Wireless LAN para la Facultad de Ingeniería de la Universidad de Buenos Aires

Ernesto Cottely y Fernando Manso

Trabajo Profesional de Ingeniería Electrónica
Facultad de Ingeniería, Universidad de Buenos Aires

Diciembre 2009

Capítulo 1

Resumen

En este informe se detalla el relevamiento físico y lógico de la red informática de la FIUBA, y se analiza el nivel de servicio que brinda actualmente. Luego, se lleva a cabo un estudio de factibilidad técnica, económica y se constituye un plan de tareas para realizar el seguimiento del proyecto a lo largo de la implementación. Posteriormente, se procede al estudio de los estándares y protocolos que son necesarios para entender los conceptos orientados a voz, vídeo y datos, de forma tal, de poder profundizar y aplicar estos conceptos en el capítulo de ingeniería en detalle. Se procede a validar la propuesta mediante las herramientas de simulación correspondientes. Se finaliza con los estudios de confiabilidad correspondientes y evaluación económica del proyecto.

Prefacio

Este trabajo está desarrollado dentro del campo de la consultoría y diseño de redes, según las normas y recomendaciones internacionales afines. Se buscó realizar un trabajo que pueda generar una mejora y por lo tanto ser de utilidad, tanto a la facultad de ingeniería, como a sus alumnos y docentes. Ha sido confeccionado por estudiantes de ingeniería electrónica próximos a recibirse y tiene como fin ser parte de la formación de futuros profesionales permitiendo obtener experiencia en esta área y resolver situaciones problemáticas reales.

Índice general

1. Resumen **1**

Índice general **3**

Índice de figuras **8**

Índice de cuadros **13**

2. Introducción **15**
2.1. Historia 15
2.2. Justificación del Proyecto 15

3. Objetivos **16**
3.1. Finalidad del proyecto 16
3.2. Planteo del problema a resolver 16

4. Relevamiento físico actual de la red **18**
4.1. Descripción topológica de la red 18
4.2. Equipos de la red 20
4.2.1. Alimentación eléctrica de los equipos 21
4.2.2. Sistema de Alimentación Ininterrumpida (UPS) 21
4.2.3. Refrigeración de los equipos 21
4.2.4. Routers Wi-Fi 21
4.3. Descripción detallada por pisos 22
4.4. Conclusiones del relevamiento 23

5. Análisis de Tráfico **24**
5.1. Introducción 24
5.2. Detalles de la realización del análisis. 24
5.3. Tráfico LAN. 24
5.4. Tráfico WAN 29
5.5. Análisis del “delay”, “jitter”y “packet loss” 30
5.5.1. Mediciones 32
5.6. Análisis del impacto de la ausencia de VLANs 33
5.7. Conclusiones. 35
5.7.1. Sobre el volumen del tráfico. 35
5.7.2. Sobre el uso de VLANs 35

6. Objetivos y estudios preliminares al diseño del producto **36**
6.1. Tendencia de uso de internet . . . 36
6.2. Casa de la calidad . . . 43
6.2.1. Requerimientos . . . 45
6.2.2. Matriz de Planeamiento . . . 47
6.2.3. Techo . . . 48
6.2.4. Matriz de interrelaciones . . . 49
6.2.5. Metas . . . 50
6.2.6. Esquema de la casa de calidad . . . 51
6.2.7. Conclusiones . . . 53
6.3. Especificaciones Técnicas . . . 53

7. Análisis de factibilidad **56**
7.1. Factibilidad operacional . . . 56
7.2. Factibilidad tecnológica . . . 57
7.2.1. Propuesta de alternativas de diseño . . . 57
7.2.2. Elección de una solución . . . 60
7.3. Factibilidad de tiempos . . . 62
7.3.1. Determinación de tareas . . . 62
7.3.2. Asignación de tiempos a las tareas . . . 66
7.3.3. Asignación del orden de precedencia . . . 67
7.3.4. Método de camino crítico . . . 69
7.3.5. Método de propagación de errores . . . 69
7.3.6. Método de simulación de Montecarlo . . . 70
7.3.7. Histograma . . . 71
7.3.8. Diagrama de Gantt . . . 72
7.3.9. Asignación de Recursos . . . 78

8. Estándares **80**
8.1. Introducción a WLAN y IEEE 802.11 . . . 80
8.1.1. Arquitectura IEEE 802.11 . . . 81
8.1.2. Capa Física . . . 82
8.1.3. Capa de datos . . . 83
8.1.4. Estándares IEEE 802.11 . . . 85
8.1.5. IEEE 802.11*b* . . . 85
8.1.6. IEEE 802.11*a* . . . 87
8.1.7. IEEE 802.11*g* . . . 87
8.1.8. IEEE 802.11*n* . . . 87
8.1.9. Codificación de los datos . . . 88
8.1.10. Número de antenas . . . 88
8.1.11. Seguridad . . . 89
8.2. Cableado Estructurado . . . 93
8.2.1. ANSI/EIA/TIA 569 Commercial Building Standards for Telecommunications Pathways and Spaces . . . 93
8.2.2. Instalaciones de entrada . . . 95
8.2.3. Salas de Equipos . . . 95

8.2.4. Canalizaciones de troncal . . . 96
8.2.5. Canalizaciones internas . . . 96
8.2.6. Armarios de telecomunicaciones . . . 96
8.2.7. Canalizaciones horizontales . . . 98
8.2.8. Otros estándares que deben observarse aparte del tratado aquí: . . . 101
8.3. IEEE 802.3 . . . 101
8.3.1. IEEE 802.3af . . . 101
8.4. Voz y Vídeo sobre IP . . . 101
8.4.1. Voz sobre IP . . . 102
8.4.2. Vídeo sobre IP . . . 103
8.4.3. Protocolos de voz y vídeo sobre IP . . . 104
8.5. IEEE 802.1Q - VLANs . . . 107
8.5.1. Introducción a las VLANs . . . 107
8.5.2. Operación de las VLANs . . . 110
8.5.3. Principios de las VLANs . . . 111
8.5.4. Normas de VLANs . . . 112
8.5.5. Norma 802.1Q . . . 112
8.6. LACP . . . 113
8.6.1. Descripción del protocolo . . . 113
8.6.2. Link Aggregation estandarizado por IEEE: . . . 114
8.6.3. Eficiencia de LACP . . . 114

9. Ingeniería de detalle 116
9.1. Dispositivos de Comunicaciones . . . 116
9.1.1. Hub (Layer 1) . . . 116
9.1.2. Bridge (Layer 2) . . . 116
9.1.3. Switch . . . 116
9.1.4. Router (Layer 3) . . . 118
9.1.5. Firewall (Layer 2...7) . . . 118
9.1.6. Proxy (Layer 1...7) . . . 127
9.1.7. IDS (Layer 2..7) . . . 128
9.1.8. Access Point o AP (Layer 2) . . . 128
9.1.9. Access Controller o AC (Layer 2 ...7) . . . 128
9.2. Arquitectura de red . . . 128
9.3. Red Privada . . . 129
9.4. Acceso de la Red Privada . . . 131
9.4.1. Definiciones . . . 131
9.4.2. Ingeniería de áreas “hotspot” . . . 131
9.4.3. Blindaje electromagnético . . . 142
9.5. Backbone de la Red Privada . . . 150
9.5.1. Dimensionamiento del tráfico . . . 150
9.5.2. Estudio de bloqueo y disponibilidad del llamado . . . 153
9.5.3. Diseño con bandejas porta cables . . . 155

10. Construcción del prototipo **163**
10.1. Equipos Propuestos . . . 163
10.1.1. Intermedia System . . . 163
10.1.2. End System . . . 178
10.2. Configuración de los equipos . . . 189
10.2.1. Firewalls . . . 189
10.2.2. Direccionamiento IP . . . 190
10.2.3. Asignación de recursos lógicos . . . 192
10.3. "Link Budget" . . . 193
10.4. Topología de la nueva red . . . 195

11. Validación del prototipo **209**
11.1. Determinación de requerimientos de la red . . . 210
11.2. Simulación de las zonas hostpot . . . 211
11.2.1. Subsuelo . . . 212
11.2.2. Entre Piso . . . 218
11.2.3. Planta Baja . . . 224
11.2.4. Piso 1 . . . 230
11.2.5. Piso 2 . . . 236
11.2.6. Piso 3 . . . 242
11.2.7. Piso 4 . . . 248
11.2.8. Piso 5 . . . 254

12. Estudios de confiabilidad de hardware y de software **260**
12.1. Introducción: . . . 260
12.1.1. Modelo de Confiabilidad: . . . 260
12.1.2. Obtención del MTBF de la red inalámbrica: . . . 262
12.1.3. Cálculo de la confiabilidad de la red: . . . 263
12.1.4. Conclusión: . . . 264
12.2. Mantenibilidad de la red inalámbrica: . . . 264
12.2.1. Modelo de mantenibilidad: . . . 266
12.2.2. Tiempo medio de reparación: . . . 268
12.3. Disponibilidad de la red inalámbrica: . . . 268
12.3.1. Conclusión: . . . 269

13. Evaluación Económica del Proyecto **270**
13.1. Análisis del "Costo - Beneficio" . . . 270
13.1.1. Costos . . . 270
13.1.2. Beneficios . . . 272
13.1.3. Flujo de Caja Descontada . . . 274
13.1.4. TIR . . . 277
13.1.5. TRI . . . 277
13.1.6. Relación costo beneficio . . . 278

14. Conclusiones **279**
14.1. Objetivos alcanzados 279
14.2. Fallos y recomendaciones para futuros diseños 279

A. Planos **280**
A.1. Primer Piso 281
A.2. Segundo Piso 282
A.3. Tercer Piso 283
A.4. Cuarto Piso 284
A.5. Quinto Piso 285
A.6. Planta Baja 286
A.7. Subsuelo 287
A.8. Entre piso 288

B. Monitoreo de Tráfico **289**

Bibliografía **308**

Índice de figuras

4.1. Diagrama lógico de la FIUBA 19

5.1. Eficiencia de Ethernet 25
5.2. Paquetes STP en el 4to Piso 26
5.3. Errores en el 4to Piso 27
5.4. Errores en la biblioteca 28
5.5. Tráfico del enlace WAN 29
5.6. Round-Trip Time 30
5.7. Calidad de servicio sobre redes IP. 31
5.8. Paquetes ARP broadcast en el 4to piso 33
5.9. Paquetes ARP broadcast en la biblioteca 34

6.1. Usuarios de internet 37
6.2. Lugares de utilización de internet 38
6.3. Principal utilización de internet 39
6.4. Tipos de usuarios de internet 40
6.5. Web 2.0 40
6.6. Actividades comerciales en internet 41
6.7. Aumento de la tendencia de la compra de notebook. 42
6.8. Posicionamiento frente a otros medios de comunicación 43
6.9. Esquema de la estructura de la casa de la calidad 45
6.10. Requerimientos de usuarios 46
6.11. Requerimientos Técnicos 47
6.12. Matriz de planeamiento 48
6.13. Techo de la casa de la calidad 49
6.14. Matriz de Interrelaciones 50
6.15. Metas de Diseño 51
6.16. QDF 53

7.1. Límite de los medios de transmisión 58
7.2. Repetidores 58
7.3. Diagrama en bloques del orden de precedencia de las tareas. 68
7.4. Distribución de probabilidad de la duración del camino crítico 72
7.5. Gráfico de Gantt con las tareas y el camino crítico. 73
7.6. Gráfico de Gantt con las tareas y el camino crítico. 74
7.7. Gráfico de Gantt con las tareas y el camino crítico. 75

7.8. Gráfico de Gantt con las tareas y el camino crítico. 76
7.9. Gráfico de Gantt con las tareas y el camino crítico. 77

8.1. IEEE 802.11 y el modelo OSI 81
8.2. Arquitectura básica de red 802 82
8.3. Canales Wi-Fi 2.4GHz en (802.11b,g WLAN) 83
8.4. RTS/CTS - Hidden Node 84
8.5. Código de Barker de longitud 7, representación en bandabase 86
8.6. IEEE 802.1x 91
8.7. Infraestructura edilicia según EIA/TIA 569A. 94
8.8. Estructura recomendada para los armarios de telecomunicaciones según EIA/TIA 569A. 97
8.9. Esquema de los ductos bajo piso 98
8.10. Esquema de los ductos bajo piso elevado. 99
8.11. Esquema de los ductos aparentes ("Cable canal"). 99
8.12. Esquema de las bandejas porta cables. 100
8.13. Arquitectura H.323 105
8.14. Arquitectura SIP 106
8.15. Arquitectura sin el uso de VLAN. 108
8.16. Arquitectura con VLAN. 109
8.17. Funcionamiento con VLAN. 110
8.18. Consulta de un paquete al switch para determinar a que VLAN pertenece. 110
8.19. Tipos de VLAN según el método de acceso. 111
8.20. Trama Ethernet con tag de 802.1Q. 113
8.21. LACP entre un switch y un servidor. 113

9.1. Mala política de utilización de VLANs. 117
9.2. Topología Bastion Host 119
9.3. Topología Dual-home host 119
9.4. Topología Firewall Básica 121
9.5. Topología DMA Opuesta 121
9.6. Topología Opuesta Dividida 123
9.7. Aislar redes 125
9.8. Entorno de desarrollo LAMP 126
9.9. Arquitectura 129
9.10. Arquitectura de red 130
9.11. Conexión en cascada de APs por cable UTP 131
9.12. Conexión en cascada de APs por backbone de switches 132
9.13. Conexión en cascada de APs por Wireless Link 132
9.14. Celdas solapadas 133
9.15. Roaming entre dos zonas de cobertura 134
9.16. Patrón de reuso de frecuencia 135
9.17. Distribución rectangular multi-planta 136
9.18. Estimación de perdidas por propagación en interiores 140
9.19. Multitrayecto 140
9.20. Probabilidad de error de bit para métodos de modulaciones típicos 141
9.21. Incidencia normal sobre una interfase 145

9.22. Blindaje de paredes con laminas conductoras 147
9.23. Sala blindada con pintura 148
9.24. Puestas a tierra interior (ES) y exterior (ESA) 149
9.25. Cinta de tierra (EB) 149
9.26. Malla de blindaje 149
9.27. Tela de blindaje 150
9.28. Esquemas de los agujeros montantes y canaletas entre pisos según la norma EIA/TIA 569A. 156
9.29. Esquema e imagen de un tramo recto de bandeja portacables. 157
9.30. Esquema de un montaje de ejemplo realizado con bandejas portacables. 157
9.31. Cupla de unión simple, la cupla de unión articulada y la bulonería. 158
9.32. Esquemas e imágenes de las uniones para derivaciones en “T”y en “Cruz”. 158
9.33. Curvas en bandejas portacables: a 90 grados, a 45 grados y curvas verticales. 158
9.34. Embudos de bajada: en forma perpendicular y en forma paralela. 159
9.35. Imágenes de las tapas y grampas de fijación para las bandejas portacables. 159
9.36. Esquemas e imágenes de los accesorios utilizados para unir bandejas portacables de diferente tamaño de base 160
9.37. Esquemas e imágenes de los pasos a través de las paredes 161
9.38. Soportes más comunes para el tendido de las bandejas portacables. 162

10.1. Access Point Colubris MSM-410. 164
10.2. Access Point Colubris MAP-320. 164
10.3. Access Point Aruba AP-125. 165
10.4. Access Point Aruba AP-60 y AP-61. 166
10.5. Access Point Proxim AP-8000. 166
10.6. Controlador Colubris MSM-750. 168
10.7. Controlador Aruba 6000. 169
10.8. Controlador Aruba 3600. 169
10.9. Switch Cisco SRW-2016. 171
10.10Switch Cisco SGE-2000P. 171
10.11Switch 3com 4200. 171
10.12Switches 3com de la familia 4900. 172
10.13Media Gateway Avaya G450 173
10.14Firewall HP Proliant ML 150 Generation 5 174
10.15Servidor SISTORE MX. 176
10.16Captura de pantalla del Sistore MX. 177
10.17Encore PCMCIA ENPWI-G2 54$Mbps$ 178
10.18D-Link 802.11g Wireless LAN USB Adapter. 179
10.19Placa de Red Linksys Wireless-g Wi Fi. 180
10.20D-link Wi-Fi PCI 54 $Mbps$ Wireless. 181
10.21Cámara VIVOTEK IP7152. 182
10.22Cámara VIVOTEK IP7139. 183
10.23Cámara DLINK DCS-3420 184
10.24D-Link DCS 2121 wireless 3G SD WIFI 185
10.25Cámara IP Inalámbrica Zavio modelo F312A Wi-Fi. 186
10.26Wireless Linksys WI-FI G WVC54GCA. 186

10.27 Teléfono Wireless Avaya 3641 . . . 187
10.28 Teléfono Wireless Avaya 3631 . . . 188
10.29 Arquitectura de red . . . 189
10.30 Recorrido del cableado en el segundo piso. . . . 196
10.31 Recorrido del cableado en el primer piso. . . . 198
10.32 Recorrido del cableado en la planta baja. . . . 200
10.33 Recorrido del cableado en el entre piso. . . . 201
10.34 Recorrido del cableado en el subsuelo. . . . 203
10.35 Recorrido del cableado en el tercer piso. . . . 204
10.36 Recorrido del cableado en el cuarto piso. . . . 206
10.37 Recorrido del cableado en el quinto piso. . . . 207

11.1. Intensidad de señal (dBm) . . . 212
11.2. Relación señal ruido (dB) . . . 213
11.3. Interferencia (dBm) . . . 214
11.4. Velocidad de datos ($Mbps$) . . . 215
11.5. Estado RF . . . 216
11.6. Motivo de fallo . . . 217
11.7. Intensidad de señal (dBm) . . . 218
11.8. Relación señal ruido (dB) . . . 219
11.9. Interferencia (dBm) . . . 220
11.10 Velocidad de datos ($Mbps$) . . . 221
11.11 Estado RF . . . 222
11.12 Motivo de fallo . . . 223
11.13 Intensidad de señal (dBm) . . . 224
11.14 Relación señal ruido (dB) . . . 225
11.15 Interferencia (dBm) . . . 226
11.16 Velocidad de datos ($Mbps$) . . . 227
11.17 Estado RF . . . 228
11.18 Motivo de fallo . . . 229
11.19 Intensidad de señal (dBm) . . . 230
11.20 Relación señal ruido (dB) . . . 231
11.21 Interferencia (dBm) . . . 232
11.22 Velocidad de datos ($Mbps$) . . . 233
11.23 Estado RF . . . 234
11.24 Motivo de fallo . . . 235
11.25 Intensidad de señal (dBm) . . . 236
11.26 Relación señal ruido (dB) . . . 237
11.27 Interferencia (dBm) . . . 238
11.28 Velocidad de datos ($Mbps$) . . . 239
11.29 Estado RF . . . 240
11.30 Motivo de fallo . . . 241
11.31 Intensidad de señal (dBm) . . . 242
11.32 Relación señal ruido (dB) . . . 243
11.33 Interferencia (dBm) . . . 244
11.34 Velocidad de datos ($Mbps$) . . . 245

11.35Estado RF 246
11.36Motivo de fallo 247
11.37Intensidad de señal (dBm) 248
11.38Relación señal ruido (dB) 249
11.39Interferencia (dBm) 250
11.40Velocidad de datos ($Mbps$) 251
11.41Estado RF 252
11.42Motivo de fallo 253
11.43Intensidad de señal (dBm) 254
11.44Relación señal ruido (dB) 255
11.45Interferencia (dBm) 256
11.46Velocidad de datos ($Mbps$) 257
11.47Estado RF 258
11.48Motivo de fallo 259

13.1. Flujo de Inversiones (U$S) 271
13.2. Beneficios (U$S) 273
13.3. Flujo de Caja Descontada 276

A.1. Plano 1er Piso 281
A.2. Plano 2do Piso 282
A.3. Plano 3er Piso 283
A.4. Plano 4to Piso 284
A.5. Plano 5to Piso 285
A.6. Plano Planta Baja 286
A.7. Plano Subsuelo 287
A.8. Plano Entre Piso 288

Índice de cuadros

4.1. Especificaciones de los switches 20
4.2. Cantidad de computadoras aproximadas por piso. 22

5.1. Resultados de delay, packet loss y jitter obtenidos 32

7.1. Asignacion de tiempos de tareas 67
7.2. Tiempos al 10 % según el método PERT 70
7.3. Frecuencia de ocurrencia de máxima duración 71
7.4. Frecuencia de ocurrencia de intervalos de duración 72
7.5. Asignación de recursos y cálculo de costos de la mano de obra 79

8.1. Características del estándar 802.1x 85
8.2. Canalizaciones en función del número de cables. 100
8.3. Resumen tecnologías Ethernet 101
8.4. Ancho de banda requerido por los diferentes codificadores 103
8.5. Comparación H.323-SIP 107

9.1. Cobertura de los APs en diferentes ambientes 137
9.2. Limites de potencia de RF en bandas no licenciadas. 142
9.3. Pinturas para blindaje electromagnético 148
9.4. Tasas de bits estimadas de datos 151
9.5. Ancho de banda estimada de voz 151
9.6. Tasas de bits estimadas para una cámara IP 153
9.7. Ancho de banda estimada de vídeo 153

10.1. Access Points propuestos 167
10.2. Access Points propuestos cont. 167
10.3. Controladores 168
10.4. Switches de borde propuestos 170
10.5. Firewall A 189
10.6. Firewall B 190
10.7. Bloques de direcciones IP Publicas 190
10.8. Tabla de ruteo del firewall A 191
10.9. Tabla de ruteo del firewall B 191
10.10. Calidad de servicio 192
10.11. Longitud del cableado aproximado por piso. 208

12.1. MTBF de los equipos utilizados. 263
12.2. Tiempos de reposición con con y sin repuestos disponibles 268
12.3. Especificaciones de los switches 268
12.4. Disponibilidad 269

13.1. Flujo de Caja Descontada 275
13.2. VAN 277
13.3. TIR 277
13.4. TRI 277
13.5. RCBN 278

Capítulo 2

Introducción

2.1. Historia

La red informática de la Facultad de Ingeniería de la Universidad de Buenos Aires (FIUBA) ya ha sido relevada y documentada previamente por Castoldi, Fernando Ariel (74.367) y Bozzuto, Javier [C&B03] y por Mora, Santiago (76256) y Gallego, José Fransisco (76791) [M&G03], pero ambos trabajos datan del año 2003. En cinco años que separan este trabajo profesional de aquellos, las especificaciones sobre la red, las nuevas tecnologías (VoIP[1], Cámaras IP, etc) y las costumbres de uso han cambiado. Los relevamientos hechos, la topología, los análisis de tráfico y las propuestas han quedado mayormente desactualizadas.

2.2. Justificación del Proyecto

Proponemos una actualización del relevamiento y estado actual de la red, y la proyección de la misma para absorber la creciente demanda generada por el aumento de computadoras y nuevas tecnologías, en la facultad.

Recordemos que en 2003 las conexiones de los usuarios eran "Dial Up"y actualmente son todas de banda ancha.

Proponemos también analizar y proyectar la red para la posible implementación de VoIP, y seguridad por medio de cámaras de vídeo IP. Para ello se trabajará en conjunto con alumnos que actualmente analizan dicha implementación para la facultad, y ofrecer por medio de este trabajo un estudio de las características que nuestra red deberá tener para incorporar esa tecnología sin que ello presente una disminución de la calidad de servicio.

Se analizará si el estado de la red actual ha mejorado con respecto a lo proyectado por los trabajos del 2003. Si las infracciones detectadas por nuestros compañeros han sido corregidas, o al menos tomadas en cuenta, y se analizará el estado actual de las infracciones y fallas de recomendaciones.

[1] Voz sobre IP.

Capítulo 3

Objetivos

3.1. Finalidad del proyecto

Los objetivos planteados para nuestro Trabajo Profesional de Ingeniería Electrónica son: llevar a cabo un proyecto que permita aplicar los conocimientos adquiridos a través de la carrera, obtener experiencia de campo que nos permita desarrollarnos profesionalmente en el ámbito laboral y al mismo tiempo posicionar en forma tecnológica a nuestra Facultad de Ingeniería en el área de la especialidad a la que hemos orientado nuestra carrera: Telecomunicaciones e Informática. Diseñar, organizar y presupuestar la red que se debería tener para mejorar la actual calidad y robustez del servicio y prepararlo para recibir y soportar debidamente VoIP, y seguridad mediante cámaras IP.

3.2. Planteo del problema a resolver

La cantidad de usuarios que utilizan la LAN[1] de la Facultad de Ingeniería de la Universidad de Buenos Aires se ha incrementando considerablemente en los últimos tiempos debido a que Internet se ha convertido en una de las herramientas prácticamente imprescindibles en el ámbito académico. Algunas de las causas que favorecen tal incremento es que se desarrollan actividades como la docencia, el desarrollo, la investigación y la formación de un considerable número de alumnos, para las cuales se necesita acceder a información tecnológica de vanguardia que la red de redes ofrece, y también por ser actualmente la forma de comunicación más rápida y eficiente para el acceso a la misma. Por consiguiente, creemos que la utilización de recursos continúa la misma línea de crecimiento y esto ha llevado a que para satisfacer tal demanda, quizás se hayan incumplido las recomendaciones que las normas explicitan.

Debido a las razones comentadas anteriormente y a los factores que deberán ser estudiados y analizados con el correspondiente relevamiento de la red actual, se aspira en este proyecto a llevar acabo el rediseño de la misma. De forma que no solo permita satisfacer el servicio actual, sino además satisfacer futuros incrementos de demanda del servicio así como también la incorporación de nuevas tecnologías con la correspondiente planificación. Para llevar a cabo tal proyecto se deberá tener en cuenta en el análisis los siguientes ítems:

[1] Local Area Network (Red de Área Local).

- Cableado estructurado
  - Cableado horizontal
  - Backbone
  - Entradas de servicios
  - Materiales
  - Salas para equipos
  - Distribución en la infraestructura
  - Sistema de alimentación
  - Puesta a tierra
- Equipos
- Costos
- Tiempos de implementación
- Recursos
- Normas

Y también aquellas recomendaciones y especificaciones técnicas que permitan a la Subsecretaría de Informática y Organización de la *FIUBA* llevar a cabo la obra de implementación de la nueva red de datos de la Sede de Paseo Colón.

La existencia de proyectos en paralelo de sistemas de seguridad y de telefonía para dicha sede que requieren transmisión de información sobre la red de datos local, serán tenidos en cuenta en el nuevo diseño de la misma. De esta forma se podrá incluir en una única estructura de red los tres servicios mencionados, realizando un trabajo integral que permita resolver conjuntamente las distintas necesidades de la facultad y buscando al mismo tiempo optimizar la utilización de recursos y los costos asociados a la realización del proyecto.

Capítulo 4

Relevamiento físico actual de la red

En esa etapa se realizó el recorrido en las instalaciones de la FIUBA con el objeto de relevar los equipos y el cableado de la red. Para esto se contó con la colaboración del Sr. Miguel Rodríguez y Lic. Javier Apat.

4.1. Descripción topológica de la red

El tendido de cable para una red de área local tiene cierta complejidad cuando se trata de cubrir áreas extensas tales como un edificio de varias plantas, como es el caso de la FIUBA.

La idea básica del cableado estructurado es simple:

- Tender cables en cada piso del edificio.
- Interconectar los cables de cada piso.

Se llama "cableado horizontal" al que se encarga de unir los puestos de trabajo permitiendo el acceso a la red en cada piso del edificio y "cableado vertical" al que vincula las conexiones entre pisos.

Usando el diagrama lógico de la Figura 4.1 como ayuda para entender la distribución física de la red podemos observar:

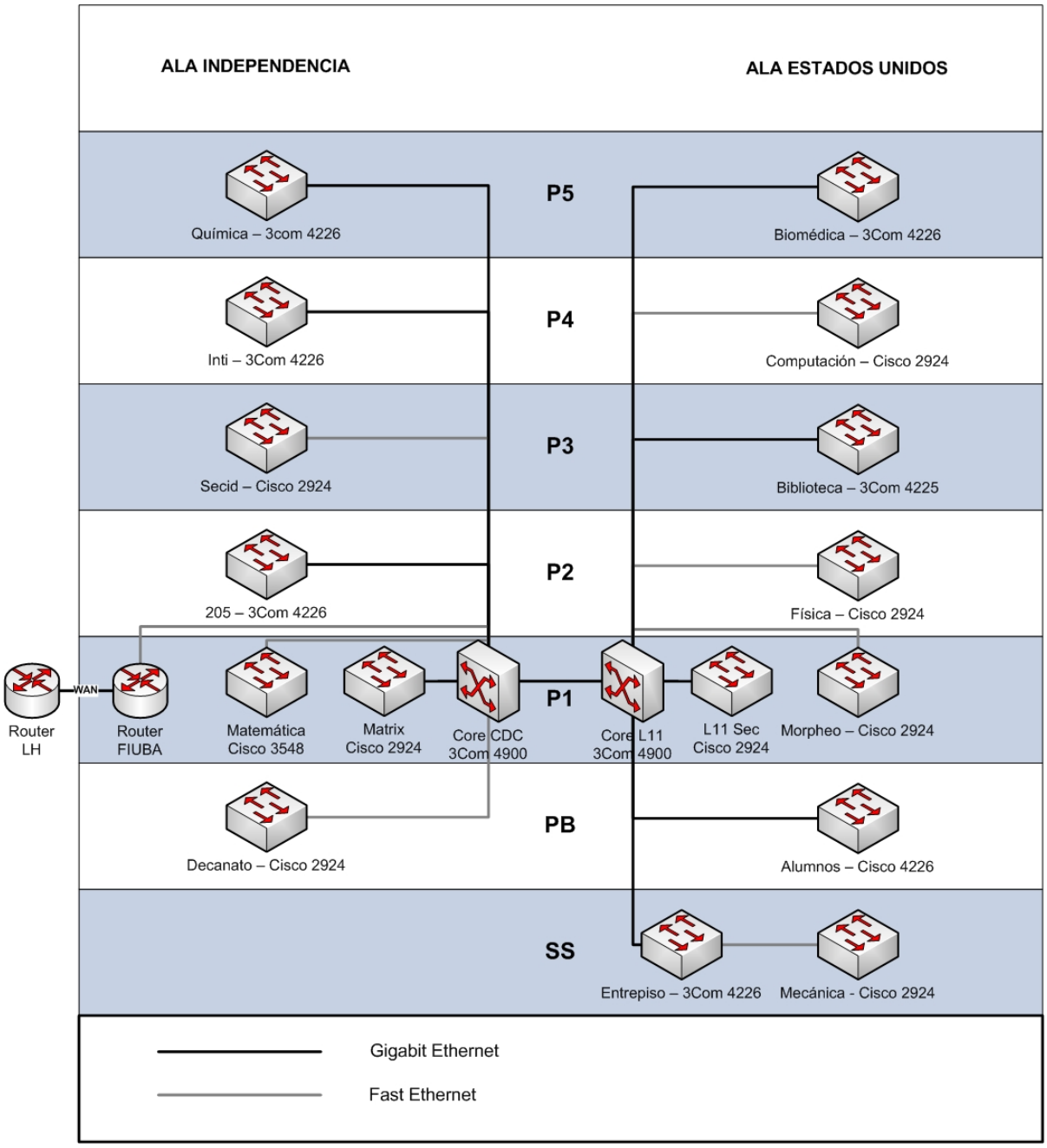


Figura 4.1: Diagrama lógico de la FIUBA

La estructura actual de la red se encuentra dividida en dos grandes secciones

- Ala Independencia
- Ala EE.UU

Estas se encargan de concentrar el cableado vertical que interconecta cada switch de piso a través del switch de core. El Ala Independencia se conecta a través del switch "Core CDC"[1] con el switch "Core L11"en el Ala EE.UU por medio de cableado UTP e interfaz Gigabit Ethernet.

[1]Centro de Cómputos

En cada piso se distribuye el cableado de acceso para llegar a las pacheras de los usuarios. En el primer piso del Ala Independencia se encuentra el enlace de fibra WAN al CCC[2]. El mismo es de $12Mbps$ y la compañía que lo gestiona es Telmex. Este se conecta a un switch que lo administra la misma empresa, y del mismo, se conecta al router FIUBA administrado por el CCC de la UBA.

De cada uno de estos switches, sube el cableado vertical que también se encuentra realizado en UTP para distribuir la conexión piso por piso. Las interfaces son Gigabit Ethernet y Fast Ethernet distinguidas en la Figura 4.1 mediante diferentes espesores de líneas. En cada piso hay un switch por ala que se encarga de distribuir la conexión a todo un sector.

El cableado horizontal se encuentra tendido por medio de cable canal de plástico amurado a elevado altura para dificultar el acceso y brindar seguridad física excepto en el sector de matemática (Ala Independencia, primer piso) que se encuentra realizado con bandeja porta cable de chapa galvanizada.

La mayor parte del tendido del cableado vertical fue realizado a través de los conductos de ventilación del primer al quinto piso que se encuentran fuera de servicio. También se emplearon los ascensores de carga que no se utilizan actualmente sobre la calle Azopardo y una conexión por el exterior del edificio. Este cableado se distingue del cableado horizontal por su color amarillo.

4.2. Equipos de la red

En la Figura 4.1 se observan equipos de marca 3Com y Cisco. Los modelos 3Com tienen interfaces "Gigabit Ethernet"y los modelos Cisco "Fast Ethernet". Cuya principal diferencia es la capacidad teórica del canal, $1Gbps$ y $100Mbps$ respectivamente.

En su mayoría los equipos, salvo contadas excepciones, se encuentran en armarios bajo llave a elevada altura para dificultar el acceso a los mismos al igual que el cableado.

En el Cuadro 4.1 se puede ver el resumen de las especificaciones de los distintos switches que componen la red obtenido de las hojas de datos pertinentes.

Switch	**3Com 4226**	**3Com 4900**	**Cisco 2924**	**Cisco 3548**
Cantidad	7	2	8	1
Layer I	10/100-BASE-TX	100/1000-BASE-TX	100/1000-BASE-TX	100/1000-BASE-TX/SX
Layer II	26 ports FE y 2 ports GE	12 ports FE/GE	24 ports FE	48 ports FE y 2 ports GE
Capacity	$8.8Gbps$	$32Gbps$	$3.2Gbps$	$10Gbps$
Forwarding rate	$6.6Mbps$	$23.8Mbps$	$3.3Mbps$	$6.5Mbps$
Latency	2.7ms	2.7ms	-	-
MAC addresses	8K MAC addresses	12K MAC addresses	2K MAC addresses	8K MAC addresses
VLANs	60	30	64	-
Link aggregation	Gigabit ports only	Si	12 ports	Si
Spanning Tree	STP y RSTP	STP y RSTP	STP	STP

Cuadro 4.1: Especificaciones de los switches

Para obtener mayor detalle de las características de los equipos se puede consultar las hojas de datos en el CD adjunto.

[2]Centro de Comunicación Científica

4.2.1. Alimentación eléctrica de los equipos

Antiguamente, los equipos de la red recibían alimentación eléctrica directamente del toma corriente más cercano, y la consiguiente administración no estaba hecha por parte del sector de redes. Esto acarreaba varios inconvenientes, entre ellos:

- Cortes involuntarios con pérdida de servicio y riesgo para el equipo
- No se garantiza la conexión segura a tierra.
- Alimentación descentralizada (ausencia de un panel central eléctrico).

Actualmente, en el Ala Independencia, se realizó un tendido eléctrico dedicado con puesta a tierra segura y se diseñó un panel central ubicado en el box de "Soporte Informático" del primer piso resolviendo parte de los inconvenientes mencionados. También está planificado realizar el mismo tendido para el Ala EE.UU.

4.2.2. Sistema de Alimentación Ininterrumpida (UPS)

Los equipos UPS[3] son dispositivos que gracias a sus baterías, pueden proporcionar energía eléctrica tras un corte de energía a todos los dispositivos que tengan conectados. Otra de las funciones de las UPS es la de mejorar la calidad de la energía eléctrica que llega a los aparatos, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de Corriente Alterna. Los UPS dan energía eléctrica a equipos críticos, que pueden ser aparatos médicos, industriales o informáticos, que como se ha dicho antes, requieren tener siempre alimentación y que ésta sea de calidad debido a la necesidad de estar en todo momento operativos y sin fallos (picos o caídas de tensión).

En el recorrido vimos tres equipos UPS, uno era el "Libert GXT" provisto por la empresa Telmex para el cuidado de sus equipos, otro para servidores del datacenter del CDC y el último para los switches de piso de la facultad.

4.2.3. Refrigeración de los equipos

Los equipos se encuentran alojados en armarios refrigerados por "coolers"o ventiladores. Los servidores, el switch "Core CDC" y "router FIUBA" están alojados en el box de Soporte Informático, refrigerado por aire acondicionado.

4.2.4. Routers Wi-Fi

Actualmente se encuentran dos zonas Wi-Fi o de acceso inalámbrico. Una de ellas se encuentra en la biblioteca y la otra en el aula L11. Este servicio está conectado por medio de una VLAN[4]. Esto permite separar el tráfico de los usuarios que acceden por este medio de forma tal de brindar mayor seguridad. Formando una canal lógico que accede directamente a una interfaz del proxy para dar conectividad a la red. Los routers utilizados como access point son Linksys WRT54G y Asus WL-520GU cuyas hojas de datos se pueden ver en el CD adjunto.

[3]Uninterruptible Power Supply.
[4]Virtual Local Area Network

4.3. Descripción detallada por pisos

En esta sección haremos una descripción más detallada de la red piso por piso. Se adjunta los planos de los mismos en el Apéndice A, en los que se puede observar la cantidad de computadoras en cada dependencia, conectividad de estas, ubicación de los equipos de red, ubicación de pisos y techos falsos y ubicación de los lugares donde hay mármol.

Presentamos la cantidad aproximada de computadoras por piso de acuerdo a los planos que obtuvimos de parte del señor Miguel Rodríguez. Los planos estaban actualizados al momento de comenzado el trabajo, pero consideramos que es posible que no sean totalmente precisos.

Piso	**Cantidad de computadoras**
1er Piso	110
2do Piso	87
3er Piso	80
4to Piso	163
5to Piso	59
Planta Baja	135
Subsuelo	97
Entrepiso	61
Total	792

Cuadro 4.2: Cantidad de computadoras aproximadas por piso.

No se puede determinar con precisión la cantidad de teléfonos, pero se estima que hay aproximadamente un total de 300 según la información que se pudo recaudar.

4.4. Conclusiones del relevamiento

Esta sección pretende destacar las deficiencias que encontramos luego de haber realizado el relevamiento con el objeto de tenerlas en cuenta en el diseño futuro, entre ellas se distinguen:

Cableado Horizontal : Como se mencionó anteriormente, se encuentra a elevada altura para dificultar su acceso. El mismo se encuentra contenido en cablecanal de plástico. Si bien esto brinda cierta seguridad, creemos que la misma no es suficiente dado que puede mejorarse empleándose bandejas porta cable.

Acceso a equipos : Se pudo ver que la mayoría de los equipos se encontraban bajo llaves en aulas o almacenados en armarios. Los que no han sido segurizados deberían serlo.

Perdidas de servicio : Notamos que frente a cualquier falla de equipo o caída de un enlace la red no ofrece soluciones de respaldo que permita mantener el servicio.

Alimentación : La alimentación de la red, en la actualidad no está totalmente centralizada.

Distancias y etapas de switches : Habiendo consultado la norma de cableado estructurado [568-B] en la sección 11.2.4.3.2 "Length requirements", que especifica que la máxima distancia para el cable UTP Ethernet $10/100/1000Mbps$ es de $100m$, se concluye de la observación de los planos de la facultad que no se sobrepasa dicha longitud, a pesar del recorrido del cableado.

Capítulo 5

Análisis de Tráfico

5.1. Introducción

Antes de cualquier etapa de diseño es importante ver los recursos utilizados por los usuarios de la red actual, esto permitiría evaluar el grado de uso de la red.

El análisis del volumen del tráfico permitirá establecer si la red está correctamente dimensionada con respecto al uso, y se podrá estimar si soportará la carga extra que representará el servicio de seguridad mediante cámaras IP y el de VoIP respectivamente, o en caso de llegar a la conclusión de que no se soportará, dimensionarlo correctamente.

También permitirá caracterizar la distribución lógica de la red, haciendo un análisis de las redes virtuales existentes.

5.2. Detalles de la realización del análisis.

El análisis aquí presentado, fue realizado en conjunto con el staff del Centro de Cómputos. Se nos facilitó de sus gráficos del tráfico de la red interna. Cabe destacar que un análisis más profundo debería haberse efectuado con varias muestras y no una sola, a lo largo de más días, para obtener una estadística más correcta.

5.3. Tráfico LAN.

Cuando un nodo tiene solo un paquete para enviar, ese nodo puede transmitir al máximo que la tecnología Ethernet le permite ($10Mbps$, $100Mbps$, o $1Gbps$). Sin embargo, como se comparte el medio de transmisión, muchos nodos querrán transmitir varios paquetes. Por lo tanto, la efectividad de la tasa de transmisión del canal puede ser mucho menor. Se define la eficiencia de Ethernet como la fracción de tiempo durante el cual los paquetes están siendo transmitidos en el canal sin colisiones, siempre y cuando haya un gran número de nodos activos, con cada nodo teniendo un gran número de paquetes para transmitir. Para poder presentar una ecuación cerrada para la eficiencia de Ethernet, supongamos que t_{prop} es el máximo tiempo que lleva a la señal propagarse entre extremo y extremo, y t_{trans} es el tiempo para transmitir un paquete de máximo tamaño en Ethernet, aproximadamente $1.2ms$ para $10Mbps$ Ethernet, si no hubo colisiones presentes al momento de transmitir. En ese caso la eficiencia sería del 100 %.

$$Eficiencia \approx \frac{1}{1+5a} \tag{5.1}$$

Donde:

$$a = \frac{t_{prop}}{t_{trans}} \tag{5.2}$$

Una demostración de esta fórmula se encuentra más allá de los objetivos de este texto, ver [B&G92] y [LAM80]. Si se grafica la Ecuación 5.1 se obtiene la Figura 5.1, donde se puede ver que la eficiencia decrece a medida que a aumenta

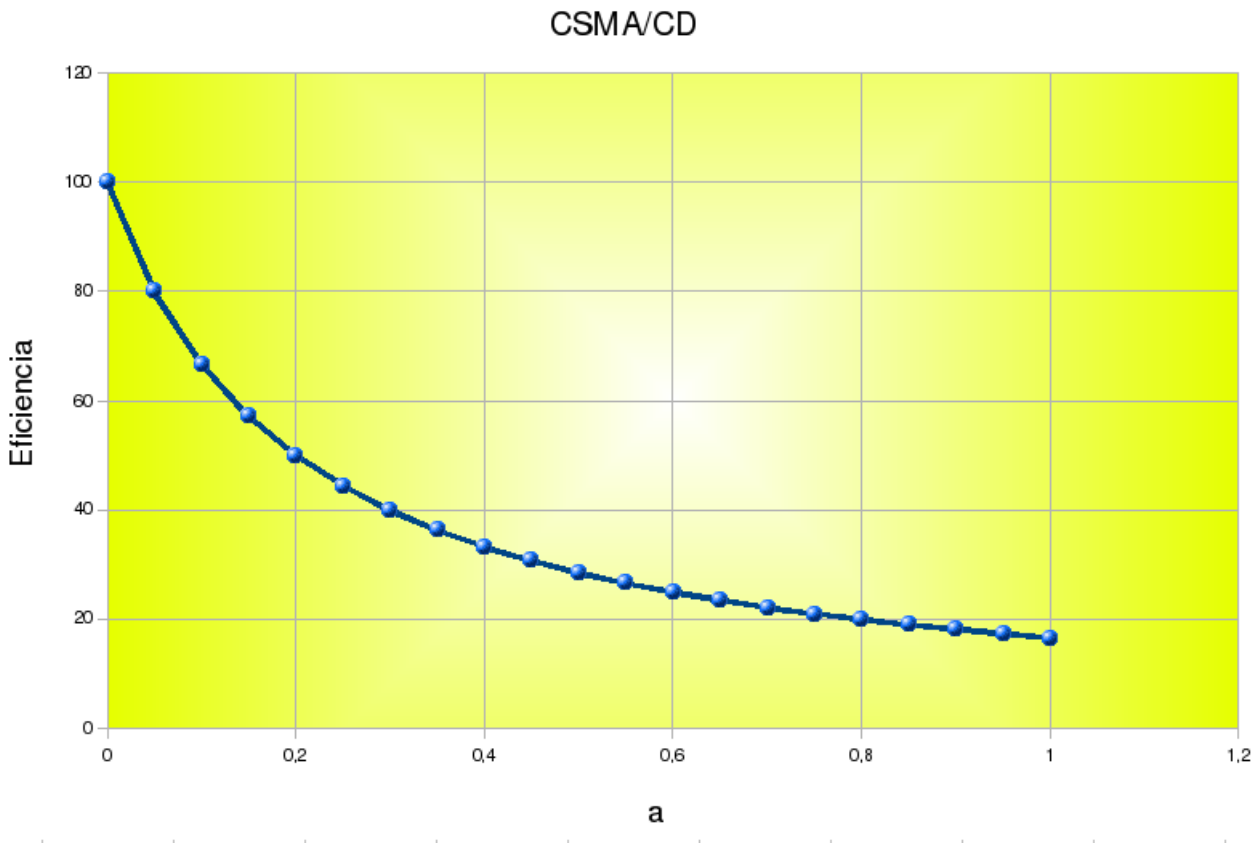


Figura 5.1: Eficiencia de Ethernet

Se considera que si el tráfico cursado, es decir a, es menor al 10 % del ancho de banda, no hay congestión debido a que la eficiencia es mayor a un 70 %. Si a se encuentra entre el 10 % y el 50 % se lo considera como una congestión leve (hasta un 30 % de eficiencia) y finalmente si es mayor a 50 %, es considerada una congestión severa (eficiencia inferior al 30 %).

Se realizó un "sniffing"de la red con la aplicación Open Source "Wireshark"y los lugares elegidos para monitorear fueron:

- El acceso Wi-Fi de la Biblioteca, ubicada en el el 3er piso.
- La sala de computación del 4to piso.

- El laboratorio abierto (LABI) del primer piso.

Los análisis fueron realizados en lapsos cortos de tiempo en el horario de las 20 horas. Estadísticamente pueden no ser considerados como representativos, pero permite formar una idea aproximada de la situación de la misma. Se hicieron descargas de archivos desde servidores de la intranet, y también desde servidores de internet, con el propósito de observar el funcionamiento y obtener conclusiones.

Este análisis se realizó con el objetivo de analizar la funcionabilidad de la red y **no** el contenido de los paquetes, preservando la privacidad de los mismos en todo momento.

Se encontró que se propagan paquetes STP[1] sin que haya ningún tipo de redundancia física que justifique la implementación de dicho protocolo. La cantidad total de estos pueden verse bajo la etiqueta "Displayed"en el cuadro de diálogo que se ve en la Figura 5.2.

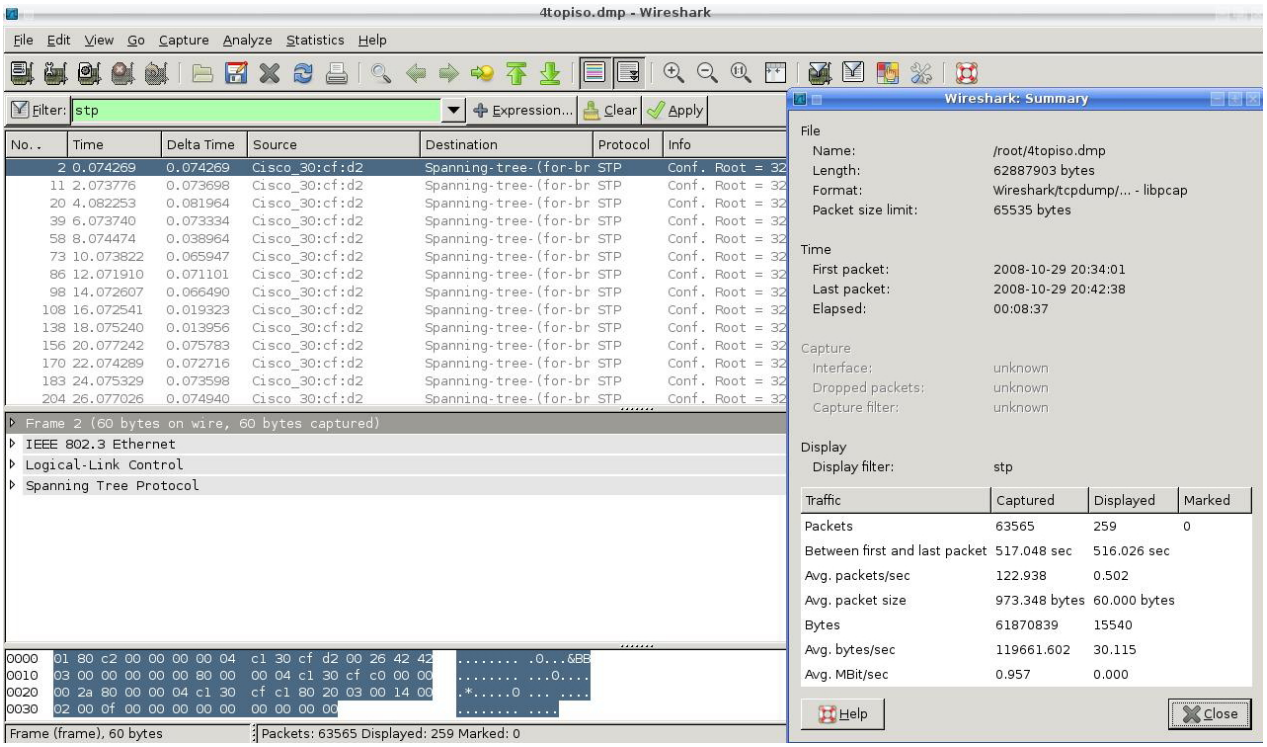


Figura 5.2: Paquetes STP en el 4to Piso

Se encontró una muy baja cantidad de errores (0.01 % sobre el total de paquetes), mayormente debido a pérdida de paquetes TCP[2] en la conexión del 4to piso, pero que se encuentran en rangos más que normales. Estos pueden verse resaltados en color amarillo en la Figura 5.3

[1]Spanning Tree Protocol.
[2]Transmission Control Protocol.

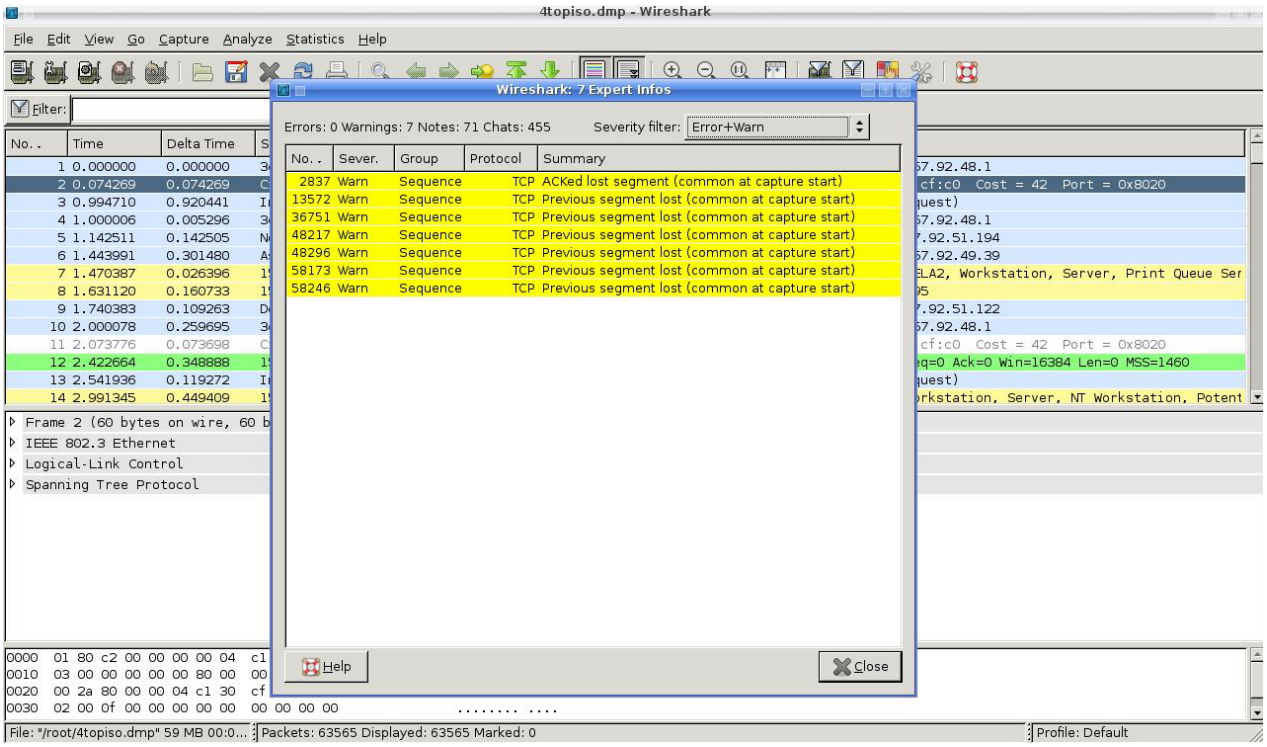


Figura 5.3: Errores en el 4to Piso

En la conexión Wi-Fi de la biblioteca, se encontró una mayor cantidad de errores (0.75 % sobre el total de paquetes). Estos también eran mayoritariamente referidos a problemas de pérdida de paquetes TCP en la conexión o ACK[3] repetidos, pero se espera que en una conexión con medio de acceso inalámbrico se tengan más problemas. De todas maneras se pudo comprobar que la conexión inalámbrica que se da en la biblioteca actualmente es de muy buena capacidad y calidad.

[3] Acknowledgement.

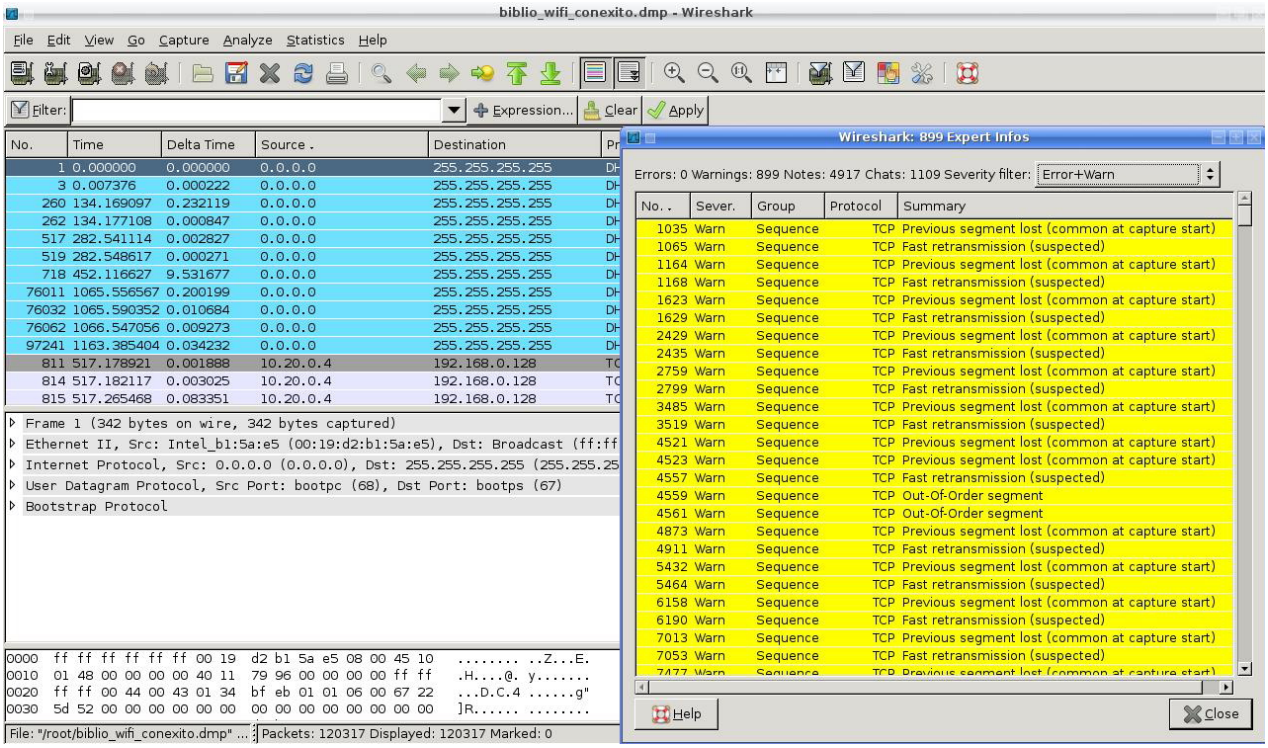


Figura 5.4: Errores en la biblioteca

En el Apéndice B se expone el monitoreo de tráfico de los distintos switches indicando los ports correspondientes de cada uno. Los mismos fueron facilitados por el personal del Centro de Cómputos y permite obtener el grado de congestión actual.

En el eje de abscisas se indica el tiempo, este tiene una duración de 33 horas. En el eje de ordenadas se indica el "bit rate", el mismo no tiene una escala fija, por lo que se fija según la intensidad de tráfico de cada uno. El tráfico correspondiente a cada port se indica en color azul para el saliente y en color verde para el entrante.

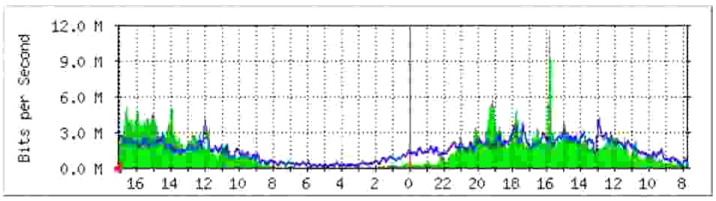
Como primera apreciación, vemos que en la mayoría de los gráficos se puede notar una "busy hour" situada alrededor de las 16 horas, indicando que esta es la hora de mayor congestión en la red. El "Port 8" del switch "CORE SW CDC " es el que mayor tráfico presenta a dicha hora, alcanzando valores máximos de $15Mbps$. Esto implica, como se explicó en los comienzos de esta misma sección, que un 15 % de la utilización del canal representa una congestión leve. Pero en general se encuentra en valores acotados que no llegan a congestionar el canal que conecta al router.

5.4. Tráfico WAN

SW DISTRIBUCION MATRIX - PORT 2 - ROUTER

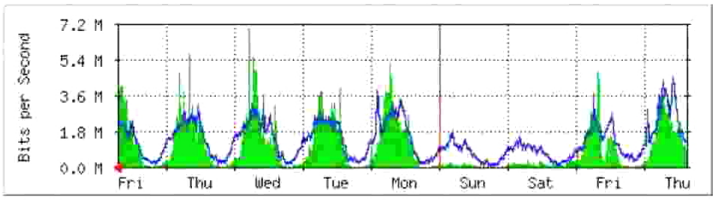
Estadísticas actualizadas el **Viernes 19 de Setiembre de 2008 a las 17:07**, **'MATRIX'** ha estado funcionando durante **60 days, 7:10:31**.

Gráfico diario (5 minutos : Promedio)



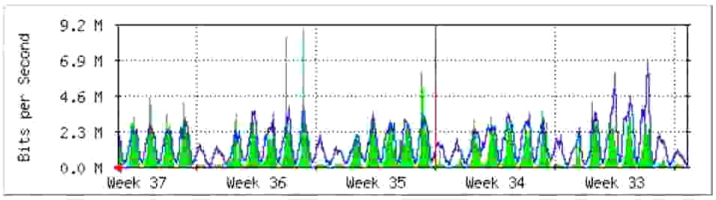
Máx Entrante 11.6 Mb/s Promedio Entrante:1599.7 kb/s Actual Entrante:2009.6 kb/s
Máx Saliente:4188.1 kb/s Promedio Saliente:1503.7 kb/s Actual Saliente:2260.3 kb/s

Gráfico semanal (30 minutos : Promedio)



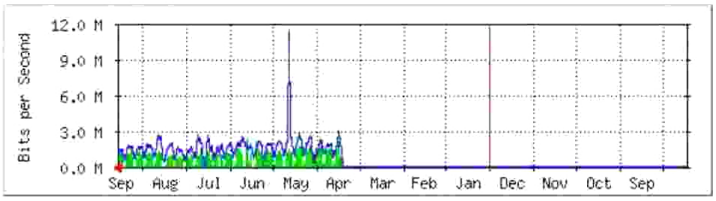
Máx Entrante 7006.6 kb/s Promedio Entrante:1111.8 kb/s Actual Entrante:3444.6 kb/s
Máx Saliente:4464.5 kb/s Promedio Saliente:1344.0 kb/s Actual Saliente:2338.8 kb/s

Gráfico mensual (2 horas : Promedio)



Máx Entrante 9015.4 kb/s Promedio Entrante:1014.3 kb/s Actual Entrante:2944.7 kb/s
Máx Saliente:6978.0 kb/s Promedio Saliente:1501.4 kb/s Actual Saliente:1824.3 kb/s

Gráfico anual (1 día : Promedio)



Máx Entrante 2633.4 kb/s Promedio Entrante: 652.8 kb/s Actual Entrante:1367.4 kb/s
Máx Saliente: 11.4 Mb/s Promedio Saliente:1030.9 kb/s Actual Saliente:1495.9 kb/s

VERDE ### Tráfico entrante en Bits por segundo
AZUL ### Tráfico saliente en Bits por segundo

Figura 5.5: Tráfico del enlace WAN

De la Figura 5.5 se observa que el uso del enlace WAN es aproximadamente de un 25 %. Este es un enlace Gigabit Ethernet punto a punto de $12Mbps$. Consideramos que el mismo se encuentra correctamente dimensionado para la demanda actual.

5.5. Análisis del "delay", "jitter"y "packet loss"

En esta sección se analizan los tiempos de delay, variación del mismo y pérdida de paquetes. Estos representan requerimientos claves a la hora de implementar servicios de tiempo real como VoIP y IPTV sobre la red.

A continuación definiremos los mismos:

RTT [4]: Es el tiempo que tarda un paquete enviado desde un emisor en volver a este mismo emisor habiendo pasado por el receptor de destino. El mismo se compone de:

- Tiempo de inserción del emisor y receptor.
- Tiempo de propagación del emisor y receptor.
- Tiempo de procesamiento.

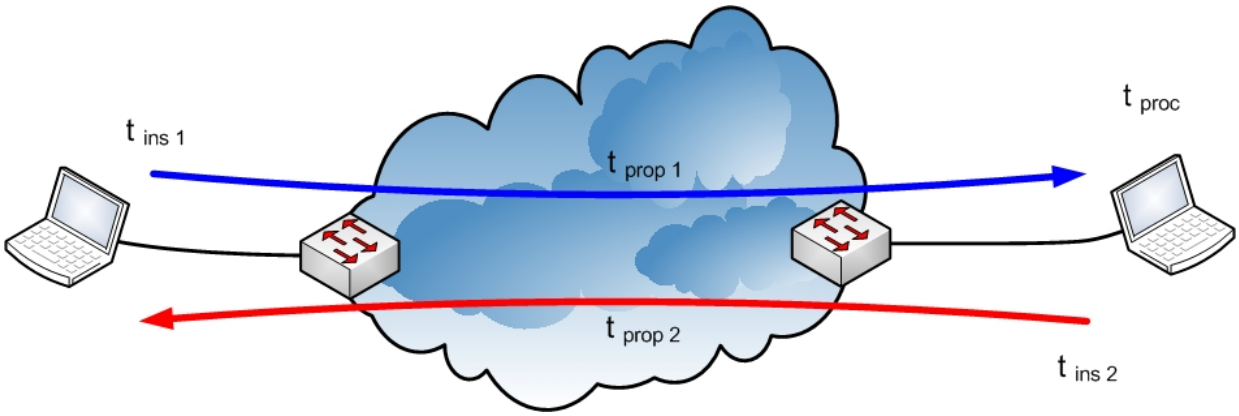


Figura 5.6: Round-Trip Time

Este se calcula de la siguiente forma:

$$\begin{aligned} RTT &= t_{ins\ 1} + t_{prop\ 1} + t_{proc} + t_{ins\ 2} + t_{prop\ 2} \\ &\cong 2(t_{ins} + t_{prop}) + t_{proc} \end{aligned} \tag{5.3}$$

"One-way delay" : Es el tiempo de propagación de un paquete de datos desde un origen a un destino, el cual se lo puede considerar como la mitad de RTT aproximadamente, debido a que el tiempo de procesamiento es despreciable por ser varios órdenes de magnitud menor que los tiempos de inserción y propagación.

"Delay jitter" : Es el desvío estadístico del RTT.

[4]Round-Trip Time.

En la Figura 5.7 se posicionan los distintos servicios en función de la calidad de servicio (QoS[5]), donde el eje horizontal representa el máximo jitter posible y el eje vertical la tasa de paquetes perdidos.

Se puede observar que la transmisión de datos es la menos exigente. Esto se debe a que si se pierden paquetes, se pueden retransmitir sin que esto afecte el servicio. En cambio, se observa que en servicios de vídeo es más exigente ya que una restransmisión fuera de término no tiene sentido. En voz sucede lo mismo, pero en el caso que la calidad disminuya tanto que el oyente no interpretase lo dicho, él mismo puede solicitar al locutor la repetición de la frase.

Con respecto a las variaciones de delay, este también es más exigente para el tráfico de tiempo real, debido a que si el mismo no fuera bajo se "entrecortaría"el flujo de datos. Como no es posible un delay jitter nulo, se implementa un buffer donde se va almacenando la información, absorbiendo ráfagas de paquetes. Si la comunicación se corta demasiado tiempo, el buffer se vacía y el flujo de información se cortaría también hasta que se restaurase la señal.

Por los motivos mencionados anteriormente se utiliza un protocolo en la capa de transmisión que no efectué retransmisiones en caso de errores y que tenga bajo overhead como UDP[6] o RTSP[7] y no TCP[8].

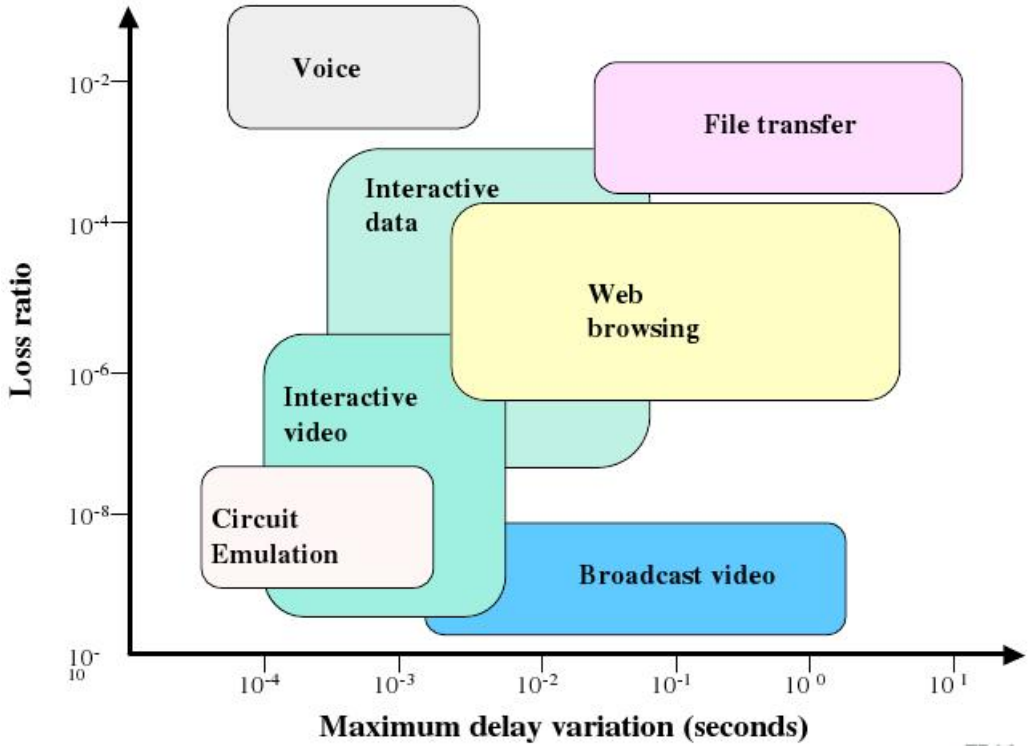


Figura 5.7: Calidad de servicio sobre redes IP.

[5]Quality of Service.
[6]User Datagram Protocol.
[7]Real Time Streaming Protocol.
[8]Transmission Control Protocol.

5.5.1. Mediciones

Para estimar los valores de delay, jitter y pérdida de paquetes se ha utilizado el comando PIGN[9] de la plataforma GNU Linux, ya que tiene una resolución del orden de los microsegundos frente a la resolución de milisegundos de la plataforma MS Windows. Este método de medición fue obtenido de las metodologías empleadas por la "Cisco IP SLA" [CISSLA]. El PING utiliza el datagrama obligatorio ICMP del protocolo ECHO_REQUEST para solicitar una ICMP ECHO_RESPONSE por parte de un servidor o una puerta de acceso. Los datagramas ECHO_REQUEST ("pings") tienen una dirección IP y "header" ICMP, seguidos por un "struct timeval"y un número arbitrario de bytes "pad" usados para completar el paquete. Las opciones que se utilizan para esta medición que simulan un "streaming"de datos son las siguientes:

Sintáxis : ping [-dfnqrvR] [-c *count*] [-i *wait*] [-l *preload*] [-p *pattern*] [-s *packetsize*]

-i *wait* : Espera *wait* segundos entre el envío de cada paquete. Por defecto se espera un segundo entre el envío de los paquetes.

-s *packetsize* : Especifica el número de bytes de datos que se van a enviar. La cantidad por defecto es 56, que pasan a ser 64 bytes de datos ICMP cuando se combinan con los 8 bytes de los datos de la cabecera ICMP. Esta opción fue utilizada para simular la longitud típica de un paquete de voz.

