acceder a sus recursos a través de un ordenador que disponga de un adaptador de red inalámbrico. Este inconveniente puede solucionarse utilizando protocolos de cifrado de información como el WEP y el WPA. El protocolo WPA es mucho más recomendable que el WEP en la protección de redes Wifi, ya que el protocolo WEP se puede "romper" en pocos minutos. Además existe el protocolo de seguridad WPA2 (versión 802.11i), que ofrece mejoras sobre el WPA y utiliza el algoritmo de cifrado de datos criptográfico AES.



Figura 44. Puntos de acceso y adaptadores inalámbricos  
<http://principiosbasicosnetworking.wikispaces.com/>



### 2.4.2.1.1 Redes WIFI de área extensa

Los puntos de acceso tienen una cobertura de al menos 30 metros y como máximo varios cientos de metros. UN punto de acceso puede soportar un grupo reducido de usuarios. En caso de que quiera construir una red con una cobertura mucho mayor de la que ofrece un solo punto de acceso, tiene que conectar varios WAP entre sí para formar una red más grande, permitiendo de esta forma aumentar no solo el alcance de cobertura de la red sino de también el número que pueden formar parte de ella.

Existen varias formas de crear redes más grandes a partir de la utilización de muchos puntos de acceso:

- Redes extendidas (EES). Consiste en configurar varios puntos de acceso con el mismo nombre y el mismo tipo de cifrado. En este tipo de redes el único parámetro que cambia entre los diferentes puntos de acceso es el canal
- Redes distribuidas (WDS). Consiste en formar una red distribuida de puntos de acceso que trabajan con la misma configuración. En este tipo de redes el canal es el mismo pero puede variar el nombre del punto de acceso.
- Interconexión de redes. Otra forma de crear redes extensas consiste en enlazar dos redes a través de una conexión punto a punto formada por varios puntos de acceso con una antena direccional

Redes extendida (ESS). Una red extendida es un conjunto de puntos de acceso que están conectados entre sí a través de una red Ethernet para formar una única red. De esta forma un usuario puede cambiar de forma automática entre los diferentes puntos de acceso sin perder la conexión a internet. Para que los puntos de acceso puedan trabajar de forma conjunta sin crear interferencias cada punto de acceso debe trabajar en un canal diferente. Además, todos los puntos de acceso deben tener el mismo nombre y la misma configuración de seguridad.



## RED DE ÁREA EXTENSA

Figura 45. Esquema representativo de una red de área extensa  
<http://red2marisolcolin.blogspot.com/2010/05/redes-2.html>

Como cada canal se corresponde con una determinada frecuencia, y a canales consecutivos las frecuencias son también consecutivas, una buena forma de establecer los canales de los puntos de acceso de una red es utilizar canales separados, un problema típico de grafos que es totalmente aplicable a las redes inalámbricas es poder colorear cualquier grafo con un número mínimo de colores sin que exista solapamiento. Dicho de otra forma el problema es poder asignar a cada zona un canal sin que exista solapamiento, para establecer los canales de una red inalámbrica extensa es recomendable utilizar los canales 1, 6, 11.

Redes distribuidas (WDS). *Wireless Distribution System*, es un sistema distribuido inalámbrico a diferencia de una red extendida ESS los puntos de acceso tienen la misma configuración de seguridad en todos los puntos de acceso trabajan en el mismo canal (en las redes ESS cada punto de acceso trabaja en un canal diferente). La única diferencia de configuración entre los diferentes puntos de acceso es el nombre de la red. Con WDS un punto de acceso puede funcionar solo como punto de acceso, como puente con otro punto de acceso o ambas funciones. De esta manera es posible crear una gran red inalámbrica dado que cada punto de acceso se conecta a cualquier punto de acceso disponible (que use WDS y a cada punto de acceso se puede conectar de forma cableada o inalámbrica).

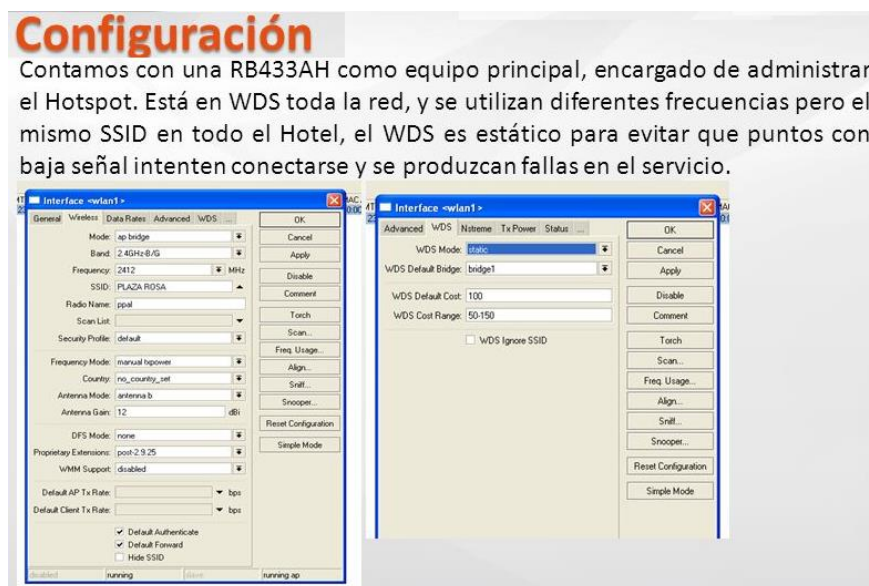


Figura 46. Ventana de configuración  
<http://mireauxms.com/web-qms/master-documents>

Interconexión de redes a larga distancia. Otra forma de utilizar las redes inalámbricas es crear un enlace punto a punto para unir dos redes alejadas. Para crear el enlace punto a punto se utiliza dos puntos de acceso conectados a dos antenas parabólicas. La configuración de la red es muy simple un punto de acceso trabaja en modo AP y el otro punto de acceso trabaja como cliente del otro punto de acceso.

En este tipo de configuraciones hay que prestar un especial cuidado en la seguridad ya que cualquier intruso puede poner en medio de la comunicación con un *sniffer* ver todo el tráfico de la red. Las medidas más básicas que puede realizar es utilizar un protocolo de encriptación WPA y filtrado de direcciones AC, aunque también es recomendable que los dos puntos de acceso estén conectados por una red VPN.

El problema que existe al crear este tipo de conexiones es que las antenas tienen que estar perfectamente alineadas para que puedan comunicarse correctamente. Para calcular la posición y el grado de inclinación de las antenas pueden utilizar la aplicación radio mobile.



Figura 47. Interconexión punto a punto 2014  
<http://www.tp-link.com/common/subject/wireless/TL-WA5210G/?siteid=18>

#### 2.4.2.2 HomeRF

La tecnología homeRf (*Home Radio Frequency*) fue creada para permitir la conexión entre dispositivos que se encuentran dentro del hogar. Al igual que *Wifi* y *bluetooth*, trabaja en la banda de frecuencia de 2.4 GHz, sin embargo no interfiere con dichas tecnologías gracias al método de salto de frecuencia que utiliza. Su radio de alcance puede llegar hasta los 50 mts. El protocolo *SWAP (Shared Wireless Access Protocol)* fue creado para las comunicaciones *homeRF*, y tiene varias versiones. La versión 1.0 tiene una velocidad de transmisión de 1.6 Mbps y la versión 2.0 alcanza los 10 Mbps aunque se sigue trabajando para que futuras versiones lleguen a alcanzar hasta los 100 Mbps. En 1998 se creó el grupo de trabajo *HRFWG (Home RF Working Group)* formado por casi 100 empresas multinacionales (entre ellas Microsoft, IBM, HP e Intel) que desembocó en el desarrollo de la tecnología de *homeRf*. Aunque inicialmente esta tecnología tenía grandes perspectivas de futuro, muchas de las empresas abandonaron el proyecto ya que la tecnología *Wifi* se ha extendido mucho más.



Figura 48. Símbolo de la tecnología HomeRF  
<http://www.umtsworld.com/technology/hrf.htm>

### 2.4.2.3 HiperLAN

El estándar hiperLan (*High Performance Radio LAN*) fue aprobado en 1996 por el ETSI (*European Telecommunications Standards Institute*), y su principal objetivo es permitir comunicaciones entre dispositivos a 10Mbps a una distancia de hasta 50 metros. *HiperLAN* no produce interferencia con otras tecnologías inalámbricas (como pueden ser *bluetooth* o *WiFi*), ya que trabaja a 5 GHz. Es decir a una banda de frecuencia diferente. En este aspecto se parece a la versión de *WiFi* 802.11a, que también trabaja a 5 GHz. A principios del año 2000 se completó el diseño de la especificación de *hiperLAN/2*, que podía ser aplicada en un gran número de redes. *HiperLAN/2* fue creado con el objetivo de transmitir información multimedia ofreciendo una buena calidad de servicio mejorando notablemente la transmisión de sonido y video. Además de mejorar en seguridad gracias a la utilización de algoritmos de cifrado, como DES o Triple-DES.

También permite la autenticación de los terminales inalámbricos con los puntos de acceso. Esta tecnología tiene un futuro incierto, ya que algunos críticos opinan que el estándar IEEE 802.11 ya le ha vencido la batalla comercial, y que la gran ventaja que ofrece *hiperLAN/2*, que consiste en el ofrecimiento de una buena calidad de servicio, no tiene realmente valor ya que internet en si ofrece un buen soporte para la QoS. (Gomez J. , 2008)



Figura 49. Símbolo de la tecnología HiperLan  
<http://www.aalcubo.it/grafica/>

### 2.4.3 Redes Inalámbricas de área metropolitana (WMAN)

Las redes inalámbricas de área metropolitana o WMAN (*Wireless Metropolitan Area Network*) pueden ofrecer una cobertura que abarca toda una ciudad. No obstante se suelen utilizar para crear redes inalámbricas más pequeñas. Como por ejemplo la red de un campus universitario o la conexión de las oficinas de varios edificios. Para crear redes inalámbricas de área metropolitana se pueden utilizar principalmente las tecnologías LMDS Y *WiMax*.

### 2.4.3.1 LMDS

LMDS (*Local Multipoint Distribution Service*) proporcionan los servicios más comunes demandados por los usuarios: acceso a internet transmisión multimedia de calidad, etc. Se aplica solo para la comunicación entre puntos fijo, es decir no se utiliza para conectar terminales que se encuentran en movimiento. La transmisión se realiza desde un solo punto, llamado estación base, hasta las múltiples instalaciones abandonadas a dicha estación base, que son los usuarios en un tipo de comunicación conocida como punto a multipunto. La comunicación es bidireccional, por lo tanto los usuarios pueden responder a la estación base estableciendo en laces punto a punto.

Las ventajas principales de esta tecnología son, por un lado, su fiabilidad y rapidez de su instalación, y por otro lado su gran escalabilidad gracias a la naturaleza modular de su arquitectura, así como su bajo coste, ya que evita las empresas de telecomunicaciones tener que invertir grandes sumas de dinero o comunicaciones por fibra óptica o pare de cobre. Respecto al alcance de la transmisión, LMDS permite distancias de hasta 35 km con una velocidad de hasta 8Mps. Para transmitir información, LMDS utiliza la banda de frecuencia de las microondas, 26Ghz también usada para las comunicaciones por satélite. Se utiliza esta banda, denominada banda Ka, porque es la única manera de conseguir anchos de banda elevados, debido a que las bajas frecuencias existe una gran congestión espectral. Sin embargo, en algunos países de Europa se trabaja en bandas en torno a los 3.5 GHz. De hecho, en España se ha trabajado en las bandas de 3,4-3,6 GHz y 24,5 GHz. Sin embargo esta tecnología también tiene una serie de inconvenientes. El primero consiste en que la comunicación entre la estación base y la antena de abonado tiene que ser directa, es decir no puede haber obstáculos entre ellos. Por lo tanto, a veces es necesario colocar varias estaciones base para amplificar y repetir señal.

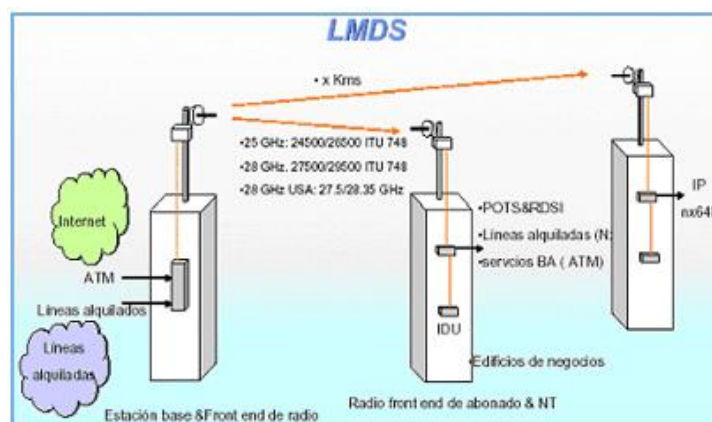


Figura 50. Esquema de funcionamiento de la tecnología LMDS  
<http://www.oocities.org/es/pdorm6000/RedesTelecomunicaciones/Foro/II.htm>

### 2.4.3.2 WiMax

*WiMax* (*Worldwide Interoperability for Microwave Access*) es otro estándar de comunicación de inalámbricas, basado en la especificación IEEE 802.16<sup>a</sup> y este *hiperMAN*, que tiene como principal objetivo la creación de red inalámbricas de área metropolitana de banda ancha.

Su principal característica es su gran alcance ya que puede llegar a los 50 km con una velocidad de transmisión de hasta 70Mbps. La calidad de servicio ofrecida es también muy buena, sobre todo está optimizado para la transmisión de video y audio, por lo tanto esta tecnología no tiene problemas con la transmisión de datos multimedia, tan demandada últimamente por los usuarios.

Al principio, el estándar 802.16 trabajaba en una banda de frecuencia entre 10 y 66 GHz, y por lo tanto se necesita la visibilidad directa entre las torres para establecer una buena comunicación. Posteriormente, en el año 2003, se presentó la versión 802.16<sup>a</sup> que trabaja en una banda de frecuencia entre 2 y 11 GHz, y como consecuencia permite que existan obstáculos entre los equipos. Más tarde, en el año 2005 se aprobó el estándar *WiMax* móvil con la especificación 802.16<sup>a</sup> con lo que es posible incorporar terminales en movimiento dentro de las comunicaciones inalámbricas.

El futuro se presenta muy prometedor para *WiMax*, ya que muchas empresas multinacionales como por ejemplo Intel, están apostando cada más por esta tecnología, invirtiendo grandes sumas de dinero en su desarrollo. Esto se debe en parte a que *WiMax* ofrece un conexión desde ordenadores portátiles o teléfonos móviles a distancias mucho mayores que las tecnologías anteriores y además la velocidad de transferencia es también muy elevada.

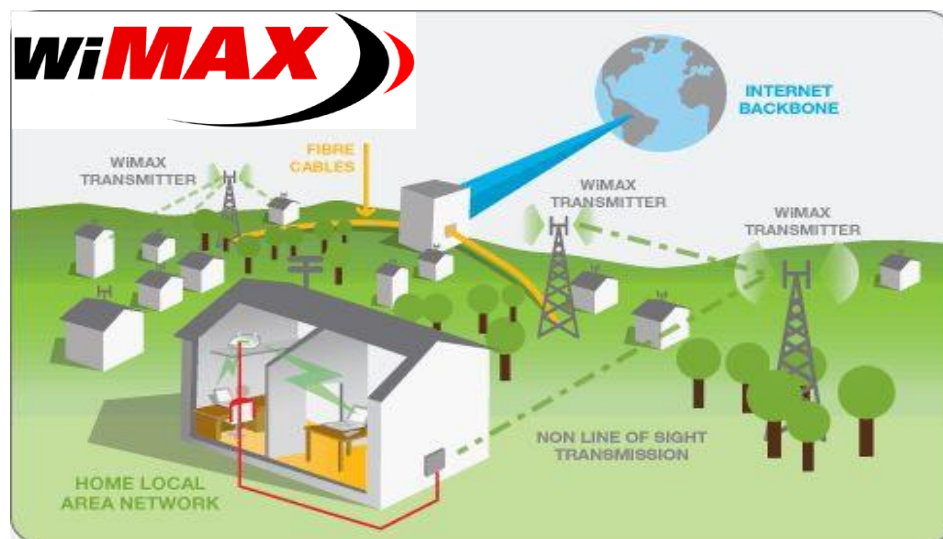


Figura 51. Funcionamiento de la tecnología WiMax  
<http://www.emfexplained.info/spa/?id=25133>

## 2.4.4 Redes Inalámbricas Globales (WWAN)

Las redes inalámbricas globales o WWAN (*Wireless Area Network*) son las que ofrecen mayor cobertura, pudiendo llegar a su alcance a todo un país, o incluso a un conjunto de países. Este tipo de redes son usadas por los sistemas de telefonía móvil o digital. Las tecnologías que se utilizan para crear redes inalámbricas globales están en continua evolución. Su clasificación gira en torno a las diferentes generaciones que han ido surgiendo teléfonos móviles.

### 2.4.4.1 GSM

GSM, o Sistema Global para las telecomunicaciones móviles es un sistema estándar completamente definido, usado para la comunicación entre teléfonos móviles basada en la tecnología digital. Lo que permite, al ser digital, que cualquier usuario pueda conectarse a través del teléfono a su PC personal, permitiéndole interactuar por e-mail, fax, acceder a Internet, y un acceso seguro a redes LAN o Intranet. También existe la posibilidad de envío de texto corto entre terminales (SMS)

GSM nace en 1982, en la Conferencia Europea de Administraciones de Correos y Telecomunicaciones (CEPT) donde se buscaba una estandarización de las comunicaciones y una posibilidad de financiar ésta de una forma global, debido al amplio coste que suponía mantener un sistema individual para cada país. Se crea entonces el *Grupe Spécial Mobile* (de donde provienen las siglas GSM, que más adelante pasaría a llamarse Estándar Mobile *Group*, usándose las siglas para el estándar) el cual desarrollará un estándar europeo de telefonía digital, finalizándose en 1990 el estándar GSM-900 y siguiéndole un año después el DCS-1800. Además empresas como Nokia lanzaron el primer teléfono celular basado en GSM (Nokia 1011).

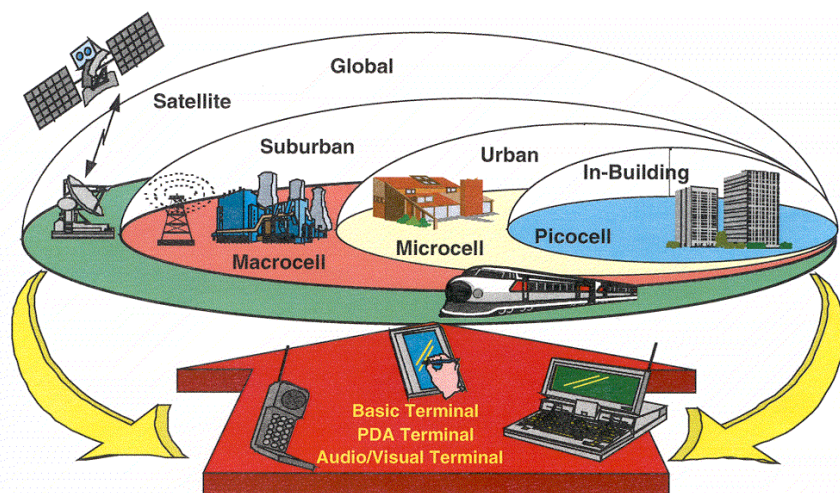


Figura 52. Tecnología GSM

<http://cordis.europa.eu/infowin/acts/rus/impacts/mobile.htm>

## 2.4.4.2 GPRS

General *Packet Radio Service* o servicio general de paquetes vía radio creado en la década de los 80 es una extensión del Sistema Global para Comunicaciones Móviles (*Global System for Mobile Communications* o *GSM*) para la transmisión de datos mediante conmutación de paquetes. Existe un servicio similar para los teléfonos móviles, el sistema IS-136. Permite velocidades de transferencia de 56 a 114 kbps. Una conexión GPRS está establecida por la referencia a su nombre del punto de acceso (APN). Con GPRS se pueden utilizar servicios como *Wireless Application Protocol* (WAP), servicio de mensajes cortos (SMS), servicio de mensajería multimedia (MMS), Internet y para los servicios de comunicación, como el correo electrónico y la *World Wide Web* (WWW). Para fijar una conexión de GPRS para un módem inalámbrico, un usuario debe especificar un APN, opcionalmente un nombre y contraseña de usuario, y muy raramente una dirección IP, todo proporcionado por el operador de red. La transferencia de datos de GPRS se cobra por volumen de información transmitida (en kilo o megabytes), mientras que la comunicación de datos a través de conmutación de circuitos tradicionales se factura por minuto de tiempo de conexión, independientemente de si el usuario utiliza toda la capacidad del canal o está en un estado de inactividad. Por este motivo, se considera más adecuada la conexión conmutada para servicios como la voz que requieren un ancho de banda constante durante la transmisión, mientras que los servicios de paquetes como GPRS se orientan al tráfico de datos. La tecnología GPRS como bien lo indica su nombre es un servicio (Service) orientado a radio enlaces (Radio) que da mejor rendimiento a la conmutación de paquetes (*Packet*) en dichos radio enlaces. (Gomez J. , 2008)

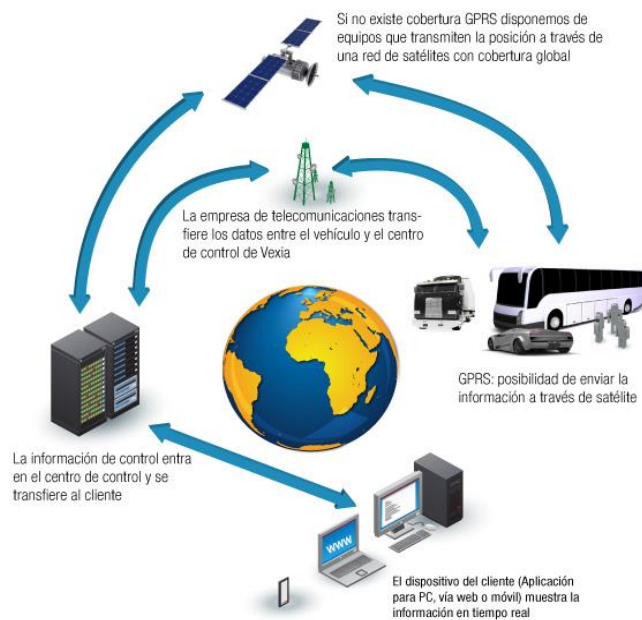


Figura 53. Funcionamiento de la tecnología GPRS  
<http://4vector.com/free-vector/gprs-69224>



### 2.4.4.3 UMTS

(Universal Mobile Telecommunications System)

El Sistema Universal de Telecomunicaciones Móviles considerado el futuro de las tecnologías móviles: Sistema universal de telecomunicaciones móviles (*Universal Mobile Telecommunications System* o UMTS) es una de las tecnologías usadas por los móviles de tercera generación, sucesora de GSM, debido a que la tecnología GSM propiamente dicha no podía seguir un camino evolutivo para llegar a brindar servicios considerados de tercera generación.

Aunque inicialmente esté pensada para su uso en teléfonos móviles, la red UMTS no está limitada a estos dispositivos, pudiendo ser utilizada por otros. Sus tres grandes características son las capacidades multimedia, una velocidad de acceso a Internet elevada, la cual también le permite transmitir audio y video en tiempo real; y una transmisión de voz con calidad equiparable a la de las redes fijas. Además, dispone de una variedad de servicios muy extensa

#### Arquitectura UMTS

El equipo UMTS debe ser compatible con el de GSM ya que el cambio de una tecnología a otra ha de ser paulatino.

Se divide en tres partes:

- Los equipos de usuario
- El UTRAN
- La red principal (Core Network)

El UTRAN (*UMTS Terrestrial Radio Access Network*) y el Core Network (Red principal) son consideradas la espina dorsal de la tecnología UMTS.

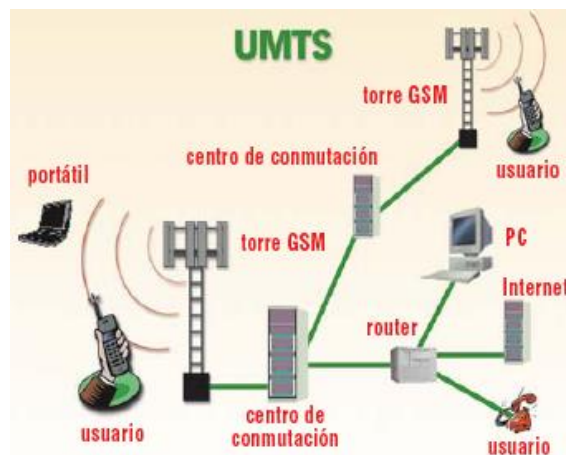


Figura 54. Tecnología UMTS

#### 2.4.4.4 HSDPA

*High Speed Down link Packet Access* la tecnología HSDPA ha supuesto un nuevo revulsivo para la tecnología móvil por la mejora de la tecnología UMTS/WCDMA que permite alcanzar tasas de hasta 14Mbps. Esta tecnología permite videoconferencia, juegos online multiusuario, películas, videos, descargas y ejecución de programas todo en tiempo real.

Esta tecnología proporciona un acceso a internet de mayor ancho de banda, para una ejecución más rápida de los servicios y recursos posibilita que un mayor número de usuarios puedan utilizar simultáneamente la red. Los operadores de telefonía 3G utilizan esta tecnología y dirigen principalmente el mercado móvil de dos terminales principalmente portátiles y las móviles 3g.

Ordenadores de pequeño tamaño: portátiles, *netbooks*, conectados principalmente mediante un modem USB que incorpora una tarjeta SIM del operador telefónico que presta el servicio. La necesidad de no depender de una conexión fija o *Wifi* para conectar a Internet y de no perder la característica de movilidad que nos ofrecen los ordenadores portátiles, hace que muchos usuarios se inclinen también por el modelo de conexión mediante modem USB facilitado por los distintos operadores de telefonía móvil.

Su principal ventaja está en que la configuración es instantánea al conectar el modem USB y teclear el número de activación (PIN) como si de un teléfono móvil se tratara. Las modalidades de ofertas dependen del precio, el tipo de modem USB, la velocidad y cantidad de datos de descargados. En el momento de elaborar esta documentación los modem USB estándar puede alcanzar los 7,2 Mbps. dependiendo de las condiciones óptimas de cobertura y señal. (Gomez, 2008)



Figura 55. Dispositivo con tecnología HSDPA  
<http://www.3g.co.uk/PR/July2007/4909.htm>

## **2.5 Tipos de conmutación**

Tienen la función de prestar servicio de conmutación para trasladar los datos de un nodo al otro hasta alcanzar el destino final. Este tipo de redes se denomina redes de comunicación conmutadas. Los datos provenientes de una de las estaciones (computadoras, terminales, servidores o cualquier dispositivo de comunicación) entran a la red conmutada y se encaminan hasta la estación de destino conmutándolos de nodo en nodo.

### **2.5.1 Difusión (*Broadcast*).**

Técnica de transmisión que no involucra cambio alguno. La información es transmitida a todos los nodos y depende de los receptores decidir si el mensaje va dirigido a ellos o no.

### **2.5.2 Conmutación de circuitos**

En la conmutación de circuitos, el camino (llamado "circuito") entre los extremos del proceso de comunicación se mantiene de forma permanente mientras dura la comunicación, de forma que es posible mantener un flujo continuo de información entre dichos extremos. Este es el caso de la telefonía convencional.

### **2.5.3 Conmutación de paquetes**

La conmutación de paquetes se trata del procedimiento mediante el cual, cuando un nodo quiere enviar información a otro lo divide en paquetes, todos del mismo tamaño, los cuales contienen la dirección del nodo destino, en este caso, no existe un circuito permanente entre los extremos y, la red, simplemente, se dedica a encaminar paquete a paquete la información entre los usuarios.

### **2.5.4 *Frame Relay* (Retransmisión de marcos).**

Este tipo aporta algunas ventajas de la conmutación de circuitos la conmutación de paquetes. Se solucionó el problema de retardo al conmutador, los paquetes pequeños (marcos, *frames*), según venían. Los nodos de conmutación, usualmente son procesadores paralelos de propósitos específico, encaminan los, marcos basándose en el examen de los primeros bits, los marcos pasan a través de como pequeños flujos de bits. (Alfredo, 2008).

## 2.6 Protocolos de comunicaciones IEEE 802.11

Estándares Oficiales:

- ANSI: American National Standards Institute. Organización Privada sin fines de lucro fundada en 1918, la cual administra y coordina el sistema de estandarización voluntaria del sector privado de los Estados Unidos.
- EIA: *Electronics Industry Association*. Fundada en 1924. Desarrolla normas y publicaciones sobre las principales áreas técnicas: los componentes electrónicos, electrónica del consumidor, información electrónica, y telecomunicaciones.
- TIA: *Telecommunications Industry Association*. Fundada en 1985 después del rompimiento del monopolio de AT&T. Desarrolla normas de cableado industrial voluntario para muchos productos de las telecomunicaciones y tiene más de 70 normas preestablecidas.
- ISO: *International Standards Organization*. Organización no gubernamental creada en 1947 a nivel Mundial, de cuerpos de normas nacionales, con más de 140 países.
- IEEE: Instituto de Ingenieros Electricistas y Electrónicos. Principalmente responsable por las especificaciones de redes de área local como 802.3 Ethernet, 802.5 *Token Ring*, *ATM* y las normas de *Gigabite Ethernet*. Es una asociación mundial técnico profesional sin ánimo de lucro que incluye entre sus voluntarios ingenieros electricistas y electrónicos de informática de biomedicina, aeroespacial telecomunicaciones mecatrónica y científicos de la computación (IEEE 802.11n). (Gomez J. A., 2005)

La versión original del estándar IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) 802.11 publicada en 1997 especifica dos velocidades de transmisión *teóricas* de 1 y 2 megabits por segundo (Mbit/s) que se transmiten por señales infrarrojas (IR). IR sigue siendo parte del estándar, si bien no hay implementaciones disponibles.

El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores.

## 802.11: formato de trama

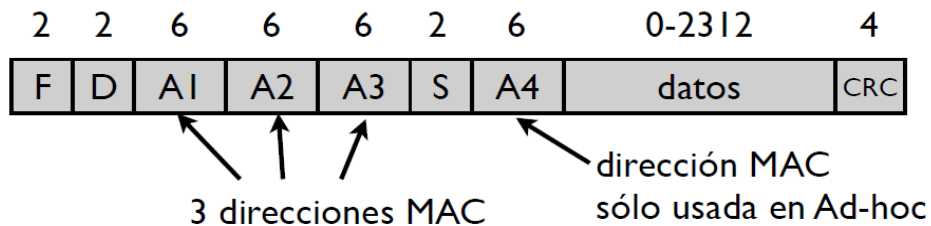


Figura 56. Funcionamiento de la trama MAC  
<http://www.gloobal.net/iepala/gloobal/fichas/ficha.php?entidad=Textos&id=7920&opcion=documento>

### 2.6.1 IEEE 802.11a

La revisión 802.11a fue aprobada en 1999. El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 GHz y utiliza 52 sub portadoras (OFDM) con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. 802.11a tiene 12 canales sin solapa, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede inter operar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

### 2.6.2 IEEE 802.11b

La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11 Mbps y utiliza el mismo método de acceso definido en el estándar original CSMA/CA. El estándar 802.11b funciona en la banda de 2,4GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5,9 *Mbits* sobre TCP y 7,1 Mbit/s sobre UDP.

### 2.6.3 IEEE 802.11g

En junio de 2003, se ratificó un tercer estándar de modulación: 802.11g, que es la evolución de 802.11b. Este utiliza la banda de 2,4Ghz (al igual que 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22,0 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a.

Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del nuevo estándar lo tomó el hacer compatibles ambos modelos. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación que fue dada aprox. el 20 de junio del 2003. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b.

Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas o equipos de radio apropiados.

Existe una variante llamada 802.11g+ capaz de alcanzar los 108Mbps de tasa de transferencia. Generalmente sólo funciona en equipos del mismo fabricante ya que utiliza protocolos propietarios.

#### **2.6.4 IEEE 802.11n**

En enero de 2004, el IEEE anunció la formación de un grupo de trabajo 802.11 (*Tgn*) para desarrollar una nueva revisión del estándar 802.11. La velocidad real de transmisión podría llegar a los 300 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y unas 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO Múltiple Input – Múltiple Output, que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas (3). Existen también otras propuestas alternativas que podrán ser consideradas.

El estándar ya está redactado, y se viene implantando desde 2008. A principios de 2007 se aprobó el segundo boceto del estándar. Anteriormente ya había dispositivos adelantados al protocolo y que ofrecían de forma no oficial este estándar (con la promesa de actualizaciones para cumplir el estándar cuando el definitivo estuviera implantado). Ha sufrido una serie de retrasos y el último lo lleva hasta noviembre de 2009. Habiéndose aprobado en enero de 2009 el proyecto 7.0 y que va por buen camino para cumplir las fechas señaladas. A diferencia de las otras versiones de Wi-Fi, 802.11n puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Gracias a ello, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5GHz, ya que está menos congestionada

y en 802.11n permite alcanzar un mayor rendimiento. El estándar 802.11n fue ratificado por la organización IEEE el 11 de septiembre de 2009 con una velocidad de 600 Mbps en capa física.

En la actualidad la mayoría de productos son de la especificación b o g, sin embargo ya se ha ratificado el estándar 802.11n que sube el límite teórico hasta los 600 Mbps. Actualmente ya existen varios productos que cumplen el estándar N con un máximo de 300 Mbps (80-100 estables). El estándar 802.11n hace uso simultáneo de ambas bandas, 2,4GHz y 5GHz. Las redes que trabajan bajo los estándares 802.11b y 802.11g, tras la reciente ratificación del estándar, se empiezan a fabricar de forma masiva y es objeto de promociones por parte de los distintos ISP, de forma que la masificación de la citada tecnología parece estar en camino. Todas las versiones de 802.11xx, aportan la ventaja de ser compatibles entre sí, de forma que el usuario no necesitará nada más que su adaptador *Wifi* integrado, para poder conectarse a la red. Sin duda esta es la principal ventaja que diferencia *Wifi* de otras tecnologías propietarias, como LTE, UMTS y *WiMax* las tres tecnologías mencionadas, únicamente están accesibles a los usuarios mediante la suscripción a los servicios de un operador que está autorizado para uso de espectro radioeléctrico, mediante concesión de ámbito nacional. La mayor parte de los fabricantes ya incorpora a sus líneas de producción equipos *Wifi* 802.11n, por este motivo la oferta ADSL, ya suele venir acompañada de *Wifi* 802.11n, como novedad en el mercado de usuario doméstico. Se conoce que el futuro estándar sustituto de 802.11n será 802.11a con tasas de transferencia superiores a 1 Gb/s.

### **2.6.5 IEEE 802.11h**

La especificación 802.11h es una modificación sobre el estándar 802.11 para WLAN desarrollado por el grupo de trabajo 11 del comité de estándares LAN/MAN del IEEE (IEEE 802) y que se hizo público en octubre de 2003. 802.11h intenta resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de Radar o Satélite.

El desarrollo del 802.11h sigue unas recomendaciones hechas por la ITU que fueron motivadas principalmente a raíz de los requerimientos que la Oficina Europea de Radiocomunicaciones (ERO) estimó convenientes para minimizar el impacto de abrir la banda de 5 GHz, utilizada generalmente por sistemas militares, a aplicaciones ISM (ECC/DEC/(04)08). Con el fin de respetar estos requerimientos, 802.11h proporciona a las redes 802.11a la capacidad de gestionar dinámicamente tanto la frecuencia, como la potencia de transmisión.

Selección Dinámica de Frecuencias y Control de Potencia del Transmisor DFS (*Dynamic Frequency Selection*) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz con el fin de evitar interferencias co-canal con sistemas de radar y para asegurar una utilización uniforme de los canales disponibles. TPC (*Transmitter Power Control*) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz para asegurar que se respetan las limitaciones de potencia transmitida que puede haber para diferentes canales en una determinada región, de manera que se minimiza la interferencia con sistemas de satélite.

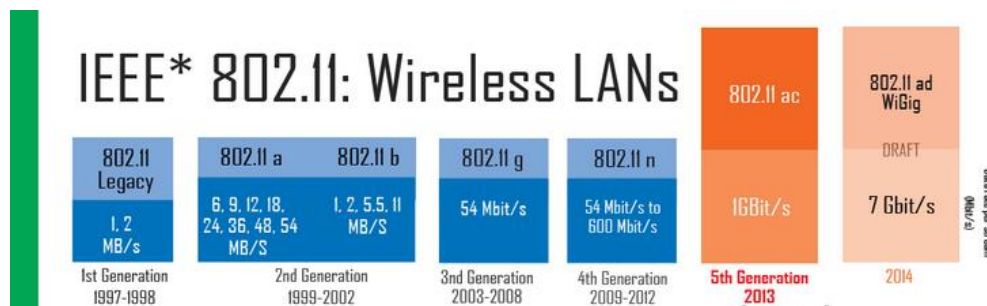


Figura 57. Estándares y velocidades de la norma 802.11  
<http://www.datuopinion.com/ieee-802-11>

## 2.7 Métodos de autenticación del estándar 802.11

Autenticación y asociación. La utilización del aire como usado como un canal de comunicación hace a las redes *wireless* vulnerables a las escuchas y robos de información. Para proporcionar cierto nivel de seguridad, el estándar 802.11 define dos métodos de autenticación: *Open System* y *Shared Key*.

Estos métodos de autenticación se realizan al comienzo de la comunicación entre un cliente *wireless* y un Punto de Acceso de la red. A continuación de la autenticación, y si ésta se ha llevado a cabo de forma exitosa, se efectúa la asociación entre el cliente y el Punto de Acceso. (Pellegero, 2006)

### 2.7.1 Autenticación Open System.

Este método permite a cualquier dispositivo *wireless* acceder a la red siempre que el SSID que proporcione coincida con el del Access Point. Dado que el SSID se transmite sin encriptar en los paquetes de la red *wireless*, es fácilmente obtenible y por tanto, no ofrece ninguna garantía de seguridad.

Además, opcionalmente, un cliente podría utilizar el SSID "ANY" para asociarse con cualquier Punto de Acceso que esté a su alcance, independientemente del valor real del SSID.



### **2.7.2 Autenticación Shared Key.**

Con este procedimiento, se exige al cliente poseer la misma clave WEP que posee el Punto de Acceso: el Punto de Acceso envía un texto en claro, denominado "desafío", al cliente, éste lo devuelve encriptado y el Punto de Acceso, lo descripta y lo compara con el texto inicial para verificar que ambos poseen la misma clave.

Como vemos, la clave no viaja en ningún momento por la red, por lo que no puede ser obtenida a partir de escuchas pasivas de los mensajes; sin embargo, dada la debilidad del protocolo WEP, es posible obtener la clave recogiendo y analizando una cantidad determinada de tráfico en la red. (internet, 2003)

## **2.8 Seguridad en redes inalámbricas**

La seguridad es una de los temas más importantes cuando se habla de redes inalámbricas. Desde el nacimiento de éstas, se ha intentado el disponer de protocolos que garanticen las comunicaciones, pero han sufrido de escaso éxito. Por ello es conveniente el seguir puntual y escrupulosamente una serie de pasos que nos permitan disponer del grado máximo de seguridad del que seamos capaces de asegurar.

Un protocolo de seguridad (también llamado protocolo criptográfico o protocolo de cifrado) es un protocolo abstracto o concreto que realiza funciones relacionadas con la seguridad aplicando métodos de cifrado de datos

Un protocolo describe la forma en que un algoritmo debe usarse. Un protocolo lo suficientemente detallado incluye detalles acerca de las estructuras de datos y representaciones, punto en el cual puede usarse para implementar versiones interoperables múltiples de un programa.

Los protocolos criptográficos se usan ampliamente para transporte de datos seguros a nivel de aplicación. Un protocolo criptográfico comúnmente incorpora por lo menos uno de los siguientes aspectos:

- Establecimiento de claves
- Autenticación de entidades
- Cifrado simétrico y autenticación de mensajes
- Transporte de datos en forma segura a nivel de aplicación
- Métodos de no repudio



Figura 58. Cifrado de datos  
[http://www.pryseguridad.com/2013\\_07\\_01\\_archive.html](http://www.pryseguridad.com/2013_07_01_archive.html)

### 2.8.1 Método SSID (*Service Set Identifier*)

Se conoce como SSID al identificador de conjunto de servicio o comúnmente al nombre de la red, este es un código de 32 caracteres alfanuméricos que contiene los paquetes de una red y los identifican como miembros de la misma

Cualquier usuario que desee conectarse a una red debe conocer el SSID para comunicarse con el AP y tener acceso a dicha red. El AP continuamente difunde este identificador de una manera automática mediante un tipo de trama especial llamada "*Beacon*" a todos los dispositivos que se encuentran dentro de su rango de cobertura. Como esta técnica de seguridad se deshabilita la difusión del SSID en el AP, de esta manera no se anuncia el nombre de la red y solo las terminales que lo conocen pueden comunicarse con el AP y conectarse. Sin embargo, esta técnica dificulta que los usuarios configuren y conecten a la red inalámbrica.



Figura 59. Triángulo de características del método SID  
<http://www.cenac.ipn.mx/sercenac/Paginas/IntegridadInformacion.aspx>

## 2.8.2 Método MAC

Hoy en día la mayoría de los AP son configurables y ello les permite almacenar así como administrara una tabla que contiene las direcciones MAC de los usuarios que gozan del privilegio de acceso de red.

La desventaja que presenta esta técnica de seguridad es que la mayoría de los AP que se encuentran en el mercado no poseen la habilidad de redistribuir los cambios hechos en sub tablas de direcciones MAC. Por ello se tiene que administrar de forma manual y de la misma manera borrar o agregar cualquier dirección MAC en cada uno de los AP pertenecientes a la red. Durante los procesos de autenticación los usuarios envían sus direcciones MAC al AP y este las compara con su tabla de direcciones MAC para decidir si gozan o no del privilegio de acceso a la red. En este intercambio de mensajes otro usuario malintencionado puede usar un capturador de tráfico o *sniffer para obtener una de las direcciones MAC validad y utilizarla posteriormente para que el AP le permita la conexión de red.*

## 2.8.3 VPN (Red privada virtual)

Algunos AP permiten la configuración de VPN en el equipo, permitiendo que el usuario que se conecte tenga que autenticarse para poder salir del AP, además ofrece una encriptación de los datos en el tránsito de datos, haciendo más difícil el husmeo de tráfico por un tercero. La desventaja que presenta es que no todos los AP tiene este servicio la autenticación en la mayoría de los casos no es centralizada y cuando la es, se tiene acceso a una parte de la red que que puede ser utilizada para otro tipo de ataques se requiere un software adicional, no todos los equipos lo soportan. Existen una gran variedad de VP, como: IPSec, L2TP, PPTP, entre otras, y pueden ser atacados por DOS o ataques de diccionario.

## 2.8.4 Captive portal

Estos permiten dar acceso a un portal donde se autentica el cliente, dando le acceso a este grupo por un tiempo determinado o bajo ciertas condiciones. Este esquema de seguridad no es muy utilizado debido a que debe estar en el AP para un mejor funcionamiento. No todos los AP *tienen soporte,os OpenAP* o soluciones fuentes abiertas (*open source*) ofrecen estas cualidades. Pueden ser atacados por DOS o ataques de diccionario. El problema aún sigue ya que el control de acceso al AP no existe.

## 2.8.5 Método WEP (Wired Equivalent Privacy)

El acrónimo de Privacidad Equivalente a Cableado (*Wired Equivalent Privacy*). En esta técnica de seguridad se utiliza una clave entre los usuarios y los AP. En este método de seguridad se utiliza al algoritmo de encriptación RC4, este se compone de un Vector de inicialización (IV o clave WEP) y de una clave secreta). El primero de ellos se genera al momento de transmitir una trama, es distinto en la transmisión de cada *frame* y tiene una longitud de 24 bits.

El segundo de ellos (la clave) se asigna de forma manual, es estática y tiene una longitud de 40 bits. Otra técnica que se utiliza el mismo principio de funcionamiento pero utilizando una clave de 40 a 104 bits se denomina WEP-2AI momento de transmitir una trama se calcula el CRC de 32 bits y se genera el vector de inicialización al cual se le añade la clave secreta, posteriormente se genera una secuencia pseudo aleatoria de la misma longitud que el CRC de 32 bits y se realiza la operación XOR u OR exclusiva entre la secuencia pseudo aleatoria y el CRC de 32 bits. Con ello se encripta la información del tipo y subtipo de la trama que está enviando.

La trama transmitida lleva en el campo “cuerpo de la trama” el Vector de Inicialización y la información cifrada. El usuario destino al recibir esta trama crea la misma secuencia pseudo aleatoria con el IV y la clave secreta. Finalmente para descifrar la información se lleva a cabo la función XOR entre la secuencia pseudo aleatoria creada por el receptor y la información encriptada que recibió en el *frame*.

En nuestros días existe numeroso software que capturan los paquetes transmitidos en una red y tienen la capacidad de descifrar la clave secreta que viaja en los *frame* cifrados, ello permite que una terminal pueda conectarse a la red de forma clandestina. (Gomez, 2008)

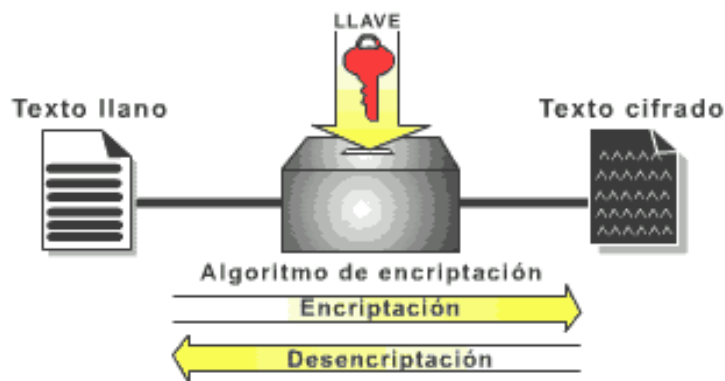


Figura 60. Proceso de encriptación

<http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml>

### **2.8.6 Método WPA (*WiFi Protected Access*)**

WPA son las siglas correspondientes al Acceso Protegido *Wi-Fi* (*Wi-Fi Protected Access*) y surge como respuesta a las debilidades que presenta WEP. Este método de seguridad continua utilizando como algoritmo de encriptación a RC4 peor con diferencia de que ahora ocupa un Vector de Inicialización de 48 bits. La clave secreta que ocupa en WPA es una clave de 128 bits y se genera de forma dinámica para cada usuario.

El método WPA usa el estándar IEEE 802.1 X para controlar el acceso a la red mediante puertos y un RADIUS server para realizar las funciones de autenticación, autorización y conteo. L primera función es para verificar la identidad de los que le fueron otorgados dentro de la red y la tercera para llevar un registro del tiempo que un usuario ha estado conectado a la red.

La técnica de seguridad WPA también puede operar de una manera semejante a WEP utilizando una Clave inicial Compartida (*Pre Shared Key – PSK*) entre los usuarios y los AP pertenecientes a la red, sin embargo, al utilizar esta variante de WPA disminuye su eficacia de seguridad puesto que presenta la mismas debilidades de la técnica WEP.

### **2.8.7 Método WPA-2 y servidor RADIUS**

El estándar IEEE 802.11 i es comúnmente conocido como WPA-2, esta técnica de seguridad es compatible con su predecesor WPA y utiliza el Estándar de Cifrado Avanzado (AES) como algoritmo de encriptación el cual es extremadamente seguro. WPA-2 además de operar en redes que soportan IEEE 802.11 también puede implementarse en redes ad-hoc.

Esta técnica de seguridad inalámbrica es la más reciente y opera de dos maneras, la primera de ellas es utilizando una clave inicial compartida entre los AP y los usuarios para autenticarlos (WPA2-Personal) y la segunda es mediante la implementación de un servidor de autenticación para permitir el acceso de los usuarios a la red (WPA2-Empresa).

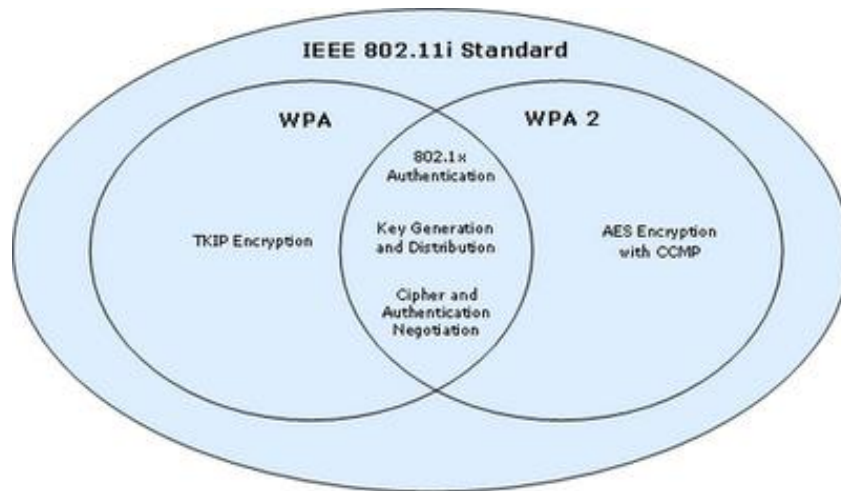


Figura 61. IEEE 802.11i  
<http://www.felipereyesvivanco.com/redes/wifi-seguridad/>

Para obtener la mayor prestación del protocolo WPA, se requiere el uso de un servidor de autenticación externo como el RADIUS. Estas dos herramientas juntas proporcionan una administración y un control de acceso centralizado de toda la red inalámbrica. Con esto, la necesidad de soluciones adicionales como VPN puede ser eliminada, al menos, en el referente al enlace inalámbrico. (Lopez, 2008)

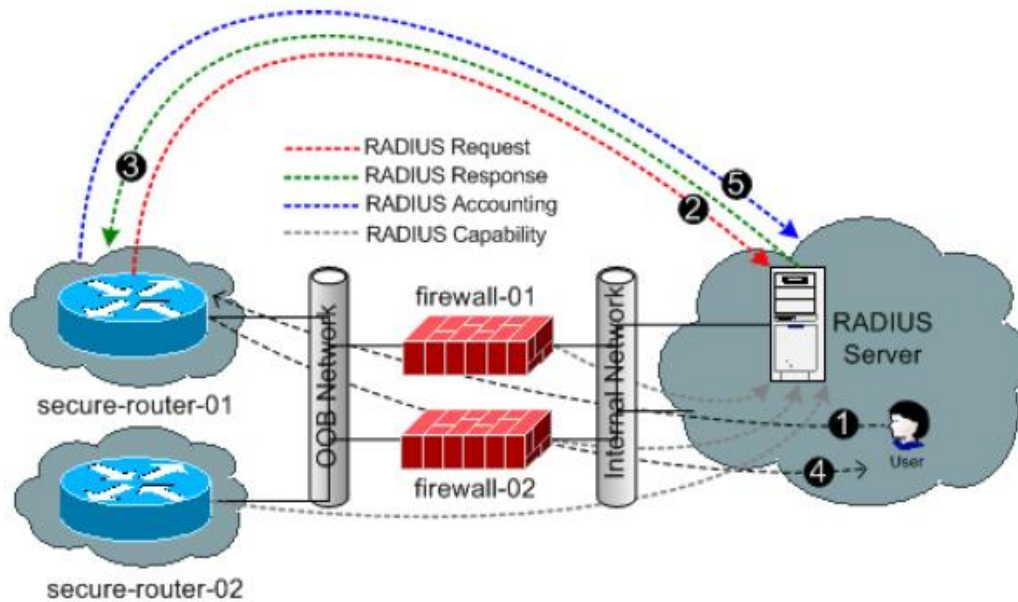


Figura 62. Radius Server  
<http://www.cymru.com/gillsr/documents/junos-radius-authentication.htm>

### **2.8.8 Proceso *Handoff* o *Handover***

Cuando un dispositivo móvil pierde conectividad con el actual AP que le brinda servicio, lleva a cabo un proceso de *Handoff Handover*. Este proceso consiste en cambiarse a un canal de otro AP vecino que tenga una buena intensidad de señal, lo que le permita o continuar en comunicación. Si el dispositivo móvil se cambia a un AP el cual se encuentra dentro de la misma LAN (*Local Area Network*) que el AP anterior, entonces se lleva a cabo un *Handoff* de capa 2 y el dispositivo móvil no cambia de dirección Ip. (Ramirez, 2012)

Cuando hablamos de *handoff* o de *handover* que en términos generales es lo mismo nos referimos a la transferencia de llamadas entre celdas, lo cual ocurre en el momento que se empieza a deteriorar una llamada en progreso, cuando existe interferencia y/o para distribuir el tráfico entre celdas; en estos casos se realiza un cambio automático de una estación base a otra llamando este progreso *Handoff* o *Handover*. Es recomendable al diseñar sistemas celulares procurar que exista un grado de confinación geográfica del canal para evitar la interferencia co-canal, que el área de cobertura de una celda sea un poco mayor y forme parte del área de cobertura de la celda más próxima para que ocurra fácilmente el handoff, en caso contrario se dificultaría el proceso y el porcentaje de pérdidas de llamadas sería mayor y más tedioso para el usuario, en el dibujo se puede visualizar claramente a lo que nos referimos.

## **2.9 Modelo de Referencia**

El modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1), más conocido como “modelo OSI” (en inglés, Open System Interconnection), es el modelo de red descriptivo, que fue creado en el año 1980 por la Organización Internacional de Normalización (*ISO, International Organization for Standardization*). Es un marco de referencia para la definición de arquitecturas en la interconexión de los sistemas de comunicaciones.

El modelo TCP/IP es una descripción de protocolos de red desarrollado por *Vinton Cerf* y *Robert E. Kahn*, en la década de 1970. Fue implantado en la red ARPANET, la primera red de área amplia (WAN), desarrollada por encargo de DARPA, una agencia del Departamento de Defensa de los Estados Unidos, y predecesora de Internet. El modelo TCP/IP, a veces se denomina como *Internet Model*, “modelo DoD” o “modelo DARPA”. El modelo TCP/IP describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que un equipo El modelo TCP/IP y los protocolos relacionados son mantenidos por la *Internet Engineering Task Force (IETF)*.

### **2.9.1 Qué es un protocolo**

En informática y telecomunicación, un protocolo de comunicaciones es un conjunto de reglas y normas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellos para transmitir información por medio de cualquier tipo de variación de una magnitud física. Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como posibles métodos de recuperación de errores. Los protocolos pueden ser implementados por hardware, software, o una combinación de ambos.

Por ejemplo, el protocolo sobre palomas mensajeras permite definir la forma en la que una paloma mensajera transmite información de una ubicación a otra, definiendo todos los aspectos que intervienen en la comunicación: tipo de paloma, cifrado del mensaje, tiempos de espera antes de dar la paloma por 'perdida' y cualquier regla que ordene y mejore la comunicación.

En el caso concreto de las computadoras, un protocolo de comunicación, también llamado en este caso protocolo de red, define la forma en la que los distintos mensajes o tramas de bit circulan en una red de computadoras.

### **2.9.2 Modelo OSI**

El modelo OSI (Open System Interconnection) fue creado en 1984 por ISO con el objetivo de establecer un estándar en las comunicaciones que acabara con la incompatibilidad de redes que existía en la época. Antes del modelo OSI, las redes utilizaban todo tipo de especificaciones diferentes que surgían de manera incontrolada como resultado de las empresas que desarrollaban tecnologías de redes privadas o propietarias. Por lo tanto tan solo aquellas redes que se utilizaba la misma especificación podían comunicarse entre sí.

Para conseguir una compatibilidad global de las redes de computadoras surgió OSI, que es un modelo que está formado por siete capas. A continuación se describen las características básicas de las capas del modelo OSI:

- **Capa física.** Se encarga de gestionar la conexión física que se establece entre la red y el ordenador, es decir la transmisión de los bits a través del canal de comunicación. Sus funciones están relacionadas con las características del medio, como por ejemplo definir el nivel del voltaje que se usara para representar un 1 y un 0, el tipo de comunicación que se establece



en el canal (*full-duplex, half-duplex*) la velocidad de transmisión, la codificación de las señales y su modulación.

- Capa de enlace. Proporciona una comunicación libre de errores para que la transmisión se realice de manera fiable. Entre sus principales funciones se encuentra la detección y corrección de errores, el control del flujo, el direccionamiento físico.
- Capa de red. Se encarga de asegurar el encaminamiento de la información desde el origen hasta un destino. Es decir, de encontrar un camino a través de las diferentes subredes de ordenadores para conseguir que dos ordenadores que se encuentren en distintas redes se puedan comunicar. También tiene como función controlar el flujo de tráfico de la red para evitar congestiones.
- Capa de transporte. Su principal función es recibir los datos de la capa de sesión, dividirlos en paquetes más pequeños y enviarlos a la capa de red.
- Capa de sesión. Permite establecer una sesión entre dos ordenadores controlando aspectos fundamentales como quien envía y recibe información. También se encarga de establecer *chekpoints* para reanudar las transmisiones en el caso de que se interrumpan por cualquier motivo.
- Capa de presentación. Se encarga de codificar la información al estándar adecuado para que los ordenadores que están comunicándose puedan entender los datos. Por ejemplo, en el caso de una transmisión de caracteres su presentación puede ser en formato ASCII, Unicode, etc.
- Capa de aplicación. Determina el protocolo que utilizan los ordenadores para comunicarse. Cada aplicación utiliza un protocolo diferente, entre los que cabe destacar: HTTP (navegación por internet). FTP (transferencia de archivos), SMTP (correo electrónico), etc. De esta forma se consigue que la comunicación sea transparente para el usuario mientras que interactúa con una aplicación sin necesidad de conocer el protocolo que utiliza.

### 2.9.3 Modelo TCP/IP

El modelo TCP/IP es un modelo de descripción de protocolos de red desarrollado en los años 70 por *Vinton Cerf* y *Robert E. Kahn*. Fue implantado en la red ARPANET, la primera red de área amplia, desarrollada por encargo de DARPA, una agencia del Departamento de defensa de los Estados Unidos, y predecesora de la actual red Internet. EL modelo TCP/IP se denomina a veces como *Internet Model*, *Modelo DoD* o *Modelo DARPA*. El modelo TCP/IP describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario. Existen protocolos para los diferentes tipos de servicios de comunicación entre equipos.

El modelo TCP/IP está formado por cuatro capas y recibe su nombre los dos protocolos más importantes que le componen: el protocolo TCP (*Transmission Control Protocol*) y el protocolo IP (*Internet Protocol*). A continuación se muestra la correspondencia que existe en las capas del modelo OSI y las del modelo TCP/IP:

- Capa de acceso. También conocida como capa host-red, incluye las capas física y de enlace del modelo OSI.
- Capa de internet. Equivale a la capa de red del modelo OSI
- Capa de transporte. Realiza la misma función que la capa de transporte del modelo OSI
- Capa de aplicación. Engloba las tres últimas capas del modelo OSI: capa de sesión, de presentación y aplicación. (Gomez, 2008)

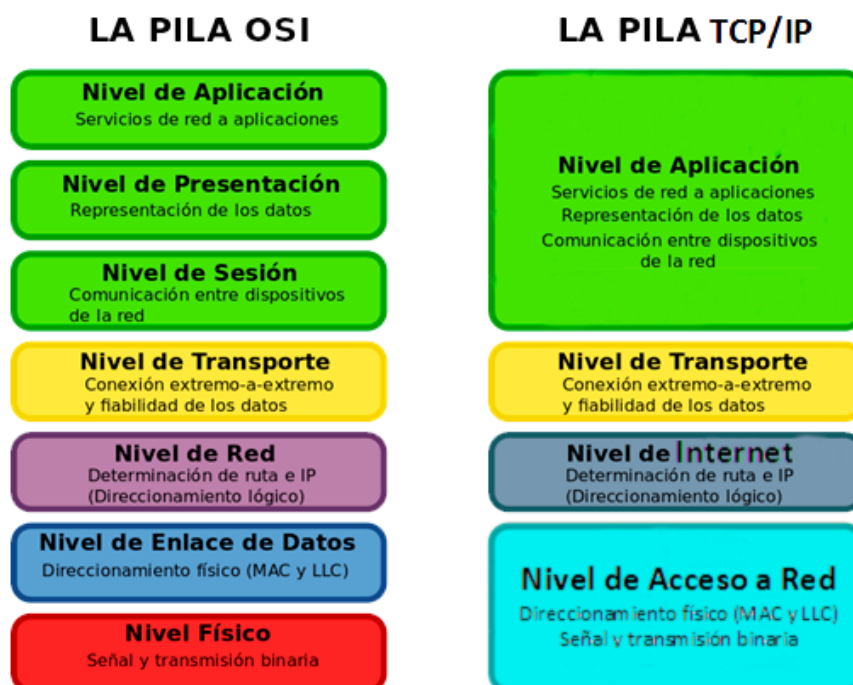


Figura 63. Modelos de referencia OSI y TCP/IP  
<http://smr.iesharia.org/wiki/doku.php/rde:ut7:caracteristicas>

# CAPÍTULO III

## REDES MESH

### III. REDES MESH (Wireless Mesh Network)

*Wireless Mesh networks (WMNs)* han surgido como una nueva tecnología de redes inalámbricas. Debido a sus ventajas sobre otras redes inalámbricas, *WMNs* han evolucionado rápidamente y actualmente existen numerosos proyectos de aplicación. Sin embargo, existen diversos problemas técnicos que están siendo sometidos a estudios y búsquedas de investigación. Para poder dar a conocer esta tecnología así como sus características, este artículo presenta una descripción detallada de la estructura de *las WMNs* y una explicación de los Diversos protocolos sobre los que se asienta. (Suarez, 2009)



Figura 64. Funcionamiento de una Red Mesh  
[http://www.qta.ufri.br/grad/06\\_2/felipe/arquitetura\\_ff.htm](http://www.qta.ufri.br/grad/06_2/felipe/arquitetura_ff.htm)

#### 3.1 Introducción

Las redes Mesh, redes acopladas, o redes de malla inalámbricas de infraestructura, unen las dos topologías de las redes inalámbricas: la topología ad-hoc y la topología infraestructura. Estas redes se auto-organizan y auto configuran dinámicamente con los nodos de la red, estableciendo Automáticamente una red ad-hoc y manteniendo la conexión. Las WMNs (Wireless Mesh Networks) están formadas por dos tipos de nodos: los *routers* Mesh y los clientes Mesh. Además de las funciones propias de un router Wireless convencional, el router Mesh contiene funciones adicionales para soportar la infraestructura Mesh. Gracias al sistema de comunicaciones *multi-hop*, se puede conseguir la misma cobertura con menos energía de transmisión. Los *routers* Mesh permiten unir a la red dispositivos que a pesar De estar fuera del rango de cobertura de los puntos de acceso (PA), están dentro del rango de cobertura de alguna tarjeta de red que directa o indirectamente está dentro del rango de cobertura de un punto de acceso de la red. (Suarez, 2009)

### 3.1.1 Primera Generación

Usa el mismo enlace de radio para la transmisión de datos entre el cliente y el nodo, así como entre nodos. Tiene transmisión store-and-forward.

Desventaja: Disminución del ancho de banda, No se puede transmitir simultáneamente por un solo canal de radio por que provocaría interferencia, congestión y contención en cada nodo. (Gonzalez, 2013)

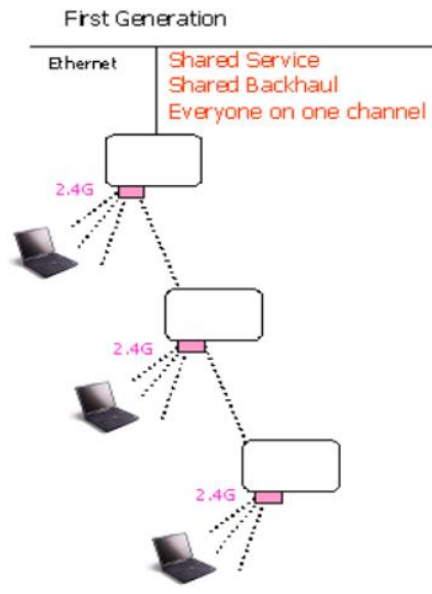


Figura 65. Esquema de la primera generación de redes Mesh  
[http://profesores.elo.utfsm.cl/~agv/elo323/2s12/project/reports/Araya\\_Lopez/generaciones.html](http://profesores.elo.utfsm.cl/~agv/elo323/2s12/project/reports/Araya_Lopez/generaciones.html)

### 3.1.2 Segunda Generación

Combina dos canales, el 802.11 b/g para dar servicio y el 802.11<sup>a</sup>, con este sistema se logró eliminar la interferencia en los nodos, ya que se trabaja con diversas bandas de frecuencia (entre 2.4Ghz y 5.8GHZ).

Desventaja: Al aumentar la demanda de servicio por parte del usuario, se presenta congestiones significativas en la parte de la radio que usa para interconectar los nodos.

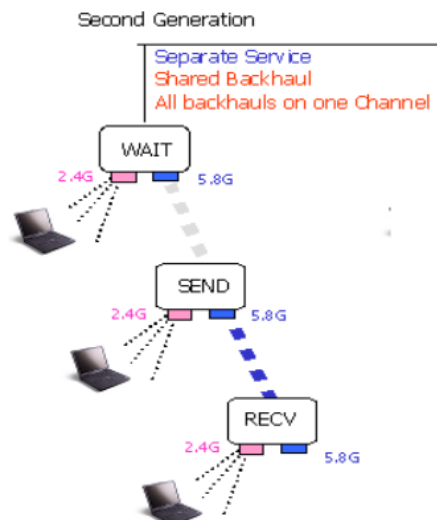


Figura 66. Esquema de la primera generación de redes Mesh  
[http://profesores.elo.utfsm.cl/~agv/elo323/2s12/project/reports/Araya\\_Lopez/generaciones.html](http://profesores.elo.utfsm.cl/~agv/elo323/2s12/project/reports/Araya_Lopez/generaciones.html)

### 3.1.3 Tercera Generación

Los canales disponibles se pueden reutilizar, haciendo que el espectro disponible sea más amplio y que el funcionamiento de la red aumente 50 o más veces.

Los equipos de esta generación se basan en productos multi-radio que soportan múltiples configuraciones de red.

Un radio de los equipos de tercera generación se usa para crear un enlace hacia su nodo *upstream* (nodo más cerca al Gateway) y otro radio se utiliza para un enlace *downstream* al nodo vecino siguiente.

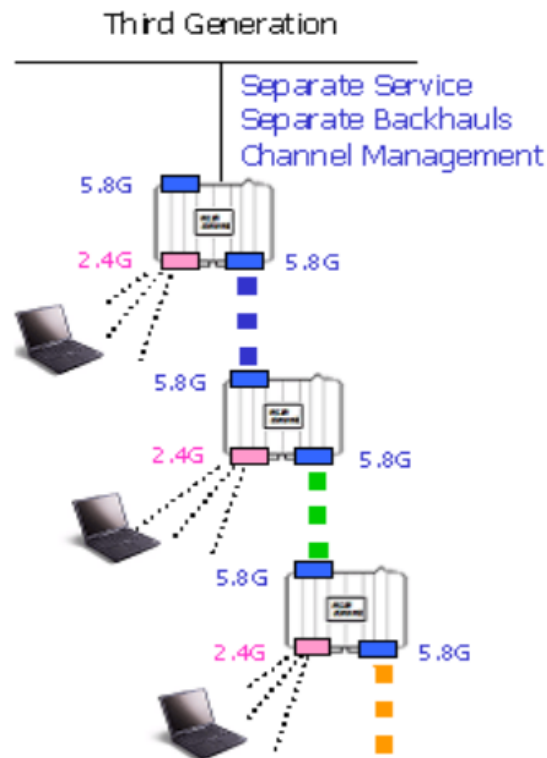


Figura 67. Esquema de la tercera generación de redes Mesh  
<http://profesores.elo.utfsm.cl/~agv/elo323/2s12/project/reports/ArayaLopez/generaciones.html>

### 3.2 Arquitectura de las Redes Mesh

La arquitectura de las redes Mesh se apoyan sobre una infraestructura modular que permite realizar un diseño escalable con tanta precisión como requiera cada aplicación individualizada, los nodos son utilizados tanto para los dispositivos de los clientes (red de acceso) como para la propia comunicación entre nodos.

Debido a la tecnología empleada en las redes inalámbricas Mesh se consigue mayor capacidad de transmisión con menor latencia, de este modo los usuarios pueden disponer de diferentes aplicaciones en tiempo real en la actualidad las tecnologías inalámbricas más utilizadas por las redes Mesh públicas son Wi-Fi y Wi-Max. (Bravo, 2008)

- Enrutadores Mesh

Los enrutadores Mesh o Mesh routers son equipos que cumplen con el trabajo de un *Access point* convencional, estos forman una malla de nodos fijos la cual es llamada red de infraestructura o *backbone*. Además estos equipos pueden trabajar con varias tecnologías de radios para la interconexión entre ellos, por ejemplo con la IEEE 811. Tienen doble función, el de proporcionar acceso a la red a los clientes y el de hacer una comunicación *multi-hop* entre ellos para el correcto direccionamiento y entrega de datos.

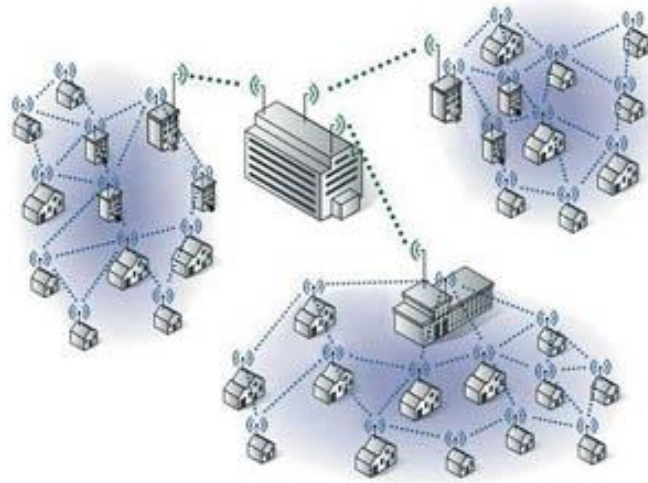


Figura 68. Nodos Mesh

<http://www.enriquedans.com/2006/06/las-consecuencias-de-tener-nuestra.html>

### 3.2.1 Características de las Redes Mesh

La tecnología de las redes inalámbricas tipo Mesh están creciendo enormemente de manera gradual a un punto donde no puede ser ignorado por la sociedad tecnológica, cuando se considera el despliegue de las tecnologías de redes inalámbricas en la actualidad. El primer despliegue de una comunidad Mesh en gran escala incluso hasta algunos cientos de nodos. Se ha demostrado suficientes ventajas para motivar futuros experimentos. Esto hace que las redes Mesh sean una de las tecnologías más prometedoras en los próximos años y estén a la vanguardia respecto a las demás.

- Las WMN son redundantes, los nodos que conforman la red están conectados unos con otros por varios caminos, mediante esta configuración obtenemos rutas redundantes por toda la red, lo cual permite que si una ruta falla otra se encargara del tráfico de datos.
- Fácil despliegue, por ser redes con capacidad de autoconfiguración (*routing* y selección dinámica de canal), permiten dar soluciones de conectividad en situaciones de emergencia o catástrofes naturales.
- Son auto-regenerables, auto-configurables, permiten la auto-reparación de rutas, por trabajar con protocolos de última generación Mesh, permiten descubrir nuevos nodos admitiéndolos en la comunidad ya existente y regenerando nuevas tablas de encaminamiento.
- Son robustas, por el tipo de enrutamiento que se aplica se contienen un gran estabilidad en cuanto a condiciones variables o en alguna falla de un nodo en particular

- Ahorran energía, para energizar cada nodo de la red mallada no solo se puede usar energía sino también energía solar, eólica, hidráulica celdas de combustible entre otras.
- Su topología permiten que sean útiles en entornos urbanos y rurales, en diferentes partes del mundo las WMN han sido propuestas para soluciones de entornos urbanos y municipales. Sin embargo estas redes también son una buena solución para problemas de conectividad en entornos rurales o lejanos.
- Mayor capacidad a bajo coste, hay estudios que han demostrado que la capacidad de una red inalámbrica puede ser mejorada mediante la utilización de repetidores existiendo un compromiso entre distancia e interferencia entre nodos.

### 3.2.2 Entornos de Aplicación

Hasta ahora. Las redes Mesh han sido mayormente propuestas para redes urbanas y redes municipales y redes en escuelas. Sin embargo hay un gran potencial para redes Mesh en zonas de conectividad rurales o lejanas donde las redes convencionales son muy costosas, o simplemente de muy difícil acceso para redes alambradas.

Para zonas rurales la combinación de enlaces Wi-Fi de larga distancia con redes Mesh representan indudablemente la forma más económicas de ofrecer conectividad y constituyen tecnologías que pueden ser instaladas por las propias comunidades, sin necesariamente depender de las empresas tradicionales de comunicaciones que a menudo son reacias a hacer las inversiones necesarias para ofrecer servicio en zonas de baja densidad de población o habitadas por gentes de escasos recursos económicos por temor a no recuperar las ingentes inversiones requeridas para dar servicio con los métodos tradicionales. (Networking, 2013)

Áreas rurales, permiten introducir servicio de banda ancha en entornos rurales para implantar servicios sociales esenciales y promocionar la sociedad de la información. La instalación en estas zonas de las redes inalámbricas malladas ofrecen innumerables ventajas: (Bravo, 2008)

- No requiere ninguna infraestructura previa de telecomunicaciones
- Su implantación resulta rentable
- Cada nodo presta cobertura a grandes extensiones
- Enlaces directos de “*Backhaul*” entre nodos
- Posibilidad de utilización de repetidores que resuelven problemas de ortografía y salvan largas distancia.

Áreas metropolitanas la aplicación de esta tecnología en grandes ciudades presenta ventajas en su instalación y uso:

- Facilidad de implantación utilizando mobiliario para la instalación
- Ajuste preciso de las zonas de cobertura sobre la calles
- Uso de nodos repetidores
- Uso de antenas directivas
- Flexibilidad de interconexión
- Aprovechamiento de infraestructura existente
- Utilización del “*Backbone*” propio



Áreas Municipales: Las redes inalámbricas Mesh son una solución natural para la implantación de nuevas tecnologías en entornos municipales. Su utilización puede destinarse a servicios como:

- Seguridad ciudadana
- Supervisión y control de tráfico
- Servicio al ciudadano en materias de Sociedad de la información acceso a internet en centros escolares y bibliotecas, así como información y orientación turística entre otros.

Aplicaciones personalizadas: La versatilidad en las redes inalámbricas Mesh simplifica su adaptación a escenarios temporales su despliegue permite dar respuesta a necesidades cambiantes que precisan de una actualización constante por la aparición continua de nuevos obstáculos, resultan por tanto extraordinario su utilización en casos como:

- Redes de seguridad y control de acceso durante la construcción de edificios
- Eventos musicales y/o deportivos
- Escenarios de desastres naturales donde es posible generar de manera casi inmediata una red de comunicaciones

Escenarios donde las redes inalámbricas WMN son una alternativa: Las redes inalámbricas son necesarias y toman ventaja frente a una infraestructura cableada cuando:

- En el lugar donde se desea implementar la red, el tendido de cables es costoso o prohibido
- Se necesitan instalaciones temporales, por ejemplo en un cambio de oficina por un corto tiempo
- Existe saturación de cables, ya sea por líneas telefónicas o la red eléctrica
- Los usuarios son móviles y necesitan tener acceso a la red
- La red se implementa donde el índice de robo de cables es muy alto.

Tipos de escenarios para las redes Mesh:

- Escenario corporativo o Empresarial
- Escenario operador/ proveedor
- Escenario usuario final

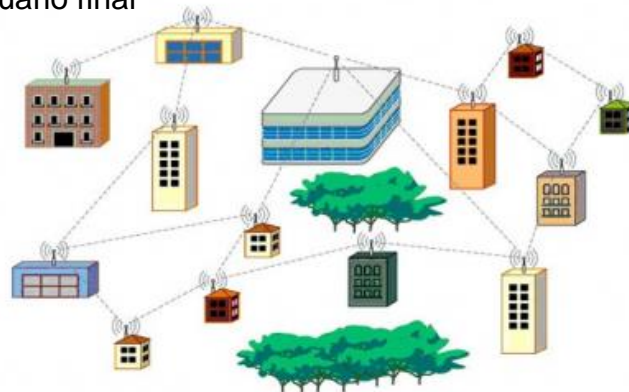


Figura 69. Red Mesh implementada en un entorno urbano  
<http://www.alibaba.com/countrysearch/RW/wireless-wi.html>

### 3.2.3 Técnicas de Funcionamiento

En las redes Mesh, cada nodo de radio múltiple soporta una cobertura de “*Backhaul*” (comunicación entre nodos) en todas las direcciones, gracias a que se utiliza una estructura circular de antenas.

Para lograr la disponibilidad del sistema de red, se combina diferentes técnicas:

- Tanto la potencia como la velocidad de transmisión cambian dinámicamente en cada uno de los enlaces para compensar efectos como “fading” o “*shadowing*” (desvanecimiento o sombreado)
- Los algoritmos de enrutamiento tienen en cuenta el estado de las conexiones de radio y seleccionan la mejor ruta basándose en la capacidad disponible la latencia y el rendimiento del enlace
- Para incrementar el tiempo de operación de los equipos y minimizar los cortes de comunicación el tráfico de cada equipo puede ser equilibrado encaminamiento a través de dos o más rutas minimizando además posibles problemas por saturación de enlaces u otros fallos
- Los equipos calculan continuamente los posibles caminos alternativos de modo que es posible enrutar el tráfico minimizando la pérdida de información debido a posibles fallos

En esta imagen se muestra el funcionamiento de los 3 diferentes nodos en una red Mesh. Los nodos de un solo radio se comunican con los de doble radio, estos a su vez se comunican con nodos de un solo radio y de varios radios y los nodos de varios radios solo se comunican con los de los dos radios. (Bravo, 2008)

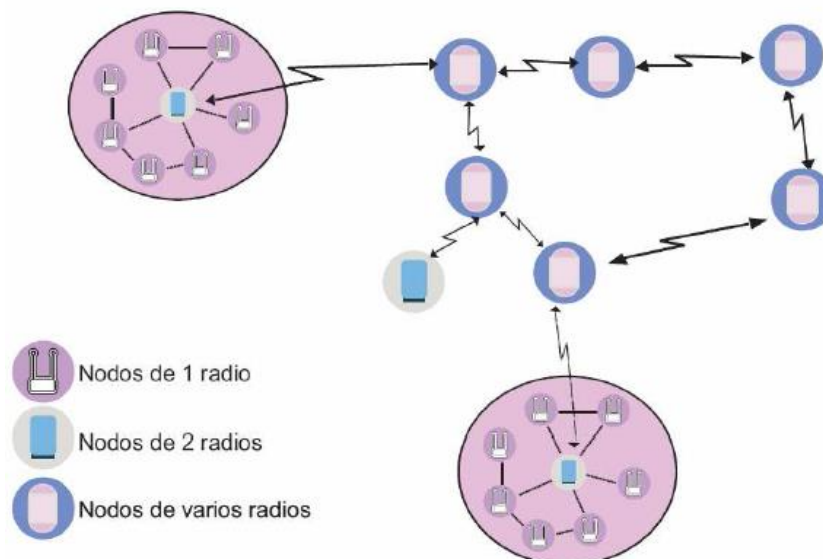


Figura 70. Funcionamiento de los nodos de una red Mesh  
<http://falcowebb.com/FreeEagleBlog/wi-fi/como-configurar-equipos-wi-fi-ubiquity-en-modo-red-mallada-mesh/>

### 3.2.4 Trafico en la red (Balanceo de Carga)

Uno de los beneficios de este tipo de redes es la redundancia de camino múltiple sin embargo algunas veces muchos nodos utilizan los mismos enlaces causando congestión mientras que otros enlaces están inactivos. Muchos consideran el balanceo de carga como un método que permite lograr equidad en una red Mesh el método de balanceo de carga puede ser aplicado: en los enlaces, en los routers Mesh, en las puertas de enlace Gateway hacia le internet. La distribución de trafico de una red Mesh es desigual, donde la mayoría de los nodos de una red Mesh se comunica con nodos de una red cableada el objetivo de balanceo de carga es ayudar a evitar enlaces con cuello de botella e incrementar la eficiencia de la utilización de los recursos de la red.

Cuando hablamos del enrutamiento de balanceo de carga se dice que está basado en la construcción de un árbol básico de manera similar como se utiliza el algoritmo de formación *spanning tree* pero haciendo énfasis que la métrica utilizada en cada nodo para determinar el nodo principal es dinámica para lograr el balanceo de carga. Para realizar la métrica la enrutamiento que se realiza es el contador de saltos *hop count* que resulta ser más estable ya que es más estático además que se produce de manera rápida la convergencia. También tenemos la capacidad residual del Gateway, en la cual tenemos más carga balanceada, así como también la red se adapta al tráfico y las rutas tienen menos intermitencias debido a que la red es dinámica. Finalmente tenemos la capacidad residual del camino debido al peso y flujo del tráfico los enlaces se modifican evitando cuellos de botella en el Gateway.

Cuando se agina u canal se conoce un punto nombrado la conexión al interface del vecino, en la cual el problema en el diseño de un algoritmo de asignación de un canal distribuido es la dependencia del canal entre os nodos. También tenemos la asignación de la interface del canal, donde par asignar canales se necesita estimar un aproximado del estado de su uso de todos los canales dentro de la interferencia de todos los nodos de la red.

Tipos de balanceo de carga:

- Balanceo de carga definido
- Balanceo de carga por ruta
- Balanceo de carga basado en el Gateway

### 3.2.5 Aplicaciones

La arquitectura inalámbrica Mesh es la única capaz de lograr que múltiples redes de alta capacidad puedan operar de modo conjunto par a satisfacer servicios públicos o privados; como por ejemplo la seguridad pública o el transporte, las redes inalámbricas Mesh de tercera generación están provistas de banda ancha que alcanzan un 100% de portabilidad y conectividad.

En una instalación de radio múltiple mientras una red puede ser dedicada para el acceso a internet a alta velocidad, otras redes pueden soportar servicios esenciales como a comunicación con la policía, bombero, servicios sanitarios información del tráfico. (Bravo, 2008)

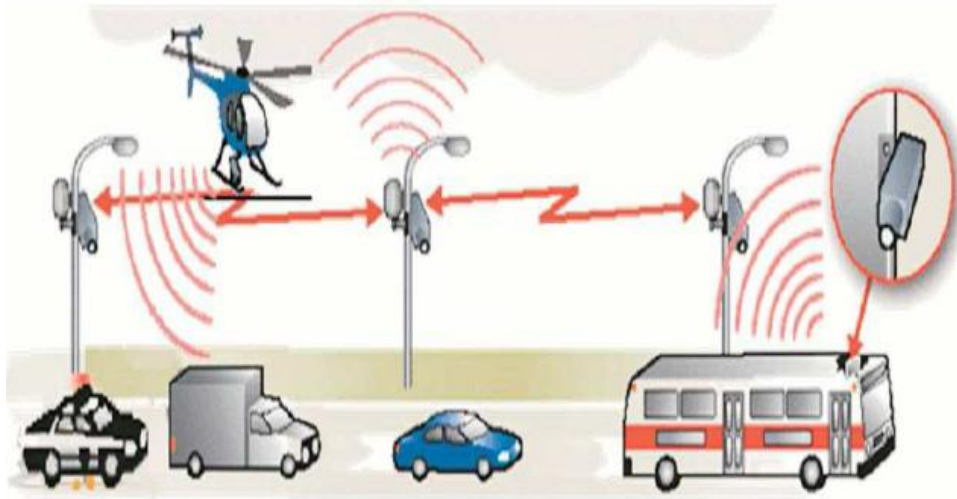


Figura 71. Aplicaciones de una red Mesh  
<http://es.slideshare.net/omarmanjarrezjuarez/mesh-16985976>

### 3.2.6 Fiabilidad y robustez

Las redes inalámbricas Mesh mejoran la fiabilidad y robustez de la comunicación. La topología de una malla parcial en una red Mesh proporciona alta fiabilidad y diversidad de rutas contra nodos y fallas en los enlaces. Los múltiples radios de una red Mesh ofrecen una importante ventaja de la solidez en la diversidad de la comunicación. Por ejemplo errores en el canal de un sistema inalámbrico puede ser altamente comparado con redes cableadas, por lo tanto, una degradación de la calidad de comunicación durante los errores de un canal alto es necesario.

El uso de interfaces de radio múltiple permite la diversidad de frecuencia, por lo que puede causar una pérdida total de la conectividad debido a la degradación de la señal a demás los radio pueden usar módulos de conmutación que sean adecuados para lograr la tolerancia a fallos en comunicación ya se por cambios de las radios, los canales o mediante el uso de múltiples radios simultáneamente.

### 3.2.7 Movilidad (Efecto *Roaming*)

El termino *roaming* corresponde al concepto de itinerancia, es un concepto utilizado en las comunicaciones inalámbricas para describir la capacidad que tiene un dispositivo o móvil para movilizarse de una zona de cobertura a otra. Cuando el *roaming* está activado, es fluido entre los diferentes puntos de acceso manteniendo la conexión si el usuario está en movimiento la red inalámbrica consiste de microceldas o áreas de cobertura para que el usuario pueda moverse libremente en un campus tanto en el interior como en el exterior de los edificios para que sea factible el *roaming* y se evite corte de comunicación, debe existir una pequeña zona de superposición conocido como *Overlapping* que está cubierta de al menos dos puntos de acceso. *Roaming* es el proceso por el que un usuario cambia entre los puntos de acceso en una red inalámbrica Mesh.

### 3.2.8 Ataques en las redes Mesh

Existen diferentes tipos de amenazas que afectan este tipo de redes inalámbricas ataques externos e internos. Los atacantes externos son puestos en marcha por intrusos que no pertenecen a la red Mesh y tratan de acceder ilegítimamente a la red, donde pueden atorar la comunicación o inyectar una información errónea. Los principales ataques se basan en la encriptación y autenticación.

Los ataques internos son aquellos que provienen de nodos que forman parte de la red, estas amenazas son más severas, puesto que los ataques internos no son tan fáciles de prevenir como los externos, debido a que tiene acceso a toda la manipulación de información y autenticación de la misma. Existen mecanismos de cooperación que ayudan a detectar y aislar los nodos conocidos como mecanismos de mal comportamiento. Podemos identificar ataques pasivos que se proponen a robar la información y espiar en la comunicación dentro de la red, y ataques activos donde el atacante modifica e inyecta paquetes en la red. Los ataques podrían apuntar a varias capas de los protocolos.

En la capa física un atacante puede embotellar las transmisiones de antenas inalámbricas o simplemente destruir el hardware de cierto nodo. Ta les ataques se pueden detectar y localizar fácilmente. En la capa MAC un atacante puede enviar paquetes de control y de datos a nodos que pertenecen a la red o personificar u nodo legal. Aquí podemos distinguir los siguientes ataques: (Manrique, 2009)

- *Eavesdropping*
- Ataque de *Jamming*
- Ataque de suplantación (*spoofing*)
- Ataque de repetición
- Ataque apresurado (*Rushing*)
- Ataque de agujero de gusano (*Wormhole*)
- Ataque del hoyo negro (*Blackhole*)

### 3.3 Estándares Mesh

Los estándares para una tecnología son necesarios ya que estos son los encargados de proporcionar y facilitar la comunicación y la interoperabilidad entre dispositivos de diferentes fabricantes, además permite que el mercado de esta tecnología sea más competitivo, permitiendo a los usuarios tomar decisiones y elegir la mejor opción entre la variedad de productos que tengan los fabricantes.

Existen varios grupos de trabajo que dependiendo del sistema mallado que se desee aplicar y el tipo de servicio que se desea proveer, están trabajando en nuevas especificaciones para las redes malladas o WMN, entre ellos tenemos el IEEE 802.15 y el IEEE 802.16.

### 3.3.1 IEEE 802.11s

En el primer capítulo se mencionó varios de los estándares de la familia del IEEE 802.11, pero estas normas solo son para comunicaciones *one-hop* (de un solo salto), por lo tanto no son apropiadas para ser aplicadas en redes *multihop* (múltiples saltos), *multichannel* (múltiples canales de transmisión) y cuando se opera con múltiples radios. Sin embargo, el IEEE creó un grupo de trabajo para que desarrolle el estándar 802.11s para ser usado en redes malladas.

Los equipos que trabajan con el estándar 802.11s, es decir que tienen funcionalidades para trabajar en una red mallada, se denominan Mesh Point (MP). Un sistema de distribución inalámbrico (WDS) es aquel conjunto de *MPs* conectados en forma de malla. Además en este estándar se involucran equipos como los Mesh Access Point (MAP) y los Mesh portal *point* (MPP) que son *MPs* específicos, los primeros trabajan como puntos de acceso (*APs*) y los segundos ayudan a interconectar redes malladas.

El estándar 802.11s tiene dos procesos importantes y necesarios para el funcionamiento de una red mallada:

- La asociación de un equipo terminal con un MAP.
- La asociación de un MAP con un nodo vecino.

La función principal del estándar propuesto es realizar la coordinación del acceso al medio denomina MCF, que incluyen procesos como: Aprender la topología de la red mallada, ruteo y *forwarding*, descubrir topologías y realizar las asociaciones entre nodos, seguridad de la red, configuraciones y monitoreo.

Cabe mencionar que existen otros estándares que pertenecen al grupo IEEE 802.11 como el 802.11a, 802.11b, 802.11g y 802.11n, que aplicándolos de una manera idónea pueden también trabajar en una red mallada, dando los mismos servicios y aplicaciones como los estándares exclusivos para WMN. (Torres, 2006)

### 3.3.2 IEEE 802.15

IEEE 802.15 es un grupo de trabajo dentro de IEEE 802 especializado en redes inalámbricas de área personal (*wireless personal area networks*, WPAN). Se divide en cinco subgrupos, del 1 al 5. Los estándares que desarrolla definen redes tipo PAN o HAN, centradas en las cortas distancias. Al igual que Bluetooth o *ZigBee*, el grupo de estándares 802.15 permite que dispositivos portátiles como PC, *PDA*s, teléfonos, *paggers*, sensores y actuadores utilizados en domótica, entre otros, puedan comunicarse e interoperar. Debido a que Bluetooth no puede coexistir con una red inalámbrica 802.11.x, se definió este estándar para permitir la interoperabilidad de las redes inalámbricas LAN con las redes tipo PAN o HAN. (Commons, 2014)

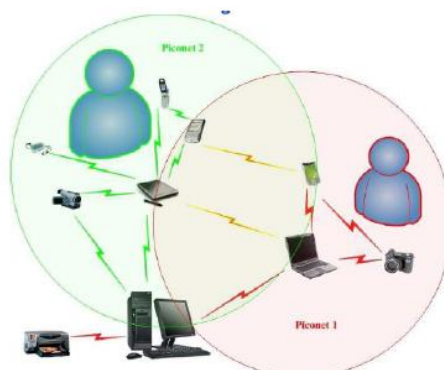


Figura 72. Wireless Personal Área Network

El IEEE 802.15 está dividido en 5 grupos de trabajo, como se muestra en la tabla:

IEEE 802.15 Wireless Personal Area Network (WPAN)		
Grupo de Trabajo	Estándar	Tema
1	802.15.1	WPAN/Bluetooth
2	802.15.2	Coexistencia
3	802.15.3	WPAN High Rate
4	802.15.4	WPAN Low Rate
5	802.15.5	WPAN Mesh

Tabla 6. Grupos de trabajo del IEEE 802.15

El estándar que se encarga de desarrollar mecanismos para un buen funcionamiento de las capas física y MAC de las WPAN malladas es el IEEE 802.15

Los objetivos de este estándar son:

- Lograr que la cobertura de la red mallada sea amplia.
- Aplicar de forma eficiente las redundancias que existen en las redes malladas.
- Que los mecanismos de autoconfiguración y auto regeneración de rutas sean sencillos.
- Tratar de aumentar la velocidad de comunicación de la información.
- Reducir las retransmisiones.

### 3.3.3 IEEE 802.16

Los estándares del grupo 802.16 son ideales para ambientes metropolitanos y rurales, porque están diseñados para *Broadband Wireless Access* (BWA) con un bajo costo de la red y proporcionando alta velocidad de transmisión, facilidad de instalación y gran cobertura.

Entre otras características de estos estándares podemos citar:

- Permiten trabajar en bandas del espectro que necesitan licencia y en las que son libres.
- El servicio que pueden proveer puede ser móvil o fijo.
- Utilizan antenas sectoriales tradicionales o antenas adaptativas con modulaciones flexibles que permiten intercambiar ancho de banda por alcance.

Así como en los grupos de trabajo anteriores el IEEE 802.16 también tienen subgrupos de trabajo, pero el estándar que tiene mecanismos para trabajar en redes malladas es el 802.16<sup>a</sup>, que tiene las siguientes características:

- Pueden trabajar en redes *Multihops*.
- Opera en el rango de frecuencia bajas 2-11GHz.
- Puede trabajar hasta una tasa de 75Mbit/s con canales de 20MHz.
- El radio de una celda es de 5 – 10km aprox.

Además, en las redes que utilizan este estándar se pueden realizar las operaciones de dos maneras diferentes: distribuida o centralizada.

En la distribuida, todos los nodos deben coordinar con los demás la manera de transmitir para evitar colisiones con los datos y evitar el control de tráfico, deben enviar por difusión (*broadcast*) su respectivo estado (recursos disponibles, peticiones y concesiones) a todos sus vecinos.

En la centralizada, los recursos se asignan de una manera más concentrada, ya que la estación base Mesh (dispositivo central de un sector de la red), recopila varias peticiones de un determinado sector y otorga los respectivos recursos para cada enlace, tanto para el *downlink* como el *uplink*, al mismo tiempo que comunica estas decisiones a las demás estaciones bases. (Ruiz, 2009)

### 3.4 Modos de operación de las redes Mesh

El conjunto de estándares 802.11 definen dos modos fundamentales para redes inalámbricas:

1. Ad hoc
2. Infraestructura
3. Híbrida

Es importante comprender que no siempre, los modos se ven reflejados directamente en la topología. Por ejemplo, un enlace punto a punto puede ser implementado en modo ad hoc o Infraestructura y nos podríamos imaginar una red en estrella construida por conexiones ad hoc. El modo puede ser visto como la configuración individual de la tarjeta inalámbrica de un nodo, más que como una característica de toda una infraestructura.

#### 3.4.1 Red Ad-hoc IBBS (*Independent Basic Service Set*).

Permite exclusivamente comunicaciones directas entre los distintos terminales que forman la red. No existe ninguna terminal principal que coordine al grupo. También se le conoce como ad-hoc, independientemente o de igual a igual (peer to peer).

También conocidas como MANET "*Mobile ad hoc networks*". AD HOC viene del latín y se refiere a algo improvisado, mientras que en comunicaciones el propósito de ad hoc es proporcionar flexibilidad y autonomía aprovechando los principios de auto-organización. Una red móvil ad hoc es una red formada sin ninguna administración central o no hay un nodo central, sino que consta de nodos móviles que usan una interface inalámbrica para enviar paquetes de datos. Los ordenadores están en igualdad de condiciones. La conexión es establecida por la duración de una sección. Los artefactos descubren otros artefactos cercanos o en rango para formar el "*network*". Los artefactos pueden buscar nodos que están fuera del área de alcance conectándose con otros artefactos que estén conectados a la red y estén a su alcance. Las conexiones son posibles por múltiples nodos. (Lesta, 2006).



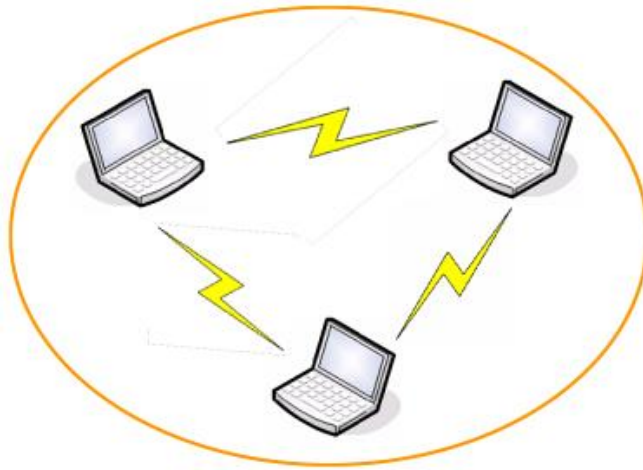


Figura 73. Red en modo Ad-hoc

[http://itlaw.wikia.com/wiki/File:Bluetooth\\_ad\\_hoc.jpg](http://itlaw.wikia.com/wiki/File:Bluetooth_ad_hoc.jpg)

### 3.4.2 Infraestructura BSS (*Basic Service Set*)

Existe un equipo llamado punto de acceso que realiza las funciones de coordinación centralizada de la comunicación entre las distintas terminales de la red. A esta modalidad de topología se le conoce como de infraestructura. Una topología de infraestructura es aquella que conecta una LAN de cable con una LAN inalámbrica a través de una estación base, denominada punto de acceso. El punto de acceso une la LAN inalámbrica y la LAN de cable y sirve de controlador central de la red LAN inalámbrica. El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica: La extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. En la modalidad de infraestructura puede haber varios puntos de acceso para dar cobertura en una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño. (Lopez, 2005)

- Modo *Manager*. Es el modo en el que el Tx se conecta al AP para que este último le sirva de concentrador
- Modo *master*. Este es el modo en el que el Tx se conecta al AP, pero en el que también pueden entrar los Tx si se dispone del firmware apropiado o de un ordenador que sea capaz de realizar la funcionalidad requerida

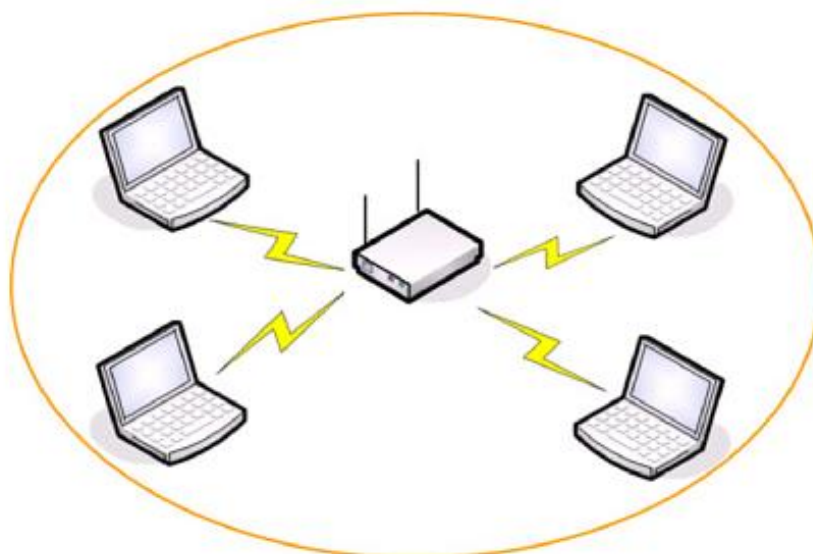


Figura 74. Red en modo Infraestructura

<http://www.myshared.ru/slide/710182/>

### 3.4.3 Modo Híbrido

Las redes inalámbricas híbridas combinan el funcionamiento tanto de las redes ad hoc como el de las redes en modo infraestructura. De este modo, la conectividad entre los dispositivos que conforman la red es más flexible y ofrecen un amplio conjunto de propiedades que pueden ser adaptadas a diversas aplicaciones. La Figura 2.3 muestra un ejemplo de la conectividad existente en esta arquitectura de red. Bajo este esquema, los APs actúan como interfaces entre los dispositivos móviles y la red cableada, mientras que los dispositivos móviles son capaces de encaminar información entre ellos y, al mismo tiempo, pueden acceder directa o indirectamente a la red cableada. Estas características incrementan sustancialmente el desempeño de la red, pues se genera un sistema interconectado, dinámico y tolerante a fallas. Bajo esta arquitectura de red, la cobertura de la red cableada se ve sustancialmente incrementada, sin embargo, dada la libertad de movimiento de los nodos móviles dicha cobertura es altamente variable y poco estable. (Cabrera, 2008)

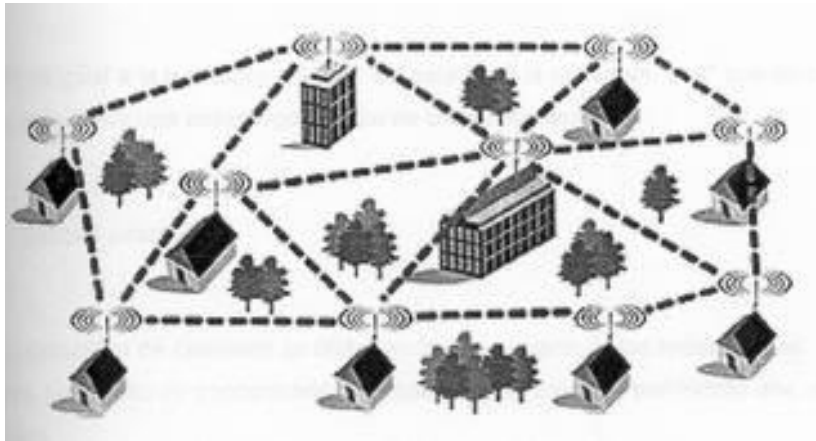


Figura 75. Red en modo Híbrido

[http://yovaniredes-redes.blogspot.com/2010/04/topologias-de-red\\_05.html](http://yovaniredes-redes.blogspot.com/2010/04/topologias-de-red_05.html)

## 3.5 Niveles o capas de las Redes Mesh

Se han diseñado varias herramientas para ayudar a los diseñadores de protocolos a entender las partes del problema de comunicación y planear la familia de protocolos. Una de estas herramientas y la más importante es el modelo de capas es solo una manera de dividir el problema de la comunicación en partes llamadas capas. La familia de protocolos puede diseñarse especificando un protocolo que corresponda a cada capa. (Riera, 2006)

### 3.5.1 Nivel Físico

La capacidad de un canal radio depende del nivel de interferencias recibido o, mejor dicho, de su SNR (*Signal to Noise Ratio*). Al tener mayor densidad de nodos en este tipo de redes y, siendo el espectro radioeléctrico limitado, es necesario optimizar al máximo la utilización del canal minimizando las interferencias. Los mecanismos básicos para la minimización de interferencias son la selección dinámica de frecuencia (DFS) y el control de potencia (TPC), aunque para ser aplicados en estas arquitecturas

necesitan un gran control por parte de los protocolos de capas superiores. La utilización de antenas inteligentes, de antenas adaptativas o de antenas auto configurables y reprogramables vía software (radios cognitivas) son algunos de los tópicos actuales de investigación que pueden mejorar a aumentar la capacidad ofrecida por estas redes. También, el uso de técnicas MIMO (*Multiple Input Multiple Output*) para aumentar la eficiencia espectral permitirán, el estándar 802.11n ya hace uso de estas tecnologías para conseguir capacidades superiores a los 108 Mbps en el enlace inalámbrico.

La utilización de varios canales radio simultáneamente también puede ser contemplado en las WMNs. Además, tal y como se muestra en la Figura 1, no tiene porqué existir una única tecnología radio para la misma red mallada, en función de la capacidad y cobertura deseada, la capa radio puede estar basada en UWB (*Ultra Wide Band*) u OFDM (*Orthogonal Frequency División Multiplex*). En un futuro, es de esperar que los distintos clientes dispongan de varias interfaces de red, empleando en cada momento la más adecuada según las necesidades del usuario. (Riera, 2006)

### **3.5.2 MAC (*Medium Acces Control*)**

El acceso al medio en las WMNs debe proporcionar mecanismos que solventen las limitaciones de los estándares actuales, como el IEEE 802.11 que se basa en CSMA/CA, con serias limitaciones en las redes multsalto debido a los problemas del nodo oculto y del nodo expuesto. Mecanismos deterministas de acceso al medio, basados en TDMA (*Time División Multiple Access*) pueden ser bastante útiles si existe una buena sincronización, mientras que la opción de emplear CDMA (*Code División Multiple Access*) puede disminuir los efectos de las interferencias, ya que dos nodos pueden ocupar simultáneamente el canal empleando códigos distintos. Por ejemplo, el modo mesh de funcionamiento del estándar IEEE 802.16 (WiMAX) emplea un mecanismo TDMA.

Hay que recordar que los equipos basados en la familia de estándares IEEE 802.11 presentan un bajo coste y una gran aceptación en el mercado, por lo que son la solución más atractiva para implementar redes multi-salto. Debido a esta razón, existen multitud de propuestas de nuevos protocolos MAC para las redes 802.11 basados en distintos objetivos de diseño y, además, el IEEE se encuentra trabajando en el estándar 802.11s, el cual incluirá en su capa MAC mecanismos para el encaminamiento a nivel 2 y un acceso al medio más eficiente.

Pero la capa MAC no solo se centra en el acceso al medio, la utilización de varios canales simultáneamente también puede ser contratada por la capa MAC o por alguna capa de enlace superior, tal y como muestran las propuestas de MMAC (*Multichannel MAC*) y HMCP (*Hybrid Multichannel Protocol*), ya que está demostrado que la utilización de varios canales simultáneos correctamente coordinados pueden mejorar la capacidad la red, En la primera, se emplean varios canales empleando una sola interfaz radio, por lo que se requiere señalización y coordinación para que todos los nodos escuchen el canal adecuado en cada momento, Por otra parte, en HMCP los nodos tienen varias interfaces, algunas que trabajan en canales fijos y otras variables, empleando los canales fijos para control y señalización. (Riera, 2006)

### 3.5.3 Nivel de Red

A nivel de red, los protocolos de encaminamiento deberán proporcionar distintos mecanismos para el descubrimiento de caídas de enlaces, balanceo de cargas proporcionando QoS y, además, en función del tipo de WMN que se desee implementar, los parámetros de diseño de los protocolos diferirán (movilidad, nivel de baterías). En resumen, muchas de las propiedades de auto-configuración y auto-reparación (de rutas) de las WMN son, en parte, proporcionadas por los distintos protocolos de encaminamiento. Debido a su flexibilidad y operación en redes sin infraestructura, el punto de partida en este punto son los protocolos de encaminamiento desarrollados por el grupo de trabajo MANET (Mobile Ad-Hoc Networks) del IETF, que tiene dos tipos de protocolos: reactivos y proactivos; con las propuestas de AODV (*Ad-Hoc On-demand Distance Vector*) y OLSR (*Optimized Link State Routing*), representando a cada tipo. De todos modos, si los *routers* mesh no tienen movilidad y sus rutas no varían tan dinámicamente, pueden emplearse otro tipo de protocolos, como el OSPF (*Open Shortest Path First*) con la extensión de movilidad que permitirá la autoconfiguración de la red en caso de caída de algún enlace. (Riera, 2006)

### 3.5.4 Métricas de los enlaces

La primera métrica que se ha utilizado en las redes Mesh, es el conteo de saltos (*Hop counting*), ampliamente utilizada en la internet cableada, no es la más adecuada en las redes inalámbricas debido a la amplia desigualdad en las prestaciones de los saltos inalámbricos. Un "salto" se define como el trayecto entre dos enrutadores adyacentes. En una red inalámbrica, las pérdidas de paquetes en un tramo entre dos enrutadores pueden ser muy elevadas y es en general muy variable, dependiendo del presupuesto de potencia de enlace. En un enlace muy largo las pérdida tienden a ser mayores por lo que a menudo un trayecto con varios radioenlaces cortos puede presentar menos pérdida que un trayecto con un solo enlace largo.

Una métrica que se presta mejor a las características de las redes Mesh es la conocida como EXT (*Expected Transmisión Count*), basada en el conteo de los errores de transmisión esperados en el tramo. Esta técnica desarrollada en MIT, ha sido aplicada a diferentes protocolos de enrutamiento en redes malladas esto permite tomar en cuenta las características de transmisión de cada enlace que se expresan con un peso o ponderado que se le asigna.

Un enlace con mayores pérdida tendrá un ponderación mayor que se va utilizar para evaluar la métrica de la trayectoria total sin embargo no toma en cuenta la posibilidad de que diferentes enlaces pueden tener anchos de banda distintos por lo que el tiempo de transmisión de un paquete será menos en el enlace con mayor ancho de banda. Esto ha motivado la propuesta de otra métrica conocida como ETT (*Expected Transmisión Time*) en la que se multiplica EXT por el tiempo tardado en correr respectivo tramo. Esto puede detener impacto significativo cuando los tramos considerados en ancho de banda, o cuando se tengan tramos que utilizan 802.11b mezclados con tramos que utilizan 802.11 a o g.

El “*fish eye routing*” es una técnica que consiste en construir un mapa de la red de resolución variable que disminuye a partir del nodo de interés en función del número de saltos. Esto se hace disminuyendo a la tasa a la cual se propaga los mensajes de enrutamiento a medida que nos alejamos del nodo origen, permitiendo así disminuir la sobrecarga de la red por los mensajes de enrutamiento. (Bravo, 2008)

### 3.5.5 Nivel de Transporte

El protocolo TCP (*Transport Control Protocol*) es la base de la mayoría de aplicaciones existentes hoy en día en las redes de datos basadas en IP. Sin embargo, su eficiencia en las redes inalámbricas se ve seriamente afectada debido a que TCP supone que las pérdidas siempre se producen por congestión en los nodos y que su correcto funcionamiento supone un RTT no muy variable (típico de redes cableadas). Estos factores no se dan en las redes inalámbricas y, mucho menos en las redes malladas donde los paquetes pueden atravesar múltiples enlaces antes de llegar a su destino. Por lo tanto, para optimizar el transporte en las redes WMN es necesario o bien modificar TCP para distinguir entre los motivos de las pérdidas o retardos (retransmisiones, etc.), o proponer totalmente nuevos protocolos de transporte [4]. A pesar de que la segunda opción sea más óptima y permita aplicar protocolos con mayor rendimiento en WMNs, la gran aceptación y asentamiento de TCP hace que la mayoría de propuestas que puedan ser utilizadas en el mundo real sean variaciones de TCP. (Riera, 2006)

### 3.5.6 Calidad de Servicio (QoS) y seguridad

Uno de los principales retos en las WMN es que puedan ofrecer mecanismos para garantizar QoS como diversos mecanismos de seguridad. En el caso de la QoS, la utilización de las métricas adecuadas para diversos tipos de servicio, como el balanceo de cargas entre distintos Gateway (por ejemplo) puede mejorar el rendimiento y facilitar la implementación de los sistemas de control de admisión. Por otra parte, tal y como señalan los autores en, la seguridad es uno de los aspectos menos trabajados actualmente en las redes WMNs, sobre todo debido a la necesidad de autenticar a los nodos que participan en el encaminamiento de paquetes, ya que las propiedades de auto-configuración de las redes hacen difícil de detectar ciertos tipos de ataques, como la detección de nodos corruptos. (Tanenbaum, 2003)



Figura 76. Icono representativo de QoS  
<http://www.viared.com/web/peplink.htm>

### 3.6 Redes Inalámbricas en Malla

Las redes inalámbricas en malla (WMN estándar IEEE 802.11s) pueden ser conceptualizadas como un nuevo paradigma de la tecnología inalámbrica. Esta propuesta tecnológica es adaptable a numerosas aplicaciones y escenarios, entre los que destacan: la extensión de cobertura de redes cableadas, redes comunitarias, redes empresariales, sistemas de automatización, sistemas de transporte inteligente, sistemas de seguridad pública. Basadas en una arquitectura de red de bajo costo, auto administrada y confiable, las WMN han cobrado el interés tanto de más comerciales como de la comunidad científica, y esto se debe a la versatilidad que ofrecen para atender eficientemente distintas necesidades. (Carrillo, 2011)

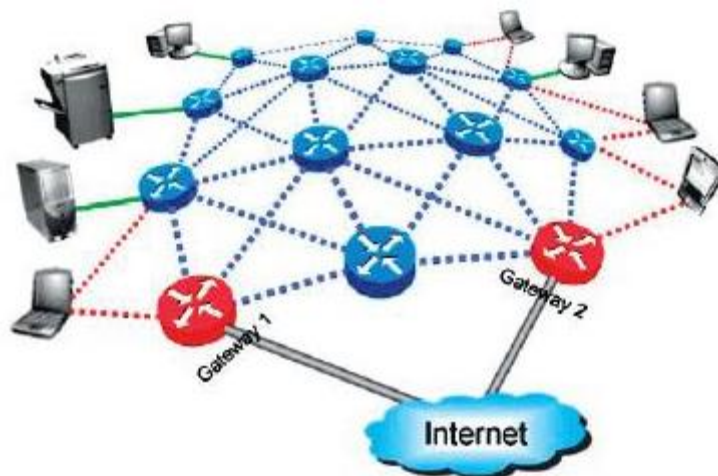


Figura 77. Topología de una red Mesh

<http://inalambricasredes.blogspot.mx/2013/03/redes-inalambricas.html>

#### 3.6.1 Introducción

A pesar de las grandes ventajas ofrecidas por las redes inalámbricas ad-hoc (e.g. ausencia de infraestructura, un despliegue sencillo de la red y movilidad), el éxito de estas se ha dado en sectores y aplicaciones muy particulares. Las aplicaciones de los sectores militares, de emergencias y de seguridad se adaptaron rápida y eficientemente en redes ad hoc y, por ende, dominaron las líneas de investigación para esta arquitectura de red.

No obstante el número creciente de usuarios de dispositivos inalámbricos, las redes ad hoc no han mostrado una aceptación generalizada por parte de los usuarios de tecnologías inalámbricas, y esto es debido principalmente al deseo generalizado de acceso a la información que reside en Internet. Por otro lado, las redes inalámbricas en modo infraestructura han mostrado una clara aceptación por parte de los usuarios de dispositivos móviles.

Esto se debe a que ofrecen acceso inalámbrico y conectividad hacia redes cableadas y particularmente hacia Internet. Sin embargo, tratar de extender la cobertura de esta arquitectura de red para ofrecer acceso, desde cualquier punto, hacia Internet, se ve limitado por los requerimientos de infraestructura. Planificación y tiempo de implementación. Las redes inalámbricas en malla han surgido como una alternativa original y novedosa para resolver las limitaciones de las arquitecturas de red mencionadas anteriormente.

Combinando algunas propiedades de las redes ad hoc y de las redes en modo infraestructura, las redes inalámbricas en malla ofrecen un conjunto de propiedades atractivas para diversos escenarios de aplicación, entre los que destaca la ampliación inalámbrica de la cobertura de redes cableadas. En este capítulo se describe la clasificación de las redes inalámbricas en malla y se detallan sus características principales.

### 3.6.2 Clasificación de las redes WMN

Las redes inalámbricas en malla son sistemas auto-organizados y auto-configurables, cuyos nodos establecen y mantienen conectividad entre ellos. Basándose en las funcionalidades y características de los nodos que componen la red, las WMN se han clasificado en tres categorías principales: redes inalámbricas de clientes en malla, redes inalámbricas en malla en modo infraestructura y redes inalámbricas en malla híbrida.

#### 3.6.2.1 Redes inalámbricas de clientes en malla

Las redes inalámbricas de clientes en malla (*Client Wireless Mesh Networks - CWMN*) son redes *peer-to-peer* entre dispositivos inalámbricos móviles. En esta arquitectura de red los dispositivos móviles son capaces de encaminar flujos de información sin necesidad de utilizar dispositivos de encaminamiento dedicados, de manera similar al comportamiento que existe en las redes ad hoc. Bajo este esquema, las funciones de configuración y de encaminamiento

Recaen en los dispositivos móviles que conforman la red, incrementando sustancialmente la complejidad de estos. La organización básica de estas redes. Las CWMN, un paquete de datos puede pasar por varios nodos de la red para llegar a un nodo destino (*red multihop*), de tal forma que la cooperación, entre los nodos de la red, es necesaria para intercambiar información entre un nodo fuente y un nodo destino lo suficientemente alejados como para comunicarse directamente entre ellos.

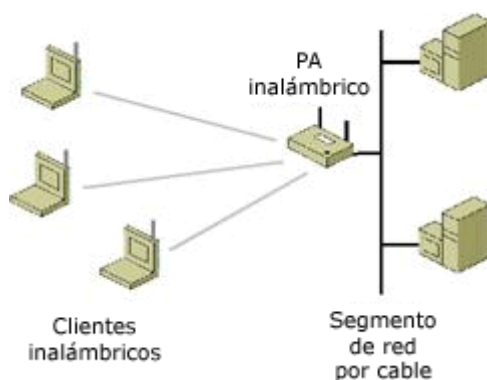


Figura 78. Red malla en modo cliente  
<http://conainfo04.blogspot.mx/2012/03/cliente-inalambrico.html>

### 3.6.2.2 Redes inalámbricas en malla en modo infraestructura/*Backbone*

Una de las subclases más importantes de las WMN son las redes inalámbricas en malla en modo infraestructura (*Infrastructure Wireless Mesh Networks* - iWMN). Esta novedosa propuesta tecnológica, ha surgido como una de las alternativas más viables para extender la cobertura de las redes cableadas.

A través de una arquitectura de red, que resultará ser eficiente, escalable, económica y fácil de implementar, las iWMN brindan acceso inalámbrico a usuarios móviles, así como las redes heterogéneas, y permite establecer conectividad entre estos elementos. El potencial de esta novedosa arquitectura le permite ser adaptada a diversos escenarios de aplicación, sin embargo, atender la creciente demanda de conectividad total es uno de los objetivos principales de esta tecnología. A diferencia de la arquitectura de red "plana" que existe en cWMN, las iWMN presentan una organización jerárquica de la red, al utilizar un conjunto de nodos dedicados a los que se les ha asignado un conjunto de funciones específicas.

Las iWMN se componen por dos elementos fundamentales: la troncal o *backbone* de la malla, y el conjunto de usuarios móviles. El *backbone* de una iWMN se compone por nodos inalámbricos estáticos y por ende se asume que estos no tienen restricciones de energía, de procesamiento o de almacenamiento.

Cada nodo que compone al *backbone* de la red, posee un rango de comunicaciones limitado, de tal forma que la cooperación entre estos nodos es la que permite establecer trayectorias de comunicación para nodos lo suficientemente distantes como para establecer comunicación directa entre ellos. De esta forma, cada nodo del *backbone* brinda sus recursos para encaminar información a través de la red y colabora en el establecimiento de rutas de comunicación (*red multihop*).

Es así como el *backbone* de la red ofrece un servicio de interconexión de bajo costo, contable y eficiente, que permite el establecimiento de comunicaciones entre usuarios móviles o bien entre usuarios móviles y otras arquitecturas de red, siendo el mejor ejemplo Internet.

Composición de las iWMN, la organización jerárquica de una iWMN se ilustra en la Figura Los nodos que componen esta arquitectura de red, así como sus funciones asociadas, se organizan de la siguiente manera:

MPP - Portal de la malla (Mesh Portal Point)

Los MPPs actúan como interfaces de enlace entre la iWMN y la red cableada. Estos dispositivos son los responsables del intercambio de paquetes entre ambas arquitecturas de red.