El PING se realiza contra el servidor http de la FIUBA debido a que se considera el peor caso ya que este presenta la mayor carga y el peor recorrido, obteniendo los siguientes resultados:

```
root@laptop:~# ping -i 0.01 -s 12500 157.92.49.219
PING 157.92.49.219 (157.92.49.219) 12500(12528) bytes of data.
12508 bytes from 157.92.49.219: icmp_seq=1 ttl=64 time=3.76 ms
12508 bytes from 157.92.49.219: icmp_seq=2 ttl=64 time=3.70 ms
12508 bytes from 157.92.49.219: icmp_seq=3 ttl=64 time=3.71 ms
...
12508 bytes from 157.92.49.219: icmp_seq=51995 ttl=64 time=3.69 ms
12508 bytes from 157.92.49.219: icmp_seq=51996 ttl=64 time=3.69 ms
12508 bytes from 157.92.49.219: icmp_seq=51997 ttl=64 time=3.70 ms

— 157.92.49.219 ping statistics —
314142 packets transmitted, 314139 received, +1 errors, 0 % packet loss, time 3154675ms
rtt min/avg/max/mdev = 3.661/3.741/16.676/0.158 ms, pipe 2999
```

Cuadro 5.1: Resultados de delay, packet loss y jitter obtenidos

Como era de esperarse, se puede observar que el "delay", el "jitter" y el "packet loss" no son variables críticas en este caso. Esto se debe a que la distancias de la red de la facultad son considerablemente pequeñas con respecto a redes MAN[10] o WAN[11]. Este es el principal factor a tener en cuenta, debido a que afecta a estas variables de la siguiente forma:

[9] Packet Internet Groupe.
[10] Metropolitan Area Network
[11] Wide Area Network

Tiempo de propagación: Una mayor distancia implica un tiempo mayor de propagación de los datos, por lo tanto, como el delay se compone por el tiempo de inserción de la trama más el tiempo de propagación de la misma, esto implicaría un incremento del mismo con la distancia.

Atenuación: Una mayor distancia implica un aumento de la degradación de la señal debido a la atenuación de la misma. Este factor afecta directamente a la perdida de paquetes, ya que los mismos son rechazados por los errores producidos.

5.6. Análisis del impacto de la ausencia de VLANs

Se analizó la proporción de paquetes ARP con respecto a la cantidad total de paquetes en la sala del 4to piso y la biblioteca, ya que en esta última se ha implementado VLAN para diferenciar el tráfico.

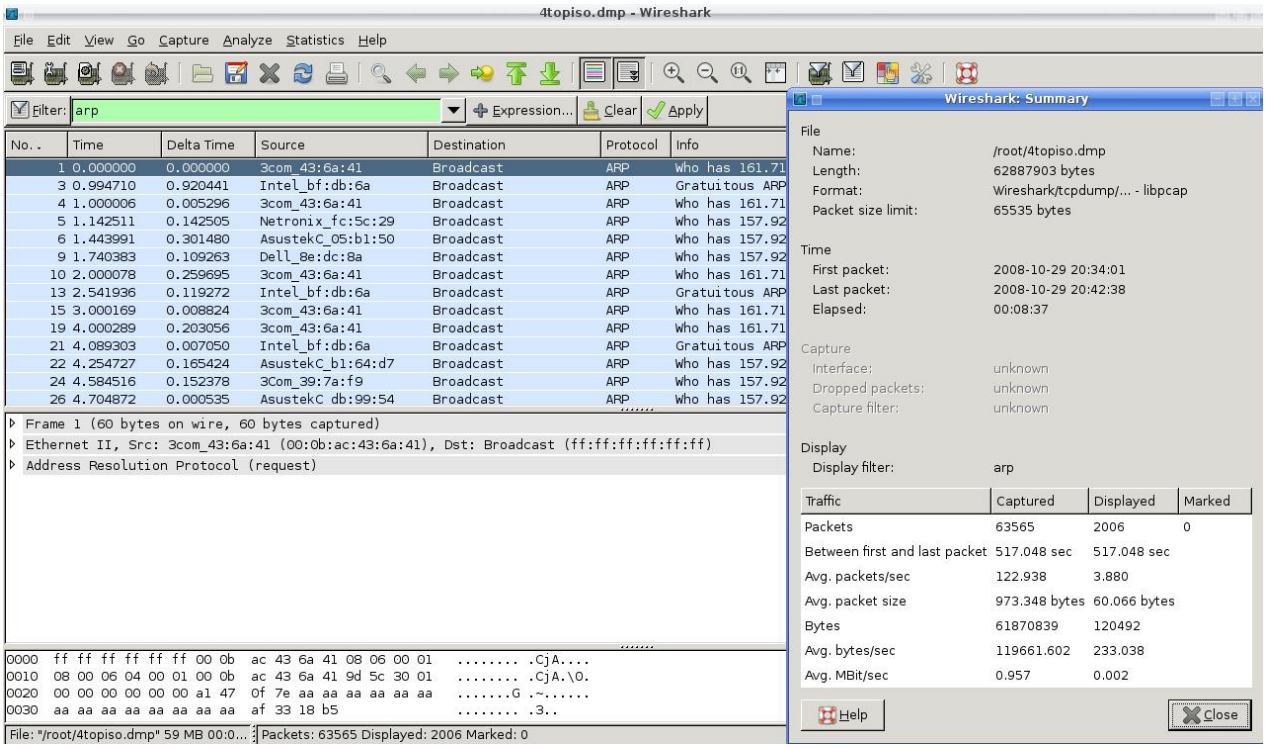


Figura 5.8: Paquetes ARP broadcast en el 4to piso

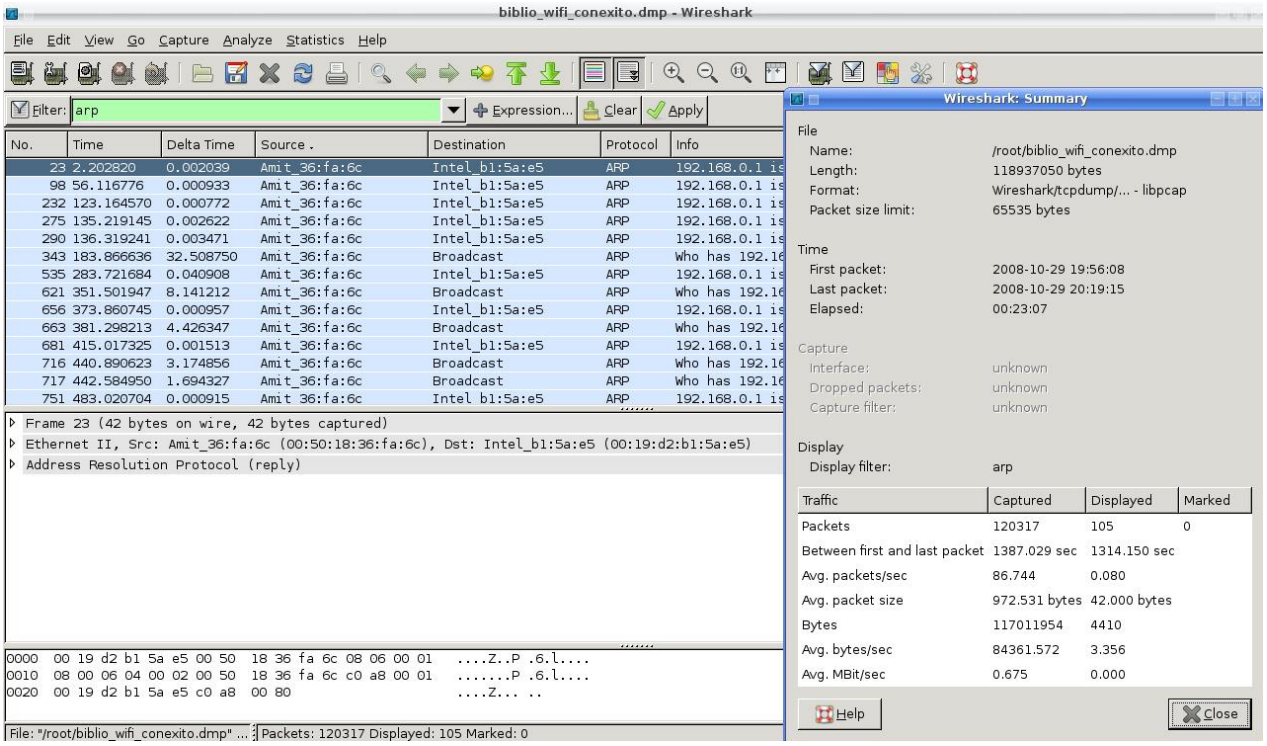


Figura 5.9: Paquetes ARP broadcast en la biblioteca

En el cuarto piso, Figura 5.8, se obtuvo una proporción de paquetes ARP del 3.15 % con respecto al total. Mientras que en la conexión por Wi-Fi, Figura 5.9, fue de 0.087 %. Esto indica que si bien la cantidad de consultas ARP de la conexión sin VLAN es mucho mayor que la otra, en ninguno de los dos casos es excesiva, lo que produciría una caída de la calidad de la conexión debido a ello.

De todas formas, se propone la implementación de VLANs por cuestiones de seguridad, independientemente de que nuestras mediciones no indiquen que la red sin esta, esté excesivamente saturada por tal motivo.

5.7. Conclusiones.

5.7.1. Sobre el volumen del tráfico.

De los estudios realizados sobre la red podemos concluir que la capa física de la misma, se encuentra correctamente dimensionada para las prestaciones actuales. Sin embargo si se quiere expandir las capacidades de la misma con el agregado de las tecnologías ya antes mencionadas (seguridad IP y VoIP) se deberán tener en cuenta los siguientes puntos entre otros:

- VoIP:

  Delay.

  Delay jitter.

  Packet Loss.

- Seguridad IP:

  Cantidad de cámaras.

  Ancho de banda usada por las mismas.

5.7.2. Sobre el uso de VLANs

Según administradores de la red, las únicas dependencias separadas por VLANs son la tesorería, la gestión de equipos y los accesos Wi-Fi.

Al no aislar el tráfico con redes virtuales, toda la red se ve afectada por los "broadcast" del mismo. El problema es que este consume ancho de banda en lugares donde no es necesario, obligando el procesamiento de paquetes a terminales o servidores innecesariamente. Este efecto se ve aumentado si la cantidad de terminales y servidores se incrementan.

Con respecto a la seguridad, cualquier persona puede conectarse a cualquier boca de red, y observar los nombres de las máquinas, dominios, sistemas operativos y otros parámetros que brindan información útil para encontrar vulnerabilidades que puedan comprometer algún servicio o usuario.

La creación de varias redes virtuales que segmenten la red, favorecerá al mejor funcionamiento de los terminales de la red, un mejor aprovechamiento del ancho de banda y mejorará la seguridad.

Capítulo 6

Objetivos y estudios preliminares al diseño del producto

Con el objetivo de satisfacer los requerimientos de los usuarios, se presentan conclusiones de un estudio realizado por una consultora especializada sobre las tendencias de uso de internet [TDUSO].

6.1. Tendencia de uso de internet

El objetivo es encontrar indicadores para conocer a los usuarios, sus necesidades y expectativas, los cuales pueden resumirse en los cuatro puntos siguientes:

1. *Adopción de Internet en la región:*

   Para el cierre del año 2008, los usuarios Latinoamericanos alcanzarán los 154 millones de personas, lo que equivale a un 27 % de penetración poblacional. Cabe resaltar que esta región, que estuvo por debajo del promedio mundial de penetración, ha sido una de las zonas más dinámicas de crecimiento en los últimos ocho años y con ello ha logrado ubicar su penetración ligeramente por encima del promedio mundial. En los próximos tres años se espera que este crecimiento se mantenga para superar un 32 % de penetración en el año 2010.

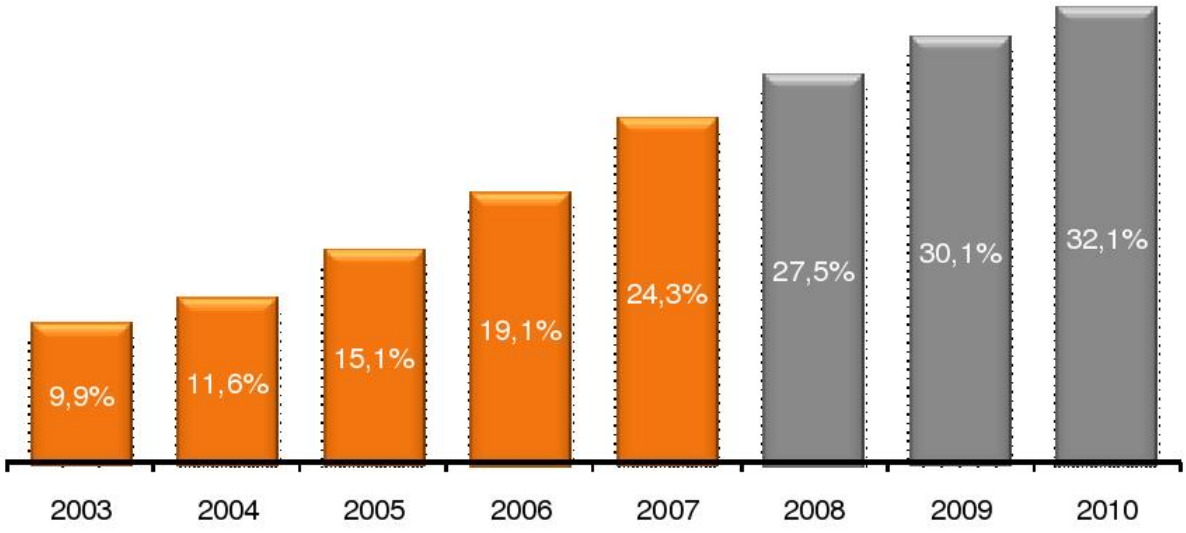


Figura 6.1: Usuarios de internet

2. *Qué se mantuvo constante con respecto al año anterior:*

   Si bien este es un espacio altamente cambiante, algunos aspectos se mantuvieron constantes en el último año. El primero de ellos se refiere a que los usuarios siguen estando caracterizados por personas menores de 24 años y con un ligero predominio del género masculino. Este último resultado es característico de un mercado en crecimiento que no se ha constituido aún en un fenómeno masivo. Igualmente, se mantuvo la importancia de los cibercafés como medio de acceso a Internet, a pesar de que las conexiones en el hogar experimentaron un importante aumento.

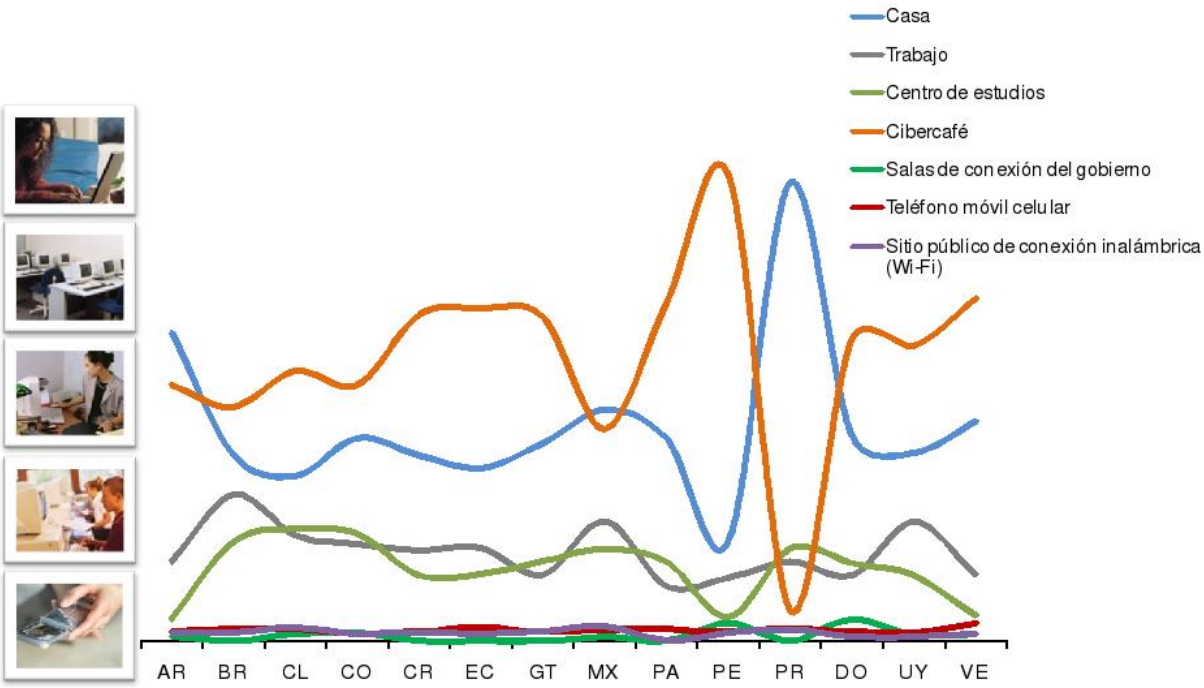


Figura 6.2: Lugares de utilización de internet

En tercer lugar, se podría decir que los tres usos principales se mantienen durante los últimos años, a saber: enviar y recibir correos electrónicos, búsqueda de información y mensajería instantánea.

Figura 6.3: Principal utilización de internet

3. *Qué cambió con relación al año anterior:*

   Por su parte, también se evidenciaron en esta investigación importantes variaciones con respecto a los años anteriores, dentro de las cuales también quisiéramos resaltar tres de ellas. El primer cambio se relaciona con la intensidad de uso de la Red. Los usuarios este año no sólo se conectan con más frecuencia y más horas a la Web, sino que se auto-califican como más conocedores de la misma, de acuerdo a las actividades realizadas, como subir archivos, escribir blogs, sindicar contenidos, entre otras.

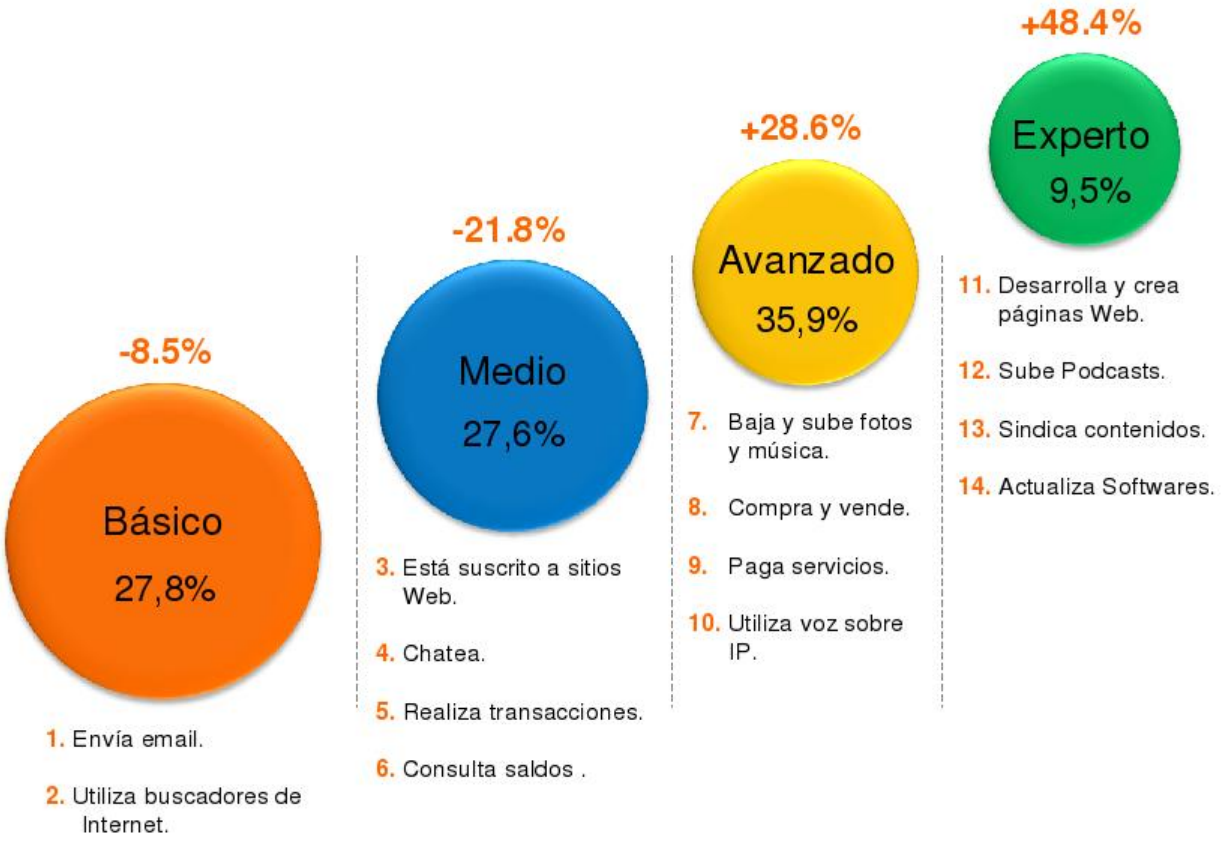


Figura 6.4: Tipos de usuarios de internet

Otro cambio relevante tiene que ver con la explosión de las redes sociales, las cuales experimentaron un crecimiento del 121 % y, específicamente de Facebook, cuyo aumento en la base de usuarios alcanzó un 800 %. Por último, cabe destacar un aumento en los usos transaccionales, no sólo de comercio electrónico sino de la banca y el gobierno electrónico.

Figura 6.5: Web 2.0

En el caso del comercio, el número de compradores se incrementó en un 67 % y rubros como los juegos de vídeos y teléfonos celulares presentaron un gran dinamismo.

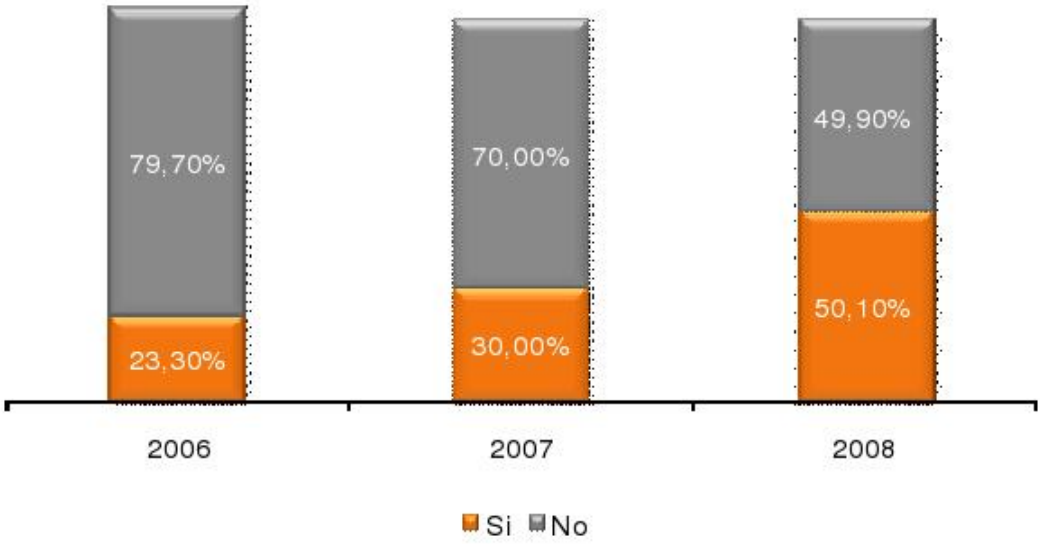


Figura 6.6: Actividades comerciales en internet

Las computadoras portátiles solían ser costosas y poco comunes, pero actualmente en Europa representan la mitad de las computadoras disponibles según estudios que revela la revista [IEEES]. Para oficinas, comercios, etc. se siguen prefiriendo computadoras de escritorio pero los consumidores ahora prefieren "notebook" principalmente porque los precios han bajado vertiginosamente. Para el 2012 se calcula que el 80 % de las computadoras que se vendan serán "notebook" como se puede observar si se sigue las tendencias de la Figura 6.7.

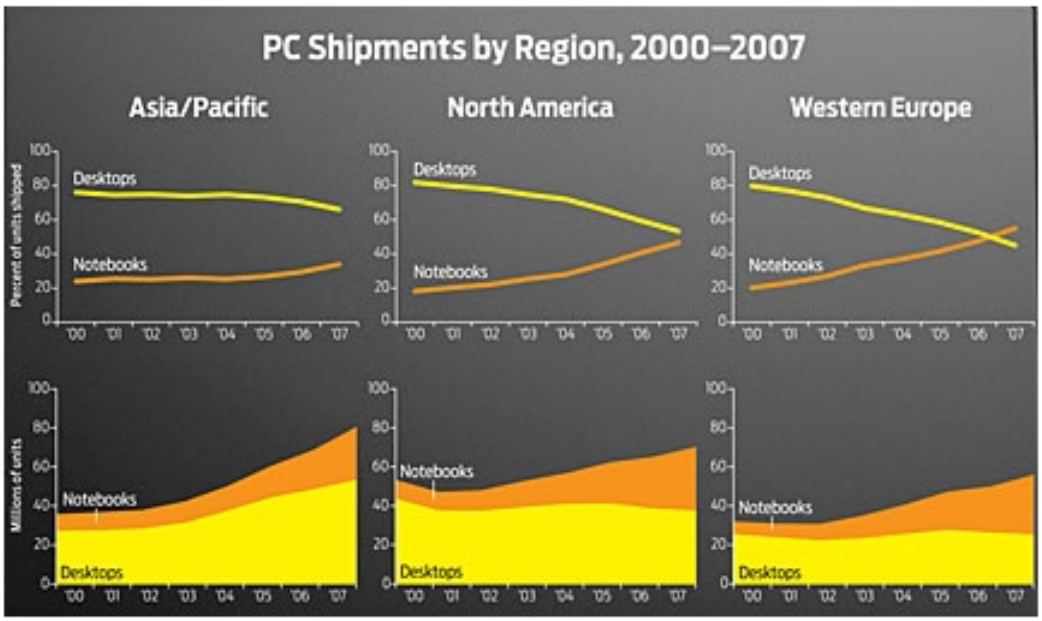


Figura 6.7: Aumento de la tendencia de la compra de notebook.

4. *Audiencias Digitales e imagen de Internet:*

   Internet se posiciona entre sus usuarios como un medio de comunicación ideal para conseguir mejor información de productos y conseguir ofertas, siendo además el medio más interactivo y global. Igualmente, al analizar el perfil de sus usuarios, se evidencia que en algunas categorías de productos y servicios Internet permite acceder a importantes audiencias, tales como los propietarios de vehículos, los cuenta habientes de un banco e incluso los consumidores de productos de consumo masivo como refrescos y caramelos, por mencionar algunos.

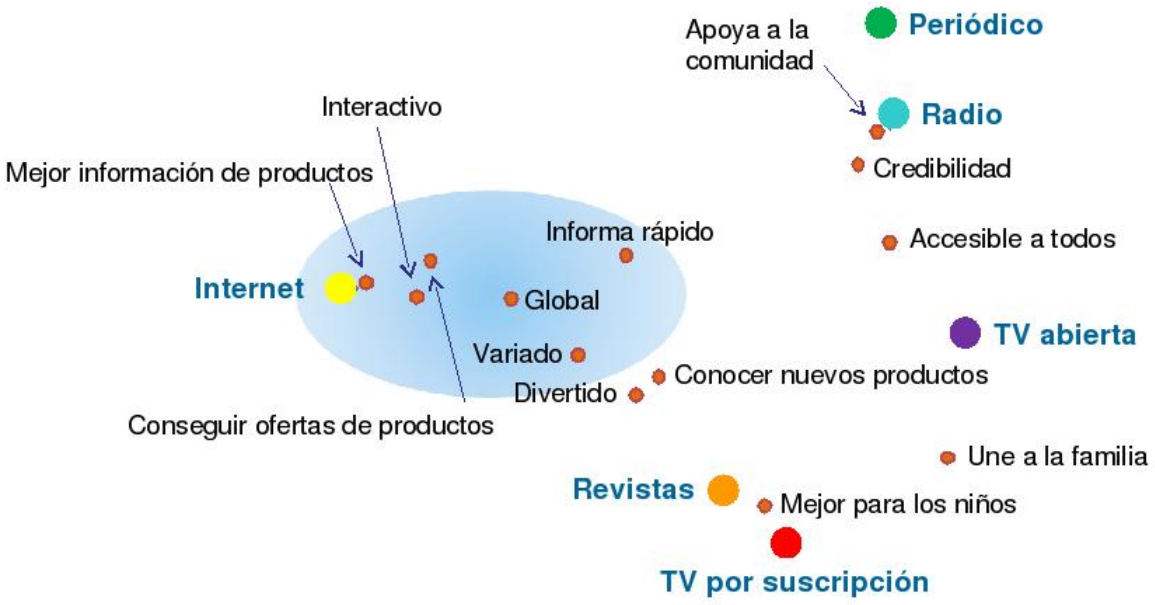


Figura 6.8: Posicionamiento frente a otros medios de comunicación

Consideraciones Finales:

- Internet se muestra como un espacio de elevado crecimiento que se convertirá en un fenómeno masivo de mercado. Esto motiva a que la red proyectada este diseñada acorde a tal demanda, permitiendo acceso rápido a la información con alta disponibilidad del servicio.
- Cada vez más, los accesos serán móviles y personales. Por lo que la red deberá estar preparada para que los usuarios accedan al servicio en forma flexible y segura mediante los distintos dispositivos.
- Internet es un espacio dinámico cuyos usuarios cada día son más intensivos en uso y conocedores del medio, requiriendo rapidez en el acceso a los contenidos.
- Los usuarios están generando gran parte de los contenidos, interactuando con las empresas y sobre todo entre ellos.
- Los usuarios cada vez están más propensos a realizar transacciones en línea. Se debe brindar privacidad e integridad de la información de los usuarios, confiabilidad y seguridad.

6.2. Casa de la calidad

En esta sección se relacionan los requerimientos del usuario con las características del diseño. Con este esquema se realiza al evaluación de la propuesta bajo la percepción del usuario, así como el análisis comparativo con respecto a los diferentes servicios, estableciendo además, una

vinculación entre los requerimientos del usuario y las características a cumplir, y su interdependencia con éstas.

Se utilizará como herramienta el modelo de despliegue de funciones de calidad o QDF [1], de Yoji Akao. El proceso QDF se basa en el uso de la llamada "casa de la calidad", un arreglo matricial realizado con el propósito de traducir los requerimientos del cliente en un conjunto apropiado de objetivos técnicos, a los cuáles se les asignan distintas prioridades, con el objeto de satisfacer las necesidades de diseño.

El formato general de la casa de la calidad se realiza a partir de seis componentes que son completados en el curso de un proceso de despliegue de funciones de calidad:

Requerimientos del usuario: Lista estructurada derivada del análisis de las necesidades o deseos de los usuarios.

Requerimientos técnicos: Conjunto estructurado de características tecnológicas medibles esenciales para el producto.

Ponderación del mercado: Determinación de los pesos de cada requisito, comparación con la situación actual y análisis de la situación.

Gráfico de la calidad: Matriz de interrelaciones entre los requisitos y las características técnicas.

Matriz de correlaciones: Permite reflejar si la mejora de una de las características afecta positiva o negativamente el resto de las características.

Evaluación técnica: Análisis técnico de la red propuesta y el de la red actual. Puede detectar contradicciones entre el comportamiento técnico de los productos y la percepción real de los usuarios, y así provocar la reorientación de los objetivos de las características de la red propuesta.

En la Figura 6.9 se muestra como se organizan estos seis componentes dentro de la casa de la calidad.

[1] Quality Function Deployment.

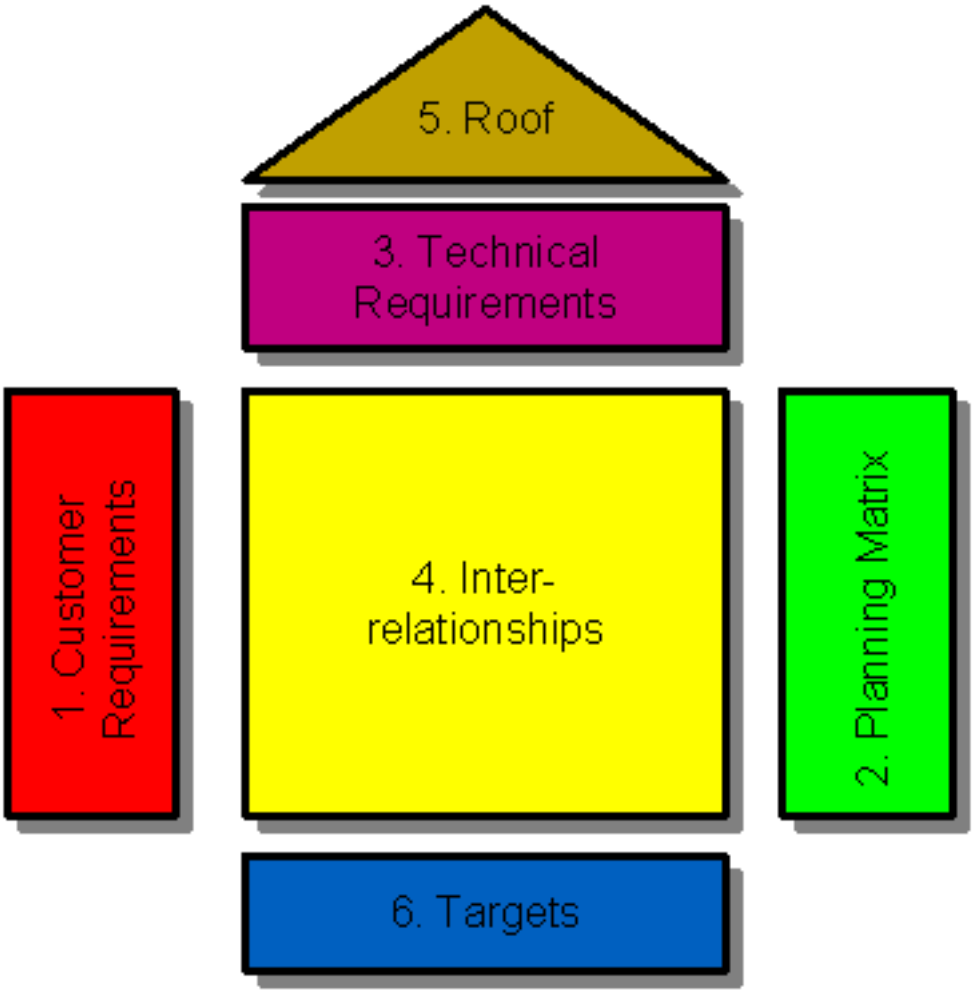


Figura 6.9: Esquema de la estructura de la casa de la calidad

6.2.1. Requerimientos

La ingeniería de requerimientos comprende todas las tareas relacionadas con la determinación de las necesidades o de las condiciones a satisfacer para el proyecto nuevo o modificado, tomando en cuenta los diversos requerimientos de los inversores, que pueden entrar en conflicto entre ellos.

El propósito de la ingeniería de requerimientos es hacer que los mismos alcancen un estado óptimo antes de seguir adelante con el proyecto. Los buenos requerimientos deben ser medibles, comprobables, sin ambigüedades o contradicciones.

Requerimientos de usuarios

Los requerimientos de los usuarios que se indican en el Cuadro 6.10, se toman como objetivos generales y se los debe analizar una y otra vez desde el punto de vista del sistema hasta determinar los objetivos críticos del funcionamiento interno que luego darán forma a los comportamientos apreciables por el usuario. La primera condición que se debe tener en cuenta es la valoración que hacen los usuarios con respecto a los requerimientos establecidos. Para esto,

se solicita que se le otorgue una valoración de 1 a 5 siendo 5, “muy importante” y 1, “sin importancia”.

Dirección de la Mejora	Peso relativo de los RQ del proyecto
Red FIUBA	
Requerimientos del Cliente	
Disponibilidad apropiada de los servicios	4
Rapidez en los servicios.	5
Flexibilidad en la conexión de computadoras ajenas a la FIUBA	3
Servicios confiables	2
Un buen servicio de inscripción	3
Cantidad apropiada de terminales	4
Privacidad e integridad de la información	3
Convergencia de servicios	5
Inteligibilidad en los llamados	4
Costo	4
Estética Edilicia	3

Figura 6.10: Requerimientos de usuarios

Requerimientos de Técnicos

Las características técnicas más representativas del sistema que conforman los requerimientos técnicos del mismo se indican en el Cuadro 6.11. Para cada uno de ellos se la dirección la tendencia de mejora que puede ser en aumento (↑) o en disminución (↓).

Requerimientos Técnicos														
▲	▲	▲	▲	▲	▲	▲	▲	▼	▼	▼	▲	▲	▲	▲
Ancho de banda LAN por piso	Ancho de banda del "backbone"	Ancho de banda WAN	Cumplimiento de normas de CE	Redundancia en enlaces y equipos.	Administracion centralizada	Clasificacion de Trafico	Priorizacion de paquetes	Delay	Delay Jitter	Packet Loss	Escalabilidad	Seguridad Fisica	Mantenibilidad	POE

Figura 6.11: Requerimientos Técnicos

6.2.2. Matriz de Planeamiento

Se asigna valores dentro de la escala de 1 a 5 siendo 1 el producto que no satisfaga de ninguna manera el requerimiento preestablecido y 5 el producto que tenga un desempeño muy satisfactorio en esa área. En este caso los productos son la red actual y la red proyectada como puede observarse en la Figura 6.12.

Una vez establecidas estas valoraciones que generan los usuarios consultados, se establecen distintas valoraciones desde el punto de vista del diseñador. Generalmente se utilizan las siguientes características:

Metas Planeadas: Cuantifica la capacidad del desarrollo en satisfacer los distintos requerimientos establecidos.

Mejora: A partir de las Metas Planeadas y las valoraciones otorgadas en relación a la red proyectada y la red actual, se puede determinar el factor de mejora como indica la siguiente ecuación:

$$Mejora = 1 + (Metas\ Planeada - V_i) \cdot 0{,}2$$

Donde V_i es la valoración dada por los usuarios y 0,2 (20 %) es el factor de mejora.

Puntos de Ventas: Se refieren a otorgar una valoración a los requerimientos que podrían ser utilizados para promover el producto. En este caso también se realiza una valoración pero otorgando a cada característica un valor entre 1 y 1,5. Como este caso no es un producto comercial, se le asigna a cada requerimiento el el valor uno.

Finalmente se genera una valoración general indicando el peso total del producto de la siguiente manera:

$$Peso\ Total = Peso\ relativo\ de\ los\ RQ\ del\ cliente \cdot Mejora \cdot Puntos\ de\ Ventas$$

A continuación se observan los valores tabulados para cada caso:

Red FIUBA	Peso relativo de los RQ del proyecto	Estado actual de la Red	Estado proyectado de la Red	Metas Planeadas	Mejora	Punto de venta	Peso Total	Peso Total %
Requerimientos del Cliente								
Disponibilidad apropiada de los servicios	4	3	4	4	1,0	1	4,0	9%
Rapidez en los servicios.	5	4	4	5	1,0	1	5,0	11%
Flexibilidad en la conexión de computadoras ajenas a la FIUBA	3	3	3	3	1,0	1	3,0	7%
Servicios confiables	2	2	5	4	1,4	1	2,8	6%
Un buen servicio de inscripción	3	3	2	4	1,2	1	3,6	8%
Cantidad apropiada de terminales	4	2	4	4	1,0	1	4,0	9%
Privacidad e integridad de la información	3	1	2	4	1,2	1	3,6	8%
Convergencia de servicios	5	1	5	5	1,0	1	5,0	11%
Inteligibilidad en los llamados	4	1	4	5	1,2	1	4,8	11%
Costo	4	1	4	5	1,2	1	4,8	11%
Estética Edilicia	3	3	3	4	1,2	1	3,6	8%
					Total 100%		**44,2**	**100%**

Figura 6.12: Matriz de planeamiento

6.2.3. Techo

Esta sección intenta relacionar los distintos requerimientos técnicos para determinar si se suplementan o se anulan entre si. La idea es establecer si la posibilidad de mejorar un requerimiento genera que otro sea deteriorado o crezca conjuntamente con el otro. Para representar esto se ubica un signo menos (−) cuando el desarrollo de un requerimiento deteriora el otro y un signo mas (+) cuando el efecto de relación es una mejora por ambos lados.

Este análisis es muy importante para el desarrollo del producto puesto que permite observar en que puntos se debe enfocar las mejoras y en que puntos se deben estudiar otras soluciones para no generar problemas en los demás puntos del diseño.

En la Figura 6.13 se muestra la matriz de correlaciones correspondiente a los requerimientos técnicos definidos para el sistema propuesto.

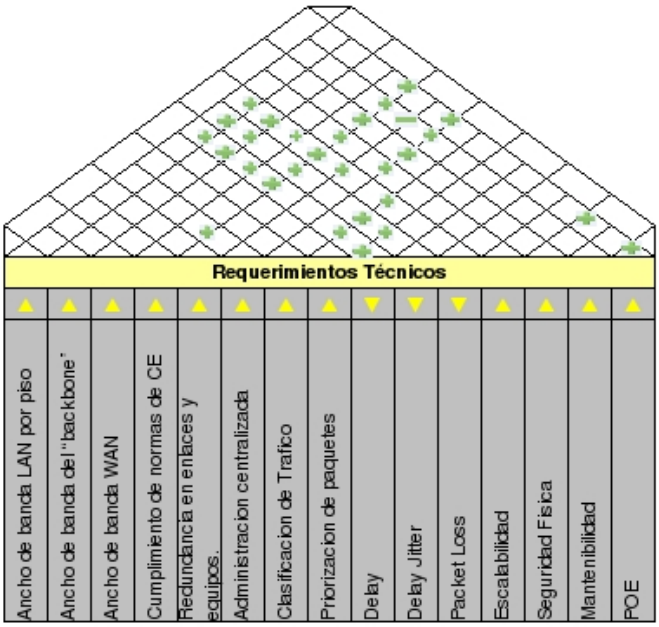


Figura 6.13: Techo de la casa de la calidad

6.2.4. Matriz de interrelaciones

Para calcular la matriz de interrelaciones entre los requerimientos del usuario y los requerimientos técnicos se procedió en primer lugar a considerar las correlaciones entre ambos conjuntos de requerimientos. La adopción tomada fue asignar el valor nueve (9) a las correlaciones fuertes, tres (3) a las medias, uno (1) a las débiles y cero (0) a las correlaciones nulas.

Red FIUBA	Ancho de banda LAN por piso	Ancho de banda del "backbone"	Ancho de banda WAN	Cumplimiento de normas de CE	Redundancia en enlaces y equipos.	Administracion centralizada	Clasificacion de Trafico	Priorizacion de paquetes	Delay	Delay Jitter	Packet Loss	Escalabilidad	Seguridad Fisica	Mantenibilidad	POE
Requerimientos del Cliente															
Disponibilidad apropiada de los servicios	3	3	3	9	3	3	3	1	3	3	9	0	9	9	3
Rapidez en los servicios.	9	9	9	1	0	0	3	3	9	1	1	0	0	0	0
Flexibilidad en la conexión de computadoras ajenas a la FIUBA	0	0	0	0	0	0	3	0	0	0	0	3	1	0	0
Servicios confiables	0	0	0	9	3	9	1	1	1	1	1	1	3	3	3
Un buen servicio de inscripción	1	3	9	1	1	0	0	0	0	0	0	0	1	0	1
Cantidad apropiada de terminales	9	9	9	3	0	0	0	1	3	3	3	9	1	1	1
Privacidad e integridad de la información	0	0	0	1	0	1	9	3	0	0	0	0	9	0	0
Convergencia de servicios	9	9	3	0	0	1	9	3	3	3	1	1	0	3	1
Inteligibilidad en los llamados	1	1	1	0	0	0	9	9	9	9	1	1	0	1	0
Costo	9	9	9	9	9	3	1	1	1	1	1	3	1	9	9
Estética Edilicia	0	0	0	9	1	3	0	0	0	0	0	3	9	3	9

Figura 6.14: Matriz de Interrelaciones

6.2.5. Metas

Esta es la última etapa de la matriz de la casa de calidad, en la cual, se establecen tres parámetros que se describen a continuación:

Prioridades técnicas: Determina la importancia relativa de los requerimientos técnicos en función de los requerimientos propuesto por el usuario. Estos se calculan a partir de la suma de los subtotales que resultan de realizar el producto entre los valores asignados en la matriz de interrelaciones y la ponderación dada al requerimiento del usuario como se expresa en la Ecuación 6.1.

$$Prioridad\ Tecnica = \sum Valor\ de\ Correlacion \cdot Peso\ Total \tag{6.1}$$

Rendimiento: Comparación del rendimiento de cada una de las características técnicas registrada por la red actual y la red propuesta.

Metas de diseño: Es el resultado de todos los elementos de la matriz y representa las características que debe cumplir el nuevo producto diseñado a partir de este análisis de calidad.

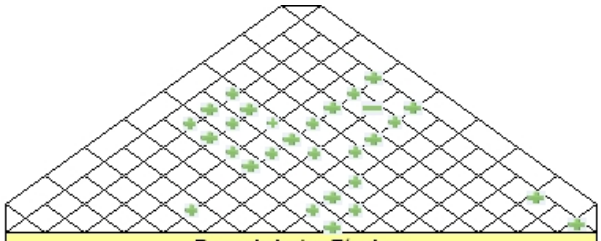
Estos parámetros se pueden observar en el Cuadro que se indica en la Figura 6.15.

Dirección de la Mejora	▲	▲	▲	▲	▲	▲	▲	▲	▼	▼	▼	▲	▲	▲	▲	
Red FIUBA / Requerimientos del Cliente	Ancho de banda LAN por piso	Ancho de banda del "backbone"	Ancho de banda WAN	Cumplimiento de normas de CE	Redundancia en enlaces y equipos.	Administracion centralizada	Clasificacion de Trafico	Priorizacion de paquetes	Delay	Delay Jitter	Packet Loss	Escalabilidad	Seguridad Fisica	Mantenibilidad	POE	
Prioridades Técnicas	190	197	188	161	71	71	164	100	135	95	70	83	125	122	109	1880
Porcentaje	10%	10%	10%	9%	4%	4%	9%	5%	7%	5%	4%	4%	7%	7%	6%	100%
Red Actual (Datos)	Fast Eth.	2 GE	12 Mbps	No	No	Si	No	No	5ms	0,15ms	~0%	No	No	Si	No	Total 100%
Red Proyectada (Datos, voz y seguridad)	Giga Eth.	2 GE	14 Mbps	Si	No	Si	Si	Si	<50ms	<10ms	<0.1%	Si	Si	Si	Si	
Metas	Giga Eth.	2 GE	12 Mbps	Si	No	Si	Si	Si	<50ms	<10ms	<0.1%	Si	Si	Si	Si	

Figura 6.15: Metas de Diseño

6.2.6. Esquema de la casa de calidad

Finalmente a continuación se indica la "Casa de la Calidad" completa:



Requerimientos Técnicos

Dirección de la Mejora	▲	▲	▲	▲	▲	▲	▲	▲	▼	▼	▼	▲	▲	▲	▲								
Red FIUBA / **Requerimientos del Cliente**	Ancho de banda LAN por piso	Ancho de banda del "backbone"	Ancho de banda WAN	Cumplimiento de normas de CE	Redundancia en enlaces y equipos.	Administracion centralizada	Clasificacion de Trafico	Priorizacion de paquetes	Delay	Delay Jitter	Packet Loss	Escalabilidad	Seguridad Fisica	Mantenibilidad	POE	Peso relativo de los RQ del proyecto	Estado actual de la Red	Estado proyectado de la Red	Metas Planeadas	Mejora	Punto de venta	Peso Total	Peso Total %
Disponibilidad apropiada de los servicios	3	3	3	9	3	3	3	1	3	3	9	0	9	9	3	4	3	4	4	1,0	1	4,0	9%
Rapidez en los servicios.	9	9	9	1	0	0	3	3	9	1	1	0	0	0	0	5	4	4	5	1,0	1	5,0	11%
Flexibilidad en la conexión de computadoras ajenas a la FIUBA	0	0	0	0	0	0	3	0	0	0	0	3	1	0	0	3	3	3	3	1,0	1	3,0	7%
Servicios confiables	0	0	0	9	3	9	1	1	1	1	1	1	3	3	3	2	2	5	4	1,4	1	2,8	6%
Un buen servicio de inscripción	1	3	9	1	1	0	0	0	0	0	0	0	1	0	1	3	3	2	4	1,2	1	3,6	8%
Cantidad apropiada de terminales	9	9	9	3	0	0	0	1	3	3	3	9	1	1	1	4	2	4	4	1,0	1	4,0	9%
Privacidad e integridad de la información	0	0	0	1	0	1	9	3	0	0	0	0	9	0	0	3	1	2	4	1,2	1	3,6	8%
Convergencia de servicios	9	9	3	0	0	1	9	3	3	3	1	1	0	3	1	5	1	5	5	1,0	1	5,0	11%
Inteligibilidad en los llamados	1	1	1	0	0	0	9	9	9	9	1	1	0	1	0	4	1	4	5	1,2	1	4,8	11%
Costo	9	9	9	9	9	3	1	1	1	1	1	3	1	9	9	4	1	4	5	1,2	1	4,8	11%
Estética Edilicia	0	0	0	9	1	3	0	0	0	0	0	3	9	3	9	3	3	3	4	1,2	1	3,6	8%
Prioridades Técnicas	190	197	188	161	71	71	164	100	135	95	70	83	125	122	109	1880				**Total 100%**		**44,2**	**100%**
Porcentaje	10%	10%	10%	9%	4%	4%	9%	5%	7%	5%	4%	4%	7%	7%	6%	**100%**							
Red Actual (Datos)	Fast Eth.	2 GE	12 Mbps	No	No	Si	No	No	5ms	0,15ms	~0%	No	No	Si	No	**Total 100%**							
Red Proyectada (Datos, voz y seguridad)	Giga Eth.	2 GE	14 Mbps	Si	No	Si	Si	Si	<50ms	<10ms	<0.1%	Si	Si	Si	Si								
Metas	Giga Eth.	2 GE	12 Mbps	Si	No	Si	Si	Si	<50ms	<10ms	<0.1%	Si	Si	Si	Si								

Peso Total = Peso Relativo de los requerimientos x Mejora x Punto de Venta

Peso total Prioridades Técnicas = Pesos individuales x
Puntuación Mapeo de requerimientos de las especificaciones

Peso Total % = Peso Total / Suma Pesos Totales

Puntuaciones del mapeo de los requerimientos del cliente	
0	Inter-relación nula
1	Baja inter-relación
3	Media inter-relación
9	Alta inter-relación

Mejoras = 1 + (Metas planeadas - Peso relativo de los RQ del proyecto) x 0.2

Figura 6.16: QDF

6.2.7. Conclusiones

Luego de la realización de la casa de calidad se concluye que uno de los puntos más importantes a tener en cuenta para el desarrollo del sistema desde el punto de vista técnico, es el ancho de banda por piso, el ancho de banda del backbone y el ancho de banda de la WAN. También son importantes el cumplimiento de las normas de cableado estructurado y la clasificación del tráfico, que implica la calidad de servicio.

Si bien el delay, jitter y packet loss son de gran importancia en la transmisión de datos en tiempo real, no son de requerimientos críticos debido a que la distancias de la red de la facultad son considerablemente pequeñas a diferencia de redes metro.

Se buscará cumplir con las normas de cableado estructurado y brindar seguridad física de forma tal de brindar un servicio confiable que brinde la seguridad e integridad de la información.

Entre los requerimientos del cliente, los más importantes fueron el costo, inteligibilidad del llamado, convergencia de servicios (que el sistema se plantee como uno solo y no como varios subsistemas que resuelven una parte del problema) y la rapidez en los servicios (relacionado con el ancho de banda)

6.3. Especificaciones Técnicas

En esta sección se desarrolla la especificación técnica completa considerando que la misma será utilizada para la implementación, contemplando todas aquellas normas nacionales o internacionales así como las recomendaciones de los organismos de aplicación y legislación vigente.

Ancho de banda LAN por piso: $1GE$.

Ancho de banda del "backbone": $2GE$.

Ancho de banda WAN: $12Mbps$.

Acceso de los usuarios a la red: Inalámbrico con cobertura en las áreas necesarias.

Normas de cableado estructurado: SI.

Redundancia en enlaces y equipos: NO.

Administración centralizada: SI.

Clasificación de Tráfico: SI.

Priorización de paquetes: SI.

Delay: $< 50ms$.

Delay Jitter: $< 10ms$.

Packet Loss: $< 0{,}1\,\%$.

Equipamiento: Se tendrá en cuenta el equipamiento homologado por la CNC[2], las normas mencionadas oportunamente, cumplimiento de las metas de capacidad, cobertura, prestaciones del fabricante, calidad y el costo del mercado.

Alimentación Centralizada e independiente con sistema eléctrico de emergencia (UPS[3]).

Normas: A continuación se indican estándares tenidos en cuenta:

IEEE 802.3: Ethernet, Fast Etheret y Gigabit Ethernet a través de coaxial, par trenzado y fibra óptica.

IEEE 802.16: Acceso inalámbrico a través de WiMax.

IEEE 802.11: Acceso inalámbrico a través de WiFi.

EIA/TIA 568-A: Estándar de cableado para edificios comerciales de telecomunicaciones.

ISO/IEC DIS 11801: Estándar de cableado para edificios comerciales de telecomunicaciones.

EIA/TIA 568B: Actualización de la ANSI/TIA/EIA568A.

EIA/TIA 569A: Estándar sobre espacios y canalizaciones de telecomunicaciones para edificios comerciales.

EIA/TIA 606: Estándar sobre administración para la infraestructura de telecomunicaciones de edificios comerciales.

EIA/TIA 607: Requerimientos de aterramiento y anclaje en edificios comerciales para la industria de Telecomunicaciones.

EIA/TIA/TSB95: Pautas de rendimiento de transmisión adicionales para cableado 4-pares 100Ω Categoría 5.

[2]Centro Nacional de Comunicaciones.
[3]Uninterruptible Power Supply.

ISO/IEC 11801:1995 FDAM 2: Tecnología de información - Cableado Genérico para el Predio del Cliente Enmienda 2.

IRAM-ISO/IEC 17799: Código de práctica para la gestión de la seguridad de la información.

IEEE 802.3af: Alimentación a través del tendido eléctrico por par trenzado (PoE[4]).

[4]Power over Ethernet.

Capítulo 7

Análisis de factibilidad

En general los análisis de factibilidad más profundos, o los estudios de factibilidad, se completan durante la fase de diseño de sistemas, durante la consideración de la evaluación de las diferentes alternativas de solución propuestas. Los estudios de factibilidad consideran la factibilidad técnica, económica y operacional de cada alternativa, así como si el proyecto es o no apropiado dados los factores políticos y otros del contexto institucional.

7.1. Factibilidad operacional

Esta factibilidad comprende una determinación de la probabilidad de que el nuevo sistema se use como se supone. Deberían considerarse por lo menos cuatro aspectos de la factibilidad operacional.

- Un nuevo sistema puede ser demasiado complejo para los usuarios de la organización o los operadores del sistema. Si lo es, los usuarios pueden ignorar el sistema o bien usarlo en tal forma que cause errores o fallas en el sistema.

- Un sistema puede hacer que los usuarios se resistan a él como consecuencia de una técnica de trabajo, miedo a ser desplazados, intereses en el sistema antiguo u otras razones. Para cada alternativa debe explorarse con cuidado la posibilidad de resistirse al cambio al nuevo sistema.

- Un nuevo sistema puede introducir cambios demasiado rápido para permitir al personal adaptarse a él y aceptarlo. Un cambio repentino que se ha anunciado, explicado y "vendido" a los usuarios con anterioridad puede crear resistencia. Sin importar qué tan atractivo pueda ser un sistema en su aspecto económico si la factibilidad operacional indica que tal vez los usuarios no aceptarán el sistema o que su uso resultará en muchos errores o en una baja en la moral, el sistema no debería implantarse.

- La probabilidad de la obsolescencia subsecuente en el sistema. La tecnología que ha sido anunciada pero que aún no está disponible puede ser preferible a la tecnología que se encuentra en una o más de las alternativas que se están comparando, o cambios anticipados en las prácticas o políticas administrativas pueden hacerse que un nuevo sistema sea obsoleto muy pronto.

En cualquier caso, la implantación de la alternativa en consideración se convierte en impráctica. Un resultado frecuente de hallazgos negativos acerca de la factibilidad operacional de un sistema es que éste no se elimina, sino que se simplifica para mejorar su uso. Otras posibilidades son que los programas de relaciones públicas o de entrenamiento estén diseñados para enfocarse a sobreponerse a la resistencia a un nuevo sistema, o se desarrollan formas para hacer fases en el nuevo sistema en un largo periodo para que el cambio total, que traumatizaría a los usuarios u operadores, se convierta en una serie de pequeños cambios.

7.2. Factibilidad tecnológica

El análisis de factibilidad técnica evalúa si el equipo y software están disponibles (o en el caso del software, si puede desarrollarse) y si tienen las capacidades técnicas requeridas por cada alternativa del diseño que se esté considerando. Los estudios de factibilidad técnica también consideran las interfases entre los sistemas actuales y nuevo. Por ejemplo, los componentes que tienen diferentes especificaciones de circuito no pueden interconectarse, y los programas de software no pueden pasar datos a otros programas si tienen diferentes formatos en los datos o sistemas de codificación; tales componentes y programas no son compatibles técnicamente. Sin embargo, puede hacerse una interfase entre los sistemas no compatibles mediante la emulación, la cual son circuitos diseñados para hacer que los componentes sean compatibles, o por medio de la simulación, que es un programa de cómputo que establece compatibilidad, pero con frecuencia estas formas de factibilidad técnica no están disponibles o son demasiado costosas. Los estudios de factibilidad técnica también consideran si la organización tiene el personal que posee la experiencia técnica requerida para diseñar, implementar, operar y mantener el sistema propuesto. Si el personal no tiene esta experiencia, puede entrenárse o pueden emplearse nuevos o consultores que la tengan. Sin embargo, una falta de experiencia técnica dentro de la organización puede llevar al rechazo de una alternativa particular. Para profundizar más estos temas, ver [SA&D].

7.2.1. Propuesta de alternativas de diseño

La arquitectura de transporte de una red de telecomunicaciones debe poseer dos capas o estratos diferenciados: el core y el acceso.

Acceso: Permite transmitir los contenidos del core al usuario y viceversa

Core: Concentra y agrega el tráfico proveniente de los accesos.

Las redes de acceso y de “core” pueden emplear tres medios físicos de transmisión:

- Cobre (Par de cobre, coaxial, UTP).
- Inalámbrico (Wi-Fi, WiMax).
- Óptico (Fibra óptica).

Como se describió en el Capitulo 4, la red actualmente presenta acceso y core a través de cobre.

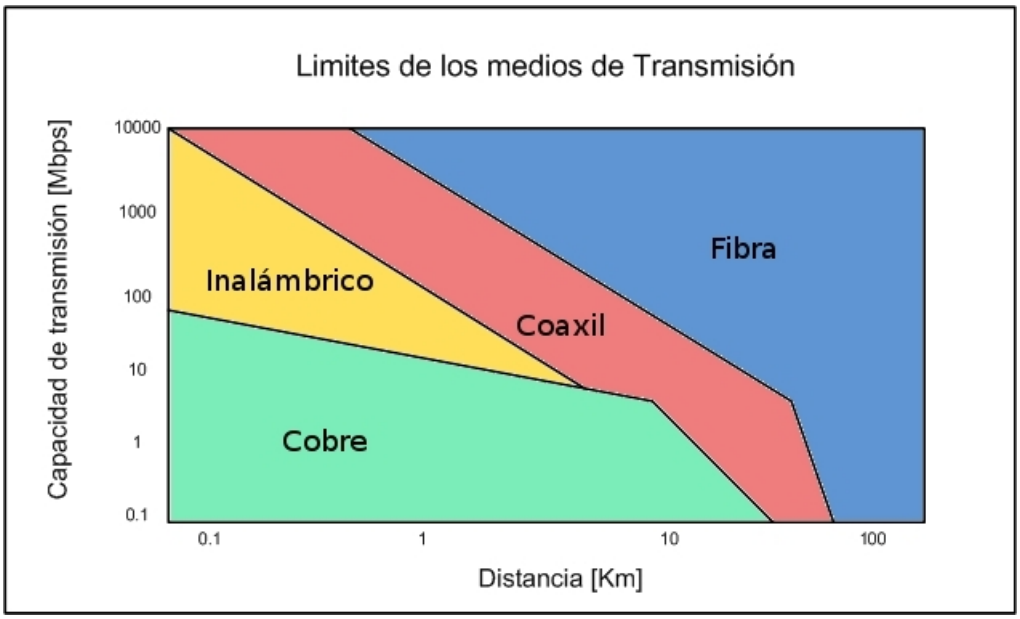


Figura 7.1: Límite de los medios de transmisión

Fibra Óptica Vs. Cable Cobre

Ventajas de la fibra óptica:

- Diámetro y peso reducidos lo que facilita su instalación
- Excelente flexibilidad
- Inmunidad a los ruidos eléctricos (interferencias)
- No existe diafonía (no hay inducción entre una fibra y otra)
- Bajas pérdidas, lo cual permite reducir la cantidad de estaciones repetidoras.

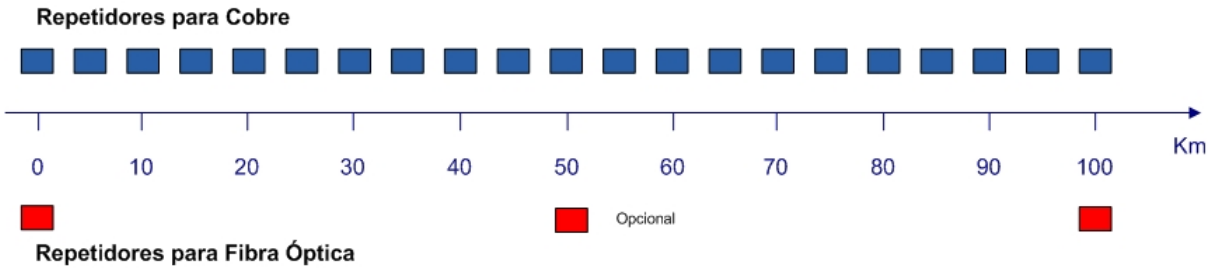


Figura 7.2: Repetidores

- Gran ancho de banda que implica una elevada capacidad de transmisión

- Estabilidad frente a variaciones de temperatura
- Al no conducir electricidad no existe riesgo de incendios por arcos eléctricos
- No puede captarse información desde el exterior de la fibra
- El Dióxido de Silicio, materia prima para la fabricación de F.O., es uno de los recursos más abundantes del planeta.

Desventajas de la fibra óptica:

- Son más caras ya que para obtener, desde la arena de cuarzo, el dióxido de silicio purificado es necesaria mayor cantidad de energía que para los cables metálicos.
- Las F.O. son muy delicadas lo cual requiere un tratamiento especial durante el tendido de cables.
- Se necesitan equipos de alta precisión para realizar mediciones, empalmes y conexiones.
- Incomodo para trabajar en la vía pública o en exteriores.
- Tiempo de vida de los dispositivos emisores de luz no muy prolongados.

Medio inalámbrico Vs. medio cableado

Los medios inalámbricos poseen una serie de ventajas, entre las cuales podemos destacar:

- Al ser redes inalámbricas, la comodidad que ofrecen es muy superior a las redes cableadas porque cualquiera que tenga acceso a la red puede conectarse desde distintos puntos dentro de un rango suficientemente amplio de espacio.
- Una vez configuradas, permiten el acceso de múltiples computadoras sin ningún problema ni gasto en infraestructura, no así en la tecnología por cable.

Los problemas intrínsecos de cualquier tecnología inalámbrica son:

- Menor velocidad en comparación a una conexión con cables, debido a las interferencias y pérdidas de señal que el ambiente pueda acarrear.
- Para varios métodos de acceso inalámbrico es necesario tener LOS[1].
- La desventaja fundamental de este medio reside en los requerimientos de la seguridad del mismo. Existen algunos programas capaces de capturar paquetes, de forma que puedan acceder a la red. Por ejemplo en Wi-Fi, las claves de tipo WEP[2] son relativamente fáciles de conseguir. El estándar Wi-Fi arregló estos problemas sacando el estándar WPA[3] y posteriormente WPA2, basados en el grupo de trabajo 802.11*i*. Las redes protegidas con WPA2 se consideran robustas dado que proporcionan muy buena seguridad.

[1] Line of Sight
[2] Wired Equivalent Privacy
[3] Wi-Fi Protected Access

- Hay que señalar que esta tecnología no es compatible con otros tipos de conexiones sin cables tales como Bluetooth, GPRS[4], UMTS[5], etc.
- Otra desventaja es la contaminación radioeléctrica que producen las redes inalámbricas pudiendo interferir otros sistemas sensibles a la misma. Por tal motivo, para el caso particular de la facultad, se estudiará en el Capítulo 9 posibles soluciones de blindaje para los sectores que deben estar aislados de interferencias.

7.2.2. Elección de una solución

Habiendo analizado las ventajes y desventajas de tecnologías cableadas frente a tecnologías inalámbricas, hemos optado por utilizar la **tecnología inalámbrica para el acceso**. Ya que aparte de sus ventajas intrínsecas podemos también destacar las siguientes:

- Mayor escalabilidad de usuarios, debido que para agregar un nuevo usuario no se requiere un nuevo cableado.
- Para aumentar la cobertura de la red no es necesario tender mas cableado, sino distribuir correctamente los AP[6].
- Favorece a la estética edilicia debido a que se reduce el tendido de cableado.
- Flexibilidad en la conexión de computadoras ajenas a la FIUBA
- Permite la convergencia de servicios que satisfagan las mismas normas inalámbricas (cámaras y teléfonos inalámbricos).
- Esta solución permitirá la utilización de equipamiento donado que se encuentran a disposición del proyecto.
- Como mencionamos en el la Sección 6.1, los accesos serán móviles y personales. Por lo que la red deberá estar preparada para que los usuarios accedan al servicio en forma flexible y segura mediante los distintos dispositivos.
- Las normas de acceso inalámbrico son capaces de cumplir las especificaciones técnicas establecidas en la Sección 6.3.

Sistemas Wi-Fi versus WiMax

Ambos estándares inalámbricos, Wi-Fi[7] y WiMax[8], pueden adecuarse a las características mencionadas en el proyecto. Sin embargo, WiMax es una técnica de acceso de banda ancha diseñada para ofrecer servicios de última milla en áreas metropolitanas[9], con una cobertura aproximada de $50Km$ desde la estación base.

[4]General Packet Radio Service
[5]Universal Mobile Telecommunications System
[6]Acces Point
[7]IEEE 802.11
[8]IEEE 802.16
[9]MAN

Desde el punto de vista económico, David Jarvis (conocido emprendedor del sector telco de Sudáfrica, destacó en la conferencia WiWorld de 2007), que actualmente no hay una alternativa clara al estándar 802.11, apuntando directamente a WiMax. Jarvis afirma que, económicamente hablando, no hay comparativa entre un punto de acceso Wi-Fi y uno WiMax. El costo para Wi-Fi está un orden de magnitud abajo con respecto a WiMax.

WiMax no está incorporada en los dispositivos de consumo, y no lo estará probablemente por mucho tiempo. En cambio Wi-Fi se está expandiendo rápidamente a más dispositivos móviles, los nuevos iPods, tags de localización y en breve será posible verlos en vehículos para comunicaciones V2V[10].

WiMax está controlado por las grandes empresas de electrónica como Motorola, Intel y Alvarion. Históricamente los grandes operadores siempre han tratado de desplegar tecnologías de acceso basadas en estándares abiertos para evitar la concentración de poder de los proveedores. Lo cual pone en duda el futuro a largo plazo de WiMax.

Por todas estas razones, **se utiliza Wi-Fi para el acceso**, descartando la opción WiMax. En la Sección 8.1 se describirá en profundidad el funcionamiento de Wi-Fi.

Elección para el Core

Con respecto al core, hemos analizado las ventajes y desventajas de la tecnología cableadas frente a tecnología de fibra óptica. Hemos optado en este caso por una **red de core cableada**. Destacaremos en la siguiente sección las ventajas y desventajas de ésta decisión.

- Es una decisión económicamente más viable, ya que permite la reutilización de los equipos y de los cables que se usan actualmente en el core, ya que estos tienen interfaces gigabit Ethernet.
- Utilizando LACP se puede extender el ancho de banda del enlace entre ambos switches de core, estos son protocolos que ambos switches soportan y están siendo utilizados actualmente.
- Como ya se explicó en la Sección 4.4, la distancia está bien cubierta por la tecnología actualmente empleada.
- Como contrapartida, nos encontraríamos al límite de los equipos actuales, en caso de querer mejorarse habría que analizar enlaces $10Gbps$ Ethernet ya sean por fibra óptica o por cobre con cables Cat6A o mejores.

Conclusiones sobre las tecnologías propuestas

Al ser estos, equipos y tecnologías que están actualmente disponibles, las capacidades técnicas requeridas por parte del personal, y por parte de los usuarios están cubiertas, (factibilidad, resistencia al cambio, etc). Agregar tendido de fibra óptica hubiera representado un aumento en la complejidad y en la diversidad de tecnologías de la red de la facultad que no vimos totalmente indispensable. Con respecto a la tecnología Wi-Fi 802.11n, si bien reconocemos sus capacidades (de las que hablaremos en la Sección 8.1.8), consideramos que todavía no está lo suficientemente definida debido a que el estándar se encuentra en etapa "Draft", ni existe disponibilidad

[10] Vehicle to vehicle

requerida de equipos para abordar un proyecto de esta magnitud y diversidad con ella. Por esa razón, **se utiliza Wi-Fi 802.11*g***, que tiene una gran diversidad de equipos y se encuentra totalmente definida actualmente. Con respecto al impacto que pudiera ocasionar el hecho de no poseer la experiencia técnica requerida para administrar y configurar la red Wi-Fi por el equipo de soporte informático de forma de atentar contra la factibilidad del diseño, recordamos que Wi-Fi ya se utiliza actualmente en la facultad. Ver Sección 4.2.4, correspondiente al relevamiento. Por lo que consideramos al proyecto factible, desde el punto de vista operacional y tecnológico.