MAP - Punto de acceso a la malla (Mesh Access Point)

Los MAPs ofrecen conectividad inalámbrica a los usuarios de la red. Estos dispositivos reciben paquetes de datos provenientes de los usuarios móviles y son responsables de enviarlos a través del *backbone* para hacerlos llegar hasta su destino.

MP - Punto de la malla (Mesh Point)



Clasificación de WMN Los MPs solo realizan funciones de encaminamiento de información dentro del *backbone* de la red.

STA - Estación móvil (*Mobile Station*) Las STAs (usuarios) utilizan el *backbone* de la red para establecer comunicaciones. Es decir, el intercambio paquetes de datos entre STAs, o bien entre STAs y otras arquitecturas de red, ej. Internet.

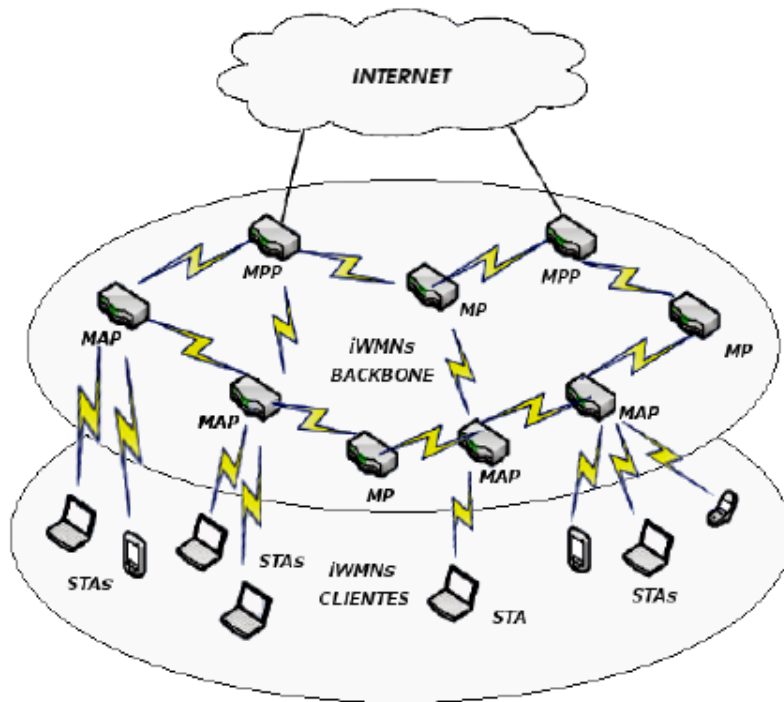


Figura 79. Nodos que componen la arquitectura Mesh  
[http://pcyti.izt.uam.mx/archivos/Tesis/Generacion2009/ICR\\_ErnestoCarrillo.pdf](http://pcyti.izt.uam.mx/archivos/Tesis/Generacion2009/ICR_ErnestoCarrillo.pdf)

### Características de las iWMN

La arquitectura de red de las iWMN puede ser considerada como una arquitectura híbrida, esta combina las características y propiedades de otras arquitecturas de red, tales como redes ad hoc y redes en modo infraestructura. Consecuentemente, las iWMN poseen un conjunto de características comunes a estas arquitecturas de red. A continuación se resumen las particularidades de esta arquitectura de red:

1. Cada uno de los nodos inalámbricos que conforman al *backbone* de la red posee un rango limitado de comunicaciones; por esta razón la cooperación de los diversos nodos de la red es necesaria para el establecimiento de caminos de comunicación. Esto induce un comportamiento multi-salto en el *backbone* de la red y asigna, a cada nodo que lo compone, las responsabilidades y funcionalidades de un dispositivo de encaminamiento.
2. El grado de movilidad de los nodos que conforman el *backbone* de la red se puede considerar nulo, mientras que para los clientes de la red se considera aleatorio e ilimitado. Esto impacta de manera directa en la topología de la red, induciendo cambios dinámicos en la misma.

3. Factores tales como la energía, el procesamiento y el almacenamiento, son comúnmente limitados para los clientes de la red; mientras que los nodos que conforman el *backbone* no tiene restricción alguna sobre estos parámetros.

4. La compatibilidad y operatividad con otras arquitecturas de red, es una característica requerida para las iWMN. Dado que deben soportar algunos hacia y desde otras arquitecturas de red, así como lujos de información P2P entre los usuarios de la red.

5. Dado que una de las principales aplicaciones de las iWMN es interconectar diferentes arquitecturas de red, la mayor parte del trabajo en la red pasar a través de los MPP. Es así que el trabajo tendrá una distribución sesgada en la red. Pues a medida que la distancia entre un nodo del *backbone* y el MPP disminuye, la cantidad de trabajo en este primer nodo aumentaría, generando constantemente cuellos de botella en las cercanías de los MPP.

### 3.6.2.3 Redes Inalámbricas en Malla híbrida

Las redes inalámbricas en malla híbridas (*Hybrid Wireless Mesh Network - hWMN*) combinan las propiedades tanto de las cWMN como de las iWMN; así los clientes pueden enviar paquetes de información a través del *backbone* o bien encaminar información entre ellos. La capacidad de encaminamiento de los clientes de la malla ofrece una conectividad mejorada así como una cobertura dinámica de la red.

La Figura, ilustra esta arquitectura de red. Si bien es una arquitectura de red mejorada, su implementación exige dispositivos móviles tecnológicamente más sofisticados y eficientes. (Carrillo, 2011)

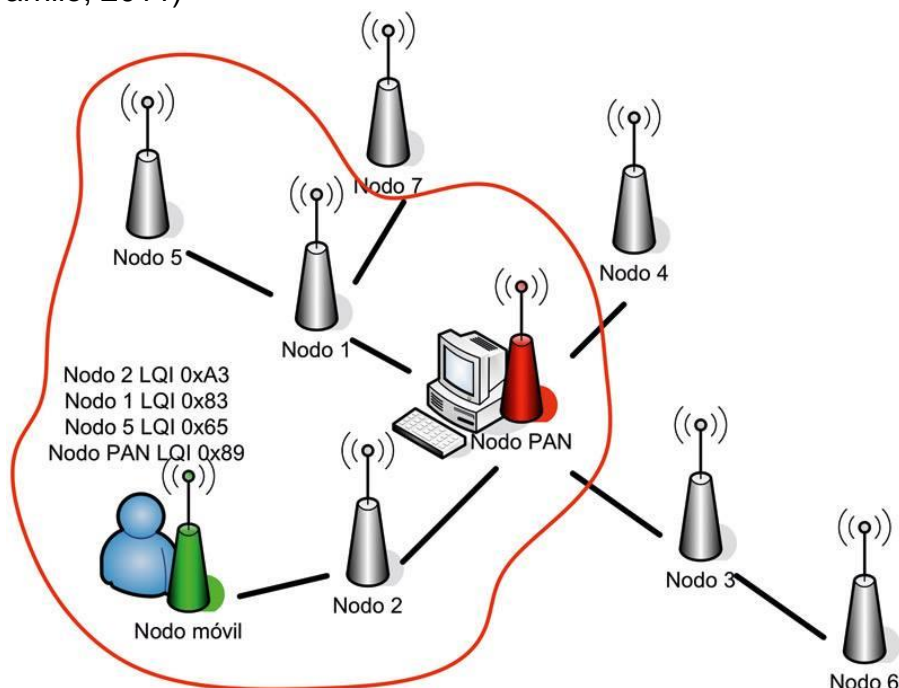


Figura 80. Arquitectura de red

<http://www.mapfre.com/fundacion/html/revistas/seguridad/n125/es/articulo1.html>

### 3.7 Algoritmos de Enrutamiento en Redes Inalámbricas

La función principal de la capa de red es enrutar paquetes de la máquina de origen a la de destino. En la mayoría de las subredes, los paquetes requerirán varios saltos para completar el viaje. La única excepción importante son las redes de difusión, pero aun aquí es importante el enrutamiento si el origen y el destino no están en la misma red. Los algoritmos que eligen las rutas y las estructuras de datos que usan constituyen un aspecto principal del diseño de la capa de red.

El algoritmo de enrutamiento es aquella parte del software de la capa de red encargada de decidir la línea de salida por la que se transmitirá un paquete de entrada. Si la subred usa datagramas de manera interna, esta decisión debe tomarse cada vez que llega un paquete de datos, dado que la mejor ruta podría haber cambiado desde la última vez. Si la subred usa circuitos virtuales internamente, las decisiones de enrutamiento se toman solo al establecerse un circuito virtual no es nuevo. En lo sucesivo los paquetes de datos simplemente siguen la ruta previamente establecida.

Este último caso a veces se llama enrutamiento de sesión, dado que una ruta pertenece vigente durante toda la sesión de usuario (por ejemplo, durante una sesión desde una terminal, o durante una transferencia de archivos).

Algunas veces es útil distinguir entre el enrutamiento, que es el proceso consistente en tomar la decisión de cuáles rutas utilizar, y el reenvío, que consiste en la acción que se toma cuando llega un paquete. Se puede considerar que un enrutador realiza dos procesos internos. Uno de ellos maneja cada paquete conforme llega, buscando en las tablas de enrutamiento la línea de salida por la cual se enviará. Este proceso se conoce como reenvío. El otro proceso es responsable de llenar y actualizar las tablas de enrutamiento. Es ahí donde entra en acción el algoritmo de enrutamiento.

Sin importar si las rutas para cada paquete se eligen de manera independiente o solo cuando se establecen nuevas conexiones, hay ciertas propiedades que todo algoritmo de enrutamiento debe poseer: exactitud, sencillez, robustez, estabilidad, equidad y optimización. La exactitud y la sencillez apenas requieren comentarios peor la necesidad de robustez puede ser menos obvia a primera vista. Una vez que una red principal entra en operación, cabría esperar que funcionara continuamente durante años sin fallas a nivel de sistema.

Durante ese periodo habrá fallas de hardware y software de todo tipo. Los hosts, enrutadores y líneas fallarán en forma repetida y la topología cambiará muchas veces. El algoritmo de enrutamiento debe ser capaz de manejar los cambios de topología y tráfico sin requerir el aborto de todas las actividades en todos los hosts y el reinicio de la red con cada caída de un enrutador. Los algoritmos de enrutamiento pueden agruparse en dos clases principales: no adaptativos y adaptativos.

Los algoritmos no adaptativos no basan sus decisiones de enrutamiento en mediciones o estimaciones del tráfico y la topología actuales. En cambio, la decisión de que ruta se usará para llegar se toma por adelantado, fuera de línea y se encarga en los enrutadores al arrancar la red. Este procedimiento se conoce como enrutamiento estático. En contraste, los algoritmos adaptativos cambian sus decisiones de enrutamiento para reflejar los cambios de topología y, por lo general también el tráfico.

### 3.7.1 Elementos de enrutamiento

Principales elementos de enrutamiento:

- Descubrimiento de nodo: Encontrar nodos mientras aparecen o desaparecen
- Descubrimiento de frontera: Encontrar los límites o bordes de una red
- Mediciones de enlace: medir la calidad de los enlaces entre nodos
- Calculo de rutas: Encontrar la mejor ruta basada en la calidad de los enlaces
- Manejo de direcciones IP: Asignar y controlar direcciones Ipm
- Manejo de *Up link/backhaul*: Manejo de conexiones de redes externas, enlaces a internet.

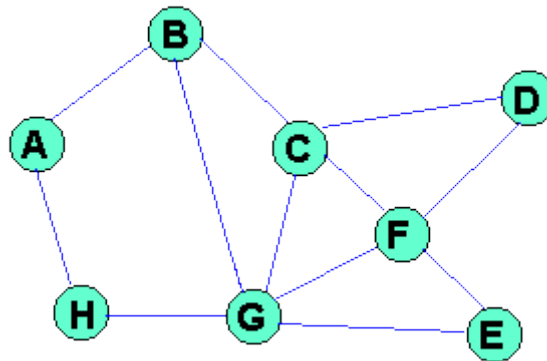


Figura 81. Descubrimiento de rutas

<http://www.profesores.frc.utn.edu.ar/sistemas/inqsanchez/Redes/Archivos/enrutam.asp>

### 3.7.2 Descripción de algoritmos de enrutamiento

Una red *multihop* es un sistema de comunicaciones conformado por múltiples nodos capaces de encaminar información. En este tipo de redes, cada paquete puede ser encaminado por diversos nodos para transitar desde un nodo fuente hasta un nodo destino. Uno de los factores clave para el desempeño de una red *multihop*, es el protocolo de encaminamiento usado en esta. El objetivo de un protocolo de encaminamiento es hallar una ruta óptima de comunicaciones para intercambiar información entre un nodo fuente y un nodo destino. Los protocolos cuyo objetivo es encontrar la distancia más corta entre fuente y destino han sido ampliamente utilizados en redes multi-salto. Las funciones elementales que realiza un protocolo de encaminamiento consisten en: el descubrimiento de rutas de encaminamiento, selección de la ruta óptima y el mantenimiento de esta.

Para descubrir el conjunto de posibles rutas de encaminamiento, el protocolo de encaminamiento utiliza mecanismos de recolección de información que le permiten determinar los puntos intermedios por donde podrá viajar la información desde un nodo fuente hasta su destino. El proceso de selección de una ruta óptima puede ser visto como un problema de optimización, en el cual las métricas de encaminamiento son parámetros de desempeño. Que el protocolo de encaminamiento deberá optimizar a través de la selección de una ruta de comunicaciones. Estas pueden ir desde la minimización del retardo y de las pérdidas, o bien la maximización del caudal de datos (*throughput*), entre otras. Finalmente, el proceso de mantenimiento de la ruta seleccionada, monitorea el estado de la trayectoria de comunicaciones y reacciona de manera oportuna ante una eventual dificultad en la misma.

La forma en la que cada protocolo de encaminamiento resuelve el problema del encaminamiento difiere en virtud del algoritmo que cada protocolo ejecute, por ejemplo un protocolo de encaminamiento puede utilizar un mecanismo de recolección de información reactivo en conjunto con la métrica de minimización del retardo y un esquema proactivo de monitoreo de conectividad en los enlaces de la ruta seleccionada. Gran parte de los protocolos de encaminamiento han sido diseñados con base en dos clases importantes de algoritmos: estado del enlace y vector-distancia. (Carrillo, 2011)

### 3.7.3 Enrutamiento por la ruta más corta

Comencemos nuestro estudio de los algoritmos de enrutamiento con una ética de amplio uso en muchas formas, porque es sencilla y fácil de entender. La idea es armar un grafo de la sub red, en que cada nodo representa un enrutador y cada arco del grafo una línea de comunicación (con frecuencia llamada enlace). Para elegir una ruta entre un par dado de enrutadores, el algoritmo simplemente encuentra en el grafo la ruta más corta entre ellos.

El concepto de ruta más corta merece una explicación. Una manera de medir la longitud de una ruta es por la cantidad de saltos. Usando esta métrica, las rutas ABC y ABE de la figura. Tiene la misma longitud. Otra métrica es la distancia geográfica en km, en cuyo caso ABC es claramente mucho mayor que ABE (suponiendo que la figura esta dibujada a escala).

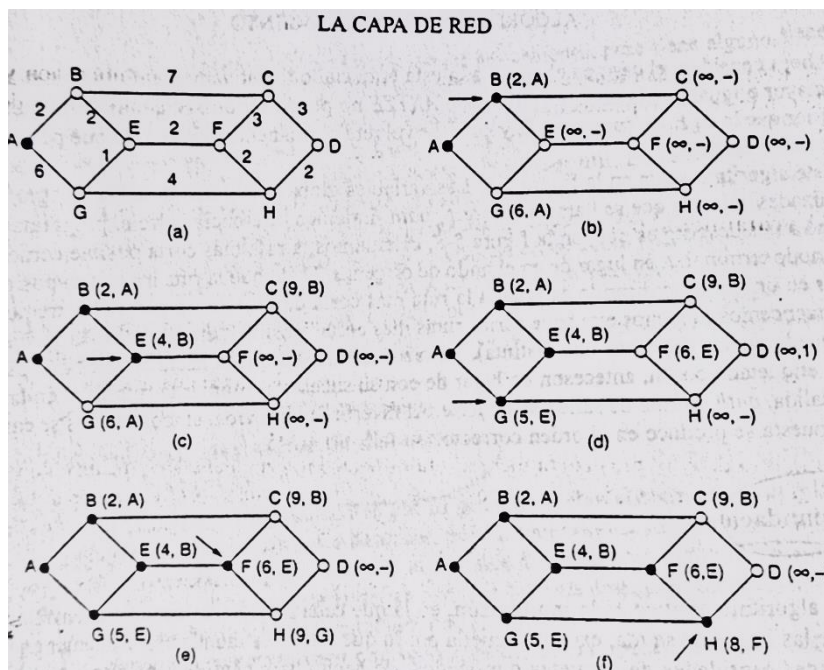


Figura 82. Ejemplos de métricas  
<http://es.slideshare.net/Osita/capa-de-red-presentation>

### 3.7.4 Inundación

Otro algoritmo estático es la inundación, en la que cada paquete de entrada se envía por cada una de las líneas de salida, excepto por aquella por la que llegó. La inundación evidentemente genera grandes cantidades de paquetes duplicados; de hecho, una cantidad infinita a menos que se tome algunas medidas para limitar el proceso. Una de estas medidas es integrar un contador de saltos en el encabezado de cada paquete, que disminuya con cada salto, y el paquete se descarte cuando el contador llegue a cero. Lo ideal es inicializar el contador de saltos a la longitud de la ruta entre el origen y el destino. Si el emisor desconoce el tamaño de la ruta, puede inicializar el contador al peor caso, es decir, el diámetro total de la subred.

Una técnica alterna para ponerle diques a la inundación es llevar un registro de los paquetes difundidos, para evitar enviarlos una segunda vez. Una manera de lograr este propósito es hacer que el enrutador de origen ponga un número de secuencia en cada paquete que recibe de sus hosts. Cada enrutador necesita una lista por cada enrutador de origen que indique los números de secuencia originados en ese enrutador que haya visto. Si un paquete de entrada está en la lista no se difunde.

Para evitar que la lista crezca sin límites, cada lista debe incluir un contador,  $K$ , que indique que todos los números de secuencia hasta que  $K$  ya han sido vistos. Cuando llega un paquete, es fácil comprobar si es duplicado; De ser así, se descarta. Es más, no se necesita la lista completa por debajo de  $K$ , pues  $K$  la resume efectivamente.

Una variación de la inundación un poco más práctica es la inundación selectiva. En este algoritmo los enrutadores no envían cada paquete de entrada por todas las líneas si no solo por aquellas que van aproximadamente en la dirección correcta. Por lo general no tiene mucho caso enviar un paquete dirigido al oeste a través de un alineamiento dirigida al este, a menos que la topología sea extremadamente peculiar y que el enrutador este seguro de este hecho.

La inundación no es práctica en la mayoría de las aplicaciones pero tiene algunos usos por ejemplo en aplicaciones militares donde grandes cantidades pueden volar en pedazos en cualquier momento es altamente deseable la excelente robustez de la inundación. Las aplicaciones distribuidas de base de datos a veces es necesario actualizar concurrentemente todas las bases de datos en cuyo caso la inundación puede ser útil. En las redes inalámbricas algunas estaciones que se encuentran del alcance de radio de una estación dada puede recibir los mensajes que esta transmite lo cual es de hecho inundación y algunos algoritmos utilizan esta propiedad. Un cuarto posible de la inundación es como métrica contra la que pueden compararse otros algoritmos de enrutamiento la inundación siempre escoge la ruta más corta posible porque escoge en paralelo todas las rutas posibles. En consecuencia, ningún otro algoritmo puede producir un retardo más corto (si ignoramos la sobrecarga generada por el proceso de inundación mismo).

### 3.7.5 Algoritmo Vector-Distancia

Las redes modernas de computadoras por lo general utilizan algoritmos de enrutamiento dinámico en lugar de los estáticos antes descritos, pues los algoritmos estáticos no toman en cuenta la carga actual de la red. En particular, dos algoritmos dinámicos, el enrutamiento por vector de distancia y el enrutamiento por estado de enlace, son los más comunes. En esta sección veremos el primer algoritmo. En la siguiente estudiaremos el segundo.

Los algoritmos de enrutamiento por vector de distancia operan haciendo de cada enrutador mantenga un atabla (es decir, un vector) que da la mejor distancia conocida a cada destino y la línea que se puede usar para llegar hay. Estas tablas se actualizan intercambiando información de los vecinos.

El algoritmo de enrutamiento por vector de distancia a veces recibe otros nombres, incluido el de algoritmo de enrutamiento *Bellman-Ford* distribuido y el de algoritmo *Ford-Fulkerson*, por los investigadores que lo desarrollaron (*Bellman*, 1957, y *Ford y Fulkerson*, 1962). Este fue el algoritmo original de enrutamiento de *ARPANET* y también se usó en internet con el nombre RIP.

En el enrutamiento por vector de distancia, cada enrutador mantiene una tabla de enrutamiento indexada por, y conteniendo un registro de, cada enrutador de la sub red. Esta entrada comprende dos partes: la línea preferida de salida hacia ese destino y una estimación del tiempo o distancia a ese destino. La métrica usada podría ser la cantidad de saltos, el retardo de tiempo en milisegundos, el número total de paquetes encolados a lo largo de la ruta, o algo parecido.

Se supone que el enrutador conoce la "distancia" a cada uno de sus vecinos. Si la métrica es de saltos, la distancia simplemente es un salto. Si la métrica es la longitud de la cola, el enrutador simplemente examina cada cola. Si la métrica es el retardo, el enrutador puede medirlo en forma directa con paquetes especiales de ECO que el receptor simplemente marca con la hora y lo regresa tan rápido como puede.

Por ejemplo, suponga que el retardo se usa como métrica y que el enrutador conoce el retardo a cada uno de sus vecinos. Una vez cada  $T$  mseg, cada enrutador envía a todos sus vecinos una lista de sus retardos estimados a cada destino. También recibe una lista parecida de cada vecino. Imagine que una de estas tablas acaba de llegar del vecino  $X$ , siendo  $X_i$  la estimación de  $X$  respecto al tiempo que le tome llegar al enrutador  $i$ . Si el enrutador sabe que el retardo a  $X$  es de  $m$  mseg, también sabe que puede llegar al enrutador  $i$  a través de  $X$  en  $X_i + m$  mseg. Efectuando este cálculo para cada vecino un enrutador puede encontrar la estimación que parezca ser la mejor y usar esa estimación así como la línea correspondiente, en su nueva tabla de enrutamiento. Observe que la vieja tabla de enrutamiento no se usa en este cálculo.

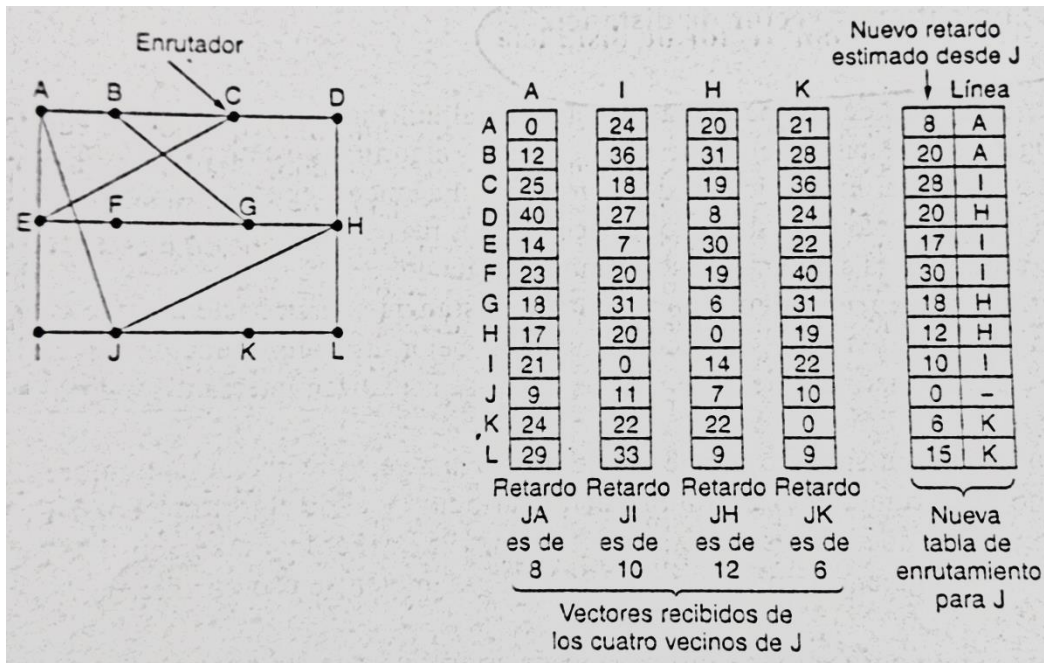


Tabla 7. Tabla de enrutamiento

<https://books.google.com.mx/books?isbn=9702601622>

- El problema de la cuenta hasta infinito

El enrutamiento por vector de distancia funciona en teoría, pero tiene un problema serio en la práctica: aunque llega a la respuesta correcta, podría hacerlo lentamente. En particular, reacción con rapidez a las buenas noticias, peor con lentitud ante las malas. Considere un enrutador cuya mejor ruta al destino X es larga. Si el siguiente intercambio el vecino A informa repentinamente un retardo corto a X, el enrutador simplemente se conmuta a modo de usar la línea de A para enviar tráfico hasta X. En un intercambio de vectores se procesan las buenas noticias.

Para ver la rapidez de propagación de las buenas noticias, considere la subred de cinco nodos (lineal) de la siguiente figura, en donde la métrica de retardo es el número de salto. Suponga que A está desactivado inicialmente y que los otros enrutadores lo saben. En otras palabras, habrán registrado como infinito el retardo de A.

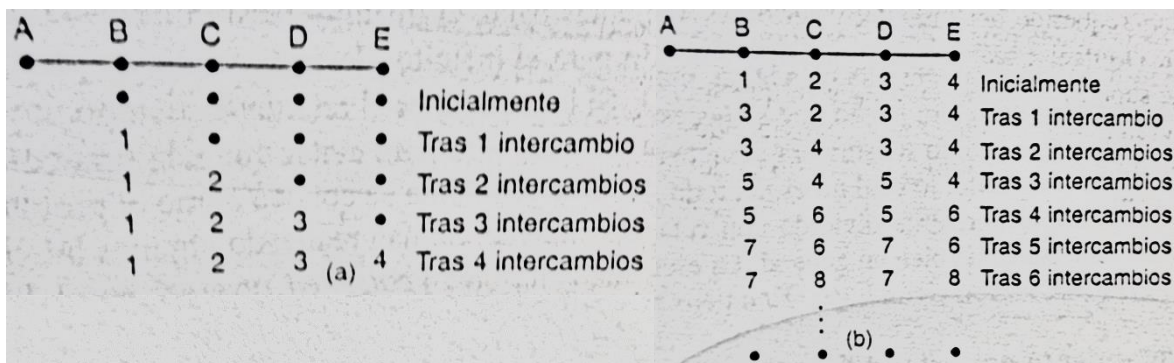


Figura 83. Teoría de la cuenta hasta el infinito

<https://books.google.com.mx/books?isbn=9702601622>



### 3.7.6 Enrutamiento por estado de alcance

El enrutamiento por vector distancia se usó en ARPANET hasta 1979 cuando fue reemplazado por el enrutamiento por estado del enlace. Dos problemas principales causaron su desaparición. Primero debido a que la métrica de retardo era la longitud de la cola no tomaba en cuenta el ancho de banda al escoger rutas. Inicialmente todas las líneas eran de 56Kbps, por lo que el ancho de banda no era importante pero una vez que se modernizaron algunas líneas a 230kbps y otras a 1.544 Mbps, el no tomar en cuenta el ancho de banda se volvía un problema importante por supuesto habría sido posible cambiar la métrica de retardo para considerar el ancho de banda pero también existía un segundo problema que el algoritmo con frecuencia tardaba demasiado en converger (el problema de la cuenta hasta el infinito). Por esta razón si el algoritmo fue reemplazado por uno completamente nuevo llamado enrutamiento por estado del enlace. Hoy en día se usan bastante algunas variantes del enrutamiento por estado del enlace. EL concepto en que se basa por estado del enlace es sencillo y puede ensuciarse en cinco partes. Cada enrutador debe:

- Descubrir a sus vecinos y conocer sus direcciones de red.
- Medir el retardo o costo para cada uno de sus vecinos.
- Construir un paquete que indique todo lo que acaba de aprender.
- Enviar este paquete a todos los demás enrutadores.
- Calcular la ruta más corta a todos los demás enrutadores.

De hecho, toda topología y todos los retardos se miden experimentalmente y se distribuyen a cada enrutador entonces puede usarse el algoritmo de Dijkstra para encontrar la ruta más corta a los demás enrutadores. A continuación veremos con mayor detalle estos cinco pasos.

- Conocimiento de los vecinos

Cuando un enrutador se pone en funcionamiento su primera tarea es averiguar quiénes son sus vecinos esto lo realiza enviando un paquete de HELLO especial a cada línea punto a punto se espera que el enrutador del otro extremo regrese una respuesta indicando quien es. Estos nombres deben ser globalmente únicos puesto que un enrutador distante escucha después de que tres enrutadores están conectados a F, es indispensable que pueda determinar si los tres se refieren al mismo F.

Cuando se conectan dos o más enrutadores mediante una LAN la situación es ligeramente más complicada en las siguientes figuras se ilustra una LAN a la que están conectados directamente tres enrutadores, A, C y F. Cada uno de estos enrutadores está conectados a uno o más enrutadores adicionales.

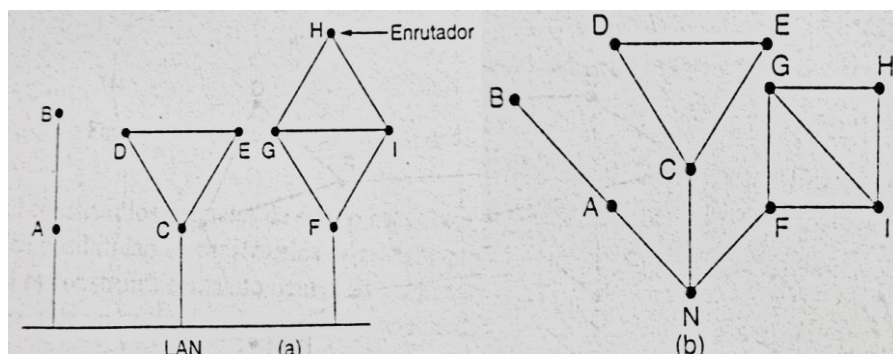


Figura 84. Conocimiento de los vecinos

- Medición del costo de línea

El algoritmo de enrutamiento por estado del enlace requiere que cada enrutador sepa, o cuando menos tenga una idea razonable, del retardo a cada uno de sus vecinos. La manera más directa de determinar este retardo es enviar un paquete ECHO especial a través de la línea y una vez que llega al otro extremo, este debe regresarlo inmediatamente. Si se mide el tiempo de ida y vuelta y se divide entre dos, el enrutador emisor puede tener una idea razonable del retardo. Para obtener mejores resultados la prueba puede llevarse a cabo varias veces y usarse el promedio. Por supuesto que este método asume de manera implícita que los retardos son isométricos, lo cual no siempre es el caso.

Un aspecto interesante es si se debe tomar en cuenta la carga al medir el retardo. Para considerar la carga, el temporizador debe iniciarse cuando el paquete ECHO se ponga en la cola. Para ignorar la carga, el temporizador debe iniciarse cuando el paquete ECHO alcance el frente de la cola.

Pueden citarse argumentos a favor de ambos métodos. La inclusión de retardo inducido por el tráfico en las mediciones implica que cuando un enrutador puede escoger entre dos líneas con el mismo ancho de banda, una con carga lata continúa y otra sin ella, considera como ruta más corta la de la línea sin carga. Esta selección resultara en un mejor desempeño.

Desgraciadamente, también hay un argumento en contra de la inclusión de la carga en el cálculo del retardo. Considere la subred de la siguiente figura, dividida en dos partes, este y oeste, conectados por dos líneas, CF y EI.

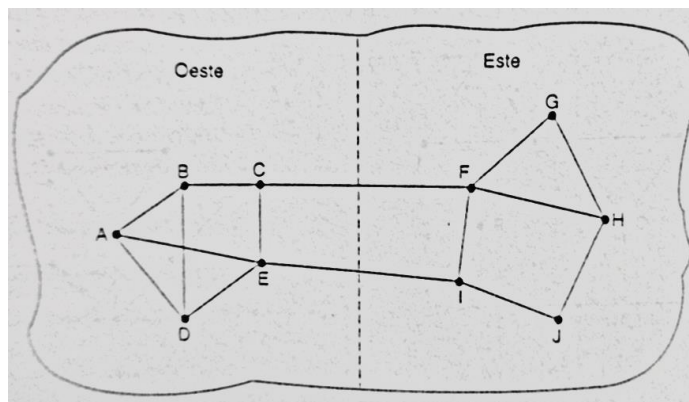


Figura 85. Ejemplo de medición

<https://books.google.com.mx/books?isbn=9702601622>

- Construcción de los paquetes de estado del enlace

Una vez que se ha recabado la información necesaria para el intercambio, el siguiente paso es que cada enrutador construya un paquete que contenga todos los datos. El paquete comienza con la identidad del emisor, seguida de un número de secuencias, una edad (que se describirá después) y una lista de vecinos. Se da el retardo de vecinos en la siguiente figura se da un ejemplo de subred, y los retardos se muestran como etiquetas en las líneas. En la siguiente figura se muestran los paquetes de estado del enlace de los seis enrutadores.

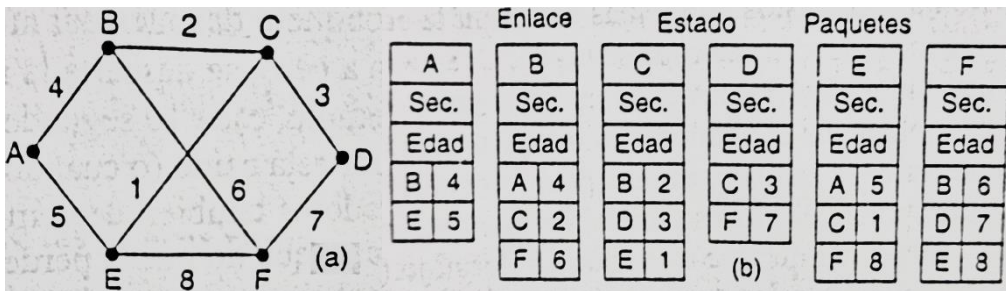


Figura 86. Construcción de la tabla de paquetes  
<https://books.google.com.mx/books?isbn=9702601622>

- Distribución de los paquetes de estado del enlace

La parte más complicada del algoritmo es la distribución confiable de los paquetes de estado del enlace. A medida que se distribuye e instalan los paquetes, los enrutadores que reciban los primeros cambiarán sus rutas. En consecuencia, los distintos enrutadores podrían estar usando versiones diferentes de la topología, lo que puede conducir a inconsistencias, ciclos maquinas inalcanzables y otros problemas.

Primero describiremos el algoritmo básico de distribución y luego lo refinaremos. La idea fundamental es utiliza inundación para distribuir los paquetes de estado del enlace. A fin de mantener controlada la inundación, cada paquete contiene un número de secuencia que se incrementa con cada paquete nuevo enviado. Los enrutadores llevan el registro de todos los pares (enrutador de origen, secuencia) que ven. Cuando llega un paquete de estado del enlace, se verifica contra la lista de paquetes ya vistos. Si es nuevo, se reenvía a través de todas las líneas excepto aquella por la que llego. Si es un duplicado, se descarta. Si llega un paquete con número de secuencia menor que el mayor visto hasta el momento, se rechaza como obsoleto debido que el enrutador tiene datos más recientes.

Origen	Sec.	Edad	Banderas de envío			Banderas de ACK			Datos
			A	C	F	A	C	F	
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

Tabla 8. Distribución de paquetes  
<https://books.google.com.mx/books?isbn=9702601622>

- Calculo de las nuevas rutas

Una vez que un enrutador ha acumulado un grupo completo de paquetes de estado del enlace, puede construir el grafo de la subred completa porque todos los enlaces están representados de hecho, cada enlace se representa dos veces una para cada dirección. Los dos valores pueden promediarse o usarse por separado.

Ahora puede ejecutar localmente el algoritmo de Dijkstra para construir la ruta más corta a todos los destinos posibles. Los resultados de este algoritmo pueden instalarse en las tablas de enrutamiento, y la operación normal puede reiniciarse.

Para una subred con  $n$  enrutadores, cada uno de los cuales tiene  $k$  vecinos, la memoria requerida para almacenar los datos de entrada es proporcional a  $kn$ . En las subredes grandes este puede ser un problema también puede serlo el tiempo de cómputo sin embargo, en muchas situaciones prácticas el enrutamiento por estado del enlace funciona bien.

Sin embargo, problemas con el hardware o el software pueden causar estragos con este algoritmo (lo mismo que con otros). Por ejemplo, si un enrutador afirma tener un enlace que no tiene, u olvida una línea que si tiene, el grafo de la subred será incorrecto. Si un enrutador deja de reenviar paquetes, o los corrompe al hacerlo, surgirán problemas.

### 3.7.7 Enrutamiento jerárquico

A medida que crece el tamaño de las redes, también lo hacen, de manera proporcional las tablas de enrutamiento del enrutador. Las tablas que siempre crecen no solo consumen memoria del enrutador sino que también se necesita más tiempo de CPU para examinarlas y más ancho de banda para enviar informes de estado entre enrutadores. En cierto momento la red puede crecer hasta el punto en que ya no es factible que cada enrutador tenga una entrada para cada uno de los demás enrutadores, por lo que el enrutamiento tendrá que hacerse de manera jerárquica, como ocurre en la red telefónica.

Cuando se utiliza el enrutamiento jerárquico los enrutadores se dividen en lo que llamaremos regiones, donde cada enrutador conoce todos los detalles para enrutar paquetes a destinos dentro de su propia región, pero no se sabe nada de la estructura interna de las otras regiones. Cuando se interconectan diferentes redes, es natural considerar cada una como región independiente a fin de liberar a los enrutadores de una red de la necesidad de conocer la estructura topológica de las demás. En las redes enormes, una jerarquía de dos niveles puede ser insuficiente, tal vez sea necesario agrupar las regiones en clústeres, los clústeres en zonas, las zonas en grupos, etc., hasta que se nos agoten los nombres para clasificarlos como ejemplo de jerarquía multinivel considere una posible forma de enrutar un paquete de California, a *Malindi, Kenya*. El enrutador de California conocería la topología detallada de Malindi pero podrá enviar todo el tráfico al exterior al enrutador de Los Ángeles.

### 3.7.8 Enrutamiento en redes WMN

El enrutamiento en iWMN es una operación compleja, que debe contemplar las características de la red para cumplir con los requerimientos de desempeño de las aplicaciones que residirán en ella. Tanto las métricas de encaminamiento así como la estrategia de encaminamiento, tienen una enorme influencia en el desempeño de los protocolos y de la red misma.

La principal aplicación de las iWMN es ofrecer acceso inalámbrico a usuarios móviles y colaborar en el establecimiento de trayectorias de comunicación con otras arquitecturas de red, y en este proceso los parámetros de optimización que un protocolo de encaminamiento debe atender son: mantener la conectividad de extremo a extremo, minimizar el retardo, optimizar el balance de la carga en la red, aumentar la confiabilidad y escalabilidad de la red, manejar eficazmente el ancho de banda y maximizar el caudal de datos (*throughput*). Para que un protocolo de encaminamiento cumpla con los requisitos planteados, debería ser, encaminamiento en redes inalámbricas capaz de enfrentar un conjunto de dificultades inherentes a la red y aprovechar al máximo las ventajas que ofrece la misma. Las iWMN heredan funcionalidades y comportamientos propios de las redes cableadas así como de las redes inalámbricas ad hoc. Esta naturaleza híbrida hace que las dificultades que enfrenta un protocolo de encaminamiento se compongan de una mezcla de problemas heredados de ambas arquitecturas.

### 3.7.9 Enrutamiento en redes Ad-Hoc

Ya vimos como relajar el enrutamiento cuando los hosts son móviles y los enrutadores son fijos. Un caos aún más extremo es uno en el que los enrutadores mismos son móviles. Entre las posibilidades se encuentran:

- Vehículos militares en un campo de batalla sin infraestructura.
- Una flota de barcos en el mar.
- Trabajadores de emergencia en un área donde un temblor destruyó la infraestructura.
- Una reunión de personas con computadoras portátiles en un área que no cuenta con 802.11.

En todos estos casos, y en otros, cada nodo consiste en un enrutador y un host, por lo general en la misma computadora las redes de nodos que están cercas entre si conocen como redes ad-hoc o *MANETs* (redes ad-hoc móviles). A continuación las examinaremos con brevedad.

Lo que distingue a las redes ad-hoc de las redes cableadas es que en las primeras se eliminaron todas las reglas comunes a cerca de las topologías fijas, los vecinos fijos y conocidos, la relación fija entre direcciones IP y la ubicación, etc. Los enrutadores pueden ir y venir o aparecer en nuevos lugares en cualquier momento. En una red cableada, si un enrutador tiene una ruta valida a algún destino, esa ruta continúa siendo válida de manera indefinida (excepto si ocurre alguna falla en algún aparte del sistema que afecte a esa ruta). En una red ad-hoc, la topología podría cambiar todo el tiempo, por lo que la necesidad o la valides de las rutas puede cambiar en cualquier momento sin previo aviso. No es necesario decir que están circunstancias hacen del

enrutamiento en redes ad-hoc algo diferente del enrutamiento en sus contrapartes fijas se ha propuesto una variedad de algoritmos de enrutamiento para las red ad-hoc. U no de los más interesantes es el algoritmo de enrutamiento AODV (vector de distancia ad-hoc bajo demanda). Es pariente lejano del algoritmo de vector de distancia *Bellman Ford* pero está adaptado para funcionar en entornos móviles y toma en cuenta le ancho de banda limitado y la duración corta de la batería de esos entornos otra característica inusual es que es un algoritmo bajo demanda, es decir, determina una ruta a algún destino solo cuando alguien desea enviar un paquete a ese destino.

- Descubrimiento de ruta

En cualquier instante dado, una red ad-hoc puede describirse mediante un grafo de los nodos (*enrutadores+hosts*). Dos nodos se conectan (es decir, tienen un arco entre ellos en el grafo) si se pueden comunicar de manera directa mediante sus radios. Debido a que unos de los dos podrían tener un emisor más poderoso que le otro es posible que A este conectado B, pero B no está conectado a A. Sin embargo, por simplicidad, asumiremos que todas las conexiones son simétricas. También debe hacerse notar que el simple hecho de que dos nodos estén dentro del alcance de radio entre si no significa que estén conectados. Puede haber edificios, colina su otros obstáculos que bloqueen su comunicación.

- Mantenimiento de rutas

Debido a que es posible mover o apagar los nodos, la topología puede cambiar de manera espontánea. Por ejemplo la siguiente figura si G se apaga A no se dará cuenta de que la ruta a I (AD-GI) que estaba utilizando ya no es válida. El algoritmo necesita ser capaz de manejar esto. Cada nodo difunde de manera periódica un mensaje de saludo (hello). Se espera que cada uno de sus vecinos responda dicho mensaje. Si no recibe ninguna respuesta, el difusor sabe que le vecino se ha movido del alcance y ya no está conectado a él. De manera similar, si el difusor trata de envía un paquete a un vecino que no responde, se da cuenta que le vecino ya no está disponible.

Esta información se utiliza para eliminar rutas que ya no funcionan. Para cada destino posible, cada nodo, N, mantiene un registro de sus vecinos que le han proporcionado un paquete para ese destino durante los últimos T segundos. Esto se llaman vecinos activos de N para ese destino. N hace esto mediante un atabal de enrutamiento codificada por destino y al contener el nodo de salida a utilizar para llegar al destino, la cuenta de saltos al destino, el número de secuencia de destino más reciente y la lista de vecinos activos para este destino. En la siguiente figura se muestra una tabla de enrutamiento posible para el nodo D en nuestra topología de ejemplo. (Tanenbaum, 2003)

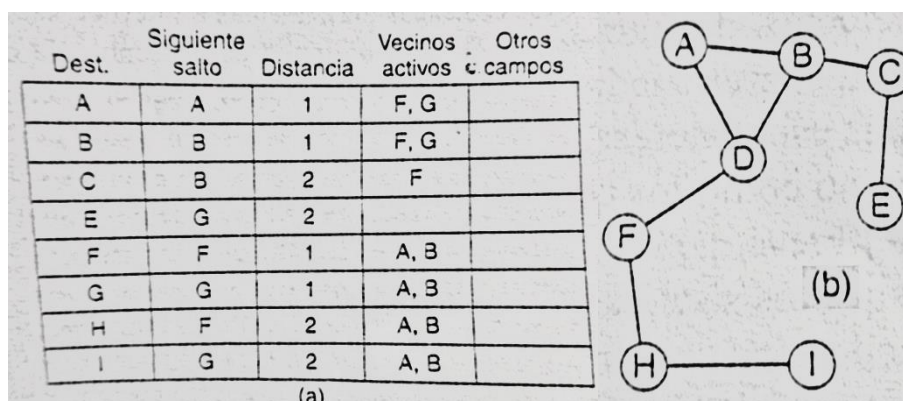


Tabla 9. Tabla de rutas

### **3.8 Clasificación de protocolos de encaminamiento**

Las diversas formas en la que pueden ser ejecutadas las funciones de encaminamiento, las diversas métricas de encaminamiento, así como las necesidades de las aplicaciones y las condiciones de tráfico en la red, han generado un amplio catálogo de propuestas de encaminamiento para redes inalámbricas ad hoc. La clasificación de estas propuestas de encaminamiento puede ser realizada basándose en diferentes criterios. Uno de los trabajos más pormenorizados sobre las diversas clasificaciones en las que se pueden catalogar los protocolos de encaminamiento. (Marquez, 2005)

#### **3.8.1 Encaminamiento Proactivo (manejo por tablas)**

En esta clase de protocolos la recopilación de información de encaminamiento y el cálculo de la ruta óptima de comunicaciones se realizan periódicamente a través del intercambio de paquetes de señalización, pues comúnmente estos proveen información acerca de la topología de la red. Cada nodo en la red mantiene conocimiento de las trayectorias hacia todos los destinos de la red en todo momento, aun sin tener la necesidad de transmitir información. Dado que la información de las rutas de encaminamiento es almacenada en tablas de ruteo, es común hacer referencia a estos protocolos como dirigidos por tabla (*table-driven*). Bajo este esquema de encaminamiento la latencia de transmisión es nula y las rutas calculadas se ajustan dinámicamente ante cualquier cambio de la topología de la red, sin embargo, la sobrecarga de señalización de encaminamiento, la escalabilidad de la red y el uso innecesario del ancho de banda son parte de los problemas que provoca el uso de este esquema de encaminamiento. (Carrillo, 2011)

#### **3.8.2 Encaminamiento Reactivo (por demanda)**

En contraste con los protocolos proactivos, en los protocolos reactivos la recopilación de información de encaminamiento y el cálculo de rutas se realiza a la demanda, es decir, solo en el momento en que un nodo requiere transmitir información y desconoce una ruta para comunicarse con el nodo destino.

El esquema petición/respuesta es utilizado usualmente por estos protocolos. Cada vez que un nodo requiere transmitir información, este inunda la red con mensajes de petición de ruta y espera que al llegar este paquete al nodo destino, este envíe un paquete de respuesta, lo cual permitirá establecer una trayectoria de comunicaciones.

Bajo este esquema de encaminamiento se evita la sobrecarga de señalización, se mejora la escalabilidad de la red y permite adaptar estos protocolos a entornos altamente dinámicos. La latencia de transmisión dependerá del tamaño de la red y una falla en una ruta de comunicaciones requerirá del redescubrimiento de una nueva trayectoria, lo cual representa demandas de tiempo, de cómputo y de recursos de la red. (Carrillo, 2011)

### 3.8.3 Encaminamiento Híbrido

Dado que los esquemas de encaminamiento proactivos y reactivos tienen propiedades que les permiten adecuarse de manera eficiente a diversos entornos, el encaminamiento híbrido combina ambos esquemas para hallar un balance entre las prestaciones que ofrece cada uno de estos. Comúnmente un protocolo híbrido asigna el uso de protocolos de encaminamiento proactivos a zonas de baja movilidad, mientras que el esquema reactivo es mayormente utilizado en zonas de la red altamente dinámicas. Esto le permite al protocolo de encaminamiento, adecuarse de manera óptima a las diferentes características de la red. (Carrillo, 2011)

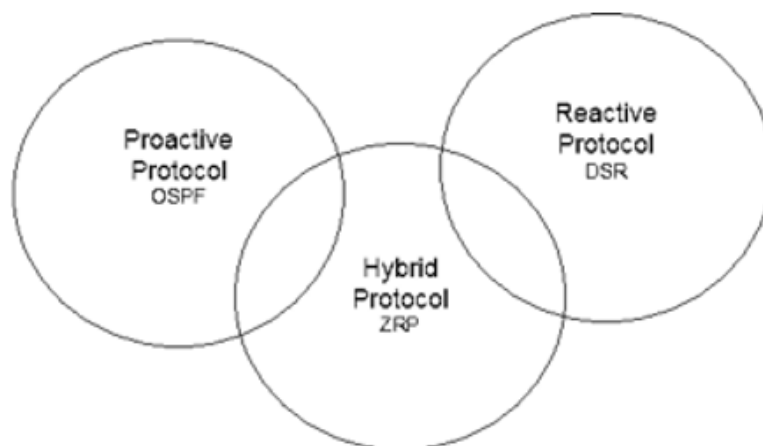


Figura 87. Clasificación de protocolos de encaminamiento

<http://www.venndiagram.net/photo-gallery>

### 3.9 Protocolos de Encaminamiento

En una Internet estática y pequeña, las tablas de encaminamiento se pueden crear y mantener manualmente. En Internet mayores los encaminadores mantienen sus propias tablas actualizadas intercambiando información unos con otros. Los encaminadores pueden descubrir dinámicamente:

Si se ha añadido una nueva red a la Internet, que el camino a un destino ha fallado y que ya no se puede alcanzar dicho destino. Se ha añadido un nuevo encaminador a la Internet. Este encaminador proporciona un camino más corto a ciertos lugares. No existe una única norma para el intercambio de información entre encaminadores. La libertad de elección del protocolo más apropiado ha estimulado la competencia y ha conseguido una gran mejora en estos protocolos.

Las funciones de red bajo el control de una organización se denominan un Sistema autónomo (*AS Autonomous System*). Una organización puede elegir el protocolo de intercambio de información de encaminamiento que desee para su propio Sistema autónomo. El protocolo de intercambio de información de encaminamiento dentro de un Sistema Autónomo se denomina Protocolo interior de pasarela (*IGP Interior Gateway Protocol*). El Protocolo de información de encaminamiento RIP (*Routing Information Protocol*) es un estándar muy usado del Protocolo de pasarela interior. RIP es muy popular por su sencillez y por su gran disponibilidad. Sin embargo, el nuevo protocolo Primero el camino abierto más corto OSPF dispone de un conjunto más rico de funciones. (Commons, Fundacion Wikimedia, 2012)



### 3.9.1 OLSR

*Optimized Link State Routing Protocol* es un protocolo proactivo que se basa en el estado de los enlaces. Se utiliza la técnica MPR (*Multipoint Relaying*) que consiste en elegir un conjunto de nodos vecinos que cubran el acceso de nodos distantes a 2 saltos o más. Se adapta bien en redes con un gran número de nodos y de alta movilidad.

El formato del paquete es igual para todos los datos del protocolo, así es fácil la extensión del mismo. Para saber el estado de un enlace se envían mensajes de HELLO. Cada nodo tiene asociado a cada vecino el estado del enlace. Cuando un nodo detecte la aparición de un nuevo vecino se debe incluir una nueva entrada a la tabla de encaminamiento e incluir el estado del enlace. Además si se detecta una variación en el estado de un enlace, se debe comprobar en la tabla de encaminamiento que el cambio ha sido reflejado. Si no se recibe información de un enlace durante un tiempo determinado se elimina de la tabla de encaminamiento el enlace y el vecino correspondiente.

Para calcular las rutas, cada nodo contiene una tabla de encaminamiento con el estado del enlace y el nodo. El estado del enlace se mantiene gracias al intercambio de mensajes periódicos. La tabla de encaminamiento se actualiza si se detecta algún cambio en el campo de enlace, de vecino, de vecino de dos saltos o en la topología. (Eduardo, 2012)

### 3.9.2 BATMAN

*Better Approach to Mobile Ad hoc Networks*, es un protocolo de encaminamiento relativamente reciente y que continúa bajo desarrollo con el objeto de reemplazar a OLSR. La principal innovación que introduce es, como su propio nombre indica, un diseño especialmente enfocado a las redes móviles inalámbricas. Resulta evidente que, cuando hablamos de dispositivos inalámbricos de bajo consumo y baja potencia computacional, como pueden ser los *routers* Mesh en un despliegue urbano, por ejemplo, la utilización de OLSR se hace dificultosa dado que obliga a mantener información sobre la topología completa de una red en constante cambio y por consiguiente, a encaminar los datos basándose en una tabla de encaminamiento altamente volátil y poco fiable. BATMAN pretende resolver este aspecto mediante la distribución del conocimiento sobre la topología de la red, de manera que cada nodo almacena y mantiene solamente la información relativa al siguiente salto para cada nodo destino.

De este modo, los nodos no almacenan las rutas completas extremo a extremo y los cambios en la topología sólo afectan localmente a los nodos cercanos en lugar de globalmente. Es un protocolo de encaminamiento dinámico y proactivo para redes malladas ad-hoc que utiliza las tablas de encaminamiento para las decisiones de encaminamiento. Este protocolo no calcula rutas completas entre un nodo origen y destino sino que selecciona un nodo de salto para utilizarlo como Gateway hacia el destino. Encuentra otros nodos y define el mejor vecino para llegar a ellos. Además hace un seguimiento de los nuevos nodos e informa a sus vecinos de su existencia. Es decir, cuando un nodo se incorpora a la red envía un paquete *broadcast* para avisar de su existencia. Este mensaje se va distribuyendo por toda la red.

El protocolo mantiene la información sobre la existencia de los nodos mientras sean accesibles. Como no hay necesidad de encontrar o calcular la ruta completa, la implementación es muy rápida y eficiente.

Los paquetes que transfiere BATMAN son muy pequeños. Cada nodo percibe y mantiene sólo la información sobre el próximo mejor salto hacia todos los otros nodos. De ahí que el conocimiento global acerca de los cambios en la topología local se convierte innecesario. El algoritmo, está diseñado para tratar con redes que están basadas en enlaces no confiables, el código fuente es liberado bajo la licencia GPL. (Eduardo, 2012)

### 3.9.3 DSDV

*Destination Sequenced Distance Routing*, es un protocolo *unicast* proactivo adaptado del tradicional protocolo RIP (*Routing Information Protocol*). Añade al protocolo RIP el número de secuencia, que es un nuevo atributo que se incluye en la tabla de encaminamiento. Esta información es útil para detectar la información más reciente y para evitar bucles. (Deco, 2000)

### 3.9.4 OSPF

*Open Short Path First*, es un protocolo de encaminamiento proactivo basado en el estado de enlace. Se puede utilizar en redes pequeñas y grandes. En redes grandes se utiliza el diseño jerárquico. Varias zonas se conectan a un área de distribución o área cero que se denomina *backbone*. Definiendo estas áreas se consiguen las siguientes ventajas: Reduce el gasto de procesamiento de información, acelera la convergencia, limita la inestabilidad de la red a un solo área y mejora el rendimiento. Cada nodo contiene la información de los nodos vecinos con su correspondiente estado de enlace y esta información es enviada a todos los vecinos. De modo que un nodo OSPF publica sus estados de enlace y los enlaces recibidos. Así cada nodo del área está informado de la base de datos y vecinos del resto de nodos. Para reducir el número de mensajes de encaminamiento entre los vecinos de la misma red, se selecciona un router designado y un router designado de respaldo que sirven como intercambiador de mensajes de información de encaminamiento. Este no fue concebido para trabajar con redes inalámbricas sino para redes cableadas. (Wang, 2005)

### 3.9.5 PWRP

*Predictive Wireless Routing Protocol*, es el único protocolo de encaminamiento proactivo desarrollado específicamente para redes inalámbricas. Además de validar el estado del enlace, como todos los demás protocolos, valida la calidad del enlace. Este protocolo recalcula 4 veces por segundo el estado de los enlaces de toda la red mallada y selecciona la ruta en función del estado de la red en cada momento. Este funcionamiento soporta redes dinámicas y proporciona la ruta más óptima en cada momento. (Eduardo, 2012)

### 3.9.6 AODV

*Ad hoc On-Demand Distance Vector*, es un protocolo diseñado para redes móviles. Permite el encaminamiento dinámico, auto configurable y *multi-salto* entre nodos. Se trata de un protocolo reactivo y *unicast* que se construye sobre el protocolo proactivo DSDV.

La mejora que realiza sobre este protocolo es que minimiza el número de *broadcast* requeridos para crear rutas. Esto es así porque al tratarse de un protocolo bajo demanda los nodos que no están en el camino elegido no tienen que mantener la ruta ni participar en el intercambio de las tablas de encaminamiento. Cuando un nodo quiere transmitir y no encuentra una ruta válida en su tabla de encaminamiento comienza con el proceso de descubrimiento de rutas.

Entonces se realiza un *broadcast* de mensajes a sus vecinos hasta que alcance al destino o a algún nodo intermedio que tenga la ruta hacia el destino creada recientemente. Para identificar si las rutas son recientes se utilizan los números de secuencia. Cuando el mensaje llega al destino o a un nodo con una ruta reciente hacia el destino, responde enviando un mensaje al vecino del que recibió el primer el mensaje y todos los nodos intermedios anotan la ruta como la más reciente hacia el destino. Por este motivo AODV sólo puede emplearse en enlaces bidireccionales. (Eduardo, 2012)

### 3.9.7 BABEL

Es uno de los protocolos más nuevos. Está basado en el algoritmo vector de distancias y diseñado para ser robusto y eficiente tanto en redes cableadas como en redes inalámbricas malladas. Se origina sobre las ideas de *Destination-Sequenced Distance Vector routing* (DSDV) y *Ad hoc On-Demand Distance Vector Routing* (AODV). Emplea varias técnicas para asegurar la ausencia de patologías de ruteo tal como ser bucles. Es proactivo, pero con características adaptativas (reactivo). Tiene múltiples estrategias para el cálculo de costos de los enlaces y métricas de ruteo. (Eduardo, 2012)

### 3.9.8 DSR

*Dynamic Source Routing*, es un protocolo donde el encaminamiento se organiza desde el origen. Se incluye en la cabecera de los datos un campo de información sobre los nodos exactos que debe atravesar, de modo que no se necesita de mensajes periódicos y se disminuye la sobrecarga de mensajes de control.

Además ofrece la posibilidad de obtener con una solicitud de una ruta, múltiples caminos hacia el destino. Cada nodo dispone de una memoria caché de rutas donde almacena las rutas ya descubiertas.

Cuando un nodo quiere transmitir lo primero que hace es consultar su tabla de encaminamiento para saber si hay una ruta hacia ese destino. Si no tiene la ruta comienza el descubrimiento mediante *broadcast* de mensajes es un protocolo reactivo. (Petinari, 2000)

### 3.9.9 TORA

*Temporally Ordered Routing Algorithm* es un protocolo de encaminamiento reactivo que se basa en ofrecer al nodo origen múltiples trayectos para alcanzar al destino. Este protocolo fue propuesto para redes muy dinámicas. Cuando se detecta un cambio en la topología se generan mensajes de control en un pequeño conjunto de nodos cercanos al cambio. Para utilizar estas funciones básicas define tres tipos de paquetes de control: QUERY (QRY), UPDATE (UPD), CLEAR (CLR). En las fases de creación y mantenimiento el paquete QRY se utiliza como petición y el paquete UPD se utiliza como respuesta. Cuando un nodo necesita descubrir una ruta hacia un destino se hace un envío *broadcast* de mensajes QRY. El destino o un nodo que posea una ruta válida hacia el destino le responde con un mensaje UPD. El paquete CLEAR se utiliza como *broadcast* para eliminar las rutas inválidas cuando un nodo es inaccesible. (Petinari, 2000)

### 3.9.10 GPSR

*Greedy Perimeter Stateless Routing* es uno de los primeros protocolos de encaminamiento basados en la posición de los nodos. Este protocolo reacciona rápidamente y es eficiente en redes móviles. Estudia la relación entre la posición y la conectividad geográfica de la red inalámbrica, utilizando las posiciones de los nodos para tomar decisiones de retransmisión de paquetes. Se utiliza en redes móviles vehiculares. Para llevar a cabo el enrutamiento de los paquetes de datos desde un nodo origen hacia un determinado destino, no establece de antemano una ruta por la cual circularán todos los paquetes, sino que cada nodo intermedio decide hacia qué nodo encaminará cada paquete recibido en base a la localización del destino final y la posición de sus nodos vecinos. Para tomar esta decisión, distingue dos modos de encaminamiento: *greedy forwarding* y *perimeter forwarding*. Con el primer modo (el empleado por defecto) el nodo transmite el paquete de datos a su nodo vecino que más cerca se encuentre del destino, de forma que el paquete se irá aproximando progresivamente al destino final. Sin embargo, cuando un nodo no tenga ningún vecino más próximo al destino que él mismo, cambiará el modo de enrutamiento a *perimeter forwarding* e intentará encaminar el paquete de datos de manera que bordeé la zona en la que no había ningún nodo disponible. Independientemente del modo de encaminamiento empleado, el proceso se repite en cada nodo re transmisor hasta que el paquete alcanza el nodo destino. Los protocolos basados en la posición normalmente muestran problemas de enrutamiento en escenarios con presencia de edificios, obstáculos, bifurcaciones e intersecciones. (Petinari, 2000)

### 3.9.11 HWMP

Es el protocolo de enrutador que especifica el nuevo estándar IEEE 802.11s para redes malladas que se aprobó en 2011. Es un protocolo híbrido que tiene un conocimiento parcial de la topología, es decir conoce sólo a los vecinos. Este protocolo debe ser implementado obligatoriamente por todos los nodos Mesh, aunque se permite usar protocolos adicionales. La principal ventaja de este estándar es que introduce un mecanismo de enrutamiento en la capa 2 (MAC), haciéndolo aparecer como un sistema LAN (802.x) para protocolos de capas superiores. Además, define no sólo cuestiones de encaminamiento sino también aspectos como acceso al medio,

sincronización o seguridad. El hecho de que el enrutamiento funcione en la capa de enlace de datos también se convierte en una desventaja, ya que de esta manera no se puede aprovechar la estructura jerárquica de protocolos de direccionamiento superiores, como IP, ni interconectar diferentes redes.

Este hecho hace que sea complicado enrutar paquetes sólo con HWMP en redes Mesh de tamaño medio o grande. Por ello se hace necesario combinar este protocolo con otros de capas superiores. HWMP combina características del protocolo AODV y técnicas de enrutamiento basadas en árbol. La combinación de elementos proactivos y reactivos permite una óptima y eficiente selección de ruta en una amplia variedad de redes Mesh (con y sin infraestructura). Utiliza un conjunto de mensajes basados en AODV, adaptados al direccionamiento MAC de la capa 2, para el descubrimiento de rutas reactivamente. Adicionalmente, se usa en otros mensajes para, de forma proactiva, construir un árbol de vectores distancia a partir de un nodo raíz. Este último método necesita que el nodo a partir del cual se calculará el árbol esté configurado como raíz.

Pueden existir varios nodos raíz en una misma red. Esta técnica suele utilizarse para construir árboles de rutas hacia nodos que cumplen un papel especial dentro de la red, como por ejemplo los nodos que actúan como portal hacia otras redes. Se contemplan dos modos de funcionamiento, no excluyentes: bajo demanda y construcción proactiva de árbol. Este modo híbrido permite combinar concurrentemente componentes reactivos y proactivos. Permite elegir cualquier métrica o combinación de métricas. (Eduardo, 2012)

Protocolo	Tipo de Protocolo	Alcance de transmisiones	Métrica de ruteo	Uso Libre/ Propietario
AODV	Reactivo	Unicast	Camino más rápido y más corto	Libre
Babel	Proactivo	Multicast	Configurable. Por default: Calidad del enlace	Libre
BATMAN	Proactivo	Multicast	próximo mejor salto para cada destino	Libre
DSDV	Proactivo	Unicast	Camino más corto	Libre
DSR	Reactivo	Unicast	Camino más corto	Libre
GPSR	Proactivo. Basado en la posición	Geocast	Utiliza la posición geográfica para reenviar paquetes a nodos más cercanos	Libre
HWMP	Híbrido	Híbrido	Permite combinación de métricas	Libre
OLSR	Proactivo	Unicast	Camino más corto	Libre
OSPF	Proactivo	Unicast	Camino más corto	Libre
PWRP	Proactivo	Unicast	Camino más óptimo (recálculo dinámico de enlaces)	Propietario
TORA	Reactivo	Unicast	Construcción de múltiples caminos utilizando DAG	Propietario

Tabla 10. Clasificación de protocolos

[http://sedici.unlp.edu.ar/bitstream/handle/10915/23759/Documento\\_completo.pdf?sequence=1](http://sedici.unlp.edu.ar/bitstream/handle/10915/23759/Documento_completo.pdf?sequence=1)

# CAPÍTULO IV

## DISEÑO Y SIMULACIÓN DE LA RED MESH

## **IV. DISEÑO Y SIMULACIÓN DE LA RED MESH EN EL PARQUE TEMATICO**

En este capítulo se propone la utilización de gráficos más detallados para el estudio del desempeño de protocolos de enrutamiento para redes ad-hoc móviles de múltiples saltos cuando se desee estudiar la factibilidad de brindar calidad de servicio a las aplicaciones de tiempo real de capas superiores.

### **4.1 Introducción**

Se aplicaron una serie de preguntas a ciento doce personas (encuesta) las preguntas fueron diseñadas con el objetivo de conocer cuántas personas que visitan el parque municipal “Las Fuentes” contaban con dispositivos móviles, otro objetivo fue conocer si era necesaria una conexión a internet además de saber el uso que le darían a dicho servicio. Para definir el tamaño de la muestra o población en este caso de tipo cuantitativa se utilizó una fórmula que nos ayudó a determinar el número de encuestas a aplicar, además se definieron las metodologías bajo las cuales se realizó dicha encuesta además de establecer los criterios de aplicación de la encuesta.

#### **4.1.1 Metodología del proceso la de encuesta:**

Planeación: Una vez definida la realización de la encuesta para encontrar las necesidades de los visitantes en cuanto a la conexión libre a internet, la fase de planeación implica la definición de los objetivos, la estrategia general, el método específico de generación de datos estadísticos. La planeación tiene diferentes niveles de realización según se trate de encuestas continuas, periódicas o de realización única.

Diseño del instrumento: En esta fase se define y justifican en forma clara y precisa los conceptos respecto a los cuales se obtendrán los datos de los visitantes del parque temático municipal “Las Fuentes” en estudio conforme a los objetivos de la encuesta, y se diseñan los instrumentos de captación considerando el panorama general de las personas que acuden al parque, además de la necesidad información confiable. Además de diseñar la presentación de resultados en este caso haciendo uso de gráficas.

Diseño muestra: En esta fase se determinó el método de muestreo y con base en los objetivos de cobertura y desglose temático y geográfico establecidos, así como de las características de la población de estudio y la información objeto de captación, una muestra es la representación de una población objeto de estudio que se usa para establecer la percepción y experiencia de los ciudadanos.

Ejecución de la encuesta: El encuestador debe tener credibilidad, habilidad para realizar la encuesta y contar con un buen respaldo institucional que permita reducir los márgenes de posibles resistencias. Una encuesta es un procedimiento de investigación, dentro de los diseños de investigación descriptivos (no experimentales) en el que el investigador busca recopilar datos por medio de un cuestionario previamente diseñado o una entrevista, sin modificar el entorno ni el fenómeno donde se recoge la información (como sí lo hace en un experimento). Este procedimiento fue aplicado a los visitantes y al personal operático del parque temático las fuentes, mediante la aplicación de un cuestionario previamente elaborado. El mismo que contiene preguntas abiertas y cerradas, permitiendo obtener información de suma importancia para determinar el diagnóstico situacional y la elaboración de la propuesta. (Johnson, 2005)

Procesamiento y análisis de los resultados: En esta fase se organizan los datos captados, en archivos de información, preparados para su explotación estadística. No se debe ocultar información “negativa” así mismo se debe garantizar la transparencia, objetividad y consistencia del proceso. En la fase de presentación de resultados se concretan los esquemas de presentación (gráficas) de resultados definidos previamente en el diseño del instrumento, mediante la elaboración de los distintos productos para su difusión. (INEGI, 2010). Es importante destacar que los métodos de recolección de datos, se pueden definir como: al medio a través del cual el investigador se relaciona con los participantes para obtener la información necesaria que le permita lograr los objetivos del análisis. Mediante la encuesta y la observación directa métodos empleados anteriormente se logró recolectar la información necesaria para identificar las necesidades en cuanto a telecomunicaciones de los visitantes del parque temático las fuentes. (Manrique, 2004)

#### **4.1.2 Criterios para la aplicación de la encuesta:**

El día 4 y 5 de abril se aplicó una encuesta a los visitantes del parque municipal las fuentes con una afluencia de 600 visitantes en fin de semana siendo estos los días con mayor asistencia, dicha encuesta se aplicó a 100 personas bajo los siguientes criterios:

- Jóvenes de entre 15 y 25 años
- Jóvenes estudiantes
- Padres de familia
- Personas con dispositivos móviles
- Personas inactivas



### 4.1.3 Determinación del Tamaño de la muestra

Cuando se necesita información para realizar estudios con datos estadísticos y no se puede contar un censo, porque es muy caro, o porque demora mucho o no se cuenta con el personal adecuado; entonces será necesario obtener una muestra, ahora. Pero viene la pregunta: ¿Cuál será el número adecuado mínimo del tamaño de la muestra? En principio existe todo un proceso para obtener una muestra representativa de la población. Si el método es aleatorio o probabilístico, entonces el número adecuado de los elementos de la muestra, se pueden calcular usando las siguientes formulas. (Tumbes, 2015)

Dónde:

P= Proporción de éxito; que se conoce por estudios anteriores o similares.

Q= (1-P). Proporción de fracaso.

Z $\alpha$ =Valor que se obtiene de la distribución normal, para un nivel de significación  $\alpha$ .

Generalmente se toma:

Z=1.96 para un nivel de significancia del 5%.

Z=2.575 para un nivel de significancia del 1%.

E=Error de estimación. Valor que lo determina el investigador. Se sugiere valores en torno al 5%.

N= Numero de los elementos de la población.

Nota:

Si no se conoce P, se puede adoptar las siguientes decisiones:

- i) Tomar una muestra piloto y calcular el valor de P.
- ii) Considerar el valor de P=0.5, lo cual dará el número de elementos de la muestra el mayor posible.

R= Valor que determina el investigador.

Cuando el estudio es de carácter cuantitativo:

Cuando el tamaño N de la población es finito:

n= 600

e= 0.05

r= 0.3

z= 1.96

$$n = \frac{NZ_{\alpha}^2 \sigma^2}{(N-1)E^2 + Z_{\alpha}^2 \sigma^2}$$

$$n = 112.5441884$$

$$n = \frac{(600)(1.96)^2(0.3)^2}{(600-1)(0.05)^2 + (1.96)^2(0.3)^2} =$$

$$n = \frac{207.4464}{1.4975 + 0.345744}$$

$$n = \frac{207.4464}{1.843244}$$

#### 4.1.4 Análisis e interpretación de Resultados (Encuesta)

Pregunta 1.

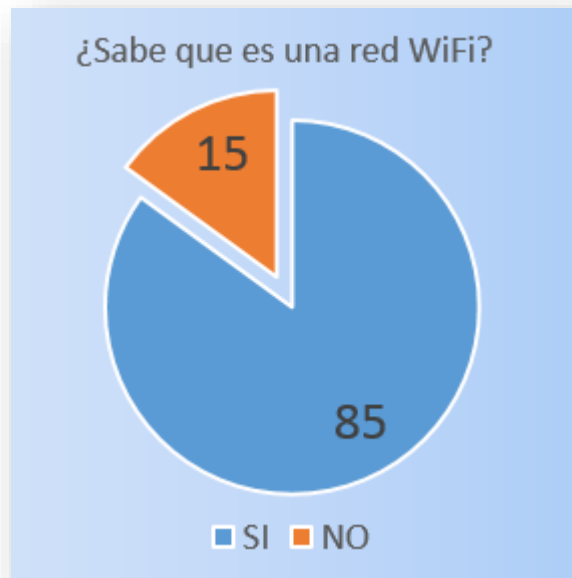


Figura 88. Gráfica 1

Fuente. Encuesta aplicada a visitantes del parque municipal "Las Fuentes", Ayuntamiento Nezahualcóyotl, Edomex 2015

Análisis: De la información recabada de las personas que asisten al parque temático se puede apreciar que el 85% conoce lo que es una red WiFi y el 15% desconoce dicha red.

Pregunta 2.



Figura 89. Gráfica 2

Fuente. Encuesta aplicada a visitantes del parque municipal "Las Fuentes", Ayuntamiento Nezahualcóyotl, Edomex 2015

Análisis: De la información obtenida el 90% de los encuestados asegura indispensable el acceso internet dentro del parque y el 10% no considera necesaria una conexión a internet.

Pregunta 3.

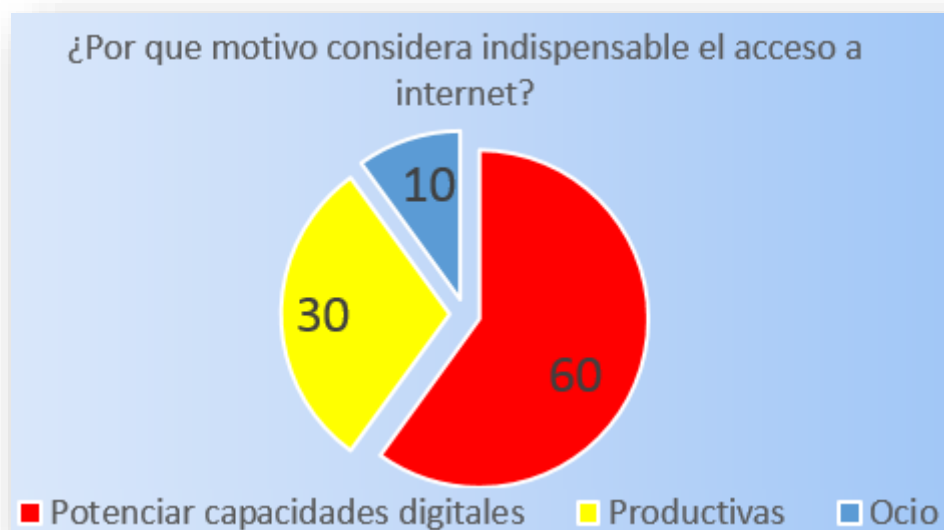


Figura 90. Gráfica 3

Fuente. Encuesta aplicada a visitantes del parque municipal "Las Fuentes", Ayuntamiento Nezahualcóyotl, Edomex 2015

Análisis: De la información obtenida el 60% asegura que el libre acceso a internet potencializa las capacidades digitales mientras que el 30% realizaría actividades productivas y el 10% serían actividades de simple ocio.

Pregunta 4.

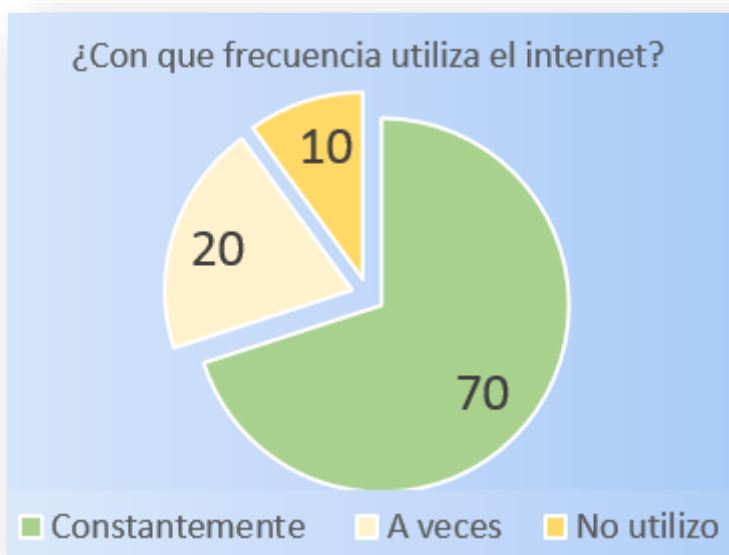


Figura 91. Gráfica 4

Fuente. Encuesta aplicada a visitantes del parque municipal "Las Fuentes", Ayuntamiento Nezahualcóyotl, Edomex 2015

Análisis: De la información obtenida nos muestra que el 70% utiliza el internet constantemente por otra parte el 20% requiere a veces la conexión a internet mientras que el 10% asegura no utilizar dicho servicio.

Pregunta 5.

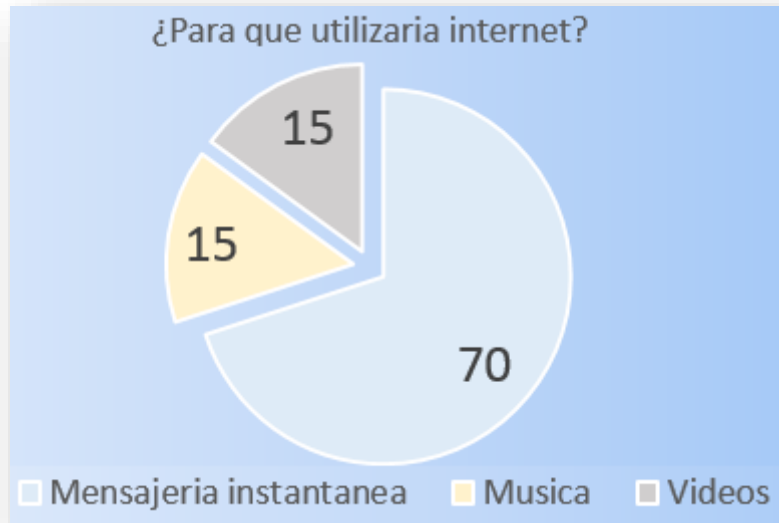


Figura 92. Gráfica 5

Fuente. Encuesta aplicada a visitantes del parque municipal "Las Fuentes", Ayuntamiento Nezahualcóyotl, Edomex 2015

Análisis: De la información obtenida el 70% de los visitantes dijeron utilizar internet para mensajería instantánea mientras que el 15% lo usaría para escuchar música y el otro 15% restante lo usaría para ver videos.

Pregunta 6.

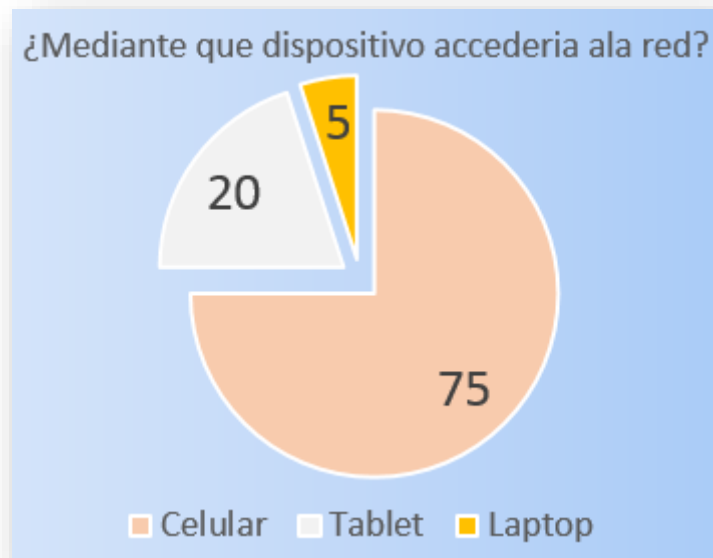


Figura 93. Gráfica 6

Fuente. Encuesta aplicada a visitantes del parque municipal "Las Fuentes", Ayuntamiento Nezahualcóyotl, Edomex 2015

Análisis: De la información obtenida el 75% menciona que se conectaría mediante un dispositivo celular mientras que el 20% utilizara una Tablet y el 5% lo haría con su laptop.

Pregunta 7.

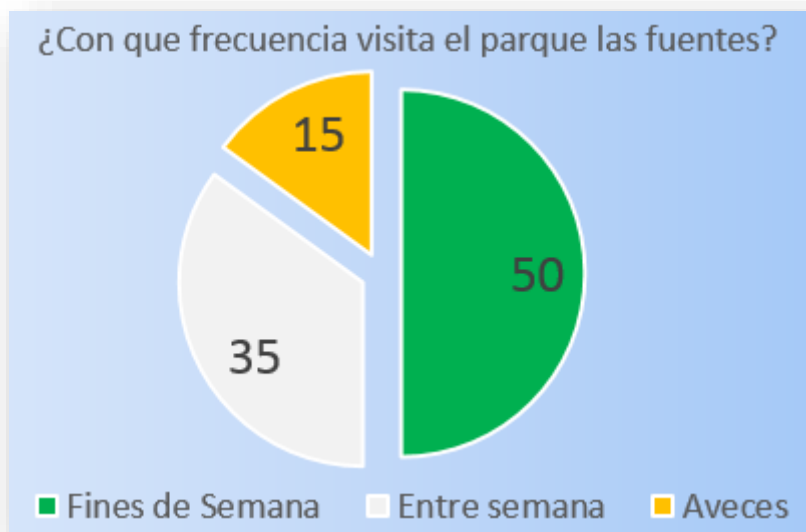


Figura 94. Gráfica 7

Fuente. Encuesta aplicada a visitantes del parque municipal "Las Fuentes", Ayuntamiento Nezahualcóyotl, Edomex 2015

Análisis: De la información recabada muestra que hay un total de 50% de visitantes los fines de semana mientras que un 35% asiste entre semana y un 15% asegura visitar el parque en algunas ocasiones.

## 4.2 Características del lugar de estudio

El siguiente lugar es un parque municipal de tipo temático llamado las fuentes.

### 4.2.1 Introducción

El gobierno municipal inauguró el parque temático Las Fuentes, la noche del viernes 6 de marzo, el cual cuenta con 110 fuentes danzantes lúdicas, interactivas, con bruma e iluminación, donde niños y jóvenes podrán bañarse; además presentará múltiples espacios, actividades recreativas y deportivas; el espacio es gratuito y se encuentra ubicado en el cruce de las avenidas Bordo de Xochiaca y Nezahualcóyotl.

Zepeda Hernández puntualizó que el parque Las Fuentes es un lugar para los vecinos y los invitó a cuidarlo y celebrar ahí cumpleaños, fiestas familiares y hacer deporte y convertirlo en un espacio que enaltezca a la demarcación y sea un orgullo de los vecinos.

El parque Las Fuentes cuenta con carritos eléctricos y mecánicos para fomentar en los niños la cultura vial en una ciudad a escala, ya que cuenta con un circuito donde los pequeños aprenderán a manejar en un espacio muy agradable, además hizo mención para evitar el desperdicio de agua, las fuentes danzantes cuentan con un sistema de reciclado de agua la cual va a estar limpia día con día, ya que cuenta con un sistema que filtra, oxigena y limpia de tal forma que basta llenar el tanque una sola vez, ya que se trata de un reciclado permanente.

Agrego el objetivo es fomentar la convivencia familiar sin afectar la economía de las familias, y ello forma parte del rescate de 70 espacios públicos en diversas modalidades, que van desde los parques acuáticos hasta los espacios deportivos. (Jornada, 2015)



Figura 95. Toma aérea del parque temático 2015  
<https://edomex.quadratin.com.mx/Construiran-parque-municipal-sobre-Bordo-de-Xochiaca-en-Neza/>

## 4.2.2 Ubicación del Parque Temático las Fuentes

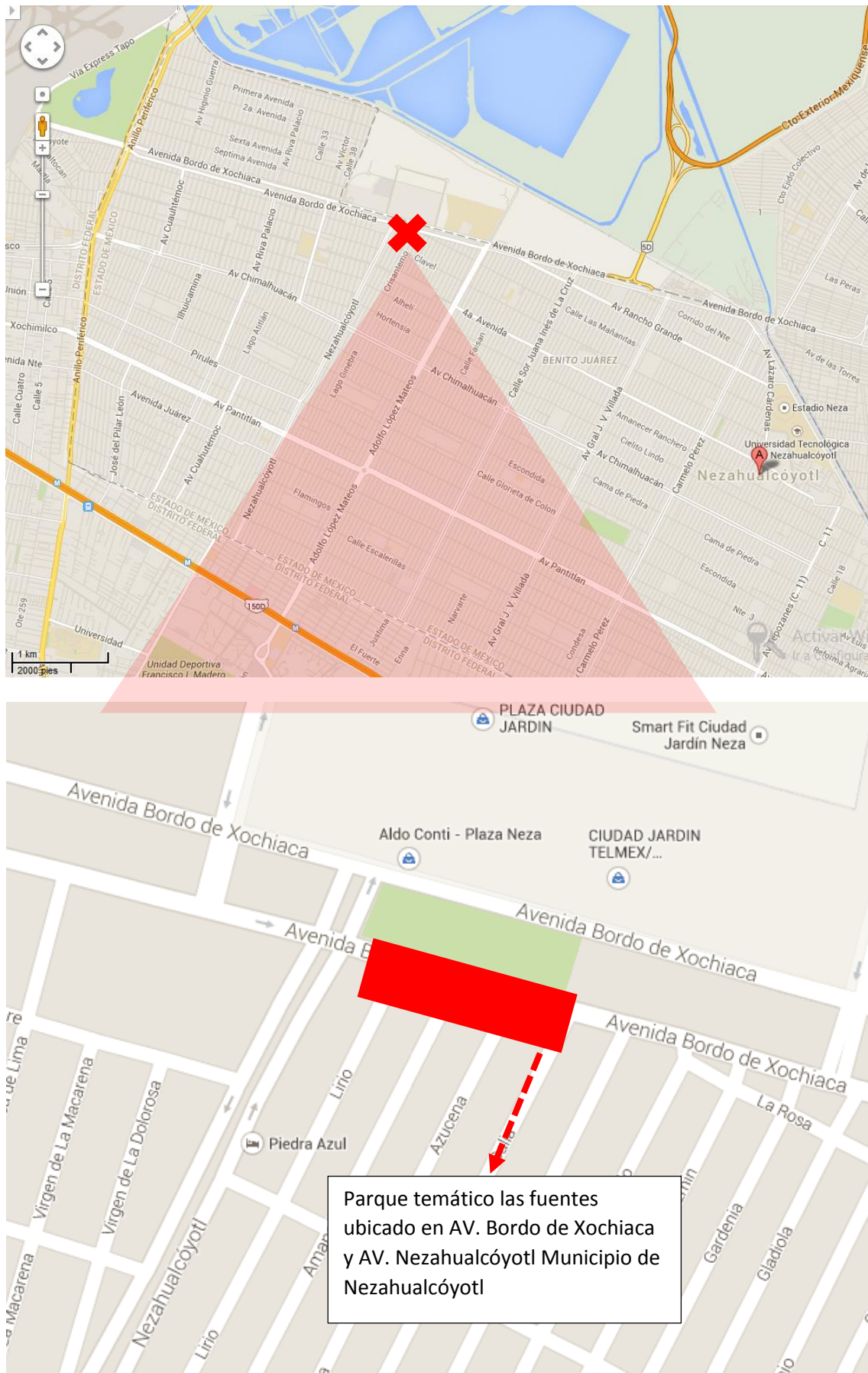


Figura 96. Ubicación con Google Maps  
<https://www.google.com.mx/maps>

#### 4.2.3 Plano de distribución del Parque Temático las Fuentes

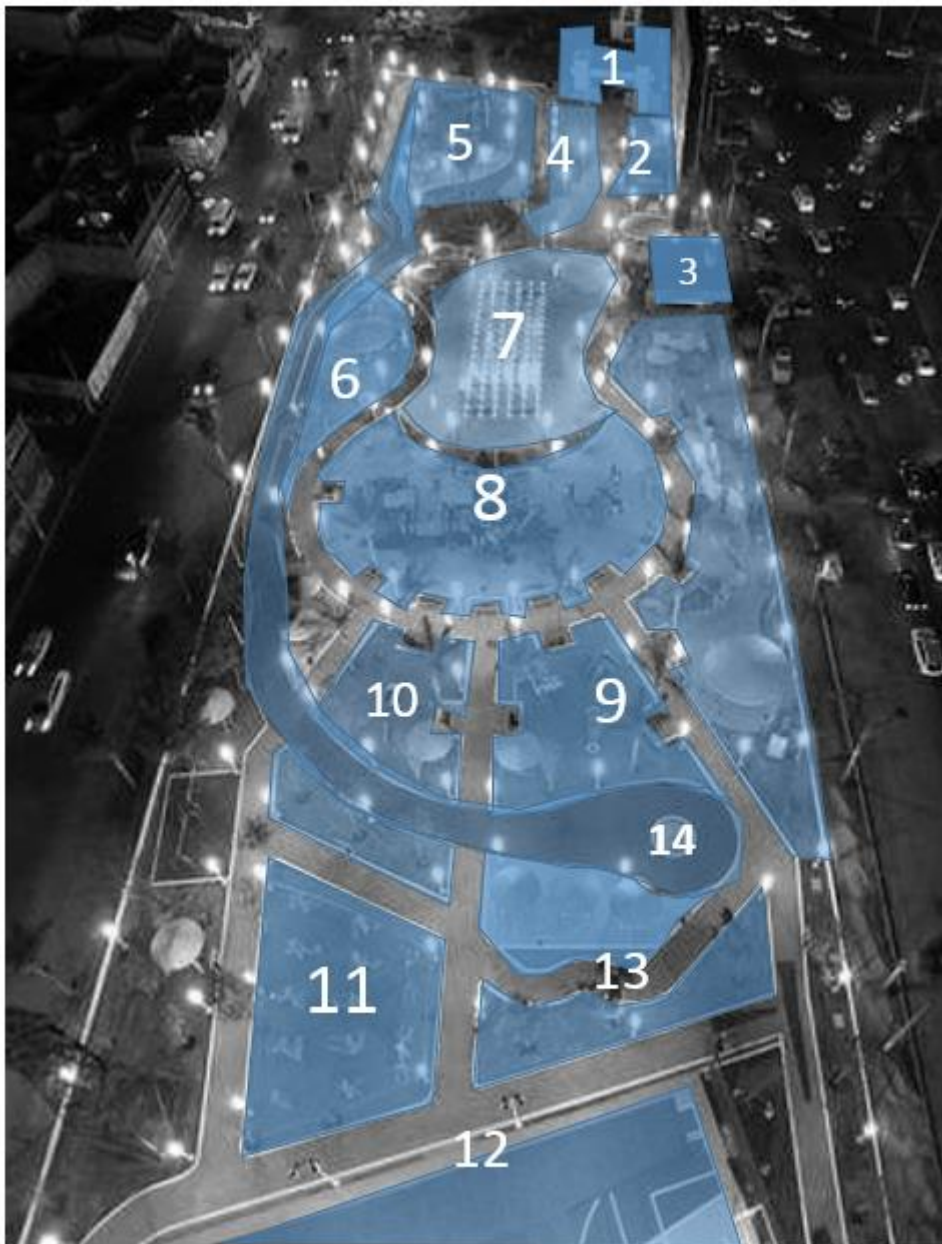


Figura 97. Plano de distribución del parque

Fuente: Ayuntamiento del Municipio Nezahualcóyotl, Parque "Las Fuentes", Edomex 2015

- |                        |                       |
|------------------------|-----------------------|
| 1- Entrada             | 8- Juego de Playa     |
| 2- Tramite de licencia | 9- Juegos Infantiles  |
| 3- Baños               | 10- Juegos Saltarines |
| 4- Juego Ciudad        | 11-Gym                |
| 5- Renta de coches     | 12-Canchas            |
| 6- Picnic              | 13-Palapas            |
| 7- Fuente Danzante     | 14-Ciclo vía          |



#### 4.2.4 Áreas del Parque Temático

Entrada del parque municipal:



Figura 98. Entrada  
Fuente: Ayuntamiento del Municipio Nezahualcóyotl, Parque  
"Las Fuentes", Edomex 2015

Área: Canchas de futbol



Figura 99. Canchas  
Fuente: Ayuntamiento del Municipio Nezahualcóyotl, Parque  
"Las Fuentes", Edomex 2015

Área: Gimnasio



Figura 100. Gym  
Fuente: Ayuntamiento del Municipio Nezahualcóyotl, Parque  
“Las Fuentes”, Edomex 2015

Área: Palapas



Figura 101 Palapas  
Fuente: Ayuntamiento del Municipio Nezahualcóyotl, Parque  
“Las Fuentes”, Edomex 2015

Área: de Juegos Saltarines



Figura 102. Juegos  
Fuente: Ayuntamiento del Municipio Nezahualcóyotl, Parque  
“Las Fuentes”. Edomex 2015

Área: de Juegos Infantiles



Figura 103. Juegos para niños  
Fuente: Ayuntamiento del Municipio Nezahualcóyotl, Parque  
“Las Fuentes”, Edomex 2015

Área: de Juego de Playa



Figura 104. Juego Playero  
Fuente: Ayuntamiento del Municipio Nezahualcóyotl, Parque  
“Las Fuentes”, Edomex 2015

Área: de Pic Nic



Figura 105. Fuentes  
Fuente: Ayuntamiento del Municipio Nezahualcóyotl, Parque  
“Las Fuentes”, Edomex 2015

Área: Fuentes Danzantes



Figura 106. Lámparas de vela  
Fuente: Ayuntamiento del Municipio Nezahualcóyotl, Parque  
“Las Fuentes”, Edomex 2015

Área: Baños



Figura 107. Baños  
Fuente: Ayuntamiento del Municipio Nezahualcóyotl, Parque  
“Las Fuentes”, Edomex 2015

Área: Ciclo vía



Figura 108. Pista

Fuente: Ayuntamiento del Municipio Nezahualcóyotl, Parque “Las Fuentes”, Edomex 2015

Área: Juego Ciudad



Figura 109. Juego de ciudad

Fuente: Ayuntamiento del Municipio Nezahualcóyotl, Parque “Las Fuentes”, Edomex 2015

Área: Préstamo de carros



Figura 110. Renta de autos  
Fuente: Ayuntamiento del Municipio Nezahualcóyotl, Parque  
“Las Fuentes”, Edomex 2015

Area: Modulo de tramite de Licencia



Figura 111. Modulo  
Fuente: Ayuntamiento del Municipio Nezahualcóyotl, Parque  
“Las Fuentes”, Edomex 2015

## Area de: Prestamo de carros



Figura 112. Carritos

Fuente: Ayuntamiento del Municipio Nezahualcóyotl, Parque “Las Fuentes”, Edomex 2015

## Módulo de Policía



Figura 113. Modulo

Fuente: Ayuntamiento del Municipio Nezahualcóyotl, Parque “Las Fuentes”. Edomex 2015



### 4.3 Proveedores de tecnología Mesh.

Existen diferentes proveedores de tecnología en el mercado de las telecomunicaciones pero en la actualidad fabricantes de equipos de tecnología Mesh que han decidido trabajar bajo el estándar de la IEEE 802.11 como norma para sus equipos ya que la mayoría de los equipos que ofrecen este servicio de la red mallada soportan dicho estándares. (Air, 2015)

Ejemplo de algunos proveedores son:

- *STRIX SYSTEM*
- *BELAIR NETWORKS*
- *CISCO SYSTEM*
- *TROPOS NETWORKS*

#### 4.3.1 BELAIR NETWORKS



Figura 114. Logo de BelAir

<http://signalstelecomnews.com/categoria/wireless/page/11/>

Una red mallada está definida por *BelAir Networks* como una aplicación inalámbrica la cual tiene una gran flexibilidad en los enlaces que se pueden ofrecer con esta tecnología, existen diferentes tipos de enlace:

- Punto a Punto
- Punto multipunto
- Multipunto a multipunto

Para *BelAir* las características principales de una red en malla son la siguientes, Topología arbitraria de nodos y conectividad entre ellos, enrutamiento del tráfico de forma automática múltiples punto de entrada y salida.

Una red en malla puede ser aplicadas en áreas donde se desea repartir servicios de red de forma inalámbrica por lo regular es en grandes extensiones de terreno

como universidades, puertos, municipios donde el objetivo es transportar grandes cantidades de información sin que exista pérdida de comunicación de tipo voz, datos o video.

Una de las soluciones que ofrece *BelAir* es sumamente atractiva ya que utiliza equipos que tienen desde uno o hasta 4 radios para comunicarse entre ellos y para proporcionar servicio.



Figura 115. Arquitectura de red con equipos BelAir  
<http://signalstelecomnews.com/categoria/wireless/page/11/>

Características de la red en malla *BelAir*:

Cobertura

- Principalmente es considerado una solución *multi-radio* ya que cada nodo costa de dos o más radios.
- Las terminales o sea equipos de los usuarios son capaces de soportar el estándar 802.11b/g.
- Es una solución aplicada para *outdoor* porque permite que la señal entre en el interior de los inmuebles para dar cobertura también en *indoor*.

Configuración, seguridad y calidad del servicio

- Es considerado una solución de nivel tipo dos refiriéndose a la capa de enlace de datos.
- Permite un máximo de 5 saltos.
- Cumple los estándares 802.1x/EAP/PEAP/WPA
- Con respecto a la encriptación cumple el estándar 802.11i/WPA2/AES-152/WEK.
- Es capaz de soportar redes tipo VLANs y múltiples SSID y VPNs.
- Hablando de la calidad del servicio es posible definir clases de servicio, prioridades y VLANs para distintos tipos de tráfico. (Air, 2015)

## Hardware Mesh BelAir



Figura 116. Hardware BelAir  
<http://www.amacnet.com/belairnetworks.html>

### 4.3.2 TROPOS NETWORKS



Figura 117. Logo de Tropos  
<http://www.greentechlead.com/smart-grid/quam-power-authority-selects-tropos-networks-for-smart-grid-project-2806>

El proveedor tropos *networks* tiene un nombre en el mercado el cual es “Tropos *metromesh*” el equipo y protocolos utilizados proporciona la capacidad de reaccionar a cualquier falla que pueda surgir comúnmente entre ellas la interferencia o pérdida de un acoplamiento si se desea obtener el máximo rendimiento del hardware Tropos *metromesh*, el proveedor implemento a sus equipos su propio protocolo de enrutamiento nombrado *Predictive Wireless Routing Protocol* (PWRP) este protocolo es una variación de las redes cableadas OSPF.



Figura 118. Arquitectura de una Metromesh  
<http://nagpurwifi.blogspot.mx/>

Dentro de la *metromesh* existe una conexión inalámbrica cableada entre los Gateway llamado *Mesh Routers*, otra función principal es que la base se puede conectar a la nube IP. Todo esto facilita múltiples caminos entre los router y así determinar la mejor ruta para el envío de la información. La interconexión entre los usuarios de la red en malla tipo WiFi comparten el estándar IEEE 802.11.

## Características de la *metromesh* Tropos

### Cobertura

El fabricante Tropos está diseñado en base a sistemas de primera y segunda generación ya que cuenta con una o dos interfaces de radio teniendo una sola interface de radio la cual opera en la banda de 2.4GHz es empleada para la comunicación entre Router permitiendo dar servicio. Cuando cuentan con dos interfaces de radio de 2.4GHz y 5GHz se conmutan dinámicamente para establecer comunicación entre *Routers* o para dar servicio. Todas las terminales deben soportar el estándar 802.11b/g. La distancia entre el router mesh y el usuario o cliente en un máximo de 7 metros.

### Configuración, seguridad y calidad del servicio

- En Tropos se configura automáticamente cuando se selecciona un camino óptimo procura aumentar el *throughput* y minimiza la latencia, dicho camino se actualiza cada 250ms y lo hace de forma dinámica.
- Si se quiere lograr el máximo *throughput* se debe tener en cuenta las medidas realizadas en el *uplink* y en el *downlink*.
- Es posible que un fallo llegue a presentarse en un enlace entonces el router buscare un enlace alternativo óptimo.
- La tecnología Tropos es posible alcanzar un máximo de tres a cuatro saltos sin dejar de lado que el *overhead* introducido es mínimo y constante esto no quiere decir que aumente en cada salto ya que solo se alimenta del 5% del ancho de banda disponible admitiendo un tope de veinte nodos/ $kn^2$ .
- Hablando de seguridad la *metromesh* hace uso del protocolo AES entre los metro *meshrouter* y WPA para el acceso a la norma IEEE 802.11.
- En cuanto a calidad del servicio se desee es posible que el usuario tenga diferentes niveles de prioridad para el tráfico. (Network, 2012)

## Hardware Mesh Tropos



Figura 119. Hardware Tropos

<http://new.abb.com/network-management/communication-networks/wireless-networks>

### 4.3.3 Strix Systems



Figura 120. Logo de Strix

<http://www.connectronics.com/strix/>

La tecnología con la que ha entrado *Strix Systems* propone una solución con equipos que manejan más de una interface de radio a esta propuesta se le ha denominado *Acces/One Networks OWS*. La topología *mesh Strix Systems* busca que la red sea relacionada fiable y redundante además de que se pueda seguir extendiendo para la conexión de innumerables dispositivos. La red *aces/One* que ha desarrollado este proveedor se puede instalar en cuestión de horas y no es necesario una planificación ni tampoco ningún tipo de mapas garantizando comunicaciones fiables.

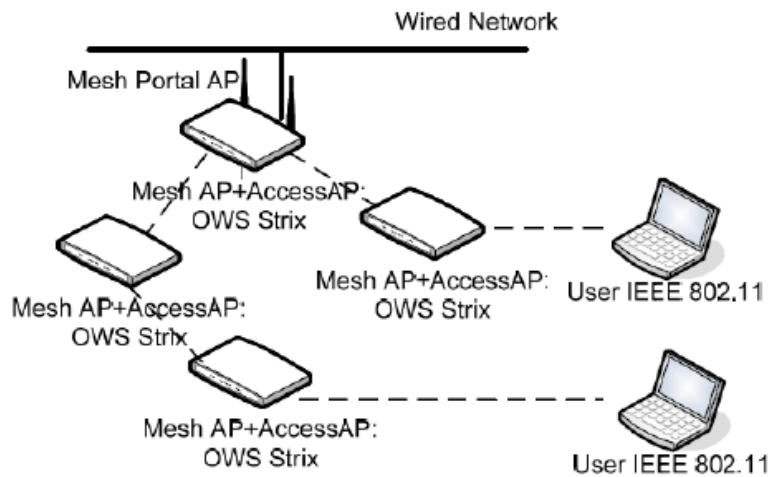


Figura 121. Red Mesh tipo Strix  
<http://slideplayer.es/slide/1094175/>

## Características de la red en malla *Strix Systems*

### Cobertura

- Los equipos *Strix System* son capaces de cumplir dos funciones router Mesh y *Access point*.
- Cuentan con dos interfaces de radio en la banda de 2.4GHz y 5GHz.
- La interface de radio utilizada para la conexión de nodos utiliza diversos canales de radio y estos son divididos para realizar la transmisión o recepción de datos.
- Una característica de los equipos *Strix System* es que las antenas se pueden sectorizar para mejorar la cobertura.
- El uso de los nodos están diseñados para estar separados a 50 metros uno del otro. Los equipos están configurados para trabajar bajo el estándar 802.11b/g.

### Configuración, seguridad y calidad del servicio

- La configuración de la red en malla *Strix Systems* ofrece ser una red escalable y auto configurable.
- Para alcanzar un camino óptimo en la transmisión de los enlaces se deben seguir los siguientes parámetros *throughput*, la señal a ruido y la disponibilidad de los enlaces.
- Esta tecnología ofrece una auto regeneración frente a los fallos si en algún momento existiera una pérdida de comunicación entre nodos o si alguno de estos se callera.
- El equipo *Strix System* está diseñado para soportar un tope de 50 a 150 usuarios por cada nodo y permite un máximo de 10 saltos.

- Hablando de la seguridad que ofrece *Strix System* dentro de sus redes utiliza un servidor de manera independiente para comprobar la autenticación por lo regular se emplea el método WPA2 y WEP.
- En cuanto a calidad de servicio de refiere se define por niveles dependiendo de la prioridad para los diferentes tipos de tráfico. (Strix, 2014).

### Hardware Mesh *Strix Systems*



Figura 122. Hardware Strix  
<http://www.strixsystems.com>

#### 4.3.4 Cisco Systems



Figura 123. Logo de Cisco  
<http://www.cisco.com>

Uno de los fabricantes más grande a nivel mundial a sido cisco cubriendo la necesidad de extender las conexiones WiFi de una manera sencilla confiable y sobre todo eficiente en cuanto a costo se refiere cisco a lanzado distintas soluciones al mercado entre ellas esta las tendencias Wireless 2.0 donde esta tecnología hace referencia a la conexión de ciudades y empresas conectadas. Las nuevas tecnologías de cisco están enfocadas para interiores como exteriores tal como es una red en malla tipo Mesh siendo este el último concepto introducido al mercado por esta compañía. La red Mesh que ofrece cisco *system* permite ofrecer servicios innovadores como implementar una red mesh en un municipio siendo útiles para administradores de locales parques y espacios públicos. (Cisco, Support Cisco, 2009)

Características de la red en malla cisco

- Con cisco es posible establecer una comunicación flexible móvil y dinámica.
- Las redes inalámbricas que ofrece cisco son una alternativa de bajo costo para aquellos lugares donde es imposible extender cableado.
- Esta tecnología Permite añadir nodos y dispositivos de red.
- Permite la integración con tecnología de red existente.
- Ofrece seguridad seguridad a toda la red distribuida.



Figura 124. Hardware Cisco  
<http://www.cisco.com>



La creación de redes de malla emplea Cisco 1520 Series puntos de acceso de malla al aire libre y Cisco 1130 y 1240 puntos de acceso de la serie de malla interior junto con el controlador de LAN inalámbrica de Cisco y Cisco Wireless Control System (WCS) para proporcionar escalabilidad, administración central, y la movilidad entre los despliegues de interior y al aire libre. Control y Aprovisionamiento de puntos de acceso inalámbrico protocolo (CAPWAP) gestiona la conexión de los puntos de acceso a la red de malla. La seguridad de extremo a extremo de la red de malla es apoyado por el empleo de cifrado *Advanced Encryption Standard* (AES) entre los puntos de acceso de malla inalámbricas Wi-Fi Protected Access 2 (WPA2) clientes. Este documento también describe la frecuencia de radio (RF) componentes a considerar en el diseño de una red exterior.

Las funciones descritas en este documento son de los siguientes productos:

- Cisco Aironet 1520 (1522, 1524) de la serie de puntos de acceso de malla al aire libre
- Cisco Aironet 1130 y 1240 de la serie de puntos de acceso de malla interior
- Malla características de controlador LAN inalámbrica de Cisco lanza 5.2 y versiones posteriores
- Malla características en Cisco WCS libera 5.2 y versiones posteriores (Cisco, 2012).

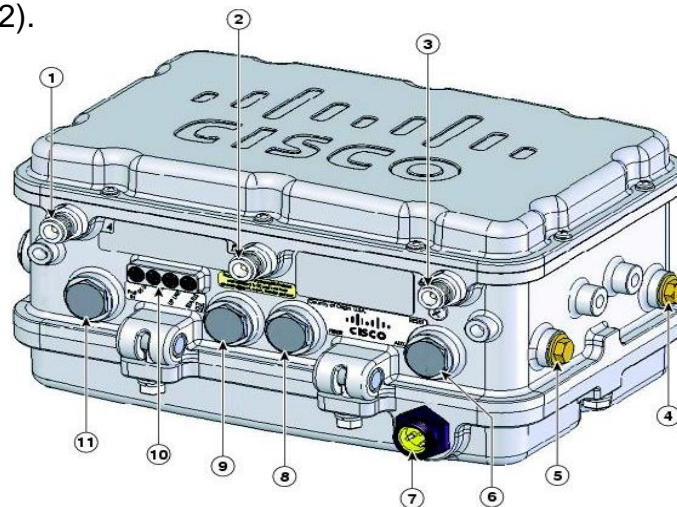


Figura 125. Cisco 1520 Series Mesh Point (Radio Side View)

[http://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/design/guide/MeshAP\\_52.html](http://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/design/guide/MeshAP_52.html)

1	Antenna port 4	7	AC input connector
2	Antenna port 5	8	Fiber port
3	Antenna port 6	9	PoE out port
4	Fiber port (optional)	10	LEDs
5	Cable POC port (optional)	11	PoE in port
6	Aux/Console port		

Tabla 11. Especificaciones del Access Point

### 4.3.5 Aruba Networks



Figura 126. Logo de Aruba Networks

<http://appsuser.net/www/2013/03/26/la-arquitectura-move-de-aruba-networks-logra-la-primer-calificacion-wi-fi-en-el-programa-de-certificacion-lync-de-microsoft/>

*Aruba MeshConfig* es ideal para el despliegue de las pequeñas y medianas redes de malla de tamaño. La herramienta *MeshConfig* basada en navegador ofrece vistas gráficas que hacen que sea fácil de gestionar de forma centralizada, supervisar y solucionar los *routers* de malla, topologías de malla, inventario y fallos.

Con *AirMesh*, municipios, organismos de seguridad pública y de las empresas industriales se benefician de una de las de mayor capacidad y más confiable redes malladas inalámbricas disponibles en la actualidad. Aruba *AirMesh* es probada en muchas de las redes de malla inalámbricas más grandes del mundo.

La solución malla empresarial *Arubasecure* es una manera eficaz de ampliar la cobertura de red para entornos empresariales exteriores e interiores sin necesidad de cables. El uso de malla, puede conectar varias LAN Ethernet o puede ampliar su cobertura inalámbrica. Dado que el tráfico atraviesa a través de puntos de acceso de malla, la red de malla automáticamente reconfigura alrededor rota o caminos bloqueados. Esta característica de auto-sanación proporciona una mayor fiabilidad y redundancia: la red sigue funcionando si un AP deja de funcionar o una conexión falla.

Controladores Aruba ofrecen una configuración centralizada y gestión de los puntos de acceso en un entorno de malla; AP malla locales proporcionan el cifrado y el reenvío de tráfico para los enlaces de malla. En este capítulo se describe la arquitectura de malla empresarial segura Aruba, en los siguientes temas:

Características de la red malla Aruba.

Mesh AP aprenden sobre su entorno cuando arrancan. Malla APs están configurados ya sea como un portal de malla (MPP), un punto de acceso que utiliza su interfaz con cable para llegar al controlador, o un punto de malla (MP), un punto de acceso que establece un camino totalmente inalámbrica al portal de malla. Mesh AP localizar y asociarse con su vecino más cercano, que ofrece el mejor camino hacia el portal de malla. Malla portales y malla puntos también se conocen como nodos de la malla, un término genérico utilizado para describir los puntos de acceso configurados para la malla. (Networks, 2014).

## Hardware Mesh Aruba Networks



Figura 127. Aruba Enrutador MSR 4000  
<http://www.arubanetworks.com/>



128. Aruba Router MST 200  
<http://www.arubanetworks.com/>



Figura 129. Enrutador MSR 1200  
<http://www.arubanetworks.com/>



Figura 130. Aruba Ap-60  
<http://www.arubanetworks.com/>



Figura 131. Aruba Ap-65  
<http://www.arubanetworks.com/>



Figura 132. Aruba Ap-80M  
<http://www.arubanetworks.com/>

#### 4.3.6 Elección del proveedor para el desarrollo de la red Mesh.

En los puntos anteriores se abordaron los principales proveedores de hardware los cuales comparten cualidades muy similares como el manejo dual de bandas además de la gestión RF, y puntos clave como son:

- Modo de funcionamiento
- Aplicación
- Garantía
- Especificaciones de radio
- Certificaciones
- Normativas
- Condiciones ambientales
- Especificaciones de diseño físico
- Montaje e instalación
- Requerimientos eléctricos

Para el desarrollo del diseño de la red Mesh en el parque temático "Las Fuentes" se eligió como proveedor a Aruba Networks por que ofrece una cartera de productos de malla que se ajustan a una variedad de requisitos técnicos y de negocio.

Características de *AirMesh* Aruba Networks.

Aruba *AirMesh* es probada en muchas de las redes de malla inalámbricas más grandes del mundo. Con *AirMesh*, las organizaciones pueden disfrutar de la misma capacidad, fiabilidad y seguridad como las redes cableadas pero con la comodidad y la flexibilidad de la tecnología.

Aruba networks para mantener el costo total de propiedad de la red en su más bajo nivel posible, ofrece un conjunto de herramientas de visualización que simplifican la planificación, despliegue y gestión de Redes *Airmesh*. La herramienta integrada que hace que sea fácil para los integradores de sistemas diseñar redes de malla inalámbrica al aire libre. Ofreciendo inigualable visibilidad en el entorno de RF, el aire libre RF Aruba *Planner* permite a los integradores de sistemas elaborar inalámbrico precisa malla de planes de despliegue que cumplen el negocio específico y requisitos técnicos de sus clientes. (Networks, Aec Networks, 2012).

La diferencia Aruba: Rendimiento y escalabilidad sin precedentes con inteligente enrutamiento de nivel 3, enorme capacidad con un multi-Radio Arquitectura 802.11n, gestión de tráfico avanzada y calidad de servicio para múltiples aplicaciones y grupos de usuarios, hardware para soportar extrema rigidez de condiciones ambientales. Malla de apoyo radios de software configurable *backhaul* y acceso Wi-Fi con flexibles selección de frecuencia (2,4 GHz y 5 GHz o 4.9 GHz).

## 4.4 Elementos que integran una red Wireless Mesh

Una red inalámbrica Wireless mesh está conformada de los siguientes elementos que se describirán a continuación cabe destacar que este tipo de redes va dirigido a espacios públicos lugares donde no se puede instalar una infraestructura muy compleja.

### 4.4.1 Servidor DHCP

Administra direcciones IP: El servidor DHCP controla una serie de direcciones IP y las asigna a los clientes, ya sea de forma permanente o durante un periodo determinado. El servidor utiliza un mecanismo de permiso para determinar durante cuánto tiempo un cliente puede utilizar una dirección que no sea permanente. Cuando se deja de utilizar la dirección, se devuelve a la agrupación y se puede volver a asignar. El servidor contiene información sobre la vinculación de direcciones IP a los clientes de sus tablas de red DHCP, con lo cual se garantiza que no haya más de un cliente que utilice la misma red.

Configura la red para los clientes: El servidor asigna una dirección IP y proporciona otra información para la configuración de red, como un nombre de host, una dirección de emisión, una máscara de subred, un portal predeterminado, un servicio de nombres y mucha otra información. La información de configuración de red se obtiene de la base de datos *dhcptab* del servidor.

El servidor DHCP también se puede configurar para llevar a cabo las siguientes funciones adicionales:

Responder a las solicitudes de clientes *BOOTP*: el servidor escucha las emisiones de los clientes *BOOTP* en las que se descubre un servidor *BOOTP* y les proporciona una dirección IP y los parámetros de inicio. Un administrador debe configurar la información de modo estático. El servidor DHCP puede actuar como servidor *BOOTP* y como servidor DHCP de forma simultánea.

Reenviar solicitudes: El servidor reenvía solicitudes de *BOOTP* y DHCP a los servidores pertinentes de otras subredes. El servidor no puede proporcionar el servicio DHCP o *BOOTP* cuando está configurado como agente de reenvío de *BOOTP*.

Proporcionar compatibilidad con inicio de red para los clientes DHCP: el servidor puede proporcionar a los clientes DHCP la información necesaria para iniciar desde la red: una dirección IP, los parámetros de inicio y la información de configuración de la red. El servidor también puede proporcionar la información que necesitan los clientes DHCP para iniciar e instalar una red de área extensa

(WAN). Actualizar las tablas DNS para los clientes que proporcionan un nombre de host: Para los clientes que proporcionan un valor y una opción *Hostname* en sus solicitudes para el servicio DHCP, el servidor puede tratar de actualizar DNS en su lugar. (Oracle, 2008)

#### **4.4.2 Servidor *Radius***

Un servidor RADIUS gestiona el acceso a las redes. Se utiliza principalmente por los proveedores de servicios de Internet para gestionar acceso a Internet a sus clientes. El nombre RADIUS es en realidad un acrónimo de "*Remote Authentication Dial In User Service*" (Dial de autenticación remoto para acceso a servicios). El protocolo no sólo logra acceso a la red, sino también a la gestión de cuentas del usuario.

Objetivo: Las funciones de un servidor *RADIUS* se resumen con las siglas "AAA" que significan: Autenticación, Autorización y Anotación. Los hacedores de servidores no reciben conexiones directas de los clientes sino que interactúan con las aplicaciones del cliente en otros equipos de la red.

Autenticación: El primer contacto del cliente es con el servidor de acceso remoto o RAS. El RAS actúa como una puerta de entrada al servidor. Antes de admitir el usuario a la red, se comunica con el servidor *RADIUS* para comprobar que el nombre de usuario y la contraseña presentada por el usuario sean correctas. Opcionalmente, el procedimiento de autenticar puede incluir comprobar la dirección de red del usuario o el número de teléfono de llamada para verificar si se trata de los detalles esperados para ese usuario. La adición de una dirección en la autenticación sin embargo, restringe el acceso del usuario a una ubicación. El servidor *RADIUS* tiene un "secreto compartido" que el equipo que intenta conectarse también debería tener almacenado. Esto es por lo general en la forma de un sistema de cifrado. El servidor *RADIUS* devuelve una frase de comprobación de la RAS, el cual lo reenvía a la computadora del usuario. El usuario entonces encripta la frase, al igual que el servidor *RADIUS*. Si la respuesta devuelta por el usuario coincide con la frase de cifrado en el servidor *RADIUS*, el usuario ha demostrado su identidad.

Autorización: El servidor *RADIUS* mantiene una lista de direcciones de protocolo en Internet e instruye al RAS para asignar al cliente como parte del proceso de autorización. ISP no tiene tantas direcciones IP como clientes. Cada computadora conectada a Internet tiene que tener una dirección IP. Todos los paquetes de datos de solicitud que se envían a los servidores deben llevar la dirección IP de ese cliente para que el servidor sepa dónde enviar la respuesta. Sin embargo, el cliente no tiene que tener la misma dirección IP a perpetuidad, sólo por la duración de una sesión.