7.3. Factibilidad de tiempos

En esta etapa del análisis se deben plantear los requisitos y lineamientos que conducen al desarrollo de su solución de forma ordenada. Esto da lugar a un proyecto que permite satisfacer la necesidad en el menor tiempo posible. Para esto es necesario también un plan que permita evaluar, desarrollar, y controlar el proyecto en sus distintas etapas. De acuerdo a este plan se conforma un programa de trabajo que establece la puesta en marcha del proyecto de acuerdo a un calendario, definiendo los recursos necesarios y los responsables de las tareas a realizar.

Para llevar a cabo estas instancias, se cuenta con el apoyo de distintas herramientas:

PERT (Program Evaluation and Review Technique): Muestra la dependencia entre tareas a partir de un grafo y maneja tiempos aleatorios para luego estimar la duración del proyecto.

Método de simulación de Montecarlo y propagación de errores: También estiman la duración del proyecto e identifican el camino crítico.

Diagrama de Gantt: Grafica una serie de tareas representadas por barras vinculadas entre sí, y que presentan una duración en horas diarias de trabajo. Este diagrama tiene en cuenta el calendario y los días hábiles de trabajo, para poder estimar el inicio y la finalización del proyecto.

La planificación propuesta en este proyecto, tiene en cuenta la posibilidad de reutilización de materiales e insumos que ya estén utilizándose en la red actual y el hecho de que mientras dure el proyecto no se puede dejar sin conectividad al personal y alumnos de la facultad.

7.3.1. Determinación de tareas

En esta sección propondremos el listado de las tareas a realizarse con una descripción breve de las mismas.

1. **Acuerdo entre las partes interesadas en el proyecto:** Debido a que este es un proyecto que se planteó como interdisciplinario entre varios equipos, en los que unos se ocuparían de la parte de seguridad con cámaras IP, otros de la parte de Telefonía IP y finalmente nosotros en la red en general, es necesario un tiempo para acordar los requerimientos que se necesitaran para la red y para organizar que no haya extrema repetición entre los trabajos.

2. **Relevamiento técnico actual de la red:** Esta tarea representa el hecho de ir físicamente a medir las propiedades actuales de la red, conocer la topología y el cableado "in situ". Lograr accesos a planos etc.

3. **Análisis del tráfico actual:** Analizar los datos recolectados en el paso anterior, para obtener conclusiones sobre el estado actual de la red y que defectos y virtudes presenta.

4. **Estudio de los estándares involucrados:** Estudio bibliográfico de los estándares que deberán cumplirse.

5. **Estudio de las tecnologías involucradas**: Investigar las tecnologías que se planean usar para el cumplimiento del proyecto.

6. **Estudio de posibles soluciones:** Planteo de distintas formas de solucionar el problema: cableado vs. wireless, uso de fibra óptica, arquitectura a usarse, modificación de la topología de la red etc.

7. **Análisis de la factibilidad de la solución:** Analisis de los factores que se relacionan con la factibilidad del proyecto y estudios mediante diferentes técnicas que lo modelan.

8. **Relevamiento de los sitios a utilizar para los nuevos equipos:**

9. **Relevamiento de los sitios para el cableado:**

10. **Diseño de la red de acceso:** Discriminar que computadoras usarán placas PCMCIA, USB, y los distintos metodos de acceso. Incluye todo lo respectivo a la red de acceso, menos el planeamiento de la cobertura de los access points.

11. **Organización de los APs:** Diseño de la cobertura con access points, blindaje electromagnético, etc.

12. **Diseño de la red de backbone:** Dimensionamiento del enlace de backbone y diseño del cableado estructurado del mismo.

13. **Calculo del cableado estructurado:** Cálculo de las distancias y materiales necesarios para realizar el cableado necesario.

14. **Busqueda de presupuesto y stock:** Elección de los equipos que cumplen las especificaciones, búsqueda en el mercado nacional de los mismos.

15. **Modificaciones en el diseño debido a falta de equipos**

16. **Presupuesto y listado de materiales final (BOM[11])**

17. **Pedido y entrega de equipos y accesorios**

18. **Instalación de los APs y sus bandejas para 2doP:**

19. **Cableado y puesta en marcha de Wi-Fi 2doP**

[11] Bill Of Materials

20. **Control de las normas y "performance" para la red en 2doP:** Controlar POE, velocidad de acceso, funcionalidad del hand-over entre access points, y todo tipo de error que pueda haber.
21. **Instalación de los APs y sus bandejas para 1erP:**
22. **Cableado y puesta en marcha de Wi-Fi 1erP**
23. **Control de las normas y "performance" para la red en 1erP**
24. **Instalación de los APs y sus bandejas para PB:**
25. **Cableado y puesta en marcha de Wi-Fi PB:**
26. **Control de las normas y "performance" para la red en PB**
27. **Instalación de los APs y sus bandejas para EP:**
28. **Cableado y puesta en marcha de Wi-Fi EP**
29. **Control de las normas y "performance" para la red en EP**
30. **Instalación de los APs y sus bandejas para SS:**
31. **Cableado y puesta en marcha de Wi-Fi SS**
32. **Control de las normas y "performance" para la red en SS**
33. **Instalación de los APs y sus bandejas para 3erP:**
34. **Cableado y puesta en marcha de Wi-Fi 3erP**
35. **Control de las normas y "performance" para la red en 3erP**
36. **Instalación de los APs y sus bandejas para 4toP:**
37. **Cableado y puesta en marcha de Wi-Fi 4toP**
38. **Control de las normas y "performance" para la red en 4toP**
39. **Instalación de los APs y sus bandejas para 5toP:**
40. **Cableado y puesta en marcha de Wi-Fi 5toP**
41. **Control de las normas y "performance" para la red en 5toP**
42. **Instalación de las cámaras IP Wi-Fi y soporte VOIP:** Incluye también comprobar el funcionamiento del servidor de vídeo.
43. **Configuración avanzada y pruebas generales:** Comprobar el funcionamiento de la solución en su conjunto.
44. **Documentación y resguardo de información importante.**

45. **Armado de la infraestructura de Administración.**

46. **Armado de la infraestructura de soporte y mantenimiento.**

Se propone a continuación el método del PERT, el cual toma en cuenta la dispersión de la duración de cada tarea. Por lo tanto, se puede modelar a la duración de la cada tarea como una variable aleatoria y se le asigna un tiempo optimista, pesimista y más probable:

Tiempo optimista (*to*): Es el tiempo mínimo en que se pudiere realizar la tarea (en las mejores condiciones) cumpliendo con lo mínimo establecido.

Tiempo pesimista (*tp*): Indica el mayor tiempo que se considera que pudiere demandar la tarea bajo las peores condiciones.

Tiempo más probable (*tm*): Es el tiempo que lleva la tarea en condiciones normales de realización.

El tiempo más probable para la concreción de una tarea puede aproximarse mediante el modelo de la función beta, cuya expresión normalizada es

$$\beta(x) = kx^p(1-x)^q \tag{7.1}$$

donde el valor de k es tal que

$$\int_0^1 \beta(x) = 1 \tag{7.2}$$

se definen $\alpha = p + 1$, $\beta = q + 1$.

Las expresiones respectivas del valor medio, la varianza y la moda de la distribución quedan definidas por

$$\begin{aligned} \mu &= \frac{\alpha}{\alpha+\beta} \\ \sigma &= \frac{\alpha+\beta}{(\alpha+\beta)^2(\alpha+\beta+1)} \\ x_m &= \frac{\alpha-1}{(\alpha-1)+(\beta-1)} \end{aligned} \tag{7.3}$$

Definidos los tiempos optimista t_o y pesimista t_p, queda definido el intervalo de incerteza de la tarea, relacionado con el intervalo de existencia de la variable beta normalizada x, de la forma

$$\begin{aligned} x &= \frac{t-t_o}{t_p-t_o} \\ \therefore t &= t_o + x(t_p - t_o) \end{aligned} \tag{7.4}$$

El tiempo medio μ_t queda establecido según

$$\mu_t = \frac{t_o + t_p + 4t_m}{6} \tag{7.5}$$

Una forma sencilla para definir los parámetros del modelo consta en adoptar $p + q = 4$, la cual lleva a un error nulo en la estimación anterior del valor medio t_e y aproxima la varianza σ_t^2 a:

$$\sigma_t^2 = (\frac{t_p - t_o}{6})^2 \tag{7.6}$$

A partir de la expresión para la moda, tenemos que:

$$x_m = \frac{p}{k} \tag{7.7}$$

o lo que es la expresión equivalente:

$$p = kx_m \tag{7.8}$$

Habiendo fijado $k = 4$ para esta aproximación, y según las consideraciones adoptadas, pueden deducirse los parámetros p y q del modelo y, en consecuencia, α y β.

$$\begin{aligned} p = \alpha - 1 = 4\frac{t_m - t_o}{t_p - t_o} \\ q = \beta - 1 = 4\frac{t_p - t_m}{t_p - t_o} \end{aligned} \tag{7.9}$$

7.3.2. Asignación de tiempos a las tareas

El cuadro de la siguiente página muestra los tiempos asignados a las tareas.

Tarea	Descripción	t_o	t_m	t_p	μ_t	σ_t^2	Tareas previas
1	Acuerdo entre las partes interesadas en el proyecto	4	5	7	5,17	0,25	–
2	Relevamiento técnico actual de la red	1	3	4	2,83	0,25	1
3	Análisis del tráfico actual	3	4	6	4,17	0,25	2
4	Estudio de los estándares involucrados	3	5	7	5,00	0,44	3
5	Estudio de las tecnologías involucradas	4	7	11	7,17	1,36	3
6	Estudio de posibles soluciones	4	5	7	5,17	0,25	4 – 5
7	Análisis de la factibilidad de la solución	3	4	5	4,00	0,11	6
8	Relevamiento de los sitios a utilizar para los nuevos equipos	1	2	4	2,17	0,25	7
9	Relevamiento de los sitios para el cableado	3	4	6	4,17	0,25	7
10	Diseño de la red de acceso	8	10	15	10,50	1,36	8 – 9
11	Organización de los APs	3	5	7	5,00	0,44	10
12	Diseño de la red de backbone	1	2	4	2,17	0,25	10
13	Calculo del cableado estructurado	2	3	4	3,00	0,11	11 – 12
14	Búsqueda de presupuesto y stock	2	4	7	4,17	0,69	13
15	Modificaciones en el diseño debido a falta de equipos	2	4	9	4,50	1,36	14
16	Presupuesto y listado de materiales final (BOM)	2	3	5	3,17	0,25	15
17	Pedido y entrega de equipos y accesorios	2	6	7	5,50	0,69	16
18	Instalación de los APs y sus bandejas para 2doP	2	3	4	3,00	0,11	17
19	Cableado y puesta en marcha de Wi-Fi 2doP	2	4	6	4,00	0,44	18
20	Control de las normas y "performance" para la red en 2doP	1	2	4	2,17	0,25	19
21	Instalación de los APs y sus bandejas para 1erP	2	3	4	3,00	0,11	20
22	Cableado y puesta en marcha de Wi-Fi 1erP	2	4	6	4,00	0,44	21
23	Control de las normas y "performance" para la red en 1erP	1	2	4	2,17	0,25	22
24	Instalación de los APs y sus bandejas para PB	2	3	4	3,00	0,11	23
25	Cableado y puesta en marcha de Wi-Fi PB	2	4	6	4,00	0,44	24
26	Control de las normas y "performance" para la red en PB	1	2	4	2,17	0,25	25
27	Instalación de los APs y sus bandejas para EP	2	3	4	3,00	0,11	26
28	Cableado y puesta en marcha de Wi-Fi EP	2	4	6	4,00	0,44	27
29	Control de las normas y "performance" para la red en EP	1	2	4	2,17	0,25	28
30	Instalación de los APs y sus bandejas para SS	2	3	4	3,00	0,11	29
31	Cableado y puesta en marcha de Wi-Fi SS	2	4	6	4,00	0,44	30
32	Control de las normas y "performance" para la red en SS	1	2	4	2,17	0,25	31
33	Instalación de los APs y sus bandejas para 3erP	2	3	4	3,00	0,11	35
34	Cableado y puesta en marcha de Wi-Fi 3erP	2	4	6	4,00	0,44	36
35	Control de las normas y "performance" para la red en 3erP	1	2	4	2,17	0,25	37
36	Instalación de los APs y sus bandejas para 4toP	2	3	4	3,00	0,11	38
37	Cableado y puesta en marcha de Wi-Fi 4toP	2	4	6	4,00	0,44	39
38	Control de las normas y "performance" para la red en 4toP	1	2	4	2,17	0,25	40
39	Instalación de los APs y sus bandejas para 5toP	2	3	4	3,00	0,11	32
40	Cableado y puesta en marcha de Wi-Fi 5toP	2	4	6	4,00	0,44	33
41	Control de las normas y "performance" para la red en 5toP	1	2	4	2,17	0,25	34
42	Instalación de las cámaras IP Wi-Fi y Soporte VOIP	5	8	10	7,83	0,69	41
43	Configuración avanzada y pruebas generales	8	10	14	10,33	1,00	42
44	Documentación y resguardo de información importante.	2	3	6	3,33	0,44	43
45	Armado de la infraestructura de Administración.	3	5	8	5,17	0,69	43
46	Armado de la infraestructura de soporte y mantenimiento	3	4	6	4,17	0,25	43

Cuadro 7.1: Asignacion de tiempos de tareas

7.3.3. Asignación del orden de precedencia

Se asigna el orden de realización de las tareas. Dado que para la ejecución de algunas de ellas hace falta haber terminado otras, así mismo, hay tareas que se pueden realizar al mismo tiempo, pues una es independiente de la otra. A continuación se indica el diagrama en bloque del orden de precedencia de las tareas, este puede verse también en el cuadro con el listado de tareas pero esta es una forma más gráfica y mucho mas simple de verlo. Para no quitarle simpleza a la figura, se optó por "resumir" las tareas de la 15 a la 41 con la flecha que indica la continuación en serie de esas tareas.

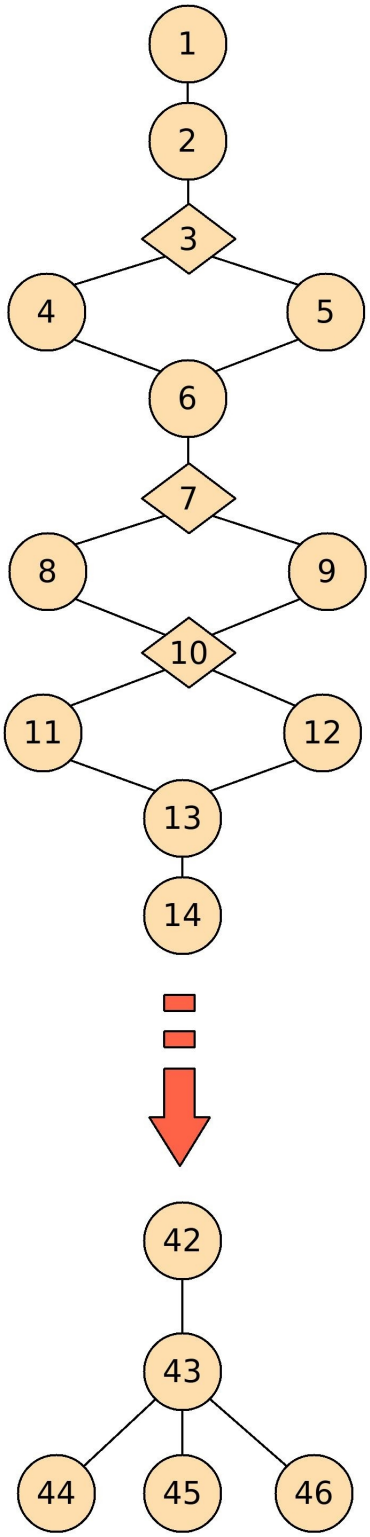


Figura 7.3: Diagrama en bloques del orden de precedencia de las tareas.

7.3.4. Método de camino crítico

Dado que hay varios posibles caminos para llegar al final del proyecto, hace falta determinar cual es el crítico, es decir: cual es el camino que depara más tiempo para su realización. A las tareas que estén en ese camino habrá que prestarles mayor atención pues el retraso en una sola de esas tareas, llevará al retraso del proyecto. También habrá que analizar si hay otros caminos semi-críticos, es decir, si en algún otro de los posibles caminos un retraso importante en alguna tarea lleva al retraso del proyecto. Teniendo en cuenta que los tiempos son aleatorios, tanto el camino crítico como la duración del proyecto son variables aleatorias, por lo tanto cualquiera de los siguientes caminos pueden ser crítico:

Una vez encontrado los caminos críticos mediante el método de PERT, se deberá comparar con el método de propagación de errores y el método de simulación de Montecarlo.

7.3.5. Método de propagación de errores

De la red de PERT se obtienen varios caminos, los cuales presentan duraciones distintas según las tareas involucradas en cada uno, por lo que la duración de éstos será la suma de la duración de cada tarea asociada:

$$t_j = \sum_{\forall\ i\ \in\ j} t_i \tag{7.10}$$

Donde cada t_i es una variable aleatoria.

Dado que la distribución de la suma de muchas variables aleatorias tiende a una distribución normal por el teorema central del límite, se puede conocer el tiempo medio que llevara la ejecución de las tareas en los diversos caminos como la suma de los valores medios de cada tarea más un tiempo que considere la incerteza. Este último es función del desvió estándar a lo largo de un camino y de un factor α que representa la probabilidad de que no pueda concretarse el proyecto en el tiempo estimado. Por lo tanto:

$$\begin{aligned} \bar{t}_j &= \sum_{\forall\ i\ \in\ j} \bar{t}_i + \alpha\sigma_j \\ \therefore \sigma_j &= \sqrt{\sum_{\forall\ i\ \in\ j} \sigma_i^2} \end{aligned} \tag{7.11}$$

Trabajando con un riesgo del 10 % ($\alpha = 0,1$) se obtienen los siguientes valores para cada camino:

Camino Nº	Ruta	μ_j	σ_j^2	σ_j	Tiempos al 10 %
1	1, 2, 3, 4, 6, 7, 8, 10, 11, 13 → 43, 44	159,17	15,31	3,91	160,70
2	1, 2, 3, 4, 6, 7, 8, 10, 11, 13 → 43, 45	161,00	15,56	3,94	162,56
3	1, 2, 3, 4, 6, 7, 8, 10, 11, 13 → 43, 46	160,00	15,11	3,89	161,51
4	1, 2, 3, 4, 6, 7, 8, 10, 12, 13 → 43, 44	156,33	15,11	3,89	157,84
5	1, 2, 3, 4, 6, 7, 8, 10, 12, 13 → 43, 45	158,17	15,36	3,92	159,70
6	1, 2, 3, 4, 6, 7, 8, 10, 12, 13 → 43, 46	157,17	14,92	3,86	158,66
7	1, 2, 3, 4, 6, 7, 9, 10, 11, 13 → 43, 44	161,17	15,31	3,91	162,70
8	1, 2, 3, 4, 6, 7, 9, 10, 11, 13 → 43, 45	163,00	15,56	3,94	164,56
9	1, 2, 3, 4, 6, 7, 9, 10, 11, 13 → 43, 46	162,00	15,11	3,89	163,51
10	1, 2, 3, 4, 6, 7, 9, 10, 12, 13 → 43, 44	158,33	15,11	3,89	159,84
11	1, 2, 3, 4, 6, 7, 9, 10, 12, 13 → 43, 45	160,17	15,36	3,92	161,70
12	1, 2, 3, 4, 6, 7, 9, 10, 12, 13 → 43, 46	159,17	14,92	3,86	160,66
13	1, 2, 3, 5, 6, 7, 8, 10, 11, 13 → 43, 44	161,33	16,22	4,03	162,96
14	1, 2, 3, 5, 6, 7, 8, 10, 11, 13 → 43, 45	163,17	16,47	4,06	164,81
15	1, 2, 3, 5, 6, 7, 8, 10, 11, 13 → 43, 46	162,17	16,03	4,00	163,77
16	1, 2, 3, 5, 6, 7, 8, 10, 12, 13 → 43, 44	158,50	16,03	4,00	160,10
17	1, 2, 3, 5, 6, 7, 8, 10, 12, 13 → 43, 45	160,33	16,28	4,03	161,96
18	1, 2, 3, 5, 6, 7, 8, 10, 12, 13 → 43, 46	159,33	15,83	3,98	160,92
19	1, 2, 3, 5, 6, 7, 9, 10, 11, 13 → 43, 44	163,33	16,22	4,03	164,96
20	1, 2, 3, 5, 6, 7, 9, 10, 11, 13 → 43, 45	165,17	16,47	4,06	166,81
21	1, 2, 3, 5, 6, 7, 9, 10, 11, 13 → 43, 46	164,17	16,03	4,00	165,77
22	1, 2, 3, 5, 6, 7, 9, 10, 12, 13 → 43, 44	160,50	16,03	4,00	162,10
23	1, 2, 3, 5, 6, 7, 9, 10, 12, 13 → 43, 45	162,33	16,28	4,03	163,96
24	1, 2, 3, 5, 6, 7, 9, 10, 12, 13 → 43, 46	161,33	15,83	3,98	162,92

Cuadro 7.2: Tiempos al 10 % según el método PERT

Se puede observar como el camino que demanda el mayor tiempo es el camino 20. Usando un margen del 10 %, la Ecuacion 7.10 y la Ecuación 7.11, se ha calculado un tiempo para finalizar el proyecto de 167.

7.3.6. Método de simulación de Montecarlo

Con el Método de Montecarlo se simula el proceso permitiendo estimar la distribución de probabilidad de la duración de cada tarea y la distribución de probabilidad de la duración total del proyecto. También permite conocer el camino crítico más probable, es decir, revela cuales de las tareas serán decisivas para cumplir el cronograma, así como su frecuencia de aparición, y esto es importante para determinar el grado de control en la ejecución de esas tareas, para que no se vuelvan críticas.

Conocidos los parámetros α y β de la distribución beta para una tarea t_k (caracterizada por t_o, t_m y t_p), un posible valor para la duración de dicha tarea estará dado por $t_k = t_o + x(t_p - t_o)$, donde x será la inversa de la función de distribución beta para un argumento aleatorio de 0 a 1, es decir $x = \beta^{-1}(random, \alpha, \beta)$.

En el CD adjunto se presentan la planilla con los resultados de la simulación para 5.000 casos por medio del método de Montecarlo, en donde se destaca el tiempo de finalización del proyecto al 50 % y al 95 % de confiabilidad.

A continuación se citan las frecuencias con que cada camino tuvo mayor duración con respecto al resto

Camino	Frecuencia
1	0
2	7
3	2
4	0
5	0
6	0
7	22
8	358
9	106
10	0
11	1
12	0
13	0
14	80
15	18
16	0
17	0
18	0
19	195
20	3331
21	859
22	1
23	19
24	2

Cuadro 7.3: Frecuencia de ocurrencia de máxima duración

En conclusión, el camino crítico es el ***Camino 20*** con una frecuencia de ocurrencia del 67 %.

7.3.7. Histograma

A continuación se cita un cuadro con intervalos de tiempo de dos días y la cantidad de ensayos que tienen una duración dentro de esos intervalos. Con los datos de dicho cuadro se construye un histograma, el cual certifica gráficamente que la duración del proyecto es de ***170 días*** con una confiabilidad mayor al 95 %.

Intervalo de duración	Frecuencia
Hasta 140	0
Entre 140 y 145	2
Entre 145 y 150	28
Entre 150 y 155	417
Entre 155 y 160	1298
Entre 160 y 165	1893
Entre 165 y 170	1072
Entre 170 y 175	261
Entre 175 y 180	28
Entre 180 y 185	2
Mayor a 185	0

Cuadro 7.4: Frecuencia de ocurrencia de intervalos de duración

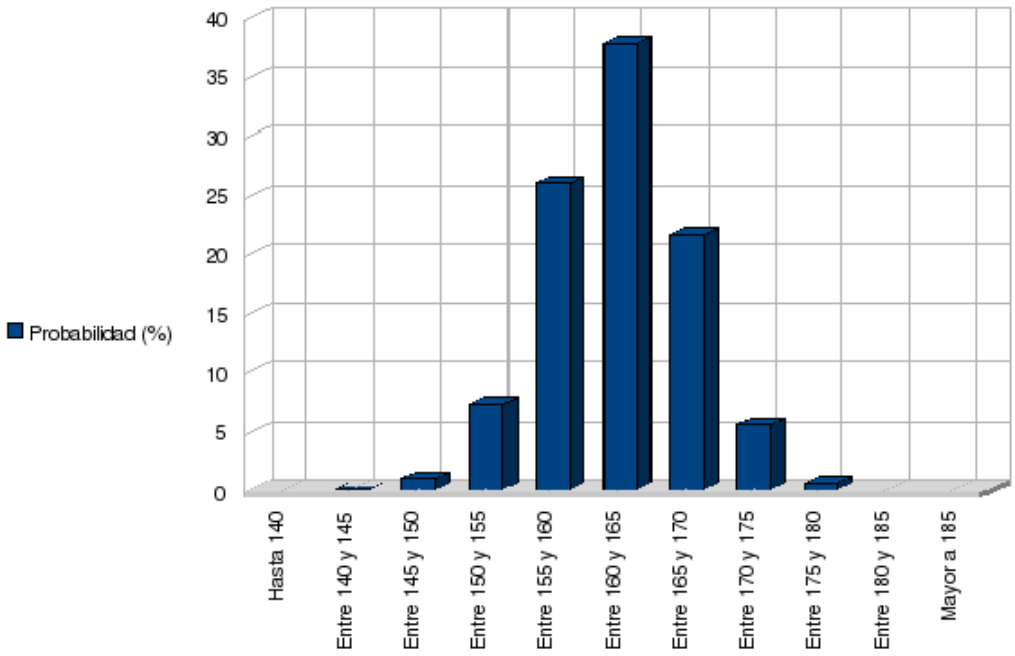


Figura 7.4: Distribución de probabilidad de la duración del camino crítico

7.3.8. Diagrama de Gantt

La programación de un proyecto se vale del diagrama de *Gantt*, el cual posee, en su eje horizontal, el tiempo calendario, en el que se destacan los días laborables. Cada tarea se representa mediante una barra horizontal y queda definida por su fecha de inicio, las precedencias a satisfacer, los días laborables, las horas diarias de trabajo y la duración de cada tarea.

A continuación se presenta el diagrama de *Gantt* realizado con *Microsoft Project*.

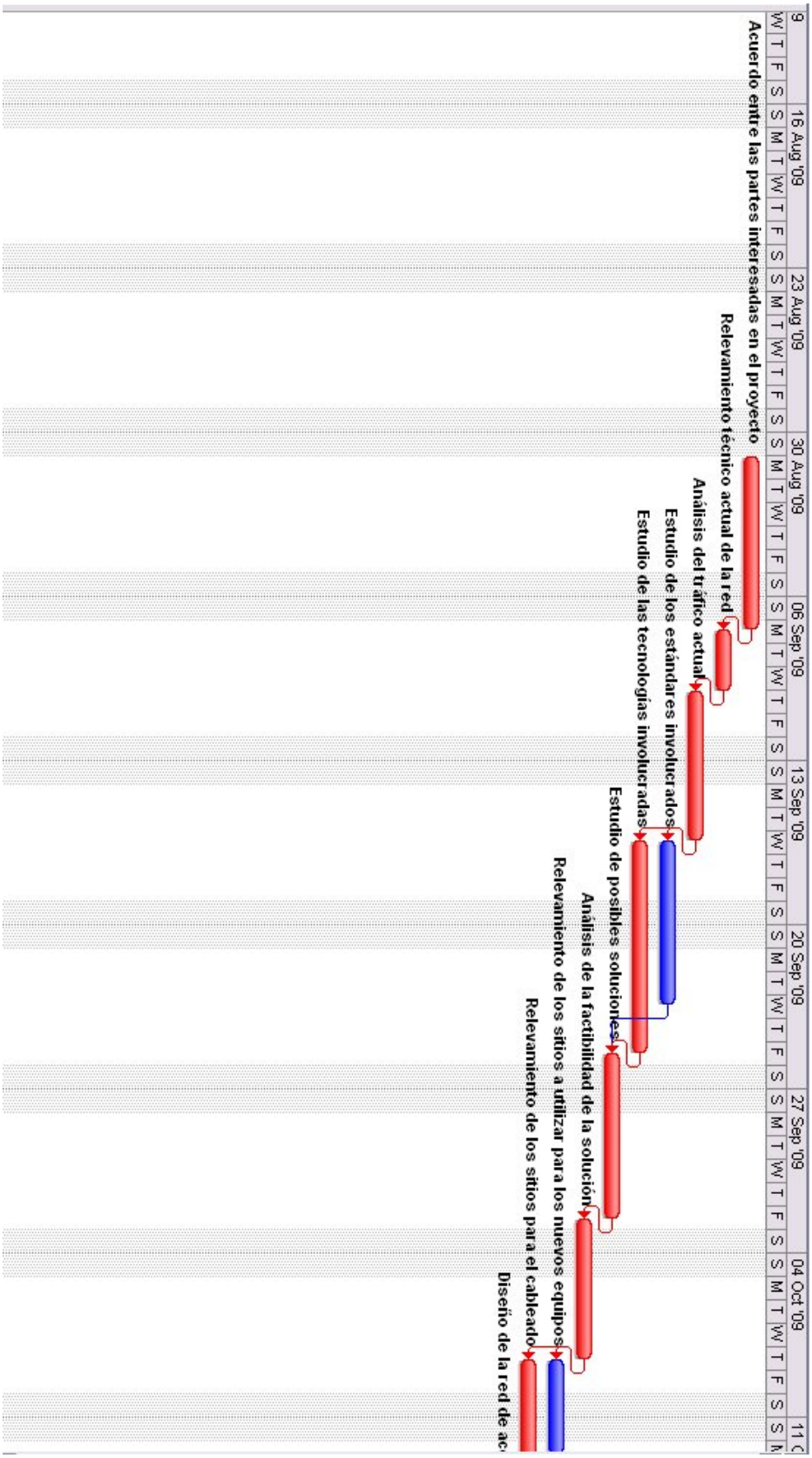


Figura 7.5: Gráfico de Gantt con las tareas y el camino crítico.

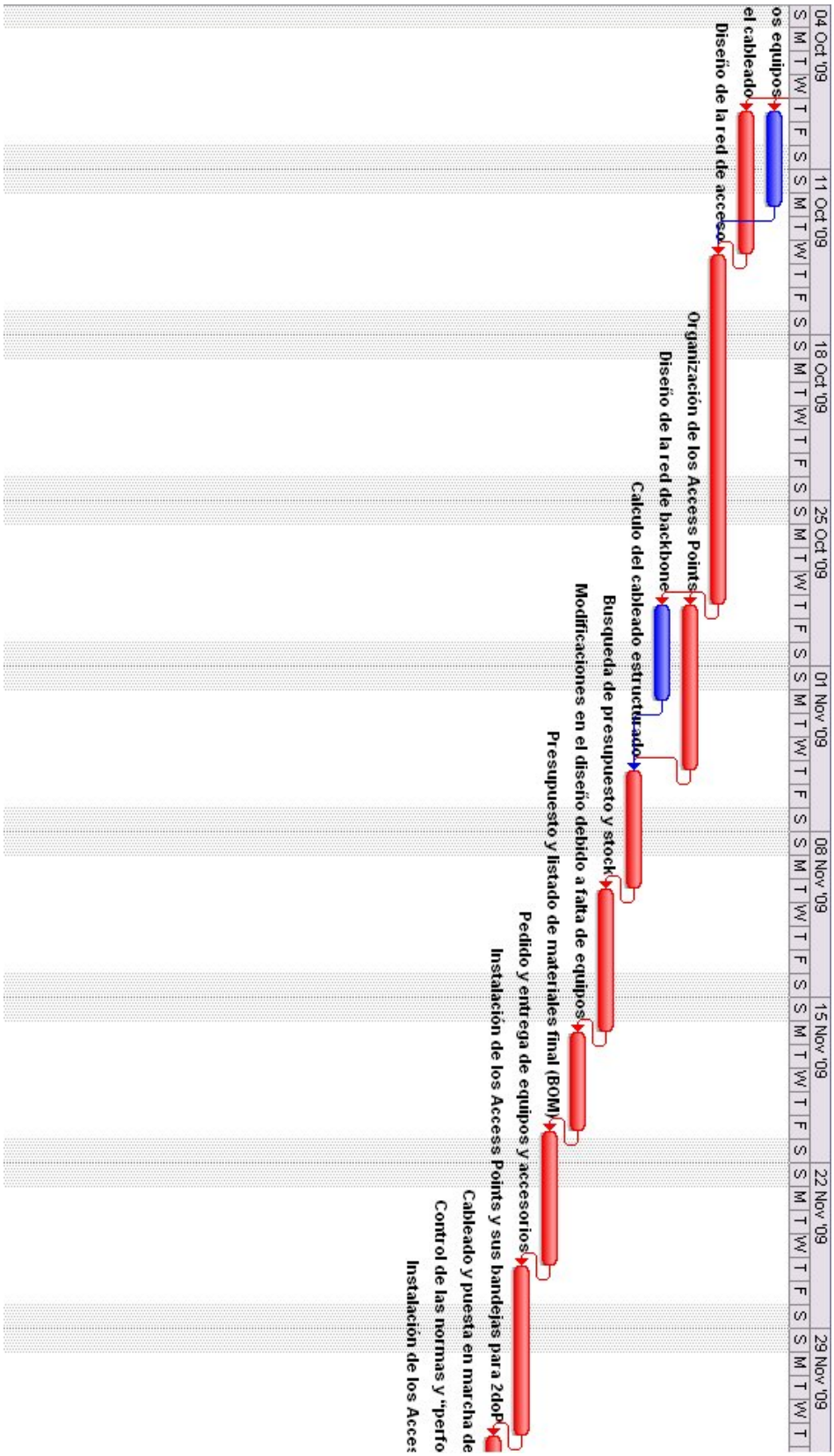


Figura 7.6: Gráfico de Gantt con las tareas y el camino crítico.

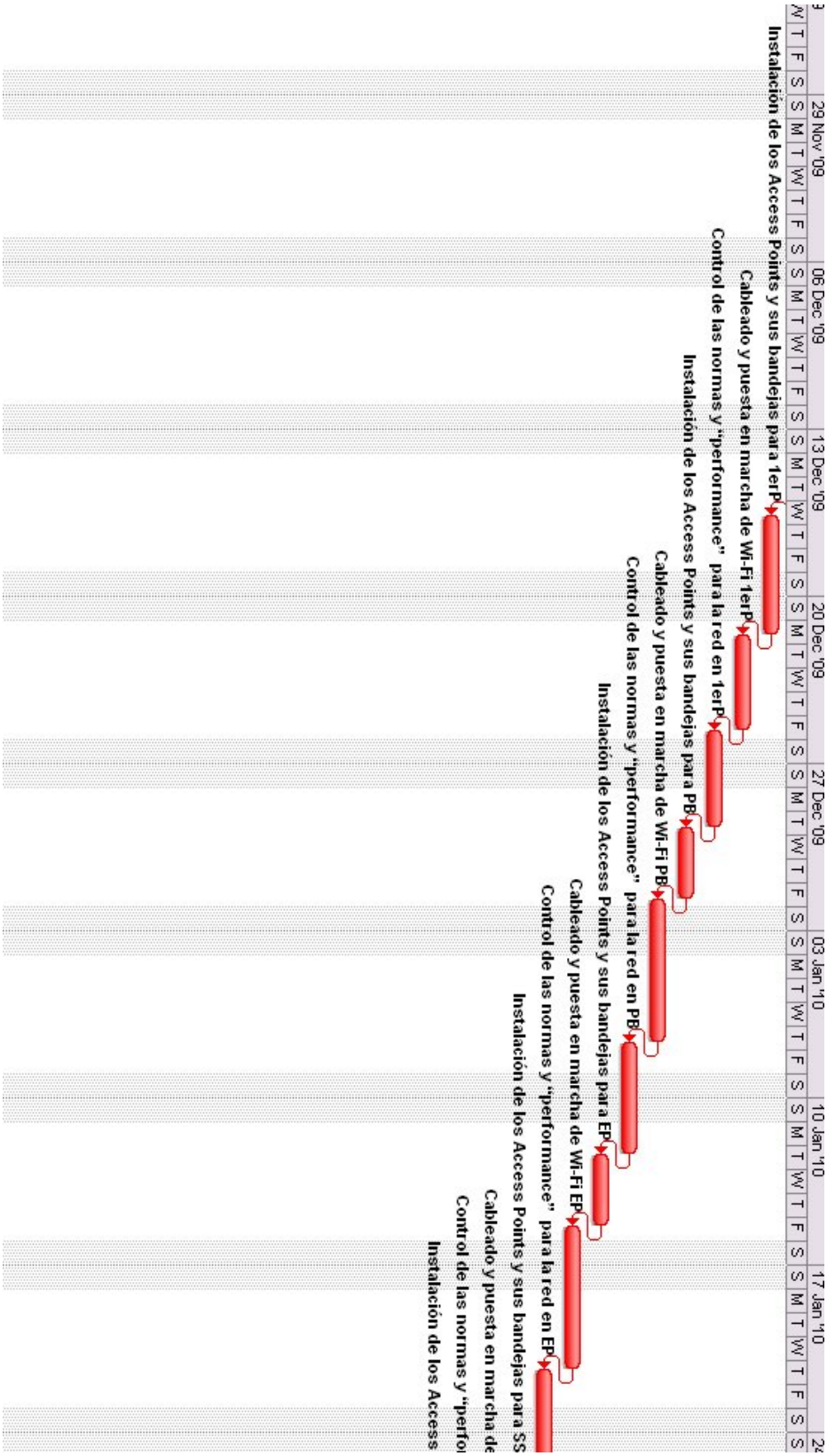


Figura 7.7: Gráfico de Gantt con las tareas y el camino crítico.

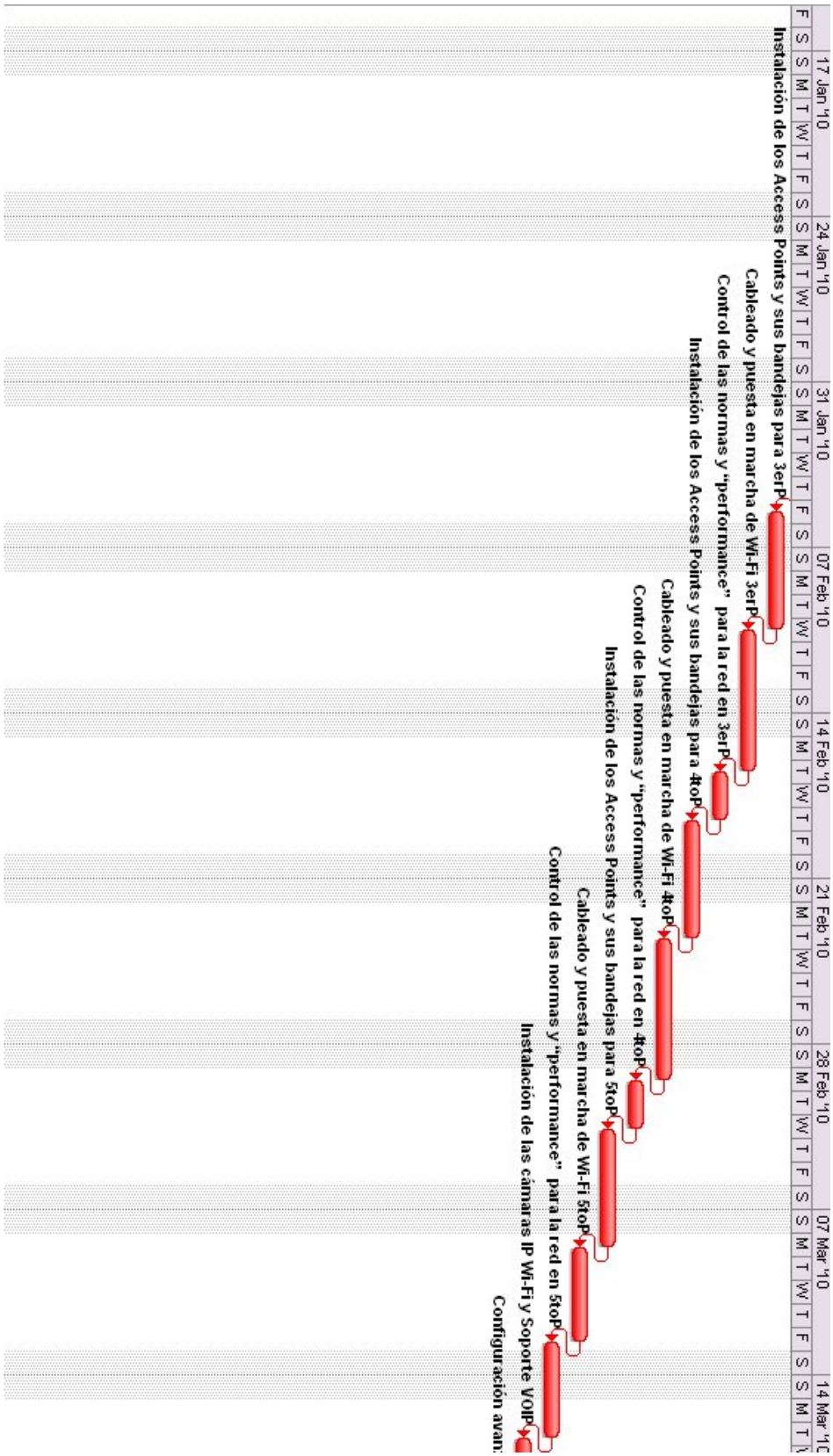


Figura 7.8: Gráfico de Gantt con las tareas y el camino crítico.

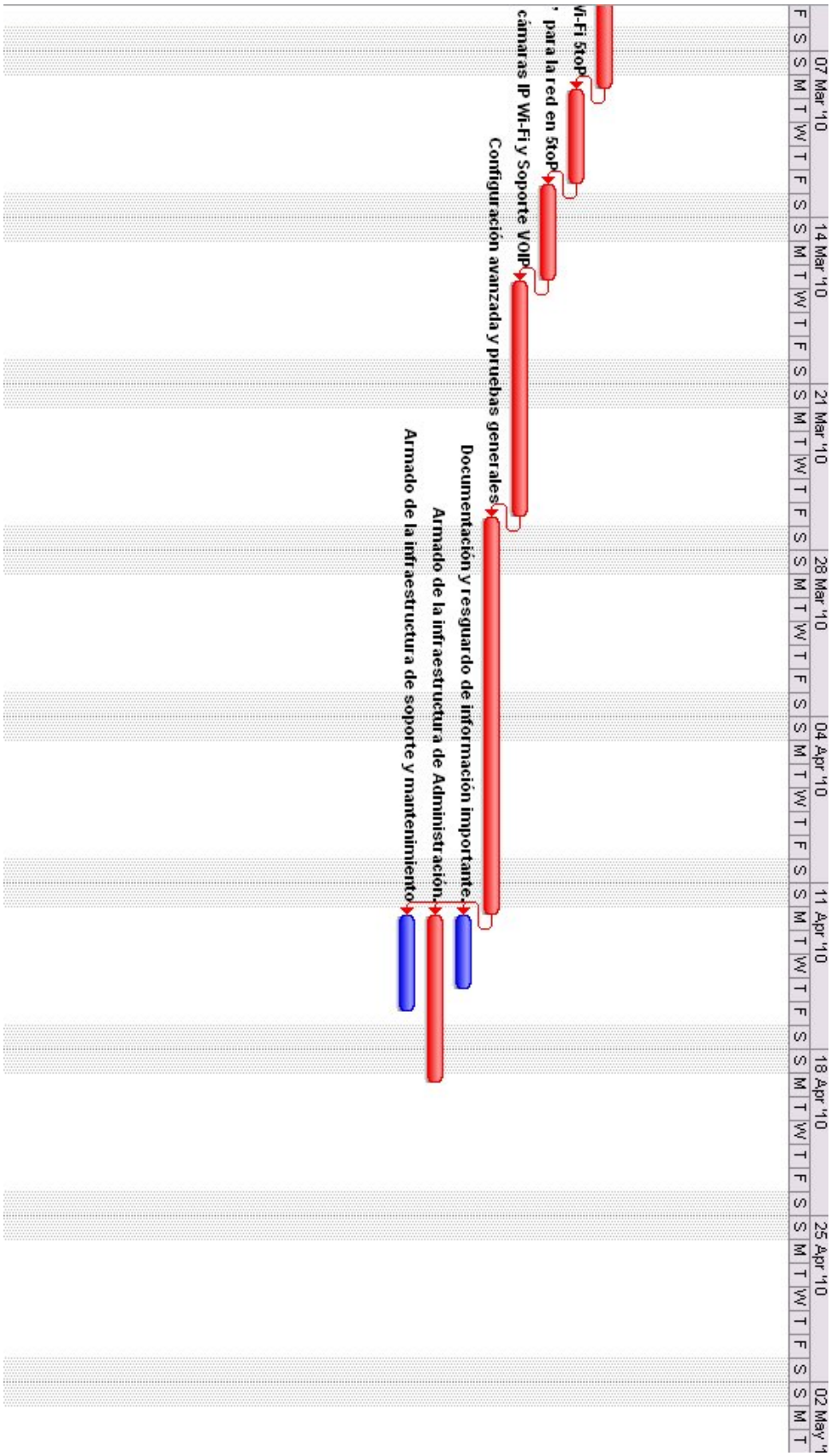


Figura 7.9: Gráfico de Gantt con las tareas y el camino crítico.

7.3.9. Asignación de Recursos

En esta sección se presenta un estudio orientativo de los costos de los honorarios por el trabajo realizado. Cuando la organizacion no es por proyecto, sino que se usan recursos de distintos departamentos, cada uno de ellos trata de ir llenando los tiempos libres manteniendo la carga de trabajo lo más nivelada posible. Para eso se aprovechan los márgenes que puedan tener las tareas. Si la empresa no tiene recursos disponibles, deberá agregar recursos asignando gente, nuevos equipos, o contratando externamente. La asignación puede ser óptima según el criterio que se considere:

- Mínimo empleo de recursos por unidad de tiempo.
- Mejor nivelación en el uso de recursos.
- Adelantar las tareas con mayor incerteza.

Se utilizó la duración de las tareas asignadas en el PERT y se calcularon los honorarios por hora para ingeniero y para técnico. De esta forma se llega a un costo aproximado de $ 114.480. A continuación se detalla la asignación de recursos humanos para las tareas y el costo operativo de las mismas.

Tarea Nº	Descripción	Días hábiles	Personal	Honorarios
1	Acuerdo entre las partes interesadas en el proyecto	5	Ingeniero	$ 2.000
2	Relevamiento técnico actual de la red	3	Técnico	$ 1.152
3	Análisis del tráfico actual	4	Ingeniero	$ 1.600
4	Estudio de los estándares involucrados	5	Ingeniero	$ 2.000
5	Estudio de las tecnologías involucradas	7	Ingeniero	$ 2.800
6	Estudio de posibles soluciones	5	Ingeniero	$ 2.000
7	Análisis de la factibilidad de la solución	4	Ingeniero	$ 1.600
8	Relevamiento de los sitios a utilizar para los nuevos equipos	2	Técnico	$ 768
9	Relevamiento de los sitios para el cableado	4	Técnico	$ 1.536
10	Diseño de la red de acceso	10	Ingeniero	$ 8.000
11	Organización de los APs	5	Ingeniero	$ 2.000
12	Diseño de la red de backbone	2	Ingeniero	$ 800
13	Calculo del cableado estructurado	3	Ingeniero	$ 1.200
14	Búsqueda de presupuesto y stock	4	Ingeniero	$ 1.600
15	Modificaciones en el diseño debido a falta de equipos	4	Técnico	$ 1.536
16	Presupuesto y listado de materiales final (BOM)	3	Ingeniero	$ 1.200
17	Pedido y entrega de equipos y accesorios	6	Técnico	$ 4.800
18	Instalación de los APs y sus bandejas para 2doP	3	Ing. y Téc.	$ 2.352
19	Cableado y puesta en marcha de Wi-Fi 2doP	4	Ing. y Téc.	$ 3.136
20	Control de las normas y “performance” para la red en 2doP	2	Ing. y Téc.	$ 1.568
21	Instalación de los APs y sus bandejas para 1erP	3	Ing. y Téc.	$ 2.352
22	Cableado y puesta en marcha de Wi-Fi 1erP	4	Ing. y Téc.	$ 3.136
23	Control de las normas y “performance” para la red en 1erP	2	Ing. y Téc.	$ 1.568
24	Instalación de los APs y sus bandejas para PB	3	Ing. y Téc.	$ 2.352
25	Cableado y puesta en marcha de Wi-Fi PB	4	Ing. y Téc.	$ 3.136
26	Control de las normas y “performance” para la red en PB	2	Ing. y Téc.	$ 1.568
27	Instalación de los APs y sus bandejas para EP	3	Ing. y Téc.	$ 2.352
28	Cableado y puesta en marcha de Wi-Fi EP	4	Ing. y Téc.	$ 3.136
29	Control de las normas y “performance” para la red en EP	2	Ing. y Téc.	$ 1.568
30	Instalación de los APs y sus bandejas para SS	3	Ing. y Téc.	$ 2.352
31	Cableado y puesta en marcha de Wi-Fi SS	4	Ing. y Téc.	$ 3.136
32	Control de las normas y “performance” para la red en SS	2	Ing. y Téc.	$ 1.568
33	Instalación de los APs y sus bandejas para 3erP	3	Ing. y Téc.	$ 2.352
34	Cableado y puesta en marcha de Wi-Fi 3erP	4	Ing. y Téc.	$ 3.136
35	Control de las normas y “performance” para la red en 3erP	2	Ing. y Téc.	$ 1.568
36	Instalación de los APs y sus bandejas para 4toP	3	Ing. y Téc.	$ 2.352
37	Cableado y puesta en marcha de Wi-Fi 4toP	4	Ing. y Téc.	$ 3.136
38	Control de las normas y “performance” para la red en 4toP	2	Ing. y Téc.	$ 1.568
39	Instalación de los APs y sus bandejas para 5toP	3	Ing. y Téc.	$ 2.352
40	Cableado y puesta en marcha de Wi-Fi 5toP	4	Ing. y Téc.	$ 3.136
41	Control de las normas y “performance” para la red en 5toP	2	Ing. y Téc.	$ 1.568
42	Instalación de las cámaras IP Wi-Fi y Soporte VOIP	8	Técnico	$ 12.800
43	Configuración avanzada y pruebas generales	10	Técnico	$ 3.840
44	Documentación y resguardo de información importante.	3	Ingeniero	$ 1.200
45	Armado de la infraestructura de Administración.	5	Ingeniero	$ 2.000
46	Armado de la infraestructura de soporte y mantenimiento	4	Ingeniero	$ 1.600
Total				**$ 114.480**

Personal	Cantidad	Honorarios por hora
Ingeniero	2	$ 25
Técnico	4	$ 12

Cuadro 7.5: Asignación de recursos y cálculo de costos de la mano de obra

Capítulo 8

Estándares

En esta sección repasaremos los conceptos de algunos estándares que consideramos importantes para el entendimiento y el correcto diseño del sistema que se propone.

8.1. Introducción a WLAN y IEEE 802.11

Una red LAN Wireless (WLAN o Wi-Fi) es un sistema de transmisión diseñado para proveer acceso a la red independientemente de la ubicación entre equipos, usando RF en vez de una infraestructura cableada.

En general, las WLAN son implementadas como el enlace final entre una red cableada coexistente y un grupo de computadoras clientes, dando a estas últimas, acceso a los recursos y servicios de la red.

La masificación y la aceptación de las WLAN dependen de la estandarización que logró la industria que asegura la compatibilidad y fiabilidad entre los diferentes fabricantes.

La especificación 802.11[1] como estándar para WLANs fue ratificada por el Instituto de Ingenieros Electrónicos y Eléctricos[2] en el año 1997. Esta versión de 802.11 proveía velocidades de 1 $Mbps$ y $2Mbps$ y el set de señalamiento para el servicio. Como todos los estándares 802 de la IEEE, el estándar 802.11 se enfocaba en los últimos dos niveles del modelo OSI: la capa física y la capa de datos. Cualquier aplicación LAN o protocolo, incluyendo TCP/IP correrá bien en 802.11 como lo hacen sobre Ethernet.

[1] [IEEE Std 802.11 (ISO/IEC 8802-11: 1999)]

[2] [Electrical and Electronics Engineers (IEEE)]

Figura 8.1: IEEE 802.11 y el modelo OSI

La mayor motivación y beneficio de una WLAN es el aumento de movilidad. Al contrario de redes convencionales, los usuarios pueden moverse casi sin restricciones y acceder a la LAN desde casi cualquier lado.

8.1.1. Arquitectura IEEE 802.11

Una red local 802.11 está basada en una arquitectura celular donde el sistema está dividido en células, denominadas Conjunto de Servicios Básicos (BSS), y cada una de estas células está controlada por una estación base denominada Punto de Acceso (AP).

Aunque una red wireless puede estar formada por una única célula (incluso sin utilizar un punto de acceso), normalmente se utilizan varias células, donde los puntos de accesos estarán conectados a través de un Sistema de Distribución (DS), generalmente Ethernet y en algunos casos sin usar cables.

La red wireless completa, incluyendo las diferentes células, sus puntos de acceso y el sistema de distribución, puede verse en las capas superiores del modelo OSI como una red 802 clásica, y es denominada en el estándar como Conjunto Extendido de Servicios (ESS).

La siguiente figura muestra una red 802.11 clásica, con los componentes descritos previamente:

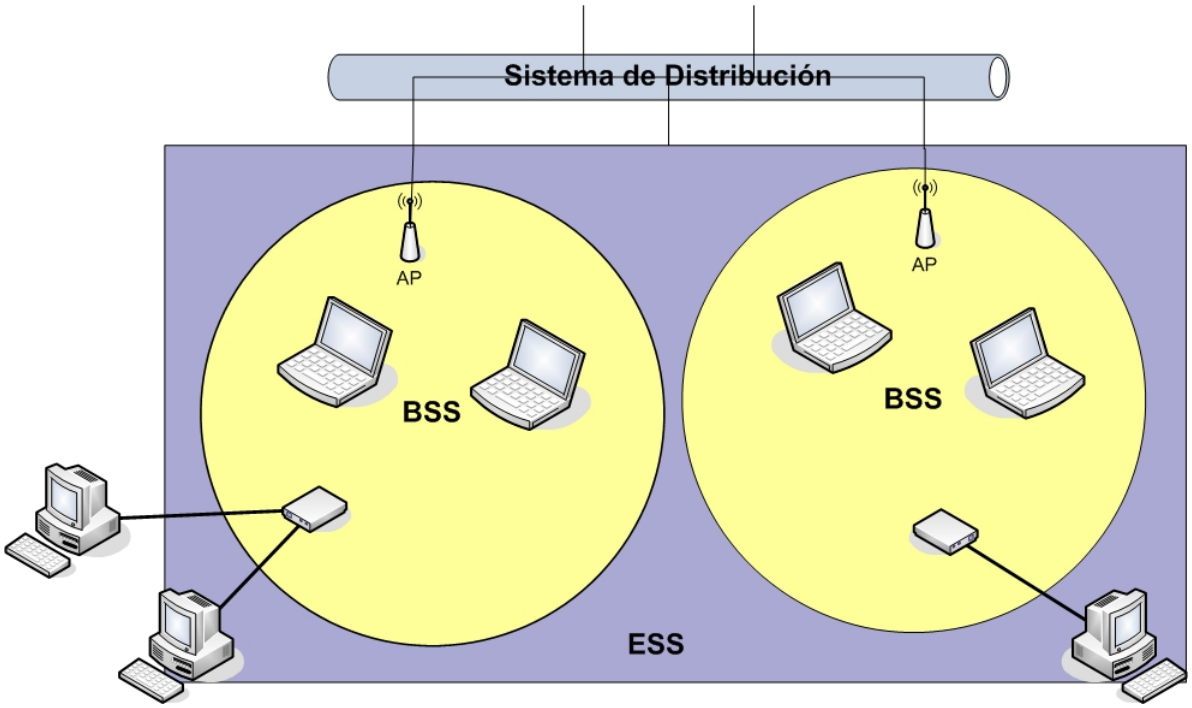


Figura 8.2: Arquitectura básica de red 802

8.1.2. Capa Física

Las tres capas físicas originalmente definidas en 802.11 incluyen: dos basadas en spread-spectrum y una en infrarrojo. Los estándares de radio funcionan dentro de la banda de los 2,4GHz. Estas frecuencias son reconocidas internacionalmente por los operadores y por lo tanto los productos basados en 802.11 no requieren licencias o permisos especiales.

Las técnicas por "Spread Spectrum", aparte de satisfacer los marcos regulatorios, como ya dijimos, aumentan la fiabilidad y aumentan el throughput. Además permiten que otros productos compartan la misma porción del espectro sin la necesidad de definir cooperación explícita y con un mínimo de interferencia.

El estándar 802.11 original define la velocidad de los datos a 1$Mbps$ y 2$Mbps$ usando FHSS[3] o DSSS [4]. Es importante notar que FHSS y DSSS son funcionalmente diferentes y no funcionan entre ellas. Usando la técnica de "Frequency Hopping" la banda de 2,4GHz es dividida en 75 canales de 1MHz. Ambas partes se ponen de acuerdo en un patrón de saltos de frecuencia, y los datos son enviados sobre esta secuencia de los canales. Cada conversación dentro de 802.11 ocurre sobre un diferente patrón de frecuencias y los patrones están diseñados para minimizar el riesgo de que dos equipos que quieren transmitir usen el mismo canal simultáneamente.

Las técnicas FHSS permiten un diseño relativamente simple, pero está limitada a velocidades de no mayores que 2$Mbps$. Esta limitación estaba principalmente por la decisión de la FCC[5]. Que restringe el ancho de banda del canal a 1Mhz. Estas regulaciones fuerzan a los sistemas FHSS a expandirse a través de toda la banda 2,4GHz, por lo que está obligado a saltar de

[3]Frequency Hopping Spread Spectrum
[4]Direct Sequence Spread Spectrum
[5]Federal Communications Commission

frecuencias más frecuentemente, que implica una gran cantidad de encabezado.

En contraste, DSSS divide la banda de 2,4GHz en 14 canales de 22MHz como muestra la Figura 8.3. Los canales coinciden unos sobre otros parcialmente, pudiendo situar tres de los 14 completamente sin solaparse. Los datos son enviados a través de estos canales de 22MHz sin que haya necesidad de saltar a otros canales Para compensar la interferencia de otros usuarios en un canal, una técnica llamada "chipping" es usada. Cada bit de datos del usuario es convertido a una serie de patrones de bits redundantes llamados "chips". La redundancia inherente de cada "chip" combinada con las características de spread-spectrum, provee una forma de chequeo de error y corrección, incluso si parte de la señal ha sido perdida, puede ser recuperada en muchos casos, minimizando la necesidad de retransmisiones.

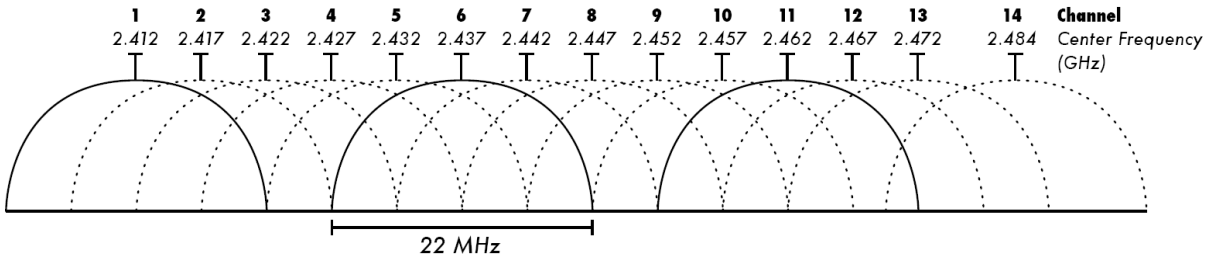


Figura 8.3: Canales Wi-Fi 2.4GHz en (802.11b,g WLAN)

8.1.3. Capa de datos

La capa de datos de 802.11 consiste en 2 subcapas:

- LLC[6].
- MAC[7]

El estándar 802.11 usa el mismo LLC de 802.2 y direcciones de 48 bits como otras LAN de 802, permitiendo la compatibilidad directa de wireless a otras redes IEEE. La capa de MAC es única para las WLAN.

La MAC de 802.11 es muy similar en concepto a la de 802.3 (Ethernet) en el sentido de que está diseñada para soportar múltiples usuarios en un medio compartido haciendo que el que quiere enviar cense el medio antes de accederlo. Para las LAN Ethernet 802.3 se utiliza el protocolo CSMA/CD[8], que regula como las estaciones Ethernet acceso el medio y como detecta y maneja las colisiones que ocurren cuando dos equipos intentan acceder simultáneamente sobre la LAN. En 802.11 las colisiones en WLAN detectar las colisiones no puede ser posible debido al problema conocido como "near/far". Para detectar una colisión, una estación debe ser capaz de transmitir y recibir al mismo tiempo, pero en sistemas de radio, la transmisión limita la habilidad de la estación de "oír" una colisión.Para sobrepasar esta diferencia, 802.11 usa un protocolo levemente modificado llamado CSMA/CA[9]. CSMA/CA intenta evitar las colisiones

[6]Logical Link Control
[7]Media Access Control
[8]Carrier Sense Multiple Access with Collision Detection
[9]Carrier Sense Multiple Access with Collision Avoidance

usando ACK[10] o acuse de recibo. Lo que implica que un ACK es enviado por el receptor para confirmar que el paquete ha llegado.

CSMA/CA trabaja de la siguiente manera. Una estación que esta por transmitir censa el medio y si no detecta actividad, espera un tiempo adicional aleatorio y luego transmite, si el medio continúa libre. Si el paquete es recibido bien, el receptor envía un ACK que si es recibido correctamente por el emisor, el proceso se considera terminado. Si el ACK no es detectado, ya sea porque no se ha logrado enviar la información o porque el mismo ACK es el paquete que se ha perdido, se asume una colisión y el paquete es retransmitido nuevamente esperando un tiempo aleatorio nuevamente y de esta forma CSMA/CA provee una forma de acceso al medio. Este mecanismo maneja la interferencia por otros equipos muy efectivamente. Por otro lado, agrega encabezados a 802.11 en comparación a 802.3, por lo que una WLAN 802.11 tiene en general un desempeño menor dadas las mismas características que una LAN 802.3.

Otro problema específico a nivel de MAC de las redes wireless es el llamado "Hidden Node" en el que dos estaciones de lados opuestos de un acceso escuchan actividad de un AP pero no de cada una, usualmente por una obstrucción o por una distancia lejana como se observa en la Figura 8.4.

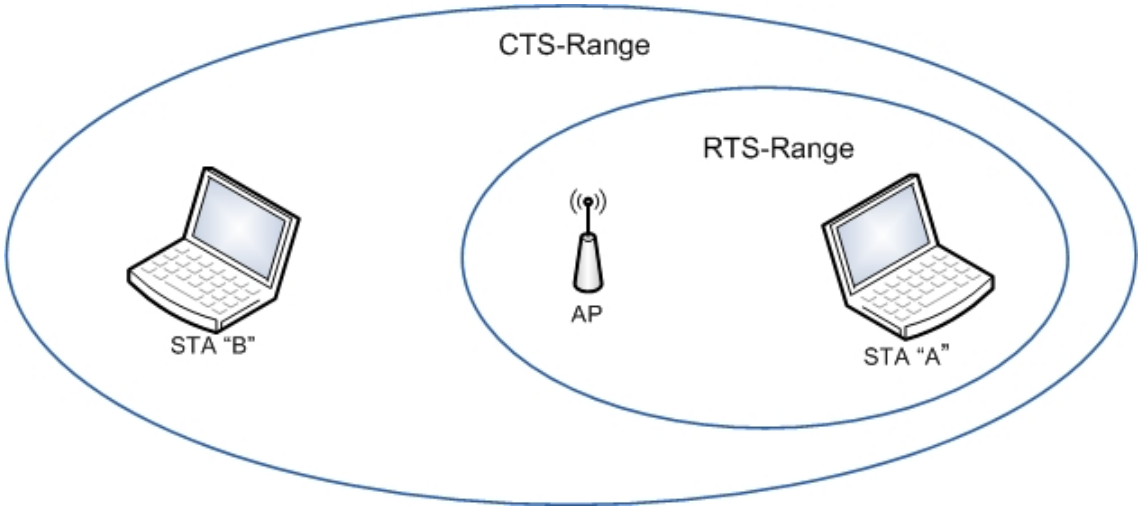


Figura 8.4: RTS/CTS - Hidden Node

Para resolver este problema, 802.11 especifica opcionalmente un RTS/CTS CD[11]. Cuando esta opción se implementa, una estación transmisora transmite un RTS y espera que el AP responda un CTS. Ya que todas las estaciones pueden oír al AP, el CTS causa que demoren cualquier transmisión que esté por darse, permitiendo a la estación transmisora enviar y recibir un paquete sin oportunidad de colisionar. Dado que RTS/CTS agrega más encabezado a la red por reservar el medio temporalmente, es utilizado solo en paquetes de gran tamaño, por los cuales una retransmisión sería costosa desde el punto de vista del ancho de banda.

Finalmente la capa MAC de 802.11 provee otras dos capacidades que le dan robustez: CRC[12] y fragmentación de paquetes. Cada paquete tiene un campo CRC que es calculado e incluido junto con cada paquete para asegurar que los datos no han sido corrompidos durante la

[10] Acknowledgement
[11] Request to Send/Clear to Send
[12] Cyclic Redundancy Check

transmisión. Esto es diferente frente a Ethernet, donde protocolos de más alto nivel tales como TCP se ocupan de corroborar el error. La paquetización permite que paquetes grandes sean segmentados en paquetes más pequeños que es útil en ambientes muy congestionados, cuando la interferencia es un factor ya que los paquetes más grandes tienen una mayor probabilidad de ser corrompidos debido a colisiones. Esta técnica reduce la necesidad de retransmitir en muchos casos, mejorando la capacidad total del enlace. La capa MAC es responsable por el rearmado de los fragmentos recibidos, liberando y haciendo transparente este proceso a capas de transporte de protocolos de más alto nivel.

8.1.4. Estándares IEEE 802.11

El problema más crítico afectando una WLAN es la velocidad limitada. Las velocidades soportadas por el 802.11 original son demasiado lentas para los requerimientos normales y demoró la adopción del uso de WLAN.

Reconociendo la necesidad crítica de dar mayor velocidad, la IEEE ratificó el estándar con el 802.11b con posibilidad de transmitir hasta 11$Mbps$. Luego del estándar 802.11b , fue ratificado el estándar 802.11a y en enero del 2002 se aprobó 802.11g.

Las letras después del número 802.11 nos dicen el orden en el que los estándares fueron propuestos. Esto significa que en su momento, el "nuevo"estándar 802.11a es en realidad mas viejo que el actual 802.11b que fue aprobado primero por el hecho de estar basado en una tecnología un poco más simple (DSSS) a diferencia de 802.11a que usa OFDM[13]. Esta tecnología un poco más compleja, permite llegar a velocidades de 54 $Mbps$.

	802.11	**802.11*a***	**802.11*b***	**802.11*g***
Velocidad Máxima	1$Mbps$-2$Mbps$	54$Mbps$	11$Mbps$	54$Mbps$
Velocidad Media	500$kbps$-1$Mbps$	27$Mbps$	5$Mbps$	22$Mbps$
Modulación	FHSS-QPSK/DSSS	OFDM	QPSK/DSSS	OFDM/DSSS
Frecuencia	2.4GHz	5GHz	2.4GHz	2.4GHz
Aprobación	1997	1999	1999	2002

Cuadro 8.1: Características del estándar 802.1x

8.1.5. IEEE 802.11*b*

La arquitectura básica y los servicios de 802.11b están definidos por el estándar 802.11 original. La especificación 802.11b afecta solo la capa física, añadiendo velocidades mayores y una conectividad más robusta.

La contribución clave de 802.11b a las WLAN fue a estandarización de la capa física y el soporte de dos nuevas velocidades: 5,5$Mbps$ y 11$Mbps$. Para lograr esto, DSSS tuvo que ser seleccionada como la técnica para el estándar, ya que "Frequency Hopping" no puede dar soporte a velocidades mayores sin violar regulaciones de la FCC. Por esta razón, 802.11b puede operar a 1$Mbps$ o 2$Mbps$ del estándar 802.11 con DSSS, pero no con 1$Mbps$ o 2$Mbps$ de sistemas FHSS.

El estándar 802.11 DSSS original utiliza un "código de Barker", en el cual un pulso de binario de datos se subdivide en una cantidad de subpulsos de igual duración y de valor +1 o

[13]Orthogonal Frequency Division Multiplexing

-1 como puede observarse en la Figura 8.5. Estos códigos tienen la propiedad que la función de correlación da lóbulos secundarios pequeños, mejorando la recepción de los datos.

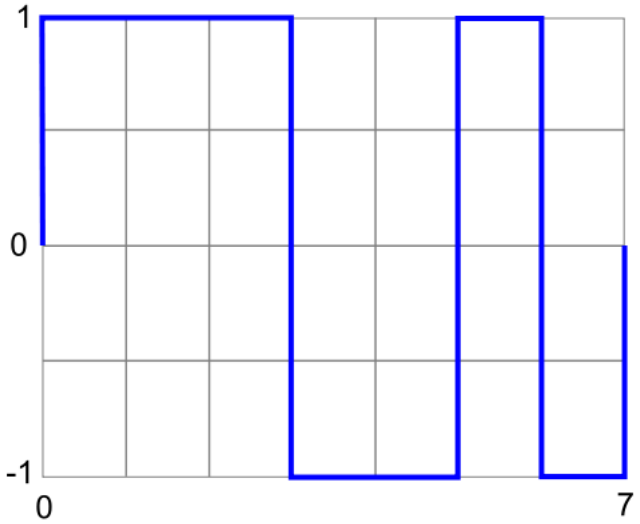


Figura 8.5: Código de Barker de longitud 7, representación en bandabase

Estos subpulsos se denominan "chips" y el estándar especifica un código de 11 chips por binit[14] para codificar los datos enviados. Estos símbolos son transmitidos a $1Mbaudio$ (1 millón de símbolos por segundo) usando BPSK[15]. En el caso de $2Mbps$ es usada una implementación mas sofisticada en QPSK[16], esto duplica la velocidad de transmisión, mejorando la utilización del ancho de banda del canal. En 802.11b se utilizan técnicas avanzadas de codificación.

En vez de usar dos secuencias de 11 chips Barker, 802.11b especifica CCK[17], que consiste en un set de 64 palabras de 8bits. Las mismas tienen propiedades matemáticas que permiten que puedan ser correctamente distinguidas una de las otras por el receptor en presencia de un ruido substancial e interferencia por multipath, tales como rebotes en la cara de un edificio cercano.

La velocidad de 5,5$Mbps$ usa CCK para codificar 4 bits por portadora, mientras que el de 11$Mbps$ codifica 8 bits por portadora. Ambos usan QPSK como técnica de modulación y señal a 1,375$Mbaudios$. Así es como estas velocidades mayores son obtenidas. Para soportar ambientes muy contaminados de ruido, y mayor distancias, las velocidades se auto ajustan permitiendo compensar la naturaleza cambiante del canal radioeléctrico. Idealmente, los usuarios se conectan a 11$Mbps$.

Una de las desventajas de 802.11b es que la banda de frecuencia está saturada y es sujeta a interferencias de otros equipos tales como celulares, hornos microondas, teléfonos inalámbricos (funcionan también en 2,4GHz), Bluetooth, etc. Esta es una desventaja, incluyendo la falta de interoperabilidad con equipos de vos y falta de QoS para el contenido multimedia.

[14]bit de información
[15]Binary Phase Shift Keying
[16]Quadrature Phase Shift Keying
[17]Complementary Code Keying

8.1.6. IEEE 802.11*a*

802.11*a* es mucho más rápido que 802.11*b*, con una velocidad máxima de 54*Mbps* y operando un el rango de los 5*GHz* y permitiendo hasta ocho canales simultáneos.

802.11*a* usa OFDM[18], una codificación que ofrece los beneficios de spread spectrum en capacidad de canal y velocidad del mismo.

La capacidad del canal es significativamente mayor debido a que hay mayor cantidad de canales independientes para usar. Se utilizan ocho canales no solapados de 20*Mhz*, en contraste con los tres canales usados por 802.11*b*.

Todas las bandas WLAN no son licenciadas, por lo que son propensos a interferencias y errores. Para reducirlos, ambos tipos de 802.11 automáticamente reducen su velocidad en la capa física. Como dijimos, 802.11*b* tiene tres velocidades más bajas: 5.5, 2 y 1*Mbps*. 802.11*a* tiene siete: 48, 36, 24, 18, 12, 9, y 6*Mbps*. Más y mayores velocidades de transmisión no son la única ventaja. También usa una frecuencia más alta, 5*GHz*, que es a su vez mas amplia y menos usada que la de 2,4*GHz* de 802.11*b*, que como ya vimos, es compartida por muchas otras tecnologías y equipos. Un ancho de banda mayor, implica que más canales pueden coexistir sin interferencia. Cada canal, corresponde a una red separada, o a un segmento switcheado de la misma red. Una desventaja es que no es directamente compatible con 802.11*b* requiriendo nuevos equipos que soporten ambas tecnologías.

8.1.7. IEEE 802.11*g*

Aunque la banda de los 5*GHz* tiene varias ventajas, para superar los problemas de compatibilidad, se desarrolló 802.11*g* que extiende la velocidad de la 802.11*b* pero también es compatible con los sistemas anteriores.

El estándar opera enteramente en 2,4*GHz* pero usa un mínimo de dos modos (ambos obligatorios) con otros dos modos opcionales. Las modulaciones obligadas son las mismas CCK ya usada en 802.11*b* (y de ahí la compatibilidad) y OFDM usado por 802.11*a* (pero en este caso en 2.4*GHz*). El modo obligado de CCK soporta 11*Mbps* y el modo OFDM tiene un máximo de 54*Mbps*. Hay otros dos modos que obtienen 22*Mbps* de velocidad, uno es PCBB-22[19], y CCK-OFDM con un máximo de 33*Mbps* respectivamente.

La ventaja obvia de 802.11*g* es que mantiene compatibilidad con 802.11*b* y que también ofrecen mayores velocidades comparables a 802.11*a* pero al utilizar la banda de 2,4*GHz* y solo tres canales es mas propensa a interferencias, por lo que alcanzar la velocidad máxima teórica es mas difícil que con 802.11*a*.

8.1.8. IEEE 802.11*n*

IEEE 802.11*n* está construido basándose en estándares previos de la familia 802.11, agregando MIMO[20] y unión de interfaces de red (Channel Bonding), además de agregar tramas a la capa MAC.

MIMO usa múltiples antenas transmisoras y receptoras para mejorar el desempeño del sistema. MIMO es una tecnología que usa múltiples antenas para manejar más información

[18] Orthogonal Frequency Division Multiplexing
[19] Packet Binary Convolutional Coding
[20] Multiple-Input Multiple-Output

(cuidando la coherencia) que utilizando una sola antena. Dos beneficios importantes que provee a $802.11n$ son la diversidad de antenas y el multiplexado espacial.

La tecnología MIMO depende de señales múltiple camino. Las señales múltiple caminos son señales reflejadas que llegan al receptor un tiempo después de que la señal de línea de visión ha sido recibida. En una red no basada en MIMO, como son las redes $802.11a/b/g$, las señales de múltiples caminos son percibidas como interferencia que degradan la habilidad del receptor de recobrar el mensaje en la señal. MIMO utiliza la diversidad de las señales múltiple camino para incrementar la habilidad de un receptor de recobrar los mensajes de la señal.

Otra habilidad que provee MIMO es el Multiplexado de División Espacial (SDM). SDM multiplexa espacialmente múltiples flujos de datos independientes, transferidos simultáneamente con un canal espectral de cierto ancho de banda. SDM puede incrementar significativamente el desempeño de la transmisión conforme el número de flujos espaciales es incrementado. Cada flujo espacial requiere una antena discreta tanto en el transmisor como el receptor. Además, la tecnología MIMO requiere una cadena de radiofrecuencia separada y un conversor AD para cada antena MIMO lo cual incrementa el costo de implantación comparado con sistemas sin MIMO.

Channel Bonding, también conocido como $40Mhz$ o unión de interfaces de red, es la segunda tecnología incorporada al estándar $802.11n$ la cual puede utilizar dos canales separados, que no se solapen, para transmitir datos simultáneamente. La unión de interfaces de red incrementa la cantidad de datos que pueden ser transmitidos. Se utilizan dos bandas adyacentes de $20Mhz$ cada una, por eso el nombre de $40Mhz$. Esto permite doblar la velocidad de la capa física disponible en un solo canal de $20Mhz$. (Aunque el desempeño del lado del usuario no será doblado.) Utilizar conjuntamente una arquitectura MIMO con canales de mayor ancho de banda ofrece la oportunidad de crear sistemas muy poderosos y rentables para incrementar la velocidad de transmisión de la capa física.

8.1.9. Codificación de los datos

El transmisor y el receptor utilizan técnicas de pre-codificación y pos-codificación, respectivamente, para lograr la capacidad de un enlace MIMO. La pre-codificación incluye beamforming y diversidad de código, donde beamforming mejora la calidad de la señal recibida en el proceso de decodificación. Diversidad de código es usada donde sólo puede usarse un canal, codificando la transmisión mediante espaciado en el tiempo y la diversidad de señales disponibles dando lugar al código espacio-tiempo. La emisión desde varias antenas basándose en principios de ortogonalidad es aprovechada para aumentar la diversidad de la señal.

8.1.10. Número de antenas

El número de flujos de datos simultáneos está limitado por el número mínimo de antenas usadas en ambos lados del enlace. Los radios individuales a menudo limitan el número de flujos que pueden llevar datos únicos. La notación $a \times b : c$ ayuda a identificar que capacidad tiene un determinado radio. El primer número (a) es el número máximo de cadenas transmisoras o cadenas RF que pueden ser usadas por el radio. El segundo número (b) es el número máximo de antenas receptoras o cadenas RF que pueden ser usadas por el radio. El tercer número (c) es el número máximo de flujos de datos espaciales que el radio puede usar. Por ejemplo, un

radio que puede transmitir en dos antenas y recibir en tres, pero sólo puede enviar o recibir dos flujos de datos podría ser $2 \times 3 : 2$.

El borrador de la especificación de 802.11n permite hasta $4 \times 4 : 4$. Configuraciones comunes de dispositivos que siguen los estándares 802.11n son $2 \times 2 : 2$, $2 \times 3 : 2$, y $3 \times 3 : 2$. Estas tres configuraciones tienen el mismo desempeño máximo y características, y difiere sólo en la cantidad de diversidad que provee los sistemas de antenas.

8.1.11. Seguridad

El acceso sin necesidad de cables, lo que hace tan populares a las redes inalámbricas, es a la vez el problema más grande de este tipo de redes en cuanto a seguridad se refiere. Los problemas de escuchas ilegales, acceso no autorizado, usurpación y suplantación de identidad, interferencias aleatorias, denegación de servicio (DoS), ataques, etc., se originan por la mala arquitectura o método de seguridad implantado en la red inalámbrica.

Para poder considerar una red inalámbrica como segura, debe cumplir con los siguientes requisitos generales:

- Las ondas de radio deben confinarse tanto como sea posible, empleando antenas direccionales y/o sectoriales y configurando adecuadamente la potencia de transmisión de los Puntos de Acceso.
- Debe existir algún mecanismo de autenticación en doble vía, que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella.
- Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva.

Filtrado de direcciones MAC

Este método consiste en la creación de una tabla de datos en cada uno de los Puntos de Acceso de la red inalámbrica. Dicha tabla contiene las direcciones MAC de las tarjetas de red inalámbricas que pueden acceder o denegar la comunicación de datos con un Punto de Acceso.

Como ventaja principal de este método es su sencillez, por lo cual se puede usar para redes caseras o pequeñas. Sin embargo, posee muchas desventajas que lo hacen impráctico para uso en redes medianas o grandes.

WEP (Wired Equivalent Privacy)

El algoritmo WEP forma parte de la especificación 802.11, y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica. WEP opera a nivel 2 del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas.

El funcionamiento del cifrado WEP establece una clave secreta en el Punto de Acceso que es compartida con los diferentes dispositivos móviles Wi-Fi. Con esta clave de 40 ó de 104 bits, con el algoritmo de encriptación RC4 y con el Vector de

Inicialización (IV) se realiza el cifrado de los datos transmitidos por Radio Frecuencia. Las principales debilidades del protocolo WEP son tres:

- El Vector de Inicialización es demasiado corto (24 bits) ocasionando problemas de transmisión en redes inalámbricas con mucho tráfico.
- Las claves WEP que se utilizan son estáticas y se deben cambiar manualmente.
- No se tiene un sistema de control de secuencia de paquetes. Los paquetes de información pueden ser modificados.

Autenticación con IEEE 802.1X

El estándar IEEE 802.1X es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red.

Este protocolo permite la autenticación de equipos y/o usuarios antes de que éstos puedan conectarse a una red cableada o inalámbrica. La autenticación se realiza con el Protocolo de Autenticación Extensible (EAP, Extensible Authentication Protocol) y con un servidor de tipo RADIUS (Remote Authentication Dial In User Services).

El protocolo 802.1X involucra tres elementos:

- El suplicante, o equipo del cliente, que desea conectarse con la red. Es una aplicación cliente que suministra las credenciales del usuario.
- El servidor de autorización/autenticación (RADIUS), que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red.
- El autenticador, que es el equipo de red (Punto de Acceso, switch, router, etc.) que recibe la conexión del suplicante. El autenticador actúa como intermediario entre el suplicante y el servidor de autenticación, y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza.

La autenticación 802.1X es un proceso de múltiples pasos que involucra al cliente o suplicante, un Punto de Acceso o autenticador, un servidor RADIUS o de autenticación y generalmente una base de datos.

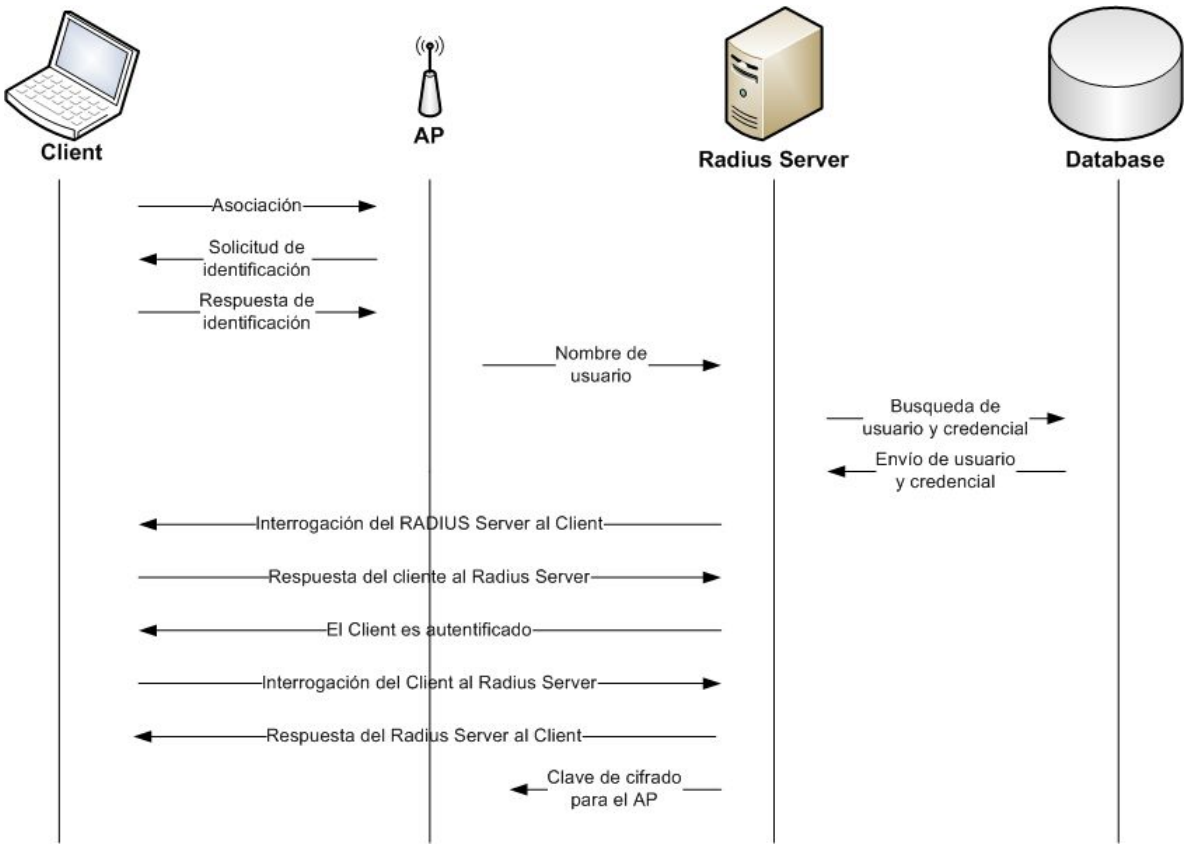


Figura 8.6: IEEE 802.1x

WPA (Wi-Fi Protected Access)

Los mecanismos de encriptación WPA y WPA2 se desarrollaron para solucionar las debilidades detectadas en el algoritmo de encriptación WEP. El nombre de WPA (Wi-Fi Protected Access, Acceso Protegido Wi-Fi) es el nombre comercial que promueve la Wi-Fi Alliance, las especificaciones y consideraciones técnicas se encuentran definidas en el estándar IEEE 802.11i.

El estándar 802.11i especifica dos nuevos protocolos de seguridad TKIP (Temporary Key Integrity Protocol, Protocolo de Integridad de Claves Temporales) y CCMP (Counter Mode CBC-MAC, Protocolo de Modo Contador con CBC-MAC).

TKIP se diseñó para ser compatible hacia atrás con el hardware existente, mientras que CCMP se diseñó desde cero.

Para solucionar los inconvenientes de WEP la Wi-Fi Alliance decidió implementar dos soluciones de seguridad:

- Una solución rápida y temporal para todos los dispositivos inalámbricos ya instalados hasta el momento, especificando al estándar comercial intermedio WPA.
- Una solución más definitiva y estable para aplicar a nuevos dispositivos inalámbricos, especificando al estándar comercial WPA2.

WPA Versión 1 (WPA)

WPA se fundamenta en el protocolo de cifrado TKIP, este protocolo se basa en el tercer borrador de 802.11i a mediados del 2003. TKIP se encarga de cambiar la clave compartida entre el Punto de Acceso y el cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave.

Las mejoras a la seguridad introducidas en WPA son:

- Se incrementó el Vector de Inicialización (IV) de 24 a 48 bits.
- Se añadió la función MIC (Message Integrity Check, Chequeo de Integridad de Mensajes) para controlar y detectar manipulaciones de los paquetes de información.
- Se reforzó el mecanismo de generación de claves de sesión.

WPA Versión 2 (WPA2)

WPA2 es el nombre comercial de la Wi-Fi Alliance a la segunda fase del estándar IEEE 802.11i dando una solución de seguridad de forma definitiva. WPA2 utiliza el algoritmo de encriptación AES (Advanced Encryption Standard, Estándar de Encriptación Avanzado) el cuál es un código de bloques que puede funcionar con muchas longitudes de clave y tamaños de bloques.

WPA2 se fundamenta en el protocolo de seguridad de la capa de enlace basado en AES denominado CCMP. CCMP es un modo de funcionamiento combinado en el que se utiliza la misma clave en el cifrado para obtener confidencialidad, así como para crear un valor de comprobación de integridad criptográficamente segura.

Para la implementación de CCMP se realizaron algunos cambios en los paquetes de información como por ejemplo en las tramas beacon, tramas de asociación e integración, etc.

Modalidades de Operación:

Según la complejidad de la red, un Punto de Acceso compatible con WPA o WPA2 puede operar en dos modalidades:

- Modalidad de Red Empresarial, para operar en esta modalidad se requiere de la existencia de un servidor RADIUS en la red. El Punto de Acceso emplea entonces 802.1X y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.
- Modalidad de Red Personal o PSK (Pre-Shared Key), tanto WPA como WPA2 operan en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el Punto de Acceso y en los dispositivos móviles. Solamente podrán acceder al Punto de Acceso los dispositivos móviles cuya contraseña coincida con la del Punto de Acceso. Una vez lograda la asociación, TKIP entra en funcionamiento para garantizar la seguridad del acceso.

Políticas de Seguridad

Las políticas de seguridad más relevantes que se deben establecer dentro de una red inalámbrica Wi-Fi son:

- Verificar que los usuarios sean capacitados en el uso de la tecnología Wi-Fi y conocen los riesgos asociados con su utilización.
- Cambiar el SSID por defecto.
- Desactivar el broadcast del SSID.
- Verificar que el SSID no contenga datos de la organización.
- Políticas de instalación de parches y actualizaciones en los dispositivos inalámbricos.
- Mantenimiento continuo de los Puntos de Acceso y Controladores de Puntos de Acceso.
- Políticas de contraseñas y claves para Puntos de Acceso y usuarios inalámbricos.
- Políticas de configuración y backups de los Puntos de Acceso.
- Auditorías periódicas de todos los dispositivos inalámbricos Wi-Fi instalados.
- Monitoreo y reconocimiento periódico del recurso de Radio Frecuencia.

La seguridad informática no solo se logra con tecnología, también las políticas de seguridad, los procedimientos y la capacitación de los usuarios inalámbricos desempeñan un papel fundamental.

8.2. Cableado Estructurado

8.2.1. ANSI/EIA/TIA 569 Commercial Building Standards for Telecommunications Pathways and Spaces

Este estándar provee especificaciones para el diseño de las instalaciones y la infraestructura edilicia necesaria para el cableado de telecomunicaciones en edificios comerciales. Se tienen en cuenta tres conceptos fundamentales relacionados con telecomunicaciones y edificios:

- Los edificios son dinámicos. Durante la existencia de un edificio, las remodelaciones son comunes, y deben ser tenidas en cuenta desde el momento del diseño. Este estándar reconoce que el cambio ocurre y lo tiene en cuenta en sus recomendaciones para el diseño de las canalizaciones de telecomunicaciones.
- Los sistemas de telecomunicaciones son dinámicos. Durante la existencia de un edificio, las tecnologías y los equipos de telecomunicaciones pueden cambian dramáticamente. Este estándar reconoce este hecho siendo tan independiente como sea posible de proveedores y tecnologías de equipo.

- Telecomunicaciones es más que “voz y datos”. El concepto de telecomunicaciones también incorpora otros sistemas tales como control ambiental, seguridad, audio, televisión, alarmas y sonido. De hecho, incorpora todos los sistemas de “bajo voltaje” que transportan información en los edificios.

Es de fundamental importancia entender que para que un edificio quede exitosamente diseñado, construido y equipado para soportar los requerimientos actuales y futuros de los sistemas de telecomunicaciones, es necesario que el diseño de las telecomunicaciones se incorpore, idealmente, durante la fase preliminar de diseño arquitectónico. El estándar identifica seis componentes en la infraestructura edilicia como puede verse en la Figura 8.7.

1. Entradas de servicios
2. Instalaciones de entrada
3. Sala de equipos
4. Canalizaciones de montantes (backbone)
5. Armarios de telecomunicaciones
6. Canalizaciones horizontales
7. Áreas de trabajo
8. Interconexión entre edificios

Figura 8.7: Infraestructura edilicia según EIA/TIA 569A.

8.2.2. Instalaciones de entrada

Se define como el lugar en el que ingresan los servicios de telecomunicaciones al edificio y/o dónde llegan las canalizaciones de interconexión con otros edificios de la misma corporación. Las instalaciones de entrada pueden contener dispositivos de interfaz con las redes públicas prestadoras de servicios de telecomunicaciones, y también equipos de telecomunicaciones. Estas interfaces pueden incluir borneras (por ejemplo telefónicas) y equipos activos (por ejemplo módems).

El estándar recomienda que la ubicación de las instalaciones de entrada, sean en lugares secos, cercanos a las canalizaciones de montantes verticales (backbone).

8.2.3. Salas de Equipos

Se define como el espacio dónde se ubican los equipos de telecomunicaciones comunes al edificio. Estos equipos pueden incluir centrales telefónicas (PBX), equipos informáticos (servidores), centrales de vídeo, etc. Sólo se admiten equipos directamente relacionados con los sistemas de telecomunicaciones. En el diseño y ubicación de la sala de equipos, se deben considerar:

- Posibilidades de expansión. Es recomendable prever el crecimiento en los equipos que irán ubicados en la sala de equipos, y prever la posibilidad de expansión de la sala.
- Evitar ubicar la sala de equipos en lugar dónde puede haber filtraciones de agua, ya sea por el techo o por las paredes
- Facilidades de acceso para equipos de gran tamaño.
- La estimación de espacio para esta sala es de 0.07 m2 por cada 10 m2 de área utilizable del edificio. (Si no se dispone de mejores datos, se puede estimar el área utilizable como el 75 % del área total). Es recomendable que esté ubicada cerca de las canalizaciones montantes, ya que a la sala de equipos llegan generalmente una cantidad considerable de cables desde estas canalizaciones.
- Otras consideraciones deben tenerse en cuenta:
    - Fuentes de interferencia electromagnética.
    - Vibraciones.
    - Altura adecuada.
    - Iluminación.
    - Consumo eléctrico.
    - Prevención de incendios.
    - Puestas a tierra.

8.2.4. Canalizaciones de troncal

- Tener en cuenta las tomas a tierra según código y ANSI/TIA/EIA-607
- Diseñar para manejar medios reconocidos tal como se especifican en ANSI/TIA/EIA-568-A "Cableado de Telecomunicaciones para Edificios Comerciales".
- No permitir en ductos de ascensores
- Instalarlas en sitios secos

Se distinguen dos tipos de canalizaciones de troncal: canalizaciones externas, (entre edificios) y canalizaciones internas al edificio.

8.2.5. Canalizaciones internas

Las canalizaciones internas del troncal, generalmente llamadas montantes son las que vinculan las instalaciones de entrada, con la sala de equipos, y la esta con los armarios de telecomunicaciones. Estas canalizaciones pueden ser ductos, bandejas, escalerillas porta cables, etc. Las canalizaciones montantes pueden ser físicamente verticales u horizontales.

8.2.6. Armarios de telecomunicaciones

Los armarios o salas de telecomunicaciones se definen como los espacios que actúan como punto de transición entre las "montantes" verticales y las canalizaciones de distribución horizontal. Estos armarios o salas generalmente contienen puntos de terminación e interconexión de cableado, equipamiento de control y equipamiento de telecomunicaciones (típicamente equipos activos de datos, como por ejemplo hubs o switches). No se recomienda compartir el armario de telecomunicaciones con equipamiento de energía.

La ubicación ideal de los armarios de telecomunicaciones es en el centro del área a la que deben prestar servicio. Se recomienda disponer de por lo menos un armario de telecomunicaciones por piso. En los siguientes casos se requiere de más de un armario de telecomunicaciones por piso:

- Si el área a servir es mayor a 1000 m2. En ese caso, se recomienda un armario de telecomunicaciones por cada 1000 m2 de área utilizable.
- Dado que la distancia de las canalizaciones de distribución horizontal desde el armario de telecomunicaciones hasta las áreas de trabajo no puede superar en ningún caso los 90 m. (nuevamente: [568-B] en la sección 11.2.4.3.2 "Length requirements") Si algún área de trabajo se encuentra a mayor distancia del armario de telecomunicaciones, debe proveerse otro armario de telecomunicaciones, para cumplir con este requerimiento.

Si es necesario disponer de más de un armario de telecomunicaciones en un mismo piso, se recomienda interconectar los armarios de telecomunicaciones con canalizaciones del tipo montante.

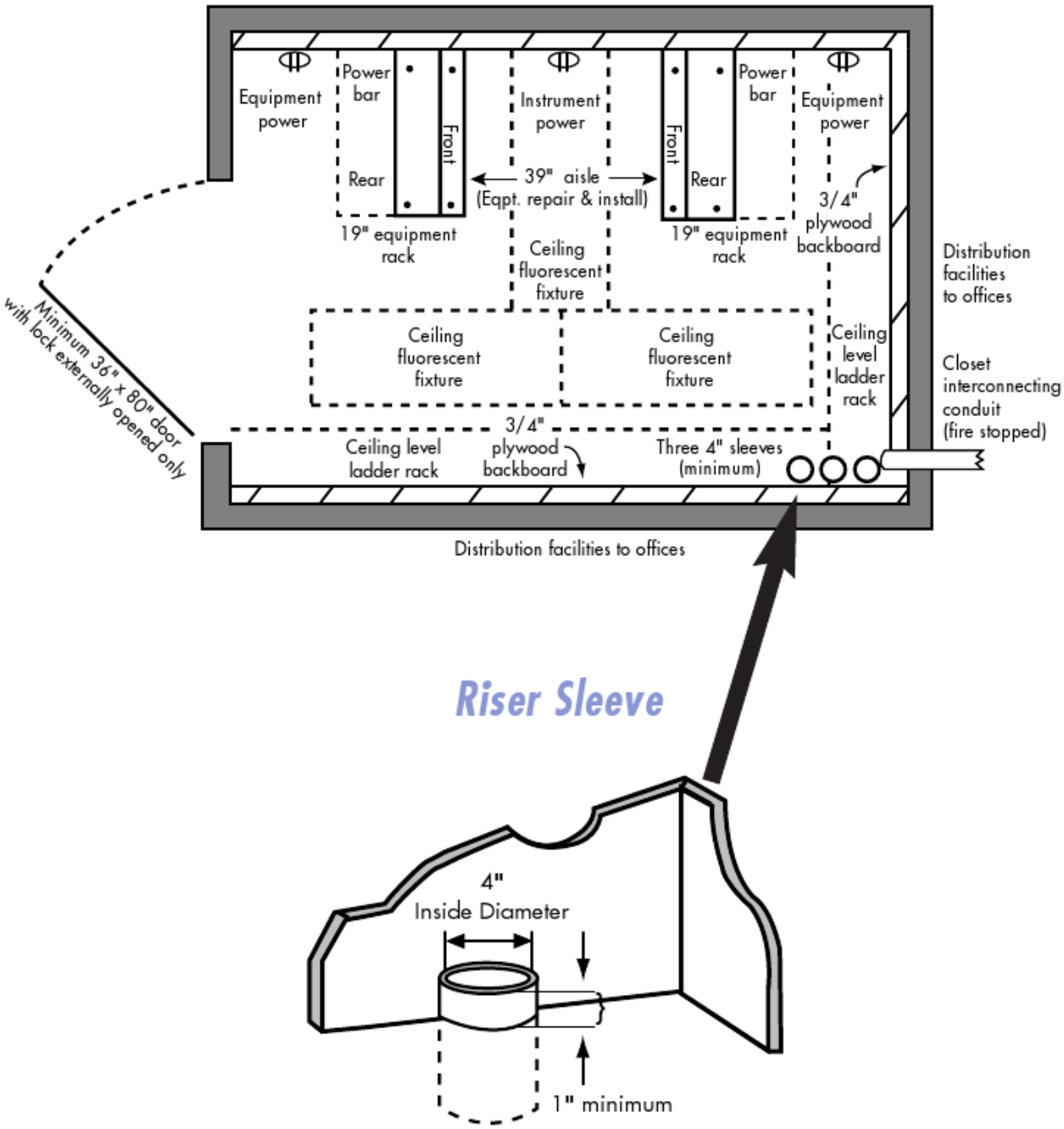


Figura 8.8: Estructura recomendada para los armarios de telecomunicaciones según EIA/TIA 569A.

Los armarios de telecomunicaciones deben estar apropiadamente iluminados. Se recomienda que el piso, las paredes y el techo sean de colores claros (preferiblemente blanco), para mejorar la iluminación. No debe tener cielorraso. Es recomendable disponer de sobre piso, o piso elevado. Se deben tener en cuenta los requerimientos eléctricos de los equipos de telecomunicaciones que se instalarán en estos armarios. En algunos casos, es recomendable disponer de paneles eléctricos propios para los armarios de telecomunicaciones. Todas los accesos de las canalizaciones a las salas de telecomunicaciones deben estar selladas con los materiales ignífugos adecuados. Es

recomendable disponer de ventilación y/o aire acondicionado de acuerdo a las características de los equipos que se instalarán en estos lugares.

8.2.7. Canalizaciones horizontales

Las canalizaciones horizontales son aquellas que vinculan los armarios de telecomunicaciones con las áreas de trabajo. Estas canalizaciones deben ser diseñadas para soportar los tipos de cables recomendados en la norma EIA/TIA 568, entre los que se incluyen el cable UTP de 4 pares, el cable STP y la fibra óptica.

Tipos de Canalizaciones

El estándar EIA/TIA-569 admite los siguientes tipos de canalizaciones horizontales:

Ductos bajo piso: En estos casos los ductos son parte de la obra civil. Bajo el piso se puede realizar una malla de ductos, disponiendo de líneas determinadas para telecomunicaciones, energía, etc. En las áreas de trabajo se dispone de puntos de acceso a los ductos bajo piso, utilizando torretas u otro tipo de accesorios. Como regla general, debe proveerse una sección de 650 mm2 por cada área de trabajo de 3 puestos que alimente el ducto.

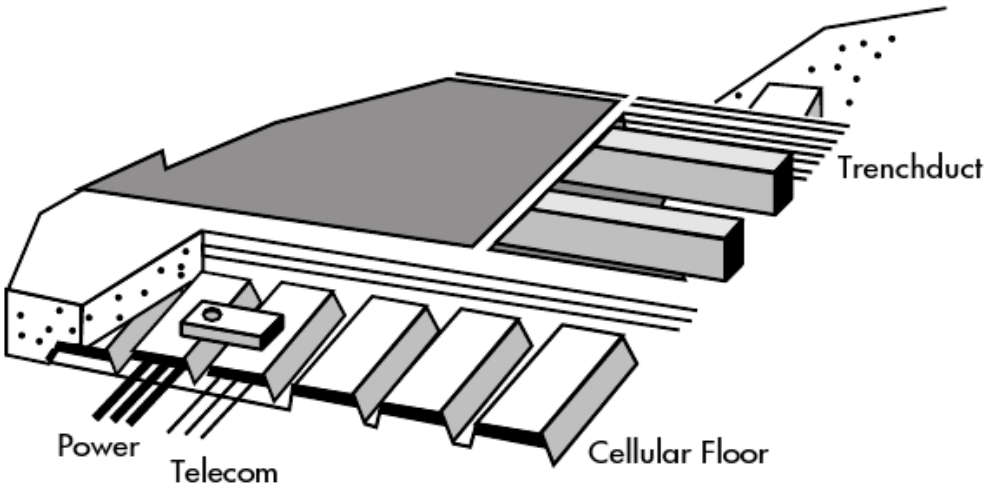


Figura 8.9: Esquema de los ductos bajo piso

Ductos bajo piso elevado: Los pisos elevados consisten en un sistema de soportes sobre el que apoyan lozas generalmente cuadradas. Son generalmente utilizados en salas de equipos. Sin embargo pueden ser también utilizados para oficinas. Debajo de este sistema de soportes puede ser instalado un sistema de ductos para cableado de telecomunicaciones, de energía, etc. No se recomienda tender cables sueltos debajo del piso elevado. Las lozas de los pisos elevados deben ser perforadas en los lugares correspondientes a las áreas de trabajo, y sobre éstas perforaciones se deben ubicar torretas u otro tipo de accesorios

adecuados para la terminación de los cables. Existen varios tipos de estos accesorios, algunos de los cuales quedan a ras del piso.

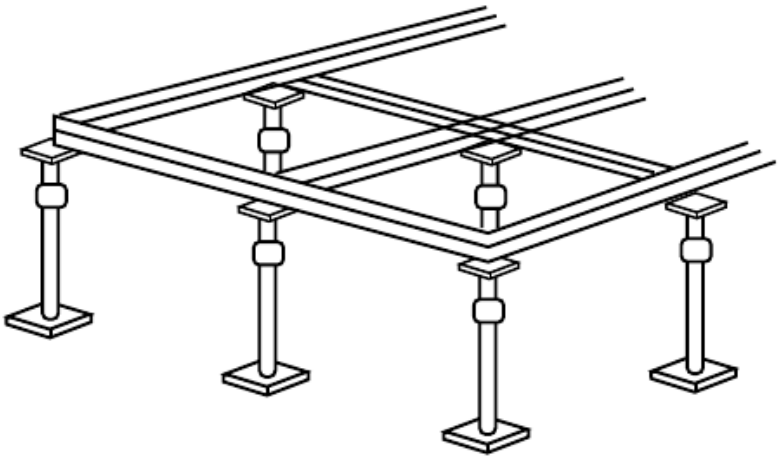


Figura 8.10: Esquema de los ductos bajo piso elevado.

Ductos aparentes: Los ductos aparentes pueden ser metálicos o de PVC, rígidos en ambos casos. No se recomiendan ductos flexibles para las canalizaciones horizontales. Las características de estos ductos y de su instalación deben ser acordes a los requisitos arquitectónicos y edilicios. Se recomienda que no existan tramos mayores a 30 metros sin puntos de registro e inspección, y que no existan más de dos quiebres de 90 grados en cada tramo.

Figura 8.11: Esquema de los ductos aparentes ("Cable canal").

Bandejas porta cables: Las bandejas porta cables consisten en estructuras rígidas, metálicas

o de PVC, generalmente de sección rectangular (en forma de U). La base y las paredes laterales pueden ser sólidas o caladas. Las bandejas de este tipo pueden o no tener tapa. Las bandejas se instalan generalmente sobre el cielorraso, aunque pueden ser instaladas debajo del cielorraso, o adosadas a las paredes.

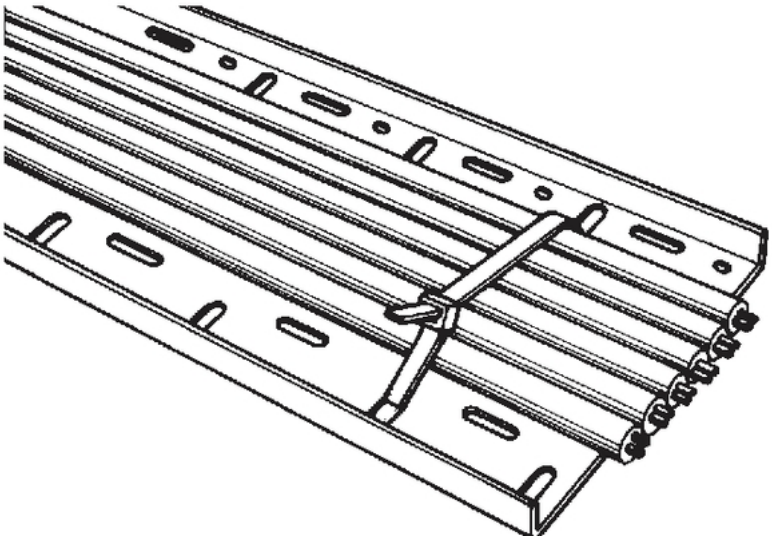


Figura 8.12: Esquema de las bandejas porta cables.

Secciones de las canalizaciones

Las secciones de las canalizaciones horizontales dependen de la cantidad de cables que deben alojar y del diámetro externo de los mismos. En el diseño se debe recordar que cada área de trabajo debe disponer por lo menos de dos cables UTP (típicamente de diámetro entre 4.5 y 5.5 mm). Asimismo se debe tener en cuenta el crecimiento futuro, dejando espacio en las canalizaciones para cables adicionales. En el Cuadro 8.2 se pueden calcular las secciones de canalizaciones necesarias en función de la cantidad de cables y su diámetro, para un factor de llenado estándar. Los valores que no están en letra negrita, indican la cantidad de cables recomendados.

Diámetro interno de la canalización		**Diámetro externo del cable (mm)**				
Denominación del ducto		**3,3**	**4,6**	**5,6**	**6,1**	**7,4**
(milímetros)	**(pulgadas)**					
15,8	1/2	1	1	0	0	0
20,9	3/4	6	5	4	3	2
26,6	1	8	8	7	6	3
35,1	1 1/4	16	14	12	10	6
40,9	1 1/2	20	18	16	15	7
52,5	2	30	26	22	20	14
62,7	2 1/2	45	40	36	30	17
77,9	3	70	60	50	40	20

Cuadro 8.2: Canalizaciones en función del número de cables.

8.2.8. Otros estándares que deben observarse aparte del tratado aquí:

ANSI/TIA/EIA-607 Grounding and bonding requirements for Telecommunication in commercial buildings

ANSI/TIA/EIA-606 Administrations Standard for Telecommunication Infrastructure of Commercial Buildings

ANSI/TIA/EIA-568-A Commercial Building Telecommunication Cabling Standards (Categorías 5 y 5e)

ANSI/TIA/EIA-568-B Commercial Building Telecommunication Cabling Standards (Categoría 6)

8.3. IEEE 802.3

A continuación se especifican un resumen de las características más importantes de la tecnología Ethernet:

Tecnología	**Capacidad**	**Medio**	**Dist. máx.**	**Topología**
10Base2	$10Mbps$	Coaxial	$185m$	Bus (Conector T)
10BaseT	$10Mbps$	Par Trenzado	$100m$	Estrella
10BaseF	$10Mbps$	Fibra óptica	$2000m$	Estrella
100BaseT4	$100Mbps$	Par Trenzado (Cat 3)	$100m$	Estr., Half y Full Duplex
100BaseTX	$100Mbps$	Par Trenzado (Cat 5)	$100m$	Estr., Half y Full Duplex
100BaseFX	$100Mbps$	Fibra óptica	$2000m$	No permite el uso de hubs
1000BaseT	$1000Mbps$	4 pares trenz. (Cat 5/6)	$100m$	Estrella. Full Duplex
1000BaseSX	$1000Mbps$	Fibra óptica (multimodo)	$5504m$	Estrella. Full Duplex
1000BaseLX	$1000Mbps$	Fibra óptica (monomodo)	$5000m$	Estrella. Full Duplex

Cuadro 8.3: Resumen tecnologías Ethernet

8.3.1. IEEE 802.3af

Es el estándar de Power Over the Ethernet, PoE permite la entrega de energía DC sobre el mismo cable de cobre de Ethernet, esto permite la posibilidad de integrar nuevos dispositivos de energía adjuntos a la red a su infraestructura LAN existente, evitando así el tendido de cable de energía o el uso de fuentes de alimentación para alimentar los dispositivos. Entre los dispositivos que pueden alimentarse utilizando PoE podemos encontrarnos APs, Camaras IP y teléfonos IP entre otros.

8.4. Voz y Vídeo sobre IP

Wi-Fi define especificaciones para la capa física y la subcapa MAC, la subcapa LLC es la encargada de la convergencia entre la MAC y las capas superiores, es decir, el tipo de información

que se encapsula en capas superiores es transparente para la MAC de Wi-Fi, y el medio usado para la transmisión es imperceptible para las capas superiores. Las aplicaciones tanto de datos, voz, y vídeo se encapsulan en las capas superiores, por lo cual para Wi-Fi el tipo de información es transparente, sin embargo, se debe tomar muy en cuenta que las aplicaciones en tiempo real no soportan retardos, por ello, tanto en capas superiores como en Wi-Fi se define un esquema de prioridades basados en los conceptos de calidad de servicio, además la MAC de Wi-Fi utiliza la funcionalidad PCF[21] para servicios que no toleran retardos.

8.4.1. Voz sobre IP

El concepto original de voz sobre IP es relativamente simple: se trata de transformar la voz en "paquetes de información" manejables por una red con protocolo de Internet (IP). La voz sobre IP convierte las señales de voz estándar en paquetes de datos comprimidos que son transportados a través de redes de datos en lugar de líneas telefónicas tradicionales. El desarrollo de la conmutación de paquetes en reemplazo de la conmutación de circuitos es una gran ventaja de la telefonía IP frente a la telefonía tradicional.

La voz sobre IP tiene una gran aceptación y desarrollo entre los usuarios, ésto por su bajo costo, el requerimiento de una estructura simple de comunicaciones, y por la posibilidad de ofrecer servicios de valor agregado como buzones y mensajería de voz. Sin embargo, la voz sobre Internet presenta desventajas frente a la telefonía clásica, la cual ofrece mayor calidad y la facilidad de ser utilizada por usuarios sin formación alguna para hacerlo.

La reducción de los costos en la telefonía sobre Internet se debe a que el sistema de encaminamiento y conmutación es más eficiente que las grandes centrales telefónicas, que necesitan un circuito por conversación, mientras que en la telefonía IP se puede enviar paquetes de varias conversaciones digitalizadas y comprimidas, transmitiéndolas como un flujo de datos multiplexando un único circuito físico, luego de haber establecido una sesión IP entre los terminales de usuarios, mismos que deben estar equipados con software compatible. Se puede establecer comunicación entre un teléfono y un computador, o bien entre dos teléfonos utilizando la red de Internet. En el primer caso es necesario disponer de un gateway con conexión por un lado a Internet y por otro a la red telefónica convencional), el gateway tiene las funcionalidades de digitalizar, comprimir y empaquetar la voz, además de realizar la traslación entre direcciones IP y números de la RTC. En el caso de llamadas entre dos teléfonos a través de Internet, es necesario un gateway en cada extremo realizando el mismo proceso.

Para asegurar calidad de voz, se debe considerar factores como:

Retardo o Latencia: Es el tiempo necesario para que un paquete o una trama de datos viajen desde la estación de origen a la de destino. La latencia, puede influir a tal punto de limitar el uso de redes de datos para transmisión de voz en ciertos entornos. El retardo entre los extremos, no puede ser superior a 150 milisegundos. El retardo o latencia se origina debido a causas como:

- Retardo de propagación.
- Retardo por elementos de red.
- Retardo por paquetización.

[21] Point Coordination Function

Jitter y Buffering: Son producidos principalmente por congestiones de red y de los sistemas de comunicaciones. El jitter se refiere a la desincronización de fase de los bits, mientras que el buffering a la fluctuación del retardo de tránsito entre los extremos.

Pérdida de Paquetes: Se debe a que las comunicaciones de voz en redes IP suelen utilizar en lugar de TCP el protocolo UDP en la capa de transporte, y UDP no admite retransmisiones en de tramas perdidas. La causa más frecuente es la congestión en algún segmento de red, o en algún equipo de la misma.

Roaming: Es un parámetro específico de las redes inalámbricas, se refiere a garantizar la movilidad de los usuarios sin perder la conexión a la red. Los usuarios tendrán ocasionalmente que cambiarse de zona de cobertura, en Wi-Fi la reasociación de un usuario a otro punto de acceso fluctúa entre 250 y 500 milisegundos, actualmente se han logrado conseguir tiempos de hasta 100 milisegundos entre celdas Wi-Fi.

Método de Codificación: El método de codificación es un factor muy importante a tener en cuenta, pues dependiendo del codificador de voz utilizado, existen los diferentes hardware-software que descomprimen en menor o mayor grado, obteniendo una mayor o menor velocidad binaria. En el Cuadro 8.4 se muestran los diferentes algoritmos de codificación existentes y sus características de ancho de banda y MOS (Parámetro que mide la calidad de voz como resultado de la opinión media), el MOS se obtiene de una prueba denominada ACR[22] que consiste en realizar pruebas de audición a un grupo heterogéneo, quienes califican la calidad entre 1 y 5. Para la elección del CODEC, se debe considerar también el retardo que introduce cada algoritmo en el esquema global y el MOS.

Algoritmo	**BW**	**Tiempo de muestreo**	**BW típico IP**	**MOS**
G711 (PCM)	$64kbps$	$0.125ms$	$80kbps$	4.1
G723.1 (ACELP)	$5.6kbps$	$30ms$	$16.27kbps$	3.65
G723.2 (ACELP)	$6.4kbps$	$30ms$	$17.07kbps$	3.9
G726 (ADPCM)	$32kbps$	$0.125ms$	$48kbps$	3.85
G728 (LD-CELP)	$16kbps$	$0.625ms$	$32kbps$	3.61
G729.a (CS-ACELP)	$8kbps$	$10ms$	$24kbps$	3.92

Cuadro 8.4: Ancho de banda requerido por los diferentes codificadores

Ancho de Banda: En el caso de Wi-Fi se tiene $11Mbps$ o 54 M$Mbps$ capacidad suficiente para las distintas aplicaciones de un gran número de usuarios. Dependerá del análisis de dimensionamiento de la red el estándar que se escoja. Otra opción para optimizar el ancho de banda es utilizar codificadores de alta velocidad, pese a se pierde nitidez en la voz, ésta no pierde lo entendible, manteniendo una calidad aceptable.

8.4.2. Vídeo sobre IP

Las señales de vídeo tradicionales se basan en tecnología analógica. Las técnicas de compresión, permiten transportar las señales compuestas de audio y vídeo sobre redes típicas de

[22] Absolute Category Rating

datos que usan IP como protocolo de red. Vídeo sobre IP es una tecnología que permite que las señales de vídeo sean capturadas, digitalizadas, secuenciadas, administradas y transmitidas sobre redes IP.

Primeramente se captura el contenido de vídeo, éste es procesado, comprimido, almacenado y editado en un servidor de vídeo. El contenido de vídeo puede ser capturado y registrado en tiempo real o prerregistrado y almacenado. Las transmisiones de vídeo son enviadas a la red para visualizarse en una o varias estaciones, las que deben disponer de hardware y software de visualización de vídeo. El vídeo sobre IP abarca tres categorías que son: VoD[23], VCoIP[24], y VBoIP[25].

VoD

El vídeo bajo demanda o VoD permite a un usuario acceder a una determinada secuencia de vídeo almacenada en un servidor, o a una visualización en tiempo real. El usuario tiene el control del vídeo, pudiendo iniciar, detener, adelantar, o retroceder la reproducción. El servicio es interactivo. VoD se utiliza para capacitaciones, mercadeo, entre otras en las cuales el usuario puede visualizar los archivos cuando lo requiera.

VCoIP

.

Es una combinación full dúplex de transmisiones de audio y vídeo, virtualmente es una conversación frente a frente entre usuarios geográficamente alejados. Cada terminal debe estar equipado con micrófono, cámara, software y hardware para reproducción de vídeo y parlantes, para la captura y reproducción del vídeo. Las aplicaciones de videoconferencia son en tiempo real y por lo general no se almacenan. VCoIP se aplica en comunicaciones corporativas principalmente.

VBoIP

Se trata de una transmisión unidireccional de vídeo. Los puntos terminales son simples visualizadores pasivos sin control sobre la sesión. Una transmisión de este tipo puede ser Unicast o Multicast desde el servidor. En una transmisión Unicast, el servidor hace una réplica de la transmisión para cada visualizador terminal, mientras que en una configuración Multicast, la misma señal es enviada sobre la red como una sola transmisión hacia varios puntos terminales. Sus aplicaciones principales son en ambientes corporativos y educativos para capacitaciones, discursos, entre otras.

8.4.3. Protocolos de voz y vídeo sobre IP

Para optimizar un sistema de comunicación de voz y/o vídeo, existen dos protocolos, los cuales garantizan la interoperabilidad entre la red telefónica y las redes de transmisión de datos en el caso VoIP. Estos protocolos son el protocolo H.323 y el protocolo de inicio de sesión SIP.

[23] Video on Demand
[24] Video Conference over IP
[25] Video Broadcasting over IP

Protocolo H323

Hace referencia a la recomendación ITU–T H.323. Es un protocolo para la transmisión en tiempo real de audio, vídeo, y comunicaciones de datos sobre redes paquetizadas. En H.323 se definen los siguientes elementos:

Terminales: Usadas para la comunicación multimedia bidireccional. Puede ser un cualquier dispositivo que soporte aplicaciones multimedia, como por ejemplo un computador personal.

Gateways: Sirven para conectar redes distintas proporcionando compatibilidad con otras tecnologías, por ejemplo las redes telefónicas tradicionales.

Gatekeepers: Es el encargado de controlar una zona H.323, que es el conjunto de dispositivos administrativamente definidos, regula el proceso de llamadas proveyendo servicios como direccionamiento, autorización y autenticación de terminales.

Unidades de Control Multipunto (MCU): Es la combinación de dos componentes fundamentales: Controlador Multipunto y Procesador Multipunto, mismos que proveen soporte para las comunicaciones multipunto entre terminales H.323.

La Figura 8.13 muestra los elementos definidos en H.323.

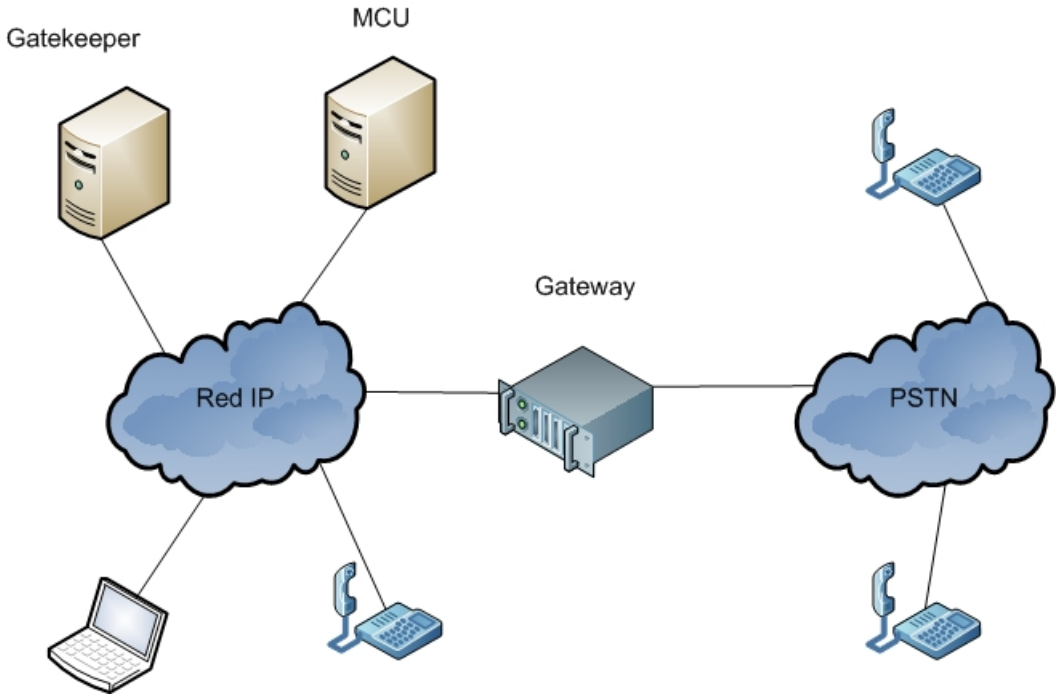


Figura 8.13: Arquitectura H.323

SIP

El protocolo SIP fue desarrollado por el grupo IETF[26]. Es un protocolo de control de capa de aplicación que puede establecer, modificar, y terminar llamadas o sesiones multimedia. SIP

[26]International Engineering Task Force

define los siguientes elementos que pueden estar dentro de un mismo hardware:

SIP User Agents (UAS): Son los terminales de usuarios, los cuales son usados para crear y administrar una sesión SIP. El User Agent Client (UAC) inicia los mensajes, y el User Agent Server (UAS) responde a dichos mensajes.

SIP Register Servers: Son bases de datos que contienen la ubicación de todos los UAS en un dominio.

SIP Proxy Servers: Acepta las solicitudes de sesión realizadas por un SIP UA y realiza una petición a la base de datos para obtener la información de direccionamiento.

SIP Redirect Servers: Devuelve la URL-SIP, donde la Terminal llamada es visible.

La Figura 8.14 muestra los elementos definidos en SIP.

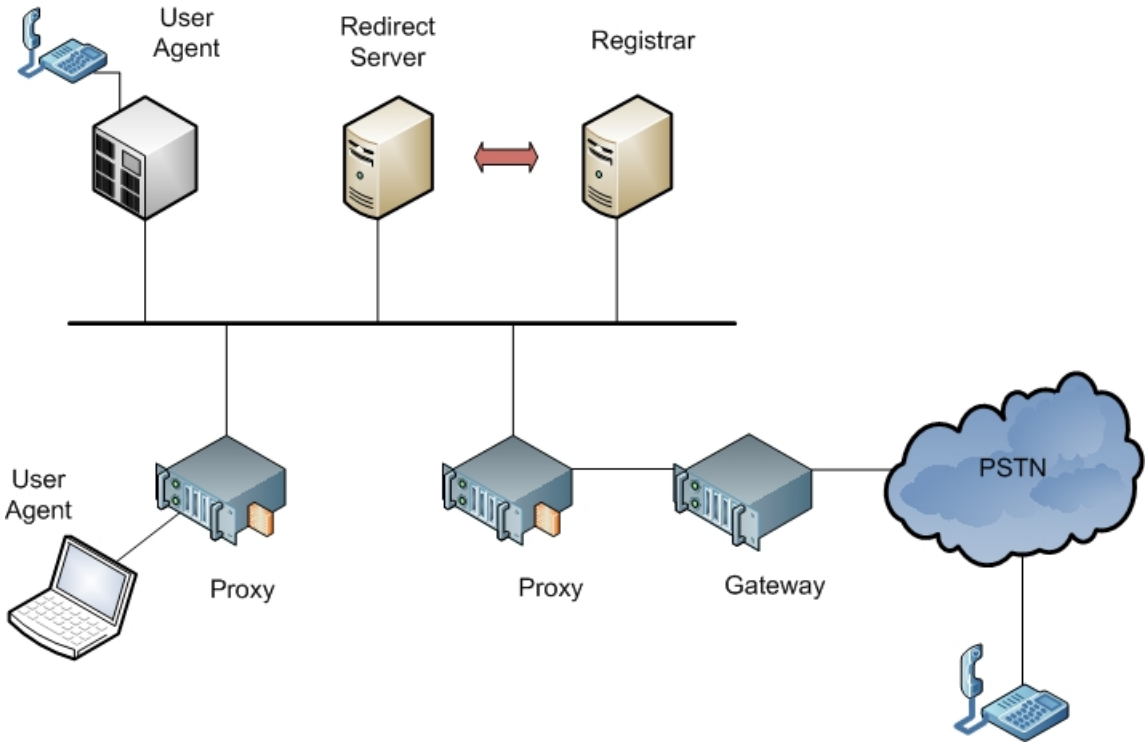


Figura 8.14: Arquitectura SIP

SIP Vs H.323

Ambos protocolos presentan diferencias, mismas que sirven para escoger el protocolo que mas se ajuste a las necesidades de la red. Las diferencias entre SIP y H.323 se resumen en el Cuadro 8.5.

Descripción	SIP	H.323
Codificación.	Textual.	Binaria
Formatos.	Tipos MIME-IANA.	Series G.XXX y H.XXX, MPEG, GSM
Servidores.	Proxy, redirect y registro.	Gatekeeper.
Autenticación.	Análogo a http.	H.235
Localización.	DNS.	Gatekeeper (puede usar DNS)
Transporte.	TCP, UDP SCTP, CDP, etc.	TCP, UDP
Cliente.	User Agent.	Terminal H.323
QoS.	Delegada a otros protocolos.	Soportada por el Gatekeeper
Complejidad.	Similar a http.	Uso de un conjunto de protocolos distintos

Cuadro 8.5: Comparación H.323-SIP

8.5. IEEE 802.1Q - VLANs

8.5.1. Introducción a las VLANs

Las VLANs [27] segmentan lógicamente las redes, basándose en funciones, equipos de trabajo, o aplicaciones de una organización, sin importar la ubicación física o las conexiones de la red. Todas las estaciones de trabajo y los servers utilizados por un grupo particular, comparten la misma VLAN, sin importar la ubicación física o las conexiones de la red. Una estación de trabajo dentro de una VLAN tiene comunicación restringida a los servidores de archivos dentro de la misma VLAN. Las VLANs funcionan mediante la división lógica de la red en diferentes dominios de broadcast para que los paquetes solo sean switcheados entre los puertos designados para la misma VLAN. Los routers en una red con topología VLAN proveen filtrado de broadcast, seguridad, y manejo del tráfico.

[27] Virtual Local Area Network.

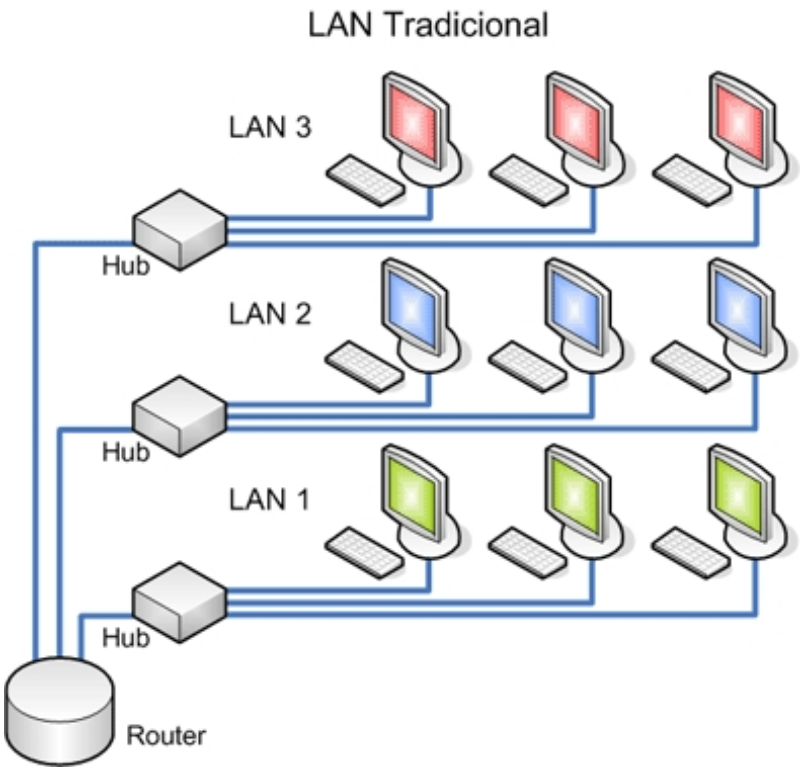


Figura 8.15: Arquitectura sin el uso de VLAN.

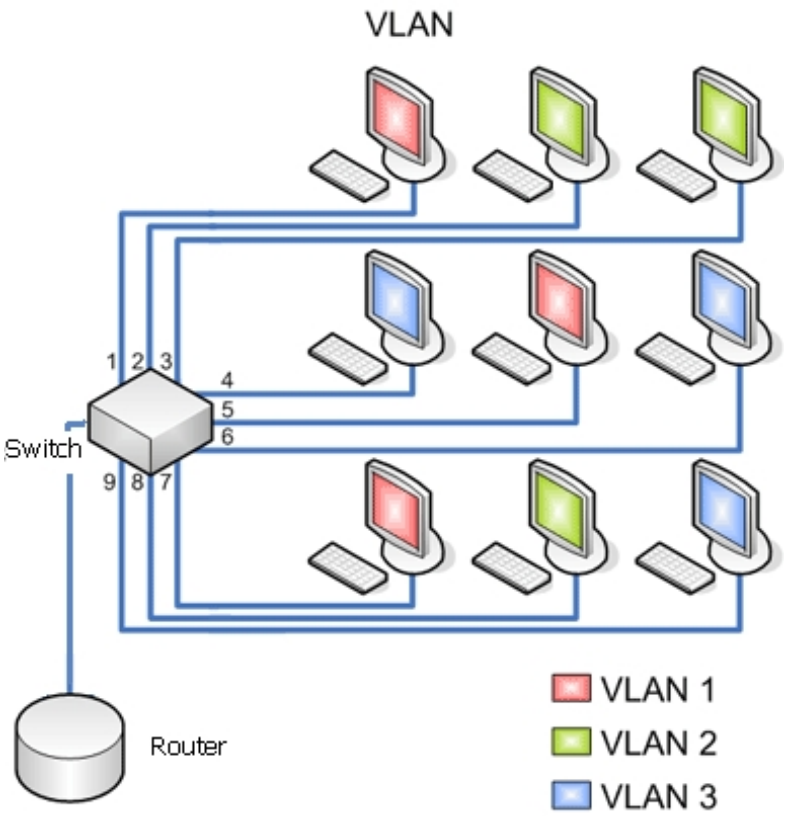


Figura 8.16: Arquitectura con VLAN.

Con el uso de VLANs se logra:

- Escalabilidad, seguridad, y manejo de la red.
- Los switches dirigen tráfico entre VLANs, de no ser así se violaría la integridad de los dominios de broadcast de la VLAN.
- El tráfico solo debe ser ruteado entre VLANs

Implementar VLANs en un switch trae aparejadas las siguientes consecuencias:

- El switch mantiene una tabla de switching separada para cada VLAN.
- Si un frame llega al switch por un puerto de la VLAN 1, el switch busca la tabla de switching para la VLAN 1.
- Cuando es recibido el frame, el switch agrega la dirección de donde vino a la tabla de ruteo, si es que la misma no se conocía.
- Se chequea en la tabla la dirección destino para poder realizar una decisión de forwarding.
- Para realizar el forwarding y crear las tablas, la búsqueda se realiza solo en la tabla de la VLAN.

8.5.2. Operación de las VLANs

Cada puerto del switch puede ser asignado a una VLAN diferente. Los puertos asignados a la misma VLAN comparten dominios de broadcast. Por contrario, los puertos que no pertenecen a esa VLAN no comparten dominios de broadcast.

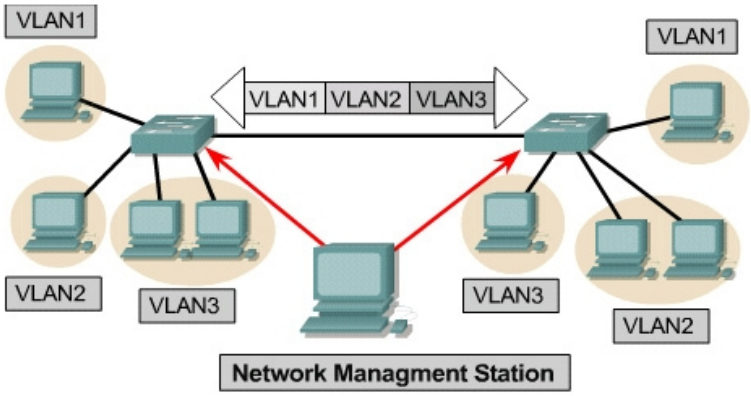


Figura 8.17: Funcionamiento con VLAN.

El beneficio clave de las VLANs es que permiten al administrador de red, organizar la LAN lógicamente en vez de físicamente. De esa forma, los usuarios en un mismo segmento comparten el ancho de banda del mismo. Cada usuario agregado al segmente representa una disminución en el ancho de banda, lo que resulta en una degradación de la "performance" de la red. Por lo tanto, las VLANs ofrecen mayor ancho de banda a los usuarios que una red compartida ya que disminuyen la cantidad de dominios de colisión por switch. La VLAN por default para cada puerto del switch es la VLAN de administración, la misma suele ser la VLAN número 1, y no debe borrarse. Las VLANs dinámicas permiten pertenecer a la misma VLAN basándose en la MAC address del dispositivo conectado al puerto del switch. Cuando un dispositivo ingresa en la red consulta en la base de datos del switch para saber a que VLAN pertenece. El encabezado de la trama es encapsulado o modificado con una identificación de VLAN, antes de que la trama sea enviada entre switches. Luego, antes de reenviar la trama hacia el dispositivo de destino, el encabezado es modificado al formato original.

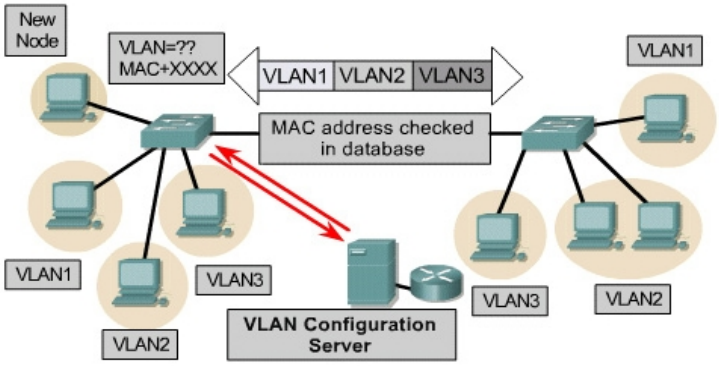


Figura 8.18: Consulta de un paquete al switch para determinar a que VLAN pertenece.

Existen tres tipos de VLAN según como sea asignado el control de paquetes (ver Figura 8.19)

- VLANs basadas en puertos
- Basadas en direcciones MAC o VLAN geográficas
- VLANs basadas en protocolos de capa 3

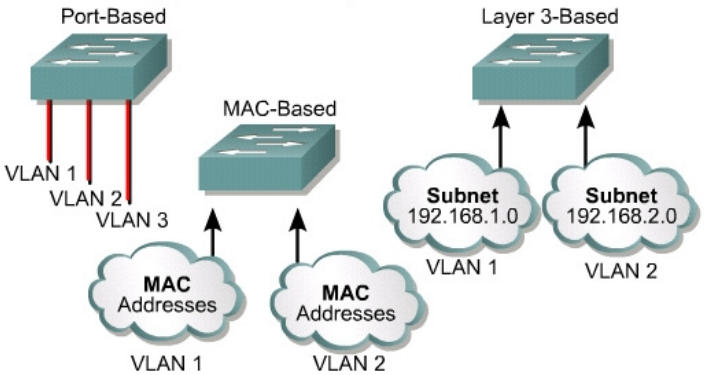


Figura 8.19: Tipos de VLAN según el método de acceso.

En una VLAN con membresía basada en puertos, el puerto es asignado a la VLAN sin importar el dispositivo o sistema que se conecte al mismo. Por lo tanto, todos los usuarios del mismo port, deberán estar conectados a la misma VLAN. Esta es una forma un poco rústica y poco segura de formar VLAN, sin embargo es una de las más utilizadas ya que es la más fácil de configurar.

8.5.3. Principios de las VLANs

En un entorno con switches, cada estación verá solamente el tráfico destinado hacia ella. El switch filtra el tráfico en la red para que la estación tenga disponible todo el ancho de banda para enviar o recibir tráfico. En un sistema compartido con un hub, solo una estación puede transmitir por vez. La red con switches permite muchas transmisiones simultáneas en el dominio de broadcast. Las VLANs pueden existir como redes de extremo a extremo o estar colocadas dentro de un entorno de asociación geográfica.

Una red VLAN de extremo a extremo tiene las siguientes características:

- Los usuarios son agrupados en VLANs acorde a un tipo de grupo o función de trabajo e independientes de su ubicación física.
- Si un usuario cambia su lugar de trabajo, debe seguir reconociéndose como perteneciente a la misma VLAN sin cambios.
- Cada VLAN tiene una misma configuración de seguridad para todos sus miembros.

VLANs estáticas y dinámicas

Las VLANs estáticas tienen puertos configurados manualmente en un switch. Estos puertos mantienen su configuración hasta que sea cambiada nuevamente en forma manual. Las funciones de VLAN dinámicas están basadas en la utilización de direcciones MAC. El switch esta preprogramado con las direcciones de MAC y número de VLAN y pueden reconocer cuando se muda una estación (gracias a la dirección de MAC) reconfigurando el nuevo port.