Anotación: Las funciones de contabilidad del servidor *RADIUS* permiten al ISP ofrecer diferentes niveles de servicio a diferentes clientes que pagan diferentes tasas. La función principal de los procedimientos de anotación de *RADIUS* es para registrar la longitud de tiempo que el cliente está conectado. Una vez completados los procesos de autenticación y autorización, el servidor de acceso envía un mensaje de inicio al servidor *RADIUS*. Cuando el usuario cierra la sesión, el servidor de acceso envía un mensaje de detención. El servidor *RADIUS* registra el período de tiempo entre el inicio y detiene los mensajes para cada sesión de cada usuario. (Galdames, 2012)

#### 4.4.3 Servidor FTP

Un servidor FTP en sus siglas significa “*File Transfer Protocol*”, Protocolo para la Transferencia de Archivos. Un servidor FTP es un programa especial que se ejecuta en un servidor conectado normalmente en Internet (aunque puede estar conectado en otros tipos de redes, LAN, MAN, etc.). La función del mismo es permitir el desplazamiento de datos entre diferentes servidores u ordenadores. Para entenderlo mejor, podemos ver un ejemplo gráfico que hemos preparado a continuación:

Observamos que intervienen tres elementos:

- El servidor FTP, donde subiremos / descargaremos los archivos.
- Usuario 1, es el usuario que en este ejemplo, sube un archivo al servidor FTP.
- Usuario 2, es el usuario que en este ejemplo, se descarga el archivo subido por el usuario 1 y a continuación sube otro archivo.

Un caso práctico son los usos son múltiples, por ejemplo en el caso de los clientes de CDmon.com, usan los servidores FTP para subir sus páginas web y su contenido a Internet.

Ejemplos:

- Como servidor para compartir archivos de imágenes para fotógrafos y sus clientes; de esta manera se ahorran tener que ir hasta la tienda para dejarles los archivos.



- Como servidor de *backup* (copia de seguridad) de los archivos importantes que pueda tener una empresa. Para ello, existen protocolos de comunicación FTP para que los datos viajen encriptados, como el SFTP (*Secure File Transfer Protocol*).
- Para establecer una conexión a un servidor FTP se realiza mediante otros programas llamados Clientes de FTP. Existen múltiples clientes FTP en Internet, hay gratuitos y de pago. (Behrouz, 2011)

#### **4.4.4 Servidor NOS**

El sistema operativo de red, de igual manera es también llamado NOS (del inglés, *Network Operating System*) permite la interconexión de ordenadores para poder acceder a los servicios y recursos. Al igual que un equipo no puede trabajar sin un sistema operativo, una red de equipos no puede funcionar sin un sistema operativo de red.

Si no se dispone de ningún sistema operativo de red, el equipo, no puede compartir recursos y los usuarios no podrán utilizar estos recursos. Un servidor es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes. Un servidor es un sistema informático que consta de un hardware y unas características especiales que son las que lo diferencian a los domésticos, este hardware es más preciso y soporta tareas más complejas. Entre otras características permite sustituir componentes dañados sin la necesidad de apagar el sistema para llevar a cabo el mantenimiento.

Se requiere un software para poder controlar el hardware, utilizarlo al 100% y que permita el mantenimiento el máximo de estabilidad. El software está enfocado a ofrecer uno o varios servicios, estos servicios pueden estar diseñados para ofrecer funcionalidades de red o en muchos casos ofrecer funcionalidades para los usuarios de la red.

Un servidor NOS puede ser utilizado o aplicado en muchos lugares por ejemplo en la administración de la red de una empresa, un negocio de internet (cyber), o incluso en el hogar en caso de tener varios equipos y se requiera administrar los recursos del equipo o del internet y mantener un estable funcionamiento. (Atribution, 2015)

#### 4.4.5 Puerta de Enlace Gateway

Una puerta de enlace es considerada un dispositivo que permite interconectar redes de computadoras con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red inicial, al protocolo usado en la red de destino.

La puerta de enlace es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones de red (*Network Address Translation*, NAT). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada enmascaramiento de IP (*IP Masquerading*), usada muy a menudo para dar acceso a Internet a los equipos de una LAN compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa.

La dirección IP de una puerta de enlace a menudo se parece a 192.168.1.1 o 192.168.0.1 y utiliza algunos rangos predefinidos, 127.x.x.x, 10.x.x.x, 192.x.x.x, que engloban o se reservan a las redes locales.

Un equipo que haga de puerta de enlace en una red debe tener necesariamente dos tarjetas de red (*Network Interface Card*, NIC). La puerta de enlace predeterminada (default Gateway) es la ruta por defecto que se le asigna a un equipo y tiene como función enviar cualquier paquete del que no conozca por cuál interfaz enviarlo y no esté definido en las rutas del equipo, enviando el paquete por la ruta predeterminada. En entornos domésticos, se usan los routers ADSL como puertas de enlace para conectar la red local doméstica con Internet; aunque esta puerta de enlace no conecta dos redes con protocolos diferentes, sí que hace posible conectar dos redes independientes haciendo uso de NAT. (Commons, 2015)

#### 4.4.6 Access Point

Un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos. Muchos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "*roaming*". (Por otro lado, una red donde los dispositivos cliente se administran a sí mismos - sin la necesidad de un punto de acceso - se convierte en una red ad-hoc). Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados.

Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada. Un único punto de

acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. Este o su antena son normalmente colocados en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada. El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: *Network Operating System*) y las ondas, mediante una antena inalámbrica. (Redes, 2013)

#### **4.4.7 Router Mesh**

Un router inalámbrico o *ruteador* inalámbrico es un dispositivo que realiza las funciones de un router, pero también incluye las funciones de un punto de acceso inalámbrico. Se utiliza comúnmente para proporcionar acceso a Internet o a una red informática. No se requiere un enlace por cable, ya que la conexión se realiza sin cables, a través de ondas de radio. Puede funcionar en una LAN cableada (local área network), en una LAN sólo-inalámbrica (WLAN), o en una red mixta cableada/inalámbrica, dependiendo del fabricante y el modelo.

Router traducido significa *ruteador* lo que podemos interpretar como simplemente guía. Se trata de un dispositivo utilizado en redes inalámbricas de área local (WLAN - *Wireless Local Area Network*), una red local inalámbrica es aquella que cuenta con una interconexión de computadoras relativamente cercanas, sin necesidad de cables, estas redes funcionan a base de ondas de radio específicas. El Router permite la interconexión de redes inalámbricas y su función es la de guiar los paquetes de datos para que fluyen hacia la red correcta e ir determinando que caminos debe seguir para llegar a su destino, básicamente se utiliza para servicios de Internet, los cuáles recibe de otro dispositivo como un módem inalámbrico de un proveedor. (Mesh, 2015)

### **4.5 Estrategias de diseño para las redes en malla.**

Para poder diseñar una red se deben tomar en cuenta diversas estrategias para llevar a cabo un diseño óptimo y eficiente, una ella es la cobertura el posicionamiento de la infraestructura para cubrir la demanda del lugar se debe tener en cuenta los diversos tipos de escenarios los cuales pueden ser zonas rurales o urbanas. (Cañarte, 2009)

#### **4.5.1 Diseño enfocado a la cobertura**

La cobertura de red es la señal que recibe el terminal o dispositivo que estás utilizando para comunicarte. Además, la cobertura comprende el área geográfica en la cual se dispone de un determinado servicio, ya sea de voz o de datos.

Es importante indicar que algunos factores pueden afectar al nivel de cobertura que podemos obtener. Los factores más importantes a tener en cuenta son:

- Distancia al Ap más cercano: Uno de los factores que influyen en la cobertura es la distancia a la que estemos del Ap, ya que cuanto mayor sea la distancia, tendremos menos señal en nuestro terminal.
- Propagación y obstáculos: La cobertura se produce mediante ondas y de modo que cualquier obstáculo del terreno que esté situado entre el dispositivo y el *access point* puede afectar a la cobertura.
- Ubicación interior o exterior: Por regla general, la cobertura suele ser peor en el interior de edificios que en el exterior.
- Tipo de dispositivo: No todos tienen la misma calidad. Además, cualquier golpe o accidente puede afectar negativamente a su normal funcionamiento. (Cañarte, 2009)

#### 4.5.1.1 Propagación de radio frecuencias en distintos escenarios

La implantación de una red en malla conlleva los siguientes los siguientes escenarios:

- Propagación en el espacio libre: Todo sistema de telecomunicación debe diseñarse para que en el receptor se obtenga una relación señal-ruido mínima que garantice su funcionamiento. Los servicios de radiocomunicaciones, radiodifusión, radiolocalización (radar), teledetección y radio ayudas a la navegación tienen en común el empleo de ondas electromagnéticas radiadas como soporte de la transmisión de información entre el transmisor y el receptor.
- Entorno terrestre: La tierra perturba la propagación de las ondas electromagnéticas, de forma que al establecer cualquier tipo de radiocomunicación en el entorno terrestre aparecerán una serie de fenómenos que modificarán las condiciones ideales de propagación en el vacío. Estos fenómenos son básicamente tres: onda de superficie, difracción y formación de la onda de espacio.



Figura 133. Propagación de señal WiFi  
<http://www.tido.es/blog/>

#### **4.5.1.2 Zonas de cobertura para enlaces de conexión.**

El índice de cobertura que proporcionara la red involucran en gran cantidad el número de *access point* que se hayan designado para el área del servicio, además tener en cuenta las condiciones ideales para obtener el mejor desempeño de nuestros dispositivos y tener un servicio eficiente.

#### **4.5.1.3 Posicionamiento adecuado de los *access point*.**

Debe llevarse a cabo una correcta instalación de puntos de acceso para que existan enlaces óptimos.

Los lugares más recurrentes para implantar puntos de acceso son paredes tejados, mástil, o techos.

Aspectos que se deben tomar para implantar un punto de acceso como es el suministro de energía debe ser continuo según las especificaciones del producto.

El lugar donde estará ubicado deberá ser sólido y seguro para su correcta instalación, resistente a condiciones climáticas, seguro para evitar daños de alteraciones o vandalismo, adecuado para evitar daños accidentales.

#### **4.5.1.4 Factores de una red de infraestructura.**

- Se debe tener bien claro el escenario de despliegue.
- La densidad de los puntos de acceso.
- Cantidad de usuarios móviles.
- Aplicaciones y servicios que brindara la red.
- Consideración del ancho de banda.

Una herramienta útil de bosquejo es un mapa de área geográfica para establecer el posicionamiento de los puntos de acceso y cobertura que brindaran.

#### **4.5.2 Diseño enfocado a la disponibilidad**

Disponibilidad de Access Point, Router, Gateway cada uno de ellos es de suma importancia para el óptimo funcionamiento de la red, si alguno de estos falla en caso:

- De ser un *access point* automáticamente el enlace debe ser re direccionado al punto de acceso más cercano y así el usuario continúe comunicado.
- En el caso del router la falla de este significaría el nulo funcionamiento de los puntos de acceso por ello un segundo router

existente de manera que estos puedan trabajar en conjunto con el Gateway así garantizando una conexión fija y confiable.

- Con respecto al Gateway se deberá tener uno extra ya configurado si se presenta falla poder cambiarlo manualmente así mismo que la red continúe operando.

#### 4.5.3 Diseño enfocado al desempeño

La velocidad en que se transmiten los datos por segundo a través de la red, la rapidez de subida y descarga de datos, Tomando en cuenta puntos clave como son:

- La tasa de transferencia se refiere a la velocidad con la cual podemos transferir información y se mide en bits / seg, es común llamar ancho de banda a la capacidad de transferir información, sin embargo, no se puede conocer los bits / seg si se cuenta exclusivamente con el ancho de banda, ya que hay que considerar la modulación empleada.
- La latencia Relacionado con el tiempo que toma un bit de viajar de un extremo de un medio al otro. Depende de tres factores: Tiempo de propagación del bit por el medio, que depende del tiempo de propagación de la corriente o luz por el medio, además de la distancia recorrida. Máxima cantidad de datos que pueden ser transmitidos por la red sin segmentarse. Al tiempo de propagación del bit en un paquete se le llama tiempo de transmisión. Tiempos de espera para difundirse un paquete a través de un conmutador, además del tráfico de la red. A este tiempo se le denomina tiempo de cola. (Cañarte, 2009)



Figura 134. Desempeño de una red Mesh  
<http://winnerscash.com/internet-marketing-y-redes-sociales/>

#### **4.5.4 Diseño enfocado en la movilidad**

El brindar movilidad al usuario es mantener la conexión en todo momento, el posicionamiento y cobertura van de la mano para mantener movilidad y evitar las (zonas muertas) que evitan al usuario seguir conectado.

#### **4.5.5 Diseño enfocado a la seguridad**

El manejo de información es una ventana importante para lo cual mantener la integridad de los mismos es fundamental, el manejo de una red pública no es totalmente confiable, se llevan a cabo mecanismos de seguridad como es el cifrado de datos, túneles y autenticación.

#### **4.5.6 Diseño enfocado en la topología**

A continuación se verán cuáles son las principales características de las WMN que la diferencian de otras topologías de redes:

- **Redundantes:** Los nodos están conectados unos con otros por varias rutas, de esta manera se obtienen rutas redundantes. Si una ruta falla habrá otra que se encargue de transmitir los datos.
- **Fácil Despliegue:** Al tener capacidad de autoconfiguración (ruteo y selección de canal dinámica), ante situaciones de emergencia o catástrofes permiten dar soluciones de conectividad.
- **Auto-regenerables y auto-configurables:** permiten la auto-reparación de rutas, por trabajar con protocolos de última generación Mesh, permiten descubrir nuevos nodos admitiéndolos en la comunidad ya existente y regenerando nuevas tablas de enrutamiento.
- **Robustez:** por el tipo de enrutamiento que se aplica se obtiene una gran estabilidad en cuanto a condiciones variables o en alguna falla de un nodo en particular.
- **Mayor capacidad a bajo coste:** hay estudios que han demostrado que la capacidad de una red inalámbrica puede ser mejorada mediante la utilización de repetidores, existiendo un compromiso entre distancia e interferencia entre nodos. (Cañarte, 2009)

## 4.6 Simulación de la Red Mesh

Estos son algunos de los términos más utilizados en la simulación de una red:

- Red conjunto de nodos y computadoras que pueden comunicarse los unos con los otros, en nuestro caso de forma inalámbrica mediante una red Mesh.
- Puerta de enlace: Se le llama así al nodo que está conectado a internet a través del modem router del proveedor de acceso.
- Repetidor: Es el nodo que repite la señal de los *gateways*.
- Nodo: Con este nombre se designa tanto a los *gateways* como a los repetidores.

El parque temático municipal las fuentes está ubicado en Av. Bordo de Xochica y Av. Nezahualcóyotl Municipio de Nezahualcóyotl frente a la plaza Telmex ciudad Jardín. Las coordenadas geográficas del parque son: Latitud 19°25'22.10"N y Longitud 99° 1'28.29"O. El área aproximada del parque temático las fuentes es de 8000 metros cuadrados el parque tiene una afluencia entre semana de 200 personas y los fines a aumenta a un promedio de y 500 visitantes de los cuales un aproximadamente un 75% cuentan con un dispositivo de conexión WiFi. (Nezahualcoyolt, 2009)

Condiciones Generales	
<b>Cantidad de nodos</b>	<b>18</b>
<b>Estándar inalámbrico</b>	<b>a,b,g</b>
<b>Potencia de transmisión por nodo</b>	<b>20 dBm</b>
<b>Sistema operativo</b>	<b>Air Wave 7.7</b>
<b>Canal inalámbrico</b>	<b>11,6</b>
<b>Protocolo</b>	<b>OLSR</b>
<b>ESSID</b>	<b>Mesh-Parque</b>
<b>Tipo de antena</b>	<b>Omnidireccional</b>
<b>Ganancia de antena</b>	<b>5 db</b>

Tabla 12. Condiciones generales de los AP



#### 4.6.1 Ubicación y determinación de los Puntos de Acceso

Para determinar el número de nodos dentro del parque se tomó en cuenta la distribución horizontal de la señal. Dando como resultado un total de 18 nodos distribuidos entre los 8000 metros cuadrados teniendo en cuenta esto los nodos tendrán una distancia entre sí de 15 a 20 metros.

Para la red Mesh del parque temático las fuentes se utilizaran los Access Point Aruba 80M, los cuales se ubicaran en áreas estratégicas en base a estándares de propagación para así poder tener una cobertura óptima en todo el parque.

Ubicación de Puntos de Acceso	
Número de AP	Área de Ubicación
AP 1	Entrada del parque
AP 2	Renta de Coches
AP 3	Módulo de tramite
AP 4	Picnic
AP 5	Fuentes Danzantes
AP 6-13	Ciclo vía
AP 7	Juego de Playa
AP 8-11-15	Palapas
AP 9	Juegos Infantiles
AP 10-12	Juegos Saltarines
AP 14	Gym
AP 16-17-18	Canchas

Tabla 13. Ubicación de los Puntos de Acceso

Ubicación de los Puntos de Acceso



Figura 135. Ubicación de los nodos  
Fuente: Ayuntamiento del Municipio Nezahualcóyotl, Parque  
"Las Fuentes", Edomex 2015

#### 4.6.2 Cobertura de los Access Point

En la siguiente figura se muestra la ubicación de los puntos de acceso y el radio de cobertura que emiten cada uno de ellos. Así como la distancia que puede existir entre cada uno de los AP Aruba 80M.

La de Potencia de emisión del AP Aruba es de 20 dBm /100 Mw\*, cuenta con interfaces hembra de tipo N (1X 2,4 GHz, 1 x 5 GHz) para soporte de antena externa. Todo esto permite una conexión estable entre Access Point a una distancia de 20 metros entre ellos.

Basado en las especificaciones del producto se han definido las distancias ideales en un ambiente al aire libre para asegurar que el enlace de transito tenga su mayor rendimiento.

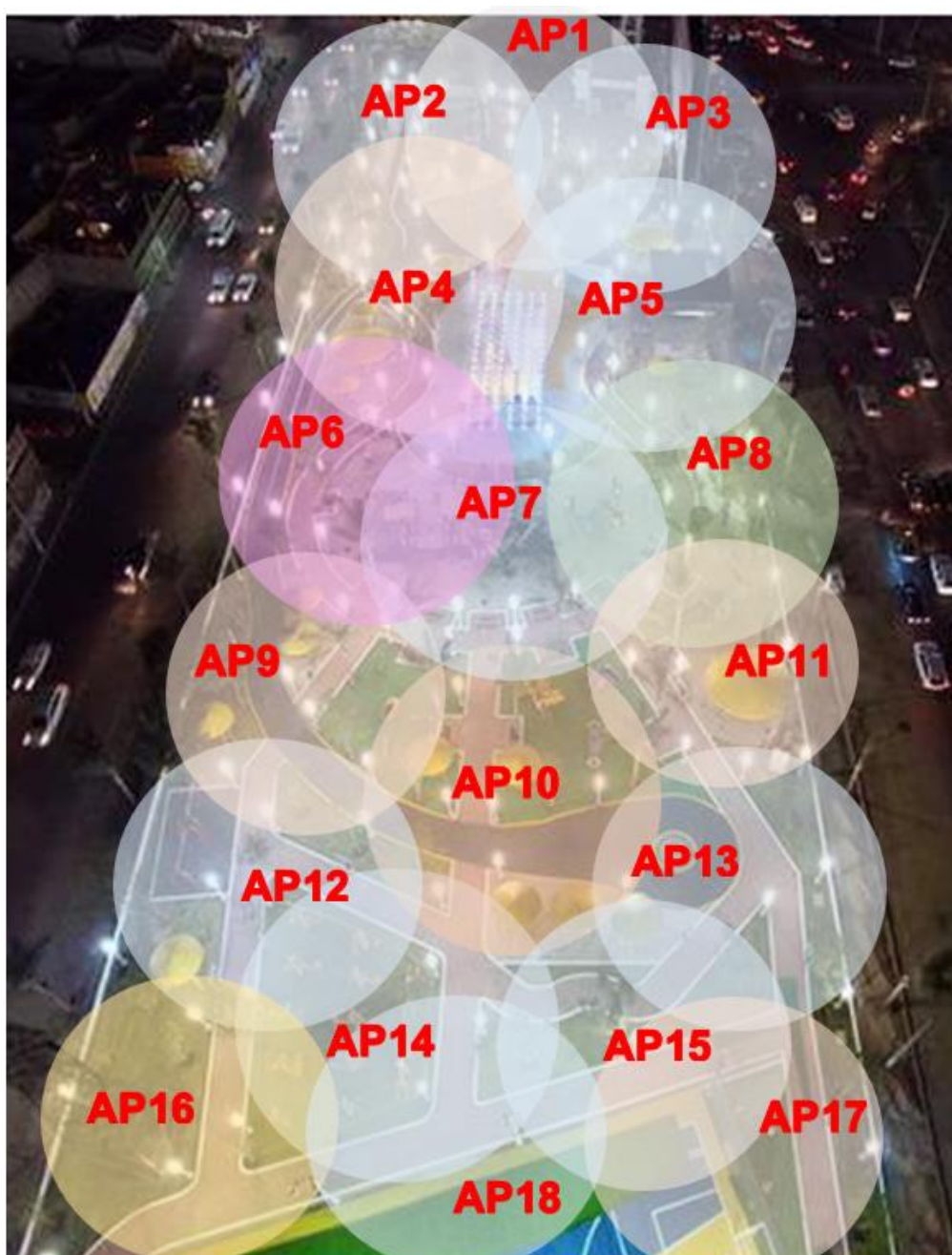


Figura 136. Cobertura de los Access Point  
Fuente: Ayuntamiento del Municipio Nezahualcóyotl, Parque  
“Las Fuentes”. Edomex 2015

### 4.6.3 Estado de los enlaces

Entorno a la ubicación de los *Access point* los enlaces de tránsito que se lograron establecer se puede apreciar la topología Mesh, diseñada enfocada al rendimiento en el parque. De esta manera optimizamos al máximo el manejo de paquetes sin crear cuellos de botellas evitando la saturación de algún punto de acceso por un mal diseño.

Un enlace de acceso marca un paquete con un valor de tipo AC esto quiere decir clase de acceso de una red Mesh, Los paquetes de aplicación tienen cuatro líneas independientes una por cada clase de acceso son capaces de solucionar colisiones internas y así seleccionar las tramas con mayor prioridad para después ser enviadas. Mecanismos de colisión: *Minimum inter-frame space (AIFSN)*, *Contention Window 8CW*.



Figura 137. Enlaces de Tránsito  
Fuente: Ayuntamiento del Municipio Nezahualcóyotl, Parque  
“Las Fuentes”, Edomex 2015

#### 4.6.4 Topología Mesh a implementarse en el Parque

ISP Proveedor de Internet

*Router Wireless*

Controlador de AP

*Access Point*

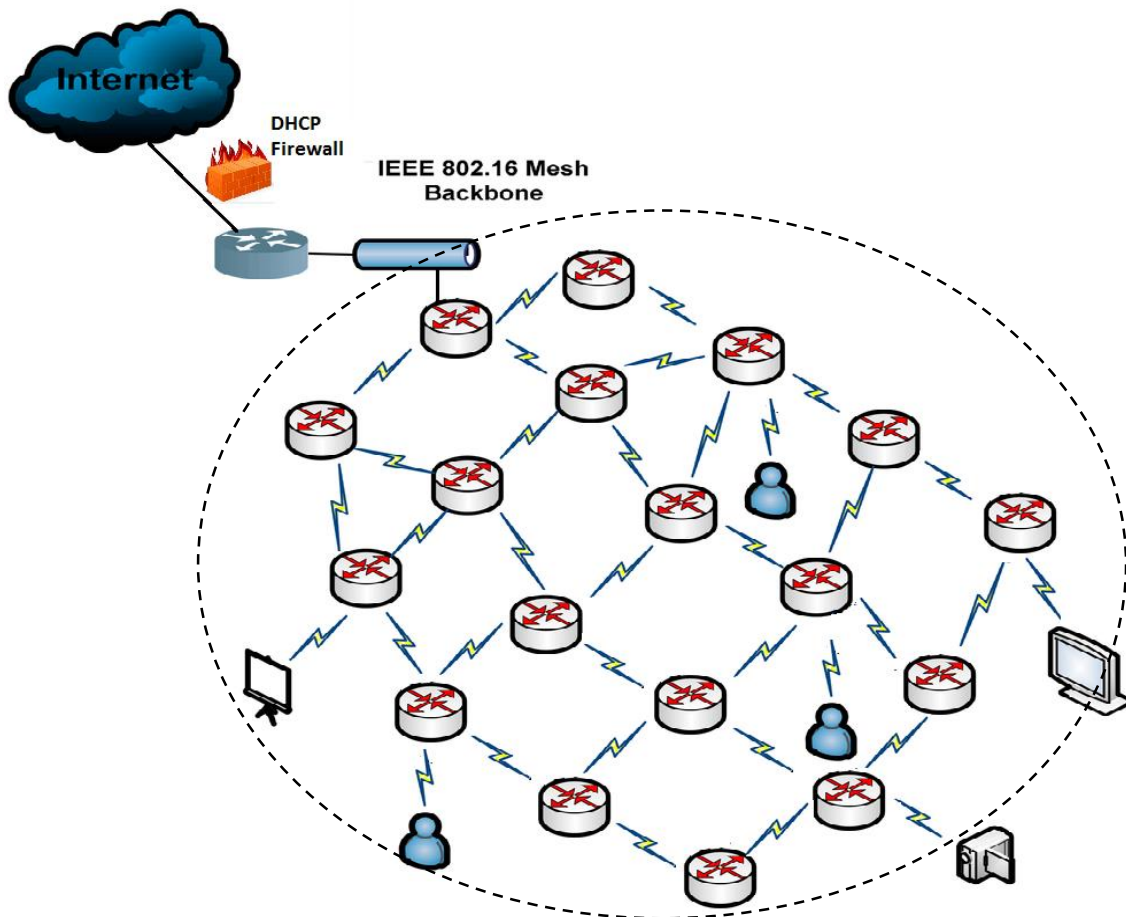


Figura 138. Diagrama de la Red Mesh a implementar  
<http://urlwwwvivianacanomurcia.blogspot.mx/>

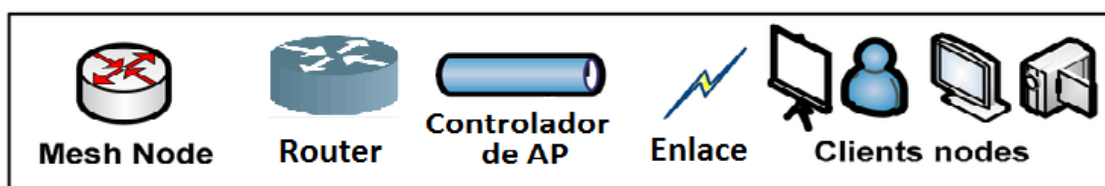


Figura 139. Simbología del diagrama de la Red Mesh  
<http://urlwwwvivianacanomurcia.blogspot.mx/>

#### 4.6.5 Herramienta de Simulación

Dentro de las herramientas que permiten simular redes, pero en este caso admiten hacer un diseño, simulación y evidenciar resultados sobre redes Mesh se tienen las siguientes: como herramienta de simulación y diseño, ofrece resultados y simulaciones efectivas pudiendo así verificar la viabilidad de muchos diseños en una futura implementación. Con esto se podrá analizar los resultados que se quiere obtener al final del proceso. En la simulación de la Red Mesh es necesario cargar varios parámetros, Aplicación y perfiles de los elementos que implica una red Mesh para el Centro Universitario UAEM Texcoco, también se es necesario configurar los equipos que accederán al medio, en este caso las pc y dispositivos móviles.

Lo antes mencionado se logra configurando cada de uno de los dispositivos que se tiene dentro de la simulación, allí se puede modificar, añadir eliminar opciones, haciendo que la simulación se acerca mucho más a su comportamiento natural y en el medio. Dentro de las características disponibles de cada dispositivo que se añaden a está simulación están: la manera en que se distribuyen en la red los canales para permitir acceso al usuario la interconexión entre dispositivos.

Los dispositivos que conforman la simulación de la red Mesh se configuran de tal manera que se puedan evaluar en cuanto a rendimiento para poder evidenciar el comportamiento de la red.

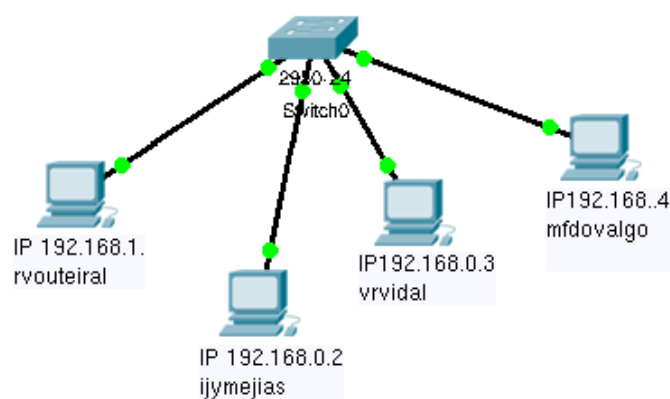


Figura 140. Ejemplo de una Simulación en Packet Tracer  
[http://yolaalvirde.blogspot.com/2013/05/construccion\\_16.html](http://yolaalvirde.blogspot.com/2013/05/construccion_16.html)

##### 4.6.5.1 Simulador *Packet Tracer*

Es un simulador gráfico de redes desarrollado y utilizado por Cisco como herramienta de entrenamiento para obtener la certificación CCNA14. *Packet Tracer* es un simulador de entorno de redes de comunicaciones de fidelidad media, que permite crear topologías de red mediante la selección de los dispositivos y su respectiva ubicación en un área de trabajo<sup>15</sup>, utilizando una interfaz gráfica.



Figura 141. Logo del Software Cisco Packet

<http://www.taringa.net/posts/apuntes-y-monografias/13659518/Cisco-Packet-Tracer-Cap-Material-Ejemplos-Practica-Todo-En-1.html>

Características generales: *Packet Tracer* es un simulador que permite realizar el diseño de topologías, la configuración de dispositivos de red, así como la detección y corrección de errores en sistemas de comunicaciones. Ofrece como ventaja adicional el análisis de cada proceso que se ejecuta en el programa de acuerdo a la capa de modelo OSI que interviene en dicho proceso; razón por la cual es una herramienta de gran ayuda en el estudio y aprendizaje del funcionamiento y configuración de redes de comunicaciones y aplicaciones telemáticas.

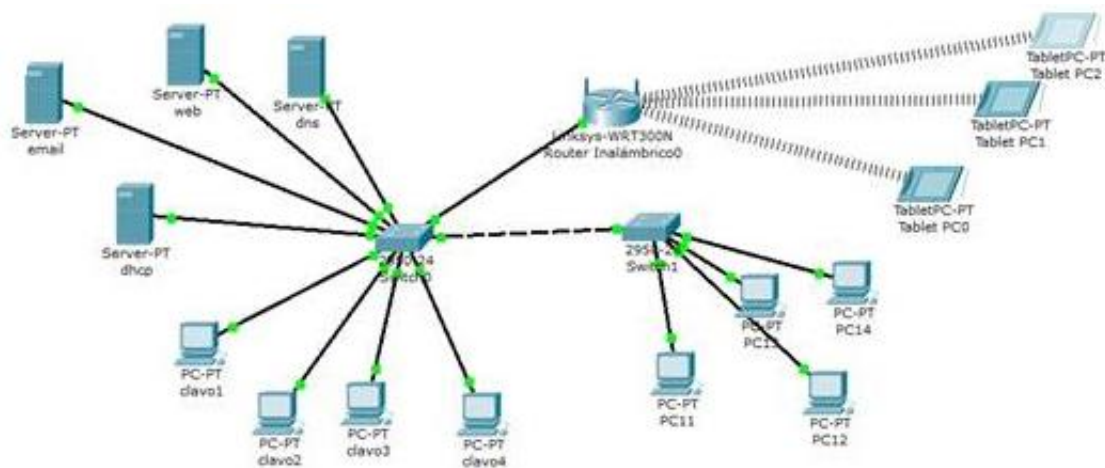


Figura 142. Simulación de una topología de Red

<http://samuel77.bligoo.com.mx/redes-wan>

Requerimientos del sistema. Para una correcta instalación y posterior uso del software de PACKET TRACER

- Sistema Operativo: Microsoft Windows 98/2000, XP, Windows 7 y Macintosh
- Requerimientos mínimos: Procesador Intel Pentium 200 MHz o equivalente, 64 MB RAM, espacio disponible en D.D. 30 MB, Macromedia Flash Player 6.0 o superior, La versión 3.2 de *Packet Tracer* no soporta computadores Macintosh.
- Recomendaciones: Tarjeta de sonido y bocinas.

Interfaz gráfica del usuario. Este software ofrece una interfaz basada en ventanas, que le ofrece al usuario facilidades para el modelado, la descripción, la configuración y la simulación de redes. *Packet Tracer* tiene tres modos de operación, el primero de estos es el modo *topology* (topología), que aparece en la ventana de inicio cuando se abre el programa, el otro es el modo simulación (Simulación), al cual se accede cuando se ha creado el modelo de la red;

Finalmente aparece el modo *realtime* (tiempo real), en donde se pueden programar mensajes SNMP para detectar los dispositivos que están activos en la red y si existen algún problema de direccionamiento o tamaño de tramas entre las conexiones. A continuación se describirá brevemente cada uno de los modos de operación de *Packet Tracer*.

Modo de operación de topología. En el modo "*Topology*", se realizan tres tareas principales, la primera de ellas es el diseño de la red mediante la creación y organización de los dispositivos; por consiguiente en este modo de operación se dispone de un área de trabajo y de un panel de herramientas en donde se encuentran los elementos de red disponibles en *Packet Tracer*.

En segundo lugar, en este modo de operación se realiza la interconexión de los Dispositivos de red del modelo. *Packet Tracer* contiene un menú con gran variedad de tipos de enlaces, los cuales pueden ser seleccionados de acuerdo con el tipo de conexión que se vaya a realizar. En la figura 18 se muestran los tipos de conexiones del programa.



Figura 143. Tipos de conexiones disponibles en Packet Tracer  
<http://webcache.googleusercontent.com/search?q=cache:yft3eihcDbQJ:tutorialesmaneioderedes.blogspot.com/+&cd=1&hl=es-419&ct=clnk&gl=mx>



Modo de operación de simulación. En el modo simulación, se crean y se programan los paquetes que se van a transmitir por la red que previamente se ha modelado. Dentro de este modo de operación se visualiza el proceso de transmisión y recepción de información haciendo uso de un panel de herramientas que contiene los controles para poner en marcha la simulación. Una de las principales características del modo de operación simulación, es que permite desplegar ventanas durante la simulación, en las cuales aparece una breve descripción del proceso de transmisión de los paquetes. (Cisco, Open Boxer, 2010)

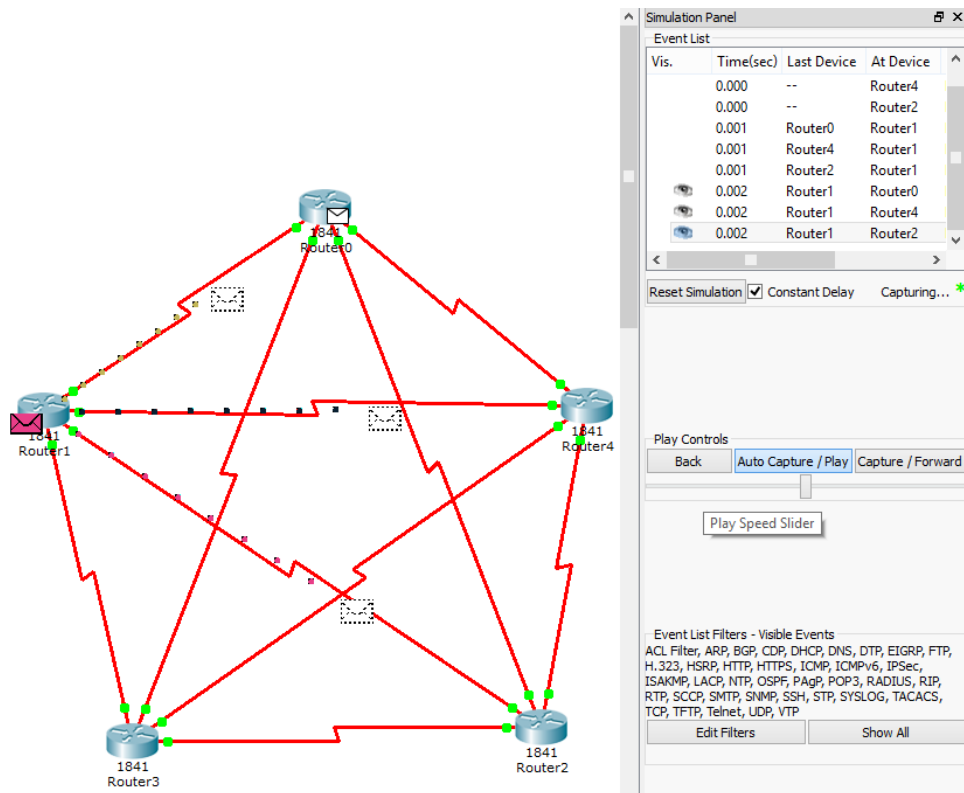


Figura 144. Ventana del modo de operación del envío de paquetes

<https://www.youtube.com/watch?v=u3lpK1X2mFo>

Ventajas: El enfoque pedagógico de este simulador, hace que sea una herramienta muy útil como complemento de los fundamentos teóricos sobre redes de comunicaciones. El programa posee una interfaz de usuario muy fácil de manejar, e incluyendo documentación y tutoriales sobre el manejo del mismo. Desventajas: Es un software propietario, y por ende se debe pagar una licencia para instalarlo. Solo permite modelar redes en términos de filtrado y retransmisión de paquetes.

#### 4.6.5.2 Simulación en Cisco *Packet Tracer*

Pantalla 1: Inicialización del software



Figura 145. Ejecución de Cisco Packet Tracer  
<http://ciscopackettracer.com>

Pantalla 2: Interfaz de inicio

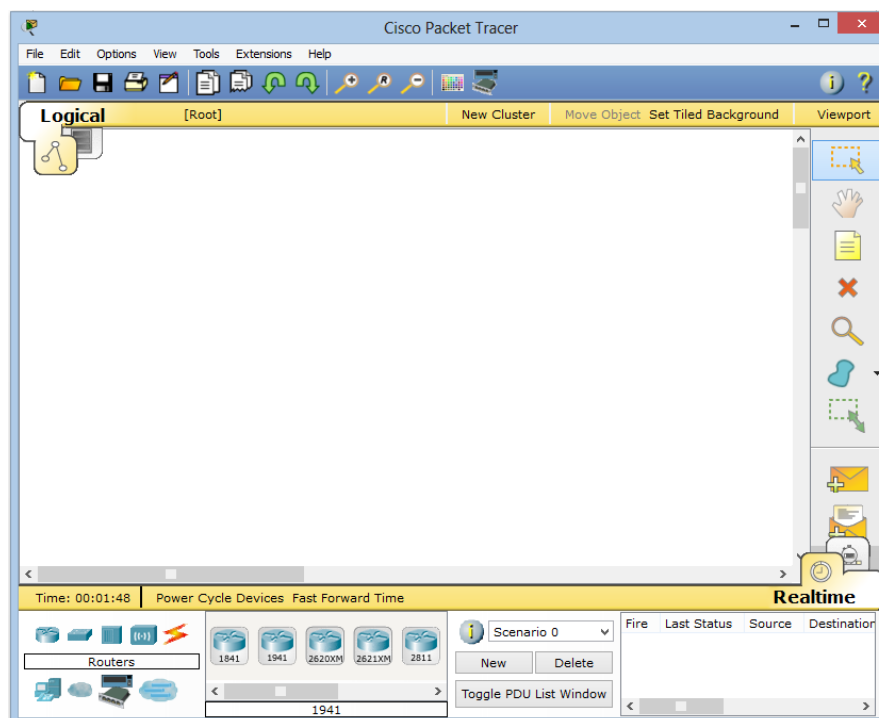


Figura 146. Hoja de trabajo Cisco Packet Tracer  
<http://www.cisco.com>

### 4.6.5.3 Configuración Del Router Maestro

Pantalla 3: En el panel de herramientas de hardware seleccionamos un *lynksys* modelo WRT300N además de una nube modelo Cloud-PT- Empty (Internet), conectándolos con un cable *Copper Straight Through* usando el puerto de internet en el *lynksys* y el puerto Ethernet 6 en la nube.

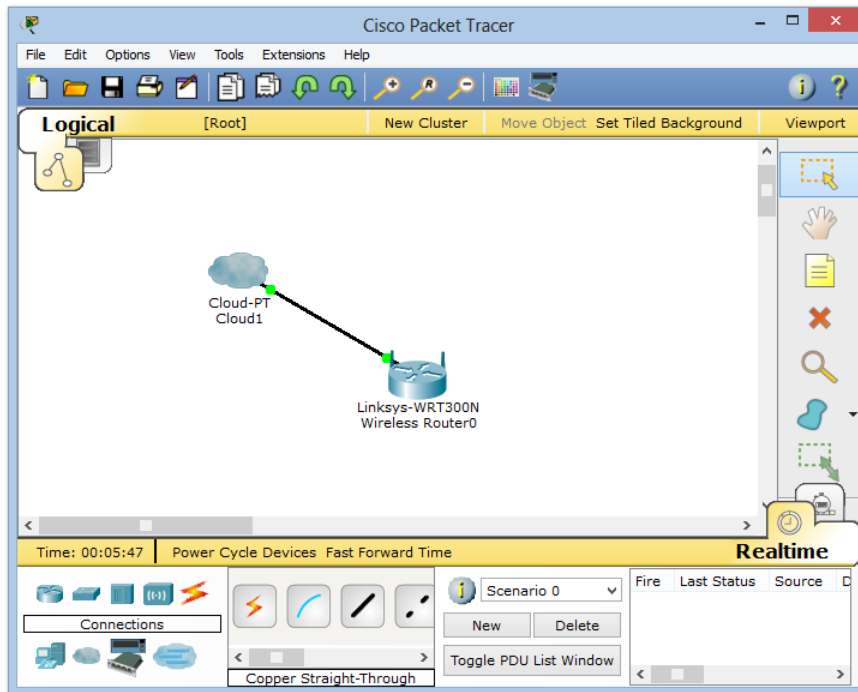


Figura 147. Conexión entre nube y un router.  
<http://www.cisco.com>

Pantalla 4: Configuración del router maestro mediante la interfaz gráfica GUI seleccionamos la pestaña de Internet Setup donde se configura el tipo de IP ya sea estática o dinámica.

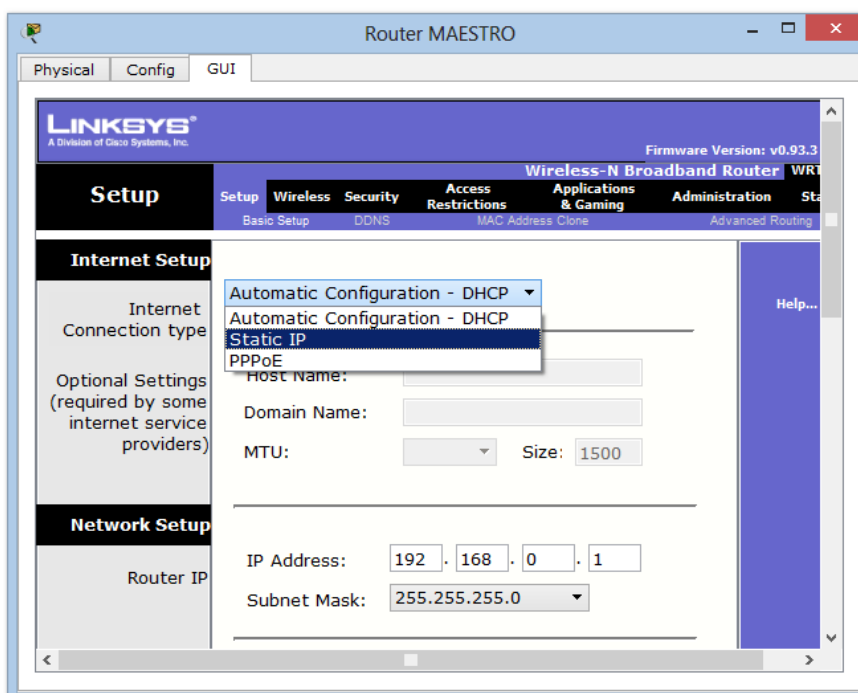


Figura 148. Interfaz GUI  
<http://www.cisco.com>

Pantalla 5: Configuración del *linksys* maestro asignando direcciones IP previamente generadas con el método del subneteo.

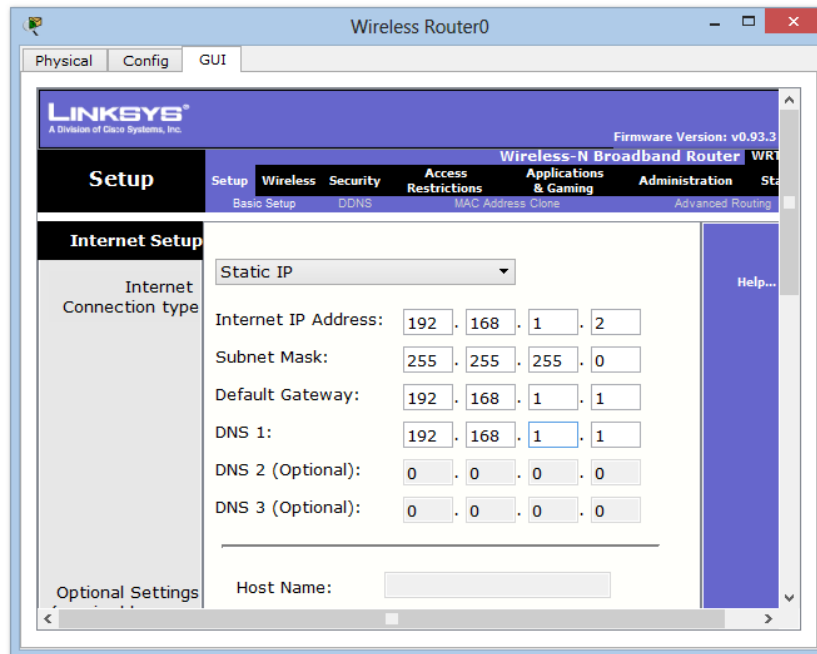


Figura 149. Interfaz de direcciones  
<http://www.cisco.com>

Pantalla 6: Ejemplo de una dirección DNS, para ver dicha dirección debe ingresar en Panel de control/ Redes e internet/ Centro de Redes y Recursos Compartidos/ Ethernet/ Detalles

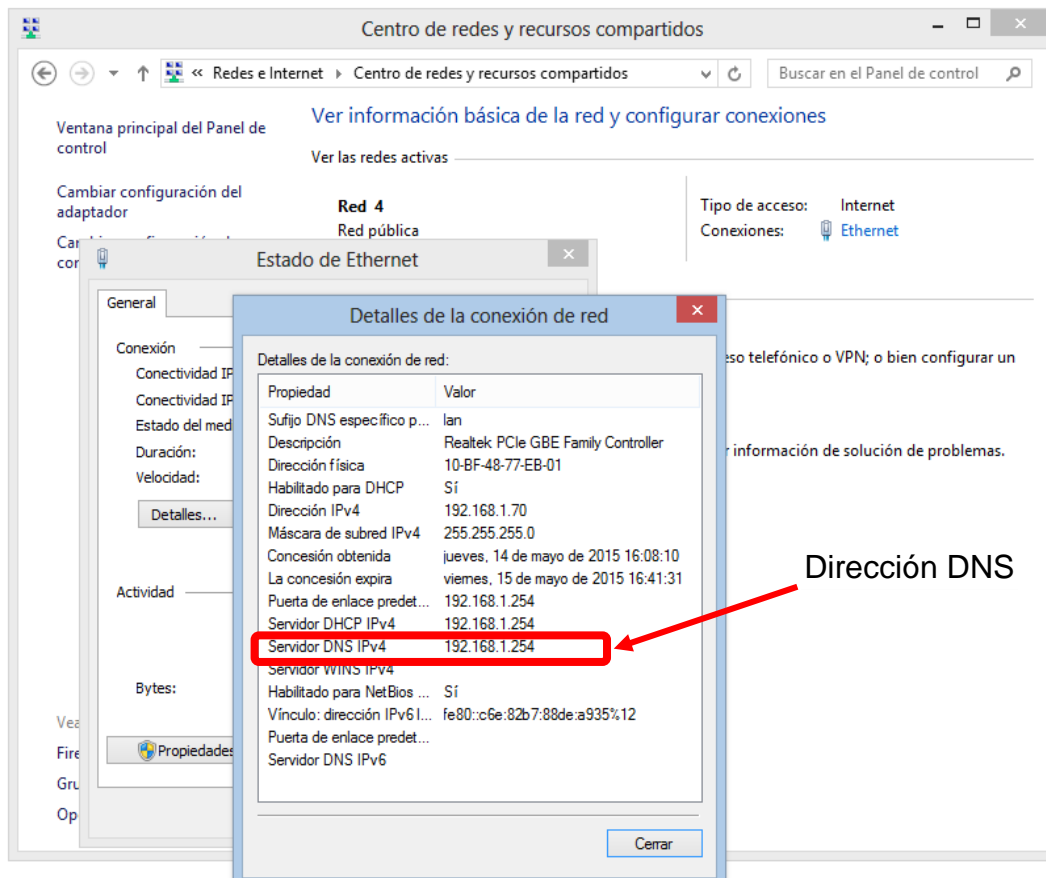


Figura 150. Ventana Detalles de la conexión de red  
<http://www.cisco.com>

Pantalla 7: Conexión de una laptop mediante puertos Ethernet al *linksys* maestro, Una vez configurado el *lynksys* maestro este asigna una dirección IP automáticamente para poder ver dicha IP asignada basta con dar clic en la laptop e ir a la opción de IP configuration.

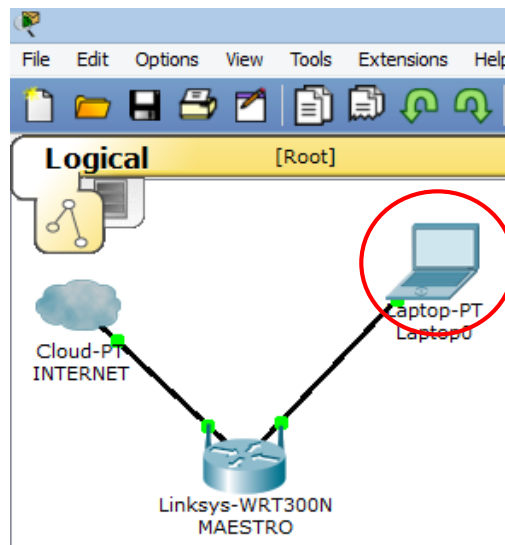


Figura 151. Simulación de conectividad de un usuario  
<http://www.cisco.com>

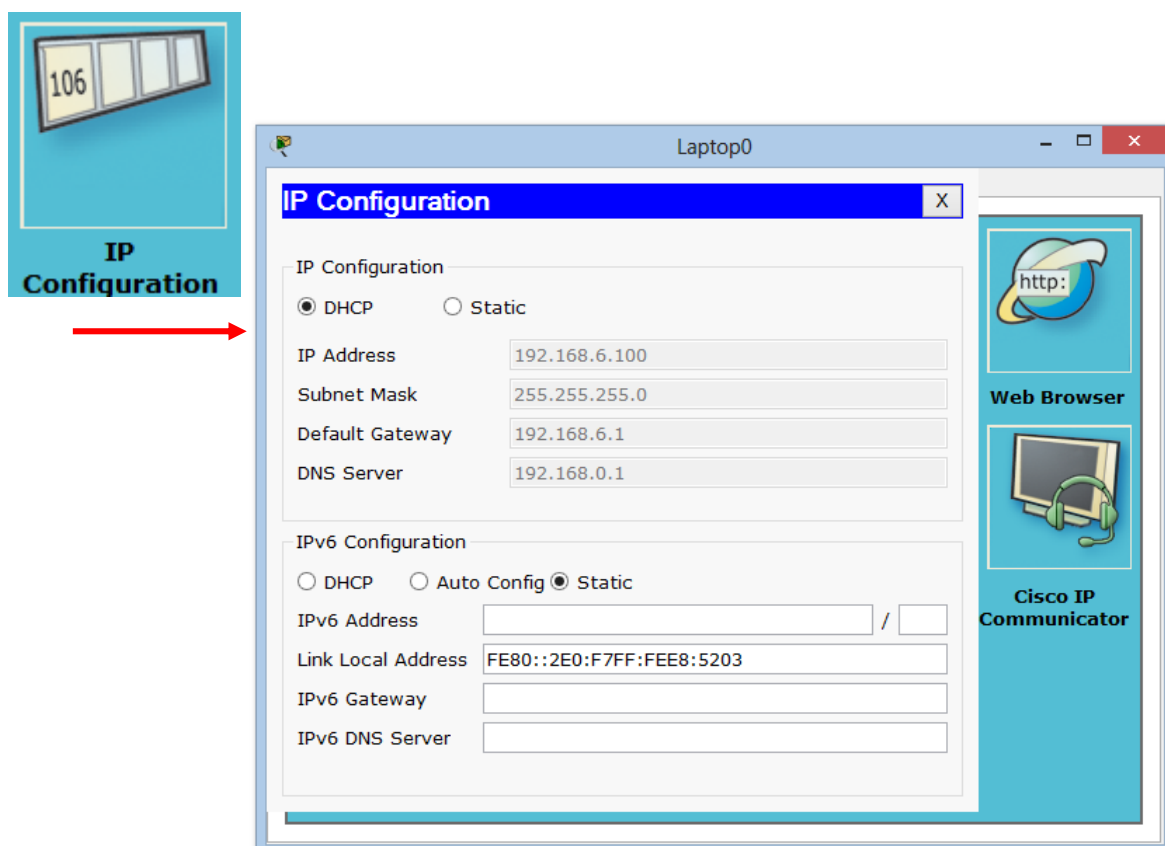


Figura 152. Interfaz de configuración de una laptop en Cisco Packet  
<http://www.cisco.com>

Pantalla 8: Se ingresara al router maestro mediante el web browser digitando la dirección Ip del router en la barra URL y nos direccionara a la ventana de configuración del router. Para ingresar al router maestro es necesario introducir la dirección Ip del router en la barra URL

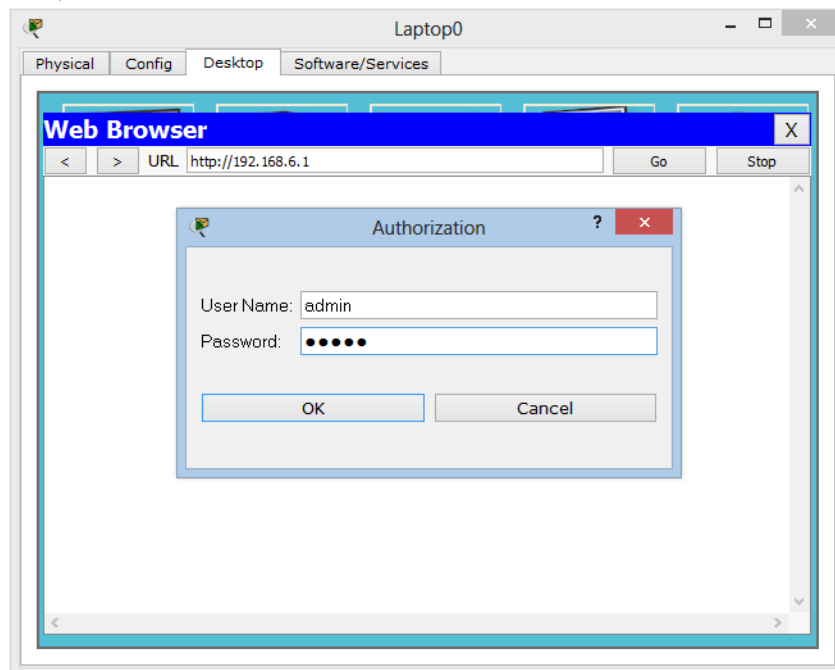
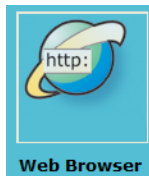


Figura 153. Ventana de autenticación  
<http://www.cisco.com>

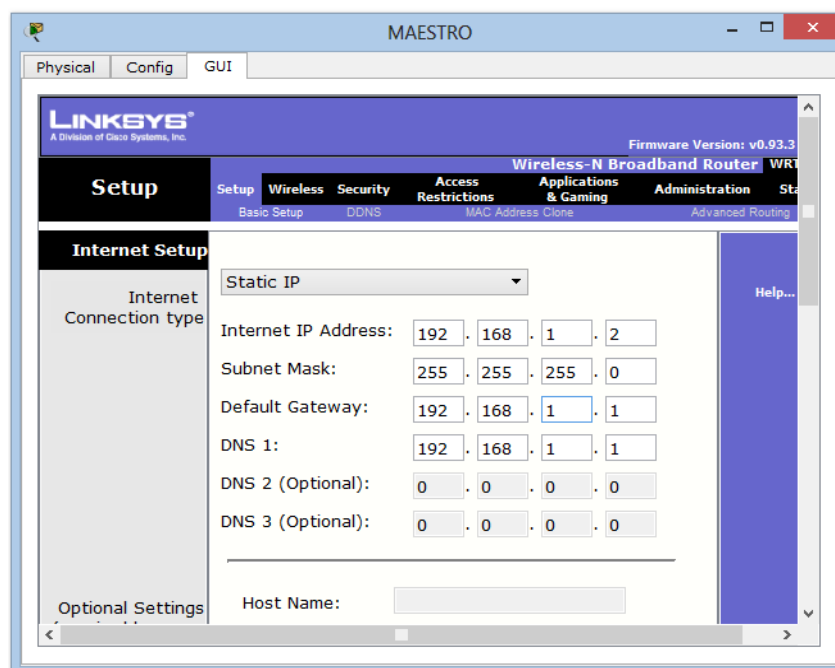


Figura 154. Ventana de setup  
<http://www.cisco.com>

Pantalla 9: Configuración de la máscara de red para 25 clientes, para determinar la máscara utilizando la fórmula  $2^n$  resultando este mayor a 25 en este caso es  $2^5 = 32$  restando  $256 - 32$  dando como resultado 224 siendo este número la máscara de red.