VLANs Geográficas

Cuando las redes corporativas deben ser mudadas para centralizar recursos, las redes de extremo a extremo se vuelven difíciles de mantener. Los usuarios necesitan utilizar recursos que ya no se encuentran dentro de su VLAN. Debido a este cambio de lugar de trabajo y utilización de recursos, las VLANs son más comúnmente creadas por fronteras geográficas que por fronteras por funciones o grupos.

8.5.4. Normas de VLANs

Uno de los requisitos más importantes de las VLANs es la posibilidad de identificar qué paquetes pertenecen a cada VLAN. En los primeros días de las VLANs, cada proveedor tenía sus propios métodos de hacer esto ya que no existían estándares en la industria. Pero cuando se necesitaba integrar redes de diferentes proveedores surgían problemas de incompatibilidades. Algunas marcas modificaron sus equipos para admitir normas de su competencia.

Algunas de las normas propias de cada marca fueron las siguientes:

- 802.10 (Cisco) - El servicio 802,10 es un mecanismo propietario utilizado por Cisco para multiplexación de grupos para troncales sobre FDDI (Fiber Distributed Data Interface).
- ISL (Cisco) - Inter-Switch Link es un protocolo propietario de Cisco que mantiene la información de VLAN como tráfico que fluye entre routers y switches en una red de ethernet.
- Secure Fast packet Switching (Cabletron / Enterasys) - Esta es una tecnología de switching orientada a conexión.
- AutoTracker (Alcatel) – Protocolo desarrollado por Alcatel

Las VLAN por protocolo de capa 3 casi se encuentran en desuso ya que actualmente casi la totalidad de las comunicaciones que pueden llegar a pasar por un switch son IP.

8.5.5. Norma 802.1Q

La necesidad de un verdadero estándar para lograr redes heterogéneas fue llevado a cabo cuando se armó un grupo para desarrollo de la norma 802.1Q. El comité para 802.1Q se encargo de desarrollar un método para permitir compatibilidades de diferentes marcas. La norma 802.1Q en un estándar de etiquetado que identifica la trama de cada VLAN. El gráfico 8.20 muestra como se realiza el etiquetado:

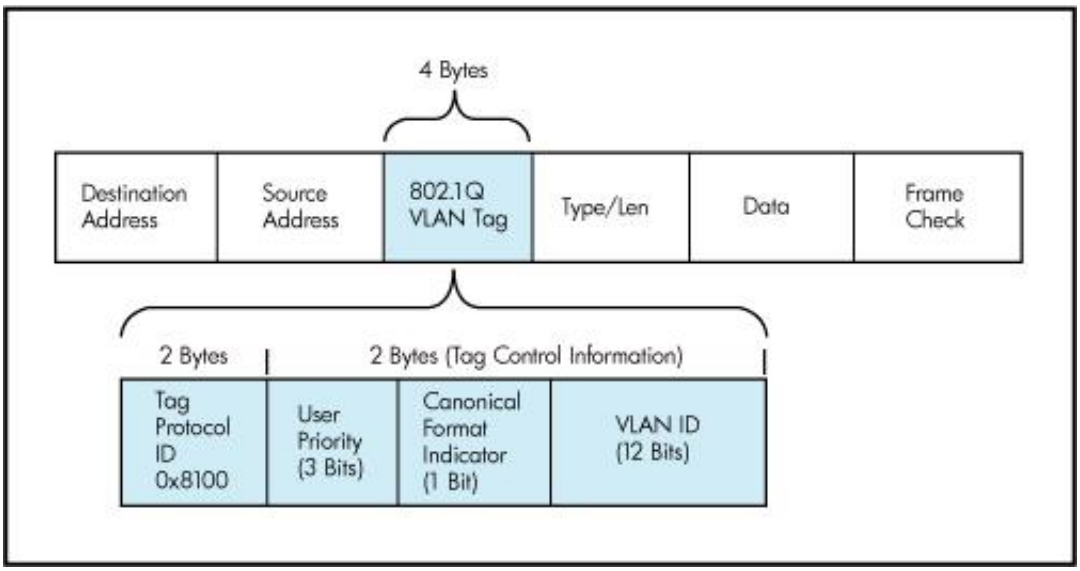


Figura 8.20: Trama Ethernet con tag de 802.1Q.

A cada trama se le agregan 4 bytes de datos. 2 bytes son llamados de Ethertype que identifican la trama como de etiquetado e indican que protocolo de trunking está siendo usado, 3 bits para información de 802.1p que identifican la prioridad en 8 niveles para cada VLAN, 12 bits que corresponden al ID de la VLAN utilizados para identificar la VLAN correspondiente. Y un último bit para identificar el tipo de direccionamiento utilizado.

8.6. LACP

LACP [28] es un protocolo que describe el uso de múltiples cables o puertos en paraleo para incrementar la velocidad del link pasando los límites de un sólo cable o puerto y para agregar redundancia incrementando así la fiabilidad.

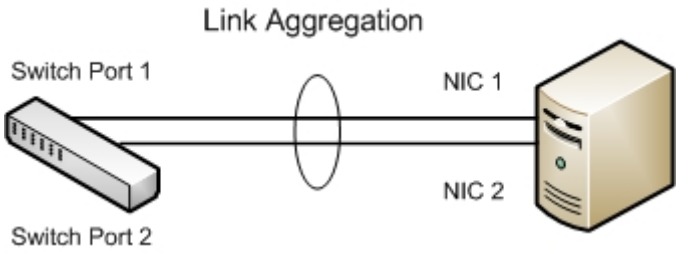


Figura 8.21: LACP entre un switch y un servidor.

8.6.1. Descripción del protocolo

LACP fue diseñado con el fin de superar dos problemas de las conexiones Ethernet:

- Limitaciones por ancho de banda.

[28] Link Aggregation Control Protocol

- Falta de redundancia.

El primer problema es debido a que el ancho de banda no se escala linealmente en Ethernet. Históricamente los anchos de banda de los enlaces han crecido en magnitud de un orden por generación: $10Mbps$, $100Mbps$, $1Gbps$, $10Gbps$, etc. En caso de necesitarse más velocidad el costo de pasar a la siguiente generación a veces es prohibitivo, no se encuentra desarrollado o no puede hacerse por otros factores como por ejemplo la distancia el enlace.

Una solución que se introdujo a principios de los años 1990 fue la de combinar dos o mas puertos como un solo puerto lógico. La mayoría de estas soluciones requerían de configuraciones manuales y tener equipamiento idéntico a ambos lados del enlace.

8.6.2. Link Aggregation estandarizado por IEEE:

Para mediados de los años 1990, la mayoría de los fabricantes de equipos para redes habían incluido la capacidad de incrementar el ancho de banda con algún protocolo propietario de Link Aggregation. El problema de esto fue que contribuyó a muchos problemas de compatibilidad entre elementos de la red. El grupo IEEE 802.3 tomó entonces la iniciativa de crear un estándar para solucionar este problema. Esto devino en el protocolo LACP conocido actualmente.

El protocolo LACP está incluido en la especificación de la IEEE como un método para el control de la unión de varios puertos físicos que forman un único canal lógico. LACP permite que la red negocie automáticamente la unión de los enlaces mandando paquetes LACP entre los equipos que se conectan.

LACP funciona mediante el envío de paquetes (LACPDUs) por todos los enlaces que han permitido el protocolo. Si un dispositivo está presente en el otro extremo del enlace, que también ha permitido LACP, se enviarán dichos paquetes a lo largo de los enlaces que unen las dos unidades para la detección de múltiples vínculos entre sí y luego combinarlos en un único vínculo lógico. LACP se puede configurar en uno de dos modos: activo o pasivo. En el modo activo siempre enviará paquetes por las interfaces configuradas. En modo pasivo sin embargo, se actúa de manera "contesto cuando se me habla", y por lo tanto puede ser utilizado como una forma para controlar la formación de bucles accidentales (siempre y cuando el otro dispositivo también esté en modo activo).

Se tienen algunas limitaciones ya que originalmente Link aggregation fue desarrollado para dar redundancia y no aumento de ancho de banda. El aumento de ancho de banda depende del método de balance de carga que se esté usando (existen diversos algoritmos de balance de carga). La forma más común de establecer el balance de carga es usar hash de capa 3. Estos hashes son calculados cuando la conexión es establecida y se mantiene en la memoria para el posterior uso. Esta es la razón por la que casi nunca se logra un balance 50-50. Alrededor de 70-30 es más usual. Los algoritmos mas avanzados de Link Aggregation usan un hash de capa 4 que acercan el balance a 50-50 mucho más.

Link Aggregation también permite aumentar la velocidad de backbone a medida que ésta va creciendo para suplir la demanda sin la necesidad de agregar más hardware

8.6.3. Eficiencia de LACP

LACP se vuelve ineficiente pasada cierta cantidad de enlaces unidos dada la cantidad de interfaces disponibles en el switch. Un switch de 24 interfaces usando 2 enlaces lógicos de 8 gigas

cada uno, totaliza 16 enlaces de sus puertos solo para 2 conexiones, dejando solo 8 interfaces más para otros usos. La misma configuración en un switch de 48 interfaces deja 32 libres para usarse por lo que los enlaces de 8 gigas serán usados mas eficientemente.

Cuando un 40 o 50 porciento de los puertos de un switch están siendo usados bajo LACP se considera que se está perdiendo eficiencia.

Otra limitación de LACP es que el grupo de interfaces que forman el enlace deben pertenecer al mismo equipo y deben ser del mismo tipo. No se pueden mezclar enlaces Fast Ethernet con Gigabit Ethernet por citar un ejemplo.

Capítulo 9

Ingeniería de detalle

9.1. Dispositivos de Comunicaciones

A continuación se enumerarán los dispositivos de comunicaciones más utilizados. Adicionalmente, para cada uno de ellos se detallarán los aspectos generales y de seguridad más relevantes.

9.1.1. Hub (Layer 1)

Dispositivo de comunicaciones sin "inteligencia"utilizado para amplificar y repetir señales a nivel físico.

9.1.2. Bridge (Layer 2)

Dispositivo que realiza "Store & Fordware", permitiéndole añadir inteligencia antes de reenviar el paquete. Es utilizado para segmentar redes, permite filtrar tráfico identificándolo por su dirección MAC. Utilizado para conectar redes LAN a una corta distancia.

9.1.3. Switch

Switch (Layer 2)

Un Switch Layer 2 es similar al bridge pero posee N interfaces y adicionalmente, posee capacidad de memorizar/priorizar tráfico. Es un dispositivo de comunicaciones que se encarga de segmentar e interconectar los segmentos de la red y por lo tanto permite eliminar el tráfico innecesario de los distintos segmentos.

Los switches de nivel 2 posibilitan múltiples transmisiones simultáneas sin interferir en otras sub-redes, es decir, separan dominios de colisión. Sin embargo no filtran broadcast, multicasts (en el caso en que más de una sub-red contenga las estaciones pertenecientes al grupo multicast de destino), ni tramas cuyo destino aún no haya sido incluido en la tabla de direccionamiento.

Dentro de un switch pueden agruparse lógicamente los diferentes puertos en distintas VLANs, con ello se logra que un switch esté dividido en N VLANs y éstas se comportarán como switches individuales. Luego por medio de un router externo se podrán intercambiar paquetes entre una VLAN y otra.

Es importante diseñar correctamente la implementación de las VLANs. Un error muy frecuente es que diferentes VLANs con diferentes niveles de seguridad estén compartidas en un mismo segmento de red. Esto violaría las recomendaciones de seguridad como se puede observar en la Figura 9.1.

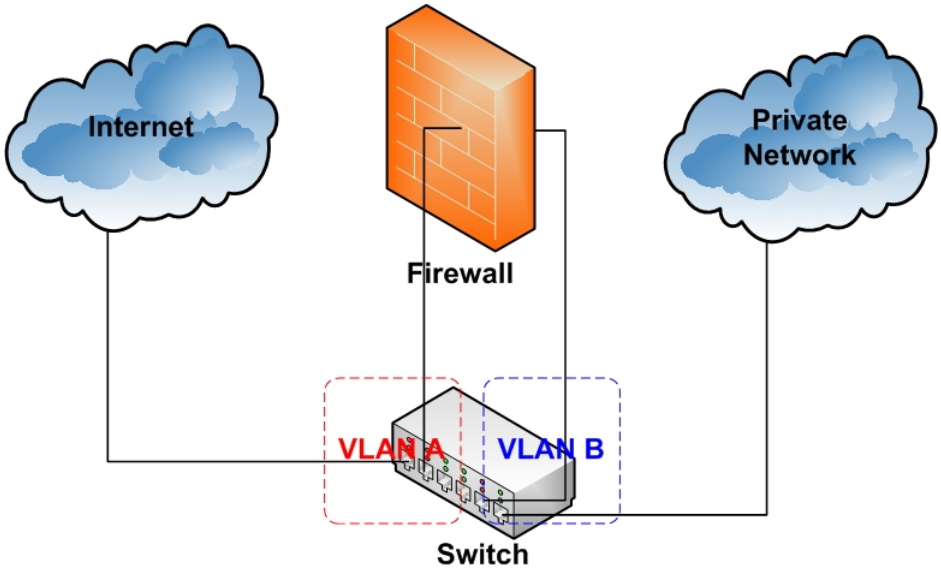


Figura 9.1: Mala política de utilización de VLANs.

Switch (Layer 3)

Son los switches que, además de las funciones tradicionales de la capa 2, incorporan algunas funciones de ruteo como por ejemplo la determinación del camino basado en informaciones de capa de red (capa 3 del modelo OSI), validación de la integridad del cableado de la capa 3 por checksum y soporte a los protocolos de routing tradicionales (RIP, OSPF, etc)

Los switches de capa 3 soportan también la definición de VLANs, y según el modelo, posibilitan la comunicación entre las diversas VLANs sin la necesidad de utilizar un router externo.

Por permitir la unión de segmentos de diferentes dominios de broadcast, los switches de capa 3 son particularmente recomendados para la segmentación de redes LAN muy grandes, donde la simple utilización de switches de capa 2 provocaría una pérdida de rendimiento y eficiencia de la LAN, debido a la cantidad excesiva de broadcasts.

Dentro de los Switches Layer 3 tenemos:

Packet by Packet: Es un caso especial de switch "Store and Forward" pues, al igual que éstos, almacena y examina el paquete, calculando el CRC y decodificando la cabecera de la capa de red para definir su ruta a través del protocolo de ruteo adoptado.

Layer 3 Cut-through: Este tipo de switch examina los primeros campos, determina la dirección de destino (a través de la información de los headers o cabeceras de capa 2 y 3) y, a partir de ese instante, establece una conexión punto a punto (a nivel 2) para conseguir una alta tasa de transferencia de paquetes. A partir del momento en que la conexión punto a punto es establecida, podrá funcionar en el modo "Store & Forward"o "Cut-Through"

Switch (Layer 4)

Están en el mercado hace poco tiempo y hay una controversia en relación con la adecuada clasificación de estos equipos. Muchas veces son llamados de "Layer 3+" o "Layer 3 Plus".

Básicamente, incorporan a las funcionalidades de un switch de capa 3 la habilidad de implementar las políticas y filtros a partir de informaciones de capa 4 o superiores, como puertos TCP/UDP, SNMP, FTP, etc.

9.1.4. Router (Layer 3)

Un Router es un dispositivo de comunicaciones que se encarga de enviar paquetes de datos entre dos o más redes distintas, para ello utiliza protocolos de capa 3 que le permiten el ruteo de los paquetes según un criterio definido. Es un dispositivo que puede "decidir"que ruta utilizará para la entrega de la información.

Inicialmente, el router posee una tabla de ruteo que contiene las redes que el mismo posee conectadas en forma directa. Mediante los métodos que se nombran a continuación, el router puede acceder a redes distantes:

- Configuración de Rutas Estáticas
- Configuración de una ruta por defecto
- Configuración de rutas dinámicas por medio de protocolos de ruteo:
  - Interiores: RIP, IGRP, OSPF, EIGRP
  - Exteriores: EGP, BGP, CIDR.

En los routers pueden definirse ACLs[1] para filtrar tráfico. Las ACLs se configuran según el origen y el destino del tráfico y adicionalmente por tipo de tráfico. Es decir, es posible configurarlas para que permitan filtrar el tráfico según una dirección de origen o destino. Luego de configurar la lista de acceso es necesario aplicarla en una interfaz del router e indicar si se la aplicará al tráfico entrante o saliente.

Es muy común encontrarse con listas de control de acceso en routers de borde (aplicando listas de acceso "de choque") o bien en routers que manejen la WAN. También es muy común aplicar los controles de acceso en los firewalls en lugar de los routers.

9.1.5. Firewall (Layer 2...7)

Un firewall es un dispositivo de comunicaciones que permite restringir el acceso entre diversas redes a través de listas de control de acceso que en este caso se denominan Reglas. Asimismo, el firewall puede cumplir otras funciones como ser ruteo.

Las topologías de firewall pueden ser:

Bastion Host: Servidor altamente segurizado que es accesible desde la red denominada como de menor seguridad, y que efectúa las conexiones hacia los equipos de la red de mayor seguridad (Ver Figura 9.2).

[1] Access Control List

Dual-homed host: Servidor que posee varias interfaces conectadas a diversas redes (Ver Figura 9.3).

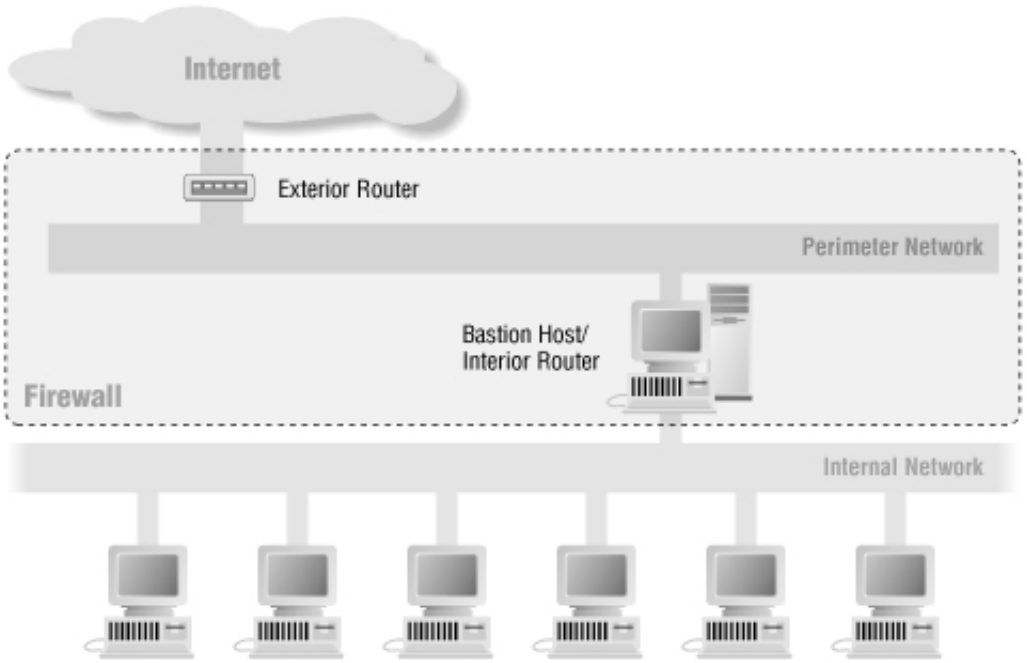


Figura 9.2: Topología Bastion Host

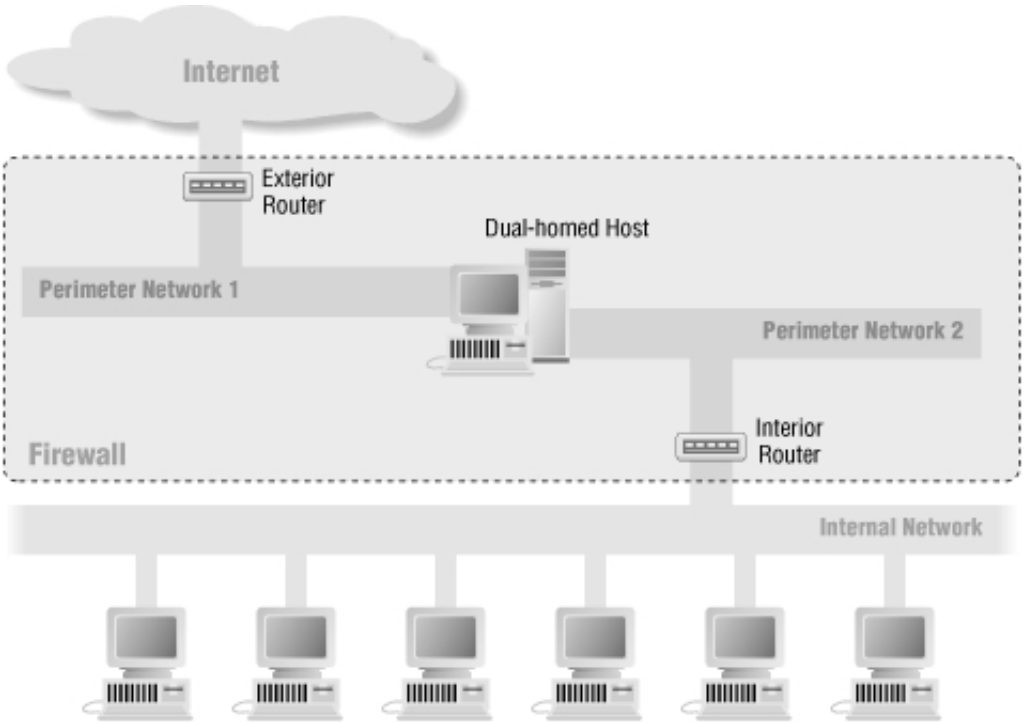


Figura 9.3: Topología Dual-home host

Clasificación:

Stateless: Procesamiento de paquetes: Únicamente filtra paquetes por dirección de origen y destino, tipo y número de puerto.

No efectúa un control del flujo de datos ni mantiene el estado de las conexiones.

Stateful: Procesamiento de paquetes: Según su estado y su evolución.

Existen protocolos que se conectan por puertos específicos y otros que se conectan por puertos asignados dinámicamente. El firewall Stateful puede efectuar un seguimiento de la negociación, análisis del flujo de datos y asignación de puertos dinámicos asignados al flujo de datos debido a que conoce el modo de funcionamiento de los servicios.

Estas características de seguimiento, decodificación y la posibilidad de analizar los protocolos, hacen que los firewall Stateful estén clasificados como "application-aware".

La configuración del firewall se encuentra formada básicamente por reglas, las cuales definen lo que se denomina como Política de seguridad del firewall. Estas reglas definen en forma detallada el control de acceso que llevará a cabo el firewall sobre el tráfico de red:

Regla 0: Por lo general existe una regla general que posee las configuraciones básicas del firewall como ser: paquetes a denegar por defecto (Ej. SYN Flood, etc)

Reglas específicas: Adicionalmente existen reglas que permiten filtrar tráfico según dirección de origen, destino y por el tipo de tráfico o protocolo utilizado.

Se denomina DMZ[2] o zona desmilitarizada, a una red de seguridad intermedia, que generalmente se encuentra entre la red privada (zona de máxima seguridad) y la red pública (zona sin seguridad). El objetivo de la DMZ es proveer servicios limitados a usuarios externos, sin permitir el acceso de los usuarios externos a la red de máxima seguridad.

No existe un límite en cantidad de redes/niveles de seguridad, por lo tanto a medida que éstas crezcan, crecerá el número de zonas y por consiguiente el número de interfaces en el/los firewall/s que conforman la arquitectura de red. Este tipo de arquitecturas forman firewalls Multi DMZs o DMZs Multi firewalls.

A continuación se describe las posibles topologías de firewall

Topología Firewall Básica

Esta configuración usa un servidor proxy inverso en el límite entre Internet y la red privada para interceptar y luego reenviar las solicitudes al servidor web adecuado situado en la intranet. Mediante un conjunto de reglas configurables, el servidor proxy comprueba que las direcciones URL solicitadas estén permitidas según la zona desde la que se originó la solicitud. A continuación, las direcciones URL solicitadas se traducen en direcciones URL internas. La siguiente ilustración muestra una topología de Firewall Básica.

[2]Demilitarized zone

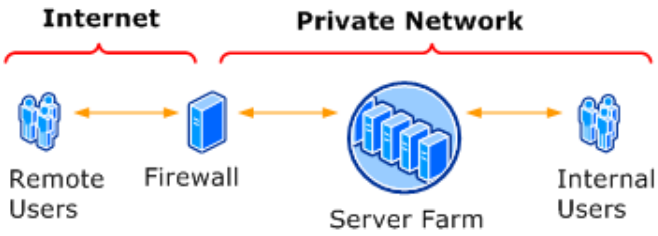


Figura 9.4: Topología Firewall Básica

Ventajas

- La solución más sencilla y la que menos hardware y configuración requiere.
- Todos los servidores se encuentra en la red privada.
- Ubicación de datos única:
  - Los datos se encuentran dentro de la red de confianza.
  - El mantenimiento de los datos tiene lugar en una ubicación.
  - Se usa una única granja de servidores para las solicitudes tanto internas como externas, lo que garantiza que todos los usuarios autorizados verán el mismo contenido.
- Las solicitudes de usuarios internos no se pasan a través de un servidor proxy para consultas en la intranet.

Desventajas

- Tiene como resultado un único firewall que separa la red privada de Internet.

Topología DMZ Opuesta

Una topología DMZ opuesta aisla la granja de servidores en una red aparte, tal como muestra la siguiente ilustración.

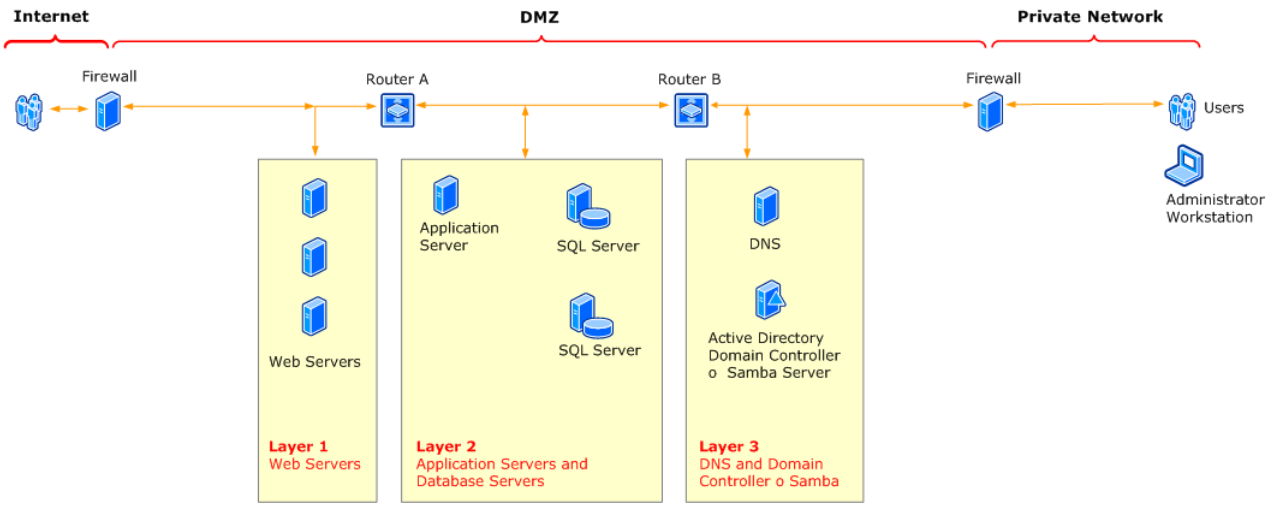


Figura 9.5: Topología DMA Opuesta

Esta topología tiene las siguientes características:

- Todo el hardware y los datos residen en la DMZ.
- Las funciones de la granja de servidores y los servidores de infraestructura de red se pueden separar en varios niveles. Combinar los niveles de red puede reducir el costo y la complejidad del sistema.
- Cada nivel puede separarse por medio de routers o firewalls adicionales para garantizar que se permitan sólo las solicitudes de niveles específicos.
- Las solicitudes de la red interna se pueden dirigir a través del servidor firewall del lado interno o ruteandose a través de la interfaz pública de la red de la DMZ.

Ventajas

- El contenido se aisla en una única granja de servidores en la extranet, lo que simplifica el uso compartido y el mantenimiento del contenido en la intranet y la extranet.
- El acceso de usuarios externos se aisla en la DMZ.
- Si la extranet se ve comprometida, es posible que los daños se limiten al nivel afectado o a la DMZ.

Desventajas

- Requiere una infraestructura y configuración de red adicionales.

Topología Opuesta Dividida

Esta topología divide la granja de servidores entre la DMZ y la red privada. Los equipos que ejecutan el software de base de datos se hospedan dentro de la red privada. Los servidores web se encuentran en la DMZ. Los servidores de búsqueda pueden hospedarse en la DMZ o en la red privada.

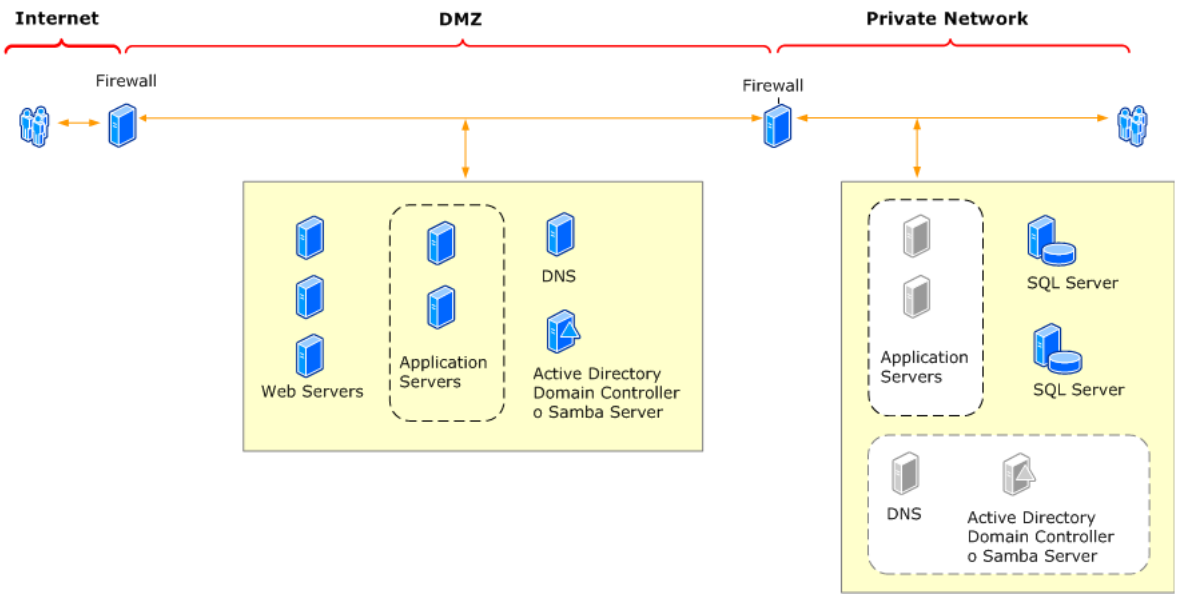


Figura 9.6: Topología Opuesta Dividida

En la ilustración de la Figura 9.6:

- El servidor de búsqueda se hospeda dentro de la DMZ. Esta opción está representada por el servidor azul dentro de la línea de guiones.
- De forma opcional, los servidores de búsqueda se pueden implementar dentro de la red privada, con los servidores de base de datos. Esta opción está representada por un servidor gris dentro de la línea de guiones. Si implementa servidores de búsqueda dentro de la red privada con los servidores de base de datos, también debe tener un entorno de Active Directory o Samba[3] para admitir estos servidores (representados por servidores grises dentro de la red privada).

Si la granja de servidores se divide entre la DMZ y la red privada con los servidores de base de datos situados dentro de la red privada, se requiere una relación de confianza de dominios si se usan cuentas de Windows para obtener acceso a la base de datos. En este escenario, el dominio de la DMZ debe confiar en el dominio privado. Si se usa la autenticación de SQL, no se requiere una relación de confianza del dominio.

[3] Samba es una implementación libre del protocolo de archivos compartidos de Microsoft Windows (antiguamente llamado SMB, renombrado recientemente a CIFS) para sistemas de tipo UNIX. De esta forma, es posible que ordenadores con GNU/Linux, Mac OS X o Unix en general se vean como servidores o actúen como clientes en redes de Windows. Samba también permite validar usuarios haciendo de Controlador Principal de Dominio (PDC), como miembro de dominio e incluso como un dominio Active Directory para redes basadas en Windows; aparte de ser capaz de servir colas de impresión, directorios compartidos y autentificar con su propio archivo de usuarios. Permite configurar directorios Unix/Linux (incluyendo sus subdirectorios) como recursos para compartir a través de la red. Para los usuarios de Microsoft Windows, estos recursos aparecen como carpetas normales de red. Los usuarios de Linux pueden montar en sus sistemas de archivos estas unidades de red como si fueran dispositivos locales, o utilizar la orden smbclient para conectarse a ellas muy al estilo del cliente de la línea de órdenes ftp. Cada directorio puede tener diferentes permisos de acceso sobrepuestos a las protecciones del sistema de archivos que se esté usando en Linux.

Para optimizar el rendimiento de las búsquedas y el rastreo, se puede colocar la función de servidor de búsqueda dentro de la red privada con los servidores de base de datos. También se puede agregar la función del servidor web a un servidor de búsqueda dentro de la red privada y configurar este servidor web para su uso dedicado por parte de la función de búsqueda para rastrear contenido. Si se colocan servidores web en la DMZ y la función de búsqueda dentro de la red privada, se debe configurar una relación de confianza unidireccional en la que el dominio de la DMZ confíe en el dominio de la red privada. Esta relación de confianza unidireccional se requiere en este escenario para admitir la comunicación entre servidores dentro de la granja de servidores, independientemente de si va a usar autenticación de SQL para obtener acceso al SQL Server.

Ventajas

Entre las ventajas de la topología opuesta dividida se encuentran las siguientes:

- Los equipos que ejecutan SQL Server no están hospedados dentro de la DMZ.
- Los componentes de la granja de servidores tanto dentro de la red corporativa como dentro de la red perimetral pueden compartir las mismas bases de datos.
- Con una infraestructura de Active Directory aparte, las cuentas de usuarios externos se pueden crear sin afectar al directorio corporativo interno.

Inconvenientes

- La complejidad de la solución aumenta en gran medida.
- Intrusos que ponen en peligro los recursos de la red perimetral podrían obtener acceso al contenido de la granja de servidores almacenado en la red corporativa mediante las cuentas de la granja de servidores.
- La comunicación entre las granjas de servidores suele quedar dividida entre dos dominios.

Autenticación, Autorización y Auditoría (AAA)

- AAA para usuarios con tareas de mantenimiento sobre el equipo.

  Autenticación y Autorización: Definición de usuarios (Administración, revisión de logs, etc).

  Auditoría sobre las tareas que éstos realizan.

- AAA para usuarios que utilizan el servicio:

  Autenticación y Autorización a través de reglas que efectúan la autenticación contra una base de datos de usuarios interna o externa.

  Auditoría específica sobre reglas críticas.

Es recomendable implementar una red aislada para administrar y monitorear los dispositivos de comunicaciones

En esta red podrían instalarse entre otros dispositivos:

- Servidor de Syslog.
- Consola de administración del firewall.
- Sistema de monitoreo y alarmas centralizado.

A continuación se presenta un ejemplo.

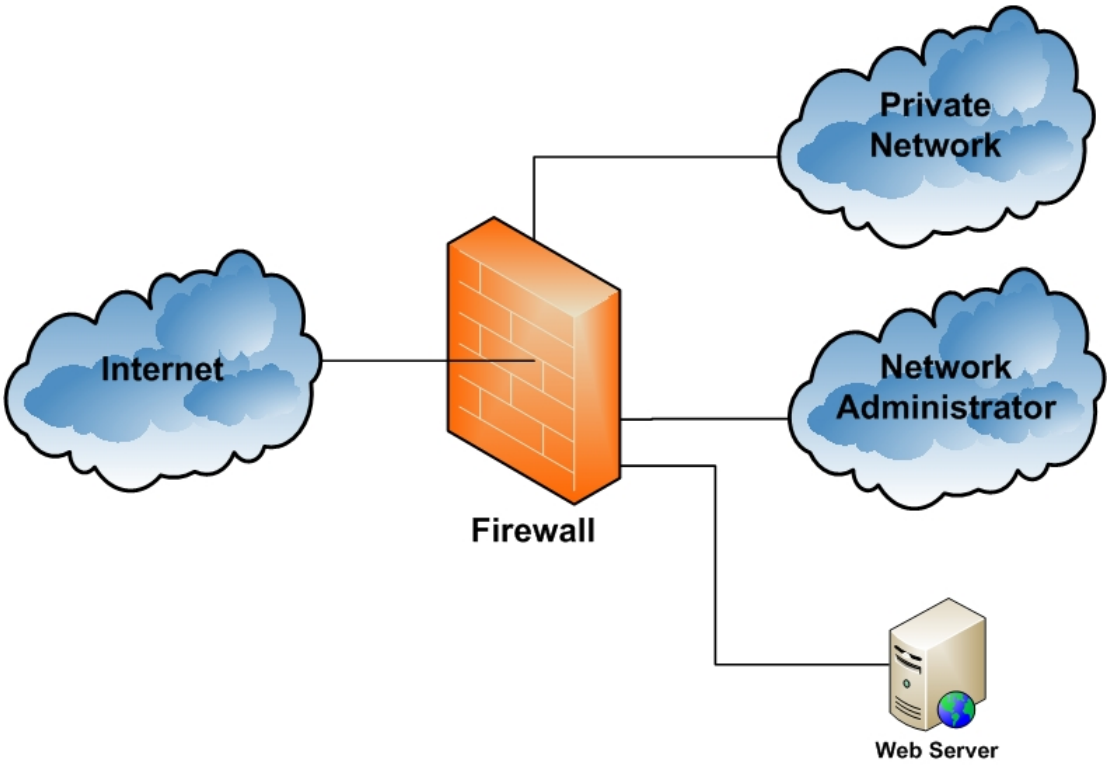


Figura 9.7: Aislar redes

Arquitectura "LAMP"

En esta sección se explica una típica aplicación de un entorno de desarrollo PHP[4] y MySQL, como la empleada por la FIUBA. Esto es importante para saber cuándo configurar la comunicación entrante y saliente en un router o firewall. Estas aplicaciones se desarrollan en la plataforma llamada "LAMP" (Linux, Apache, MySQL y PHP), donde cada uno de los componentes desempeña un rol específico e importante :

- El OS GNU/Linux proporciona la base del entorno de servidor.
- El servidor web Apache intercepta las peticiones HTTP y sirve directamente la consulta o transmite al intérprete PHP para su ejecución.
- El intérprete PHP parsea y ejecuta el código PHP, y devuelve los resultados al servidor web.

[4]Hypertext Preprocessor

- El MySQL RDBMS sirve como el motor de almacenamiento de datos, aceptando conexiones de la capa de PHP e inserta, modifica o recupera datos.

La Figura 9.8 ilustra estos componentes en acción.

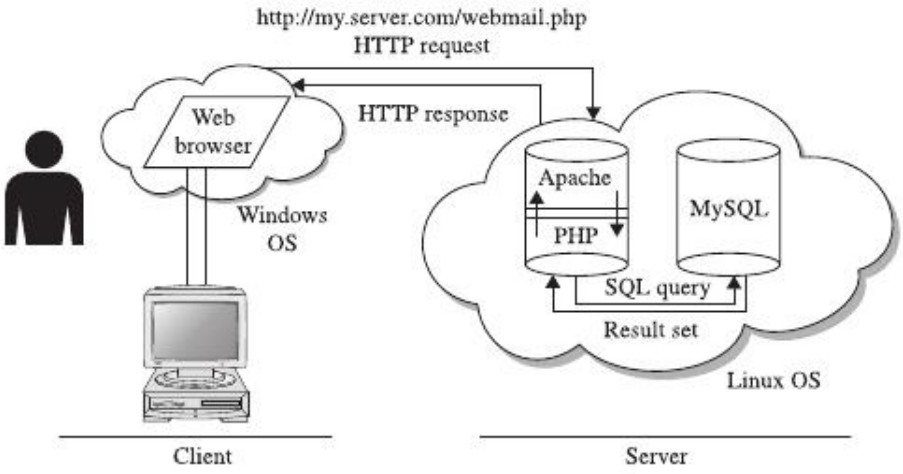


Figura 9.8: Entorno de desarrollo LAMP

Esto es lo que pasa en la Figura 9.8:

1. El usuario (cliente) abre su navegador web en su casa y tipea la dirección URL de su correo web online. Después de buscar el dominio, el navegador de del cliente envía una petición HTTP/S a la dirección IP del servidor correspondiente.

2. El servidor web Apache, que maneja las peticiones HTTP de dominio, recibe la solicitud y detecta que el URI termina con el sufijo ".php". Debido a que el servidor está programado para redirigir automáticamente todas las solicitudes a la capa PHP, simplemente invoca el intérprete PHP y pasa a este el nombre del archivo.

3. El intérprete PHP analiza el archivo, ejecutando el código PHP. Si el código incluye consultas de base de datos, el intérprete PHP abre una conexión cliente con el MySQL RDBMS y ejecuta estas. Una vez que el intérprete de secuencia de comandos ha finalizado la ejecución del script, devuelve el resultado en el navegador, limpia después el cache, y vuelve al modo de hibernación.

4. Los resultados devueltos por el intérprete se transmiten al navegador del cliente por el servidor Apache.

De la anterior explicación, debe quedar claro que para utilizar aplicaciones PHP y MySQL, su entorno de desarrollo debe incluir un servidor web (esto no siempre tienen que ser de Apache, aunque eso es lo más común) y las instalaciones de trabajo de PHP y MySQL.

A continuación, se describen los puertos y protocolos que son necesarios para la comunicación entre funciones de servidor.

Acceso de cliente: Puerto TCP 80 (HTTP), puerto TCP/SSL 443 (HTTPS).

Servicio de uso compartido de archivos e impresora: Puerto TCP/UDP 445 (SMB).

Comunicación con la base de datos: Puerto TCP/SSL 1521 (Oracle), Puerto TCP/SSL 3306 (MySQL).

NAT

NAT[5], básicamente se trata de la traducción de direcciones IP desde una red hacia otra. Para efectuarla el firewall modifica las direcciones IP de origen y/o destino de los paquetes y mantiene el estado de las conexiones establecidas. Pueden realizarse traslaciones tanto de IPs privadas como públicas.

Posibles casos son:

- De una dirección IP privada a una dirección IP estática públicas o a un pool de dirección IP publicas.
- Una dirección IP privada y un puerto TCP a una dirección IP estática pública o a un pool de direcciones IP rotativas públicas.
- Una dirección IP pública a algunas direcciones de un pool IP mediante round robin.

Marcas de Firewall

Las marcas más conocidas de firewall son:

- Cisco PIX
- Checkpoint Firewall-1
- ISA
- Raptor
- NetScreen
- Soluciones Freeware (Linux + Software específico)

9.1.6. Proxy (Layer 1...7)

Un Proxy es un dispositivo de comunicaciones que se encuentra entre el cliente y el servidor destino. Intercepta todos los pedidos y observa si los puede resolver él con el contenido previo almacenado (Cache). En caso contrario, efectúa la solicitud al servidor destino.

Sus principales tareas son las de optimizar la "performance", filtrar contenido y mejorar la seguridad de la arquitectura.

Las tecnologías existentes son:

Web proxy: Es el primer servicio que prestaron los proxy y consiste básicamente en hacer de proxy de las solicitudes HTTP y HTTPS.

[5]Network Address Translation

Socks proxy: Socks es básicamente un protocolo para manejo de tráfico TCP a través de un proxy. El mismo puede ser utilizado virtualmente para cualquier aplicación TCP incluídos los browsers WEB, los clientes FTP, etc.

9.1.7. IDS (Layer 2..7)

Sistema de detección de intrusos encargado de detectar los posibles intrusos que intentan obtener acceso no autorizado a través de la red o en un servidor.

9.1.8. Access Point o AP (Layer 2)

Se denomina así al equipo de acceso a la red Wi-Fi encargado de irradiar y captar las señales Wi-Fi dentro de una área de determinada. Este equipo es el encargado de captar las señales Wi-Fi del aire y enviar todo el trafico a los Access Controllers/Gateways remotos. Cuando el área de cobertura es extensa, se pueden interconectar varios APs en cascada para extender el área de cobertura.

9.1.9. Access Controller o AC (Layer 2 ...7)

Se denomina así al equipo al cual se conectan uno o más APs definiendo un área hotspot. Puede tener también la capacidad de irradiar y recibir señales Wi-Fi, en este sentido también funciona como un AP. Este equipo suele proveer la facilidad de desarrollo de todos los servicios, como DHCP server, firewall, DNS rely, RADIUS rely, portal cautivo, etc. tenga capacidad Wi-Fi.

9.2. Arquitectura de red

En la Figura 9.9 se presenta la red propuesta en la que intervienen dos firewalls que conforman la barrera de seguridad en una aplicación típica de tres capas “Front-End/Application Server/Database”.

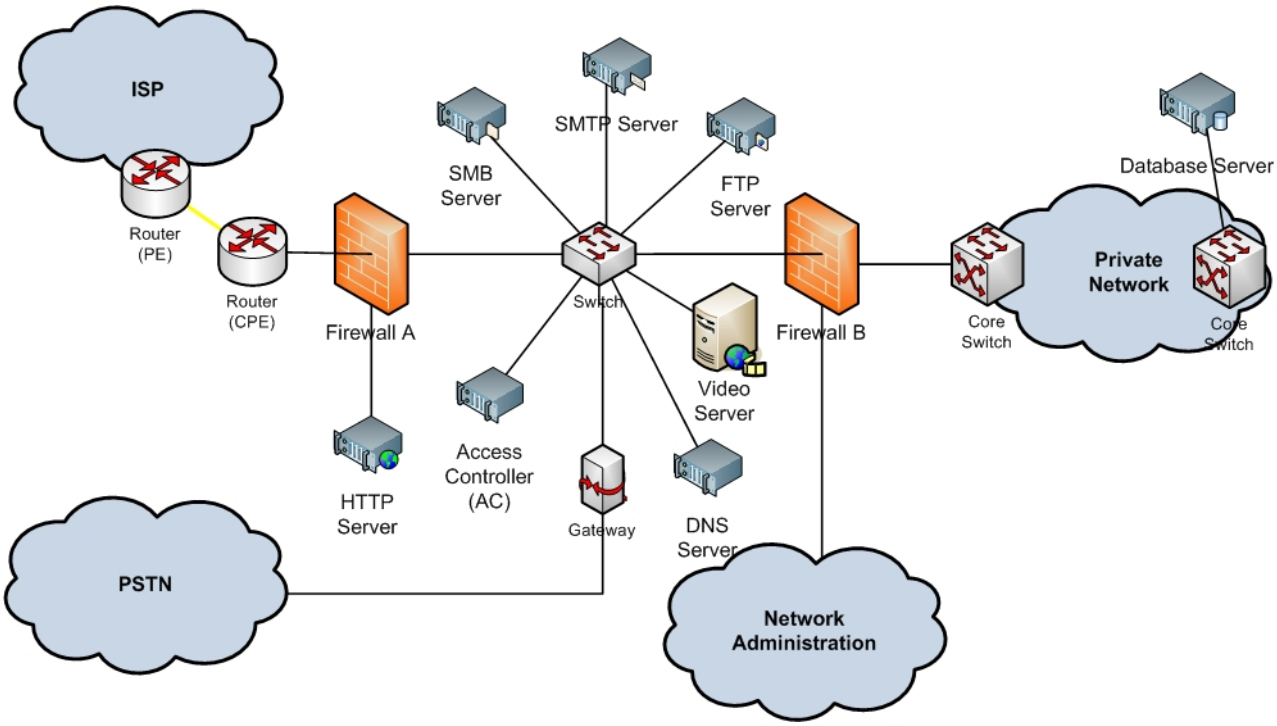


Figura 9.9: Arquitectura

9.3. Red Privada

La red esta formada por distintos equipos que interactúan para brindar el servicio Wi-Fi como se puede observar el la Figura 9.10.

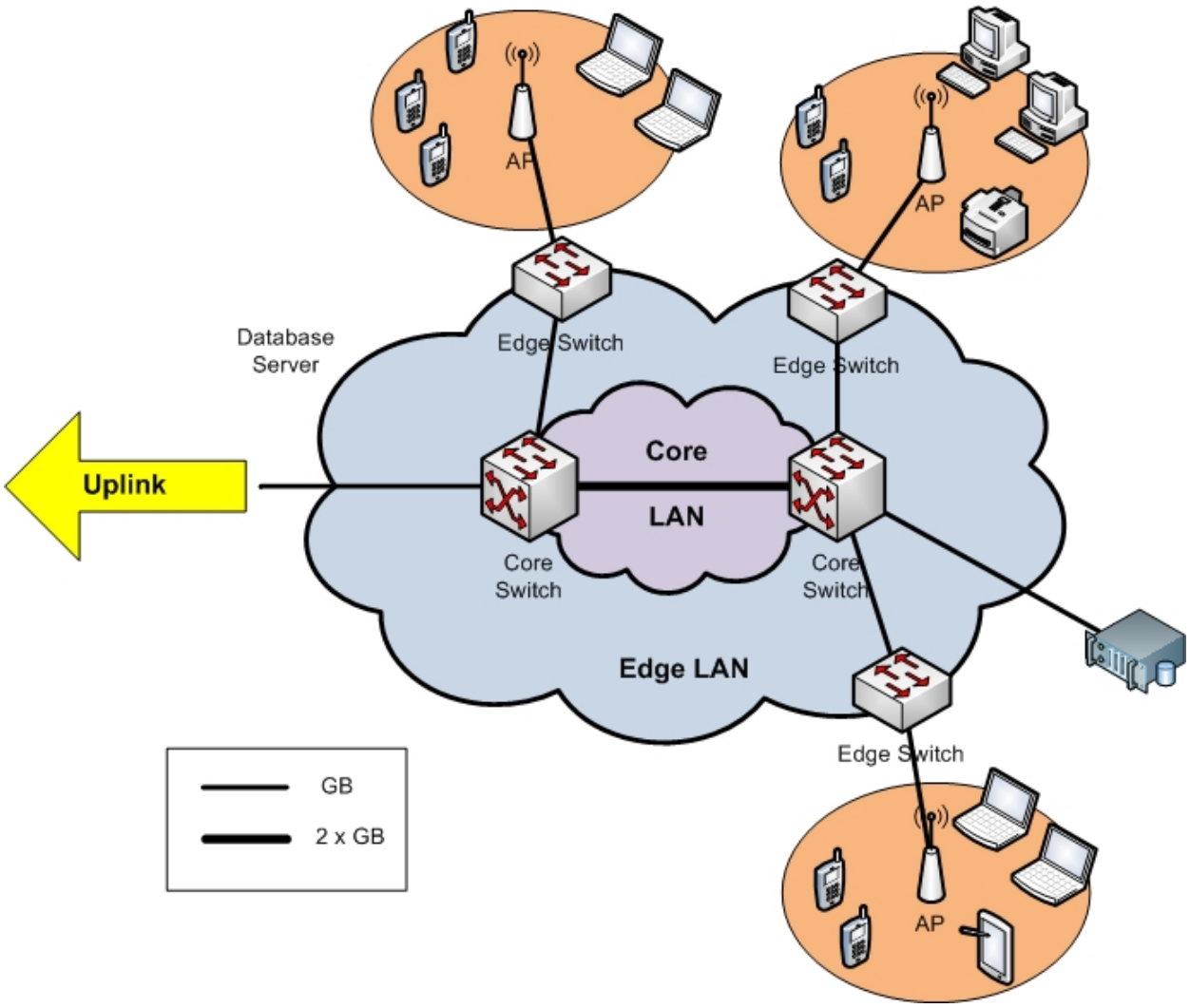


Figura 9.10: Arquitectura de red

En esta arquitectura se pueden ver esquemáticamente todos los elementos involucrados en la red Wi-Fi. Esta se puede diferenciar en dos secciones:

Acceso: La red de acceso esta determinada por la zona de cobertura y es la encargada de brindar acceso a los servicios a los usuarios.En el área hotspot se encuentran los Access Points (AP) distribuidos de forma tal de tener cubiertas las áreas de interés donde se quiere brindar el acceso Wi-Fi. Los APs se interconectan entre si en forma de cascada, ya sea a través de una red LAN cableada o utilizando lo que se denomina wireless link (conexión inalámbrica entre APs), de cualquiera de las dos formas todos los APs de la misma área convergen (o tributan) a un AC[6], el cual es el encargado de recibir todo el tráfico generado por los clientes Wi-Fi captado por los APs. El AC además puede proveer servicios adicionales como DHCP server, DNS relay, firewall, NAT, etc si así es requerido.

"Backbone": El backbone da interconexión troncal al acceso mediante una red cableada de switches, los cuales se los puede clasificar en dos grupos:

[6]Access Controller

Edge Switches: Son los switches que interconectan a los APs a la red para acceder a los servicios de la red y de internet.

Core Switches: Son los switches que concentran y agregan el tráfico proveniente de los switches de acceso.

9.4. Acceso de la Red Privada

9.4.1. Definiciones

9.4.2. Ingeniería de áreas "hotspot"

Conexión en cascada de equipos APs y AC

Para extender el área de cobertura de un área hotspot, es necesario agregar uno o más APs a lo que se llama "conexión en cascada" de equipos APs. Esta conexión en cascada puede realizarse de dos formas: Mediante el tendido de un cableado UTP (o utilización de una red de switches) o bien a través lo que se denomina "wireless link" que es la conexión inalámbrica entre APs/AC.

Conexión en cascada por cable UTP : Esta conexión se puede observar en la Figura 9.11. Se realizará utilizando el port de uplink downlink que disponen los AP/AC. La mecánica es conectar el port de downstream del 1er AP al port de upstream del 2do AP. Luego, conectar el port de downstream del 2do AP al de upstream del siguiente, y así continuar hasta el ultimo AP. De esta forma pueden conectarse todos los AP en cascada extendiendo el área de cobertura de la zona hotspot.

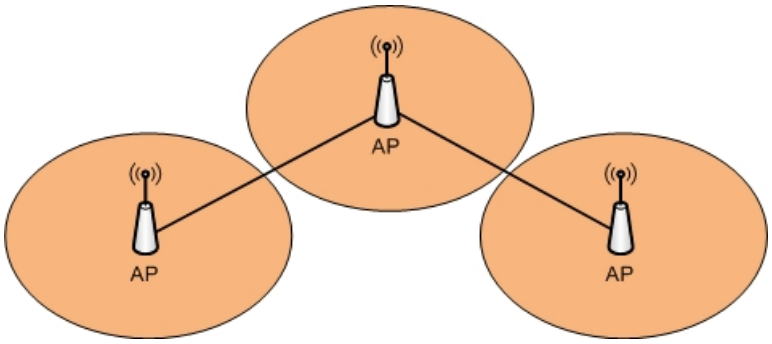


Figura 9.11: Conexión en cascada de APs por cable UTP

Conexión en cascada por red de switches: En caso de disponerse de una red de switches, se realiza la interconexión de los APs al AC directamente a través de la misma como puede observarse en la Figura 9.12.

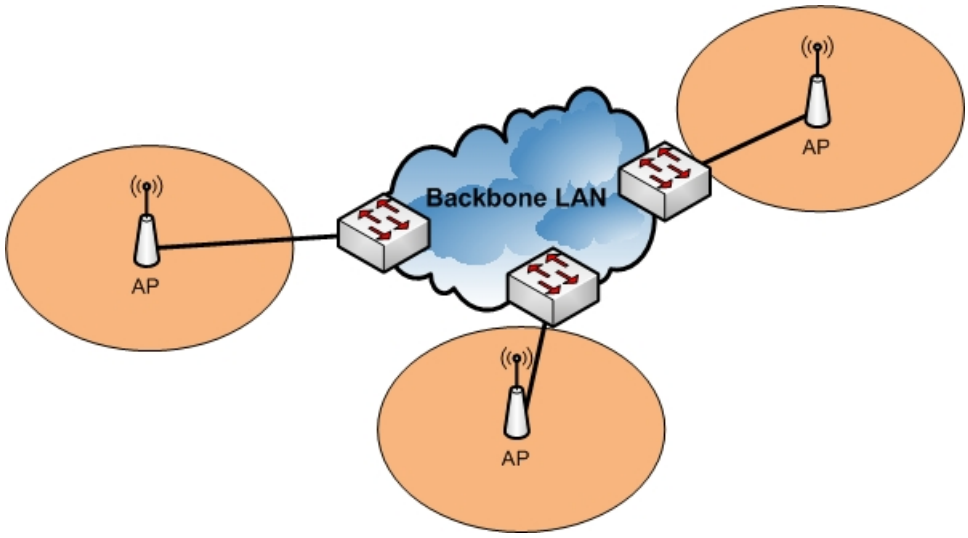


Figura 9.12: Conexión en cascada de APs por backbone de switches

Conexión en cascada por Wireless Link: "Wireless Link" es una solución que permite prescindir del tendido de cableado para la LAN interna entre APs y AC como se puede observar en la Figura 9.13.

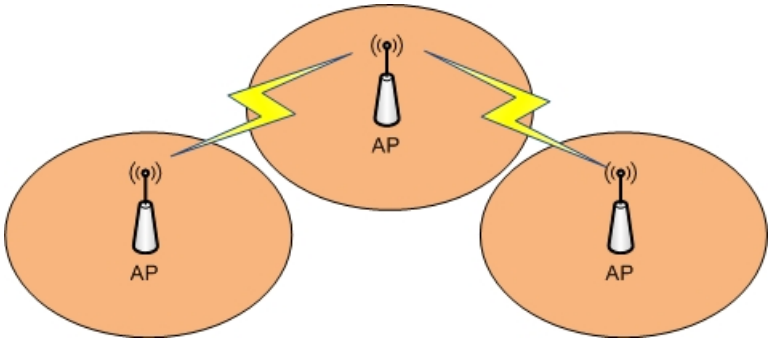


Figura 9.13: Conexión en cascada de APs por Wireless Link

Esta forma de conexión tiene la ventaja de sencillez y rápido despliegue, por lo que es especialmente útil en el caso de instalaciones temporarias (como es el caso de instalaciones para eventos, por ejemplo). Sin embargo este tipo de conexión tiene ciertos limitantes que se detallan a continuación:

- Reducción del throughput entre APs. Esto es debido a que los AP deben estar configurados en el mismo canal de radio para transmitir el tráfico a los otros APs.
- La distancia máxima entre dos APs conectados a través de wireless link deben tener "linea de vista" (libre de obstáculos) y que no sobrepase la distancia de alcance que el fabricante indique.

Observación: La conexión inalámbrica entre APs y AC utilizando "Wireless Link" igualmente requiere la conexión de cada AP/AC a la red eléctrica.

Asignación de radiofrecuencias de las celdas

En la asignación de radiofrecuencias de las celdas se tienen en cuenta básicamente las siguientes pautas:

- Cantidad y ubicación de los APs de forma tal de lograr máxima cobertura .
- No sobredimensionar la cantidad APs inútilmente, porque esto incrementaría el costo innecesariamente.
- Evitar el solapamiento de las celdas con la misma frecuencia de trabajo como indica la Figura 9.14. En el caso de los escenarios con arreglos multicelda donde dos o más AP están dentro del radio de cobertura del otro (celdas adyacentes), se deberá tener especial cuidado para la asignación de las frecuencias de cada uno de ellos a modo de minimizar la interferencia y maximizar el throughput en cada celda. Las principales causas que afectan el desvanecimiento del throughput en la red wireless son los paquetes que son transmitidos y se pierden, y el aumento del delay. El siguiente ejemplo muestra dos celdas cuyas áreas de cobertura se solapan, si no se eligieran diferentes frecuencias para cada una de ellas el número de retransmisiones sería elevado y por consiguiente el throughput se verá degradada

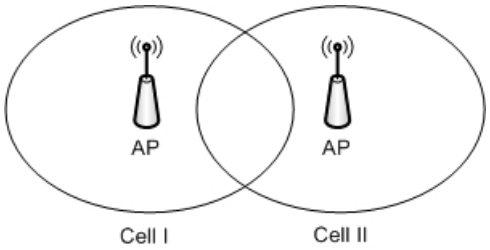


Figura 9.14: Celdas solapadas

  Para arreglos multicelda de este tipo se asignarán frecuencias diferentes para cada AP con la máxima separación posible entre las frecuencias de AP adyacentes.

- El hand-over es la capacidad de una estación móvil de desplazarse físicamente sin perder comunicación. Para permitir el hand-over a usuarios móviles es necesario colocar los Puntos de Acceso de tal manera que haya una superposición (over-laping) de aproximadamente el 15 % entre los diversos radios de cobertura. En la Figura 9.15 la zona de superposición permite que las estaciones móviles se desplacen del área de cobertura A a la B sin perder la comunicación, en definitiva el usuario se conecta del AP A al B de forma transparente. La Figura 9.15 muestra las zonas de cobertura de cada AP A y B, y la superposición de las mismas. Dado que el estándar 802.11 no define las especificaciones para el hand-over, cada fabricante diseña el algoritmo de decisión de cambio del área de cobertura según sus especificaciones más convenientes, por lo tanto pueden existir problemas cuando en una empresa se tienen Puntos de Acceso de diferentes fabricantes.

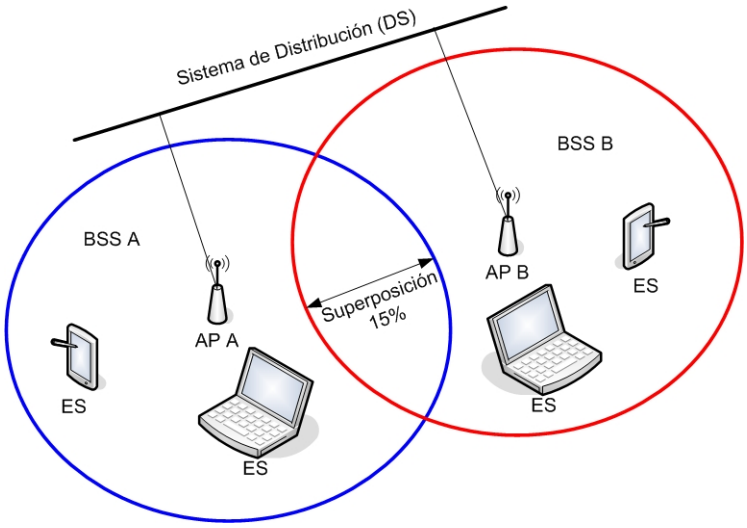


Figura 9.15: Roaming entre dos zonas de cobertura

- Las ondas de radio deben confinarse tanto como sea posible, empleando antenas direccionales y/o sectoriales y configurando adecuadamente la potencia de transmisión de los Puntos de Acceso por cuestiones de seguridad.
- Cada zona hostpot tiene una capacidad de usuarios que surge de compartir el medio de accesos entre los mismos en un mismo hotspot. Por lo tanto, en una zona de baja densidad de usuarios se tiende a elevar el nivel de potencia del AP para extender el área de cobertura de forma tal que más cantidad de usuarios puedan conectarse. Mientras que que en una zona densamente poblada de usuarios se busca disminuir la potencia del AP de forma tal de disminuir el área de cobertura logrando mayor reutilización de frecuencia, y por lo tanto mayor capacidad de usuarios.

El planeamiento de radiofrecuencias puede ser realizado basándose en un patrón de reuso de frecuencias como el que indica la Figura 9.16, considerando a las áreas de cobertura de los AP cómo celdas hexagonales. Los estudios técnicos y de planificaciones de los sistemas celulares se basan de celdas de forma hexagonal ya que el hexágono es el polígono regular que proporciona la mayor superficie por celda, por lo que será mínimo el número de celdas necesarias para la cobertura de un área determinada.

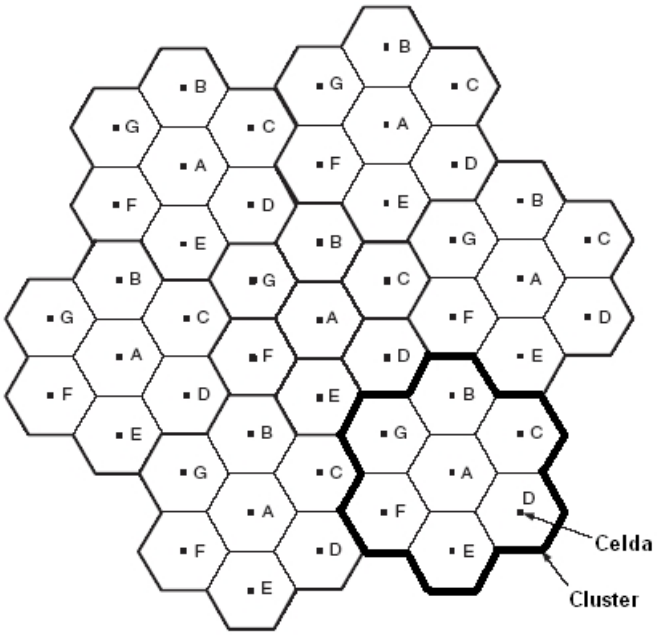


Figura 9.16: Patrón de reuso de frecuencia

En general, surgen dos clasificaciones básicas posible de los edificios: rectangular o lineal y planta simple o multiplanta. De acuerdo al caso en que nos encontremos podrá ser seguido un determinado patrón para la ubicación eficiente de los APs. En el caso particular del edificio de la facultad, nos encontramos con una distribución rectangular y multiplanta, por lo que deberemos utilizar un patrón de distribución de frecuencias como se observa en la Figura 9.17

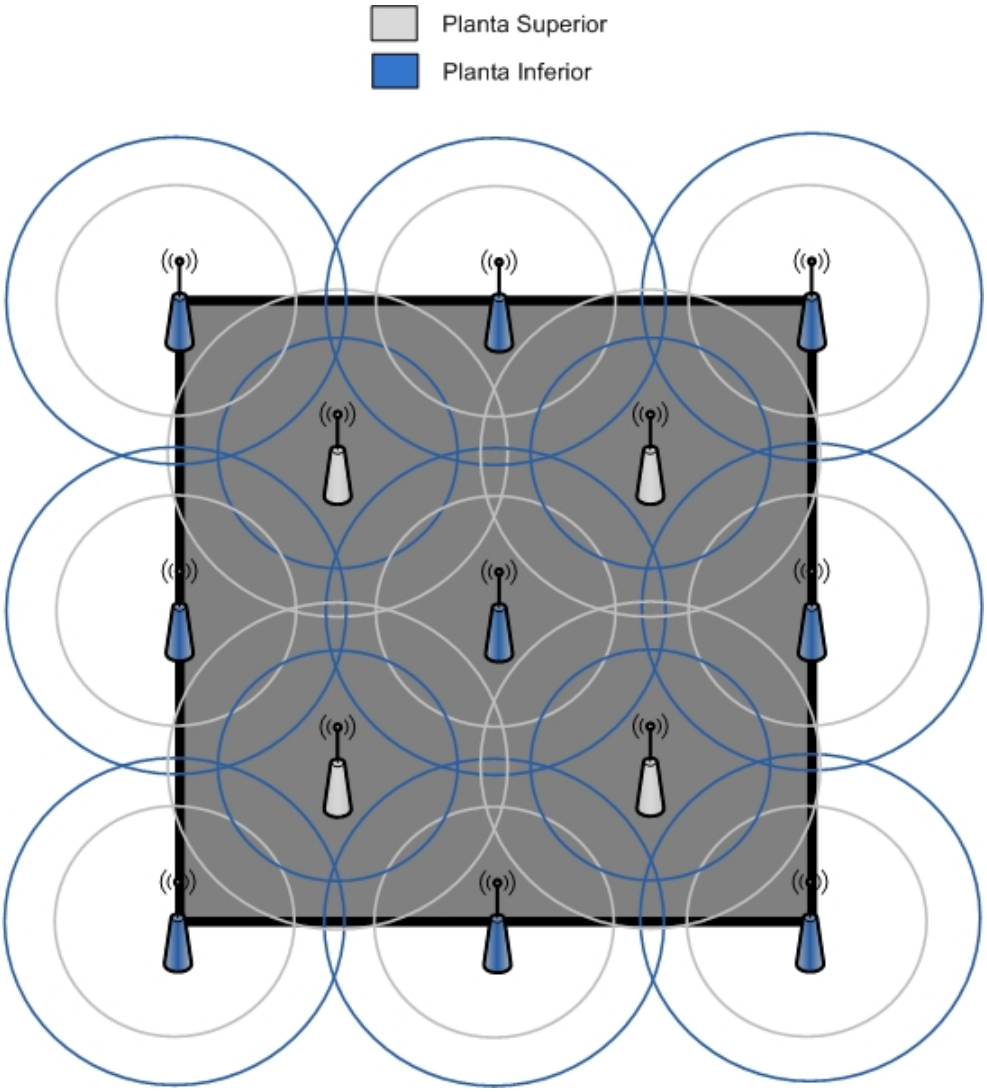


Figura 9.17: Distribución rectangular multi-planta

Determinación de la cobertura

La cantidad de AP instalados en una zona hotspot es en función del área que se pretende cubrir y los obstáculos presentes en el lugar. La siguiente tabla da una idea de los rangos de alcance de los AP/AC.

La cobertura tanto para los APs depende del tipo de ambiente donde sea instalado. Se discriminan tres tipos diferentes de ambientes:

Abierto: Ambiente sin ninguna obstrucción física entre el cliente Wi-Fi y el AP/AC.

Semi abierto: Existencia de tabiques de material sintético o madera.

Cerrado: Ambiente con paredes, piso y cielo rasos de concreto, ladrillos, etc.

para los cuales se detalla la cobertura estimada[7]:

[7]Observación: Estos radios de cobertura son aproximados por lo que deben tomarse como un valor de referencia.

Ambiente	300Mbps	54Mbps	11Mbps	5.5Mbps	2Mbps	1Mbps
Abierto	300m	140m	160m	270m	400m	550m
Semi abierto	100m	45m	50m	70m	90m	115m
Cerrado	60m	20m	25m	35m	40m	50m

Cuadro 9.1: Cobertura de los APs en diferentes ambientes

El estudio del sitio es un procedimiento previo a la instalación de una red inalámbrica. La finalidad es determinar el lugar óptimo de localización de los Puntos de Acceso y detectar las zonas oscuras, es decir, zonas con mucho ruido o zonas sin cobertura.

Para la realización de un estudio del sitio es importante seguir un procedimiento definido de la siguiente forma:

1. Utilización de los planos arquitectónicos del sitio.
2. Reconocimiento físico de las instalaciones y determinación de obstáculos.
3. Determinar la ubicación preliminar de cada AP.
4. Probar utilizando un software de monitoreo el nivel de señal de cada AP y comprobar la cobertura y rendimiento.
5. Evaluar la reubicación de los APs para lograr mejores coberturas y rendimientos.
6. Evaluar la posibilidad de añadir o quitar Puntos de Acceso rediseñando cada micro-celda.
7. Identificar la existencia de fuentes de energía y conexiones de red para los Puntos de Acceso a ser instalados.
8. Planificar la asignación de canales de radio frecuencia para cada AP; de tal forma que se evite la interferencia co-canal.
9. Documentar la ubicación final de todos los Puntos de Acceso con sus respectivas configuraciones de radio frecuencia y conexiones de red.

Varios proveedores ofrecen productos que cumplen con las regulaciones de la FCC[8] para operar a $2,4GHz$ sin licencia. Estos reglamentos permiten potencia radiada de hasta $1W$ de espectro cuando se utilizan técnicas de modulación. Hay muchas aplicaciones para las que la complejidad impuesta por el uso de radios de espectro ensanchado son más resistentes a la interferencia y tienen mayor potencia de RF permitida por las regulaciones de la FCC.

La frecuencia libre que comprende la banda de $2,4GHz$ es la utilizada por los dispositivos Wi-Fi. Esto también es un factor que debe tenerse en cuenta ya que esta banda es la utilizada por otras tecnologías que pueden interferir con las redes wireless. Entre ellas están los hornos microondas y otros dispositivos comerciales con tecnología Bluetooth que trabajan usando la misma banda o incluso teléfonos inalámbricos o emisores/receptores inalámbricos de audio o vídeo.

También es posible la pérdida de señal por materiales medioambientales. Una clasificación breve sería:

[8]Federal Communications Commission

Interferencia baja: materiales como la madera (tabique en construcciones viejas), el vidrio (ventanas), el amianto (techos) o el yeso (paredes interiores).

Interferencia media: materiales como el ladrillo (paredes interiores y exteriores) o las hojas (árboles y plantas).

Interferencia alta: materiales como el agua (lluvia o niebla), la cerámica (tejas).

Interferencia muy alta: metales en general (vigas, armarios) y el plomo en particular (pinturas aislantes).

Además de las indicadas anteriormente, una fuente de interferencia de gran problemática es la existencia de otras redes Wi-Fi cercanas.

El éxito de diseño de enlaces inalámbricos de alta velocidad de datos implica muchos factores. Este es el primer paso que tendrá que tomar un ingeniero con el fin de determinar la viabilidad de cualquier sistema dado:

Conceptos de comunicaciones: En el análisis de un enlace inalámbrico, las tres preguntas más importantes a ser respondidas son:

1. ¿Cuánta potencia de RF disponemos?
2. ¿Cuánto ancho de banda se dispone?
3. ¿Cuál es la fiabilidad necesaria (según la definición de BER[9])?

En general, la potencia y el ancho de banda efectivo determina un límite superior de la capacidad de un enlace de comunicaciones. El límite superior en términos de velocidad de transmisión de datos está dado por el Teorema de Capacidad del canal de Shannon:

$$C = BW \log_{10}(1 + \frac{S}{N}). \tag{9.1}$$

Donde:

C**:** Capacidad del canal en $(bits/s)$

BW**:** Ancho de banda del canal (Hz)

S**:** Potencia de señal $(Watts)$

N**:** Potencia de ruido $(Watts)$

Esta ecuación significa que para un sistema ideal, el BER es cero si la tasa de transmisión de datos está por debajo de la capacidad del canal. En la práctica, este límite depende de la técnica de modulación y ruido recibido.

Para todos los sistemas de comunicaciones, el ruido del canal está íntimamente ligada al ancho de banda. Todos los objetos que tienen temperatura transmiten energía de RF en forma de ruido aleatorio Gaussiano. La cantidad de radiación emitida puede ser calculada por:

[9] Bit Error Rate

$$N = kTBW. \tag{9.2}$$

Donde:

N**:** Potencia de ruido ($Watts$).

k**:** Constante de Boltzman ($1,38\ 10^{-23}\frac{J}{K}$).

T**:** Temperatura del sistema (K). Por lo general supone que $290°K$.

BW**:** Ancho de banda de canal (Hz).

Este es el nivel de ruido más bajo posible para un sistema con una determinada temperatura física. Para la mayoría de las aplicaciones, la temperatura típica es la temperatura ambiente ($290°K$). Las ecuaciones 9.1 y 9.2 demuestran que el ancho de banda y la potencia de RF se pueden variar para alcanzar un determinado nivel de rendimiento (según el BER requerido).

Distancia y pérdidas por propagación: Otra consideración clave es la cuestión de la distancia. Como las ondas de radio se propagan en el espacio libre, la potencia disminuye al cuadrado de la distancia. Si se duplica la distancia, la potencia que llega a la antena del receptor es atenuado por un factor de cuatro. Este efecto se debe a la atenuación de las ondas de radio a medida que se propagan a través del medio, y puede ser calculado como sigue:

$$FSPL = (\frac{4\pi d}{\lambda})^2 = (\frac{4\pi df}{c})^2. \tag{9.3}$$

$$FSPL(dB) = 20log_{10}(\frac{4\pi df}{c}). \tag{9.4}$$

Donde:

d**:** Distancia entre transmisor y receptor.

f**:** Frecuencia(Hz).

λ**:** Longitud de onda ($\lambda = c/f$).

c**:** Velocidad de la luz en el vacío ($3\ 10^8 m/s$).

Las ecuaciones 9.3 y 9.4 describen la pérdida de señal por propagación en espacio libre (FSPL[10]) en línea de vista (LOS[11]).

En situaciones NLOS[12], donde existen obstrucciones que presentan las construcciones, las pérdidas de propagación pueden ser mucho mayores en interiores. La experiencia ha demostrado que la propagación para LOS tiene validez sólo alrededor de los primeros 20 pies ($6m$). Más allá de 20 pies ($6m$), las pérdidas de propagación en interiores aumentan hasta $30dB$ por cada 100 pies ($30m$) en entornos densos, como se puede observar en la Figura

[10]Free-Space Path Loss
[11]Line of Sight
[12]Non Line of Sight

9.18. Esta es una buena aproximación, debido a que supone el peor caso. La perdidas por propagación reales pueden variar significativamente dependiendo de la construcción y el diseño.

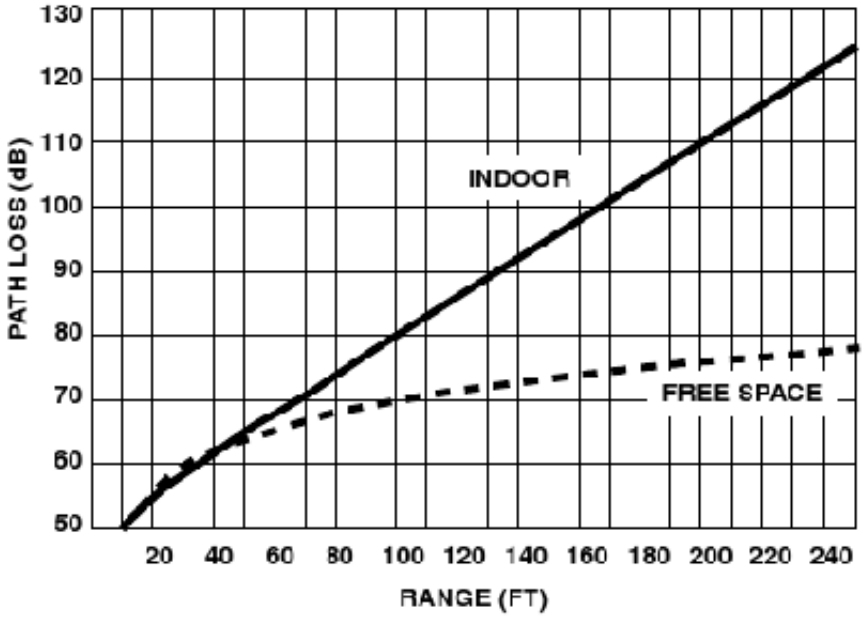


Figura 9.18: Estimación de perdidas por propagación en interiores

Multitrayecto y Margen de potencia: "Multipath"o multitrayecto ocurre cuando las ondas emitidas por el transmisor, viajan a lo largo de trayectorias diferentes e interfieren destructivamente con las ondas que viajan en una línea de visión directa como puede observarse en la Figura 9.19. Esto es denominado a veces "signal-fading". Este fenómeno se produce cuando las ondas que se propagan a lo largo de diferentes caminos pueden estar completamente fuera de fase cuando llegan a la antena del receptor, cancelándose unas con otras. Como la cancelación de señal casi nunca es completa, un método de mejora de este problema es transmitir con más potencia. En un medio ambiente de interiores, el multitrayecto está casi siempre presente y tiende a ser constantemente variable.

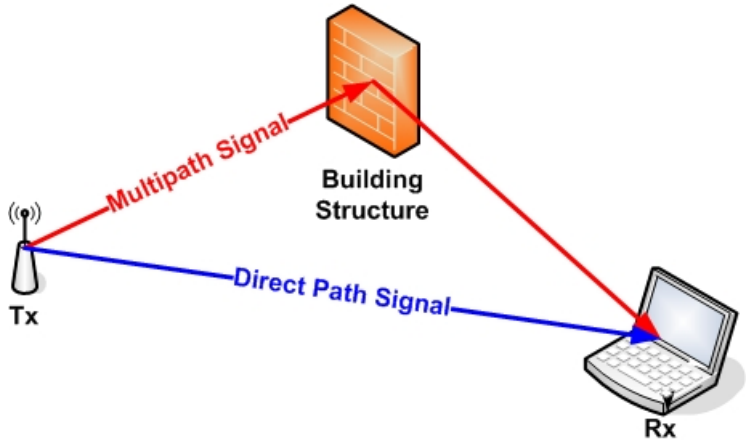


Figura 9.19: Multitrayecto

La pérdida de potencia por multitrayecto pueden producir un "fading"o desvanecimiento que puede resultar en una reducción de más de $30dB$ de la señal. Por lo tanto, es esencial proporcionar suficiente margen de potencia en el enlace, para superar esta pérdida en el diseño de un sistema inalámbrico. El no hacerlo correctamente, afectará negativamente a la fiabilidad del mismo.

Los sistemas de espectro ensanchado son robustos en presencia de señales multitrayecto. Los sistemas que utilizan DSSS rechazan las señales reflejadas que se retrasaron con respecto a la trayectoria directa o señal más fuerte. Esta es la misma propiedad que permite que múltiples usuarios compartan el mismo ancho de banda en sistemas de CDMA. En sistemas FHSS también se presenta un cierto grado de inmunidad al multitrayecto. Debido a que un transmisor FHSS está continuamente cambiando de frecuencias, siempre pasa a alguna frecuencia que recibe poca o ninguna pérdida por multitrayecto. En un medio ambiente donde el problema del multipath está presente, el rendimiento de un sistema FHSS se reducirá, pero es poco probable que el vínculo se pierda por completo.

Técnicas de modulación: La técnica de modulación es una consideración clave. Este es el método por el cual la información analógica o digital se convierte a señales de RF en las frecuencias adecuadas para su transmisión. La selección del sistema de modulación, determina el ancho de banda, eficiencia de la potencia, sensibilidad y complejidad.

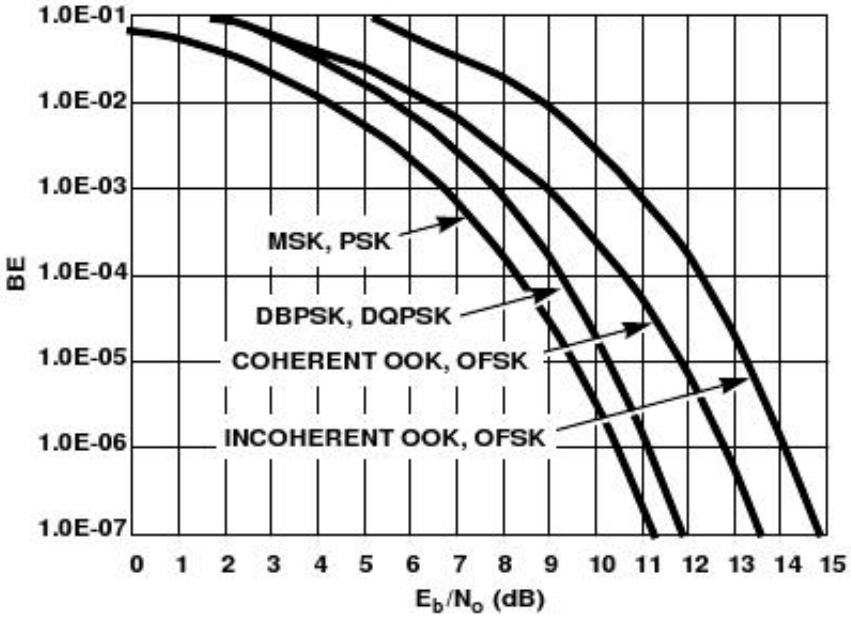


Figura 9.20: Probabilidad de error de bit para métodos de modulaciones típicos

A los efectos del análisis del balance de potencia del enlace, el aspecto más importante de una técnica de modulación es la relación señal-ruido (SNR) necesaria para alcanzar en el receptor un determinado nivel de fiabilidad en términos del BER. Un gráfico de E_b/N_o vs BER se muestra en la Figura 9.20. El E_b/N_o es una medida de la energía requerida por bit relativo a la potencia de ruido. Notar que el E_b/N_o es independiente de la tasa de

velocidad de los datos del sistema. Se puede pasar de E_b/N_o a SNR como se muestra a continuación:

$$SNR = \frac{E_b/T_b}{N_o BW} = \frac{E_b}{N_o}\frac{R_b}{BW}. \tag{9.5}$$

Donde:

E_b**:** Energía requerida por bit de información

N_o Ruido térmico en $1Hz$ de ancho de banda

R_b**:** Tasa de bits de datos.

T_b**:** Tiempo de bits de datos.

BW**:** Ancho de banda del sistema.

Transmisores de espectro ensanchado: Como se explicó en otras secciones, las técnicas de espectro ensanchado simplemente hacen que la energía radiada por el transmisor se extienda a lo largo de un ancho de espectro mayor que de la que hubiera sido utilizado sin esa técnica. Por la expansión de energía, es mucho menos probable que los dos usuarios que comparten el mismo espectro se interfieran unos con otros. Esta es una consideración importante en una banda sin licencia por lo que las autoridades reguladoras imponen el uso de espectro ensanchado en portadoras que transmiten a más de $-1dBm$ (alrededor de $0,75mW$):

Banda	**FCC REGS (US)**	**ETSI (EUROPE)**	**MPT (JAPAN)**
902 - 928*MHz*	$< 1000mW$	N/A	N/A
2400 - 2483,4*MHz*	$1000mW$	$100mW$	N/A
2471 - 2497*MHz*	N/A	N/A	$10mW/Hz$
5725 - 5875*MHz*	$1000mW$	$100mW$	N/A

Cuadro 9.2: Limites de potencia de RF en bandas no licenciadas.

En los EE.UU., estas bandas son designadas colectivamente para industria, ciencia y medicina (banda ISM). Los dispositivos aprobados que operan en estas bandas no requieren una licencia de la FCC. Gracias a que no se requiere licencia, estas bandas se han hecho accesibles a todos. Esto explica principalmente porque las bandas ISM son tan importantes para las aplicaciones comerciales y de consumo.

Como se mencionó anteriormente, los transmisores que emplean la técnica de espectro ensanchado pueden irradiar hasta $1000mW$ ($30dBm$), en comparación con menos de $1mW$ para las que no lo utilizan esta técnica.

9.4.3. Blindaje electromagnético

Propagación de Ondas Electromagnéticas en materiales

En esta sección se va analizar la propagación de ondas electromagnéticas en un medio material, suponiendo campos armónicos como indica la Ecuación 9.6.

$$
\begin{aligned}
\overrightarrow{E}(\overrightarrow{r},t) &= \overrightarrow{E}(\overrightarrow{r})e^{i\omega t} \\
\overrightarrow{D}(\overrightarrow{r},t) &= \overrightarrow{D}(\overrightarrow{r})e^{i\omega t} \\
\overrightarrow{H}(\overrightarrow{r},t) &= \overrightarrow{H}(\overrightarrow{r})e^{i\omega t} \\
\overrightarrow{B}(\overrightarrow{r},t) &= \overrightarrow{B}(\overrightarrow{r})e^{i\omega t}
\end{aligned}. \tag{9.6}
$$

Del análisis del comportamiento de los materiales para campos electrodinámicos es que, para campos armónicos, es posible establecer las siguientes relaciones lineales:

$$
\begin{aligned}
\overrightarrow{D} &= \varepsilon(\omega)\overrightarrow{E} \\
\overrightarrow{j} &= \sigma(\omega)\overrightarrow{E} \\
\overrightarrow{B} &= \mu(\omega)\overrightarrow{H}
\end{aligned}. \tag{9.7}
$$

Donde los parámetros $\varepsilon(\omega)$[13], $\sigma(\omega)$[14] y $\mu(\omega)$[15] son parámetros complejos que dependen de la frecuencia de los campos armónicos. La existencia de parámetros complejos describe un desfasaje en el tiempo entre los fasores involucrados.

Consideremos un recinto del espacio donde existe un medio material de propiedades definidas por sus parámetros ε, σ y μ, dependientes de la frecuencia. Para evitar generalidades sin correlato práctico, consideramos que μ es real, mientras que $\varepsilon = \varepsilon' - i\varepsilon''$ y $\sigma = \sigma' + i\sigma''$ son la permitividad y conductividad complejas. Las ecuaciones de Maxwell sin fuentes resultan:

$$
\begin{aligned}
0 &= \nabla\overrightarrow{E}(\overrightarrow{r}) \\
0 &= \nabla\overrightarrow{H}(\overrightarrow{r}) \\
0 &= \nabla \times \overrightarrow{E}(\overrightarrow{r}) + i\omega\mu\overrightarrow{H}(\overrightarrow{r}) \\
0 &= \nabla \times \overrightarrow{H}(\overrightarrow{r}) - (i\omega\varepsilon + \sigma)\overrightarrow{E}(\overrightarrow{r})
\end{aligned}. \tag{9.8}
$$

Desacoplando las ecuaciones del rotor, se obtiene las ecuaciones de Helmholtz:

$$
\begin{aligned}
\nabla^2\overrightarrow{E}(\overrightarrow{r}) + \gamma^2\overrightarrow{E}(\overrightarrow{r}) &= 0 \\
\nabla^2\overrightarrow{B}(\overrightarrow{r}) + \gamma^2\overrightarrow{B}(\overrightarrow{r}) &= 0
\end{aligned}. \tag{9.9}
$$

Siendo $\gamma = \beta - i\alpha = \sqrt{\omega^2\mu\varepsilon - i\omega\mu\sigma}$ un número complejo.

La solución es de la Ecuación 9.9 es:

$$
\begin{aligned}
\overrightarrow{E}(\overrightarrow{r},t) &= \overrightarrow{E}_{0_+}e^{-\alpha z}e^{i(\omega t-\beta z)} + \overrightarrow{E}_{0_-}e^{\alpha z}e^{i(\omega t+\beta z)} \\
\overrightarrow{H}(\overrightarrow{r},t) &= \frac{\overrightarrow{E}_{0_+}}{\eta}e^{-\alpha z}e^{i(\omega t-\beta z)} - \frac{\overrightarrow{E}_{0_-}}{\eta}e^{\alpha z}e^{i(\omega t+\beta z)}
\end{aligned}. \tag{9.10}
$$

Donde α es el factor de atenuación, β es el factor de propagación de la onda y $\eta = \mu\omega/\gamma$ es la impedancia intrínseca.

Si aplicamos estas expresiones en los casos particulares de interés:

[13]Permitividad Eléctrica.
[14]Conductividad Eléctrica.
[15]Permeabilidad Magnética

Dieléctrico sin perdidas: Un material dieléctrico se polariza en la presencia de un campo eléctrico aplicado. Empleando el modelo de Drude-Lorentz para el caso de un dieléctrico sin pérdidas $\varepsilon \in \mathbb{R}$, $\sigma = 0$ y $\mu = \mu_0$, entonces la expresión γ queda como:

$$\gamma = \beta - i\alpha = \sqrt{\omega^2\mu\varepsilon - i\omega\mu\sigma} = \omega\sqrt{\varepsilon_0\mu_0\varepsilon_r} = \frac{\omega\sqrt{\varepsilon_r}}{c} \tag{9.11}$$

De la Ecuación 9.11 se observa que no hay atenuación y la profundidad de penetración es infinita (en la práctica, existe cierta atenuación).

Conductor: En un conductor los electrones son libres, de manera que podemos usar el modelo de dieléctricos para el movimiento electrónico anulando el término de la fuerza de cohesión de Drude. En este caso se tienen los parámetros: $\varepsilon = \varepsilon_0$, $\mu = \mu_0$ y σ real.

$$\begin{aligned} \gamma = \beta - i\alpha &= \sqrt{\omega^2\mu\varepsilon - i\omega\mu\sigma} = \sqrt{\omega^2\mu_0\varepsilon_0 - i\omega\mu_0\sigma} \\ &= \frac{\omega}{c}\sqrt{1 - i\frac{\sigma}{\omega\varepsilon_0}} \approx \frac{\omega}{c}\sqrt{-i\frac{\sigma}{\omega\varepsilon_0}} = \sqrt{\frac{\omega\mu_0\sigma}{2}}(1-i) = \frac{1-i}{\delta} \end{aligned} \tag{9.12}$$

De la Ecuación 9.12 se observa que en los conductores $\alpha = \beta = \frac{1}{\delta}$. Como el valor de σ en los conductores es muy alto:

$$\sigma_{Cu} \approx 6 \cdot 10^7 (\Omega m)^{-1} \Rightarrow \delta \cong \frac{92}{f} mm \Rightarrow \delta \cong 1{,}9 mm \ a \ f = 2{,}4 GHz \tag{9.13}$$

Entonces, la profundidad de penetración de la la OEM[16] δ es despreciable y no se propaga dentro del conductor.

Habiendo visto la propagación de ondas en medios ilimitados, se analiza el comportamiento de los campos cuando ondas electromagnéticas inciden sobre una interfase que separa dos medios de propiedades (simbolizadas por su impedancia intrínseca) diferentes. Se considera una OEM plana monocromática linealmente polarizada que incide normalmente desde un medio 1 sobre un plano interfase que lo separa de un medio 2 como se muestra en la Figura 9.21.

[16] Onda Electromagnética.

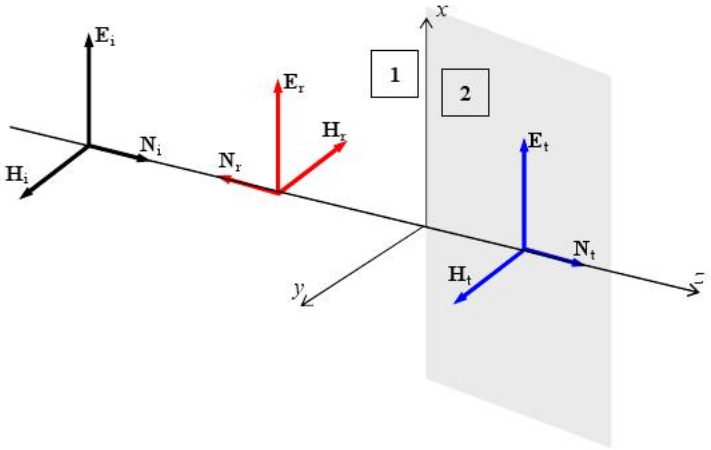


Figura 9.21: Incidencia normal sobre una interfase

La dirección de propagación es perpendicular al plano interfase y se supone que el medio de incidencia 1 no tiene pérdidas ($\gamma_1 = \beta_1$ y η_1 reales). El medio de transmisión 2 tendrá en general parámetros complejos η_2 y γ_2. Planteando las ecuaciones de los campos en las dos regiones:

Medio 1:

$$\begin{aligned} \overrightarrow{E}_1(\overrightarrow{r},t) &= E_{0_+} e^{i(\omega t - \beta_1 z)}\hat{x} + E_{0_-} e^{i(\omega' t + \beta_1' z)}\hat{x} \\ \overrightarrow{H}_1(\overrightarrow{r},t) &= \frac{E_{0_+}}{\eta_1} e^{i(\omega t - \beta_1 z)}\hat{y} - \frac{E_{0_-}}{\eta_1} e^{i(\omega' t + \beta_1' z)}\hat{y} \end{aligned} \tag{9.14}$$

Medio 2:

$$\begin{aligned} \overrightarrow{E}_2(\overrightarrow{r},t) &= E_{0_t} e^{i(\omega'' t - \gamma_2 z)}\hat{x} \\ \overrightarrow{H}_2(\overrightarrow{r},t) &= \frac{E_{0_t}}{\eta_2} e^{i(\omega'' t - \gamma_2 z)}\hat{y} \end{aligned} \tag{9.15}$$

En la región de incidencia, debe haber en general una onda incidente y una onda reflejada, debido a la presencia de la interfase que implica una discontinuidad en el medio donde ocurre la propagación. En la región de transmisión, supuesto semi-infinito, sólo hay una onda transmitida. Las frecuencias de estas tres ondas son en general diferentes.

Los campos deben cumplir las condiciones de contorno en la interfase $z = 0$. Como ambos campos son tangenciales a la superficie de separación, se conservan:

$$\begin{aligned} E_1(z=0,t) = E_2(z=0,t) &\Rightarrow E_{0_+} e^{i\omega t} + E_{0_-} e^{i\omega' t} = E_{0_t} e^{i\omega'' t} \\ H_1(z=0,t) = H_2(z=0,t) &\Rightarrow \frac{E_{0_+}}{\eta_1} e^{i\omega t} - \frac{E_{0_-}}{\eta_1} e^{i\omega' t} = \frac{E_{0_t}}{\eta_2} e^{i\omega'' t} \end{aligned} \tag{9.16}$$

Estas ecuaciones se deben cumplir para todo t. Como las funciones exponenciales complejas son ortogonales para distintos valores de ω, debe ser $\omega = \omega' = \omega''$.

$$\begin{aligned} E_{0_+} + E_{0_-} &= E_{0_t} \\ \frac{E_{0_+}}{\eta_1} - \frac{E_{0_-}}{\eta_1} &= \frac{E_{0_t}}{\eta_2} \end{aligned} \tag{9.17}$$

De estas dos ecuaciones podemos despejar E_{0_-} y E_{0_t} en función de $E0_+$:

$$\begin{aligned} \rho &= \frac{E_{0_-}}{E_{0_+}} = \frac{\eta_2 - \eta 1}{\eta_2 + \eta 1} \\ \tau &= \frac{E_{0_t}}{E_{0_+}} = 1 + \rho = \frac{2\eta_2}{\eta_2 + \eta 1} \end{aligned} \tag{9.18}$$

Las expresiones de la Ecuación 9.18 definen los coeficientes de reflexión y transmisión ρ y τ.

Dieléctrico sin perdidas: En este caso $\eta_2 \in \mathbb{R} \Rightarrow \rho \in \mathbb{R}$.
El campo reflejado se hallará en fase con el campo incidente en $z = 0$ si $\eta_2 > \eta_1$ y en contrafase en caso contrario. Sólo si las impedancias intrínsecas de ambos medios coinciden no habrá reflexión (caso de un único medio, no existe interfase).

Conductor: En este caso $\eta_2 \in \mathbb{C}$ y tiene un valor muy pequeño con respecto a la impedancia intrínseca en el vacío (η_0): $\eta_2 = (1+i)/\sigma\delta \to 0$ debido a que $\sigma \to \infty$ en los conductores. En tal caso $\rho = -1$ y se forman ondas estacionarias de E y H en el medio de incidencia. La onda de E estará desfasada en $\pi/2$ en tiempo y espacio respecto de la onda de H. Toda la potencia incidente se refleja.

En resumen, la incidencia sobre una capa dieléctricas es de interés en el diseño de superficies antirreflectantes usadas para aplicaciones ópticas y cámaras anecoicas. El caso de capas conductoras da las bases para el análisis de la efectividad y aplicación de los blindajes de alta frecuencia.

Blindaje de paredes

Existen varios métodos para aislar o blindar electromagnéticamente una área que lo requiera basados en los principios explicados en la Sección 9.4.3. Esto se detalla dado que es un requerimiento para ciertos laboratorios de la facultad que deben estar libres de interferencia electromagnética.

Láminas conductoras: Este tipo de blindaje se suele utilizar donde se emplea instrumental sensible a la radiación como por ejemplo equipos médicos de alta complejidad, como puede ser tomógrafos o equipos de resonancia magnética. Todos los componentes (puertas, ventanas , guías de onda, anclajes, uniones) deben ser es blindados como se indica en la Figura 9.22. La capacidad de atenuación es aproximadamente de $100dB$.

Figura 9.22: Blindaje de paredes con laminas conductoras

Los materiales que suelen ser utilizados son:

- Chapa de cobre y/o aluminio de 0,3/0,5mm espesor.
- Perfiles de aluminio.
- Encastres y anclajes.

Una empresa en Argentina que realiza este tipo de servicios es llamada Imglobal[17]

Pinturas: Una buena alternativa para blindar los interiores es usar una pintura conductiva diseñada específicamente para aislar radiación que proviene de las radio bases celulares, DECT[18], Wi-Fi, transformadores, redes de alta tensión, etc. Estas se componen de partículas de carbón contenidas en una emulsión de acrílico puro de alta calidad, es decir no contiene ningún componente metálico. Es resistente al agua y tiene una alta adherencia a las superficies como la pintura plástica, tableros de la construcción, cemento, yeso, poliestireno, superficies de la albañilería, mármoles, etc. La pintura es recomendada tanto para aplicaciones interiores como para exteriores, y tiene una eficiencia de blindaje de hasta $40dB$ (reducción por 99,99 %). Se aplica en las paredes como una pintura plástica normal. Luego, se puede pintar encima de la capa con una pintura plástica. Se comercializa en envases de 1 y 5 litros. Para interiores, la cobertura típica es de $7,5m^2$ por

[17]Contacto: José Echeverría 243, Barrio Alto Alberdi , CP 5003 , Córdoba Capital. Teléfono/Fax: +54-351-4806597. e-Mail: info@imglobal.com.ar

[18]Digital Enhanced Cordless Telecommunications

litro; para exteriores, la cobertura típica es de $5m^2$ por litro. Se aplica como si fuera una pintura plástica decorativa; no se necesita ninguna pericia o conocimiento técnico especial y se aplica mediante un rodillo de buena calidad.

Figura 9.23: Sala blindada con pintura

En el Cuadro 9.3 se observa una comparativa de las características de diferentes pinturas de la marca "YSHIELD"de origen Alemán.

	NFS34	**NFS54**	**NFS55**	**NFS91**
Blindaje de altas frecuencias	SI	SI	SI	SI
Blindaje de bajas frecuencias	NO	SI	SI	SI
Blindaje con 1 capa	$40dB$-99 %	$33dB$-99.98 %	$27dB$-99.8 %	$47dB$-99.999 %
Blindaje con 2 capas	$40dB$-99 %	$33dB$-99.98 %	$27dB$-99.8 %	$47dB$-99.999 %
Color	Negro	Negro	Negro	Verde aceituna
Interior/exteriores	SI/SI	SI/SI	SI/SI	SI/SI
Rendimiento en interiores	$10m^2/l$	$7{,}5m^2/l$	$7{,}5m^2/l$	$10^2/l$
Rendimiento en exteriores	$7{,}5m^2/l$	$5m^2/l$	$5m^2/l$	$7{,}5^2/l$
Compatibilidad ecológica	Buena	Buena	Buena	Buena
Base de composición	Carbono	Carbono	Carbono	Plata
Aditivo	Acrilato	Acrilato	Acrilato	Acrilato
Disolvente	Agua	Agua	Agua	Agua
Contenido VOC según CEE	$0,2g/l$	$0,2g/l$	$0,2g/l$	$0,3g/l$
Toma de tierra para interior	ES+EB	ES+EB	ES+EB	ES+EB
Toma de tierra para exterior	ESA+EB	ESA+EB	ESA+EB	ESA+EB
Disponibilidad	1/5/20 litros	1/5/20 litros	5/20 litros	1/5 litros

Cuadro 9.3: Pinturas para blindaje electromagnético

Aunque los sistemas de apantallamiento para interiores basados pinturas conductivas no necesitan una conexión a tierra para funcionar como blindaje contra la radiación, es recomendable realizar una toma de tierra para evitar la generación de campos eléctricos de baja frecuencia por el acoplamiento con el sistema eléctrica de la lugar como se puede ver en la Figura 9.24

Figura 9.24: Puestas a tierra interior (ES) y exterior (ESA)

En el caso que aparezcan grietas en las paredes en el futuro, que desconectarían posiblemente unas partes de las superficies afectadas de la toma de tierra, la cinta asegurará una conexión a tierra.

Figura 9.25: Cinta de tierra (EB)

Malla de blindaje: En nuevas construcciones o renovaciones se pueden incorporar la mallas de blindajes en el exterior, dentro o interior de las paredes y estructuras de hormigón. Estas son mallas de fibras de acero inoxidable entretejidas con una capa conductiva, resistentes a la putrefacción y a las heladas, por eso, es muy apta para aplicaciones exteriores. Una imagen de esta se puede ver en la Figura 9.26.

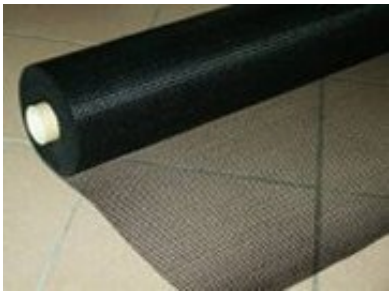


Figura 9.26: Malla de blindaje

El material tiene una eficiencia de blindaje a una frecuencia de $1GHz$ de $20dB$ (reducción de 99 %). En relación con la colocación exterior de la malla, como en techos, terrazas, etc, es aconsejable cubrir la malla después de su colocación por razones de seguridad (la tela es conductiva) y para protegerla contra cualquier posibilidad de daño. Por ejemplo: se puede sellar la tela dentro de una capa de hormigón y después colocar baldosas; se puede simplemente sellar la tela dentro de una capa de hormigón; se puede colocar baldosas encima de la tela (evitando daño a la tela); o se puede cubrir la tela con asfalto u otra forma de impermeabilidad.

Blindaje de ventanas

Para blindar las ventanas, se usa una tela tejida especial para confeccionar visillos como se puede obervar en la Figura 9.27. Esta tela, de carácter textil y sin conductividad superficial, es lavable (30°C, sin usar secadora), y mientras que parece un material de visillo cualquiera, incorpora hilos delgados de cobre cubiertos con una capa de laca para proporcionar su propiedades de blindaje contra la radiación electromagnética. La tela tiene una alta eficiencia de blindaje en todos los rangos de frecuencias usados por las redes de telefonía móvil ($32dB$, o reducción de 99,94 %, a una frecuencia de $900MHz$ y viene en rollos de 2,6m de ancho.

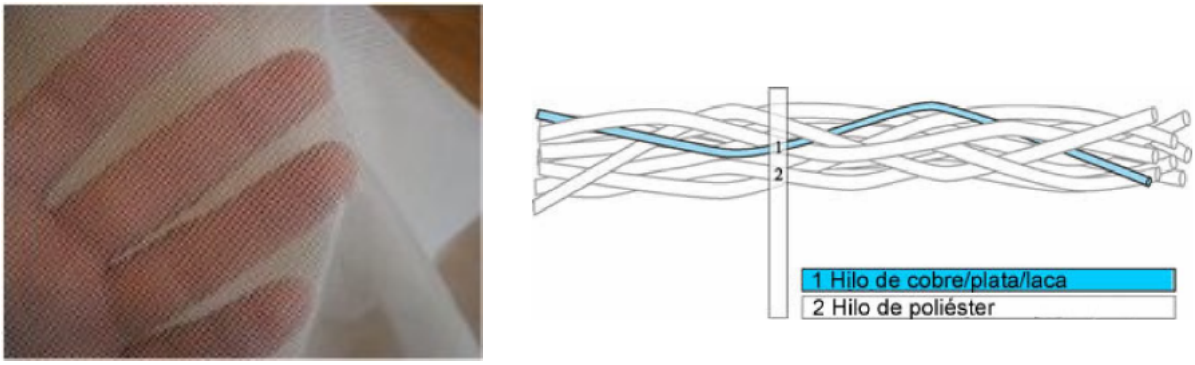


Figura 9.27: Tela de blindaje

Nota: El estándar que determina bajo que condiciones se debe determinar las características de blindaje (reducción o atenuación de potencia, frecuencia de medición, etc) los determina la norma IEEE 299-1997 "Standard Method for Measuring the Effectiveness of Electromagnetic Shielding Enclosures".

9.5. Backbone de la Red Privada

9.5.1. Dimensionamiento del tráfico

La implementación del sistema requiere que la red inalámbrica sea capaz de soportar el tráfico de datos generado por los diferentes "end system". Como ya fue estudiado, la red inalámbrica bajo el estándar IEEE 802.11g maneja una velocidad máxima teórica de 54 Mbps. La velocidad requerida por el conjunto de "end system" no se puede calcular de manera determinista, esto se debe a que el tráfico de datos generado por cada dispositivo varía de acuerdo a diferentes factores.

El ancho de banda total estimado en la red es de **80*Mbps*** teniendo en cuenta el tráfico de datos, voz y vídeo. Por lo tanto, un dimensionamiento apropiado de la red es implementar enlaces de 1*Gbps* de capacidad, exceptuando el enlace entre los switches de core que utilizan dos enlaces de 1*Gbps* que emplean LACP. Esto se debe a que como se comento en la Sección 5.3 sobre la eficiencia de Ethernet, estaría por debajo de una congestión leve con una eficiencia aproximada del 80 % en la "busy hour". A continuación se describe la obtención del cálculo del ancho de banda total desglosado en los diferentes tipos tráficos.

Tráfico de datos

Como se indicó en la Sección 5.3 sobre el análisis de tráfico LAN, la "busy hour" es de 15*Mbps*. Teniendo en cuenta la escalabilidad de la red para tráfico de datos para los usuarios en un futuro, se tendrá en cuenta un incremento del tráfico del 100 %, llegando a un total de:

Tasa de bit estimada de datos:	**30*Mbps***

Cuadro 9.4: Tasas de bits estimadas de datos

Tráfico de voz

Como se analizó en la Sección 8.4.1, el ancho de banda empleado en una comunicación telefónica depende del método de codificación empleado. Tomando el de mejor calidad, es decir mayor MOS (PCM), cada llamada demanda 80kbps de ancho de banda como se indica enl Cuadro 8.4. La cantidad de teléfonos empleados actualmente en la facultad es de un total de 300 (ver Sección 4.3), pero sabiendo que el Gateway que se propondrá en la Sección 10.1.1 puede direccionar un total de 216 llamadas simultáneas como máximo, podemos estimar que el ancho de banda total debido al tráfico de voz es aproximadamente de:

BW estimada de voz:	**18*Mbps***

Cuadro 9.5: Ancho de banda estimada de voz

Tráfico de vídeo

El tráfico de datos generado por cada cámara varía de acuerdo a una serie de factores según la referencia de estimaciones del ancho de banda de *BOSCH TECHNOLOGIES*:

- *Método de compresión de vídeo:* Típica temporal o compresión espacial: MPEG-4, M-JPEG, Wavelet y MPEG-2.
- *Tasa de imágenes:* Imágenes por segundo: 1-30 IPS.
- *Resolución de imágenes:* Número de pixeles horizontales y verticales: QCIF, CIF, 2CIF, 4CIF (conocido como full D1).
- *Actividad en la escena:* Cantidad de actividad en el campo de visión de la cámara: Baja, media y alta.

- *Tiempo muerto:* Fracción de tiempo en la que no hay movimiento (importante para los algoritmos de compresión temporal como MPEG-4, ya que se puede disminuir ancho de banda durante este tiempo): 8:00 p.m. - 6:00 a.m. Lunes - Viernes, todo el Sábado y Domingo llega cerca del 50 % del tiempo muerto.

De todos los factores descriptos anteriormente, solo la "Actividad en la Escena" es impredecible y no la podemos configurar de acuerdo a nuestra conveniencia, como es el caso de los factores restantes. Adicionalmente, la actividad en escena afecta en gran medida al método de compresión MPEG-4 utilizado en las cámaras, de tal forma, que cuando la actividad en escena es grande, MPEG-4 genera un tráfico mayor comparado al generado cuando la actividad de la escena es nula.

Es importante conocer cuál es el requerimiento de velocidad de cada cámara en distintas circunstancias y horas, de esta manera se podrá calcular de forma aproximada el consumo máximo y mínimo del sistema en su totalidad, con el fin de no sobrepasar el recurso limitado de ancho de banda que nos ofrece la red inalámbrica. Si la capacidad de la red es saturada, el sistema puede presentar:

- Pérdida de imágenes, ocasionando un vídeo entrecortado.
- La resolución del vídeo puede caer a niveles en que la imagen sea poco clara.
- El vídeo se puede congelar completamente y se puede perder la conexión.

A diferencia de las redes cableadas, las redes inalámbricas no permiten conocer de forma efectiva la capacidad de la misma, por lo tanto en el diseño se tratará de ofrecer un margen de reserva con el fin de evitar saturación incluso en las peores circunstancias.

Para obtener una determinación aproximada del ancho de banda requerido por el sistema en su totalidad, se analizará el tráfico generado por una de las cámaras con restricción en fps (frames per second) y resolución, con un nivel de actividad en escena Medio. De esta manera, se multiplicará este requerimiento por el total de las cámaras, obteniendo así una aproximación del ancho de banda generado por el sistema.

La reconocida empresa *BOSCH* indica una tabla de valores estimados de las tasas de bits generadas por las cámaras en varias configuraciones. Los valores mostrados son estimados y fueron obtenidos de una gran cantidad de proyectos previos realizados; es decir son el resultado de la experiencia.

Resolución	IPS	Nivel de Actividad	Tasa de bit (kbps)
CIF	3	Medio	160
CIF	7	Medio	185
CIF	15	Medio	200
CIF	30	Medio	500
2 CIF	3	Medio	320
2 CIF	7	Medio	370
2 CIF	15	Medio	400
2 CIF	30	Medio	1000
4 CIF	3	Medio	640
4 CIF	7	Medio	740
4 CIF	15	Medio	800
4 CIF	30	Medio	2000

Cuadro 9.6: Tasas de bits estimadas para una cámara IP

Los parámetros para la configuración de las cámaras IP que garanticen la calidad de imagen para un sistema de seguridad son:

- *Cuadros por segundo:* 15fps
- *Resolución:* 352x288 (CIF[19])
- *Nivel de actividad:* Medio

Según el Cuadro 9.6 se puede estimar la tasa de bits generada por cada cámara es de 200kbps. Colocando en promedio 20 cámaras IP por piso, se estima que el ancho de banda total del tráfico de vídeo es de:

Ancho de banda estimada de vídeo:	**32*Mbps***

Cuadro 9.7: Ancho de banda estimada de vídeo

9.5.2. Estudio de bloqueo y disponibilidad del llamado

El Erlang[20] es una unidad adimensional utilizada en telefonía como una medida estadística del volumen de tráfico. El tráfico de un Erlang ($1Erl$) corresponde a un recurso utilizado de forma continua, o dos canales utilizados al 50 %, y así sucesivamente. Por ejemplo, si una oficina tiene dos operadores de teléfono y ambos están ocupados durante todo el tiempo, esto representa dos Erlangs de tráfico.

De forma alternativa, un Erlang puede ser considerado como multiplicador de utilización por unidad de tiempo, así un uso del 100 % corresponde a 1 Erlang, una utilización de 200 % son $2Erlangs$, y así sucesivamente. Por ejemplo, si el uso total del móvil en un área por hora es de $180minutos$, esto representa $180/60 = 3Erlangs$. En general, si la tasa de llamadas entrantes

[19]El formato CIF (Common Intermediate Format) se utiliza para compatibilizar los diversos formatos vídeo digital. CIF corresponde a una resolución de 352 x 288.

[20]Ingeniero Danés A. K. Erlang, pionero de la teoría de colas.

es de λ por unidad de tiempo y la duración media de una llamada es h, entonces el tráfico A en Erlangs puede calcularse como se ve en la Ecuación 9.19.

$$A = \lambda h \tag{9.19}$$

Esto es usado para dimensionar un sistema telefónico. Por ejemplo, el tráfico medido sobre muchas horas de ocupación puede ser usado para un T1 o un E1 para determinar cuántas líneas (troncales) debieran de utilizarse durante las horas de mayor ocupación.

El tráfico medido en Erlangs es usado para calcular el nivel de servicio[21]. Hay diferentes fórmulas para calcular el tráfico entre ellas: Erlang B, Erlang C y la fórmula de Engset. Explicaremos el modelo de Erlang B y luego el modelo de Engset que es un caso particular del anterior, ya que nos basaremos en estos calculos para dimensionar el modelo del Gateway.

Fórmula Erlang B

La fórmula de Erlang B asume una población infinita de orígenes (como usuarios de telefonía), la cual ofrece tráfico en conjunto a N servidores (como líneas en un grupo de troncales). La tasa de llegadas de nuevas llamadas (tasa de nacimiento) es igual a λ y es constante, no depende del número de recursos activos, porque se asume que el total de recursos es infinito. La tasa de abandono (tasa de mortandad) es igual al número de llamadas en progreso dividida por h, la media del tiempo de llamadas en espera. La fórmula calcula la probabilidad de bloqueo en una pérdida del sistema, si un requerimiento no es atendido inmediatamente cuando trata de utilizar un recurso, y este es abortado. Por lo tanto no son encolados. El bloqueo ocurre cuando hay un nuevo requerimiento de recursos, pero todos los servidores ya están ocupados. La fórmula asume que el tráfico que es bloqueado se libera inmediatamente.

$$B(N, A) = \frac{\frac{A^N}{N!}}{\sum_{i=0}^{N} \frac{A^i}{i!}} \tag{9.20}$$

A continuación se muestra cómo puede ser expresado recursivamente, en una forma que es usada para calcular tablas de la fórmula de Erlang B:

$$B(0, A) = 1\, B(N, A) = \frac{AB(N-1, A)}{N + AB(N-1, A)} \tag{9.21}$$

donde:

B: Es la probabilidad de bloqueo

N: Es el número de recursos como servidores o circuitos en un grupo

A = λh: Es la cantidad de tráfico entrante expresado en Erlangs

La fórmula Erlang B se aplica a los sistemas con pérdidas, tales como sistemas telefónicos tanto fijos como móviles, que no ofrecen almacenamiento de llamadas (es decir, no permiten dejar la llamada "en espera"), y no se pretende que lo hagan. Se asume que las llegadas de llamadas pueden ser modeladas por un proceso de Poisson, pero es válida para cualquier distribución estadística de tiempos entre llamadas.

[21] Grade of Service

Erlang B también es una herramienta para dimensionar tráfico entre centrales de conmutación de voz.

Fórmula de Engset

La fórmula Engset[22], está relacionada con la fórmula de Erlang, pero funciona con una población finita de S orígenes en lugar de la población infinita de orígenes que asume Erlang:

$$E(N, A, S) = \frac{A^N \begin{pmatrix} S \\ N \end{pmatrix}}{\sum_{i=0}^{N} A^i \begin{pmatrix} S \\ i \end{pmatrix}} \tag{9.22}$$

Esto puede puede ser expresado recursivamente del siguiente modo, en una forma que es usada para calcular las tablas de la fórmula Engset:

$$E(0, A, S) = 1\, E(N, A, S) = \frac{A(S - N + 1)E(N - 1, A, S)}{N + A(S - N + 1)E(N - 1, A, S)} \tag{9.23}$$

donde:

E: es la probabilidad de bloqueo

A: es el tráfico en Erlangs generado por cada origen cuando está desocupado

S: es el número de orígenes

N: es el número de servidores

De nuevo, se asume que las llamadas que llegan pueden ser modeladas por una distribución Poisson y que los tiempos de espera son descriptos por una distribución exponencial negativa. Sin embargo, debido a que hay un número finito de servidores, la tasa de llegada de las nuevas llamadas decrece a medida que nuevos orígenes (como abonados telefónicos) se vuelven ocupados y por lo tanto no pueden originar nuevas llamadas. Cuando $N = S$, la fórmula se reduce a una distribución binomial.

9.5.3. Diseño con bandejas porta cables

Distribución del cableado troncal

Este tiene que ser según la norma, por dentro del edificio. La forma más utilizada es con agujeros pasantes de piso a piso, con la menos cantidad de curvas posible. La norma EIA/TIA 569A especifica como es que tienen que ser estos agujeros. Se puede pasar cables a través de tuberías u otros medios, previendo un pasaje para cables mínimo de $100mm$ por cada $5000m^2$ a abastecer, y dos iguales de repuesto. En el caso de que estos agujeros no estén alineados, hay que hacer una canal por donde pasan las tuberías u otros medios para el soporte de cables.

[22] Tore Olaus Engset (1865 - 1943)

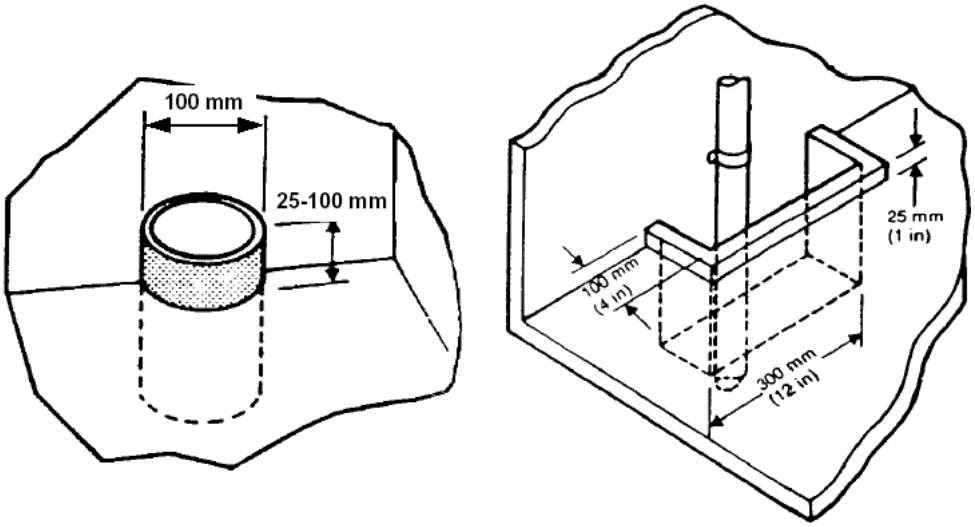


Figura 9.28: Esquemas de los agujeros montantes y canaletas entre pisos según la norma EIA/TIA 569A.

En las figuras anteriores, se puede visualizar las medidas mínimas para estos pasajes especificados por la norma. Aquí cabe destacar esto no toma en cuenta el hecho de que cableado se utiliza, ni que norma para la transmisión y que puede resultar poco práctico lo que especifica la norma. Más allá de todo esto más adelante se indicará la forma de hacer estos agujeros pasantes.

Distribución del cableado horizontal

El cableado horizontal hasta los puntos de acceso Wi-Fi (access points) se hará con el soporte de bandejas portacables cerradas de chapa de acero galvanizada y perforadas, en su mayoría por sectores que no son públicos. Hay sectores donde si bien no queda otro remedio, se dará una solución alternativa. Solo en el caso del subsuelo y entrepiso del subsuelo se pasaran las bandejas por sectores públicos, esto debido a que no posee mucha estética el lugar, y tampoco tiene sentido preservarla. Además las características de las tareas que se llevan a cabo en los predios internos de estos pisos en general pueden afectar al cableado. En el caso del área de matemática, del primer piso, que ya esta hecho con bandejas portacables, se dejará como esta implementado. El cable UTP a utilizar será cable 4 pares UTP Cat5e, preferentemente nuevo. Está la posibilidad de la reutilización de cable, si es que es de esta categoría y esta en buenas condiciones, pero se recomienda el uso de estos para el armado de cables “patch-cords” o para los cables que van desde el terminal a la roseta.

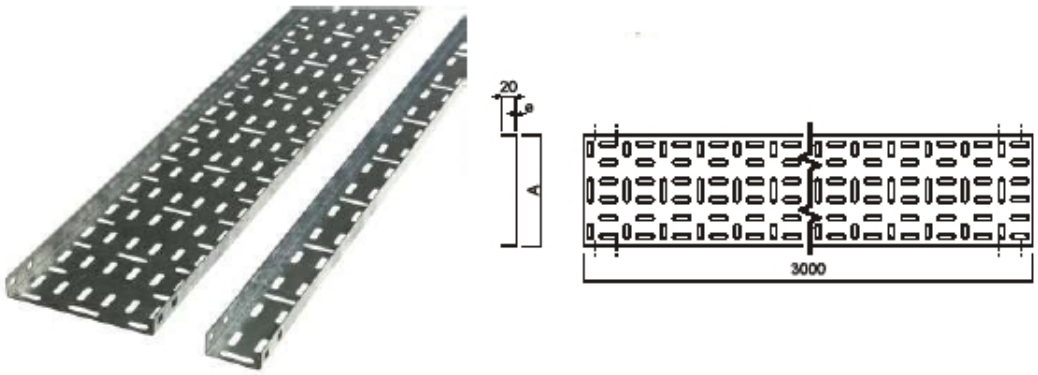


Figura 9.29: Esquema e imagen de un tramo recto de bandeja portacables.

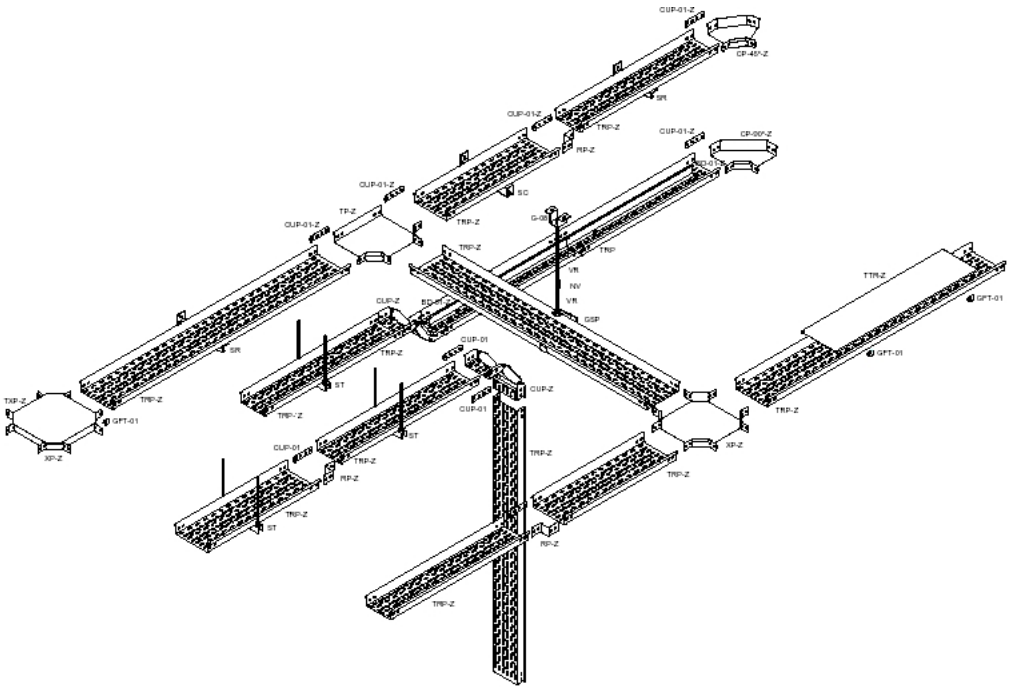


Figura 9.30: Esquema de un montaje de ejemplo realizado con bandejas portacables.

En general, las bandejas portacables, se van armando con tramos rectos, en general de tres metros de largo, y uniéndose con accesorios. Estas varían de tamaño en el ancho de su base y en el ala, que es la altura de las chapas laterales a la base. Entre ellos se unen entre si a través de cuplas de unión, estas pueden ser simples o articuladas en el caso de que las piezas a unir no estén en el mismo plano. En la Figura 9.32 se pueden visualizar estas. Todas las imágenes que se presentarán a modo de ejemplo, son de ala $50mm$ y las medidas son ilustrativas.

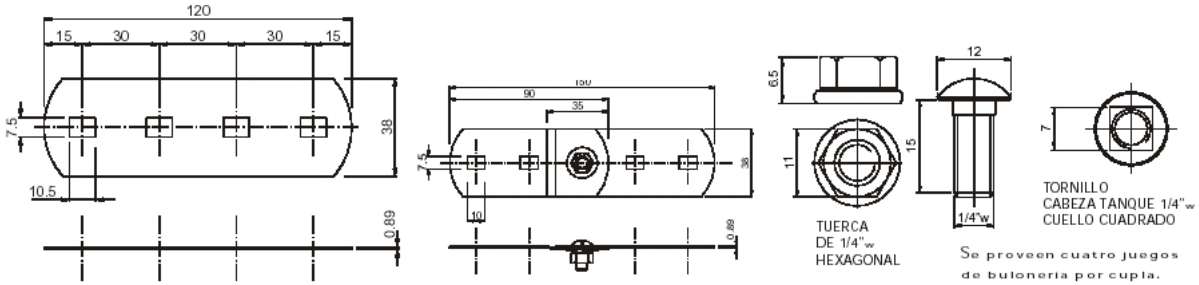


Figura 9.31: Cupla de unión simple, la cupla de unión articulada y la bulonería.

Para realizar uniones de más de 2 piezas, sea el caso de derivaciones se utilizan los accesorios que se indican en la Figura 9.33.

Figura 9.32: Esquemas e imágenes de las uniones para derivaciones en “T”y en “Cruz”.

Para realizar curvas en las bandejas portacables se utilizan los accesorios que se indican en la Figura 9.33.

Figura 9.33: Curvas en bandejas portacables: a 90 grados, a 45 grados y curvas verticales.

Para la bajada de cables a los gabinetes en los centros de distribución se utilizan los accesorios que se ilustran en la Figura 9.34.

Figura 9.34: Embudos de bajada: en forma perpendicular y en forma paralela.

Para que las bandejas portacables queden cerradas, se usan tapas, que se adaptan a cada pieza que compone las bandejas, estas se unen por medio de grampas de fijación.

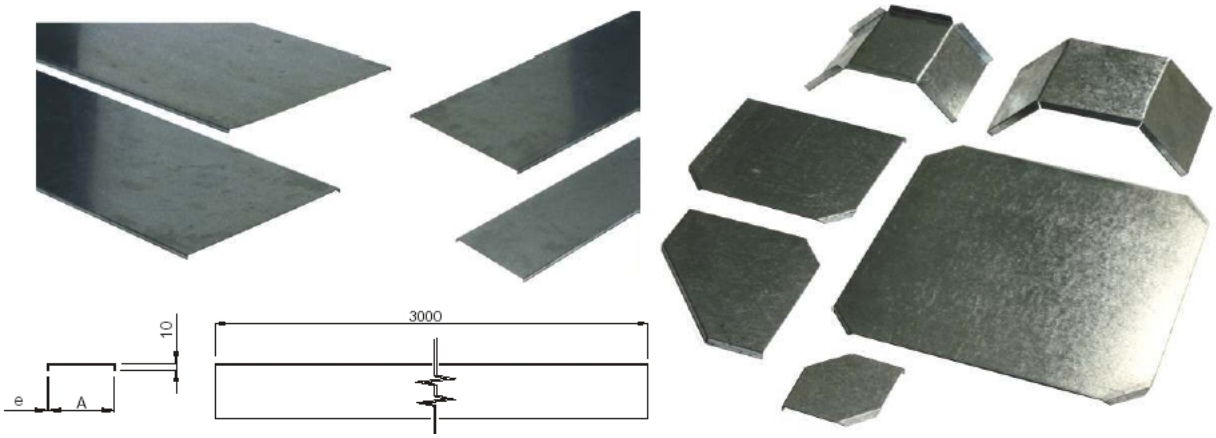


Figura 9.35: Imágenes de las tapas y grampas de fijación para las bandejas portacables.

Se usarán tres tamaños diferentes de bandeja, de acuerdo a la cantidad de cables que tienen que soportar, mismo cuando se parta del armario de telecomunicaciones con el tamaño grande de bandeja, una vez que se hayan distribuido cierta cantidad de cables y la cantidad restante pueda ser soportada por la bandeja de menor tamaño, se realizará una adaptación para poder continuar con la de menor tamaño. Solo se prescindirá de la bandeja cuando la cantidad de cables sea tal que ya no amerite el uso de tal soporte y se encuentre en un lugar que no sea público. A partir del cual se continuará con canal para cables ("cable canal"). Por una cuestión de seguridad solo se usará canal para cables en los puestos de trabajo, en la distribución no se pueden dejar expuestos los cables, por más que los cables sean pocos.

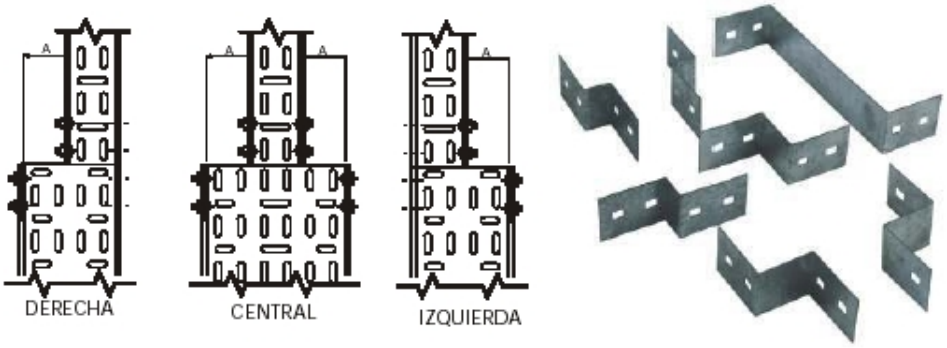


Figura 9.36: Esquemas e imágenes de los accesorios utilizados para unir bandejas portacables de diferente tamaño de base

La elección del tamaño de las bandejas es bastante controversial, esto debido a los requerimientos que imponen las normas, los accesorios disponibles para las bandejas, el criterio económico a utilizar y la conservación de la estética. En la norma EIA/TIA 569A se especifica que es recomendable para construcciones nuevas que la cantidad de cables que ocupan la bandeja, sea solo el 50 % de la capacidad de esta, así teniendo en cuenta futuras ampliaciones. Y la norma IRAM-ISO/IEC 17799 que estas tienen que estar cerradas (con tapa) en todo su trayecto.

El próximo problema a solucionar, es el como pasar las bandejas a través de las paredes, y como instalarlas para que estas soporten los cables. En construcciones existentes, el hecho de romper las paredes para el paso de bandejas portacables para después darle la terminación correcta a cada pared, es una tarea que no es recomendable en absoluto. Primero, porque llevaría un esfuerzo tremendo, no solo de trabajo, sino de tiempo y dinero. Segundo, se estaría integrando la bandeja portacables al edificio, haciendo que esta no se pueda escalar en un futuro. Otra cuestión interesante a considerar es el hecho de que si las bandejas atraviesan las paredes, se complica mucho que tengan tapas. Otra forma de paso de cables de las bandejas a través de las paredes, es la llamada "firewall penetration", en la cual se hacen agujeros circulares en las paredes, por donde solo pasan los cables. Se pueden hacer la cantidad de agujeros requerida con el fin de pasar los cables que sean necesarios, y aumentar la cantidad de estos en caso que se requiera escalar la cantidad de cables que pasan por allí.

La Figura 9.37 ilustra el paso de cables a través de las paredes y la continuidad de los tramos de las bandejas portacables, mediante la penetración firewall.

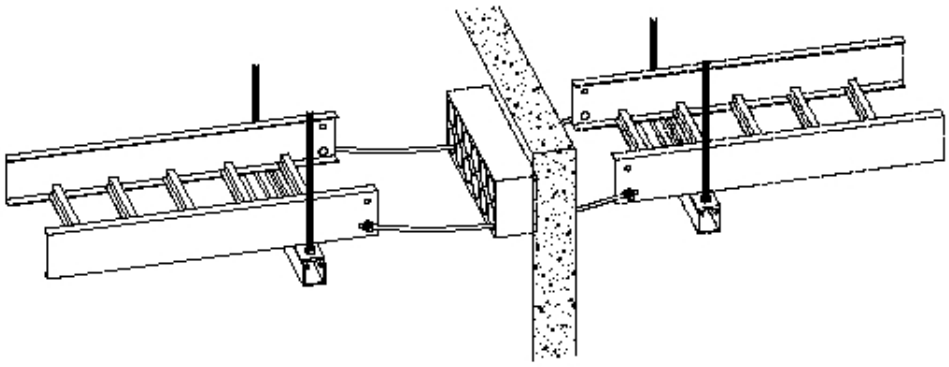


Figura 9.37: Esquemas e imágenes de los pasos a través de las paredes

El sistema de bandejas y sus soportes se vuelve totalmente independiente del paso de cables a través de la pared. De esta manera se pueden cambiar las bandejas en un futuro si es requerido. A través de unos cables conectores especiales brindados por el fabricante de las bandejas, se puede interconectar ambos extremos de los tramos de las bandejas, con el fin de que estas puedan estar conectadas a tierra en todo su trayecto. Una vez pasados los cables, se llenan los agujeros con un material removible que brinde aislamiento acústico y corte el fuego en caso de incendio. En general esta forma de paso de cables, deja los cables expuestos en la pared, pero si se quiere cumplir con la norma IRAM-ISO/IEC 17799, la bandeja tendrá que terminar justo en la pared, de forma tal que los cables no queden expuestos. Hay varias formas de lograr esto, una seria superponiendo bandejas de forma tal de que la ultima que linda con la pared, quede perfectamente ajustada a esta, otra seria que el fabricante de bandejas nos brinde las bandejas a medida. También se comercializan como accesorios, extensiones para bandejas, con el fin de aumentar discretamente el largo de estas, ya que en general estas se comercializan con un largo estándar de 3m. Hay que tener mucho cuidado en no cortar las bandejas de chapa de acero galvanizada prefabricadas e instalarlas sin ningún tratamiento previo, ya que esto llevaría a que con el tiempo estas se arruinen, mismo por oxidación. Si se cortan hay que pintarlas en los bordes cortados con un aditivo que hace que queden protegidas. En general las bandejas de chapa de acero galvanizadas se venden ya prefabricadas, en medidas estándar. Si se pide mucha cantidad, o es que se piden a medida, hay que esperar que construyan las chapas de zinc, y posteriormente las manden a galvanizar, esto hace que una vez hecho el pedido, la entrega de estas sea muy lenta. También se puede usar bandejas de otro material, que se pueda cortar sin problemas, como ser bandejas de fibra de vidrio o de aluminio por dar ejemplos. Pero cabe destacar que el costo se incrementa con estas opciones. Ahora con esta forma de pasar los cables por las paredes e interconectar las bandejas, si se puede mezclar bandejas con diferente tamaño de ala sin que los cables resulten expuestos. El único requerimiento para hacer esto es que haya una pared en un sector privado, en el cual se pueda hacer este tipo de penetración. Los agujeros en las paredes se pueden hacer con perforadoras con brocas de diamante o con coronas dentadas de diamante. La herramienta se fija en un soporte especial para taladrar sin necesidad de herramientas y puede fijarse sin problemas en las paredes con tacos o una bomba de vacío. El sistema completo (máquina con soporte) tiene un peso aproximado de $25kg$, por lo que resulta ideal para fijarlo en la pared.

Estas mismas maquinas son las necesarias para hacer los agujeros pasantes de piso a piso en el cableado troncal. Esta ofrece numerosas ventajas frente a otras herramientas similares.

Es ideal para taladrar sin sacudidas y de manera muy precisa en hormigón armado y muros de ladrillo. Además, en combinación con la bomba de vacío, es capaz de taladrar en mármol.

Como se menciono anteriormente, una limitación importante es la falta de algunos planos de servicios, esto lleva a tener un cuidado especial donde es necesario hacer perforaciones. El hecho de dañar un caño de gas u otros riegos que podrían causar una catástrofe, o de encontrarse con una viga, que pueda romper la herramienta o simplemente haber hecho un agujero enorme a la mitad, lleva a que antes de hacer una perforación hacer un análisis de lo que pueda haber en el medio. Mismo no solamente antes de la perforación, sino en la etapa de validación del diseño de distribución de bandejas portacables, antes de realizar el pedido de las mismas. De esta manera se minimizan los imprevistos en la etapa de instalación. El análisis a realizar es por medio de detectores de objetos, estos detectan objetos de todo tipo dentro de la pared, no solamente metales. Hay muchos tipos de detectores, y estos varían mucho en precio y en la penetración del análisis. Mismo se pueden utilizar para seguir cañerías y cables.

En lo que se refiere al soporte de las bandejas portacables, estas estarán sostenidas por un soporte trapecio desde el techo y desde la pared lateral donde esto no sea posible.