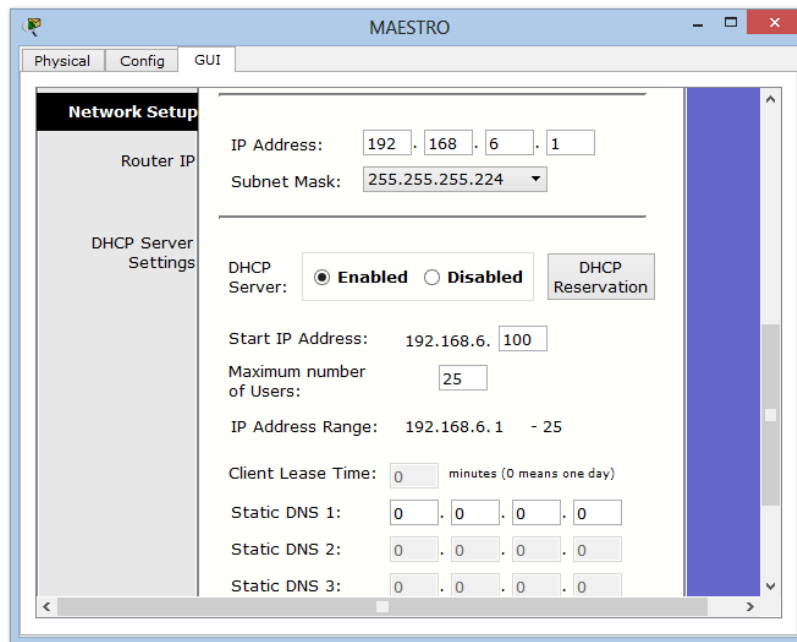


Figura 155. Establecimiento de máscara de red  
<http://www.cisco.com>

#### 4.6.5.4 Configuración del *Linksys* dependiente (Repetidores)

Pantalla 10: En esta pantalla se muestra la configuración se desactiva el modo DHCP (*Disabled*) se asigna un número IP a cada repetidor en este caso es el número 3 y así sucesivamente hasta direccionar los 18 puntos de acceso

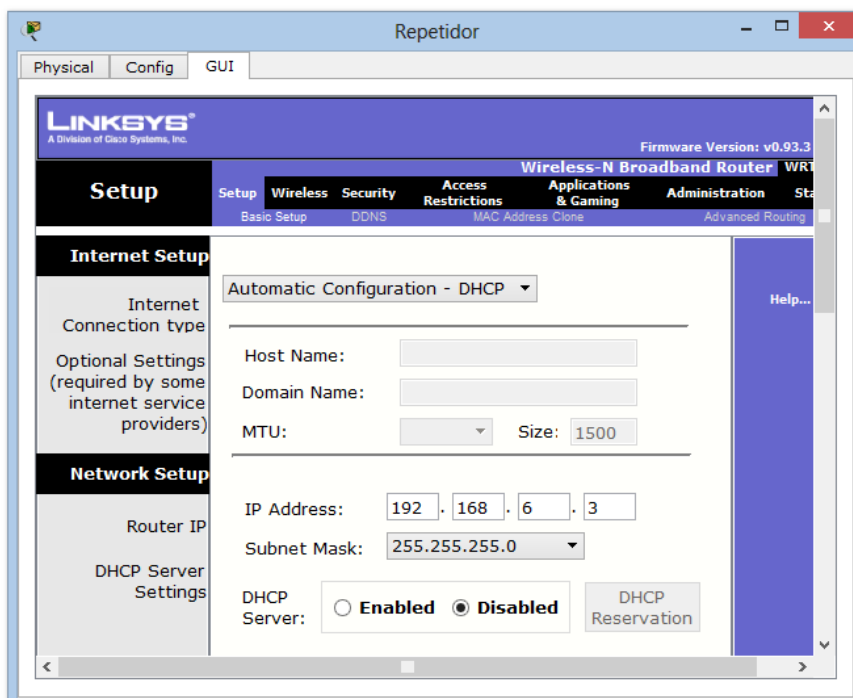


Figura 156. Desactivación del DHCP  
<http://www.cisco.com>

Pantalla 11: Construcción de la topología en malla con repetidores *lynksys*

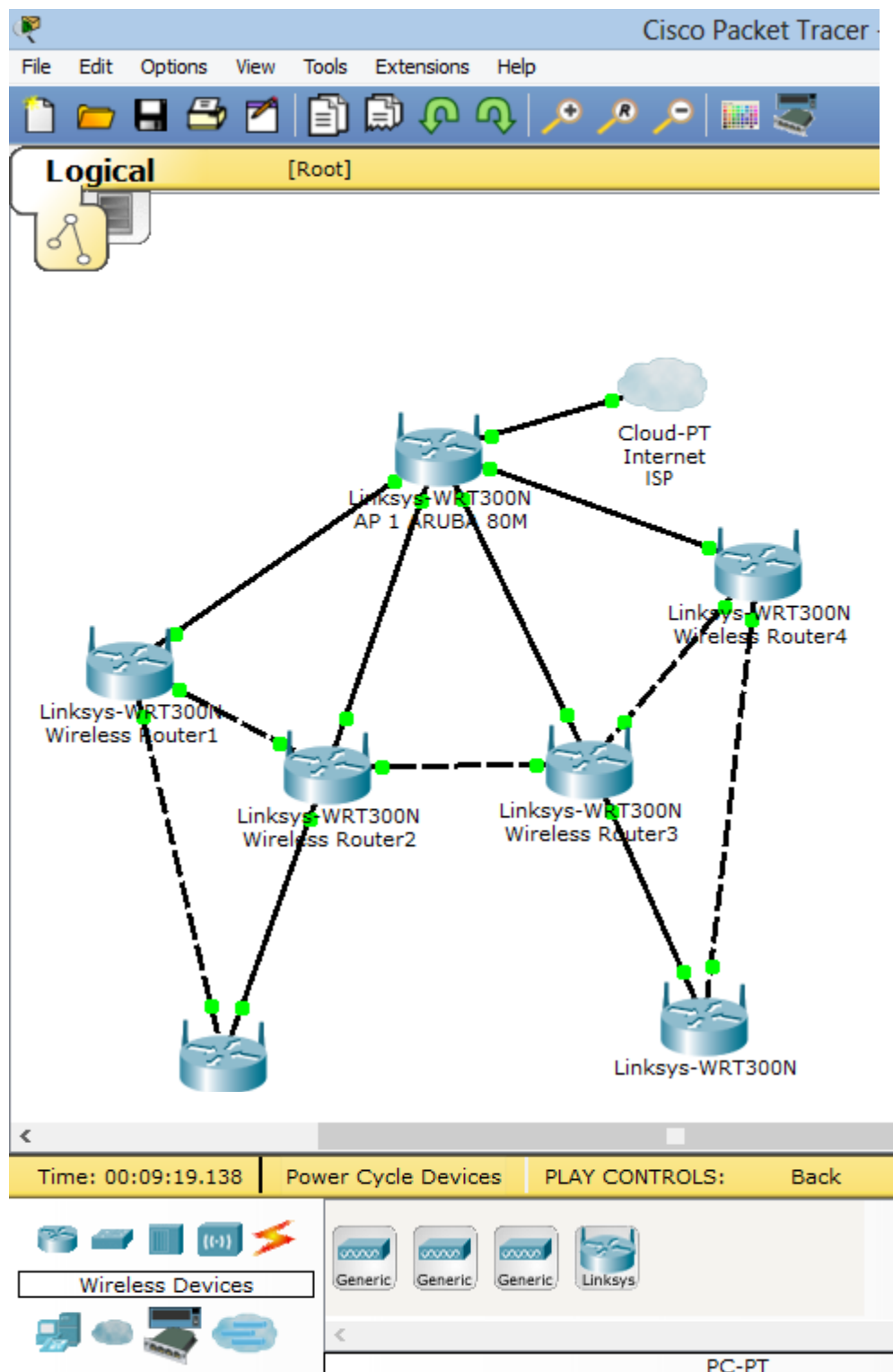


Figura 157. Esquema de conexión entre Linksys <http://www.cisco.com>



Pantalla 12: Instalación de tarjeta inalámbrica a un dispositivo móvil (Laptop) en este caso se muestra como se reemplaza la tarjeta Ethernet por una tipo Wifi, para instalar la tarjeta se debe apagar el equipo y arrastrar la tarjeta inalámbrica hacia el puerto en este caso se usara una tipo: Linksys-WPC300N para hacer posible la conexión del dispositivo a la red.

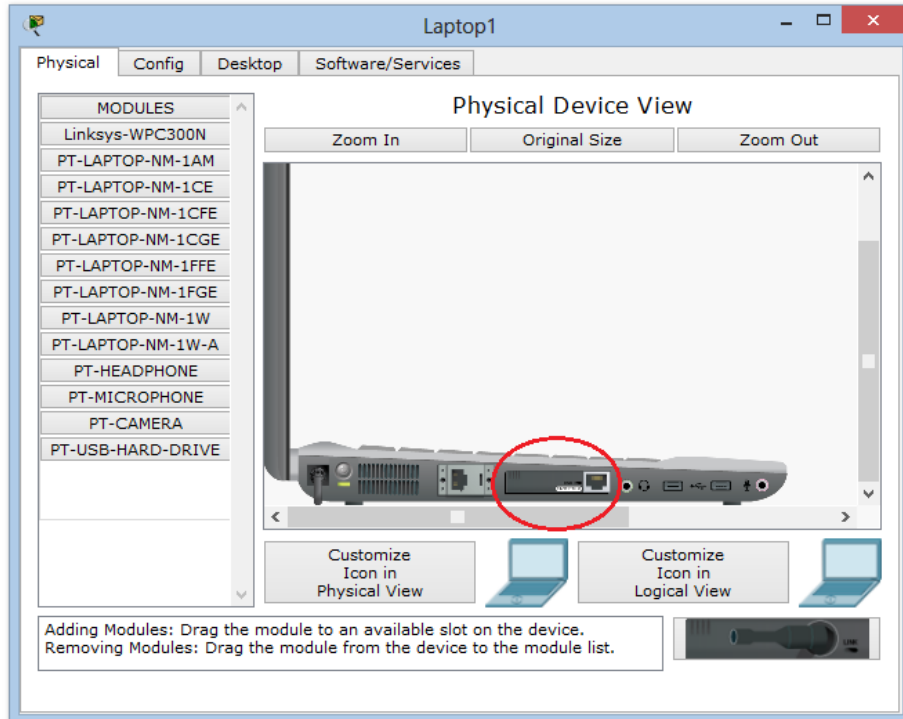


Figura 158. Dispositivo con tarjeta Ethernet  
<http://www.cisco.com>

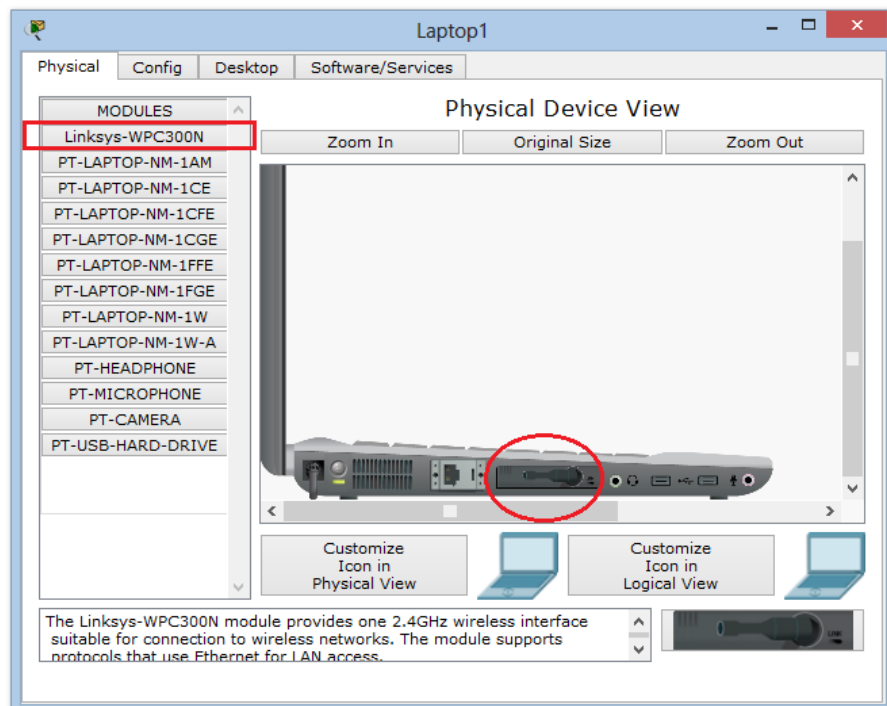


Figura 159. Esquema de conexión entre Linksys  
<http://www.cisco.com>

Simulación terminada en cisco

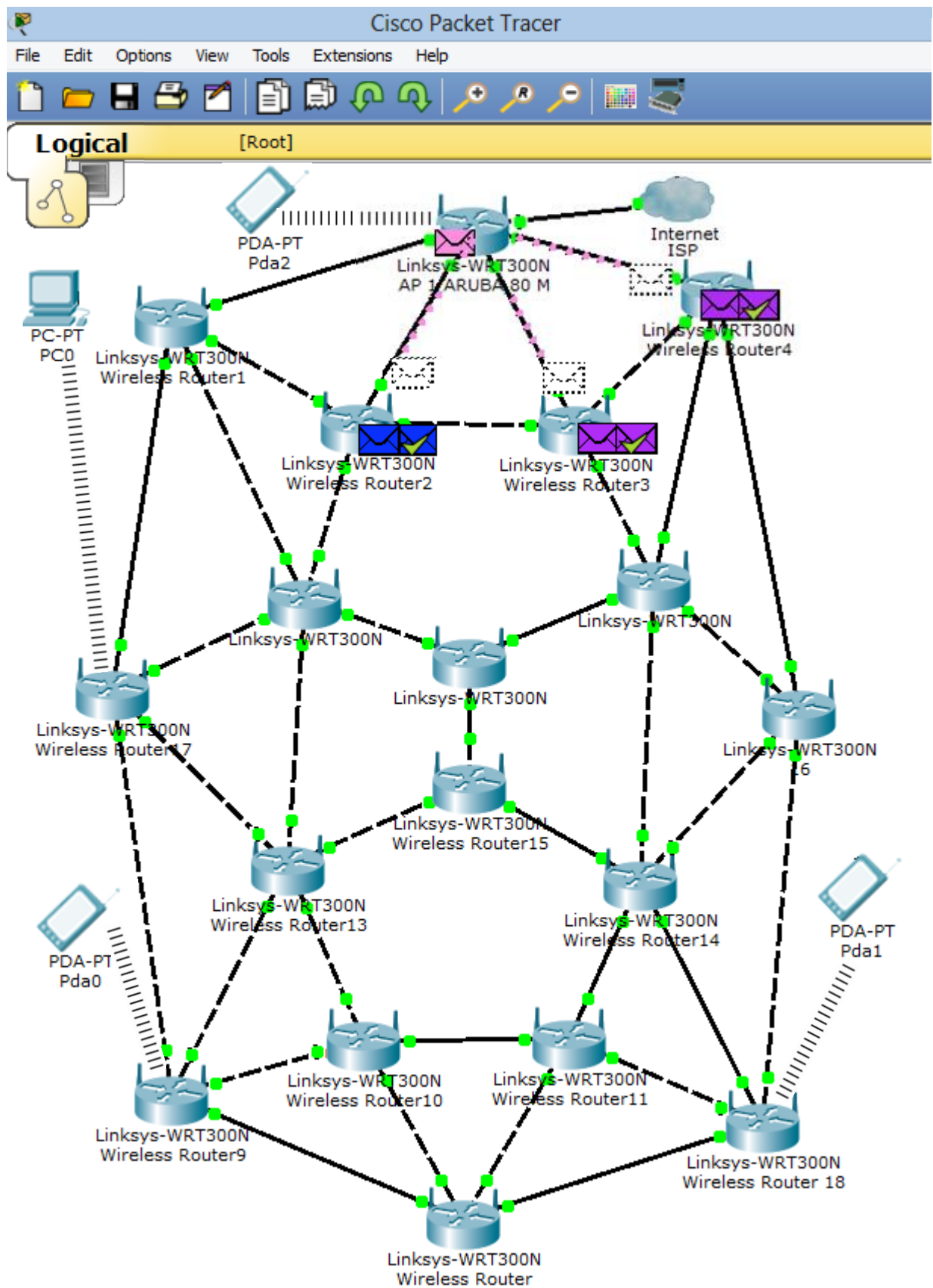


Figura 160. Simulación de la Red Mesh adecuada para el parque temático  
<http://www.cisco.com>

## 4.6.6 Direcccionamiento IP

### Clasificación de direcciones IP

Existen 3 clases de redes, denominadas A, B y C cada clase permite 1111 número limitado de direcciones de red y de Host. Las redes de clase A permiten definir hasta 126 redes y una cantidad ilimitada de host, mientras que las redes de clase C definen una cantidad casi ilimitada de redes pero solo 255 host por red. Cuando se instalan los servicios TCP/IP también será necesario especificar la máscara de subred, la cual identifica la parte del identificador de host de la dirección basada en la clase de red.

**CLASE A:** El primer byte es un número del 1 al 127. Los últimos 3 bytes identifican host en la red. La máscara de la subred 255.0.0.0

**CLASE B:** El primer byte es un número del 128 al 191. El segundo bytes es parte de la dirección de red. El 3 y 4 bytes solo identifica host en la red. Mascara de subred: 255.255.0.0

**CLASE C:** EL primer byte es un número de 192 al 254. El segundo y tercer byte son parte de la dirección de red, el 4 byte solo identifica hasta 255 host. Mascara de subred 255.255.255.0. (Lexcx, 2014)

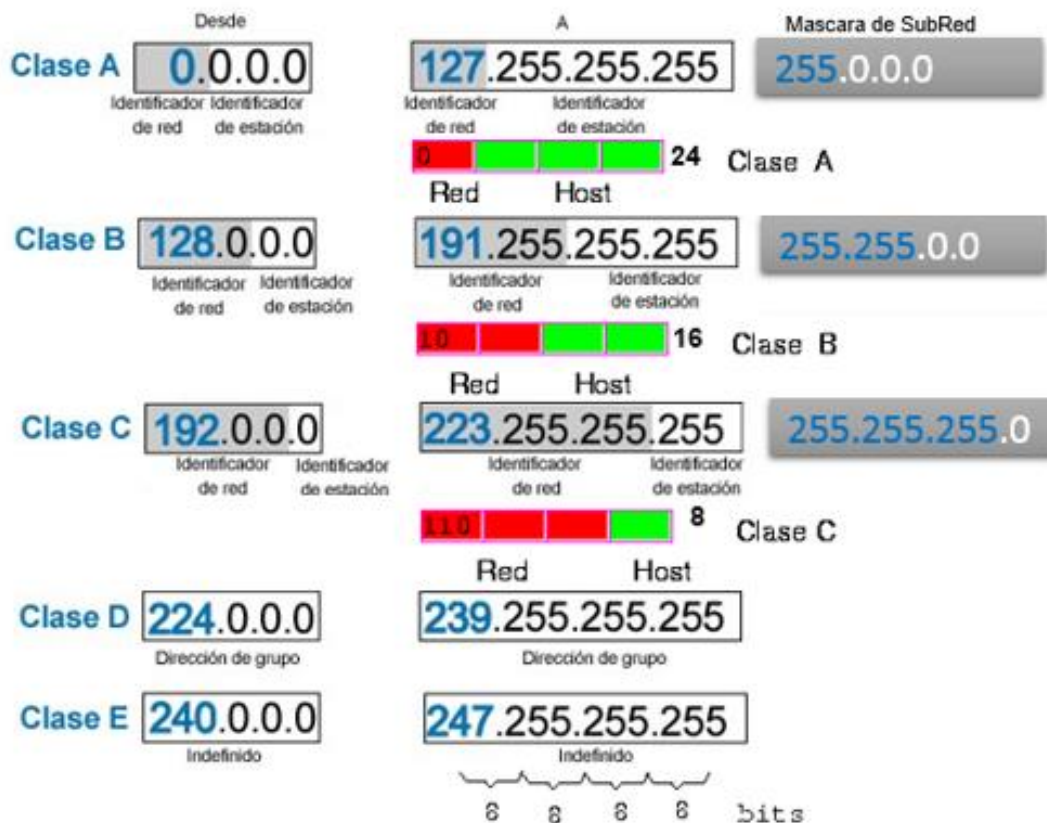


Figura 161. Clasificación de Direcciones IP  
<http://www.es.slideshare.net>

## Mascara de Subred

Una máscara de subred es el principal modo en que TCP/IP limita el número de posibles direcciones con que tenga que tratar una máquina en un momento dado. La máscara de red es una manera de enmascarar o esconder unas partes de la red de otras. La máscara de red para su dirección determina cuántos de los números que componen la dirección IP serán vistos en realidad por otras máquinas como una dirección local de la red. Por eso es importante que las computadoras en una misma parte local de la red usen la misma máscara de subred. (Martinez, 2008)

Existen 3 modos en DHCP para poder asignar direcciones IP a otros equipos:

- Asignación manual: El administrador configura manualmente las direcciones IP del cliente en el servidor DHCP. Cuando la estación de trabajo del cliente pide una dirección IP, el servidor mira la dirección MAC y procede a asignar la que configuró el administrador.
- Asignación automática: Al cliente DHCP (ordenador, impresora, etc.) se le asigna una dirección IP cuando contacta por primera vez con el DHCP Server. En este método la IP es asignada de forma aleatoria y no es configurada de antemano.
- 3Asignación dinámica: El servidor DHCP asigna una dirección IP a un cliente de forma temporal. Digamos que es entregada al *client Server* que hace la petición por un espacio de tiempo. Cuando este tiempo acaba, la IP es revocada y la estación de trabajo ya no puede funcionar en la red hasta que no pida otra.

DHCP es un protocolo diseñado principalmente para ahorrar tiempo gestionando direcciones IP en una red grande. El servicio DHCP está activo en un servidor donde se centraliza la gestión de la direcciones IP de la red. Hoy en día, muchos sistemas operativos incluyen este servicio dada su importancia.

Subneteo: Es el acto de dividir las grandes redes en redes más pequeñas para que estas redes puedan funcionar mejor en cuanto a recepción y envío de paquetes a través de la red de internet. Este término es un término netamente utilizado en el campo de la Computación e Informática en la rama de las redes cuando se arma una red y se quiere dividir esta red en subredes.

Subnetando la red tendremos, en su conjunto, una sola IP *address* dividida en varias subredes más pequeñas bien diferenciadas, consiguiendo un mayor control y reduciendo el congestionamiento por los *broadcast*. (Gomez, 2009).

Parque Temático las Fuentes: Asignación de direcciones IP mediante *subnetting*

**IP 128.30.0.0/16**

Clase B

Mascara: 255.255.0.0

Subredes: 4

Numero de SubRedes  $2^{n-2} \geq$

SubRedes Validas  $2^{3-2}=6$

Donde n= 3

Mascara de Red

**11111111.11111111.00000000.00000000**

**255        255        0        0**

Como n=3 (Numero de 1" Prestados)

Mascara de SubRed

**11111111.11111111.11100000.00000000**

**255        255        224        0**

Numero de Hosts por SubRed=  $2^{m-2}$

m= Numero de ceros  $2^{13} = 8190$  Host por SubRed

Numero de saltos  $256 - 224 = 32$

$2^n$	128	64	32	16	8	4	2	1
$n$	7	6	5	4	3	2	1	0

Tabla 14. Potencias

Direcciones de Red				
SubRedes	IP de Sub Redes	Rango de IP Asignables		Broadcast
		Desde	Hasta	
1	128.30.0.0	128.30.1.0	128.30.30.255	128.30.31.255
2	128.30.32.0	128.30.33.0	128.30.62.255	128.30.63.255
3	128.30.64.0	128.30.65.0	128.30.94.255	128.30.95.255
4	128.30.96.0	128.30.97.0	128.30.126.255	128.30.127.255
5	128.30.128.0	128.30.129.0	128.30.158..255	128.30.159.255
6	128.30.160.0	128.30.161.0	128.30.190.255	128.30.191.255

Tabla 15. Asignación de direcciones IP

#### **4.6.7 Hardware seleccionado para la Red Mesh el Parque Temático**

Como se estableció anteriormente para el desarrollo del diseño y simulación de la red Mesh para el parque Temático las Fuentes se utilizaran los equipos de ARUBA Networks. (Aruba, 2012)

- Router Aruba Air Mesh MSR2000
- Controlador de AP Aruba 2400
- Access Point Aruba 80M

##### **4.6.7.1 Access Point Aruba 80M.**

El Aruba AP-80M es un totalmente endurecido,, dual-radio-exterior nominal (Banda dual 802.11a más b / g concurrente) inalámbrica de alto rendimiento punto de acceso, capaz de soportar múltiples funciones incluyendo WLAN acceso, control de transmisión / detección de intrusiones inalámbricas y la prevención, seguro de alto rendimiento malla empresarial al aire libre y LAN de puente a través de los espectros de RF 2.4 hasta 2.5 GHz y 5 GHz. El acceso AP-80Mpunto soporta diversas opciones de implementación, entregando el usuario seguro servicios y aplicaciones al aire libre alrededor de redes empresariales centradas áreas comunes del campus, estacionamientos, y los puntos de guardia de seguridad, así como en los patios de almacenamiento, almacenaje interior / exterior y entornos de producción industrial. Gestiona de forma centralizada desde una movilidad Aruba controlador, la AP-80M faculta al administrador de la red con un control sin precedentes sobre los servicios, la seguridad y modelos de despliegue. La AP-80M cuenta con interfaces duales, antena desmontable y es totalmente exterior nominal, Es diseñado para el despliegue en entornos adversos, capaces de soportar la exposición a temperaturas extremadamente altas o bajas, humedad y precipitación, y completamente sellado para protegerse de los contaminantes del aire. La AP-80M es un ideal punto de malla de la empresa para la entrega de puente LAN o servicios de malla inalámbrica.

La solicitud

- Recintos empresariales al aire libre, almacenes, contenedores yardas de transporte, instalaciones de producción industriales. Interior exterior despliegues en entornos difíciles.

Modo operativo

- Multi-servicio 802.11a + b / g WLAN, 802.11a + b / g monitor de aire, híbrido
- combinación de WLAN / AM y AP remoto.

- Las radios
- Dual Radio - software configurable para 802.11ay 802.11b / g

#### Gestión de RF

- Automático transmite control de energía y la gestión de canales con
- corrección agujero cobertura de automóviles a través de *Adaptive Radio Management (ARM)*

#### La prestación de servicios de movilidad

- Virtuales Servicios AP:
- Múltiples portales cautivos por SSID
- Soporta cualquier combinación de cifrado / tipos de autenticación por SSID
- El equilibrio de carga VLAN
- Creación de la cuenta Invitado / gestión

#### Energía

##### Suministrada mediante inyector de alimentación

- Entrada:  
100-240 V AC / 1,5 A
- Salida:  
48 V DC hasta 1,2 A 30 vatios pico *Power-over-Ethernet (PoE)*, a través de Adaptador de alimentación suministrado de serie) interfaz de 8 pines DIN. (Networks, Matriz de Productos, 2007)

#### Montaje

##### Estándar:

- Articular poste ajustable o mástil kit de montaje

##### Kit de montaje opcional:

- Soporte de pared



Figura 162. Access Point 80M

<http://69.16.194.131/tagged/On-Point-Radio-NPR/images>

#### 4.6.7.2 Controlador de Access Point Aruba 2400

El controlador de movilidad Aruba MC-2400 es un controlador de LAN inalámbrica que incorpora todas las funciones necesarias y permite agregar hasta 48 puntos de acceso o AP controlados para proporcionar una seguridad y un control centralizados en los despliegues inalámbricos. El controlador MC-2400 proporciona una auténtica experiencia de red centrada en el usuario que ofrece una conectividad “*follow-me*”, un acceso basado en identidad y servicios de continuidad de aplicación, muy adecuados para despliegues inalámbricos en sedes regionales u oficinas densas. Se despliega fácilmente como una superposición sin interrumpir la red existente de cable y se puede gestionar de forma centralizada con *ArubaOS* o el sistema de gestión de movilidad Aruba. Las funciones de convergencia avanzadas, tales como el Control de Admisión de Llamadas (*CAC*, en inglés *Call Admission Control*), la gestión RF con reconocimiento de voz y la calidad de servicio estricta en el aire, permiten al controlador MC-2400 ofrecer funcionalidades VoIP móviles.

Así mismo, el controlador MC-2400 se puede desplegar como un *gateway* de seguridad basado en identidad para autenticar los usuarios conectados por cable e inalámbricos, aplicar las políticas de control de acceso basadas en roles y poner en cuarentena a los clientes finales no seguros para que no accedan a la red corporativa. Los usuarios invitados se soportan fácilmente y con seguridad mediante el servidor de portal cautivo incorporado y los servicios avanzados de red. El controlador MC-2400 puede crear un entorno de red seguro sin necesidad de otros dispositivos VPN/cortafuegos gracias a las funcionalidades VPN y NAT sitio a sitio integradas, túneles *split-tunneling* y un cortafuegos *stateful* conforme a ICASA. El soporte de VPN sitio a sitio se puede integrar con los principales concentradores VPN para facilitar que la integración con las VPN existentes de la organización sea un éxito.

#### Rendimiento y capacidad del controlador

- AP controlados 48
- Usuarios 768
- Direcciones MAC 4.096
- Interfaces de VLAN IP 128
- Puertos *Fast Ethernet* (10/100) 24
- Puertos *Gigabit Ethernet* (GBIC) 2
- Sesiones activas del cortafuegos 64.000
- Túneles *IPsec* simultáneos 768

#### Funciones de seguridad y control de lan inalámbrica

- Seguridad 802.11i (certificación WFA, WPA2 y WPA)
- Autenticación 802.1X de usuario y máquina



- Soporte de EAP-PEAP, EAP-TLS y EAP-TTLS
- Cifrado AES-CCM, TKIP y WEP centralizado
- Autenticación basada en dirección MAC, SSID y ubicación
- Modo distribuido de WLAN para despliegues de AP remotos

#### Funciones de seguridad basadas en identidad

- Autenticación de usuarios conectados por cable e inalámbricos
- Autenticación por portal cautivo, 802.1X y dirección MAC
- Asociación del Nombre de usuario, dirección IP, dirección MAC y clave de cifrado para crear una sólida identidad de red
- Verificación de la identidad por paquete para evitar suplantaciones
- Análisis del estado del dispositivo, puesta en cuarentena y remedio

#### Funciones de gestión de radio adaptativa (arm™)

- Selección automática de canal y potencia para los AP controlados
- Monitorización del aire simultánea con los servicios de usuario final
- Cobertura autorregeneradora basada en las condiciones de RF dinámicas
- Opciones de despliegue denso para la optimización de capacidades
- Reparto de carga AP basado en el número de usuarios

#### Especificaciones de la alimentación del controlador

- Consumo de energía 300 W
- Voltaje de entrada CA 90~132/180~264 V CA
- Frecuencia de entrada CA 47-63 Hz

#### Garantía

- Hardware 1 año para componentes/mano de obra
- Software 90 días\* (Networks, aec Network, 2013)



Figura 163. Controlador de Ap Aruba 2400

<http://www.bernatech.co/ControladoresdeMovilidadArubaNetworks.html>

#### 4.6.7.3 Router Aruba AirMesh MSR 2000

El Aruba *AirMesh* MSR2000 ofrece alta enrutamiento de malla inalámbrica rendimiento para al aire libre entornos donde la conectividad con conexión de cable poco práctico o no disponible.

Reforzado y endurecido para soportar las más extremas condiciones ambientales, la MSR2000 es ideal para despliegue en zonas metropolitanas e industriales, campos petroleros, minas y puertos de embarque. Un multi-radio, arquitectura multi-frecuencia y adaptativo Enrutamiento de nivel 3 utilizando el operativo Aruba *MeshOS*™ sistema de hacer la MSR2000 único. Juntos, proporcionar capacidad sin igual, fiabilidad, baja latencia y transferencias sin costura para voz, vídeo de calidad HD y otra aplicaciones en tiempo real. Inteligente de enrutamiento Mesh inalámbrica.

Integrado con Aruba MeshOS, adaptable *Wireless Routing*™ (AWR™) optimiza automáticamente las rutas de tráfico entre los *routers* de malla inalámbrica y crea una verdaderamente adaptativa infraestructura de malla. Con AWR, la infraestructura de malla se ajusta dinámicamente a los niveles de tráfico y fuerza de la señal RF para garantizar una alta disponibilidad y un rendimiento óptimo a través de múltiples saltos de red.

#### Modo operativo

Cada radio puede estar configurado para operar en los siguientes modos:

- 802.11a / b / g / n punto de acceso para el acceso de clientes
- 802.11a / b / g / n malla enrutador para *backhaul*

#### Seguridad

- De extremo a extremo WPA / WPA2, TKIP (128 bits), PSK, AES (128 bits)
- Autenticación: 802.1X (radio), métodos EAP
- filtrado de direcciones MAC e IP
- Lista de control de acceso (ACL)
- Los certificados digitales

#### Radios

- Dos radios multifunción capaces de 2,4 GHz, 5 GHz o Operación de 4.9 GHz
- Las radios implementan 2x2 MIMO con dos flujos espaciales, que proporciona hasta 300 Mbps de velocidad de datos por la radio

- Relación de cadena doble receptor máxima combinando (MRC) para mejora el rendimiento del receptor

#### Mecánico

- Dimensiones: 225 mm x 225 mm x 105 mm (8,9 "x 8,9" x 4,1 "), con exclusión de los conectores
- Peso (MSR2KP): 3,5 kg (7,7 libras)
- Peso (MSR2KAC): 4,25 kg (9,4 libras)

#### Ambiental

- En funcionamiento:
- Temperatura de almacenamiento y transporte de la gama: -30° C a 70° C (-22° F a 158° F)
- Clasificación climática: IP66
- supervivencia del viento: hasta 165 mph
- Golpes y vibraciones: ETSI 300-19-2-4 spec t41.E clase 4M3
- Transporte: ISTA 2A

#### Instalación

- Kit de montaje



Figura 164. Router Aruba AirMesh MSR 2000  
[www.pghnetworks.com](http://www.pghnetworks.com)

#### 4.6.8 Presupuesto

En la tabla siguiente se muestra el tipo de infraestructura que se ha elegido de acuerdo a las necesidades del parque y al estudio que se realizó anteriormente. Se muestra el número de equipos que se utilizarán y el precio total de dicha infraestructura para la red mesh en el parque temático.

Costo de Hardware:

<b>Hardware ARUBA Networks</b>			
<b>Hardware</b>	<b>Unidades</b>	<b>Costo por unidad</b>	<b>Costo total</b>
<b>Access Point Aruba 80M</b>	<b>18</b>	<b>2,938</b>	<b>52,884</b>
<b>Controlador de Ap Aruba 2400</b>	<b>1</b>	<b>47,650</b>	<b>47,650</b>
<b>Router Aruba AirMesh MSR 2000</b>	<b>1</b>	<b>23,483</b>	<b>23,483</b>
<b>Total</b>			<b>124,017</b>

Tabla 16. Cotización de Hardware

Costo de Infraestructura

Para el router, así como para los Access Point se necesita ubicar mástiles aproximadamente de 3 metros, en lo que respecta al controlador de AP no necesitara instalación adicional debido a que se encontrara ubicado en el módulo de seguridad. A continuación se muestra una tabla con los costos por instalación de Router y Access Point:

<b>Costo de Infraestructura</b>			
<b>Material</b>	<b>Precio Unitario</b>	<b>Cantidad</b>	<b>Precio total</b>
<b>Mástil 3 Mts</b>	<b>210</b>	<b>20</b>	<b>4200</b>
<b>Base para mástil</b>	<b>45</b>	<b>20</b>	<b>900</b>
<b>Total</b>			<b>5100</b>

Tabla 17. Cotización de Infraestructura

Costo total neto:

<b>Costo Total de Recursos</b>	
<b>Hardware</b>	<b>124.017</b>
<b>Infraestructura</b>	<b>5100</b>
<b>Costo total</b>	<b>129.117</b>

Tabla 18. Total de cotizaciones



Figura 165. Logo Aruba Networks Mesh  
<http://www.arubanetworks.com>

## CONCLUSIÓN

Las redes inalámbricas demuestran ser una solución innovadora a la necesidad cada vez mayor de estar comunicados en todos los ámbitos ya sean sociales o económicos. Una de las tecnologías emergentes más interesantes en redes inalámbricas es la tecnología Mesh, utilizándola podemos interconectar varios puntos de acceso Wi-Fi también llamados nodos y formar una red Mesh o malla estas redes proporcionan una infraestructura robusta flexible e innovadora es por eso que nos proporcionan de una conexión y cobertura muy extensa ya que los nodos son capaces de establecer comunicación entre ellos en cuanto sus zonas de cobertura se comunican entre sí, brinda confiabilidad debido a que por medio de los protocolos de enrutamiento.

Los paquetes de información se pueden distribuir uniformemente teniendo en todo momento conocimiento sobre el estado de la red, tomando cálculo de ruta por si algún camino se encuentre bloqueado saber que ruta se debe tomar para optimizar él envío, aligerando así el tráfico existente en la red. Siendo así de infraestructura a bajo costo, llevando a cabo la instalación adecuada, es posible desplegar la red económica disponiendo de los dispositivos sugeridos en el proyecto y fundamentalmente una alta flexibilidad.

Por lo tanto el brindar conexión a internet en espacios públicos pone al descubierto todas la ventajas que ofrece la tecnología Mesh, de ofrecer un servicio de conexión a internet en el parque temático las Fuentes durante su estancia los usuarios podrán conectar sus equipos portátiles a Internet, de manera tal que se potencien sus capacidades digitales, creativas, productivas y de ocio. Esto hace que las redes Mesh sean una de las tecnologías más prometedoras debido a su funcionamiento, bajo coste y fácil instalación lo que la lleva a estar a la vanguardia sobre las demás.

La simulación resulto ser un método factible para observar el comportamiento de una red mesh conforme a los requerimientos del parque municipal “Las fuentes”, de acuerdo a los resultados el 90% de las personas encuestadas afirman que es indispensable el acceso a internet, el 70% de los visitantes utilizan internet de manera constante, el 75 % de los visitantes aseguran que acceden a la red mediante su teléfono celular.

La red Mesh resolvería los problemas de comunicaron del personal que trabaja dentro del parque y a su vez beneficiaria los visitantes.

Con una inversión de 130 mil pesos equivalente al 0.4% del total de la inversión del parque que es de 35 millones se resuelve el problema de comunicación.

## RECOMENDACIONES

- Se recomienda hacer uso de un software que pueda gestionar el estado de los Access Point para detectar alguna falla o caída de alguno de ellos.
- Se recomienda trabajar con las filiales como Alestra o Unet y no directamente con el proveedor de internet (ISP) para una mejor calidad en el servicio.
- Se recomienda un ancho de banda 32 MB para satisfacer 500 usuarios.
- Se recomienda el uso de antenas omnidireccionales en lugares donde la comunicación se dificulte o exista alguna interferencia.
- Se recomienda hacer actualizaciones al software de manera programada para tener en óptimas condiciones los equipos asegurando al usuario un buen servicio.
- Si se desea extender la cobertura al interior de un edificio se recomienda utilizar el punto de acceso AP 70 Aruba ya que es idóneo para interiores además de ser compatible con el concentrador de AP.
- Se recomienda segmentar la red con el proceso de subneteo manejando una red de clase B para así poder tener un correcto, ordenado y adecuado direccionamiento además de una mejor administración de la red.
- Para conocer el comportamiento de la red de manera virtual en un escenario al aire libre se recomienda usar el planificador de la marca Aruba exterior RF.

## GLOSARIO

WPAN	Wireless Personal Area Network, Red Inalámbrica de Área Personal o red de área personal inalámbrica, es una red de computadoras para la comunicación entre distintos dispositivos (computadoras, puntos de acceso a internet, teléfonos celulares, PDA, dispositivos de audio, impresoras) cercanos al punto de acceso.
WLAN	Wireless local área network, es un sistema de comunicación inalámbrico flexible, muy utilizado como alternativa a las redes de área local cableadas o como extensión de éstas. Usan tecnologías de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas.
WMAN	Wireless Metropolitana Network. En términos muy básicos, la WMAN o Red Metropolitana Inalámbrica por su traducción al español, es una versión inalámbrica de MAN, la cual puede llegar a tener un rango de alcance de decenas de kilómetros.
WWAN	Wireless Local Area Network Wireless WAN o Red Inalámbrica de Área Amplia es una red que es capaz de brindar cobertura inalámbrica en un área geográfica relativamente grande.
HTTP	Hypertext Transfer Protocol o HTTP (en español protocolo de transferencia de hipertexto) es el protocolo usado en cada transacción de la World Wide Web.
WIMAX	siglas de Worldwide Interoperability for Microwave Access (interoperabilidad mundial para acceso por microondas), es una norma de transmisión de datos que utiliza las ondas de radio en las frecuencias de 2,3 a 3,5 GHz y puede tener una cobertura de hasta 50 km.
WIFI	mecanismo de conexión de dispositivos electrónicos de forma inalámbrica, Los dispositivos habilitados con wifi, tales como un ordenador personal, una consola de videojuegos, un Smartphone, o un reproductor de audio digital, pueden conectarse a Internet a través de un punto de acceso de red inalámbrica
SIFS	Espacio corto entre tramas

QoS	Calidad del servicio término que se refiere a la garantía de entregar una cantidad de datos en un determinado tiempo
VHF	(Very High Frequency) es la banda del espectro electromagnético que ocupa el rango de frecuencias de 30 MHz a 300 MHz.
MHZ	Un megahercio (MHz) es una unidad de medida de la frecuencia; equivale a $10^6$ hercios (1 millón). Se utiliza muy frecuentemente como unidad de medida de la frecuencia de trabajo de un dispositivo de algo, o bien como medida de ondas.
AM	La modulación de amplitud (AM) es una técnica utilizada en la comunicación electrónica, más comúnmente para la transmisión de información a través de una onda transversal de televisión.
FM	La modulación de frecuencia, o frecuencia modulada (FM), es una técnica de modulación que permite transmitir información a través de una onda portadora variando su frecuencia. En aplicaciones analógicas, la frecuencia instantánea de la señal modulada es proporcional al valor instantáneo de la señal moduladora.
Backbone	Se refiere a las principales conexiones troncales de Internet. Está compuesta de un gran número de routers comerciales, gubernamentales, universitarios y otros de gran capacidad interconectados que llevan los datos a través de países, continentes y océanos del mundo mediante cables de fibra óptica.
MAP	Punto de acceso a la malla
WECA	Wireless Ethernet Compatibility
IEEE	El Instituto de Ingeniería Eléctrica y Electrónica <sup>1</sup> —abreviado como IEEE, leído i-triple-e en Hispanoamérica o i-e-cubo en España; en inglés Institute of Electrical and Electronics Engineers es una asociación mundial de técnicos e ingenieros dedicada a la estandarización y el desarrollo en áreas técnicas.



MBPS	Un megabit por segundo (Mb/s, Mbit/s o Mbps) es una unidad que se usa para cuantificar un caudal de datos equivalente a 1024 kb/s.
SSID	Service Set Identifier
VPN	Red Privada Virtual
WEP	Wired Equivalent Privacy
DNS	Domain Name System o DNS (en español «Sistema de Nombres de Dominio») es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.
HIPERLAN	Estándar global para anchos de banda inalámbricos LAN que operan con un rango de datos de 54 Mbps en la frecuencia de banda de 5 GHz. HIPERLAN/2 es una solución estándar para un rango de comunicación corto que permite una alta transferencia de datos y Calidad de Servicio del tráfico entre estaciones base WLAN y terminales de usuarios.
TCP/IP	Transmission Control Protocol/ Internet Protocol
OSI	El modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1(Open System Interconnect), es el modelo de red descriptivo, que fue creado en el año 1980 por la Organización Internacional de Normalización (ISO, International Organization for Standardization).
ADSL	Línea de suscriptor digital asimétrica,(Asymmetric Digital Subscriber Line), es un tipo de tecnología de línea de abonado digital (DSL) que consiste en la transmisión analógica de datos digitales apoyada en el cable de pares simétricos de cobre que lleva la línea telefónica convencional o línea de abonado (Red Telefónica Conmutada, PSTN).

MAC	En las redes de computadoras, la dirección MAC (siglas en inglés de media access control; en español "control de acceso al medio") es un identificador de 48bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red.
WMN	Wireless Mesh Network
GSM	Sistema global para las comunicaciones móviles (Global System for Mobile communications, GSM, es un sistema estándar, libre de regalías, de telefonía móvil digital.
AD-HOC	Las redes de este tipo Mobile ad hoc network (denominadas también MANET como acrónimo de Mobile ad hoc network) en algunas ocasiones denominada también como malla de nodos móviles (mobile mesh network), se trata de una red de dispositivos conectados por wireless y que poseen propiedades de auto-configuración, además de poseer cierta movilidad (es decir se encuentran montados en plataformas móviles).
INFRA	Existe un equipo llamado punto de acceso que realiza las funciones de coordinación centralizada de la comunicación entre las distintas terminales de la red. A esta modalidad de topología se le conoce como de infraestructura.
IBBS	Independent Basic Service Set
BSS	Basic Service Set
3G	Es la abreviación de tercera generación de transmisión de voz y datos a través de telefonía móvil mediante UMTS (Universal Mobile Telecommunications System o servicio universal de telecomunicaciones móviles).
CSMA/CA	En comunicaciones, CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) o, en español, acceso múltiple con escucha de portadora y evasión de colisiones, es un protocolo de control de acceso a redes de bajo nivel que permite que múltiples estaciones utilicen un mismo medio de transmisión.

## Bibliografía:

- Air, B. (12 de abril de 2015). *Nas Wireless*. Obtenido de Nice Wireless Products: <http://naswireless.com/wanlanwlan-products/belair-networks/>
- Android. (10 de Marzo de 2015). *Wikipedia Org*. Obtenido de Android Central: [http://es.wikipedia.org/wiki/Hotspot\\_%28telecomunicaciones%29](http://es.wikipedia.org/wiki/Hotspot_%28telecomunicaciones%29)
- Aruba. (4 de Abril de 2012). *Bernatech Proveedores*. Obtenido de Controladores de Movilidad: <http://www.bernattech.co/ControladoresdeMovilidadArubaNetworks.html>
- Attribution, C. (28 de Abril de 2015). *Wikipedia Org*. Obtenido de Wikimedia: [http://es.wikipedia.org/wiki/Sistema\\_operativo\\_de\\_red](http://es.wikipedia.org/wiki/Sistema_operativo_de_red)
- Avaya. (27 de Diciembre de 2010). *Deploying Avaya Ip Office*. Obtenido de Ipoofficeinfo: [http://www.ipofficeinfo.com/pdf/ip500v2\\_installation.pdf](http://www.ipofficeinfo.com/pdf/ip500v2_installation.pdf)
- A., J. E. (20 de Febrero de 2013). *Monografias*. Obtenido de Monografias S.A: <http://www.monografias.com/trabajos/redesinalam/redesinalam.shtml>
- Alfredo, C. A. (20 de Enero de 2008). *Itzamna* . Obtenido de Ipn : <http://itzamna.bcnt.ipn.mx/dspace/bitstream/123456789/438/1/LUCERNA.pdf>
- Attribution/Share-Alike, C. C. (12 de Marzo de 2013). *Wikipedia*. Obtenido de Enciclopedia Libre: [http://es.wikipedia.org/wiki/Puerta\\_de\\_enlace](http://es.wikipedia.org/wiki/Puerta_de_enlace)
- Bravo, W. G. (25 de Marzo de 2008). *Estudio de las Redes Mesh*. Obtenido de cdigital uv: <http://cdigital.uv.mx/bitstream/123456789/29463/1/Bravo%20Gonzalez.pdf>
- boulder, P. (1 de Marzo de 2012). *Center Ibm*. Obtenido de Publib Ibm: [http://www.publid.boulder.ibm.com/html/as400/v4r5/ic2931/info/RZAI2SUBNET\\_MASK.HTM](http://www.publid.boulder.ibm.com/html/as400/v4r5/ic2931/info/RZAI2SUBNET_MASK.HTM)
- Behrouz, F. (26 de Abril de 2011). *Wikimedia*. Obtenido de Protocol Suite: [http://es.wikipedia.org/wiki/File\\_Transfer\\_Protocol](http://es.wikipedia.org/wiki/File_Transfer_Protocol)
- Cañarte, M. I. (5 de Mayo de 2009). *Espol* . Obtenido de Universidad de Ecuador: <http://www.Espoltel.net>
- Cabrera, J. L. (2008). *Redes locales.configuracion basicas*. mexico: RA-MA SA Editorial y publicaciones.
- Carrillo, C. E. (26 de febrero de 2011). *Biblioteca Uam*. Obtenido de Analisis de Protocolos de Encaminamiento Para Redes Inalambricas: <http://148.206.53.84/tesiuami/UAMI15536.PDF>
- Cisco. (5 de abril de 2009). *Support Cisco*. Obtenido de Support Cisco: [www.cisco.com/cisco/web/support/LA/10/106/106286\\_ap-faq.html](http://www.cisco.com/cisco/web/support/LA/10/106/106286_ap-faq.html)
- Cisco. (5 de Mayo de 2010). *Open Boxer*. Obtenido de Packet Tracer: <http://www.openboxer.260mb.com/asignaturas/redes/simuladoresRedes.pdf>
- Cisco. (2 de abril de 2012). *Enbex*. Obtenido de Enbex: [http://www.enbex.es/noticias/rss/enbex\\_feed.php?page=1](http://www.enbex.es/noticias/rss/enbex_feed.php?page=1)
- Commons. (28 de Abril de 2015). *Wikipedia*. Obtenido de Wikimedia: [http://es.wikipedia.org/wiki/Puerta\\_de\\_enlace](http://es.wikipedia.org/wiki/Puerta_de_enlace)

- Cabrera, J. L. (2008). *Redes Locales Instalacion Y configuracion Bsicas*. Mexico: RA-MA Editorial .
- Commons, C. (18 de Marzo de 2015). *wikipedia org*. Obtenido de wikimedia: [http://es.wikipedia.org/wiki/Ancho\\_de\\_banda](http://es.wikipedia.org/wiki/Ancho_de_banda)
- Commons, C. (16 de Marzo de 2015). *wikispaces*. Obtenido de Fundamentos de Redes: <https://fundamentosderedesenero7422.wikispaces.com/5.1.1+DIRECCIONAMIENTO+MAC?responseToken=0ff7e084ea5495ae2a3607fe8441c7b4f>
- Cisco. (26 de Diciembre de 2007). *Linksys A Division Of Cisco*. Obtenido de Switches: <https://www.cisco.com/c/dam/en/us/td/docs/switches/lan/csbms/srw208/administration/guide/srw208.pdf>
- Cisco. (23 de Diciembre de 2008). *Cisco Product*. Obtenido de Routers: <http://www.cisco.com/c/en/us/products/routers/2900-series-integrated-services-routers-isr/index.html>
- Com, 3. (25 de Diciembre de 2008). *Cyber Puerta*. Obtenido de Hardware y Redes: <http://www.cyberpuerta.mx/Computo-Hardware/Redes/Switches/Switch-3COM-Baseline-2026-G-26-Ptos-24X-Fast-Ethernet-2X-Gigabit-Ethernet.html>
- COMDIEL. (25 de Diciembre de 2009). *Telecomunicaciones, Redes de Datos Seguridad*. Obtenido de Patch Panel Panduit: <http://www.comdiel.cl/patch-panel-24-puertos-rj45-panduit-dp5e-categoria-5e-s-2760.html>
- Commons, C. (20 de Diciembre de 2013). *Wikipedia*. Obtenido de Redes Informaticas: [http://es.wikipedia.org/wiki/Main\\_distribucion\\_frame](http://es.wikipedia.org/wiki/Main_distribucion_frame)
- commons, C. (29 de Diciembre de 2014). *Wikipedia Org*. Obtenido de Encyclopedia: <http://www.enwikiopedia.org/wiki/Linksys>
- Commons, L. C. (31 de Diciembre de 2014). *Wikipedia*. Obtenido de Encyclopedia: <http://es.wikipedia.org/wiki/Rack>
- Commons, C. (9 de Febrero de 2012). *Fundacion Wikimedia*. Obtenido de Wikipedia Org: [http://es.wikipedia.org/wiki/Protocolos\\_de\\_encaminamiento](http://es.wikipedia.org/wiki/Protocolos_de_encaminamiento)
- Commons, C. (10 de Febrero de 2014). *Wikipedia Org*. Obtenido de IEEE: [http://es.wikipedia.org/wiki/IEEE\\_802.15](http://es.wikipedia.org/wiki/IEEE_802.15)
- Deco, C. (19 de Marzo de 2000). *Sedici Unlp*. Obtenido de Protocolo de Encaminamiento: [http://sedici.unlp.edu.ar/bitstream/handle/10915/23759/Documento\\_completo.pdf?sequence=1](http://sedici.unlp.edu.ar/bitstream/handle/10915/23759/Documento_completo.pdf?sequence=1)
- DELL. (26 de Diciembre de 2010). *Dell Poweredge*. Obtenido de Server: [http://www.dell.com/downloads/global/products/pedge/en/pe\\_r200\\_spec\\_sheet\\_new.pdf](http://www.dell.com/downloads/global/products/pedge/en/pe_r200_spec_sheet_new.pdf)
- D-Link. (26 de Diciembre de 2013). *D-Link Building Networks For People*. Obtenido de Amtel: [http://www.dell.com/downloads/global/products/pedge/en/pe\\_r200\\_spec\\_sheet\\_new.pdf](http://www.dell.com/downloads/global/products/pedge/en/pe_r200_spec_sheet_new.pdf)

- Eduardo, R. (17 de Marzo de 2012). *Biblioteca Digital*. Obtenido de UCA: <http://bibliotecadigital.uca.edu.ar/repositorio/revistas/redes-inalambricas-comunitario.pdf>
- Falcon, J. A. (2004). *Como Construir una Red Inalambrica*. España : RA-MA Editorial S.A .
- Gomez, J. (2008). *Guia de Campo de Wi Fi*. Mexico: R-A MA S.A Editorial y Publicaciones.
- Gomez, J. A. (2005). *Redes Locales* . Mexico: Editex.
- Galdames, A. (24 de Marzo de 2012). *ehow en español*. Obtenido de Hobb: [http://www.ehowenespanol.com/servidor-radius-info\\_376327/](http://www.ehowenespanol.com/servidor-radius-info_376327/)
- General, P. e. (22 de Abril de 2015). Parque Tematico. (Guido, Entrevistador)
- Gomez, J. A. (2009). *Servicios en Red*. Mexico: Editex.
- Ges, F. H. (22 de Diciembre de 2009). *DT- Com*. Obtenido de Routers: <http://www.dt-com.com/index.php/home/products/tabletop-modems-router/modem-router/shdsl-router-efm-2p-detail>
- Gonzalez, T. P. (16 de abril de 2013). *Universidad de Almeria*. Obtenido de Redes Mesh: [http:// adminso.es/recursos/Proyectos/PFM/2010\\_11/PFM\\_mesh.pdf](http://adminso.es/recursos/Proyectos/PFM/2010_11/PFM_mesh.pdf)
- Hoy, I. (20 de marzo de 2007). *Tecnologia e Internet sin Complicaciones*. Obtenido de Sitio Web Informatica: <Http://www.informatica-hoy.com.ar/redes/LAN-WAN-MAN-WLAN-WMAN-WWMAN-SAN-PAN.php>
- Huawei. (24 de Diciembre de 2014). *Huawei Products*. Obtenido de Optix: <http://huawei.com/es/products/transport-network/wdm-otn/osn8800/index.htm>
- Intracom. (28 de Diciembre de 2009). *Intelligent Networks Solution*. Obtenido de Convertidor de medios: <http://www.intellinet-network.com/es-US/products/9270-convertidor-de-medios-fast-ethernet>
- Julio, G. L. (2008). *Guia de Campo WiFi*. Mexico: R-A MA Editorial y Publicaciones.
- Johnson, R. (14 de Abril de 2005). *Wikipedia Org*. Obtenido de Fundacion Wikimedia: <http://es.wikipedia.org/wiki/Encuesta>
- Jornada, L. (20 de Abril de 2015). Gobierno de Neza Inagura Parque Tematico. *La Jornada*, pág. 1.
- internet, g. (3 de Febrero de 2003). *Consultoria y Servicios de internet*. Obtenido de wireless gamma internet: <http://wireless.gammainternet.com/autenticacion.html>
- Lopez, P. A. (2008). *Seguridad Informatica 4*. Mexico: Editex.
- Lesta, A. (2006). *Fundamentos y Aplicaciones de Seguridad*. Barcelona España: Marcombo.
- Lopez, F. J. (2005). *Grupos A y B de Informatica Bloque Especifico*. España: MAD-EDUFORM.
- Lexcx, G. (9 de Mayo de 2014). *Slideshare*. Obtenido de Direccionamiento: <http://es.slideshare.net/Gisellexcx/7red-punto-a-punto-estrella-y-clasificacion-de-direcciones-ip>

- Lynksys. (19 de Enero de 2012). *shopping*. Obtenido de trending: <http://lynksys.com>
- Moya, L. M. (12 de Abril de 2013). *ciencia y tecnologia*. Obtenido de Cienteccr: <http://cienteccr.blogspot.mx/2013/02/electromagnetismo-y-celulares.html>
- Manrique, C. (20 de abril de 2009). *Space Espol*. Obtenido de Wireless Mesh Network: <http://www.dspace.espol.ed.ec/bitstream/123456789/10529/4/Wireless%20Mesh%20Network.ps>
- Marquez, A. G. (2005). Protocolo de Enrutamiento Para la Capa de Red en Arquitecturas de Redes de Datos. *Informatica Cooperativa de Colombia*, 20.
- Manrique, F. M. (16 de Abril de 2004). *Monografias*. Obtenido de Recoleccion de Datos: <http://www.monografias.com/trabajos18/recoleccion-de-datos/recoleccion-de-datos.shtml>
- Martinez, M. A. (2008). *Redes locales Instalacion y Configuracion Basicas*. Mexico: RA-MA S.A Editorial y Publicaciones .
- Mesh, O. (24 de Marzo de 2015). *Cloud Managet*. Obtenido de Wireless Network: <http://www.open-mesh.com/>
- Moguel, E. A. (2005). *Metodologia de la Investigacion*. Tabasco: Universidad Autonoma.
- Mora, J. (11 de Abril de 2013). *Slideshare*. Obtenido de Instrumentos de Investigacion: <http://es.slideshare.net/jenifermora28/instrumentos-de-investigacion-cualitativa>
- Nave, M. O. (5 de Marzo 17 de 2007). *hyper physics*. Obtenido de Clasificacion de Polarizacion: <http://hyperphysics.phy-astr.gsu.edu/hbasees/phyopt/polclas.html>
- Networking, C. (12 de Marzo de 2013). *Router Switch*. Obtenido de Cisco 1900 : <http://www.cisco1900router.com/how-to-design-outdoor-wireless-networks-for-campus-mobile-classrooms.html>
- Network, A. (23 de Abril de 2015). *Hp Company*. Obtenido de Aruba Support Center: [https://support.arubanetworks.com/Default.aspx?TabId=77&DMXModule=512&Command=Core\\_ViewDetails&EntryId=7698](https://support.arubanetworks.com/Default.aspx?TabId=77&DMXModule=512&Command=Core_ViewDetails&EntryId=7698)
- Network, T. (6 de abril de 2012). *Infomine*. Obtenido de Abb Tropos: [http://www.infomine.com/index/suppliers/ABB\\_Tropos\\_Wireless\\_Communication\\_Systems.html](http://www.infomine.com/index/suppliers/ABB_Tropos_Wireless_Communication_Systems.html)
- Networks, A. (5 de abril de 2007). *Matriz de Productos*. Obtenido de Aruba Networks Products: [http://www.arubanetworks.com/pdf/products/MAT\\_AP\\_SP.pdf](http://www.arubanetworks.com/pdf/products/MAT_AP_SP.pdf)
- Networks, A. (8 de abril de 2012). *Aec Networks*. Obtenido de Aec Networks Fabricantes: <http://www.aec.co.cr/fabricantes/productos/aruba-networks>
- Networks, A. (6 de abril de 2013). *aec Network*. Obtenido de aec Fabricantes : [www.aec.co.cr/fabricantes/productos/aruba-networks](http://www.aec.co.cr/fabricantes/productos/aruba-networks)
- Networks, A. (5 de abril de 2014). *Wi-Fi Performance*. Obtenido de Wi-Fi Performance: [http://www.arubanetworks.com/pdf/technology/TR\\_Aruba\\_WiFi\\_Performance.pdf](http://www.arubanetworks.com/pdf/technology/TR_Aruba_WiFi_Performance.pdf)
- Nezahualcoyolt, A. d. (1 de Mayo de 2009). *Gobierno del Estado de Mexico*. Obtenido de   
de Municipio de Nezahualcoyolt:

[http://es.wikipedia.org/wiki/Nezahualc%C3%B3yotl\\_%28estado\\_de\\_M%C3%A9xico%29](http://es.wikipedia.org/wiki/Nezahualc%C3%B3yotl_%28estado_de_M%C3%A9xico%29)

- Nezahualcoyotl, A. (07 de Abril de 2015). *neza gob*. Obtenido de Nezahualcoyotl Edomex: <http://www.neza.gob.mx/boletines.php?pagina=96>
- Networks, A. (30 de Diciembre de 2014). *Aruba 130 Series* . Obtenido de Access Point: [http://www.arubanetworks.com/assets/ds/DS\\_AP130Series.pdf](http://www.arubanetworks.com/assets/ds/DS_AP130Series.pdf)
- Pellegero, I. (2006). *Redes WLAN Fundamentos y Aplicaciones de Seguridad*. Barcelona España: Marcombo.
- Ordoñez, J. L. (26 de Marzo de 2011). *Ciencia y Tecnología*. Obtenido de acta.es: [http://www.acta.es/medios/articulos/ciencias\\_y\\_tecnologia/062017.pdf](http://www.acta.es/medios/articulos/ciencias_y_tecnologia/062017.pdf)
- Oracle. (2 de abril de 2008). *Oracle Guía de Administración* . Obtenido de Docs Oracle: [http://docs.oracle.com/cd/E24842\\_01/html/820-2981/dhcp-overview-14a.html](http://docs.oracle.com/cd/E24842_01/html/820-2981/dhcp-overview-14a.html)
- Portátiles, O. y. (2014). El protocolo DHCP y su Funcionamiento. *Ordenadores y Portátiles, 2*.
- Ramirez, J. A. (27 de Marzo de 2012). Modelado de la Red. Mexico, D.F, Mexico.
- Russell, J. T. (2005). *Publicidad*. Mexico: Pearson.
- Russell, R. (02 de Abril de 2005). *Ventanas al Universo*. Obtenido de Windows 2: [http://www.windows2universe.org/physical\\_science/magnetism/em\\_radio\\_waves.html&lang=sp](http://www.windows2universe.org/physical_science/magnetism/em_radio_waves.html&lang=sp)
- Petinari, M. (26 de Marzo de 2000). *Sedici Unlp*. Obtenido de Protocolos de Encaminamiento: [http://sedici.unlp.edu.ar/bitstream/handle/10915/23759/Documento\\_completo.pdf?sequence=1](http://sedici.unlp.edu.ar/bitstream/handle/10915/23759/Documento_completo.pdf?sequence=1)
- Ramirez, A. Q. (17 de Diciembre de 2014). Antecedentes UAEM Texcoco. (Guidos, Entrevistador)
- Ramirez, A. Q. (Diciembr de 2014). Antecedentes UAEMEX. (GUIDOS, Entrevistador)
- Riera, J. L. (20 de Febrero de 2006). *Research*. Obtenido de Mobiliti Int TCP/IP Networks : [http://research.ac.upc.edu/CompNet/doct/curso-0506/WMN\\_JosepLluisFerrer.pdf](http://research.ac.upc.edu/CompNet/doct/curso-0506/WMN_JosepLluisFerrer.pdf)
- Ruiz, P. M. (2009). *Ad-Hoc, Mobile and Wireless Network*. España: Springer.
- Redes. (30 de Abril de 2013). *Todo Redes*. Obtenido de Todo Redes: <http://todo-redes.com/access-point-punto-de-acceso.html>
- Suarez, B. G. (2009). Wireless Mesh Networks. *Enginyeria Informatica, 4*.
- Server, W. (22 de Marzo de 2008). *Technet Microsoft*. Obtenido de Funcion Servidor DNS: <http://technet.microsoft.com/es-es/library/cc753635%28v=ws.10%29.aspx>
- Staff, U. (2007). *Tecnico en Redes*. USA: Usershop.
- Segundo, J. d. (3 de Abril de 2012). *Jorge Nova Fails*. Obtenido de Gns3: <https://jorgedenovasri.files.wordpress.com/2012/09/gns3.pdf>

- Strix. (7 de Abril de 2014). *Networks Without Wires*. Obtenido de System Strix:  
<http://www.strixsystems.com/>
- Tenero, M. d. (2006). *Redes Locales*. España: Paraninfo.
- Tanenbaum, A. S. (2003). *Redes de Computadoras*. USA: Pearson Educacion .
- Torres, J. J. (26 de Abril de 2006). *bibing*. Obtenido de IEEE:  
<http://www.bibing.us.es/proyectos/abreproy/11138/fichero/memoria%252FCap%EDtulo+3.pdf>
- Wang, A. (2005). *Wireless Mesh Network*. USA: Elsevier.