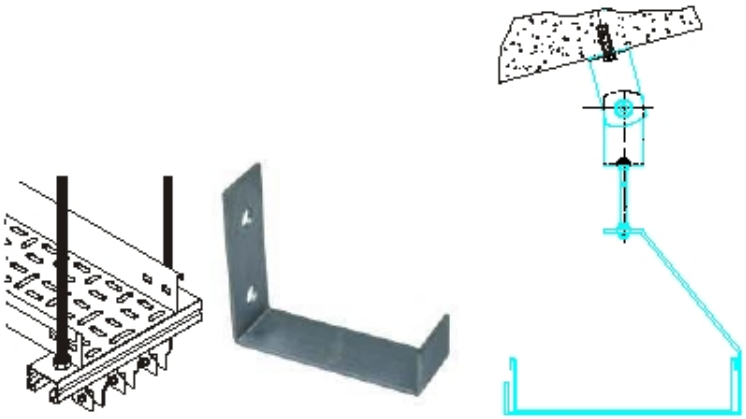


Figura 9.38: Soportes más comunes para el tendido de las bandejas portacables.

Los temas relacionados con los soportes y su ubicación, son la deflexión de las bandejas y su carga de trabajo. A continuación se hará una introducción del significado de estos parámetros y como tienen que ir ubicados los soportes en las bandejas portacables.

Capítulo 10

Construcción del prototipo

10.1. Equipos Propuestos

10.1.1. Intermedia System

Access Points

Los equipos que funcionan bajo el estándar 802.11n no están homologados, y en general, es difícil conseguir información sobre los mismos debido a que la norma IEEE 802.11n se encuentra en etapa de desarrollo. Si bien muchas empresas promocionan equipos que dicen cumplir dicha norma, son pocas las que actualmente los venden. Por esta razón y para que el proyecto resulte factible, es que se decide emplear equipos que cumplan el estándar IEEE 802.11g aunque las ventajas que promete la norma 802.11n sean más que obvias.

El modelo Colubris MSM-410 que se puede apreciar en la Figura 10.1, permite una conexión bajo múltiples estándares: 802.11$a/b/g/n$. Cuenta con una antena de 2,7dBi a 2,4GHz y una potencia de transmisión y una sensibilidad a la recepción de buena calidad. También cuenta con la posibilidad de ser alimentado directamente mediante POE[1] y sus puertos son Gigabit Ethernet. Lamentablemente no está homologado por la CNC[2] por ser un equipo muy nuevo. Sus prestaciones son muy buenas teniendo en cuenta que además estaría preparado para transmitir en 802.11n en caso de querer empezar a hacerlo, pero lo hemos descartado por no haber conseguido suficiente información sobre el mismo, y por lo dicho en el párrafo anterior sobre la disponibilidad de 802.11n

[1] Power Over Ethernet
[2] Comisión Nacional de Comunicaciones

Figura 10.1: Access Point Colubris MSM-410.

El modelo Colubris MAP-320 que se puede apreciar en la Figura 10.2, en realidad es parte de una familia de varios modelos entre los que se encuentran también el MAP-330 Dual Radio Access Point y el MAP-320R Outdoor MultiService Access Point. La diferencia radica en que el MAP-320 es para uso indoor y el MAP-320R tiene la posibilidad de funcionar transmitiendo en modo dual (a 2,4GHz y 5GHz a la vez). El MAP-320 es un equipo un tanto antiguo comparado con el Colubris MSM-410 ya que no brinda 802.11n ni es Gigabit Ethernet, sin embargo es POE y tiene buena potencia de transmisión y sensibilidad en su receptor. Además cuenta con la homologación por parte de la CNC, razón por la que fue considerado.

Figura 10.2: Access Point Colubris MAP-320.

El modelo Aruba AP-125 que se puede apreciar en la Figura 10.3, es un equipo de similares características al Colubris MSM-410 ya que es 802.11n, tiene interfaces Gigabit Ethernet y POE. Como diferencia podemos observar que cuenta con antenas externas MIMO. Como desventaja tiene el no estar homologado en la CNC, algo que comparte con todos los equipos 802.11n que investigamos.

Figura 10.3: Access Point Aruba AP-125.

El modelo Aruba AP-61 que se puede apreciar en la Figura 10.4 junto con el Aruba AP-60 es un equipo que compite con el Colubris MAP-320 ya que tampoco es 802.11n y se encuentra entre la gama de los mejores equipos 802.11g que es en lo que estamos particularmente interesados. EL AP-60 cuenta con antenas externas intercambiables lo que permitiría una ganancia extra con el uso de buenas antenas, pero notamos que el que viene con la antena dual omni-direccional integrada ya cuenta con una buena ganancia por lo que nos enfocaremos en el AP-61. El mismo cuenta con interfaces Fast Ethernet y POE, cuenta con las mejores especificaciones de potencia de salida que pudimos encontrar: $20dBm$ ($100mW$), al límite de lo que permite el estándar: ($100mW$). Cuenta también con la homologación correspondiente por parte de la CNC.

Figura 10.4: Access Point Aruba AP-60 y AP-61.

Finalmente, el modelo Proxim AP-8000 que se puede apreciar en la Figura 10.5 es un equipo que puede funcionar en 802.11n como el modelo Aruba AP-125 y el Colubris MSM-410. Presenta interfaces Gigabit Ethernet y POE. Cuenta con antenas MIMO, para aprovechar al máximo las características del protocolo 802.11n. Tiene la capacidad de transmitir en modo dual (2.4GHz y 5GHz)

Figura 10.5: Access Point Proxim AP-8000.

En los Cuadros 10.1 y 10.2 se puede apreciar un resumen de las características de los equipos propuestos, junto con sus costos.

Marca	**Colubris**	**Colubris**	**Aruba**
Modelo	MSM-410	MAP-320	AP-125
POE	Sí	Sí	Sí
Costo	-	U$S 405	-
Antena	2,7dBi @ 2,4GHz	Sin Ganancia	Sin Ganancia
Transmisor	18dBm	18dBm	20dBm
Sensibilidad	$-87dBm$	$-87dBm$	$-88dBm$
Velocidad	Gigabit Ethernet	100Mb Ethernet	Gigabit Ethernet
Homologado por CNC	No	Sí	No
Tecnología	802.11a/n 802.11$b/g/n$	802.11$a/b/g$	802.11a/n 802.11$b/g/n$

Cuadro 10.1: Access Points propuestos

Marca	**Aruba**	**Proxim Wireless**
Modelo	AP-61 Single Radio	AP8000
POE	Sí	Sí
Costo	U$S 320	-
Antena	2,4GHz – 2,5GHz / 2,8dBi	1,5dbi @ 2,4GHz
Transmisor	20dBm	19,5dBm
Sensibilidad	$-85dBm$	-
Velocidad	Fast Ethernet	Gigabit Ethernet
Homologado por CNC	Sí	No
Tecnología	802.11$a/b/g$	802.11a/n 802.11$b/g/n$

Cuadro 10.2: Access Points propuestos cont.

Dentro de los access points que se han propuesto, se opta finalmente con el que mejor se ajusta a las especificaciones fijadas. Se propone el empleo del AP Aruba AP-61 Single Radio, ya que este cuenta con la homologación por parte de la CNC y a diferencia del Colubris que también está homologado, tiene mayor ganancia de antena y un costo inferior. También cuenta con una de las potencias de transmisión más elevadas entre los equipos considerados (20dBm) y una sensibilidad dentro del rango de todos los equipos. Cuenta también con la posibilidad de configurar WVLANs y de soportar todos los protocolos de seguridad que ya hemos mencionado cuando tratamos la especificación. Sin embargo cabe destacar que eso mismo es también soportado por todos los equipos aquí presentados.

Con respecto a los equipos 802.11n si bien no se decidió por ellos a favor de un trabajo más cerrado, y que tenga la posibilidad de cumplir con los requisitos de la materia para los cuales se necesita conocer el costo de los equipos y tiene que estar disponible toda la documentación necesaria para que los equipos sean configurables por los empleados del centro de cómputos, se los analizó en profundidad aquí y se estudió el protocolo correspondiente 8.1.8. Esto deja sentadas las bases para una futura actualización de los APs a unos que cumplan dicho protocolo cuando éste sea un estándar cerrado.

Controladores

En la sección 9.4.1 se habló de la importancia y necesidad de usar un controlador para los APs. En el Cuadro 10.3 se puede ver un resume de las características de aquellos que fueron estudiados para este proyecto.

Marca	**HP - Colubris**	**Aruba**	**Aruba**
Modelo	MSM750	6000	3600
Capacidad de Usuarios	2000	32768	2048
Capacidad de APs	200	8192	512
Costo	-	-	U$S 12.240

Cuadro 10.3: Controladores

Figura 10.6: Controlador Colubris MSM-750.

Figura 10.7: Controlador Aruba 6000.

Figura 10.8: Controlador Aruba 3600.

Entre los controladores propuestos, se observa que el AC Aruba 3600 tiene dimensionamiento acorde al que se necesita para la cantidad de usuarios de la facultad (ver Figura 10.8). En la Sección 4.3 se determinó que la cantidad de PCs actuales ronda las 800 y, si bien no se puede determinar con precisión la cantidad de teléfonos, se estima que hay aproximadamente 300. Por lo tanto, para satisfacer las necesidades de la facultad en la actualidad, seria necesario 1100 conexiones Wi-Fi posibles. El equipo seleccionado duplica este número. Con respecto a la cantidad de AP posibles de controlar, nos encontramos con un margen muy amplio, ya que a razón de alrededor de 12 APs por piso deberíamos estar calculando una centena de AP en toda la facultad. Habiendo hecho este simple cálculo, se puede apreciar que el Aruba 6000, que se puede apreciar en la Figura 10.7 es excesivo, ya que cuenta con la posibilidad de controlar hasta 32768 usuarios, y tiene la posibilidad de que se le agreguen varias bahías de expansión. No se ha optado por el equipo de Colubris (Figura 10.1), si bien está dentro del rango del Aruba 3600, para mantener consistencia de fabricantes y evitar incompatibilidades, y porque no se encontró un costo realista para el mismo.

Switches

Switches de borde: Como se analizó en la Sección 9.5.1 se requieren interfaces Gigabit Ethernet ya que permitirán una posible migración al uso de Access Points que cumplan el estándar IEEE 802.11n más fácilmente, ya que estos utilizan interfaces de estas características para soportar los 300$Mbps$ de velocidad que promete la norma. Esto se tuvo en cuenta a pesar de haber elegido Access Points para usar en 802.11g por las razones ya explicadas en esta misma sección.

No debe dejarse de lado en los requerimientos, que los switches mismos alimenten los APs a través de POE[3], ya que de lo contrario, los mismos deberían ser alimentados independientemente mediante fuentes de 48V con todas las desventajas que esto presenta. Otra razón para que se requiera POE es que ayuda a centralizar la alimentación eléctrica permitiendo que los APs compartan la fase con el switch. Los administradores de la red podrán realizar un empleo eficiente de la misma, segurizando mediante UPS y disyuntores en forma centralizada, de forma tal que se logre alimentar independientemente los equipos del resto de la Universidad de una forma adecuada.

Con respecto a la cantidad de interfaces: se utilizarán aproximadamente veinte APs por piso para satisfacer los requerimientos de cobertura, divididos entre dos switches de piso. Por lo que orientamos nuestra búsqueda a switches de 16 o 24 interfaces.

En el Cuadro 10.4 se presenta un resumen de las características más importantes de los switches propuestos.

Marca	**Cisco**	**Cisco**	**3Com**
Modelo	SRW-2016	SGE-2000P	4200G PWR
POE	Sí	Sí	Sí
Costo	U$S 371	U$S 877	U$S 1.280
Ubicación	Borde	Borde	Borde
Puertos	16	24	24
Velocidad	Gigabit Ethernet	Gigabit Ethernet	Gigabit Ethernet

Cuadro 10.4: Switches de borde propuestos

Se tiene en cuenta que todos los switches considerados soportan VLAN, QoS y SNMP[4].

[3]Power Over Ethernet
[4]Simple Network Managment Protocol

Figura 10.9: Switch Cisco SRW-2016.

Figura 10.10: Switch Cisco SGE-2000P.

Figura 10.11: Switch 3com 4200.

La oferta y variedad de switches es realmente imponente, hemos tratado de incluir un equipo por marca, entre las que consideramos como fabricantes de switches más importantes: Cisco y 3Com. Es importante destacar que cada una de ellas tiene una enorme

diversidad de modelos, y que existe un modelo de switch que se acomoda a nuestras necesidades dentro de cada una. Es por eso que la elección no solo contempla requerimientos técnicos sino también la experiencia y la calidad ya sabida de ciertos fabricantes. Cisco especialmente cuenta con muchos años de experiencia y robustez en equipamiento. Es por eso que nos hemos inclinado hacia un equipo de la mencionada marca.

Por estas razones observamos que el Switch Cisco SRW-2016 cumple con todas estas características y posee el menor costo.

Switches de core: Los dos switches actuales cumplen con los requerimientos técnicos, por lo que se propone reutilizar los Switch 3Com 4900 cuyo modelo se puede observar en la Figura 10.12. Es importante destacar que estos switches se encuentran actualmente discontinuados por la marca 3Com. Creemos que no es necesario el cambio de estos equipos.

Figura 10.12: Switches 3com de la familia 4900.

Media-Gateway

Dentro de los muchísimos parámetros a tener en cuenta al decidir un modelo de media-gateway, los dos parámetros más importantes son:

- La cantidad máxima de terminales que pueden conectarle.
- La cantidad máxima de llamadas que puede procesar simultáneamente.

La cantidad máxima de terminales que pueden conectarse físicamente al equipo no es un problema en este caso ya que al usar acceso inalámbrico esto no consiste en una limitación. En caso de usarse una red cableada, habría que decidir que tipo de teléfono usar si analógico TDM, digital o IP y agregar al gateway el módulo de expansión correspondiente para albergar dichos terminales.

Para la cantidad máxima de llamadas simultáneas, utilizaremos la fórmula de Engset (Ecuación 9.22) ya que contamos con un número finito de líneas entrantes (los teléfonos).

Como se hizo notar en el relevamiento original, se cuenta actualmente con 300 teléfonos distribuídos en toda la facultad, tomando entonces una base de 450 teléfonos (aprovechando este trabajo para planear un crecimiento de líneas del 50 %) con una utilización importante o sea un tráfico excesivo de 0,25$Erlangs$ (lo que implica que la línea esta siendo usada un 25 % del tiempo, tenemos un tráfico total de 112,5$Erlangs$) permitiendo un bloqueo (la imposibilidad de realizar un llamado en el momento) del 1 % son necesarios 128 canales lógicos. Con un bloqueo del 0.1 % la cantidad de líneas aumenta a 138.

Por estas razones el media-gateway Avaya G450 se ajusta a nuestras necesidades ya que puede controlar hasta 206 llamadas simultáneas, un número mucho mayor que las 32 que soporta el modelo anterior en capacidad, el Avaya G350.

Figura 10.13: Media Gateway Avaya G450

En la Figura 10.13 se muestra un G450 con varias placas de expansión. En el caso de la facultad solo se necesitará el modulo del servidor (el módulo Avaya S8300) que se aloja únicamente en el primer slot del equipo. El mismo es el que controla las funciones del G450 y aloja el sistema operativo Linux con el software de administración propietario de Avaya® (Communication Manager). El costo del equipo básico incluyendo el servidor Avaya S8300 es de U$S 4720.

Firewall

Para la implementación de los firewalls se recomienda emplear una soluciones freeware, es decir, implementar software libre especifico sobre plataforma GNU/Linux. La principal ventaja que esta solución presenta es que se puede obtener similares prestaciones pero a costos muy reducidos y sin la necesidad de pagar licencias. La distribución linux podría ser "Gentoo" o "Red Hat", las cuales se puede encontrar mucha información en foros. En la Figura 10.14 se puede observar el hardware recomendado para emplear en el firewall por su capacidad de procesamiento, escalabilidad y por poseer interfaces GB Ethernet.

Figura 10.14: Firewall HP Proliant ML 150 Generation 5

Las principales carácteristicas se describen a continuación:

- Procesador: 1x Procesador Intel® Xeon® E5405 Quad Core de $2GHz$. Ampliable a doble procesador.
- Memoria caché interna: 2 x 6 MB de caché integrado de nivel 2.
- Chipset: Chipset Intel® 5100.
- Memoria: DIMMs PC2-5300 de memoria intermedia registrada (DDR2-667). $2GB$ de memoria estándar extendible a $16GB$. Bus frontal de $1333MHz$. 6 ranuras DIMM.

- Interfaz de red: Adaptador servidor integrado HP NC105i PCI Express Gigabit 10/100/1000 WOL (Wake on LAN, conex. remota de ordenador).
- Puertos de E/S externos: Paralelo - 0; serie - 1; dispositivo de puntero (ratón, PS2) - 1; gráficos - 1; teclado (PS2) - 1; USB 2.0 Puertos dedicados USB - 8 en total (4 posteriores, 2 en panel frontal, 2 internos), 1 (disponible para conectividad con cinta USB); Red RJ-45 (Ethernet) - 1 (10/100/1000 *Gbps*); Gestión remota: 1 (10/100) a través de tarjeta de gestión remota HP ProLiant 100 G5 Lights-Out 100c.
- Ranuras de expansión: Dos (2) PCI-Express x8, Tres (3) PCI-Express x4 (8 conectores) y una (1) PCI (32 bits/33 MHz). Una ranura designada para tarjeta opcional de gestión remota HP ProLiant 100 G5 Lights-Out 100c.
- Costo: U$S 725.

Servidor de vídeo

El mercado ofrece gran diversidad de aplicaciones de software que permiten la administración de cámaras, ofrecen interfaces amigables y son soportados por diversos sistemas operativos. El sistema SISTORE MX NVS de Siemens, está diseñado para integrar sistemas de seguridad independientes y centralizar su monitoreo.

SISTORE MX NVS cuenta con las siguientes características:

- Permite la grabación y monitoreo de vídeo proveniente de hasta 32 cámaras IP.
- Detección de movimiento integrado.
- Detección de sabotaje de cámara integrado.
- Fácil orientación de cámaras de acuerdo a las características del sitio.
- Acceso remoto usando RemoteView software.
- Escalabilidad, soporta desde una cámara hasta miles.

SISTORE MX NVS es un software para grabación de vídeo de red, permite la visualización de imágenes en tiempo real, grabación de dichas imágenes, revisión de imágenes grabadas anteriormente y acceso remoto para más de 32 cámaras IP por sistema instalado. Este software de vídeo satisface los requerimientos para aplicaciones especiales de seguridad con óptimos resultados.

En la Figura 10.15 se puede observar el servidor para el almacenamiento de vídeo, cuyas principales características son:

- El software SISTORE MX graba las imágenes provenientes de las cámaras directamente en discos locales o en unidades ópticas CD-R/CD-RW o DVD-R/DVD-RW.
- Los archivos grabados por este software tienen extensión .AVI o .k26.
- La resolución de las imágenes grabadas es de 384 x 288 píxeles (estándar) o de 704 x 288 píxeles (alta resolución).

- Compresión: M-JPEG, configurable: variable entre 10 y 80 KB.
- Velocidad de grabación de hasta 200fps configurable por cámara.
- Entradas de vídeo: 32 (16 for type 3204)x CVBS (BNC sockets), 1 Vpp / 75 Ohm, 32 IP entradas de cámara sobre 1x LAN.
- Salidas: 1 x VGA, 2 x CVBS (BNC socket).
- Interfaces: Interfaces 2 x RS485, 1 x LAN, 4 x USB, 1 x SCSI, 1 x VGA, 1 x Audio in, 1 x Mic in, 1 x Audio out.
- Capacidad de Memoria: 250/500/1000 GB memoria de datos.
- Medio Externo: almacenamiento conexión vía red, USB.
- Busqueda Imagen por medio de fecha, hora,numero de cámara, grabación evento, busqueda actividad grafica , logbook, SmartSearch.
- Control Eventos: evento-disparo grabación de cámaras individual o por grupo de cameras con slot-tiempo de pattern configurable. Eventos: contactos de alarma, detección de movimiento, control de tiempo, comandos TCP/IP.
- Señalización Alarmas vía conexión monitor, salida digital, LAN/WAN a estación remota RemoteView.

Figura 10.15: Servidor SISTORE MX.

La Figura 10.16 muestra un ejemplo de la pantalla principal del software, en ella se observan los campos que se necesita conocer al momento de operar el sistema y que se indican a continuación:

Figura 10.16: Captura de pantalla del Sistore MX.

1. Información y condiciones del sistema: Muestra la fecha y hora actual del sistema. Además de un grupo de indicadores de cambio de estado de alguno de los dispositivos instalados, ya sean cámaras o entradas digitales de alarma. Adicionalmente presenta la capacidad disponible del disco duro expresada en porcentaje, este dato informa al administrador del sistema cuando el disco esta próximo a llenarse y se debe realizar los respaldos correspondientes para proceder a vaciarlo. Las alternativas de las señales de estado se detallan más adelante.

2. Cuadro inicial: Muestra la presentación del software, marca y modelo.

3. Barra de estado: Muestra información general del sistema.

4. Área de visualización de vídeo: En esta área se muestra la imagen de las cámaras, se puede configurar el número de cámaras que se visualizan al mismo tiempo.

5. Ventana de cámara: Área que muestra la imagen captada por una cámara específica.

6. Barra de herramientas: Las opciones posibles se detallan en el siguiente sección.

7. Barra de menú: Contiene las principales funciones de administración y configuración del sistema.

Las característica de este sistema son suficiente para la aplicación del presente proyecto, el costo del mismo ronda en los U$S 3836.

10.1.2. End System

Receptores Wi-Fi

Para los receptores Wi-Fi, propondremos del tipo PCMCIA para las laptops que pudieran no tenerlo ya incorporado, dispositivos con conexión USB para brindar otra opción a PCs o laptops y placas PCI Wi-Fi estándar para ser montados en PC de escritorio. De esta forma se podrán utilizar todas las PC disponibles actualmente por la facultad para integrar la red Wireless.

Placa PCMCIA Encore ENPWI-G2 54*Mbps* Cardbus II: Este es un receptor para notebook cuya imágen se puede observar en la Figura 10.17. Las principales características son:

- Soporta WPA, WPA2, y 64/128 bits WEP cifrado de datos para la seguridad de la red
- Estándar: IEEE 802.11g y IEEE 802.11b
- Wireless Frequency Band: 2,400 - 2,4835 GHz
- 13 Channels (Japan) / 13 Channels (mayoría de los países europeos, ETS)
- Antena Tipo: 2dBi de ganancia.
- Sensibilidad del receptor:
  - 54$Mbps$: Típico - 73dBm @ 10 % PER
  - 11$Mbps$: Típico - 85dBm @ 8 % PER
- Rangos de frecuencias: 2412 2484 MHz Band ISM (canales 1 14)
- Esquemas de modulación: DBPSK/DQPSK/CCK/OFDM
- Potencia del transmisor:
  - Mínimo 15dBm @ 802.11b
  - Mínimo 12dBm @ 802.11g

Figura 10.17: Encore PCMCIA ENPWI-G2 54$Mbps$

Con respecto a sus características wireless podemos observar que está al nivel de otros equipos del mercado. Elegimos este por tener una buena disponibilidad en Argentina y un precio de mercado competente. Su costo es de U$S 24,4.

D-link 802.11*g* Wireless LAN USB Adapter: Con respecto al dispositivo USB, nos orientamos en la búsqueda de uno que cumpla con las características necesarias de conectividad y que además tenga disponibilidad en el país. Tal es el caso del D-link 802.11*g* Wireless LAN USB Adapter el cual se puede observar en la Figura 10.18. Su costo es de U$S 15,8.

Figura 10.18: D-Link 802.11*g* Wireless LAN USB Adapter.

- Estándares soportados:
  - 802.11*g*: velocidad hasta 54$Mbps$.
  - 802.11*b*: velocidad hasta 11$Mbps$.
- Tecnología de transmisión: DSSS
- Rangos de frecuencias: 2412 2484MHz Band ISM (canales 1 14)
- Tipos de modulación: DBPSK, DQPSK, CCK, OFDM
- Potencia de transmisión en 802.11*g*:
  - $+10dBm$ @ 54$Mbps$ y 48$Mbps$
  - $+12dBm$ @ 36$Mbps$ y 24$Mbps$
  - $+14dBm$ @ 18, 12, 9 y 6$Mbps$
- Sensibilidad del receptor en 802.11*g* (@ 10 % PER): $-66dBm$ at 54$Mbps$

Placas de Red:

- *Linksys Wireless-g Wi-Fi:* En la Figura 10.19 se puede observar la respectiva placa de red.

Figura 10.19: Placa de Red Linksys Wireless-g Wi Fi.

A continuación se detalla las principales carácteristicas:

- Opera en el espectro de las frecuencias de $2.4GHz$ con un flujo máximo de $54Mbps$
- Cumple con las normas IEEE $802.11g$ y compatible con el estándar $802.11b$
- Soporta hasta 128 bits de encriptación WEP y seguridad WPA
- Interfaz PCI de 32 bits
- 11 Canales (América)
- 13 Canales (Europa y Asia)
- Antena de $5dBi$
- Potencia de transmisión:
  - $15dBm$ @ $54Mbps$
  - $19dBm$ @ $11Mbps$
- Sensibilidad:
  - $-70dBm$ @ $54Mbps$
  - $-85dBm$ @ $11Mbps$

- *D-link Wi-Fi Pci 54Mbps Wireless:* La misma se puede observar en la Figura 10.20.

Figura 10.20: D-link Wi-Fi PCI 54 *Mbps* Wireless.

Presenta las siguientes características bajo el estándar IEEE 802.11g:

- Esquemas de radio y modulación: BPSK, QPSK, 16QAM 64QAM y OFDM
- Frecuencia de operación: $2.4GHz$ a $2.4835GHz$
- Canales:
  - 11 para EE.UU y América Latina
  - 13 para Europa
- Potencia de salida del transmisor: $17dBm$ (típica)
- Sensibilidad del Receptor: $-72dBm$ @ $54Mbps$

Habiendo comparado ambas placas, notamos que si bien ambas comparten la mayoría de las prestaciones, la Placa de Red D-link Wi-Fi PCI $54Mbps$ Wireless tiene un mejor desempeño en cuanto a potencia de transmisión y sensibilidad. Por lo que nos hemos decidido por ella. Su costo es de US$ 25,75.

Cámaras IP

Las cámaras necesarias para el presente proyecto deben cumplir entonces niveles de calidad en imagen y en desempeño correctas pero sobretodo nos centraremos en las prestaciones acordes a Wi-Fi en potencia del transmisor y sensibilidad de receptor necesarias.

La cámara VIVOTEK IP7152 presentada en la Figura 10.21 está equipada con sensor CCD de escaneo progresivo, ofrece una calidad superior de vídeo para aplicaciones profesionales de vigilancia. Puede capturar imágenes nítidas y claras de alta resolución de objetos en movimiento. En combinación con el alto rendimiento del sensor CCD de exploración progresiva y su filtro IR (removible) ofrece imágenes de alta calidad incluso en condiciones de baja luminosidad. Compresión MJPEG y MPEG-4.

Figura 10.21: Cámara VIVOTEK IP7152.

Características principales:

- Sensor CCD de escaneo progresivo con resolución VGA.
- Lente verifocal de 2,9 8,2mm, autoiris.
- Selección apropiada de Lente con montaje CS.
- Filtro IR Removible para funciones de Día y Noche.
- Compresión MJPEG y MPEG-4 (Dual-Codec) en tiempo real.
- Soporta secuencia dual simultánea.
- Soporta IEEE 802.11b/g.

La cámara Vivotek IP7139 presentada en la Figura 10.22, es una cámara de red profesional con resolución de mega píxeles para aplicaciones de vigilancia en interior y supervisión de detalles remotos. Equipado con un sensor CMOS de 1.3 Mega-píxeles (1280x1024) que brinda detalles superiores de imagen la cual podría ser la mejor opción para monitorear áreas extensas.

Figura 10.22: Cámara VIVOTEK IP7139.

Características principales:

- Sensor CMOS de un Mega-píxel.
- Selección Apropiada de Lentes con Montaje CS.
- Tarjeta Slot CF para Almacenamiento Local.
- Compresión de Vídeo MPEG-4 y MJPEG (Codecs Dual).
- Soporta Secuencia Dual Simultáneamente (Secuencia RTSP para Modo MPEG-4 con resolución superior a 800x600: Servidor MJPEG con resolución superior a 1280x1024).
- Soporta Vigilancia móvil 3GPP.
- Soporta Audio de 2 vías.
- PoE (Power Over Ethernet) compatible 802.3af incorporado.
- Un D/I y un D/O para Sensor y Alarma.
- Soporta IEEE 802.11*b/g*.

La cámara IP inalámbrica DLINK modelo DCS-3420 presentada en la Figura 10.23 está equipada con un sensor CCD de alta calidad, zoom digital, capacidad de grabación con poca luz o ausencia de luz y funciones avanzadas de software para la gestión y el control.

Figura 10.23: Cámara DLINK DCS-3420

Características Principales:

- Alta resolución de imagen, la DCS-3420 usa el modo de perfil simple MPEG-4 para transferir imágenes en directo a hasta 25 fps para conseguir la visualización en tiempo real.
- Sensor CCD, y la funcionalidad de zoom digital 4x.
- Capacidad de grabación nocturna.
- Wi-Fi compatible con los dispositivos IEEE 2.4GHz 802.11b/g.
- Admite encriptación WEP y WPA-PSK de 128-bits.
- Potencia del transmisor:
  - 16dbm para 802.11b
  - 12dbm para 802.11g
- Sensibilidad del receptor:
  - 11g @ PER 10 % y 54$Mbps$: $-67dbm$
  - 11b @ PER 8 % y 11$Mbps$: $-81dbm$

La D-Link DCS 2121 wireless 3G SD Wi-Fi presenta las siguientes características:

Figura 10.24: D-Link DCS 2121 wireless 3G SD WIFI

- Sensor CMOS de 1.3MegaPix
- Conectividad LAN y WLAN:
  - 10/100BASE-TX
  - 802.11b/g Wireless con WEP/WPA/WPA2
- Potencia del transmisor:
  - 16dbm para 802.11b
  - 12dbm para 802.11g
- Sensibilidad del receptor:
  - 11g Packet Error Rate @ 10 % y 54$Mbps$: $-66dbm$
  - 11b Packet Error Rate @ 8 % y 11$Mbps$: $-82dbm$

La Cámara IP Inalámbrica Zavio modelo F312A Wi-Fi, presenta las siguientes características:

Figura 10.25: Cámara IP Inalámbrica Zavio modelo F312A Wi-Fi.

Cuenta con un sensor CMOS de 1.3Megapix una lente de 4,0mm. Posee seguridad mediante WPA-/WPA2-PSK, WPA-/WPA2-AES,WEP.

Desafortunadamente no pudimos encontrar datos concisos sobre la potencia de transmisión o sensibilidad del receptor, por lo que, aunque la cámara cuenta con buenas prestaciones hemos decidido no considerarla en nuestra elección final.

Finalmente la cámara Wireless Linksys WI-FI G WVC54GCA presenta las siguientes características:

Figura 10.26: Wireless Linksys WI-FI G WVC54GCA.

- Presenta un sensor CMOS de 1.3 Megapixel como las otras cámaras analizadas.
- Estándares soportados:
  - IEEE 802.11g
  - IEEE 802.3
  - IEEE 802.3u
- Protocolos de seguridad:
  - WEP-64
  - WEP-128
  - WPA y WPA2

Como nos centramos en las características técnicas de transmisión y recepción, solamente nos detendremos a analizar las cámaras DLINK DCS-3420 (Figura 10.23) y la DLINK DCS-2121 (Figura 10.24) ya que han sido las únicas que presentan estos datos. Sabiendo esto hemos elegido a la DLINK DCS-3420 como modelo de nuestros cálculos ya que presenta todas las características necesarias y además cumple con nuestros requerimientos en el área de transmisión y recepción. Su costo es de US$ 295.

Teléfonos IP Wireless

En esta sección presentamos los teléfonos wireless propuestos para el proyecto. Nos centramos basicamente en dos modelos: el Teléfono Wireless Avaya 3641 que puede apreciarse en la Figura 10.27 y el Teléfono Wireless Avaya 3631 Figura 10.28. Ambos comparten practicamente las mismas características, pero el Avaya 3631 tiene un diseño que lo hace más costoso, siendo ello la principal diferencia.

Figura 10.27: Teléfono Wireless Avaya 3641

Figura 10.28: Teléfono Wireless Avaya 3631

A continuación se describen las características más importantes que además justifican nuestra elección por dichos modelos de teléfonos.

- Transmisión: 802.11b, 802.11g (2,4-2,4835GHz) y 802.11a (5,150-5.250GHz 5,250-5.350GHz 5,470-5.725GHz 5,725-5,825GHz)
- Método de acceso: Direct-sequence spread spectrum (DSSS)
- Velocidad de transmisión: Hasta 54$Mbps$
- QoS: SpectraLink Voice Priority (SVP)
- Seguridad: Wired Equivalent Privacy (WEP) (de 40-bit y 128-bit); Cisco FSR; WPA-PSK; WPA2-PSK
- Administración: DHCP, TFTP
- Códecs de voz: G.711 y G.729a/ab
- Protocolo VoIP: CCMS

El costo del teléfono Avaya 3641 es de U$S 202,4, mientras que el modelo 3631 es de U$S 306,2. Siendo la principal diferencia el diseño y no funcionalidades adicionales, se recomienda utilizar Teléfono IP Wireless Avaya 3641 por ser más económico.

10.2. Configuración de los equipos

10.2.1. Firewalls

En la Figura 10.29 se puede observar las distintas redes que componen a la red de la FIUBA, indicándose las asignaciones de bloques CIDR[5] (ver Sección 10.2.2), las direcciones IP de las interfaces y los diferentes elementos que la componen.

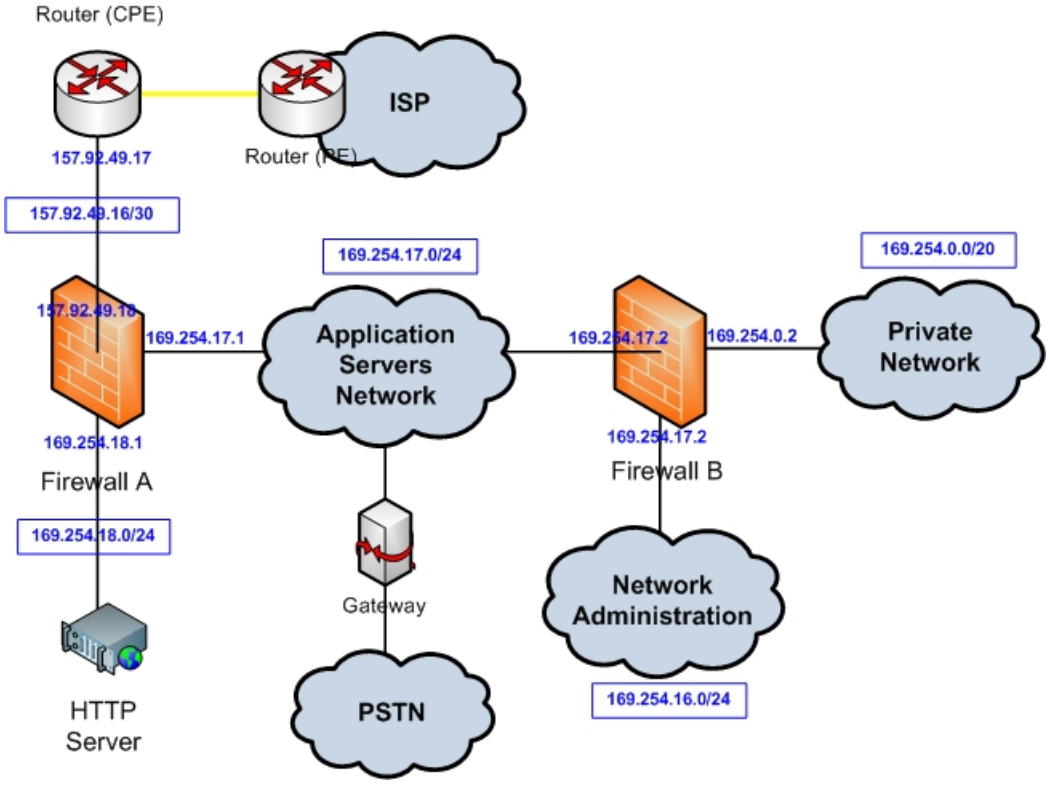


Figura 10.29: Arquitectura de red

En los Cuadros 10.5 y 10.6 se indican las reglas de los *Firewalls A* y *B* respectivamente indicados en la Figura 10.29.

Action	Source Addr.	Dest. Addr.	Protocolo	Source Port	Dest Port
Permit	Public Network	Web Server	TCP	Any	80 y 443
Permit	Public Network	ASN	TCP	Any	20, 25 y 53
Permit	Web Server	ASN	TCP	Any	25, 53 y 80
Permit	ASN	Public Network	TCP	Any	80, 443 y 53
Permit	ASN	Web Server	TCP	Any	80 y 443
Dany	Any	Any	Any	Any	Any

Cuadro 10.5: Firewall A

[5]Classless Inter-Domain Routing

Action	Source Addr.	Dest. Addr.	Protocolo	Source Port	Dest Port
Permit	Private Network	ASN	TCP	Any	80, 443, 445, 1812 y 20
Permit	NA	ASN	TCP	Any	80, 443, 22, 23 y 161
Permit	NA	Private Network	TCP	Any	22, 23 y 161
Permit	ASN	Private Network	TCP	Any	1521 o 3306
Dany	Any	Any	Any	Any	Any

Cuadro 10.6: Firewall B

10.2.2. Direccionamiento IP

En esta sección se asignará las direcciones IP, y para ello, se emplearan direcciones de IP privadas con el obsjetivo de no emplear direcciones IP públicas debido a su escasez.

En Internet normalmente se configuran los equipos de manera tal que descarten cualquier tráfico dirigido a direcciones IP privadas. Este aislamiento le brinda a las redes privadas una forma de seguridad básica, dado que por lo general no es posible que alguien desde fuera de la red privada establezca una conexión directa a una máquina por medio de estas direcciones. Debido a que no es posible realizar conexiones entre distintas redes privadas a través de Internet, distintas compañías pueden usar el mismo rango de direcciones privadas sin riesgo de que se generen conflictos con ellas. Es decir, no se corre el riesgo de que una comunicación le llegue por error a un tercero que esté usando la misma dirección IP.

Si un dispositivo de una red privada necesita comunicarse con otro dispositivo de otra red privada distinta, es necesario que cada red cuente con una puerta de enlace con una dirección IP pública, de manera de que pueda ser alcanzada desde fuera de la red y así se pueda establecerse una comunicación, ya que un router podrá tener acceso a esta puerta de enlace hacia la red privada. Típicamente, esta puerta de enlace será un dispositivo de traducción de dirección de red (NAT) o un servidor proxy. Por tal motivo, el *Firewall A* de la Figura 10.29 debe soportar NAT, ruteo de capa 3 y además ser un HTTP proxy server. Esto se puede implementar mediante una soluciones Freeware como se comentó en la Sección 10.1.1.

Las direcciones de internet privadas son[6]:

CIDR	Rango de direcciones IP	Número de IPs	Descripción de la clase
10.0.0.0/8	10.0.0.0 – 10.255.255.255	16.777.216	clase A simple
172.16.0.0/12	172.16.0.0 – 172.31.255.255	1.048.576	16 clases B continuas
192.168.0.0/16	192.168.0.0 – 192.168.255.255	65.536	256 clases C continuas
169.254.0.0/16	169.254.0.0 – 169.254.255.255	65.536	clase B simple

Cuadro 10.7: Bloques de direcciones IP Publicas

Suponiendo la "Private Network" contiene un total máximo estimado de 2260 terminales que provenientes de:

	1600	Desktop & Notebook
+	800	Teléfonos
	160	Cámaras (20 cámaras por piso)
	2260	Terminales

[6]Definidas en la RFC 1592 (original), RFC 1918, RFC 3330 y RFC 3927.

Entonces se necesitará un mínimo de 2260 direcciones IP para asignarle a cada terminal. Por lo tanto, la cantidad de bits que se necesitan para tener un mínimo de 2260 direcciones IP es $N \geq log_2(2240) = 11{,}1$. Es decir, con 12 bits se pueden obtener $2^{12} - 2 = 4096 - 2$ direcciones IP que son suficientes para asignar a todos los terminales de la "Private Network". Para el resto de las redes (Network Administration, Application Servers Network, HTTP Server Network) se estima que cada red no supera un máximo de $256 - 2$ direcciones IP. Por lo tanto, con un total de 8 bit para cada red es suficiente.

En total se tiene $4096 + 3 \cdot 256 = 4864$ direcciones IP. Por otro lado, como se vio en el Cuadro 10.7, una Clase B contiene 65.536 direcciones IP. Por lo tanto si se utiliza una Clase B para la asignación de direcciones, se cubre la cantidad de direcciones IP necesarias más un margen amplio en caso que se requiera más redes.

A continuación se indica la asignación de bloques CIDR y sus respectivas máscaras de subred:

Private Network: 169.254.0.0/20

Network Administration: 169.254.16.0/24

Application Servers Network: 169.254.17.0/24

HTTP Server Network: 169.254.18.0/24

Enlace CPE-Firewall A: 157.92.49.16/30[7]

En los Cuadros 10.8 y 10.9 se puede observar las tablas de ruteo de los firewalls de la Figura 10.29.

Network	Mask	Next Hop	if	Metric
157.92.49.16	/30	-	Sl0	1
169.254.16.0	/24	168.254.17.2	Eth1	2
169.254.17.0	/24	-	Eth1	1
169.254.18.0	/24	-	Eth0	1
169.254.0.0	/24	168.254.17.2	Eth1	2
0.0.0.0	/0	157.92.49.17	Sl0	1

Cuadro 10.8: Tabla de ruteo del firewall A

Network	Mask	Next Hop	if	Metric
169.254.16.0	/24	-	Eth1	1
169.254.17.0	/24	-	Eth0	1
169.254.0.0	/24	-	Eth2	1
0.0.0.0	/0	169.254.17.1	Eth0	2

Cuadro 10.9: Tabla de ruteo del firewall B

[7]Bloque CIDR /30 perteneciente a la FIUBA.

10.2.3. Asignación de recursos lógicos

El estándar IEEE 802.1q asigna un campo de 12 bits para realizar la identificación del VLAN ID (identificador de Virtual LAN), resultando en un máximo teórico de $2^{12} = 4.096$ VLANs posibles, de las cuales únicamente 4.094 estarán disponibles para el servicio (las VLANs "0" y "4.095" se encuentran reservadas).

Se empleará VLANs basadas en el encabezado de la capa 3 del modelo OSI, es decir, se realiza un mapeo de que direcciones IP están autorizadas a entrar en una VLAN. Para esto se dividirá en subbloques del bloque IP 169.254.0.0/20 y asignará cada uno de estos según el tipo de terminal:

Administración (VLAN1): 169.254.16.0/24

Cámaras IP (VLAN2): 169.254.0.0/22

Computadoras (VLAN3): 169.254.4.0/22

Teléfonos IP(VLAN4): 169.254.8.0/22

Otros (VLAN5): 169.254.12.0/22

De esta forma, se podrá asignar mayor prioridad al tráfico de voz y vídeo otorgando una mayor prioridad a las VLANs de los teléfonos y cámaras respectivamente.

Calidad de Servicio

En esta sección se definen las políticas de QoS a establecer. La aplicación de políticas de QoS en la capa 2 del modelo OSI debe estar acorde con las políticas adoptadas en la capa 3 del modelo, por tal motivo los tags de priorización deben estar relacionados. En la siguiente cuadro se muestran los valores que adopta capa 2 (802.1P) y capa 3 (DSCP/TOS):

Tipo de tráfico	**DSCP**	**TOS/802.1P**
Real Time: Streaming de vídeo y audio	Expedited Forwarding (EF) 101 110	5 101
Aplicaciones interactivas: Vídeo conferencia; vídeo telefonía;	Assured Forwarding (AF41) 100 010 Class 4; Low Drop Prec	4 100
Señalización de VoIP y vídeo, capa de control: H323, SIP, Telnet/SSH	Assured Forwarding (AF31) 011 010 Class 3; Low Drop Prec	3 011
Mission-Critical: Broadband de Vídeo/Voz	Assured Forwarding (AF21) 010 010 Class 2; Low Drop Prec	2 010
Best-Effort: Tráfico de datos convencional:	Default DSCP 000 000	0 000

Cuadro 10.10: Calidad de servicio

IEEE 802.1P: Es un estándar que proporciona priorización de tráfico y filtrado multicast dinámico. Esencialmente, proporciona un mecanismo para implementar Calidad de Servicio o QoS a nivel de MAC[8].

Existen 8 clases diferentes de servicios, expresados por medio de 3 bits del campo prioridad de usuario (user_priority) de la cabecera IEEE 802.1Q añadida a la trama, asignando a cada paquete un nivel de prioridad entre 0 y 7. Aunque es un método de priorización bastante utilizado en entornos LAN, cuenta con varios inconvenientes, como el requerimiento de una etiqueta adicional de 4 bytes (definida en el estándar IEEE 802.1Q). Además solo puede ser soportada en una LAN, ya que las etiquetas 802.1Q se eliminan cuando los paquetes pasan a través de un router.

No está definida la manera de cómo tratar el tráfico que tiene asignada una determinada clase o prioridad, dejando libertad a las implementaciones. IEEE, sin embargo, ha hecho amplias recomendaciones al respecto.

802.1P se encuentra integrado en los estándares IEEE 802.1D y 802.1Q.

DSCP: DSCP[9] hace referencia al segundo byte en la cabecera de los paquetes IP que se utiliza para diferenciar la calidad en la comunicación que quieren los datos que se transportan.

Originalmente se definió este byte para un uso con otro formato: ToS[10] pero con el mismo objetivo de diferenciar el tráfico.

Se utilizan los bit de 6 de los 8 bits.

10.3. "Link Budget"

Para determinar el radio de cobertura de un AP, es necesario plantear el balance de potencia de un enlace o "link budget". Este cálculo se basa en las ganancias y pérdidas de potencia desde el transmisor, a través del medio de transmisión, hasta el receptor y queda determinado por la siguiente inecuación:

$$P_{R_X} - C_{min} \geq Perdidas - Ganancias. \tag{10.1}$$

$$P_{R_X} - C_{min} \geq L_{T_X} + L_{R_X} + FSPL + L_M - G_{T_X} - G_{R_X}. \tag{10.2}$$

Donde:

C_{min}**:** Potencia mínima de entrada al receptor para determinado objetivo de calidad (dBm). En las hojas de datos se especifica como sensibilidad del receptor.

P_{T_X}**:** Potencia de salida del transmisor (dBm)

G_{T_X}**:** Ganancia de antena del transmisor(dBi)

L_{T_X}**:** Perdidas del transmisor (coaxial, conectores, etc.) (dB)

[8]Media Access Control
[9]Differentiated Services Code Point. Definido en la RFC 2474
[10]Type of Service

$FSPL$**:** Perdida de señal por propagación en espacio libre descripta en la Sección 9.4.2 (dB)

L_M**:** Margen de desvanecimiento para determinado objetivo de calidad (dB)

G_{R_X}**:** Ganancia de antena en el receptor (dBi)

L_{R_X}**:** Pérdidas en el receptor (coaxial, conectores, etc) (dB)

El margen de desvanecimiento es un factor ficticio que se incluye en la ecuación para tener en cuenta las características no ideales como la propagación por múltiples trayectorias, tipo de terreno, causas atmosféricas, confiabilidad del sistema. La ecuación de Barnett-Vignant para el calculo del margen de desvanecimiento es:

$$L_M = 30log(d) + 10log(6ABf) - 10log(1 - R) - 70. \tag{10.3}$$

Siendo:

d**:** Distancia (Km).

f**:** Frecuencia (GHz).

R**:** Confiabilidad (en decimales).

A**:** Factor de aspereza:

- 4 Para agua o terreno liso.
- 1 Para terreno promedio
- 0,25 para terreno áspero y montañoso

B**:** Factor de disponibilidad:

- 0,5 Para zonas cálidas o húmedas.
- 0,25 Para zonas continentales promedio.
- 0,125 Para zonas muy secas o montañosas

De la Ecuación 10.2 se observa que dependiendo de las características del equipo receptor, el nivel de señal recibido es suficiente para una velocidad de transmisión determinada si esta sobrepasa la sensibilidad del mismo.

La sensibilidad de un equipo wireless depende de la velocidad de transmisión. Por lo tanto, el cálculo de balance de potencia del enlace se establece en base a los equipos que cumplen la norma IEEE 802.11g, a una tasa de transmisión de $54Mbps$ con 10 % de PER[11].

Según especificaciones de las Sección 10.1, estos son:

AP:

- P_{T_X}: $20dBm$

[11] Packet Error Rate

- G_{Antena}: $2,8dBi$.
- $Sensibilidad$: $-85dBm$.

End System (caso más desfavorable):

- P_{T_X}: $10dBm$.
- G_{Antena}: $0dBi$.
- $Sensibilidad$: $-60dBm$.

Se debe tener tener en cuenta de realizar el cálculo en el sentido inverso debido a que la comunicación es bidireccional. Es decir, si se parte de la base que el transmisor es la placa wireless y el AP el receptor, posteriormente se debe considerar al AP como receptor y a la tarjetas wireless como transmisor.

Iterando en la Ecuación 10.2 se obtiene que las distancias máxima son:

AP → End System: $47m$.

End System → AP: $62m$.

Por lo tanto, el radio máximo teórico es de $47m$. El cálculo resulta aproximadamente similar a lo especificado por los fabricantes en espacios semi-abiertos como se puede observar en el Cuadro 9.1.

10.4. Topología de la nueva red

En esta sección se presenta el cableado como deberá estar conformado para la nueva red de APs. Se trató de conservar el recorrido actual del cableado siempre que se pudo y se tuvo en cuenta que el mismo no debe superar los 100 metros. Se presenta también una medición estimada de la longitud del recorrido para poder presupuestar luego las bandejas portacables necesarias.

Se toma como punto de inicio el segundo piso ya que ahí se encuentran todos los servidores y los switches de backbone. De este piso, bajará el troncal a los pisos inferiores y subirá a los pisos superiores por los troncales verticales de las alas que dan a las calles EE.UU e Independencia y también para el caso de los ascensores de la calle Azopardo. Puntualmente para el troncal de Azopardo el AP más lejano del primer piso cumple con la norma y se encuentra a menos de 100 metros, pero para los pisos inferiores habrá que regenerar la señal con un switch en planta baja para irrigar dicha zona en planta baja, el entre piso y el subsuelo. Una situación similar se encuentra yendo hacia arriba, al 3er y 4to piso, ya que las distancias son correctas para el 3er piso pero para el 4to piso se necesita regenerar la señal. Se resolvió de esta forma teniendo en cuenta que esta es la solución de menor compromiso y la que mejor se ajusta al dilema que presenta el cableado en un edificio de estructura tan compleja como el que presenta nuestra Facultad.

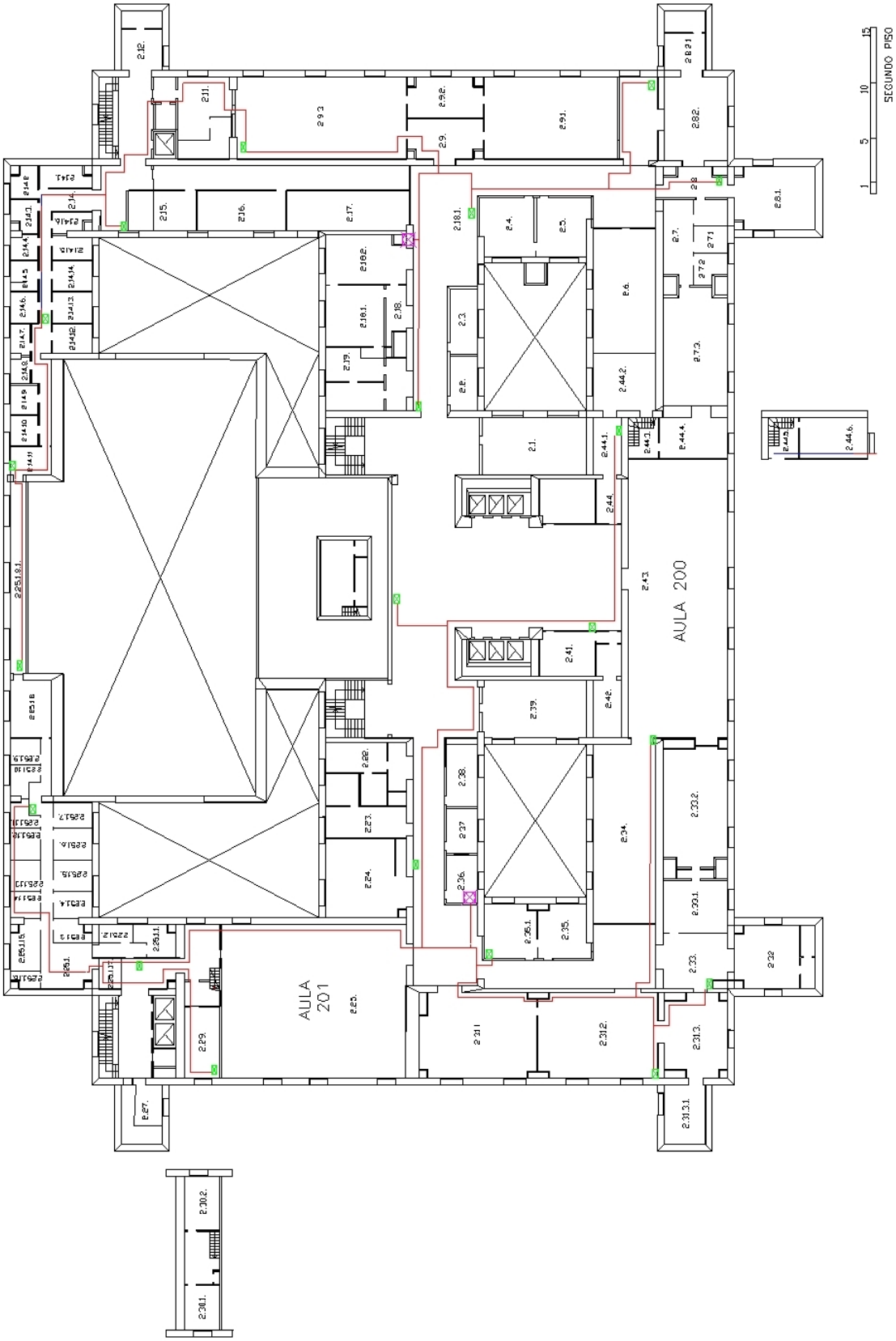


Figura 10.30: Recorrido del cableado en el segundo piso.

En el cableado del primer piso se puede observar que sigue haciendo falta pasar cables verticalmente por los ductos de ascensores que dan a la calle Azopardo ya que sino se excede la distancia máxima permitida. Otra opción seria extender la distancia con otro switch, pero se optó por aprovechar el cableado como se encuentra actualmente reduciendo la mano de obra y notando que extender el cableado a través de otro recorrido incluiría el paso a través del salón de actos hacia el piso superior atentando contra la estética edilicia e incrementando el costo y complejidad de la obra de cableado. Es importante recordar que los ascensores están deshabilitados y por lo tanto esto no implica una violación al protocolo de cableado estructurado

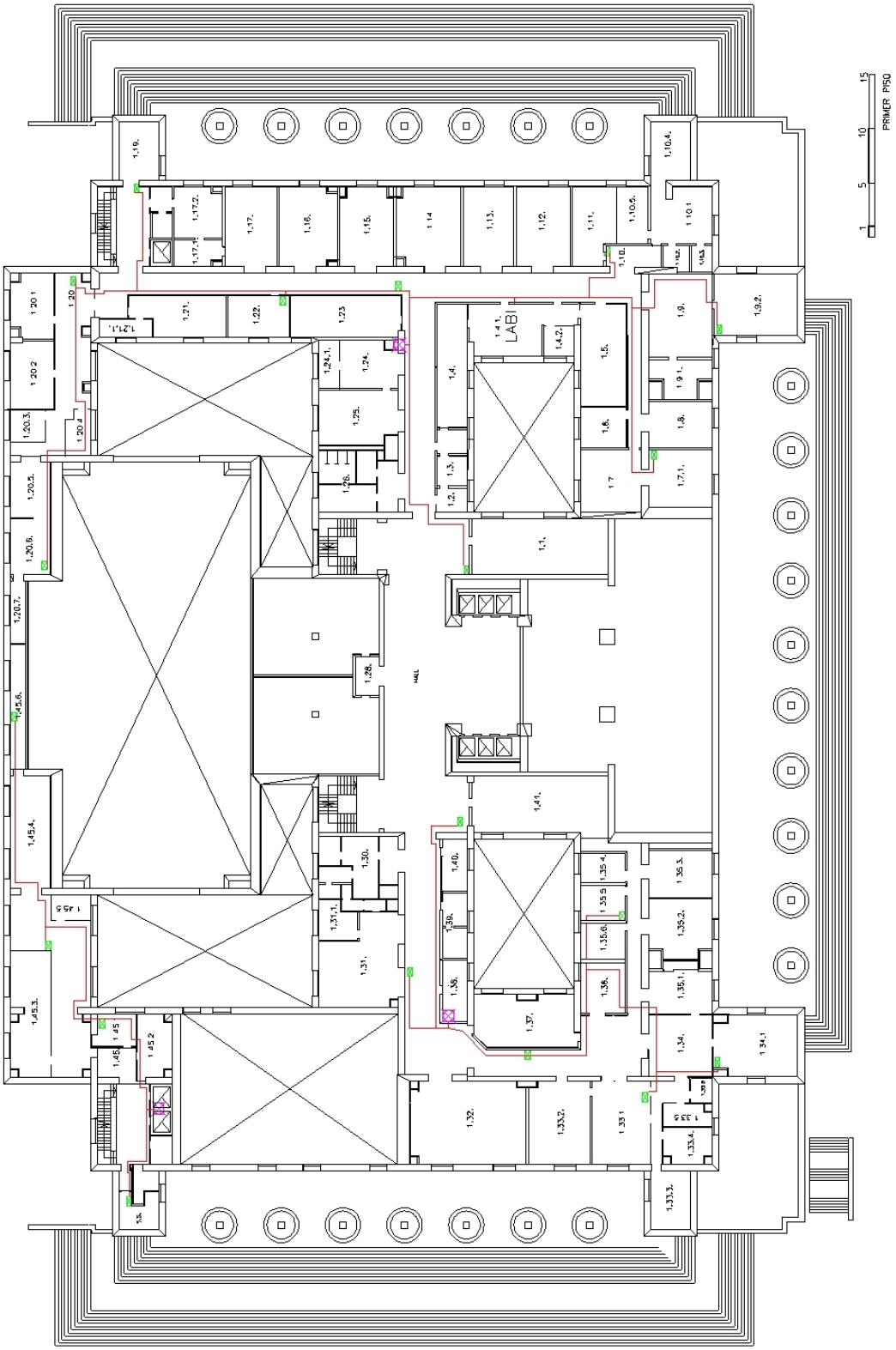


Figura 10.31: Recorrido del cableado en el primer piso.

Como se explicó en el piso anterior, se recuerda que el cableado de la zona de la calle Azopardo viene del segundo piso atravesando el primero, para no dañar el salón de actos ni agregar cableado en él. Se recomienda no realizar un tendido extremadamente largo a través del gimnasio que hubiera además perjudicado la estética del hall principal de planta baja. En planta baja, cerca de la zona de los ascensores que dan a calle Azopardo habrá que agregar un switch que regenere la señal para llegar al entre piso y subsuelo con un cableado de distancia menor a los $100m$.

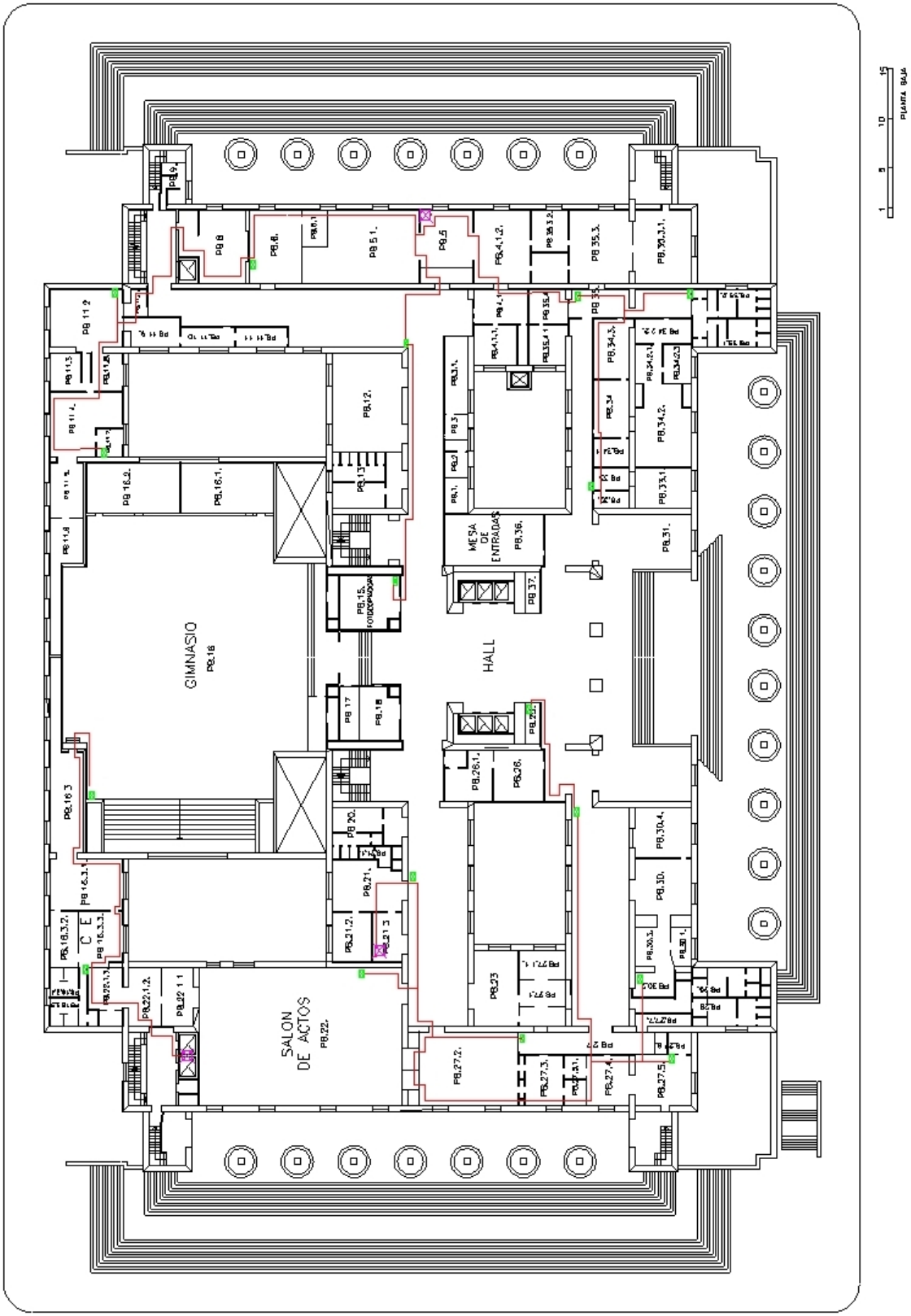


Figura 10.32: Recorrido del cableado en la planta baja.

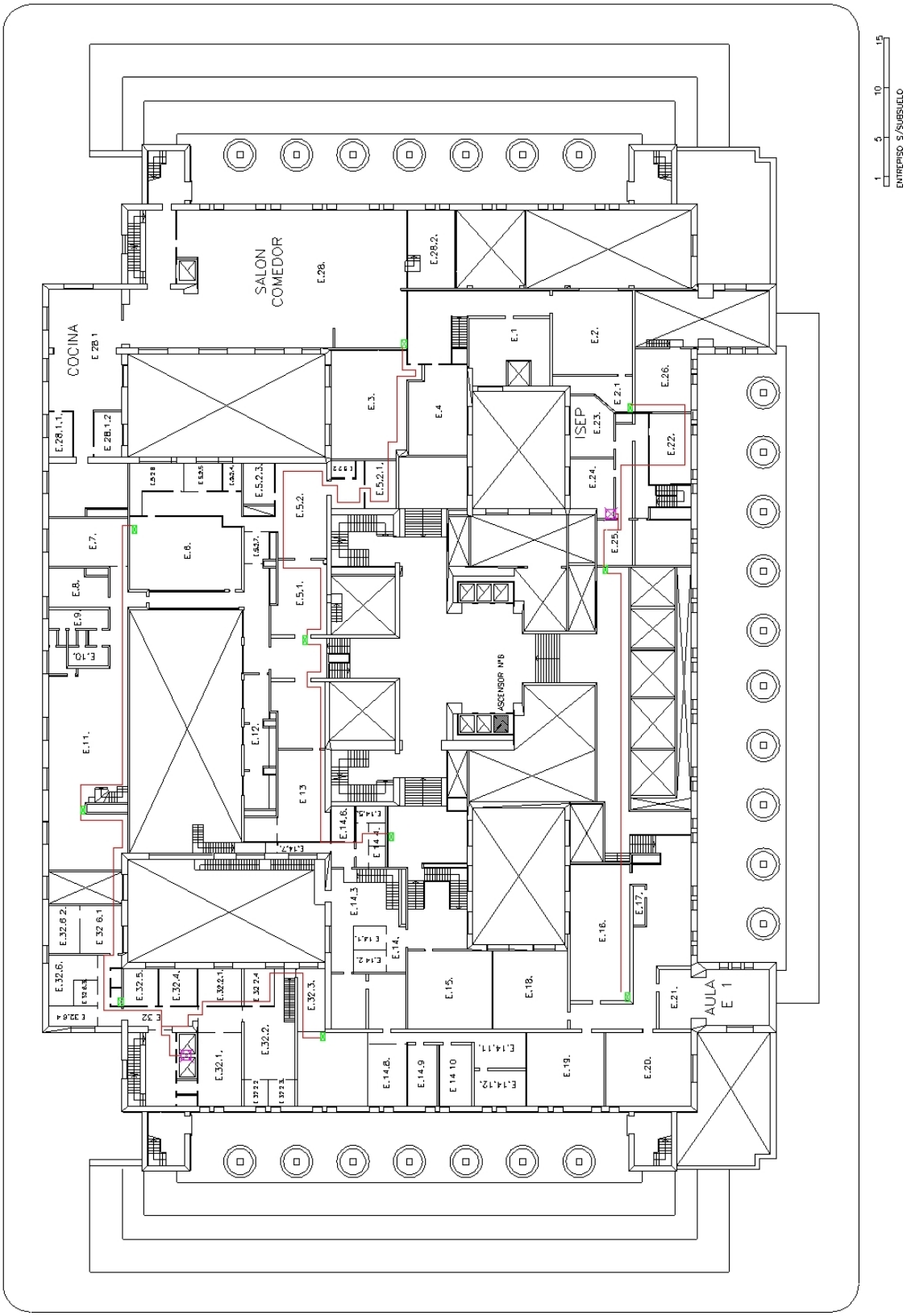


Figura 10.33: Recorrido del cableado en el entre piso.

El cableado en el subsuelo es el más complejo ya que se necesitó una mayor cantidad de AP debido a la estructura compleja del mismo que no permitía un buen desempeño para la red Wireless. Como ya se explicó anteriormente, la zona que da a la calle Azopardo recibe la señal del switch de planta baja. Para lo demás se recomienda el troncal vertical de ambas alas como en los otros pisos procurando no superar los $100m$ con especial cuidado ya que el cableado pasa por recovecos y presenta un recorrido con muchas vueltas

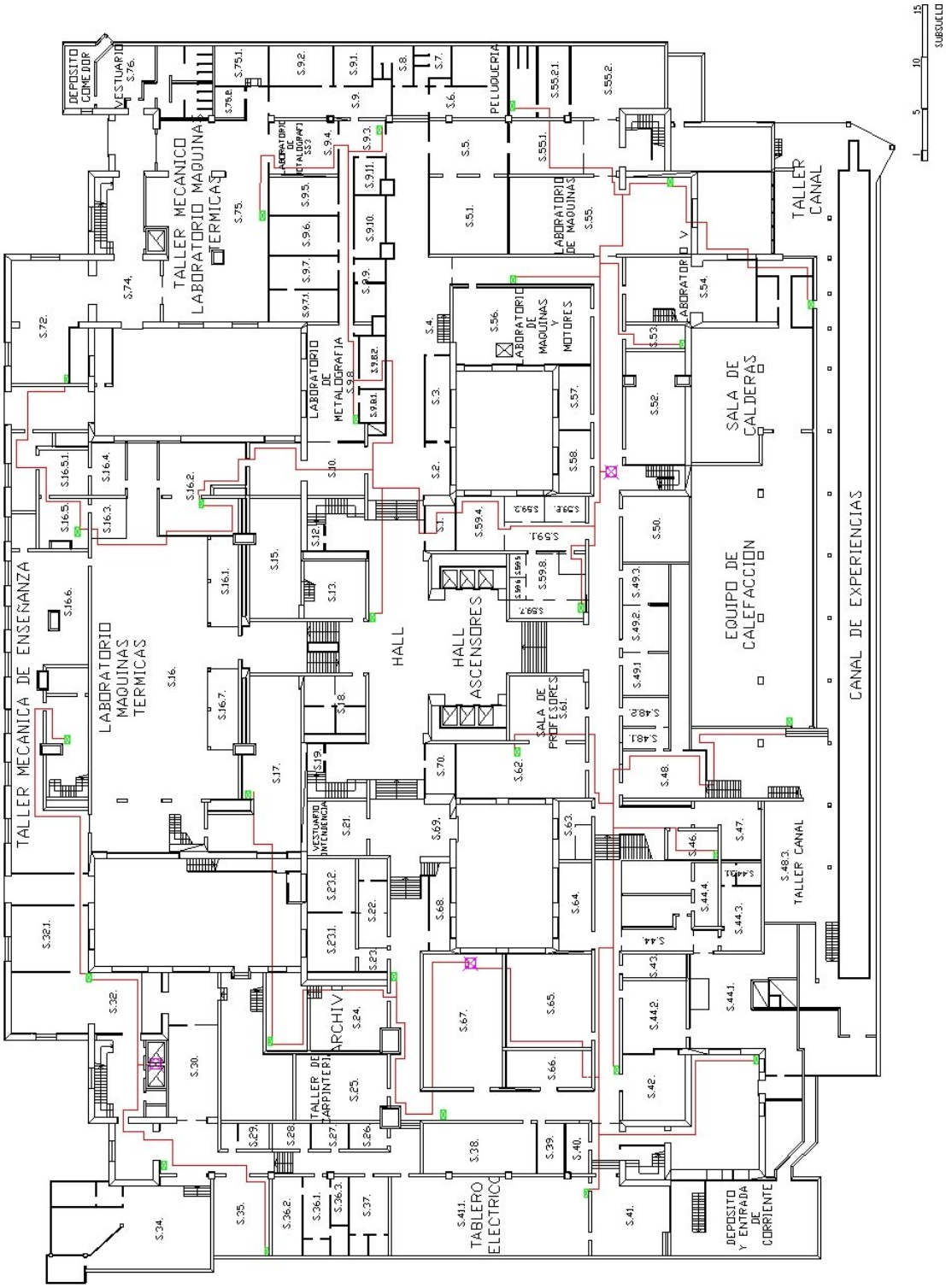


Figura 10.34: Recorrido del cableado en el subsuelo.