## **ANEXO A**

### **Cuestionario aplicado a usuarios del parque temático**

1 ¿Sabe que es una red WiFi?

2 ¿Cree indispensable el acceso a internet en el parque las fuentes?

3 ¿Porque motivo considera indispensable el acceso internet?

4 ¿Con que frecuencia utiliza internet?

5 ¿Para que utiliza internet?

6 ¿Mediante que dispositivo accede a la red?

7 ¿Con que frecuencia visita el parque las fuentes?

## **ANEXO B**

### **Encuesta aplicada a RTIC”S**

- 1 ¿Qué velocidad provee el ISP de Toluca?
  
- 2 ¿Qué velocidad de datos se tiene actualmente?
  
- 3 ¿De cuánto es el ancho de banda que se ofrece a los usuarios?
  
- 4 ¿Cuántas direcciones IP dispone el C.U Texcoco?
  
- 5 ¿Cuántos equipos de cómputo disponen para personal administrativo y Docentes?
  
- 6 ¿Cuántos equipos de cómputo hay por laboratorio?
  
- 7 ¿Control escolar maneja algún tipo de intranet?
  
- 8 ¿Cuál es el estado de conexión de la biblioteca a la red?
  
- 9 ¿La red WiFi eta diseñada para dar movilidad en cualquier lugar del centro?
  
- 10 ¿Cómo se lleva acabo el mantenimiento de la red?

## ANEXO C

### Simuladores

#### Simulador GNS3

GNS3 es un simulador gráfico de red que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos.

Para permitir completar simulaciones, GNS3 está estrechamente vinculada con:

- Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarios imágenes IOS de Cisco Systems.
- Dynagen, un front-end basado en texto para Dynamips

Un emulador de PIX.GNS3 es una excelente herramienta complementaria a los verdaderos laboratorios para los administradores de redes de Cisco o las personas que quieren pasar sus CCNA, CCNP, CCIE DAC o certificaciones.

La principal característica de GNS3 es que es multiplataforma, podremos usarlo tanto en Microsoft Windows, Linux como en Mac OS X, y todo ello de forma completamente gratuita.

En la nueva versión de GNS3 sigue dando soporte para todos los protocolos y características que las anteriores versiones del software, sin embargo han cambiado por completo el aspecto visual de su interfaz gráfica, haciéndola mucho más actual y atractiva. Asimismo también han cambiado por completo el aspecto visual de su página web oficial, con un diseño muy similar al de la propia herramienta. (Segundo, 2012)

Ventana principal Simulador GNS3:

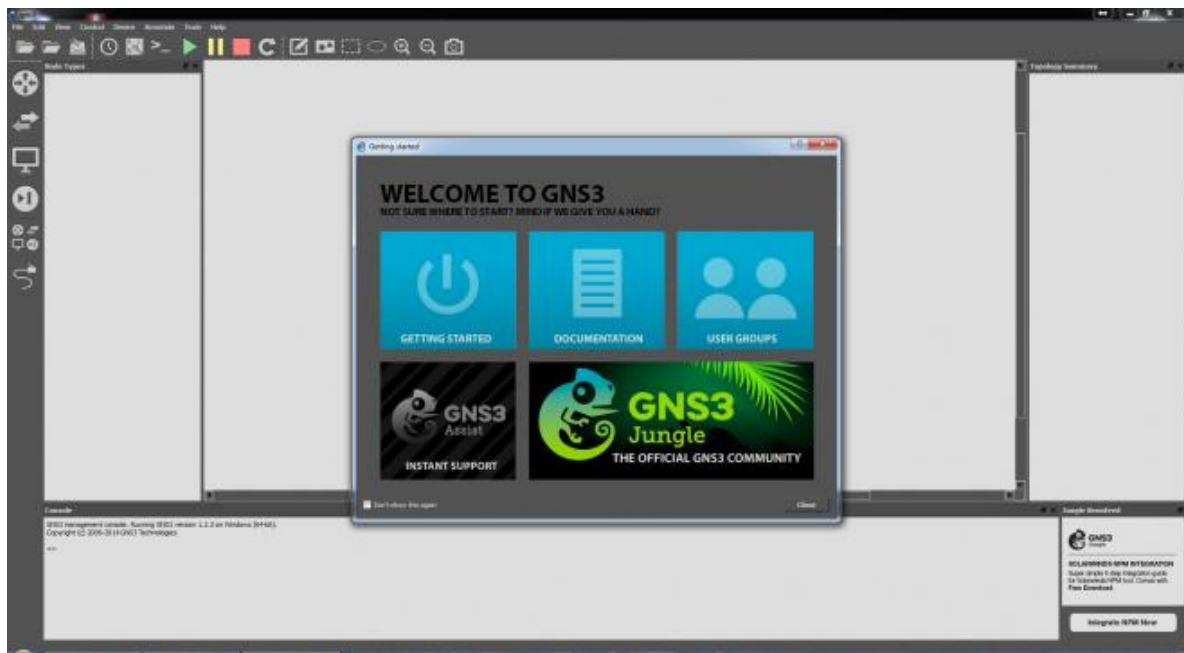


Figura 166. Interfaz del GNS3  
<http://www.itknowledge.com.au/>

## OPNET MODELER

OPNET Modeler es un programa ampliamente utilizado en la industria para modelar y simular sistemas de comunicaciones; permite diseñar y estudiar redes, dispositivos, protocolos y aplicaciones, brindando escalabilidad y flexibilidad, cualidades que le permiten ofrecer a sus usuarios, trabajar en procesos de investigación y desarrollo. MODELER es un software desarrollado por OPNET; orientado a simular objetos mediante un editor gráfico que permite diseñar una topología de red, soporta un amplio rango de tecnologías tipo LAN, MAN y WAN.

Características generales. Originalmente fue desarrollado por MIT e introducido al mercado en 1987 como el primer simulador comercial. Esta herramienta se utiliza para el modelado y simulación; está basada en la teoría de redes de colas e incorpora las librerías para facilitar el modelado de las topologías de red. El desarrollo de los modelos se realiza mediante la conexión de diferentes tipos de nodos, utilizando diferentes tipos de enlaces. Mediante OPNET MODELER, se deben especificar tres tipos de modelos, como se muestra a continuación.

- Modelo de red: redes y subredes
- Modelo de nodos: nodos y estaciones
- Modelo de procesos: especifica la funcionalidad de cada nodo.

El modelo de la red, involucra la creación de nodos, los cuales internamente están constituidos por distintos tipos de módulos y conexiones; finalmente se define la función que desempeñará cada módulo o nodo durante la simulación, a través de los modelos de proceso.



Figura 167 Interfaz del OPNET MODELER

<http://pacific.sdsu.edu/cfd/opnet/>

Requerimientos del sistema. Este programa es multiplataforma y requiere las siguientes especificaciones para su correcta instalación y posterior uso.

- Sistema operativo : Windows NT, 2000, XP y UNIX
- Requerimientos mínimos del sistema: Procesador Intel Pentium III de 500 MHz, 64 MB en RAM y 100 MB disponibles en disco duro. Monitor SVGA, 8 MB en memoria de video y tarjeta de sonido

Interfaz gráfica de usuario. OPNET MODELER está basado en una serie de editores jerárquicamente organizados, los cuales permiten diseñar y configurar los modelos de red, de nodos y de procesos en las topologías de red que se van a simular con este programa. Los editores trabajan en forma directa y paralela la estructura real de la red, los equipos y los protocolos.

Editor de proyecto. Mediante este editor se representa gráficamente la topología de una red de comunicaciones, haciendo uso de un panel de herramientas o importándolo de las librerías de OPNET MODELER; además, esta herramienta provee un contexto geográfico configurable, un menú de configuración rápida de protocolos y especificaciones de vista, para aplicarse a la red que se va a simular.

Editor de Nodos. Este editor captura la arquitectura de una red, un dispositivo o un sistema, describiendo el flujo de los datos entre elementos funcionales, a los cuales se les conoce como “módulos”. Cada módulo, puede generar, enviar o recibir paquetes a los demás módulos de la red, de acuerdo a la función que representa dicho nodo. Generalmente, los módulos representan aplicaciones, protocolos, algoritmos o recursos como: buffers, puertos y buses, entre otros; es decir que todo nodo es asignado a un proceso o evento dentro de la simulación, y esto se logra, mediante el editor de procesos.

Editor de procesos. Dentro del editor de procesos, se encuentran unas máquinas, llamadas FSM22; estas herramientas soportan las especificaciones, detalles, protocolos, recursos y aplicaciones que se desean configurar en la red modelada gráficamente con los editores de proyecto, de nodos respectivamente. (Cisco, Open Boxer, 2010)

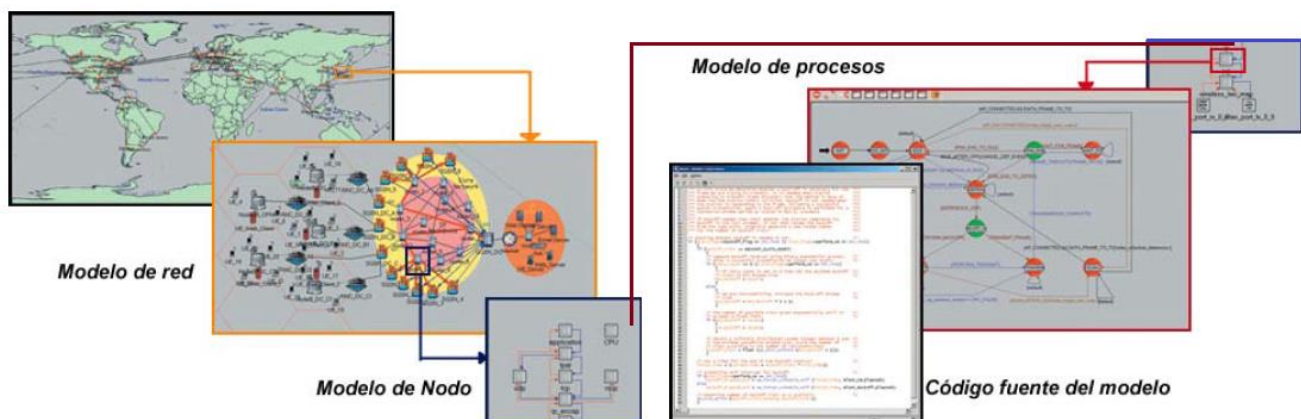


Figura 168. Modelos del GNS3

## ANEXO D

### Planificador Aruba Exterior RF

Diseñar una red de RF puede ser una tarea complicada, incluso para los integradores de sistemas con experiencia y red arquitectos. El Planificador de Aruba exterior RF hace que sea rápido y fáciles de diseñar con precisión las redes Mesh 802.11n para cumplir con los requisitos técnicos y de negocio de los clientes.

El Planificador de RF al aire libre es una aplicación gratuita basada en la Web esto es especialmente diseñado para aplicaciones en exteriores. Sistemas integradores pueden utilizar la herramienta de planificación de topología gráfica de visualizar completamente la red de malla inalámbrica, incluyendo Mapas RF calor cobertura, el acceso de clientes y enlaces de malla. Ella proporciona el diseño de redes de malla experto orientación y elimina la necesidad de tiempo cálculos manuales.

El Planificador de RF exterior acelera el proceso de diseño de las redes de malla al aire libre. En muchos casos, los integradores de sistemas pueden reducir el tiempo de planificación de semanas a días o incluso horas. La herramienta de planificación está diseñado para ser utilizado tanto por los ingenieros de RF y los ingenieros de red, y puede proporcionar una gran cantidad de información sobre la planificación antes de hacer ninguna de las visitas in situ o encuestas.

Como una aplicación basada en la web, el Planificador de RF al aire libre pone complejidad en la nube - no en el ordenador del ingeniero. El planificador de RF al aire libre hace que los cálculos de la red de malla utilizando un innovador método de escala en la marcha. Los diseñadores pueden cambiar fácilmente los parámetros de RF, y el diseño es uniforme y escalado rápidamente. (Network A. , 2015)

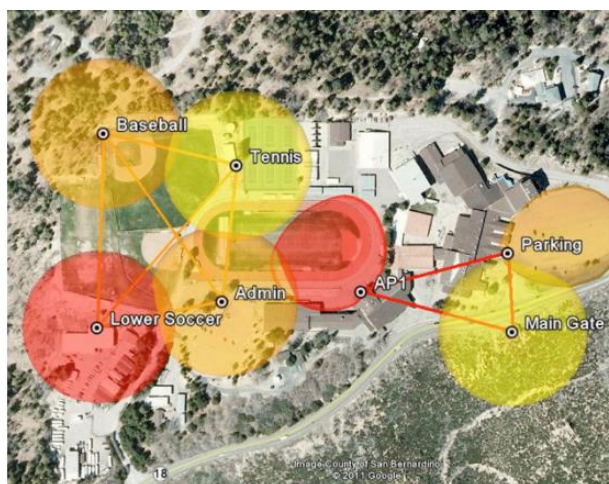


Figura 169. Visualización de cobertura WiFi  
<http://www.prologixme.com/IT-Infrastructure/Networking-Wireless/Wireless-Tool-RF-Planner>

## ANEXO E

### Diagrama de una Red Mesh/Backbone

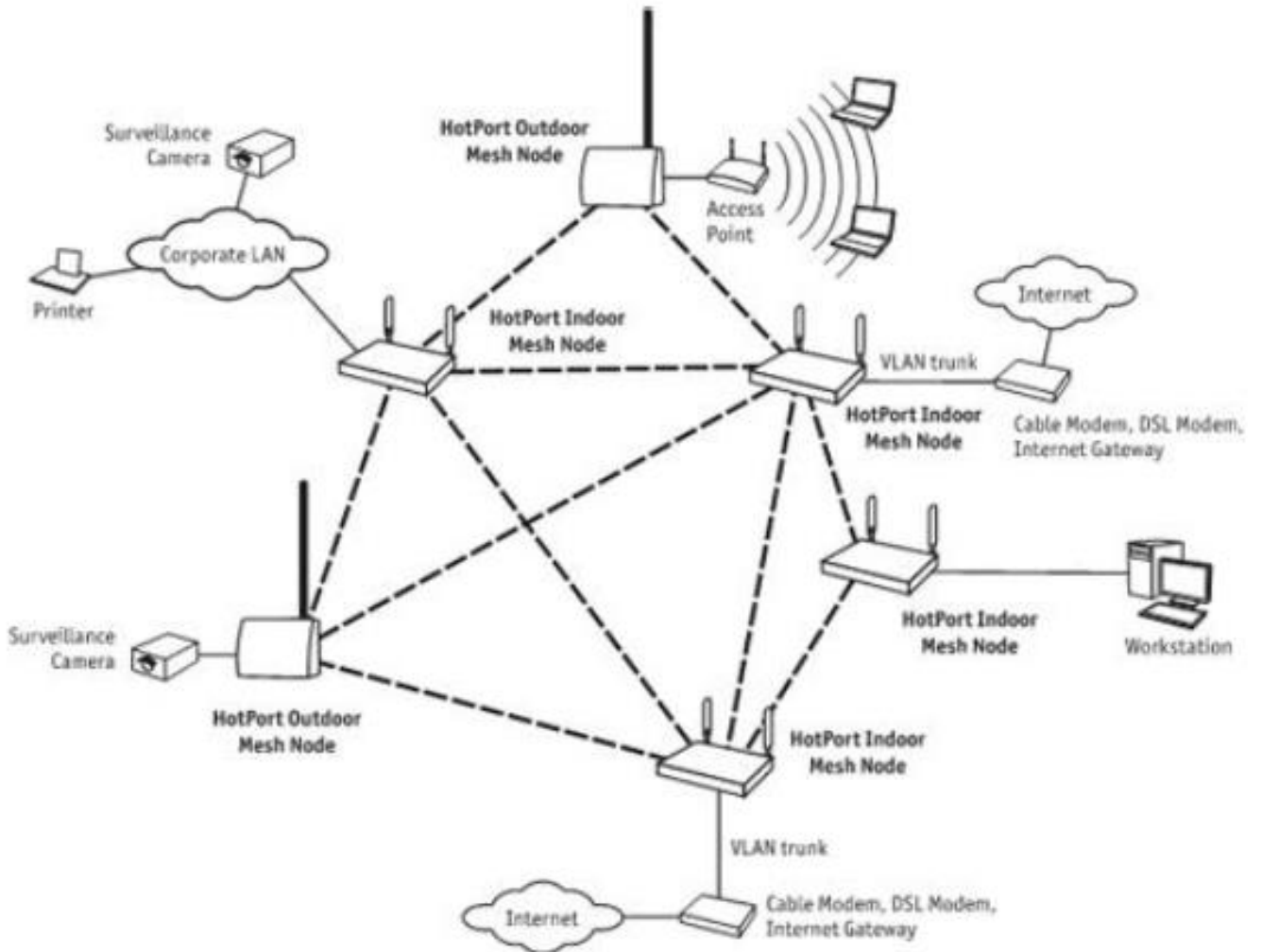


Figura 170. Topología de una Red Mesh  
<http://es.slideshare.net/andresgom/investigacion-red-inalambrica-comunitaria>

## ANEXO F

### Posibles escenarios para simulación de la Red

1. Guerrero Chimalli Ubicado en Av. Bordo de Xochiaca Municipio de Chimalhuacán



Figura 171. Guerrero Chimalli

[http://www.tiempo.com.mx/\\_notas/2044850](http://www.tiempo.com.mx/_notas/2044850)

2. Hospital General Dr. Gustavo Baz Ubicado en Av. Adolfo López Nezahualcóyotl



Figura 172. Hospital Dr. Gustavo Baz

[http://salud.edomex.gob.mx/Html/umedicasvista3i.htm?cve\\_clues=MCSSA004231](http://salud.edomex.gob.mx/Html/umedicasvista3i.htm?cve_clues=MCSSA004231)



3. Centro Universitario UAEM Texcoco. Ubicación Av. Jardín Zumpango s/n, Fraccionamiento el Tejocote 56159 Texcoco Mex.



Figura 173. C.U UAEM Texcoco

[http://sic.conaculta.gob.mx/ficha.php?table=universidad&table\\_id=1725](http://sic.conaculta.gob.mx/ficha.php?table=universidad&table_id=1725)

4. Municipio de Nezahualcóyotl Estado de México

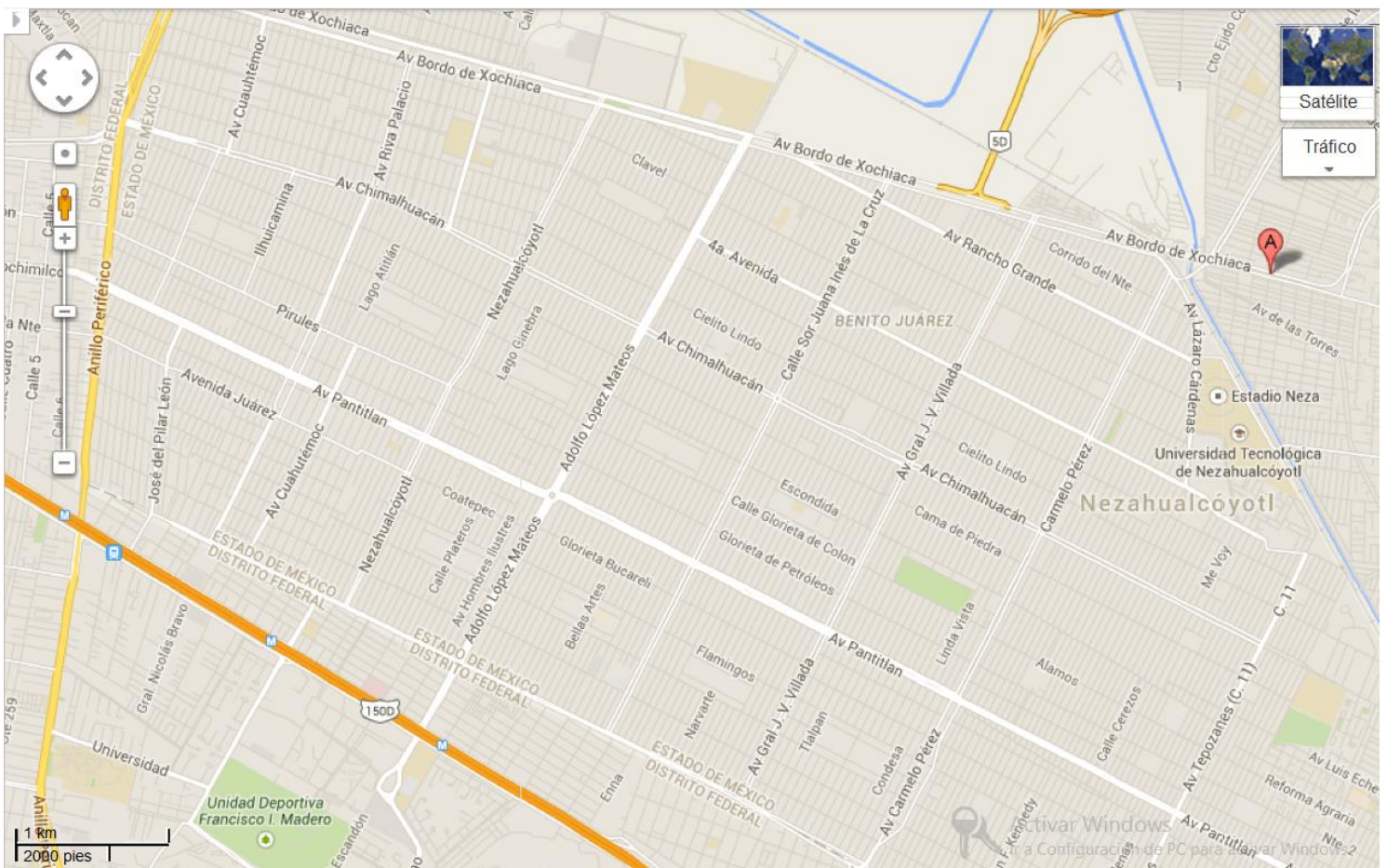


Figura 174. Municipio de Nezahualcóyotl

<https://www.google.com.mx/maps>

## ANEXO G

### HOTSPOT

En el contexto de las comunicaciones inalámbricas, un hotspot («punto caliente») es un lugar que ofrece acceso a Internet a través de una red inalámbrica y un enrutador conectado a un proveedor de servicios de Internet.

Usualmente, los "hotspots" son zonas de alta demanda de tráfico, y que por tanto el dimensionamiento de su cobertura está condicionado a cubrir esta demanda por parte de un punto de acceso o varios, y de este modo proporcionar servicios de red a través de un proveedor de servicios de Internet Inalámbrico (WISP).

Los hotspots se encuentran en lugares públicos, como aeropuertos, bibliotecas, centros de convenciones, cafeterías, hoteles, etcétera. Este servicio se puede cubrir mediante Wi-Fi y permite mantenerse conectado a Internet en lugares públicos. Puede brindarse de manera gratuita o pagando una suma que depende del proveedor. (Android, 2015)



Figura 175. Logo WiFi Hotspot

[http://www.123rf.com/photo\\_22372224\\_free-internet-wifi-hotspot-rectangle-sign.html](http://www.123rf.com/photo_22372224_free-internet-wifi-hotspot-rectangle-sign.html)



Figura 176. Logo WiFi Poste Caliente

<http://yourkomposition.com/virtual-router-plus-free-wifi-hotspot-software/>

## ANEXO H

### AYUNTAMIENTO DE NEZAHUALCOYOTL

Este proyecto fue llevado al palacio municipal de Nezahualcóyotl estado de México con el fin de una sustentación más sólida y factible, dicho proyecto fue dirigido de primera instancia al departamento de obras públicas ya que es el encargado del desarrollo de la infraestructura del municipio y por consiguiente es quien destina los recursos para llevar acabo dichas obras, unas ves mencionado el proyecto fue canalizado a la dirección de administración donde se evaluaría más a fondo por el director de la área ya mencionada el Lic. Juan Manuel Pérez Ramírez el cual planteo algunas cuestiones económicas dicho todo esto el director del área nos menciona que el proyecto no puede entrar o ser sujeto a concurso sin antes concluir dicha administración la cual termina a finales del año en curso, pasada la fecha el ayuntamiento contemplaría el proyecto llevándolo a una aprobación para ponerlo en marcha. (Nezahualcoyolt, 2009)



Figura 177. Lobo súper sayayin  
<https://www.facebook.com/Ayuntamiento.Neza>



Figura 178. Palacio Municipal Nezahualcóyotl  
<http://www.alianza.mx/nota.php?nota=803>

ANÁLISIS DE LA RED DEL  
CENTRO UNIVERSITARIO  
UAEM TEXCOCO  
(APORTE)

## **Análisis de la Red del Centro Universitario UAEM Texcoco (Aporte)**

En este capítulo se realizó un explícito y muy detallado análisis de la infraestructura de red del Centro Universitario UAEM Texcoco, teniendo en cuenta modelos especificaciones técnicas, precios e información del personal encargado de las telecomunicaciones, todo esto nos llevó a obtener y conocer el estado actual de la red así como los términos y condiciones además de la eficiencia en que opera dicha red. Una vez realizado este análisis hemos generado estadísticas con la diferente tipo de información que han arrojado nuestras investigaciones, la información ha sido evaluada y analizada, esto nos ayudó a determinar y con esto detectar fortalezas como debilidades de la red. Este análisis nos ha sido de gran ayuda para mejorar no solo la infraestructura de red sino también para mejorar la calidad de la educación que ofrece el centro universitario.

## **Antecedentes de la Red del Centro Universitario UAEM Texcoco**

El Centro Universitario UAEM Texcoco tiene una tasa de alumnos de 3600 dividido en dos turno matutino con 2000 y vespertino con 1600, la universidad ha estado sujeta a diversos proyectos de actualización y restructuración de red incluyendo herramientas de enseñanza en las aulas auditorios etc. Este proceso evolutivo no se ha concretado por falta de recursos. La red actual del centro ha sido paulatinamente complementada por diversas implementaciones un ejemplo de esto es la implementación de fibra óptica en todo el centro situando el rack en la sala central del edificio B.

En la actualidad la tecnología de redes informáticas han revelado su gran utilidad, esto permite aprovechar y maximizas los métodos de enseñanzas de las instituciones educativas. La red informática son herramientas en las que el centro universitario ha puesto un gran interés para adoptarlo como apoyos para la enseñanza educativa. El contar con una red informática por cada centro universitario significa un gran paso en las telecomunicaciones en este caso la comunicación entre los mismos y por supuesto con la máxima casa de estudios (UAEM Toluca).

Para esto el Centro Universitario cuenta con una red informática constituida por medios guiados y no guiados con una conexión a internet que esta provista por el ISP de Toluca servicio que es compartido por todos los usuarios de la comunidad estudiantil, en este caso para bajar información enviar datos realizar diversas tareas curriculares, cabe mencionar que todo esto está coordinado por personal de RTIC personal capacitado encargado de dar soporte técnico y mantenimiento a las telecomunicaciones del centro. Cabe mencionar que UAEM Texcoco recibe mantenimiento de manera lógica desde C.U Toluca por medio del túnel (VPN) que permite la comunicación entre las dos instituciones.

En el siguiente diagrama se observa el esquema general de red de C.U Texcoco y la comunicación con el ISP de Toluca así como como la distribución de señal con los demás centros universitarios: (Ramirez, Antecedentes UAEM Texcoco, 2014)

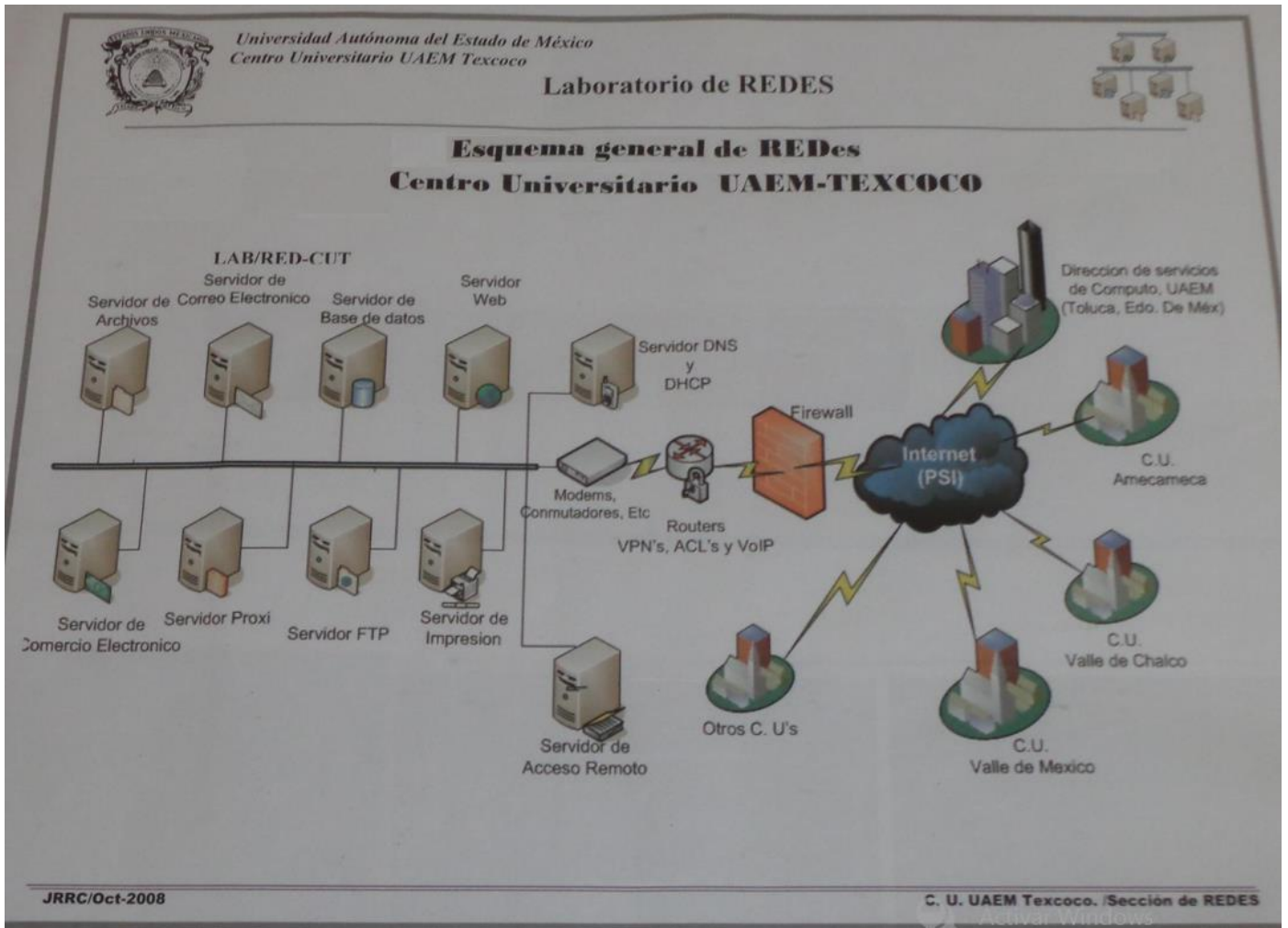


Figura 179. Esquema general de la red UAEM Texcoco  
 Fuente: Laboratorio de Redes C.U Texcoco, Fraccionamiento el Tejocote, 2014

## Ubicación del Centro Universitario UAEM Texcoco

Ubicación: Google Maps



Figura 180. Mapa de la ubicación de UAEM Texcoco, 2014  
<http://www.google.es/maps>

## Plano de distribución de C.U Texcoco



Figura 181. Distribución de UAEM Texcoco

[http://www.sic.conaculta.gob.mx/ficha.php?table=universidad&table\\_id=1725](http://www.sic.conaculta.gob.mx/ficha.php?table=universidad&table_id=1725)

- 1- Edificio A Ciencias Sociales y Humanidades
- 2- Edificio B Ciencias Aplicadas
- 3- Edificio C Ciencias Económico Administrativas
- 4- Edificio D Posgrado
- 5- Edificio E Incubadora
- 6- Gimnasio
- 7- Edificio F Biblioteca
- 8- Edificio G
- 9- Aulas Móviles
- 10- Caseta de Vigilancia
- 11- Estacionamiento
- 12- Canchas



## Diario de Antecedentes

El siguiente diario de antecedentes se aplicó por el encargado de la oficina de RTIC durante un periodo de quince días y estas fueron las fallas más comunes:

- Saturación de red: Un punto fundamentalmente importante los usuarios que demandan conexión a internet vía Wifi se ve fallida debido a un ancho de banda sumamente bajo le es imposible brindar de señal a innumerables clientes, sufriendo así la des configuración del Access Point principal.
- Contagio de virus: Se hacen presentes en las salas de cómputo debido al constante intercambio de información con dispositivos extraíbles y el no tomar las medidas correspondientes como el análisis de la misma mediante el uso de antivirus, el funcionamiento de los equipos no es óptimo.
- Problemas de impresión: Las impresoras que se encuentran activas, pero cuando se envía un trabajo de impresión, este simplemente no sale debidamente por causas distintas desde papel atascado, falta de tinta o tóner en su defecto niveles insuficientes, además de una lenta reacción al momento de imprimir debido a los datos tan abundantes que se mandan a imprimir tarda mucho en procesarse.
- Cables dañados El dispositivo se puede conectar, pero el rendimiento es muy pobre. En otros casos el dispositivo no se puede conectar.
- Duplicidad de IP: Esto sucede principalmente cuando tenemos dispositivos con IP fija, la misma se auto asigna a otra PC y es cuando tenemos conflictos de asignatura de IP.
- Pérdida de gestión de AP Principal: Teniendo un concentrador de Ap Aruba, el cual continuamente se pierde la gestión sobre los Ap debido a la saturación por usuarios provocando la caída de conexión a internet. (Ramirez, Antecedentes UAEM Texcoco, 2014)

# Infraestructura del Centro Universitario UAEM Texcoco

## Diagrama del estado actual de la red

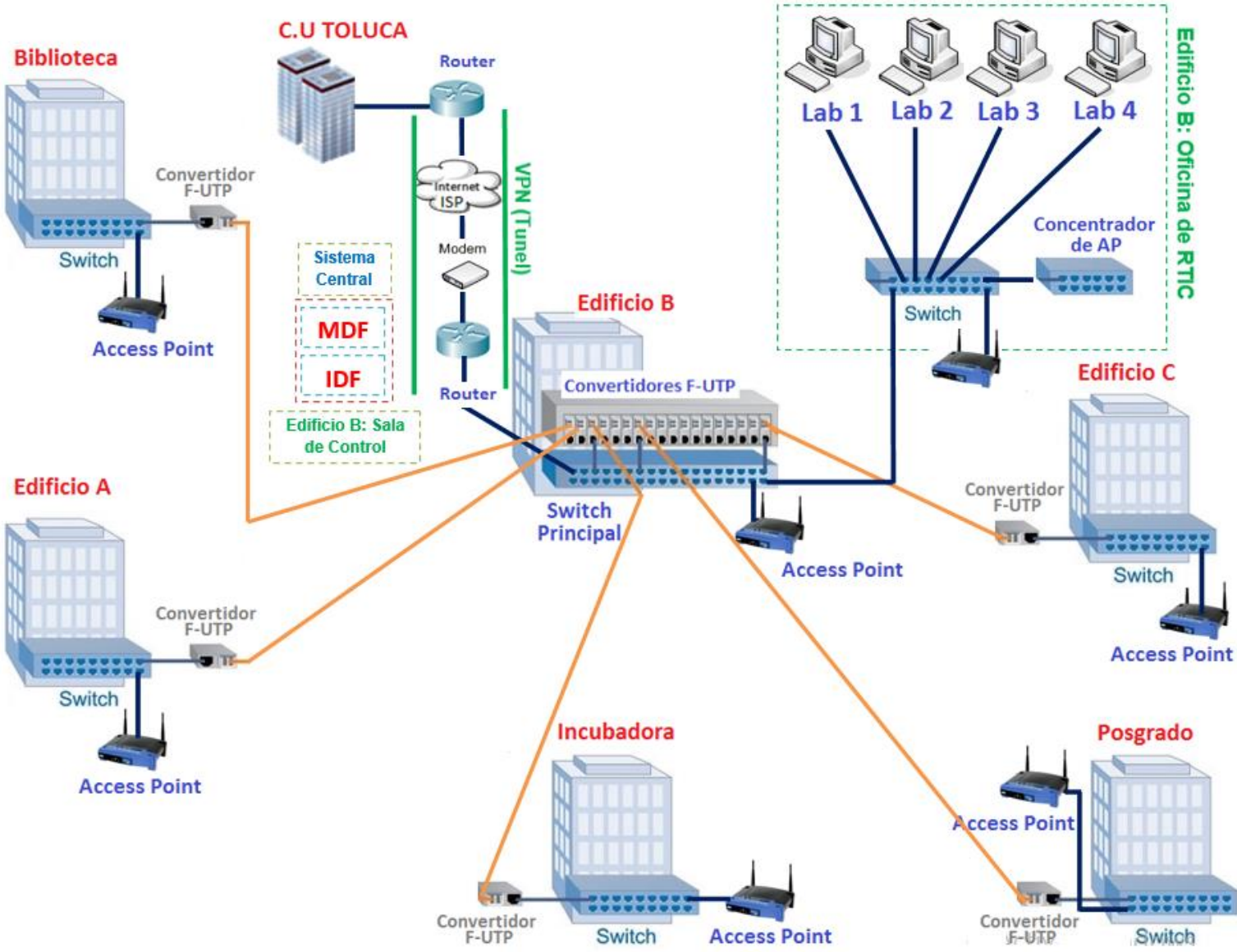


Figura 182. Red actual de UAEM Texcoco  
Fuente: Infraestructura C.U Texcoco, Fraccionamiento el Tejocote, Texcoco 2014

# Red Inalámbrica C.U Texcoco

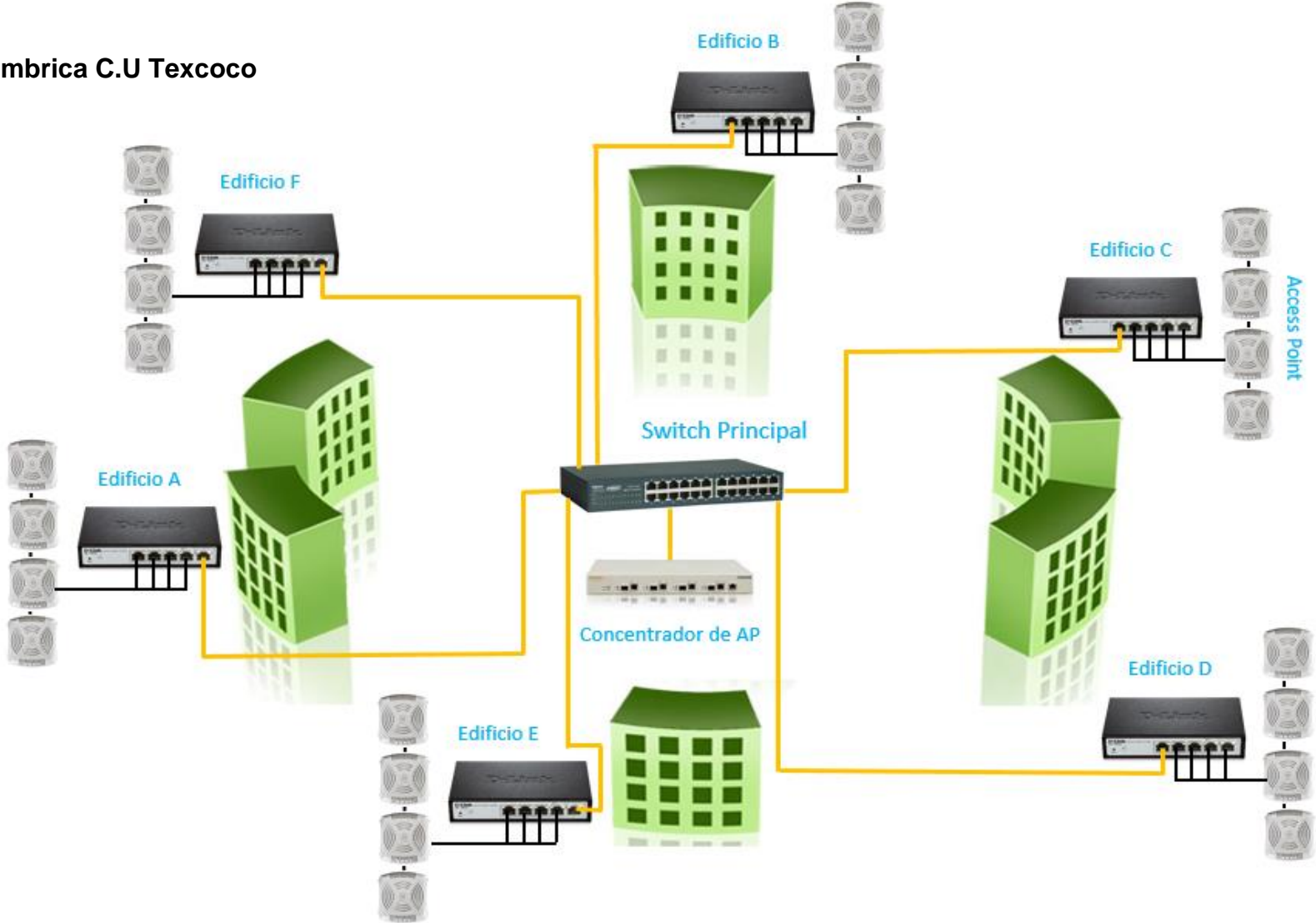


Figura 183. Red inalámbrica actual de UAEM Texcoco  
Fuente: Infraestructura C.U Texcoco, Fraccionamiento el Tejocote, Texcoco 2014

## Plano de los laboratorios de Cómputo (Edificio B Planta alta)

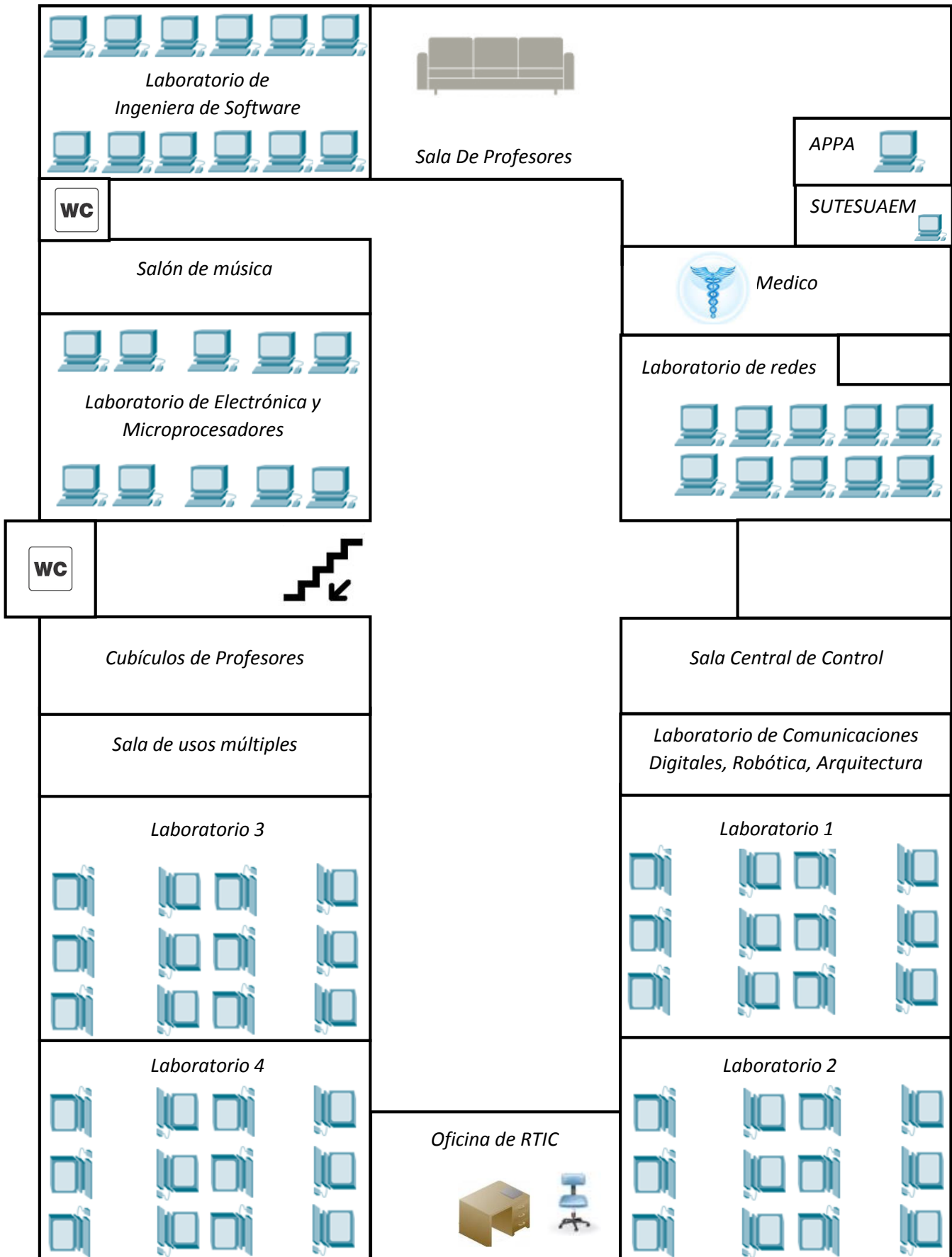


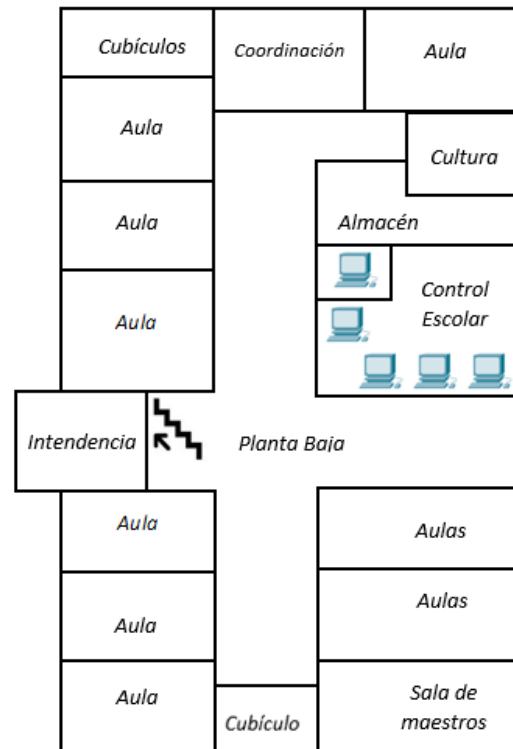
Figura 184. Distribución de los laboratorios de computo C.U Texcoco  
 Fuente: Infraestructura C.U Texcoco, Fraccionamiento el Tejocote, Texcoco 2014

## Descripción de los equipos de cómputo

Plano de Control Escolar: cuenta con una conexión directa a C.U Toluca por medio del VPN (Túnel)

Cuenta con 5 máquinas con las siguientes características:

HP PRO 3200 Series Mt  
Procesador AMD  
4gb en RAM  
Disco duro de 500gb  
Windows 7



Laboratorio de Ingeniería de Software:  
32 equipos Hp Compaq 6005  
Procesador AMD Ahlon II X2  
2gb de RAM  
500gb en Disco duro  
Windows 7  
Monitor 15"



Laboratorio de Redes  
36 Equipos Hacer Aspire AM3970  
Procesador Core i5 2320  
RAM 12gb  
Disco duro 2tb  
Lector DVD  
LAN 10/100/1000 Integrado  
Windows 7



Figura 185. Plano de control escolar y equipos de cómputo  
Fuente: Infraestructura C.U Texcoco, Fraccionamiento el Tejocote, Texcoco 2014

---

Laboratorio de Electrónica  
30 Maquinas HP P7 1180  
Procesador Core i7  
RAM 8gb  
Disco duro 2tb  
Windows 7



---

Laboratorios 1-2-3-4  
Cuenta con 20 máquinas cada uno  
Hp Pro 3200 Series Mt  
Procesador AMD E2  
4gb RAM  
Disco Duro 500gb  
Windows 7



---

Figura 186. Computadoras Hp  
<http://www.hp.com>

### **Descripción de la estructura y paredes de los edificios**

- Planta alta del edificio B en su mayoría los departamentos están contruidos en este edificio son de concreto solido separados por paredes de ladrillo hueco y algunas otras cuentan con divisiones elaboradas con tabla roca, cuentan con mobiliario habitual de una oficina ( escritorios, sillas gavetas etc.) Es por eso que en el área existe la perdida de señal de internet.
- Auditorios: Están alfombrados, casi en su totalidad sus paredes son de concreto, tienen una revestida de madera en el área del exposición cuentan con butacas y varios proyectores conectados alambicamente.
- Laboratorios de cómputo: Los laboratorios de cómputo cuentan con paredes de concreto y ladrillo hueco y una división de un muro corredizo.

## Descripción técnica de la infraestructura de Red

### Definición de MDF

En telefonía, un Main Distribution Frame (MDF, Main Frame o en ocasiones denominado Site) es una estructura de distribución de señales para conectar equipo de redes y telecomunicaciones a los cables y equipos que corresponden al proveedor de servicios de telefonía, Internet, entre otros. El MDF es un punto final dentro de la central telefónica local donde el equipo y las terminaciones de bucles locales son conectados por un jumper. Todos los pares de cable de cobre que proveen de servicios a través de líneas telefónicas llegan al MDF y son distribuidos hacia los equipos dentro de la central, tales como repetidores y DSLAM. Asimismo, los cables de los IDFs, es decir, de estructuras intermedias de distribución de señales, también deben terminar en el MDF. El IDF es un recinto de comunicación secundaria para un edificio que usa una topología de red en estrella. El tipo más común de un MDF grande es un estante largo de acero, accesible desde ambos lados. En uno de ellos, las terminales eléctricas son acomodadas horizontalmente en el frente de las repisas del estante. (Commons, 2013)

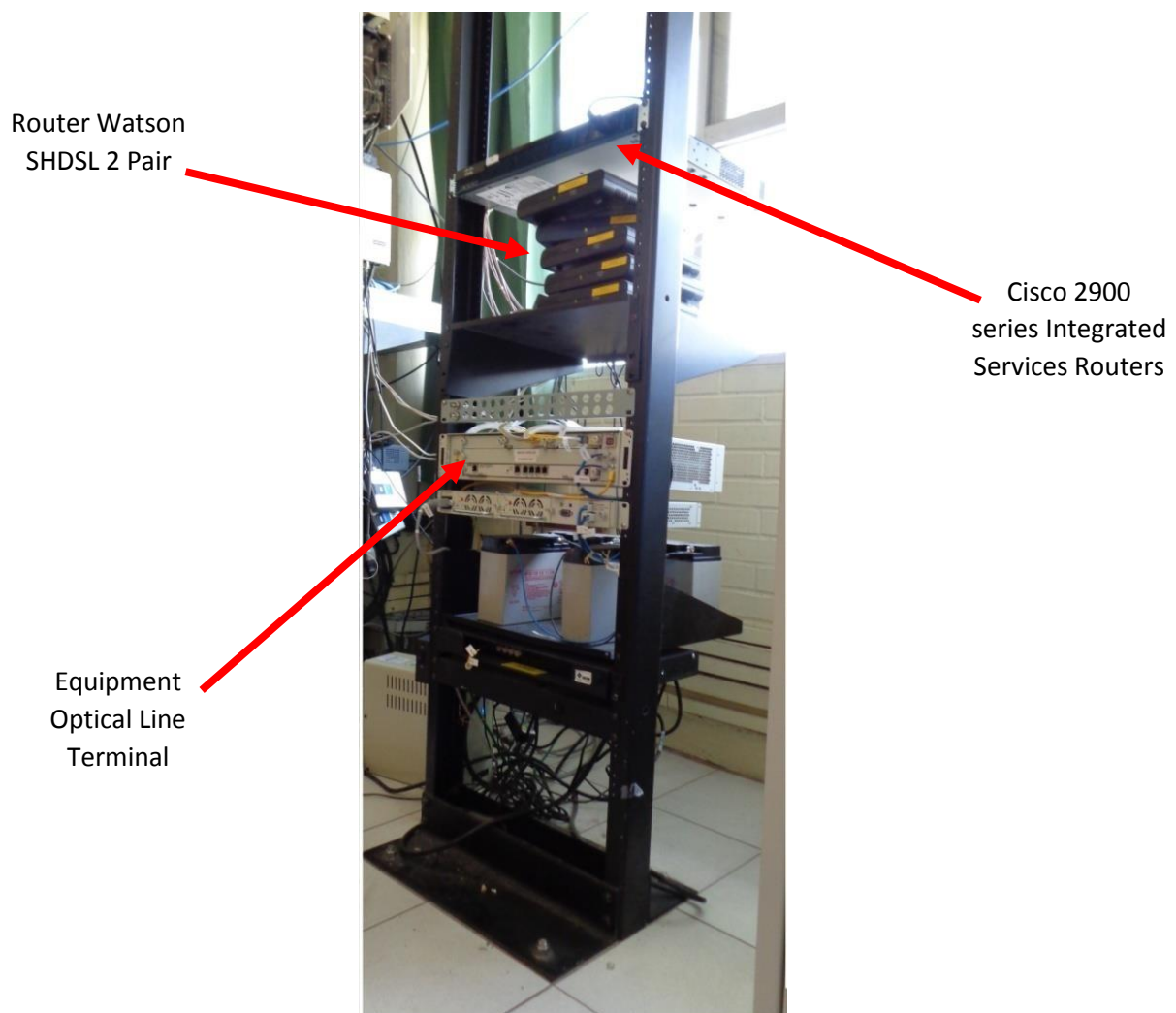


Figura 187. : Recinto de comunicación principal MDF

Fuente: RTIC, Infraestructura C.U Texcoco, Fraccionamiento el Tejocote, Texcoco 2014

## Componentes del MDF:

### Router Watson SHDSL 2 Pair

Watson serie de routers SHDSL de Schmid Telecom es una innovadora solución DSL de próxima generación diseñada para permitir simétrico a Internet de alta velocidad o la conectividad punto a punto a los clientes de negocios. Enrutador Watson SHDSL utiliza Ethernet en la tecnología Primera Milla (EFM), que es una extensión transparente de las LAN basadas en Ethernet en redes de área amplia. No se requiere ninguna conversión de formatos de paquetes al transitar entre la LAN y WAN.

Esta transparencia simplifica enormemente las operaciones de red, reduce los costos de implementación, y aumenta los niveles de servicio. EFM incluye funciones de mantenimiento que hacen que la operación de grandes redes Ethernet de área amplia posible. La serie de routers Watson SHDSL cuenta con dos o cuatro puertos SHDSL. Velocidades de datos simétricas de hasta 5.7Mbit / s están disponibles en cada par de cobre. Utilizando EFM vinculación de los pares, velocidades de datos de 22,8 Mbit / s más de 4 pares de cobre se puede lograr.

El router Watson SHDSL integra también un conmutador Ethernet de ocho puertos y una puerta de enlace VPN, que proporciona características de seguridad Firewall robustos y Virtual Private Network túnel estándar IPsec. La larga experiencia de Schmid Telecom en soluciones DSL asegura que la serie del router Watson SHDSL entrega más largo alcance y alto rendimiento. (Ges, 2009)



Figura 188. Router Watson SHDSL 2 Pair

<http://www.schmid-telecom.ch/page.php?t=template2&templateID=318&language=en>



## Cisco 2900 Series Integrated Services Routers

Cisco 2900 Series Integrated Services Routers (ISR) están diseñados para satisfacer las demandas de las aplicaciones de ramas medianas de hoy y de evolucionar a los servicios basados en la nube. Entregan aplicaciones virtuales izadas y colaboración altamente segura a través de la más amplia gama de conectividad WAN de alto rendimiento que ofrece servicios simultáneos de hasta 75 Mbps. **(Cisco, 2008)**



Figura 189. Cisco 2900 Series  
<http://www.cisco.com>

## Equipment Optical Line Terminal

Una terminación de línea óptica (OLT), también llamado un terminal de línea óptica, es un dispositivo que sirve como el proveedor de servicios de punto final de una red óptica pasiva . Proporciona dos funciones principales:

- para llevar a cabo la conversión entre las señales eléctricas utilizadas por los equipos del proveedor de servicios y las de fibra óptica señales utilizadas por la red óptica pasiva.
- para coordinar la multiplexación entre los dispositivos de conversión en el otro extremo de dicha red (llamada ya sea terminales de red ópticos o unidades de red óptica ).

OLTs incluyen las siguientes características:

- Un medio de procesamiento de tramas de aguas abajo para recibir y produciendo un modo de transferencia asíncrono célula para generar una trama de aguas abajo, y la conversión de un conjunto de datos paralelos de la trama de aguas abajo en una serie de datos de los mismos.
- Un medio de multiplexación por división de longitud de onda para la realización de un / conversión electro óptico de la serie de datos de la trama de aguas abajo y la realización de una multiplexación por división de longitud de onda de la misma.
- Un medio de procesamiento de tramas aguas arriba para extraer datos de los medios de multiplexado por división de longitud de onda, en busca de un campo de arriba, la delimitación de una frontera ranura, y el procesamiento de una administración operaciones de la capa física y mantenimiento (PLOAM) celular y una ranura dividido por separado.
- Un medio de generación de señal de control para realizar un control de acceso de medios (MAC) de protocolo y de generación de variables y señales de temporización utilizado para los medios de procesamiento marco de aguas abajo y los medios de procesamiento marco de aguas arriba.

- Un medio de control para controlar los medios de procesamiento de trama descendente y el procesamiento de tramas de aguas arriba significa mediante el uso de las variables y las señales de temporización de los medios de generación de señal de control.

## **Huawei OptiX 155/622**

El Metro OptiX 1000 puede acceder a múltiples tipos de servicios y se puede utilizar en la capa de acceso de las redes de área metropolitana (MAN) y redes de transmisión locales para acceder a líneas privadas VIP, estaciones base inalámbricas, y multiplexores de acceso de línea de abonado digitales (DSLAM). En el caso de los servicios Ethernet, los Metro 1000 apoyos que transmiten los servicios en los dos dominios siguientes en una red: la multiplexación por división (TDM) dominio del tiempo tradicional y la red de transporte de paquetes domain. In el caso de los servicios de Ethernet en el dominio de paquetes, el OptiX Metro 1000 proporciona una función de convergencia de pequeña escala. Específicamente, el equipo converge servicios de múltiples puertos FE en una sola GE port. In en el caso de que el dominio TDM y el dominio de paquetes se admiten en la misma red, una migración suave desde la red TDM a la red de paquetes se puede lograr.

## **Huawei Optix Metro 1000 SS-TDA**

Especificaciones

Multifunciones señales de audio analógicas

señales de datos de baja velocidad en señales E1

Descripción del producto

**Metro OptiX 1000** producto es un nueva generación de STM-1 / STM-4 equipos compatibles con la transmisión de múltiples servicios, proporciona t él STM-1 / STM-4 función de sincronización de transmisión óptica, su velocidad de línea se puede actualizar en línea desde STM-1 a STM-4. Metro OptiX 1000 producto proporciona rico s interfaz de negocio y la capacidad tapón potente de conexión cruzada. (Huawei, 2014)

### **Características del producto**

Tamaño pequeño con bajo consumo de energía.

El tamaño de la caja de la máquina es de 436 mm x 293mm x 86mm (W x D x H), la altura es de 2U, con una configuración típica, el consumo de energía es menos de 50W, y se puede acceder a-48V, 24 V, 110 V / directamente 220V.

M interfaz multiservicio s

Configuración flexible

La creación de redes flexibles

Bien protegido-

Modo de transmisión flexible DCC

Función maduro NMS

Excelentes funciones de gestión SSM

Características físicas:

OptiX Metro 1000

El acceso de la energía 220V AC / DC 48V / + 24V DC

Apoyo a la gestión de la batería

Formas de instalación: montado en la pared, y ETS 300mm gabinete profundo, ETS gabinete de profundidad 600 mm, instalado en un gabinete de 19

pulgadas.

Tamaño: 436 mm x 293mm x 86mm (W x D x H)

Peso <8.1kg

Consumo de energía <100W

### **Stm-1 Equipment Huawei Metro 1000**

Especificaciones. Huawei Optix Metro 1000 (155 / 62H) apoya STM-1, STM-4 y STM-16 Rate.Descripción del producto:

Metro OptiX 1000 producto es un multi-servicio de equipos de transmisión de nueva generación de STM-1 / STM-4 compatible, la función de la transferencia sincrónica proporcionar STM-1 / STM-4 luz, velocidad de línea se puede actualizar en línea desde STM-1 a STM -4. Metro OptiX 1000 producto proporciona una rica interfaz de negocio y poderosa capacidad de cruzar.

Características

Tamaño pequeño, bajo consumo de energía, el tamaño de la caja de la máquina 436 mm x 293mm x 86mm (W x D x H), la altura de 2U), una configuración típica, el consumo de energía es menos de 50W, puede acceder a-48V directamente, 24 V, 110 V de potencia / 220V.

- Interfaz de negocio Rich
- Interfaz de servicio SDH
- Interfaces de servicios PDH
- Interfaz de servicio de datos
- Interfaz de servicios de voz
- Servicio Privado interfaz de línea
- Interfaz SHDSL
- Interfaz óptica de la serie completa
- Una variedad de especificaciones de la interfaz óptica STM-1
- Una variedad de especificaciones de la 4 interfaces ópticas STM

Las interfaces auxiliares ricos: Sus potentes capacidades de procesamiento de arriba para proporcionar a los usuarios una serie de interfaces de datos Interfaz telefónica analógica de dos hilos, para proporcionar segmentos segmento / reutilización renovables contacto oficial, los usuarios pueden personalizar la interfaz de datos transparente, cambie las entradas y cambiar la interfaz de salida Interfaz de gestión de red Ethernet 10M RS-232 de vigilancia de alimentación

Configuración flexible: Configuración Metro OptiX 1000 es bastante flexible. Cada NE se puede configurar como una sola STM-1/4 TM o el sistema de ADM también se pueden configurar para STM-1, STM-4 interfaces de combinación de sistema de ADM multi, y puede darse cuenta de conexión cruzada multi-sistema; acceder a la necesidad de servicios de datos de ancho de banda puede estar basada en el usuario la flexibilidad para configurar el ancho de banda de transmisión y el puerto Ethernet, para satisfacer la demanda del usuario para el aumento de ancho de banda sin aumentar el puerto y la chapa.

La creación de redes flexibles OptiX Metro 1000 puede proporcionar una variedad de formación de la red, es compatible con una variedad de topologías de red, incluyendo punto a punto, cadena, anillo, anillo con cadena intersectar ring, ring tangente, en forma de malla.

Bien protegido-OptiX Metro 1000 es compatible con una variedad de protección a nivel de red, incluyendo el modo MSP protección, modo de protección SNCP, modo de protección de PP, así como el modo de protección ruta virtual fibra compartida, la protección del reloj, fuente de alimentación 1 1 protección de protección a nivel de dispositivo .

Modo de transmisión flexible DCC: A través del puerto de reloj externo para transferir la información DCC en nuestro equipo; para apoyar DCC de paso a través de la red de equipos de transmisión de información de gestión de otras empresas; la interfaz de gestión de red también puede estar conectado a la placa de interfaz de Ethernet, la información de gestión de la red de transmisión.

NMS destacado OptiX Metro 1000 y productos de la serie Optix adoptan una plataforma de gestión de red unificada para la operación centralizada, mantenimiento y gestión (OAM), configuración del circuito y la programación y funcionamiento de la red.

Excelentes funciones de gestión SSM Metro OptiX 1000 reloj NE tiene las funciones de gestión de SSM. Su puerto de sincronización externa pueden recibir directamente cronómetro información de sincronización puerto de salida externa con el MSE, y se puede ajustar con flexibilidad la poco SSM en 2048 kbit / externa s de la señal, la señal de entrada de 2 MHz está ajustado manualmente los mensajes SSM en soporte externo, fácil con otro equipos de fabricantes umbral SSM de cada elemento de red se puede configurar, a fin de facilitar la gestión de la red de sincronización.

Un rendimiento de la sincronización de reloj superior, Como fuente de oscilador de cristal interno del estado de la técnica de alta precisión, con una dedicada al chip de procesamiento de reloj, para asegurar que los indicadores técnicos en pleno cumplimiento con los requisitos de la Recomendación UIT-T G.813 recomiendan. El sistema de distribución puede funcionar en modo de seguimiento, el modo y el modo de oscilación libre sostener. El sistema de cronometraje proporciona la SSM. Cuando se trabaja en el modo de seguimiento, se puede seleccionar arbitrariamente línea, rama, una de la fuente de sincronización de reloj externa como fuente de reloj de referencia; seleccionada la función de reloj prioridad, para garantizar un funcionamiento fiable del sistema de temporización de la red. (Huawei, 2014)

Características físicas:

- OptiX Metro 1000
- el acceso de energía
- 220V AC / DC 48V / + 24V DC
- Apoyo a la gestión de la batería
- instalación
- Montado en la pared, y ETS 300 mm de profundidad gabinete, el gabinete de profundidad ETS 600 mm, instalaron un bastidor de 19 pulgadas
- tamaño
- 436 mm x 293mm x 86mm (W x D x H)
- peso
- <8.1kg
- consumo de energía

### **IDF Definición:**

Instalación de distribución intermedia recinto de comunicación secundaria para un edificio que usa una topología de red en estrella. (Commons, 2013)

Topología estrella extendida:

Una red en estrella es una red en la cual las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de éste. Dado su transmisión, una red en estrella activa tiene un nodo central activo que normalmente tiene los medios para prevenir problemas relacionados con el eco.

Se utiliza sobre todo para redes locales. La mayoría de las redes de área local que tienen un enrutador (router), un conmutador (switch) o un concentrador (hub) siguen esta topología. El nodo central en estas sería el enrutador, el conmutador o el concentrador, por el que pasan todos los paquetes.

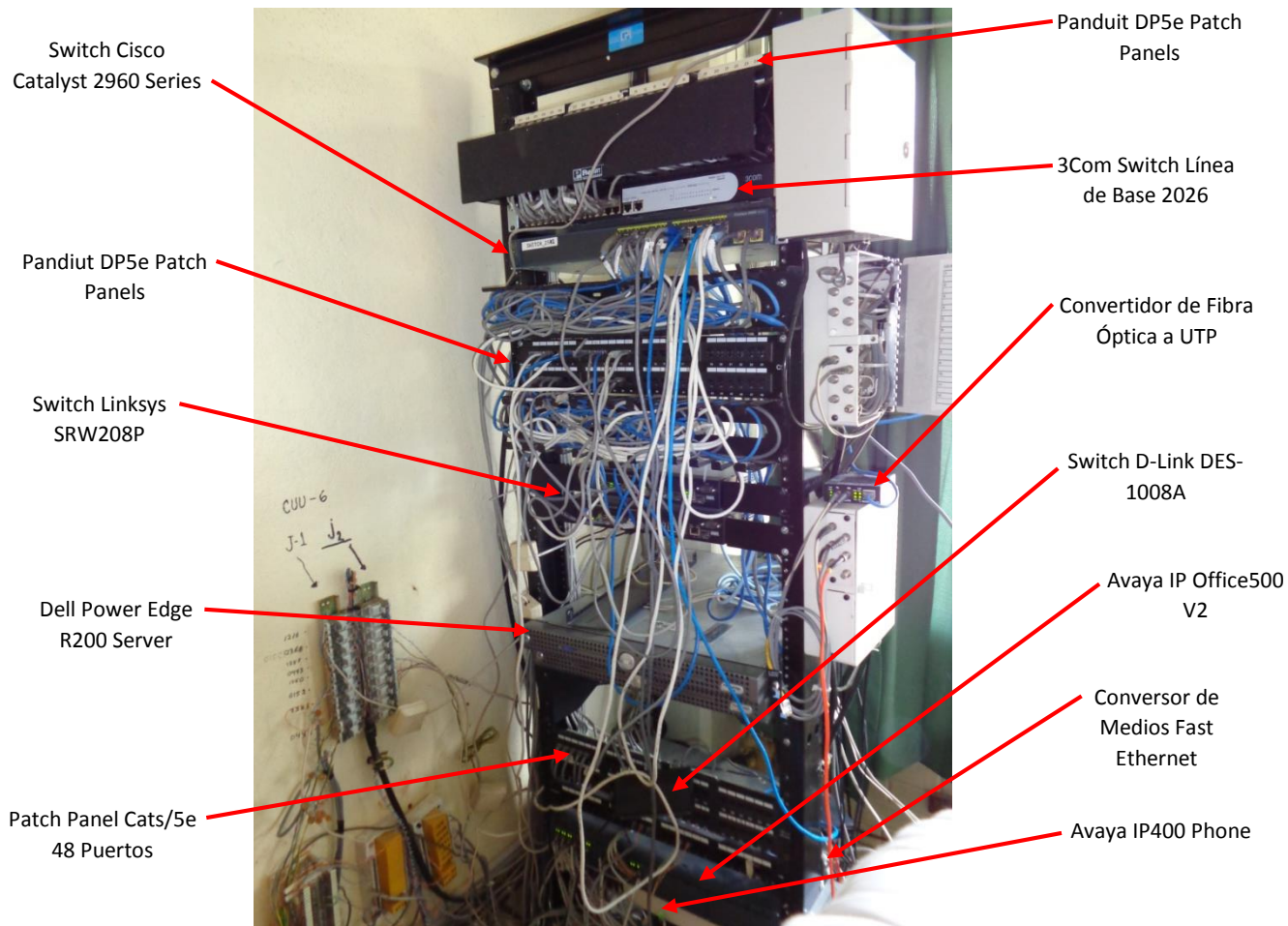


Figura 190. Recinto de comunicación secundaria IDF

Fuente: RTIC, Infraestructura C.U Texcoco, Fraccionamiento el Tejocote, Texcoco 2014

### Componentes del IDF:

#### Panduit DP5e Patch Panels

Con paneles de parcheo Panduit DP5e y DP6 Plus, sus sistemas de redes y de telefonía pueden ser fácilmente organizados independientemente de la complejidad de la aplicación. Al conectar todos los cables en este centro, a evitar la confusión de cables desordenados y que no dejan huella. Los paneles pueden ser utilizados para configuraciones Cat5e o Cat6 cable Ethernet. (COMDIEL, 2009)



Figura 191. Patch panel DP5e

<http://www.schmid-telecom.ch/page.php?t=template2&templateID=318&language=en>

### 3Com Switch Línea de base 2026 (3CBLUF26)

El 3Com Switch Línea de base 2026 es versátil y fácil de usar, conmutador no administrado. Es ideal para los usuarios que desean el rendimiento de alta velocidad de conmutación 10/100 pero que no necesitan funciones de gestión sofisticadas. El interruptor se envía listo para su uso, y operativo en línea recta de la caja. Sin configuración es necesario. Su 3Com Switch Línea de base incorpora lo último en verde La tecnología para producir más de 20% de ahorro de energía que la generación anterior productos. (Com, 2008)

Tabla 19: Especificaciones técnicas del switch:

Dimensiones	(H x W x D, mm) 44 x 440 x 170 (1,73 x 17,32 x 6,81 in.)
Peso	1,8 kg (3,97 libras).
Puerto Ethernet	10/100 Mbps Puertos: 24
Cantidad:	10/100/1000 Mbps Puertos: 2
Montaje	De pie, o en rack de 19 pulgadas.
Toma de alimentación	IEC 320
Entrada de CA Tensión nominal	Nominal Rango de voltaje: 100 240 V CA, 50/60 Hz
Máximo Clasificación actual	0.45Amp
Máximo Energía Consumo	12 W
Operativo temperatura	0 ° C a 40 ° C (32 ° F a 104 ° F)
Almacenamiento temperatura	-40 ° C a + 70 ° C (-40 ° F a 158 ° F)
Operativo humedad	5% a 95% (sin condensación)
Almacenamiento humedad	5% a 95% (sin condensación)



Figura 192. Switch 2026  
<http://www.3com.com>

## Switch Cisco Catalyst 2960 Series

Los switches de Cisco Catalyst 2960 soportan voz, video, datos y acceso seguro. Ofrecen una administración escalable conforme cambian las necesidades de su negocio. (Cisco, 2008)



Figura 193. Switch Cisco Catalyst 2960 Series  
<http://www.cisco.com>

## Patch Panels Cat5/5e de 48 puertos (TC-P48C5E)

Preparase para el gigabit Ethernet sobre cobre con los patch panels de TRENDnet. Los TC-P16C5E, P24C5E, P48C5E son certificados 100MHz CAT 5, los que requieren las redes de Ethernet Gigabit sobre cobre. Los paneles de TRENDnet son ideales para r redes Ethernet/ Fast Ethernet /Gigabit Ethernet (1000 Base-T). Utilizar los paneles de TRENDnet le prepara para el ancho de banda del futuro y evita tener que recablear la red. (COMDIEL, 2009)

Descripción:

- Conectores Krone de categoría CAT 5e con etiquetado por códigos de color para esquemas de cableado T568A y 568B
- Preparado para Gigabit Ethernet sobre cobre de 1000Base-T
- Compatible con cableado CAT 3, 4, 5
- Cumple con las normas EIA/TIA 568a y ISO/IEC 11801
- Garantía limitada de 1 año
- Panel de 48 puertos para instalar en bastidor, listo para conexiones Gigabit
- Los paneles de conexiones Cat5e transmiten de forma continua a 100Mhz a conmutadores Gigabit cobre.
- Solución ideal para aplicaciones Ethernet, Fast Ethernet y Gigabit.
- Utilícelo con la ponchadora "Punch Down" TC-PDT de TRENDnet



Figura 194. Patch panel TC-P48C5E 48 puertos  
<http://www.commdiel.com>



## Switch Linksys SRW208P

El Switch Linksys SRW208P con WebView trae un nuevo nivel de inteligencia y seguridad a la infraestructura de red. La combinación de su inteligencia y su pequeño tamaño lo hace ideal para una sala de conferencias o sala de entrenamiento donde la seguridad y el tiempo de actividad son importantes. Cuenta con dos puertos para conexión Gigabit de cobre o interfaces ópticas a un conmutador central.

Para implementaciones inalámbricas o VoIP, el SRW208P soporta el estándar IEEE 802.3af Power over Ethernet. Con detección automática de carga, el circuito de control de potencia detecta automáticamente Alimentación a través de Ethernet en el dispositivo final antes de proporcionar el poder. Alimentación de energía de Ethernet limitado para los puertos / 100BASE-TX 10BASE-T fijos. La solución puede proporcionar la máxima potencia de salida por puerto PoE hasta 15,4 W en 4 puertos o 7,5 W por puerto PoE en 8 puertos simultáneamente. También incluye la sobrecarga independiente y protección contra cortocircuitos para cada puerto y los indicadores LED para el estado de energía por puerto PoE. (Cisco, Linksys A Division Of Cisco, 2007)



Figura 195. Switch Linksys SRW208p  
<http://www.lynksys.com>

## Dell PowerEdge R200 Server

El crecimiento del centro de datos ha estimulado la necesidad de servidores en el espacio consciente que pueden ofrecer apoyo a aplicaciones sin ocupar el valioso metros cuadrados. El procesador del servidor PowerEdge R200 opciones y chasis rack denso significa que usted puede empacar la cantidad correcta de energía en una forma pequeña factor.

Con la serie de procesadores Quad-Core Intel Xeon 3300 y 3200, el PowerEdge R200 le permite disfrutar de los beneficios de la tecnología de cuatro núcleos. Esta tecnología combina cuatro núcleos de procesamiento en un solo chip del procesador para un rendimiento excepcional y eficiencia energética. Es ideal para ejecutar múltiples aplicaciones y tareas de subprocesos múltiples comunes en muchos de software de hoy aplicaciones.

Para entornos que requieren menos capacidad de procesamiento, el servidor PowerEdge R200 también es compatible con el Dual-Core serie 3000, que ofrece una relación precio / rendimiento generoso para un valor increíble. También puede elegir el procesador Intel Core™ 2 Dúo, Pentium Dual-Core o Celeron® procesador para tareas simples tales como las aplicaciones de impresión y archivos.

El servidor PowerEdge R200 está diseñado para ser capaz de crecer a medida que sus necesidades crecen y como la tecnología evoluciona. La nueva arquitectura de alto rendimiento PCI Express™ ofrece flexibilidad y la inversión protección. El PowerEdge R200 cuenta con una opción de dos bandas-uno con x4 (conector x8) y PCIe x8 ranuras, una segunda con ranura PCIe x8 y PCI-X® 64/133 ranura. Plus, tarjetas de red Gigabit integradas duales ofrecer una alta conectividad de red de ancho de banda, balanceo de E / S de la carga de tráfico y de conmutación por error para el rendimiento y la disponibilidad de datos.

Además, el servidor soporta hasta 8 GB de ECC DDR2-667 / 800 memoria y es capaz de soportar Aplicaciones de 64 bits de modo que usted puede tomar ventaja de las últimas novedades tecnológicas. Ella También soporta hasta dos cableados SATA o SAS discos duros que permite hasta un 2,0 TB de almacenamiento interno capacidad para satisfacer las crecientes demandas de almacenamiento de datos. (DELL, 2010)



Figura 196. Dell PowerEdge R200 Server  
[Hyttp://www.bargainhardware.co.uk](http://www.bargainhardware.co.uk)

## Switch D-Link DES-1008A

El DES-1008A es un Switch No Administrable de 8 puertos Fast Ethernet 10/100BASE-TX. No requiere de configuración y su instalación es fácil y rápida. Soporta MDI/MDI-X en todos sus puertos. **(D-Link, 2013)**

Puertos e Interfaces	Tecnología de cableado Ethernet de cobre 100BASE-TX, 10BASE-T Cantidad de puertos básicos de conmutación RJ-45 Ethernet 8.
Red	Estándares de red IEEE 802.3, IEEE 802.3u, IEEE 802.3x
Control de energía	2.5 W
Condiciones ambientales	Intervalo de temperatura de almacenaje -10 - 70 °C Intervalo de temperatura operativa 0 - 40 °C
Transmisión de datos	Tasa de transferencia (máx) 0.1 Gbit/s Tabla de direcciones MAC 1000 entradas Capacidad de conmutación 1.6 Gbit/s Tasas de transferencia soportadas 10/100 Mbps
Otras características	Velocidad de transferencia (paquete) 14880 - 148800 pps Tecnología de conectividad Alámbrico

Tabla 20. Comparativa entre tecnologías



Figura 197. Switch D-Link DES-1008<sup>a</sup>  
<http://www.link.co.in>

## AVAYA iP Office 500 V2

La Central Telefónica Avaya IP Office 500 es una Plataforma de Comunicaciones que ofrece potentes capacidades de gestión de llamadas para los entornos de comunicaciones más ajetreados.

Las características y flexibilidad de IP Office mejoran el rendimiento y la productividad de todos los que lo utilizan. Las comunicaciones inteligentes para pequeñas y medianas empresas se ocupan de las necesidades básicas de telefonía, aprovechan las capacidades de convergencia y sacan el máximo partido de las robustas aplicaciones unificadas para ofrecer inteligencia tanto a usted como a sus clientes. Avaya IP Office 500 ofrece soluciones que simplifican procesos y racionalizan el intercambio de información entre sistemas para crear experiencias beneficiosas. (Avaya, 2010)



Figura 198. AVAYA IP Office 500 V2  
<http://www.avaya.com>

## AVAYA iP 400 Phone System

Soporta 12 módulos de expansión que ofrecen una combinación de hasta 360 teléfonos analógicos, digitales y teléfonos IP, con capacidad para 8 troncales analógicas o 4 troncales digitales (96 canales T1 / PRI o 120 canales E1). Opcionalmente, también se admiten enlaces troncales SIP. Soporte para troncales analógicas adicionales se puede lograr mediante el uso de módulos de expansión. Las características incluyen 2 puertos LAN conmutada de forma independiente y soporte opcional para hasta 60 canales de compresión de voz.

Proporciona puertos POT para teléfonos analógicos. El módulo del teléfono IP Office 412 está disponible en 3 versiones que dan 8, 16 o 30 extensiones. Teléfonos pueden ubicarse hasta a 1 km de la unidad utilizando cableado CAT5 (ver Auricular longitudes de cable). Este módulo es compatible con el actual sistema de Office de Avaya IP IP 412 y es compatible con la discontinuada IP 403, y plataformas IP 406 IP Office de Avaya. (Avaya, 2010)



Figura 199. AVAYA IP 400 Phone System  
<http://www.avaya.com>

## Convertidor de UTP a Fibra Óptica

EEE802.3u Ethernet admite dos tipos de medios de comunicación para la conexión a la red tales como 10 / 100Base-TX y 100Base-FX. El convertidor de medios de puente está diseñado con un controlador del interruptor y la memoria tampón que conecta dos segmentos tipos de operación sin problemas. Este convertidor puede ser utilizado como unidad independiente o como unidad que permite conexión en el bastidor 483mm (19 ") del convertidor Chasis para su uso en un armario central de cableado. (D-Link, 2013)

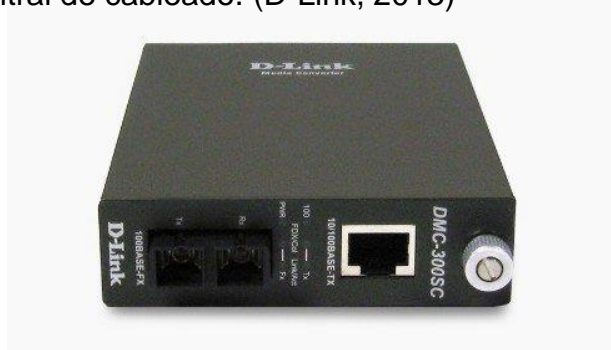


Figura 200. Convertidor de fibra óptica  
[www.fibraopticahoy.com](http://www.fibraopticahoy.com)

## Conversores de Medios Fast Ethernet (TX a FX Fast Ethernet con convertidor de medios conectores de fibra ST multimodo)

Conexiones de fibra óptica: El rango de Allied Telesis de medios Fast Ethernet convertidores ofrece una familia completa de dispositivos de conversión, permitiendo a los usuarios ampliar la tamaño de las redes UTP con el uso de la fibra cableado. Soporta tanto SC y fibra ST conectores, estos convertidores se pueden utilizar para extender redes de hasta 2 km de multimodo fibra o 40 kilómetros de fibra monomodo.

La característica MissingLink permite la fibra óptica puertos del convertidor de medios para pasar el 'Enlace' estado de sus conexiones a cada otro. Cuando el convertidor de medios detecta un problema con uno de los puertos, tales como la pérdida de conexión a un nodo final, los medios de comunicación se cierra convertidor abajo de la conexión con el otro puerto, por lo tanto notificar al nodo que la conexión ha sido perdida. (Intracom, 2009)



Figura 201. Conversor de medios Fast Ethernet  
<http://www.intracom.com>

### **Linksys modem ADSL AM300**

El Linksys módem ADSL ofrece una conexión de alta velocidad instantánea a la Internet. La tecnología ADSL permite acceder a Internet a través de sus líneas telefónicas existentes, sin interferir con su servicio telefónico de voz. Usted puede hablar por teléfono y navegar por la red al mismo tiempo. Navegar por la Web y su e-mail están disponibles al instante, en cualquier momento.

La instalación es rápida y sencilla. Conecte directamente a cualquier PC con un puerto USB o Ethernet, y ya está listo para navegar por Internet. O conectarlo a un router Linksys y compartir el acceso a Internet de alta velocidad con cada uno en su red. (commons, 2014)



Figura 202. Linksys modem ADSL AM300  
<http://www.linksys.com>

### **Access Point Aruba 135**

La multifunción AP-135 se puede configurar a través del Controlador de movilidad para proporcionar acceso WLAN con el aire a tiempo parcial monitoreo para IPS inalámbricos y análisis de espectro. Puede ser configurado como monitores de aire dedicados dentro de la WLAN campus o puede estar situado de forma remota. Pueden permitir malla inalámbricas la creación de redes de backhaul de red de alto rendimiento donde cableada cableado no está disponible.

El AP-135 puntos de acceso 802.11n de interior (AP) maximizar el rendimiento de los dispositivos móviles en muy alta entornos Wi-Fi densidad y garantizar una fuerte protección contra amenazas utilizando seguridad integrada MACSec. Estos puntos de acceso multifuncionales ofrecen un rendimiento similar a un alambre en los datos velocidades de hasta 450 Mbps por radio. Aprovechando 802.11n tecnología, AP-135 emplean tres flujos espaciales para entregar un 50% más de rendimiento y apoyar a un 50% más móvil, dispositivos en entornos de alta densidad en comparación con Previous- AP generación. Cuenta con dos MIMO 3x3 de doble banda de 2,4 GHz / 5 GHz radios con interfaces de antena interna, está diseñado para proporcionar años de funcionamiento sin problemas y están respaldados por una limitada garantía de por vida. Autenticación y cifrado en MACSec puertos Ethernet permiten asegurar el despliegue AP por inter operar con el MACSec capacidad de acceso a los interruptores de movilidad Aruba y otro cableado dispositivos armario. El AP-135 cuentan con doble 10/100 / 1000BASE-T Interfaces Ethernet y operar desde 802.3af estándar y Fuentes

(PoE) en Ethernet sobre el poder-802.3at. El secundario Interfaz Ethernet (activa sólo cuando el suministro 802.3at PoE o DC poder para el punto de acceso) permite backhaul autorizados seguras para los dispositivos conectados a la red cableada.

Trabajando con la línea de controladores de movilidad centralizados de Aruba, el AP-135 entregar servicios de red seguros, de alta velocidad que los usuarios se mueven a una "inalámbrico cuando sea posible, Wired, donde modelo de acceso a la red es necesario". La red puede entonces rightsized eliminando puertos de conmutación Ethernet no utilizados y, con ello la reducción de los costos de operación.

La clave para garantizar el rendimiento y la fiabilidad de alambre es de Aruba única gestión adaptativa de radio y análisis de espectro capacidades, que gestionan las bandas de radio de 2,4 GHz y 5 GHz para ofrecer el máximo rendimiento del cliente al tiempo que mitiga cualquier interferencia de RF.

Aplicación: AP 802.11n interiores diseñados para soportar el máximo rendimiento para la densidad máxima del cliente, con máxima flexibilidad de despliegue y la seguridad, Modo de funcionamiento AP Campus, monitor de aire (AM) y el monitor de espectro AP remoto, AM y monitor de espectro

Radios: radio dual configurable por software capaz de soportar 2,4 GHz y 5 GHz. Gestión de RF Automático transmite control de energía y la gestión de canales con corrección agujero cobertura de automóviles a través de Manejo adaptativo Radio (ARM) análisis de espectro escanea las bandas de radio de 2,4 GHz y 5 GHz Para proporcionar una mayor visibilidad de la interferencia de RF no 802.11n Fuentes y su efecto en la calidad del canal 802.11n. (Networks, 2014)

#### Características avanzadas

- AP remoto, análisis de espectro, malla empresarial segura y protección de intrusiones inalámbricas.
- Seguridad MACSec de autorización y cifrado de datos entre los puertos de AP y la capa de acceso por cable (requiere MACSec apoyo en el conmutador de acceso por cable).
- Integrado de Trusted Platform Module (TPM) para el almacenamiento seguro de credenciales y claves.
- SecureJack con capacidad para hacer un túnel seguro de tráfico Ethernet por cable.
- Antena:AP-134: Tres interfaces de antena RP-SMA para dual externo antenas de banda
- AP-135: Seis downtilt interna antenas omnidireccionales; tres por banda de frecuencia
- 2.4GHz / 3.5dBi
- 5GHz / 4.5dBi



Figura 203. Access Point Aruba 135  
<http://www.arubanetworks.com>

### 3.4.5 RACK Definición:

Un rack es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas para la anchura están normalizadas para que sean compatibles con equipamiento de distintos fabricantes. También son llamados bastidores, cabinas, Gabinetes o armarios. Externamente, los *racks* para montaje de servidores tienen una anchura estándar de 600 milímetros (mm) y un fondo de 600, 800, 900, 1000 y ahora incluso 1200 mm. La anchura de 600 mm para *racks* de servidores coincide con el tamaño estándar de las losetas en los centros de datos (CPD). De esta manera es muy sencillo hacer distribuciones de espacios en centros de datos (CPD). Para el cableado de datos se utilizan también *racks* de 800 mm de ancho, cuando es necesario disponer de suficiente espacio lateral para el guiado de cables. (Commons L. C., 2014)

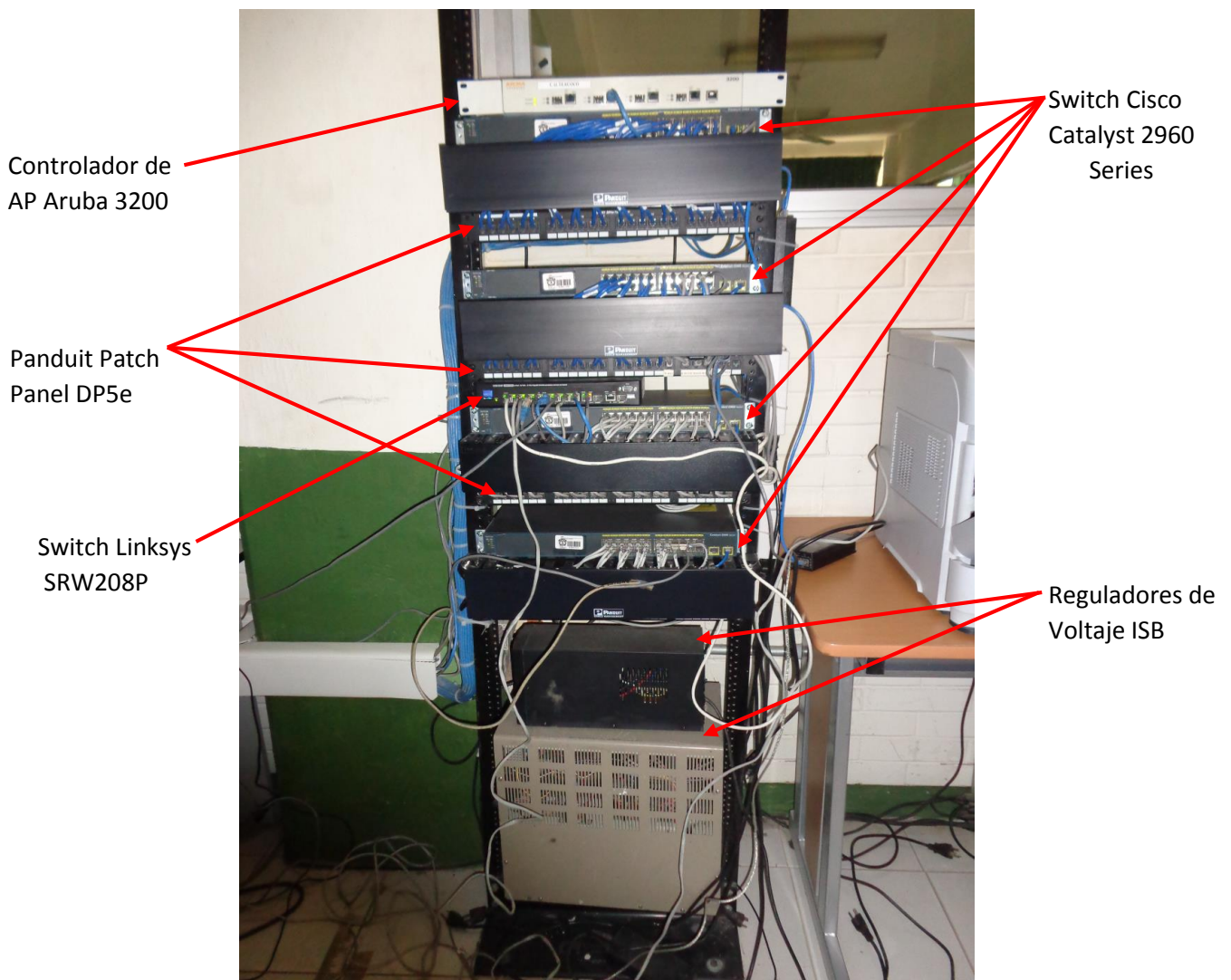


Figura 204. Rack Ubicado en la oficina de RTICS  
Fuente: RTIC, Infraestructura C.U Texcoco, Fraccionamiento el Tejocote, Texcoco 2014



## Compones del Rack:

### Controlador de Ap Aruba 3200

La gama de controladores de movilidad multiservicio Aruba MMC-3000 es una familia de tres controladores con todas las funciones necesarias y a los que se les pueden agregar hasta 32, 64 y 128 puntos de acceso (AP) conectados al campus, respectivamente. La gama MMC-3000 proporciona una auténtica red centrada en el usuario con conectividad “follow-me”, acceso basado en identidad y servicios de continuidad de aplicación. El modelo MMC-3200 está diseñado para oficinas pequeñas o sucursales.

La gama MMC-3000 se puede desplegar fácilmente como una superposición, sin interrumpir la red existente de cable. Las funciones avanzadas de voz sobre WLAN, como el control de admisión de llamadas (CAC, en inglés Call Admission Control), la gestión RF con reconocimiento de voz y la calidad de servicio por aire estricta, permiten a la gama MMC-3000 ofrecer funcionalidades VoIP móviles. La gama MMC-3000 se gestiona mediante ArubaOS o el sistema de gestión de Aruba Mobility Management System.

Asimismo, la gama MMC-3000 se puede desplegar como un Gateway de seguridad centrado en el usuario para autenticar los usuarios conectados por cable e inalámbricos, aplicar las políticas de control de acceso basadas en roles y poner en cuarentena a los dispositivos finales no seguros para que no accedan a la red corporativa. Los usuarios invitados se soportan de forma sencilla y con seguridad mediante el servidor de portal cautivo incorporado y los servicios de red avanzados. La gama MMC3000 puede crear un entorno de red seguro sin necesidad de otros dispositivos VPN/cortafuegos gracias a las funcionalidades VPN sitio a sitio y NAT integradas, el split-tunneling y un cortafuegos de estado. El soporte de VPN sitio a sitio se puede integrar con los principales concentradores VPN para facilitar que la integración con las VPN existentes de la organización sea un éxito. (Networks, 2014)



Figura 205. Controlador de AP Aruba 3200  
<http://www.arubanetworks.com>

Tabla 21: Rendimiento y capacidad del controlador MMC-3200

AP conectados al campus	Hasta 32/64/128
AP remotos Hasta	Hasta 128/256/512
Usuarios	Hasta 512/1.024/2.048
Direcciones MAC	Hasta 64.000
Interfaces IP VLAN	128
Puertos Gigabit Ethernet (RJ-45 o SFP)	4
Sesiones activas del cortafuegos	Hasta 128.000
Túneles IPsec simultáneos	Hasta 512/1.024/2.048
Capacidad del cortafuegos	3/4/4 Gbps
Capacidad de cifrado (3DES, AESCBC256)	1,6/4/8 Gbps
Capacidad de cifrado (AES-CCM)	0,8/2/4 Gbps

#### Funciones de seguridad y control de la LAN inalámbrica

- Seguridad 802.11i (certificaciones WPA2 y WPA de la WFA)
- Autenticación 802.1X de usuario y máquina
- Soporte de EAP-PEAP, EAP-TLS y EAP-TTLS
- Cifrado AES-CCM, TKIP y WEP centralizado
- Caché de PMK 802.11i para aplicaciones de roaming rápido
- EAP Offload para la escalabilidad y la supervivencia del servidor AAA
- Autenticación 802.1X de estado para los AP autónomos
- Autenticación basada en direcciones MAC, SSID y ubicación
- Soporte Multi-SSID para el funcionamiento de múltiples WLAN
- Selección de servidor RADIUS basado en SSID
- Gestión y control seguros de los AP por IPsec o GRE
- Compatibilidad con CAPWAP y actualizable
- Modo WLAN distribuido para despliegues de AP remotos
- Soporte simultáneo de WLAN centralizada y distribuida

## Funciones de seguridad basadas en identidad

- Autenticación de usuarios conectados por cable e inalámbricos
- Autenticación de portal cautivo, 802.1X y dirección MAC
- Asociación del nombre de usuario, dirección IP, dirección MAC y clave de cifrado para crear una sólida identidad de red
- Verificación de identidad por paquete para evitar suplantaciones
- Valoración del estado del dispositivo final, puesta en cuarentena y remedio
- Soporte de Microsoft NAP, Cisco NAC y Symantec SSE
- Soporte de servidores AAA basados en RADIUS y LDAP
- Base de datos de usuarios interna para protección en caso de caída del servidor AAA
- Autorización basada en roles para eliminar privilegios excesivos
- Potente aplicación de políticas con inspección de estado de los paquetes

## Funciones de red y servicios avanzados

- Conmutación L2 y L3 por aire y por cable
- VLAN Pooling para diseños de red sencillos y escalables
- Movilidad VLAN para roaming L2 sin interrupciones
- Mobile IP proxy y Proxy DHCP para roaming L3
- Servidor DHCP y DHCP relay incorporados
- Redundancia de controlador N+1 basada en VRRP (L2)
- Redundancia de controlador N+1 basada en el aprovisionamiento de AP (L3)
- Modo de concentrador de acceso por cable para una seguridad centralizada
- Soporte de Etherchannel para la redundancia de enlace
- STP (Spanning Tree Protocol) 802.1d

## Etiquetas VLAN 802.1Q

### Especificaciones de la alimentación (requisitos para la entrada CA)

- Aruba MMC-3200:
- Voltaje de entrada CA: 90-264 V~, entrada universal
- Corriente de entrada CA: 1,5 A
- Frecuencia de entrada CA: 47-63 Hz

## Especificaciones de funcionamiento y dimensiones

- Rango de temperaturas en funcionamiento De 0°C a 40°C
- Rango de temperaturas de almacenamiento De 10°C a 70°C
- Humedad, sin condensación Del 5 al 95%
- Altura 44 mm (1,75½”) Ancho 351 mm (13,8½”) Profundidad 297 mm (11,7½”)
- Peso Aruba MMC-3200 3,2 kg (7,1 lb) (sin la caja)
- Garantía hardware 1 año para componentes/mano de obra Software 90 días

## Switch Cisco Catalyst 2960 Series

Los switches de Cisco Catalyst 2960 soportan voz, video, datos y acceso seguro. Ofrecen una administración escalable conforme cambian las necesidades de su negocio. Puntos destacados los switches de Catalyst 2960 Series soportan:

- Comunicaciones integrales: Obtenga soporte de datos, tecnología inalámbrica y voz de forma que cuando esté listo para implementar estos servicios disponga de una red que admita todas sus necesidades empresariales.
- Inteligencia: Dé prioridad al tráfico de voz o al intercambio de datos para ajustar la entrega de información a sus requisitos empresariales.
- Seguridad mejorada: Proteja la información importante, mantenga a los usuarios no autorizados alejados de la red y consiga un funcionamiento ininterrumpido.
- Confiabilidad: Aprovechese de las ventajas de los métodos basados en normas para conseguir una mayor confiabilidad y una rápida recuperación de errores, también puede agregar un suministro de energía redundante para obtener una confiabilidad adicional.
- Fácil configuración: Utilice Cisco Network Assistant para simplificar la configuración, las actualizaciones y la solución de problemas.

### Características:

- Cisco Catalyst 2960G-24TC - conmutador - 20 puertos
- Tipo de dispositivo Conmutador
- Factor de forma Externo - 1U
- Dimensiones (Ancho x Profundidad x Altura) 44.5 cm x 32.8 cm x 4.4 cm
- Peso 4.5 kg
- Memoria RAM 64 MB
- Memoria Flash 32 MB
- Cantidad de puertos 20 x Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T
- Velocidad de transferencia de datos 1 Gbps
- Protocolo de interconexión de datos Ethernet, Fast Ethernet, Gigabit Ethernet
- Puertos auxiliares de red 4x10/100/1000Base-T/SFP (mini-GBIC)(señal ascendente)
- Protocolo de gestión remota SNMP 1, RMON, Telnet, SNMP 3, SNMP 2c
- Modo comunicación Semidúplex, dúplex pleno
- Auto-sensor por dispositivo, soporte de DHCP, negociación automática, soporte VLAN, snooping IGMP
- Cumplimiento de normas
- IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah
- Alimentación CA 120/230 V ( 50/60 Hz )
- Garantía limitada de por vida (Cisco, Cisco Product, 2008)



Figura 206. Switch Cisco Catalyst 2960 Series  
<http://www.cisco.com>

## Switch Linksys SRW208P

Switch Linksys de 8 puertos (10/100) + 2 puertos Gigabit (10/100/1000) y 2 miniGBIC combinado.

### Características

**Flexibilidad** una amplia gama de combinaciones de puertos y velocidades le permite elegir con libertad el producto que mejor se adapte a su presupuesto y a sus necesidades de rendimiento. Todos los switches gestionados Linksys ofrecen una funcionalidad superlativa, independientemente de su tamaño.

**Seguridad** las medidas de seguridad avanzada protegen la red y los datos al otorgar acceso sólo a los usuarios con los debidos privilegios.

**Fiabilidad** los switches gestionados ofrecen varias características de redundancia y calidad para maximizar la disponibilidad de la red. Su empresa podrá seguir avanzando sin tener que lidiar con interrupciones inoportunas de la red o conexiones que puedan llegar a ser o catalogarse de baja calidad.

**Facilidad de Ampliación** los switches gestionados Linksys para pequeñas empresas admiten diversos protocolos de calidad y alimentación que posiblemente no necesite desde el principio. Sin embargo, a medida que crezca su empresa y esté en condiciones de realizar un despliegue de las redes más avanzadas, estas características acompañarán a su crecimiento. (lynksys, 2012)



Figura 207. Switch Linksys SRW208P  
<http://www.lynksys.com>

Puertos	<ul style="list-style-type: none"> <li>• 8 x Conectores RJ-45 para 10BASE-T y 100BASE-TX</li> <li>• 2 x Puertos Gigabit (10/100/1000) y 2 x miniGBiC combinados</li> <li>• Puerto Consola</li> <li>- Auto MDI/MDI-X</li> <li>- Ajuste Autonegotiate/Manual</li> </ul>
Tipo de Cableado	• UTP CAT 5 ó superior para 10BASE-T/100BASE-TX
LEDs	• 10/100 Link/Actividad, Velocidad, Sistema
Capacidad de Conmutación	• 1.6 Gig antibloqueo
Velocidad de Reenvío	• 1.19 Mbps rendimiento de velocidad por cable
Tamaño de Tabla MAC	• 8K
Número de VLAN	• 256 VLAN activas (rango 4096)
VLAN	<ul style="list-style-type: none"> <li>• VLAN basada en puerto y VLAN basada en ficha 802.1Q</li> <li>Gestión de VLAN</li> </ul>
Bloqueo HOL	• Prevención de bloqueo de cabeza de línea
Seguridad	• 802.1x - Autenticación RADIUS. Encriptación MD5
Control de Acceso	<ul style="list-style-type: none"> <li>• ACL - Límite de caída o velocidad basado en:</li> <li>- MAC de origen y destino</li> <li>- Dirección IP de origen y destino</li> <li>- Protocolo</li> <li>- TOS/DSCP</li> <li>- Puerto</li> <li>- VLAN</li> <li>- Ethertype</li> </ul>
Niveles de Prioridad	• 4 colas de Hardware
Estándares	<ul style="list-style-type: none"> <li>• 802.3 10BASE-T Ethernet</li> <li>• 802.3u 100BASE-TX Fast Ethernet</li> <li>• 802.3ab</li> <li>• 802.3x Flow Control</li> <li>• 802.3ad LACP</li> <li>• 802.1D STP</li> <li>• 802.1Q/p VLAN</li> <li>• 802.1w Rapid STP</li> <li>• 802.1s Múltiple STP</li> <li>• 802.1x Autenticación de puerto de acceso</li> </ul>
Certificaciones	• FCC Parte 15 Clase A, CE Clase A, UL, cUL, marca CE, CB
Alimentación	• Adaptador de alimentación CA externo
Dimensiones	• 279 mm x 44 mm x 170 mm
Peso	• 1 Kg

## **Panduit DP5e Patch Panels**

Con paneles de parcheo Panduit DP5e y DP6 Plus, sus sistemas de redes y de telefonía pueden ser fácilmente organizados independientemente de la complejidad de la aplicación. Al conectar todos los cables en este centro, a evitar la confusión de cables desordenados y que no dejan huella. Los paneles pueden ser utilizados para configuraciones Cat5e o Cat6 cable Ethernet. Paneles de parcheo Panduit Cat5e y Cat6 se utilizan para velocidades de transmisión de alta velocidad de LAN de hasta 155Mbps, estos paneles de conexión se han desarrollado con una tecnología de placa de circuito impreso de propiedad que se traduce en rendimiento para cumplir con EIA / TIA 568A Categoría 5E mejorada y Categoría 6 TIA / EIA 568 especificaciones -B.2-1. Categoría 6 permite la transmisión de Gigabit Ethernet y otras aplicaciones de alta velocidad

Información técnica Patch panel DP5e:

Categoría 5e / Clase DS supera los requisitos de canal de ANSI / TIA-568-C.2 Categoría 5e y. Canal y componente Normas D 11801 Clase ISO en frecuencias barridas 1-100 MHz. Rendimiento, supera los requisitos de los componentes de la norma ANSI / TIA-568-C.2 Categoría 5e y las normas D 11801 Clase ISO en frecuencias barridas 1-100 MHz. FCC y ANSI. Cumple con las normas ANSI / TIA-1096-A; contactos chapados con 50 micras de oro. Cumplimiento, Para un rendimiento superior. IEC cumplimiento: Cumple con la norma IEC 60603-7. PoE cumplimiento: Cumple con los requisitos de IEEE 802.3af y IEEE 802.3at para aplicaciones PoE. UL nominal: UL 1863 aprobado. Terminación Conductor Compatible con 22 a 26 AWG cable CBI sólido o trenzado con conductor. rango: diámetros de aislamiento de 0.048 en.

Opción de montaje:

Se monta en el estándar EIA de 19 "o 23" bastidores (con extensor opcional soporte); Versión de 12 puertos puede ser montado en la pared con soporte opcional 89D. Embalaje, incluye tornillos de montaje M6 y # 12-24.

Características y ventajas claves, probado rendimiento 100%. La confianza en que cada módulo conector entregará el crítico requisitos de rendimiento eléctricos. Individualmente serializado. Cada puerto está marcado con el número de control de calidad para la futura trazabilidad.

Interfaz RJ45: Interfaz estándar de la industria ofrece un enchufe rápido y fácil y jugar conexión con cables de conexión RJ45; compatible con versiones anteriores.

Identificación: Puede estar claramente identificados con etiquetas opcionales e iconos para identificación del puerto.

Esquema de cableado universal: Esquemas T568A y T568B claramente identificados, estándar de la industria, solo alambre 110 herramienta de impacto (PDT110) asegura conductores. Herramienta de terminación, están totalmente terminado.



Bloquee el dispositivo (opcional): Proporciona un método sencillo y seguro para controlar el acceso a los datos puertos mientras no esté en uso.

Diseño en ángulo (opcional): Facilita el control del radio de curvatura adecuado y minimiza la necesidad para administradores de cables horizontales.

Módulo de puerto de reemplazo: La posibilidad de sustituir el terreno puertos dañados para la utilización panel completo. (COMDIEL, 2009)



Figura 208. Patch Panel DP5e  
<http://www.panduit.com>

## Diagnóstico de la Red

Las diferentes opciones de diseños, formas y arquitecturas de redes hace que el proyecto que vamos a desarrollar, sea implementado bajo un ambiente seguro y dinámico como es una simulación basada en todo el análisis previamente realizado, el análisis y el diagnóstico de la red actual se ha obtenido en base a las experiencias dentro de la universidad sin dejar de lado la base principal que es la teoría y por supuesto la parte práctica, para esto realizamos la obtención de datos tomando como base la información proporcionada por el personal docente encargado de la red bajo el cargo de RTIC, personal administrativo alumnos e investigadores del Centro Universitario UAEM Texcoco. (Ramirez, Antecedentes UAEM Texcoco, 2014)

## Análisis de necesidades

El centro universitario UAEM Texcoco al ser una universidad que cuenta con una taza bastante alta de estudiantes sin mencionar al personal que labora tal como profesores administrativos e investigadores el centro tiene la necesidad de dar un servicio de internet a dicha comunidad estudiantil y a su personal ya mencionado; muchas de estas solicitudes son para equipos móviles. Es capaz poder integrar cierta cantidad de nodos inalámbricos a la red del centro pero es claro que no sería suficiente puesto que no se cuenta con una infraestructura suficiente, aunado a esto la solución más óptima es rediseñar la red inalámbrica que cumpla con las necesidades de cada usuario por medio de la creación de perfiles y permisos para poder proveer movilidad y satisfacción al usuario.

## **Distribución de la planta**

Edificio B Planta baja: Tiene un área de 700 m<sup>2</sup> donde están ubicados los departamentos de coordinación, difusión cultural, almacén control escolar donde también se recibe a otro tipo de usuarios que necesitan acceso a internet. Planta alta: Tiene un área de 700 m<sup>2</sup> donde están ubicados los laboratorio de cómputos, laboratorio de redes, laboratorio de electrónica, cubículos de profesores, oficina de RTIC donde está ubicado el RACK, sala de control donde se encuentra el IDF y el MDF. (Ramirez, Antecedentes UAEMEX, 2014)

## **Situación actual**

El edificio B cuenta con dos plantas, plata alta es el lugar más concurrido por los usuarios para la red alámbrica e inalámbrica puesto que esta planta se encuentra la mayoría de los laboratorio de cómputo y la oficina de RTIC que además de cubrir con funciones de soporte técnico cuenta con equipo de impresiones fotocopiado escáner etc. De acuerdo al encargado del área se tiene una demanda de conexión de 100 usuarios conectados por cada access point que solo tiene capacidad de establecer conexión con 25. (Ramirez, Antecedentes UAEM Texcoco, 2014)

## **Análisis de Requerimientos**

En esta parte realizamos un análisis del conocimiento que el personal, Docente, Administrativo y Estudiantes tienen en cuanto al rendimiento, disponibilidad, seguridad, capacitación y soporte técnico de los servicios que brinda actualmente la Red LAN e Inalámbrica, dividiendo los requerimientos en:

- Requerimientos a nivel de usuario.
- Requerimientos a nivel de Tecnología y Red.

### **Requerimientos a nivel de Usuario.**

Este análisis de requerimiento, nos permitirá conocer las necesidades actuales y futuras de los usuarios, como también las limitaciones que se presentan actualmente en la red, con respecto al crecimiento y actualización de la Red. Es necesario analizar y plantear los costos así como los diferentes beneficios que conllevan obtener evidencias para una mejora de la red en beneficio de la comunidad estudiantil.

Los requerimientos presentados a nivel de usuario son:

- En el centro universitario UAEM Texcoco, deben facilitar la conexión a internet así como a los diferentes servicios de la red, mejorar el ancho de banda.

- Proporcionar movilidad compartiendo recursos físicos y lógicos a nivel de todo el campus

### **Requerimientos a nivel de Tecnología y Red.**

La información que puede ser enviada a través de la red por medio de los cables de fibra óptica utilizando una unidad del total de ancho de banda proporcionado por el ISP de C.U Toluca no es lo suficiente para satisfacer las necesidades de los usuarios del C.U Texcoco que desean acceder al mismo tiempo

- El usuario espera demasiado tiempo para poder acceder a la red desde el momento que ingresa el usuario y contraseña hasta que la información es recibida, es decir el tiempo de respuesta es demasiado largo y esto determina que la red no es capaz de satisfacer la necesidad del usuario.
- La red implementada que opera actualmente no permite que todos tengan accesos a internet por lo tanto no brinda flexibilidad alguna, sin embargo dicha red está en proceso de incorporación de nuevos dispositivos para así poder mejorar su rendimiento sin afectar la infraestructura actual.

### **Estudio de Factibilidad**

Este estudio determina la factibilidad de los recursos necesarios que existen actualmente en el C.U Texcoco para llevar a cabo los procesos y tareas curriculares para el mejor desempeño y aprendizaje de la comunidad estudiantil dicho estudio contempla los recursos disponibles o aquellos que puedan ser proporcionados mismo que están divididos en los siguientes:

- Técnico
- Operativo
- Económico

### **Factibilidad Técnica**

Analizamos si el equipamiento tanto como la distribución de la red del Centro Universitario UAEM Texcoco tiene la capacidad de poder satisfacer las necesidades en las condiciones en que se instaló configuro y diseño dicha infraestructura por medio de los siguientes recursos:

### **Recursos Técnicos**

La red del centro universitario UAEM Texcoco está constituida por un MDF, IDF situados en la sala de control así como un RACK ubicado en la oficina de RTIC, la red alámbrica está formada por cable coaxial y fibra óptica dicha red está distribuida en 8 laboratorios de computo situados en su totalidad en el edificio b y uno más en biblioteca, control escolar tiene un total de cinco computadoras con comunicación directa a C.U Toluca gracias a la conexión VPN mediante el túnel

establecido, En cuanto a la red Inalámbrica está constituida por cuatro access point por cada edificio conectados a un concentrador de AP, el centro universitario tiene un total de 650 computadoras conectadas a la red.

### **Factibilidad Operativa.**

El análisis realizado a la red actual del Centro Universitario UAEM Texcoco considera que es operativo debido a que existe la posibilidad de conectar en red casi todas las maquinas que existen en el campus sin embargo la red inalámbrica no es capaz de hacer una conexión estable y mucho menos satisfacer la demanda de acceso a internet por parte de los usuarios.

### **Factibilidad Económica.**

Realizamos un estudio de costos de toda la infraestructura de red establecida en el Centro Universitario UAEM Texcoco principalmente incluye el costo de los dispositivos, instalación y configuración como lo muestra la siguiente tabla:

Hardware	Modelo	Piezas	Costo Unitario
Modem	Linksys ADSL AM300	2	\$ 536
Ip Office	Avaya IP office 500 v2	1	\$ 4,744
	Avaya ip400 phone	1	\$US 334
Convertidor	D-link convertidor de TX-FX	8	\$ 1,056
Servidor	Dell PowerEdge R200 Server	2	\$US 140
Controlador	Aruba 3200 Controlador de AP	1	\$US 3,725
Patch Panel	Panduit DP5e 24 Puertos	6	\$US 169
	Panduit DP5e 48 Puertos	2	\$US 399
Access Point	Aruba 135	18	\$US 985
Router	Cisco 2900 Series (ISR)	1	\$US 1,109
Switch	Cisco Catalyst 2960	5	\$ 8,912
	Switch D-Link DES-1008A	1	\$ 169
	Switch Linksys SRW208P	3	\$ 3,769
	3Com Switch Línea de base 2026	1	\$ 4,100
Modem Router	Modem Watson 2 Pair	5	\$ 200

Tabla 23. Cotización de infraestructura de la red de C.U Texcoco

### **Acceso a internet**

La conexión de la red a internet lo suministra Toluca mediante un ISP proveedor de servicios de internet es decir el ancho de banda es de 10 Mb distribuido en las maquinas manejando una velocidad de trasmisión de 100 Mbps en un rango operativo real de 20 a 50 Mbps. La red que asigna C.U Toluca es la sub red .98 contado con 2 de la 98 por subneting con la que está trabajando actualmente el Centro Universitario UAEM Texcoco. (Ramirez, Antecedentes UAEM Texcoco, 2014)