Se analiza el cableado del segundo piso hacia los pisos superiores empezando por el 3er piso. La zona de la calle Azopardo puede tomarse sin inconvenientes del segundo piso sin necesidad de regenerar la señal. El AP que se encuentra en la biblioteca hacia la calle Independencia es

el que se encuentra a mayor distancia del switch del ala de la calle EEUU. Sin embargo la distancia se estima en alrededor de los $93m$ para este caso, corroborando que el cableado no hará perder eficiencia a la transmisión de datos a dicho AP.

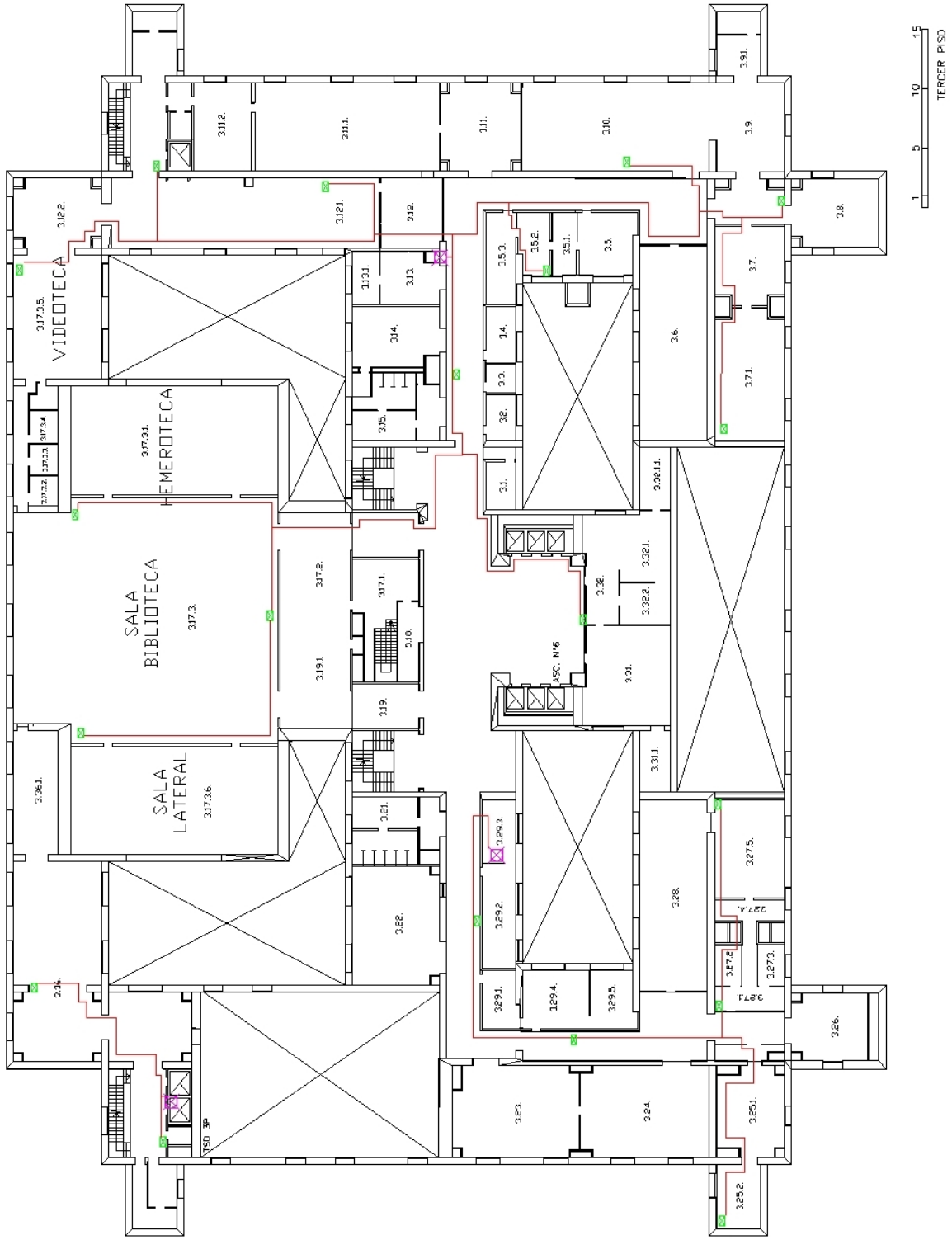


Figura 10.35: Recorrido del cableado en el tercer piso.

De la misma forma que en planta baja, la distancia al switch se excede para cablear la zona que da a la calle Azopardo y es necesario pasar el cableado por los ascensores de dicha zona e incluir un switch para regenerar la señal en este piso. El AP de la sala de depósito lateral de la biblioteca se encuentra a 98m pero consideramos que es mejor que esté cableado de esta forma que obteniendo la señal de la otra ala de la facultad teniendo que pasar cable por el techo de la sala central de la biblioteca de alguna forma. Nuevamente se prioriza la estética edilicia especialmente en zonas como la biblioteca, el hall central el salón de actos y las aulas-anfiteatro.

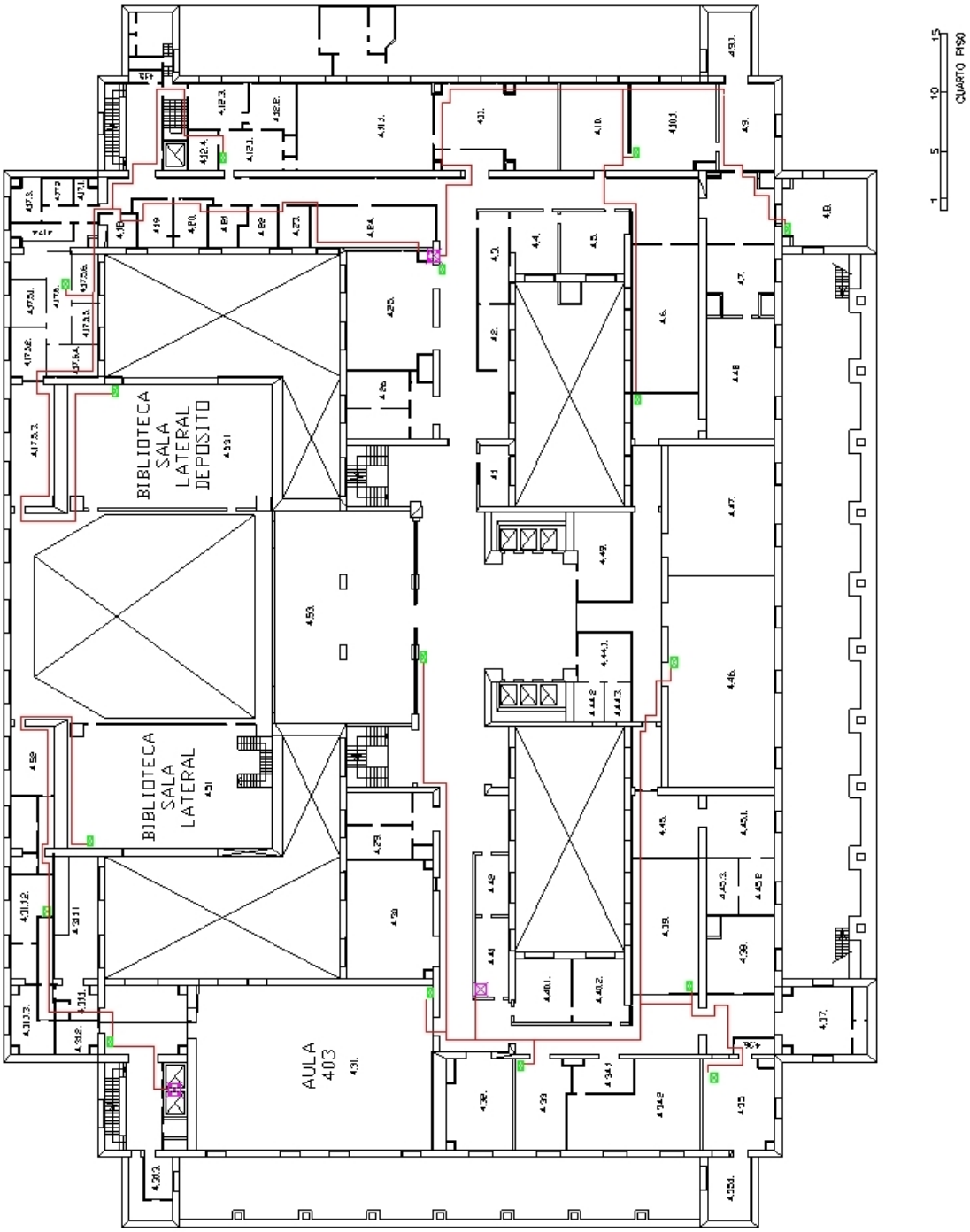


Figura 10.36: Recorrido del cableado en el cuarto piso.

En el 5to piso se llega a los APs sobre la calle Azopardo sin la necesidad de pasar por un troncal vertical que no sean los que se encuentran en el ala de Independencia y EEUU, por lo que no se necesita nunca consideración especial.

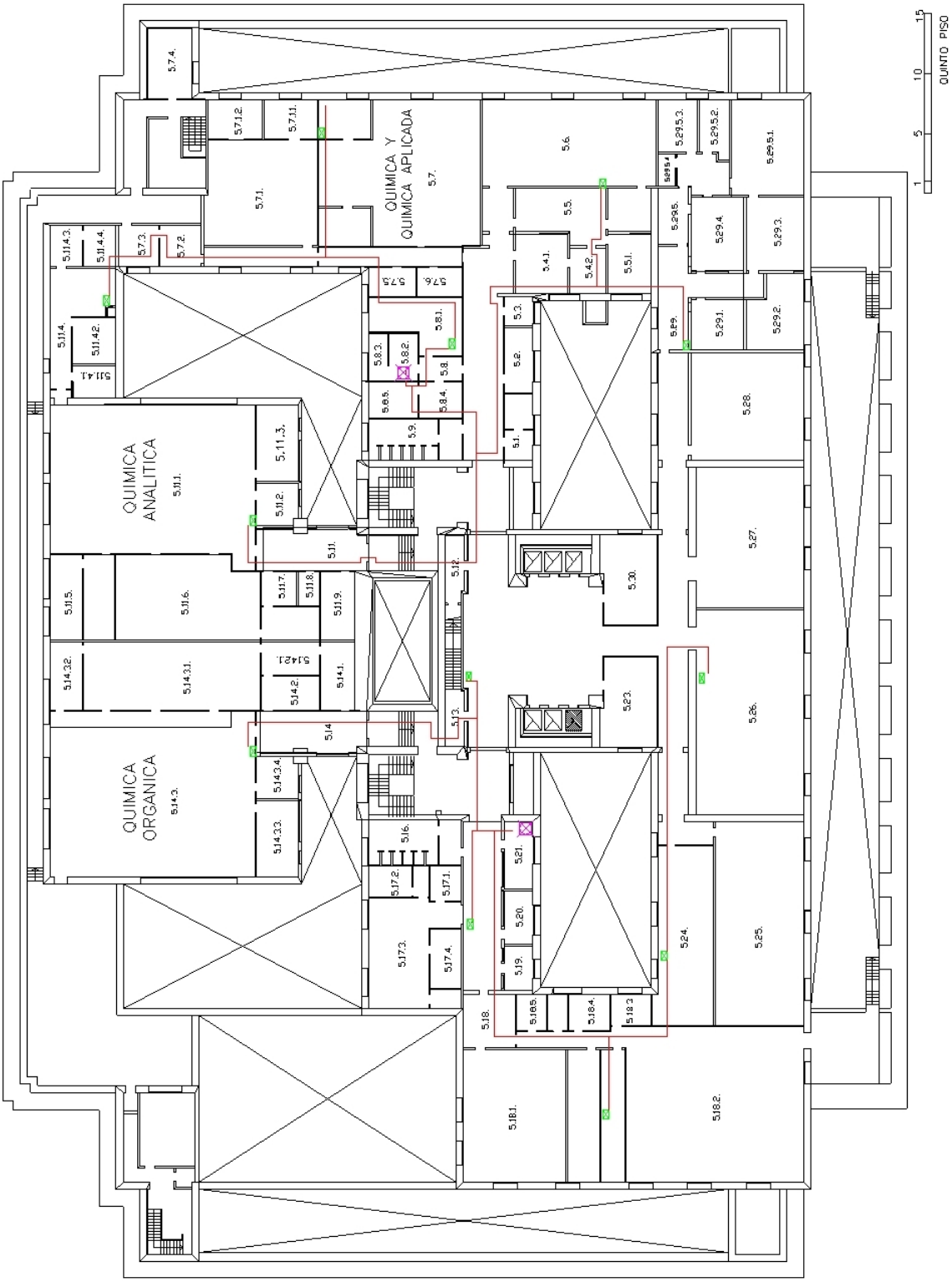


Figura 10.37: Recorrido del cableado en el quinto piso.

En el Cuadro 10.11 se presenta la distancia aproximada de la longitud del cableado para cada piso. Es necesario este dato para realizar un presupuesto de las bandejas portacable necesarias. Para ello se utilizarán bandejas de 2 pulgadas ya que como se hizo notar en el capítulo de estándares, en la sección 8.2.7. se pueden acomodar hasta 14 cables UTP en una bandeja de dichas características. En los casos puntuales donde se necesiten ubicar mas de 14 cables se utilizará una medida mayor, pero estos lugares son mínimos por lo que en el presupuesto se supondrán todas las bandejas de la medida mencionada.

Piso	**Cableado en metros**
1er Piso	371
2do Piso	410,6
3er Piso	487
4to Piso	443,5
5to Piso	358,6
Planta Baja	359,5
Subsuelo	585,4
Entrepiso	246
Total	3261,6

Cuadro 10.11: Longitud del cableado aproximado por piso.

Capítulo 11

Validación del prototipo

El "Site Survey" o estudio de cobertura es un procedimiento realizado para analizar el sitio en el que se implementará una red inalámbrica. Los datos proporcionados por el estudio de cobertura permitirán realizar la mejor configuración de la red a implementar, de tal manera de obtener rendimiento más óptimo.

El estudio de cobertura desarrollado en el presente proyecto se ha realizado utilizando el software *InterpretAir WLAN Survey 2.2 Copyright* © 2000 – 2007 de la empresa *Fluke Networks*.

Este análisis permite determinar:

- Mejor ubicación de los APs.
- Canal óptimo para reducir interferencia.
- Niveles de señal, SNR y velocidad aceptable en puntos de interés.
- Niveles de interferencia. La visualización "Interferencia" muestra qué ocurre cuando todos los puntos de acceso seleccionados o bloqueados envían datos en el intervalo especificado.
- Si los requerimientos de la red se están cumpliendo mediante la visualización "Estado de RF". Si se cumplen todos los criterios, se muestra un color verde. El color rojo se usa si uno o varios de los criterios no se cumplen. No se mostrará ningún color en las zonas en las que no se realiza ningún estudio de cobertura. Los criterios se basarán en los requerimientos indicados en la Sección 11.1.
- Cuáles de los criterios no se están cumpliendo, si hay alguno que no se cumpla. A esta visualización se la denomina "Motivo de Fallo" y esta relacionada con la visualización "Estado de RF". No se muestra ningún color en las zonas que superan la visualización "Estado de RF" (que presentan el color verde en "Estado de RF").
- El número de APs de cada ubicación con respecto a la intensidad de señal mínima seleccionada, de forma tal de poder garantizar una cobertura con "backup" en caso de caída de un AP, debido a la existencias de áreas de cobertura superpuestas.

La mejor localización del AP se determina luego de varias pruebas de ensayo y error. El software utilizado muestra los distintos niveles de señal en los puntos de interés. Se deben analizar

dichos resultados conjuntamente con la forma, materiales y localización de los obstáculos para determinar de ubicación más adecuada del AP.

La determinación de la ubicación de APs depende también de la potencia de radiación del equipo y del uso de antenas extra. En muchos casos se utiliza antenas direccionales para encaminar y limitar la señal a un cierto sector, en otros casos se puede usar antenas omnidireccionales con determinada ganancia para aumentar la potencia de emisión.

11.1. Determinación de requerimientos de la red

Los estándares 802.11g y 802.11b disponen de 3 canales no solapados (1, 6 y 11, según las especificaciones FCC) para América y 4 canales no solapados (1, 4, 9 y 13, según las especificaciones ETSI) para Europa como se detalló en la Sección 8. Por lo tanto, se empleará para la asignación de frecuencia los canales que especifica la FCC para América.

La velocidad de transmisión de una conexión inalámbrica depende del nivel de potencia del AP y de la sensibilidad del dispositivo receptor.

Cuando se realiza un estudio "in situ" de una solución Wireless, es importante definir un rango basado en el SNR para la conexión. El SNR de un acceso medido en el equipo, decrece con la distancia al AP debido al aumento de la perdida en el espacio libre. De la misma manera el ruido aumenta ya que a mayor distancia también aumentan las interferencias en RF debido a celulares, hornos microondas, etc.

El SNR impacta directamente en la "performance" de una WLAN. Una señal mas fuerte implica menor cantidad de retransmisiones ya que se pierden menos paquetes.

Siguiendo las recomendaciones del artículo de Jim Geiner: "Wi-Fi": Define "Minimum SNR Values for Signal Coverage" publicado por "Wi-Fi Plant" consideraremos los siguientes márgenes.

- $> 40dB$ SNR = Excelente señal
- $25dB$ a $40dB$ SNR = Buena señal
- $15dB$ a $25dB$ SNR = Baja señal
- $10dB$ a $15dB$ SNR = Muy baja señal
- $< 10dB$ SNR = Sin señal

Por otro lado CISCO recomienda $25dB$ SNR si se van a llevar acabo VoWLAN[1], ver [CISSLA]. Otros requerimientos de que Cisco recomienda para implementar redes de VoWLAN de alto rendimiento para adaptadores estándar que cumplan la norma IEEE802.11a/b/g son:

Mínima intensidad de señal: $-67dBm$.

Mínima SNR: $25dB$ a la velocidad de datos mínima.

Mínima cantidad de APs : 2 con una intensidad de señal mínima de $-90dBm$.

Mínima velocidad de datos: $11Mbps$.

[1] Voice over Wireless LAN

Máxima interferencia: $-86dBm$.

Como este es nuestro caso, es decir, diseñar una red de alto rendimiento con VoWLAN tomaremos las recomendaciones de CISCO como valores de referencia.

11.2. Simulación de las zonas hostpot

InterpretAir permite simular el comportamiento de la red ubicando los APs en un mapa del sitio cargado con la escala correcta. Los obstáculos como puertas, paredes y ventanas se especifican en el plano y se les asigna un valor de atenuación de acuerdo al material correspondiente. A continuación se puede observar las simulaciones realizadas en las diferentes plantas basadas en los criterios explicados en la Sección 9.4.2 y la Sección 10.3.

11.2.1. Subsuelo

Intensidad de señal

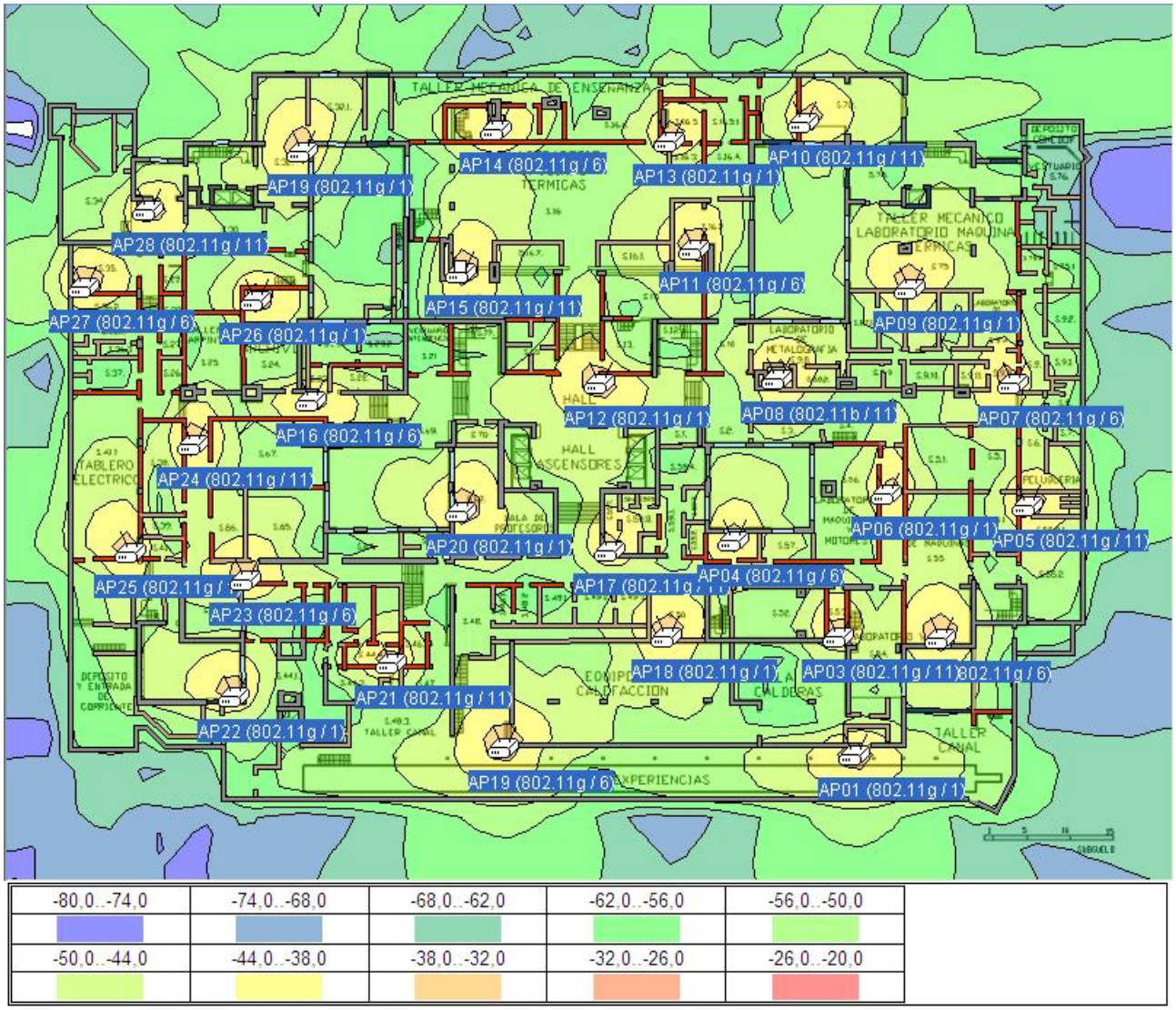


Figura 11.1: Intensidad de señal (dBm)

Relación señal ruido

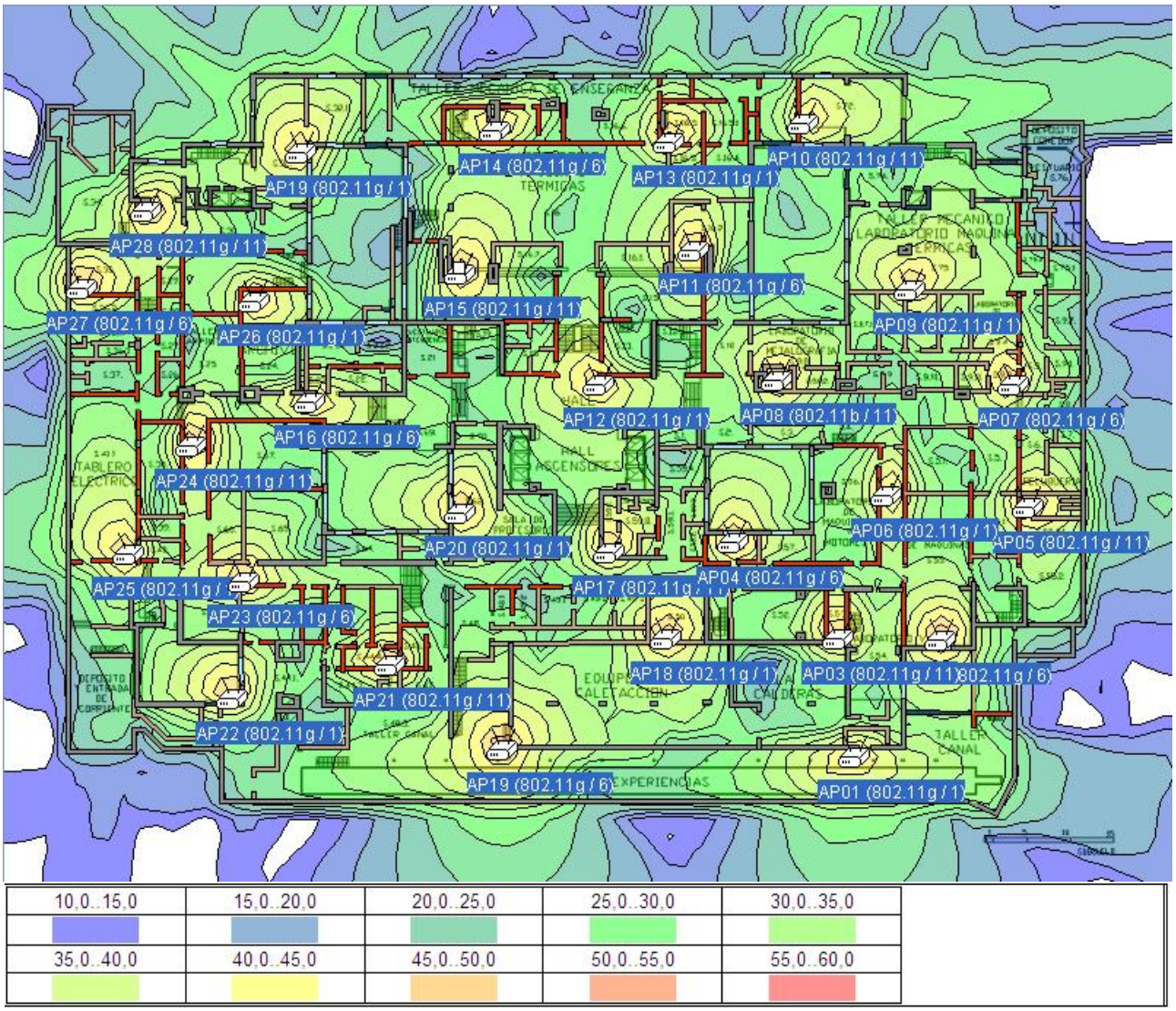


Figura 11.2: Relación señal ruido (dB)

Interferencia

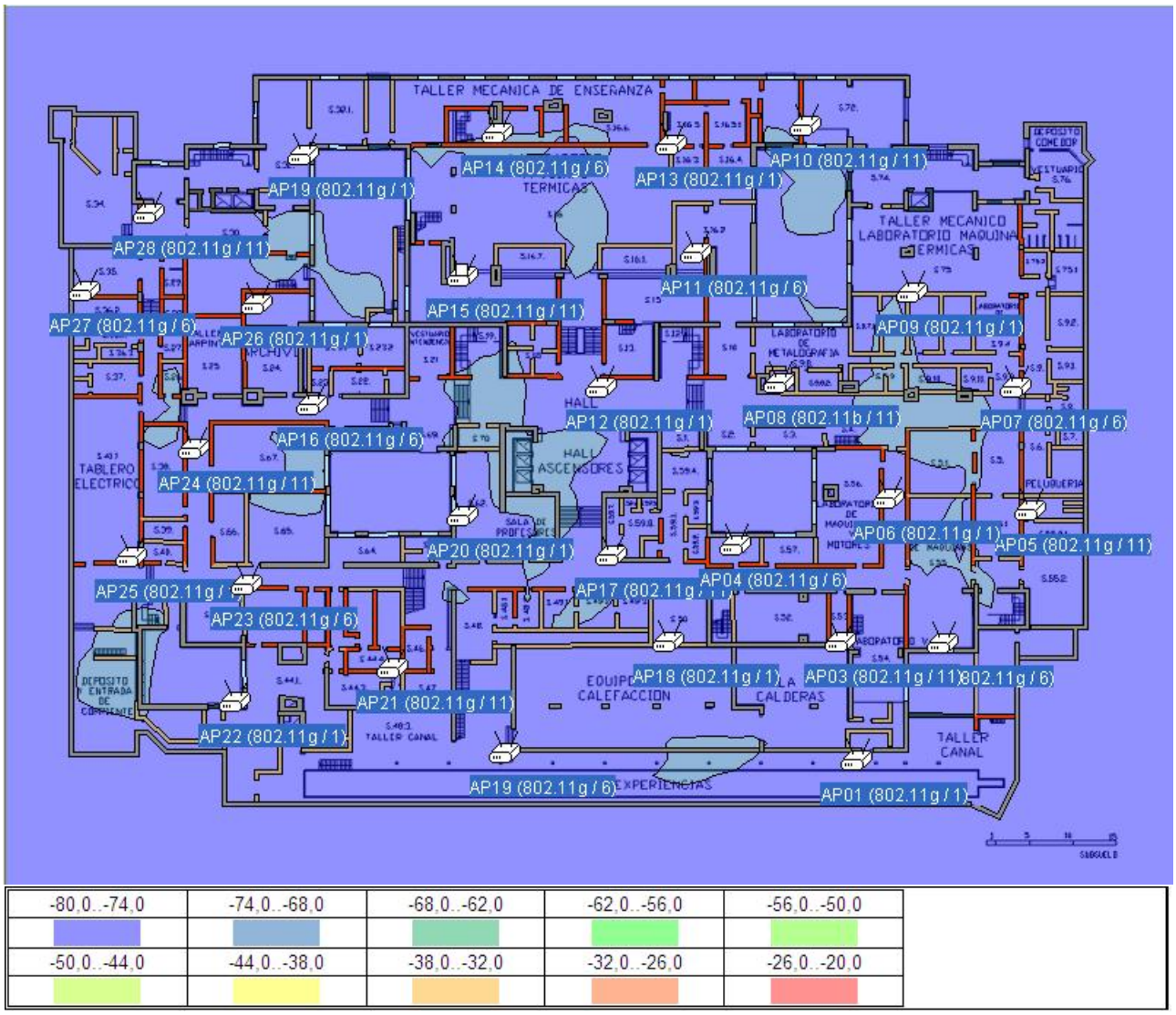


Figura 11.3: Interferencia (dBm)

Velocidad de datos

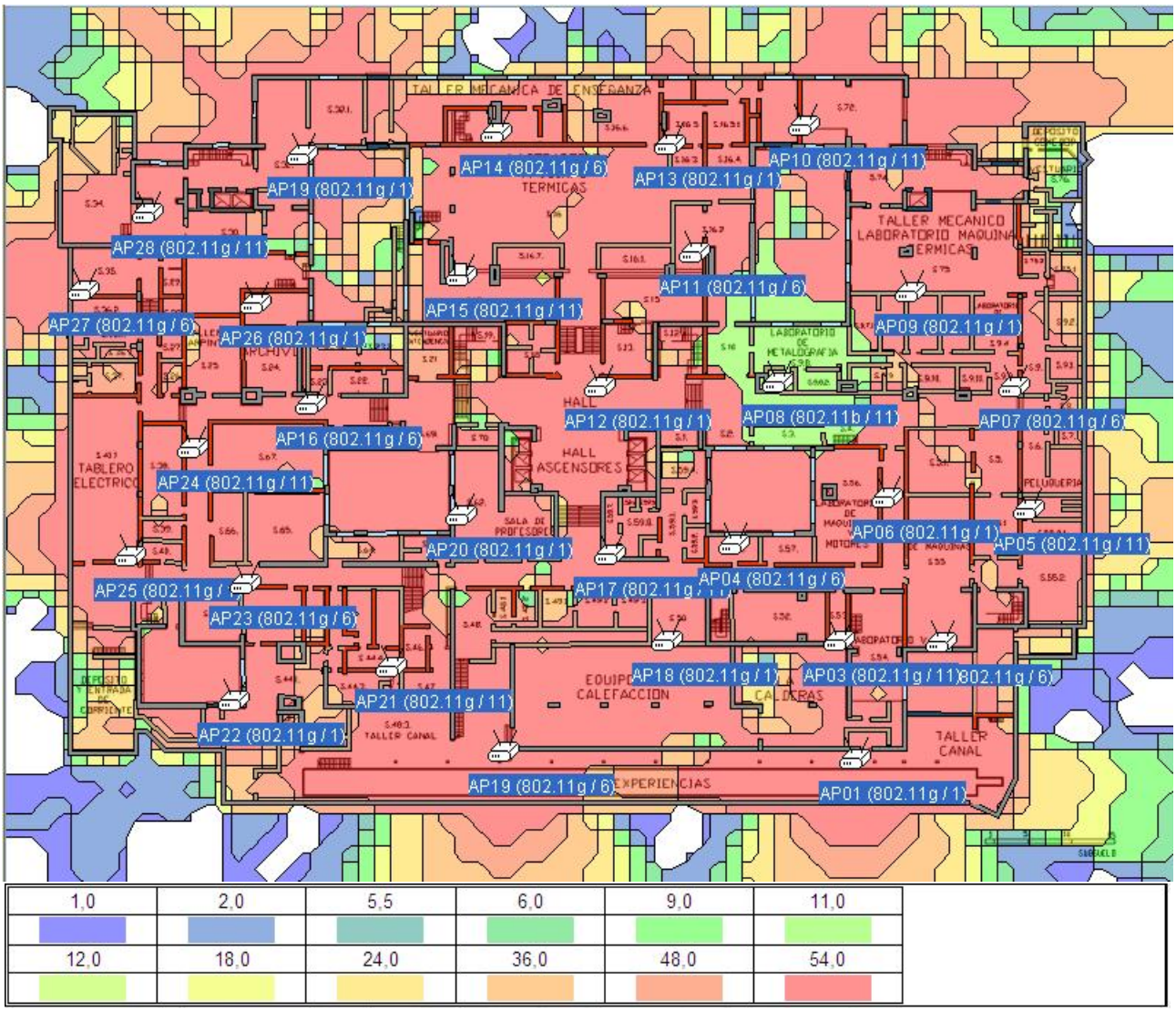


Figura 11.4: Velocidad de datos ($Mbps$)

Estado de RF

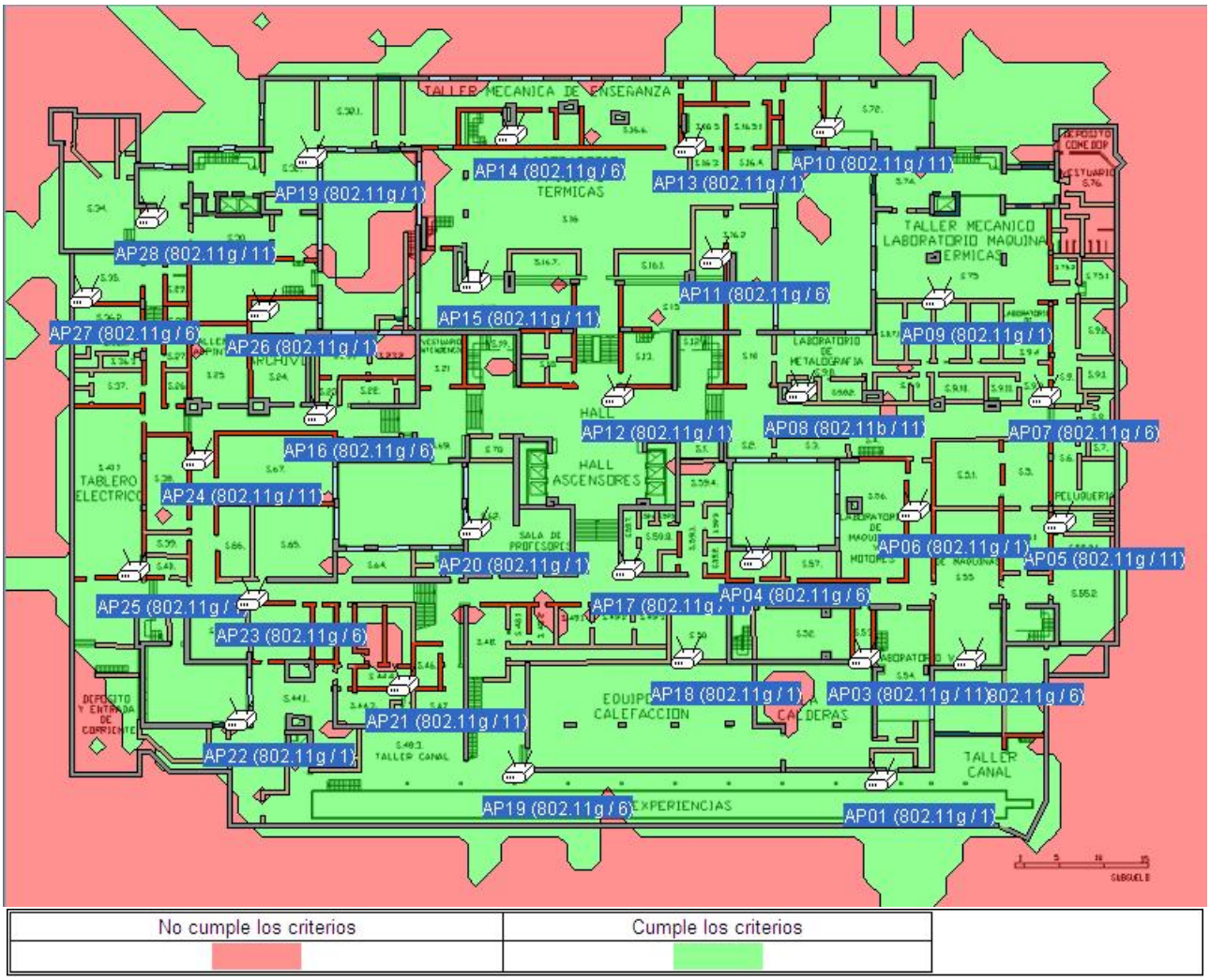


Figura 11.5: Estado RF

Motivo de fallo

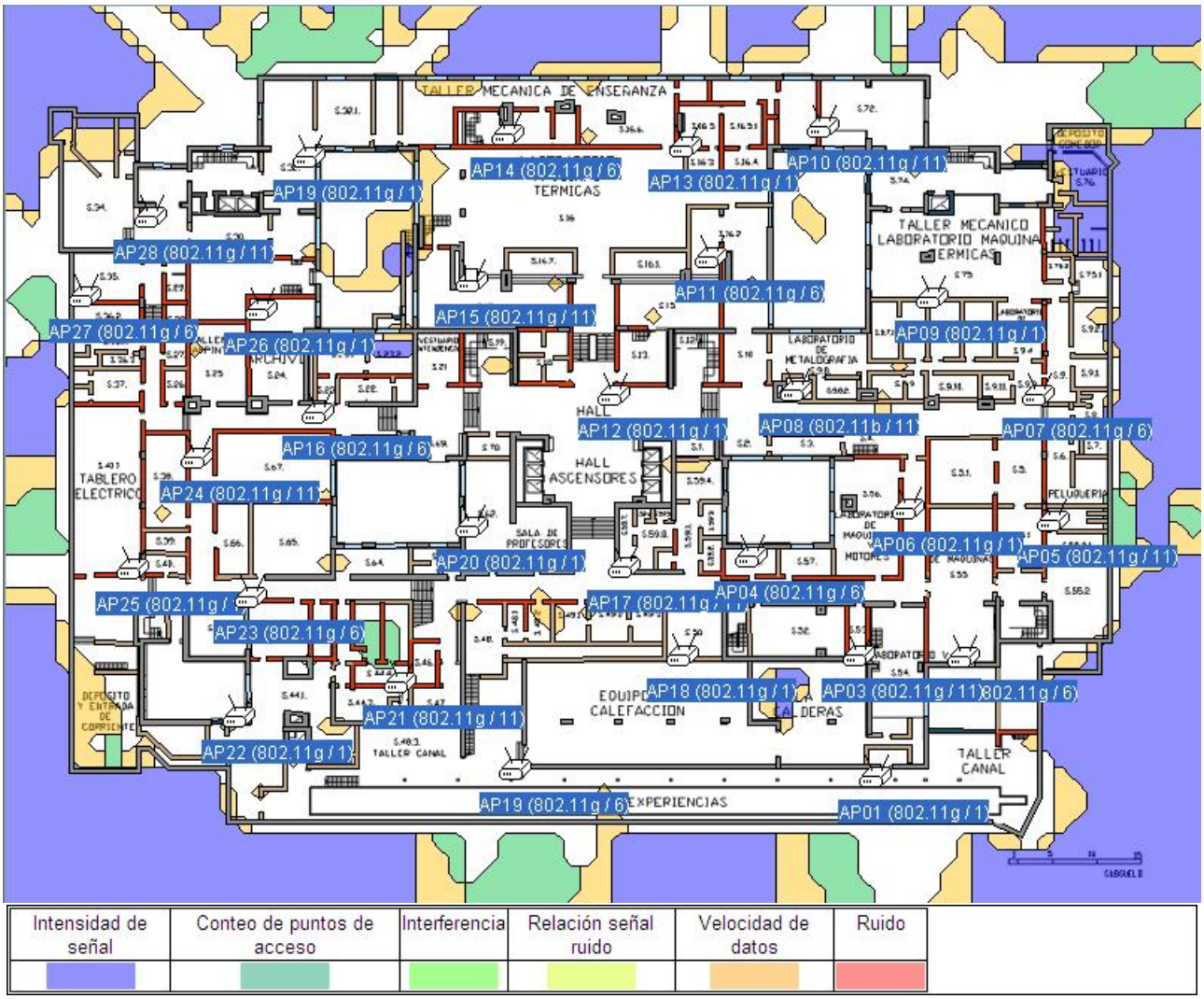


Figura 11.6: Motivo de fallo

11.2.2. Entre Piso

Intensidad de señal

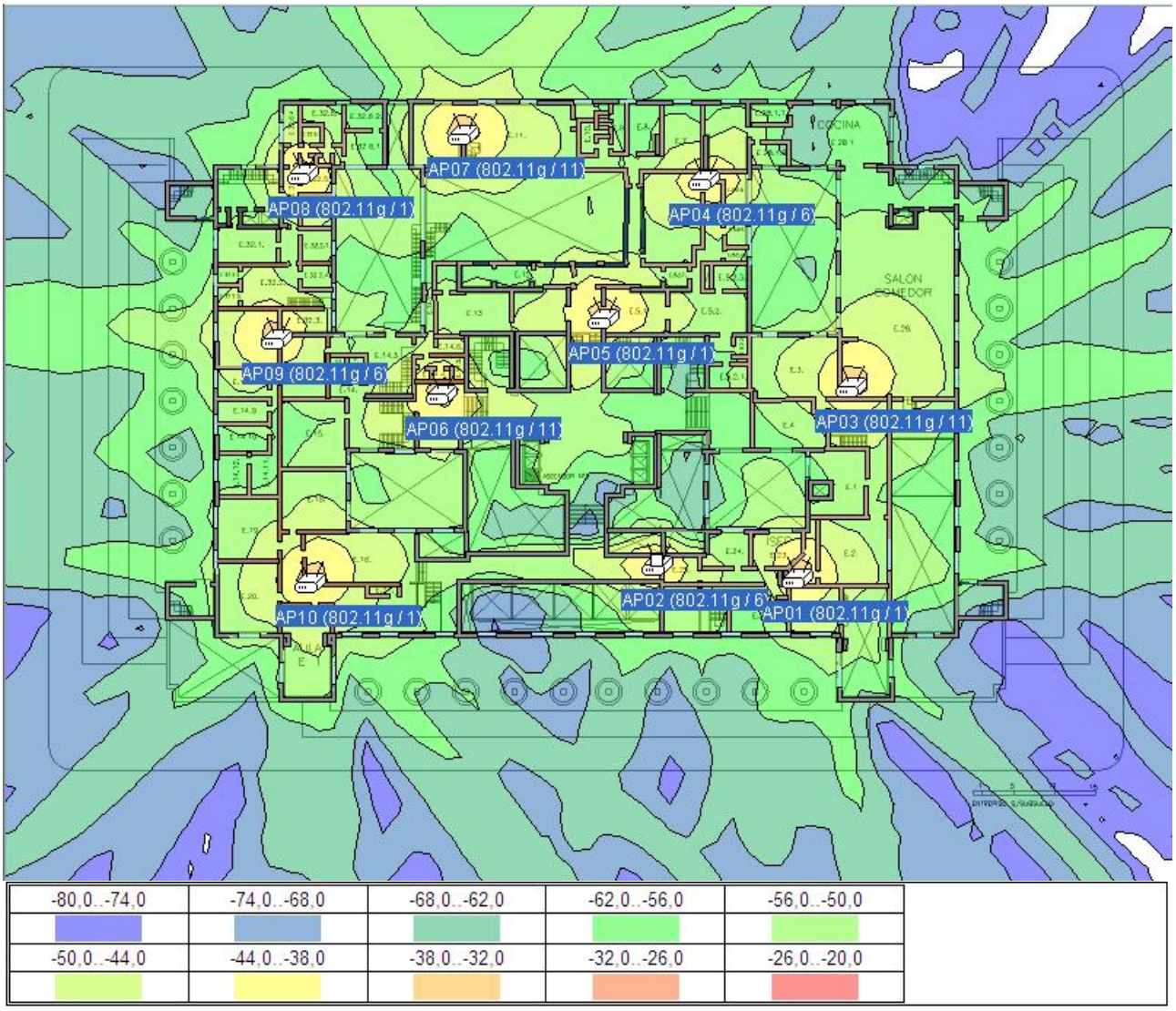


Figura 11.7: Intensidad de señal (dBm)

Relación señal ruido

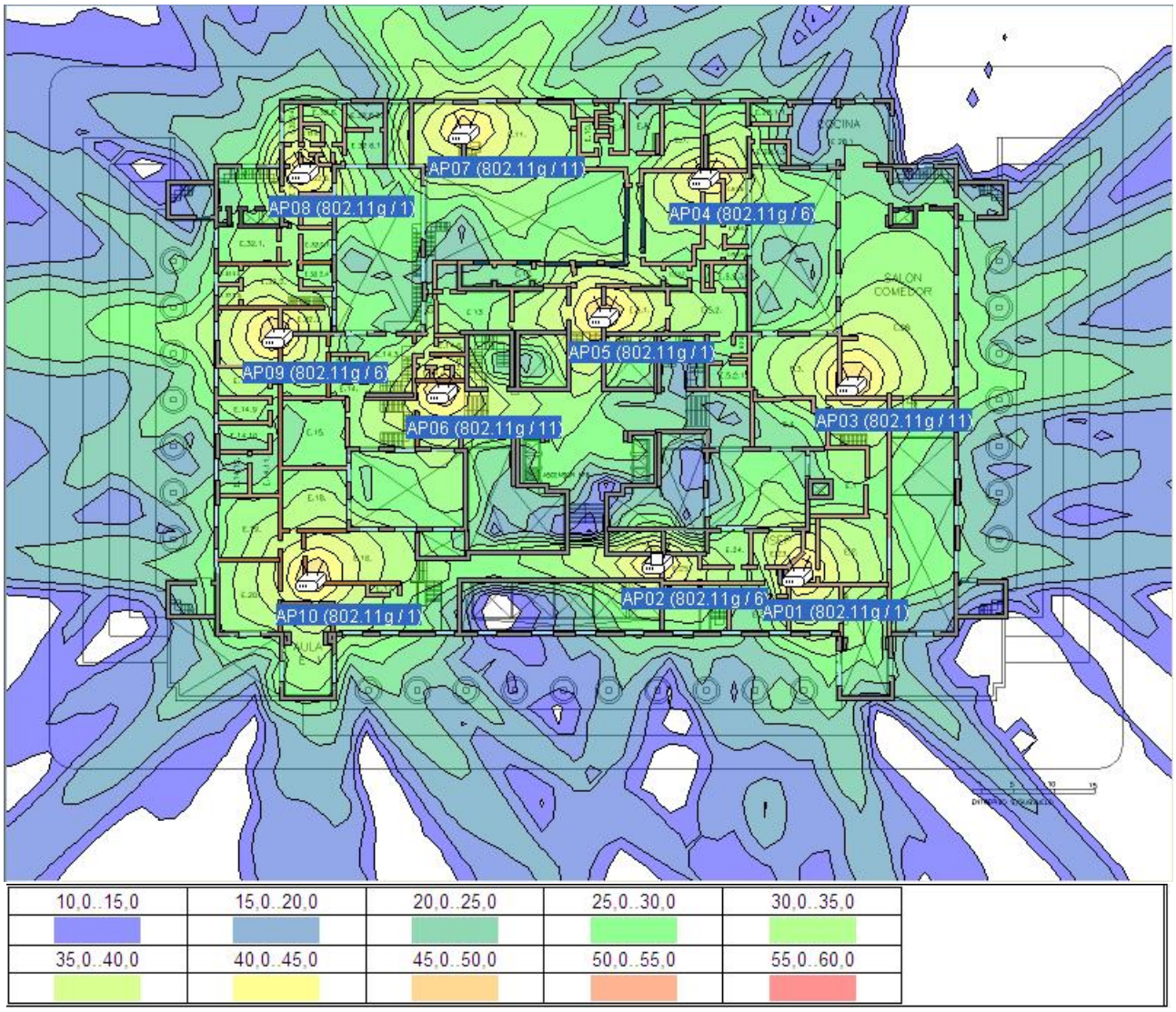


Figura 11.8: Relación señal ruido (dB)

Interferencia

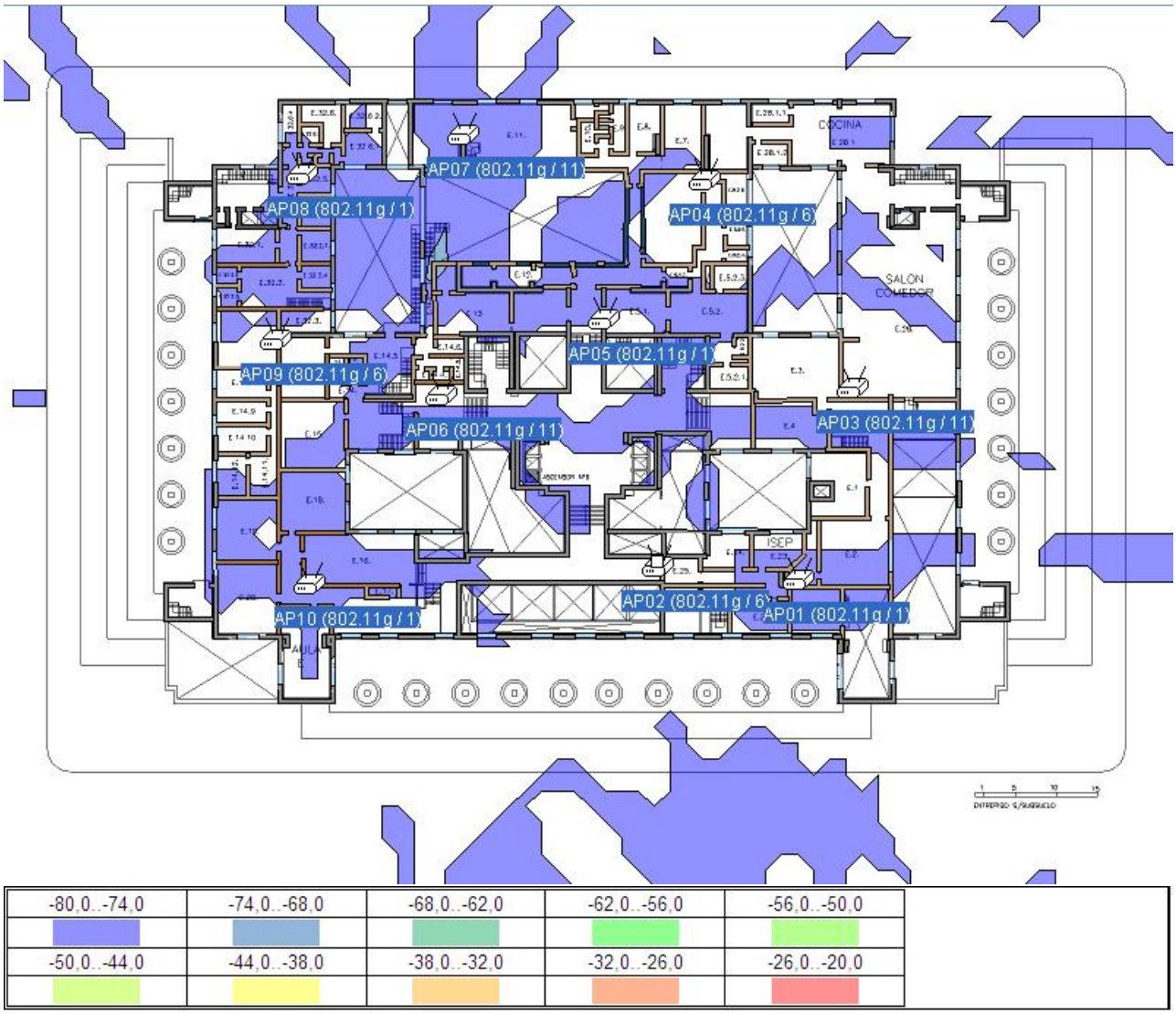


Figura 11.9: Interferencia (dBm)

Velocidad de datos

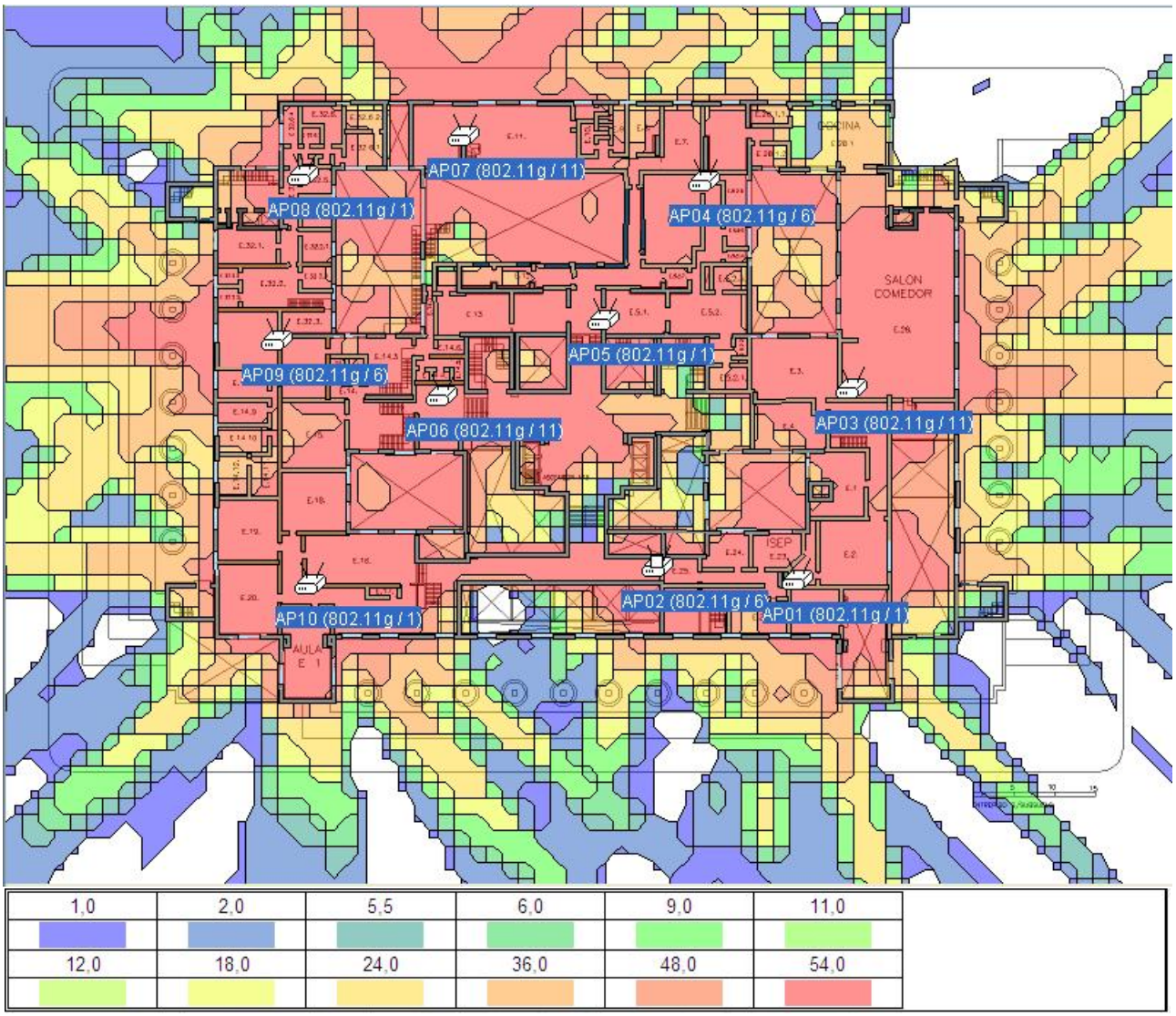


Figura 11.10: Velocidad de datos ($Mbps$)

Estado de RF

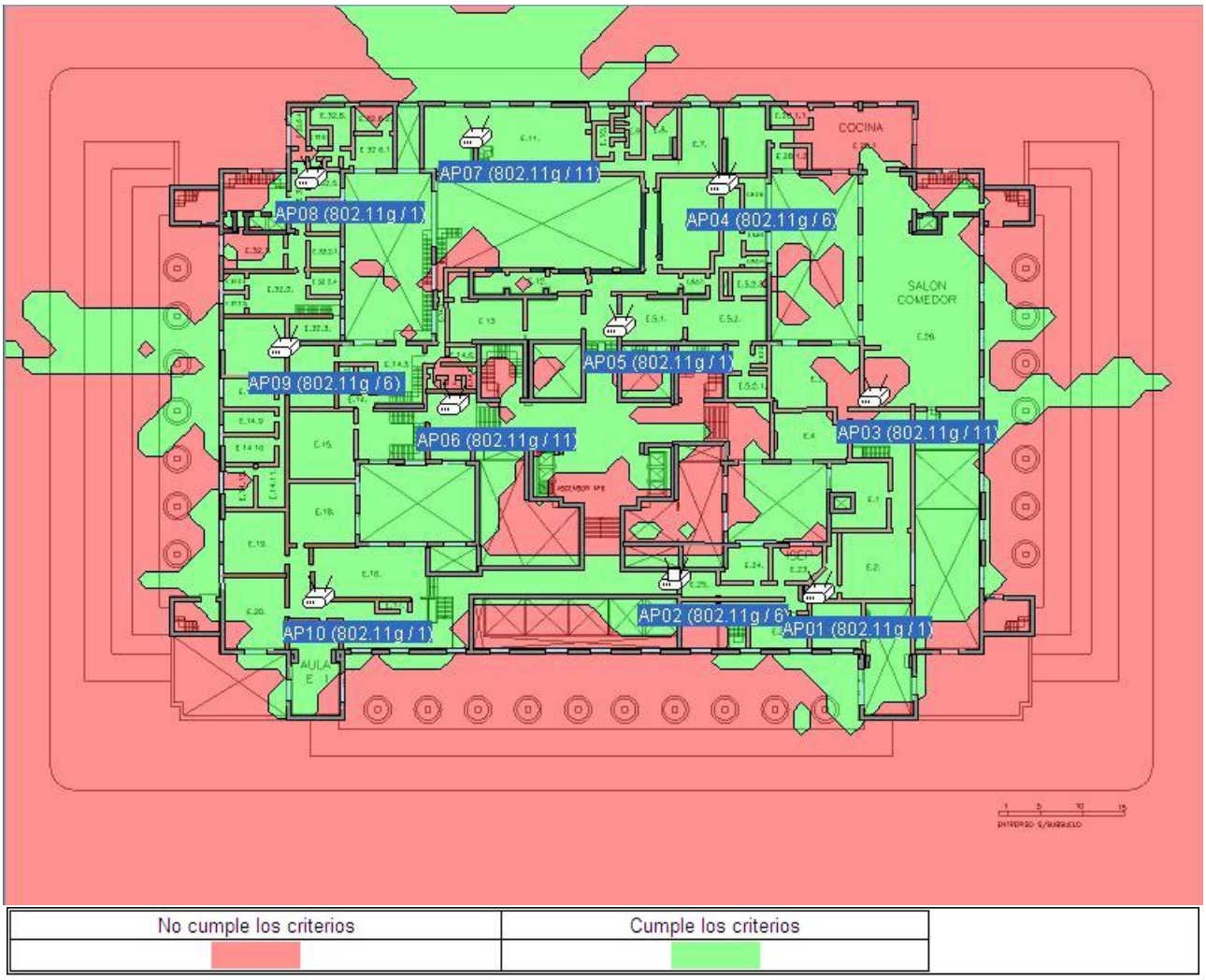


Figura 11.11: Estado RF

Motivo de fallo

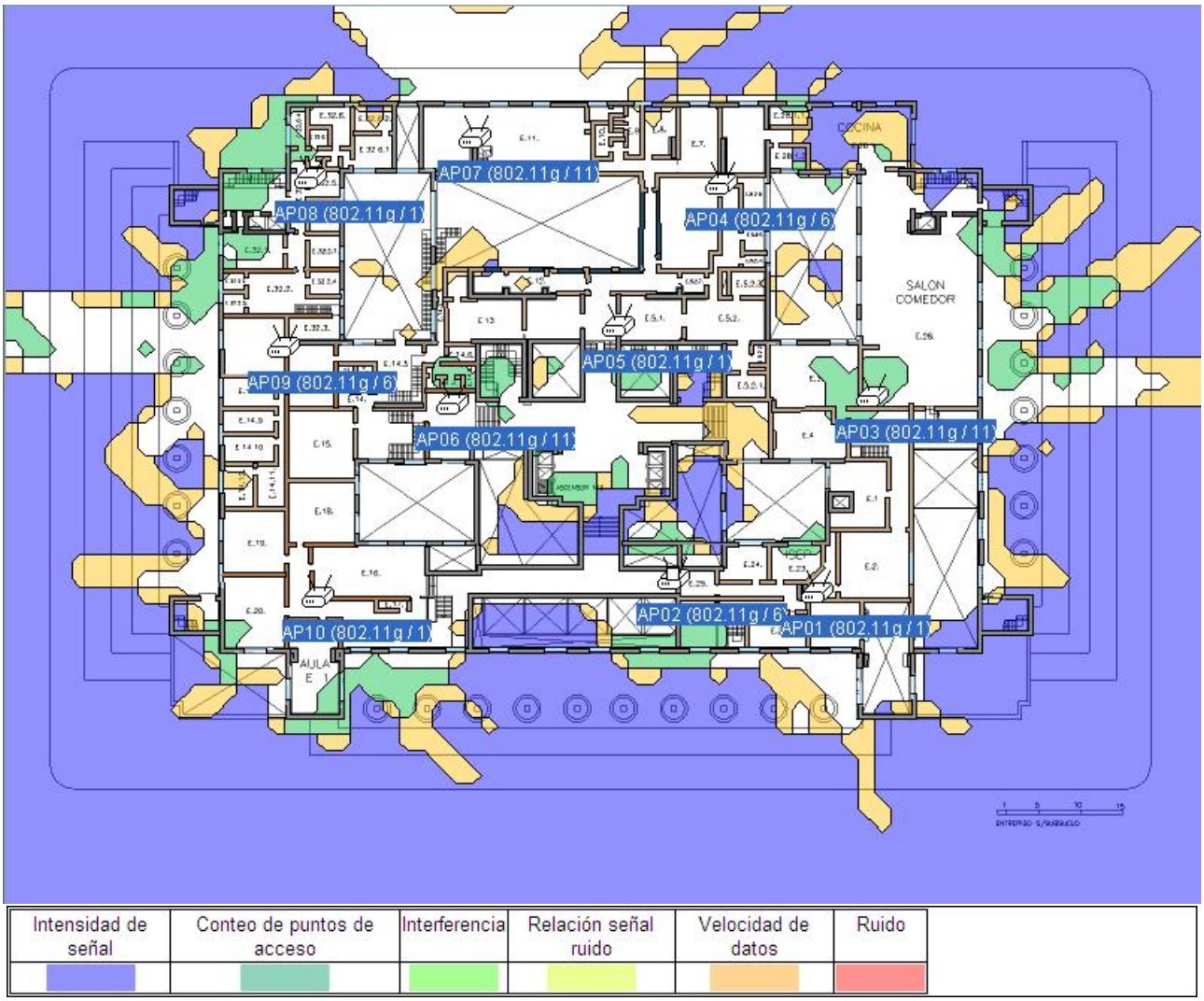


Figura 11.12: Motivo de fallo

11.2.3. Planta Baja

Intensidad de señal

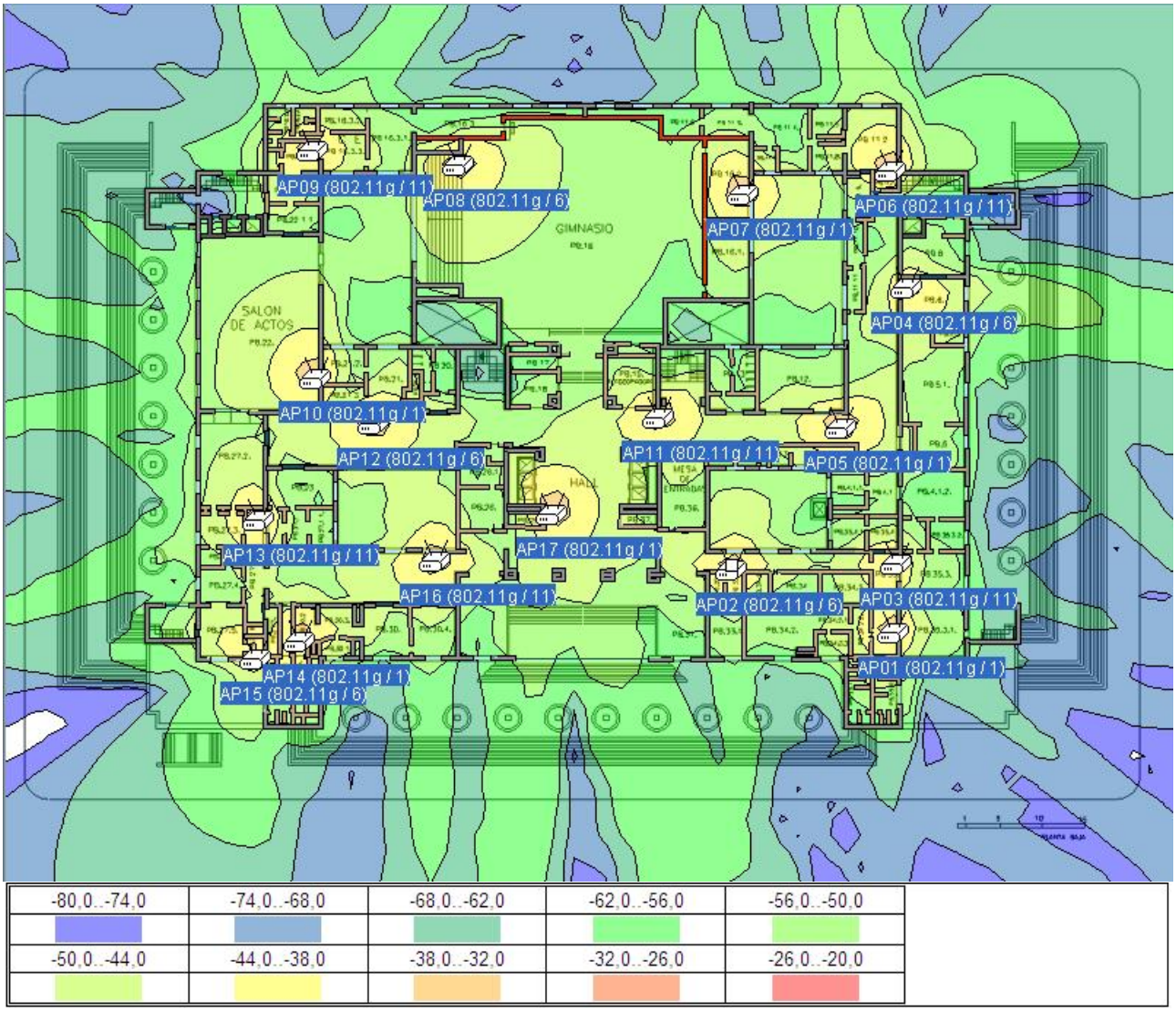


Figura 11.13: Intensidad de señal (dBm)

Relación señal ruido

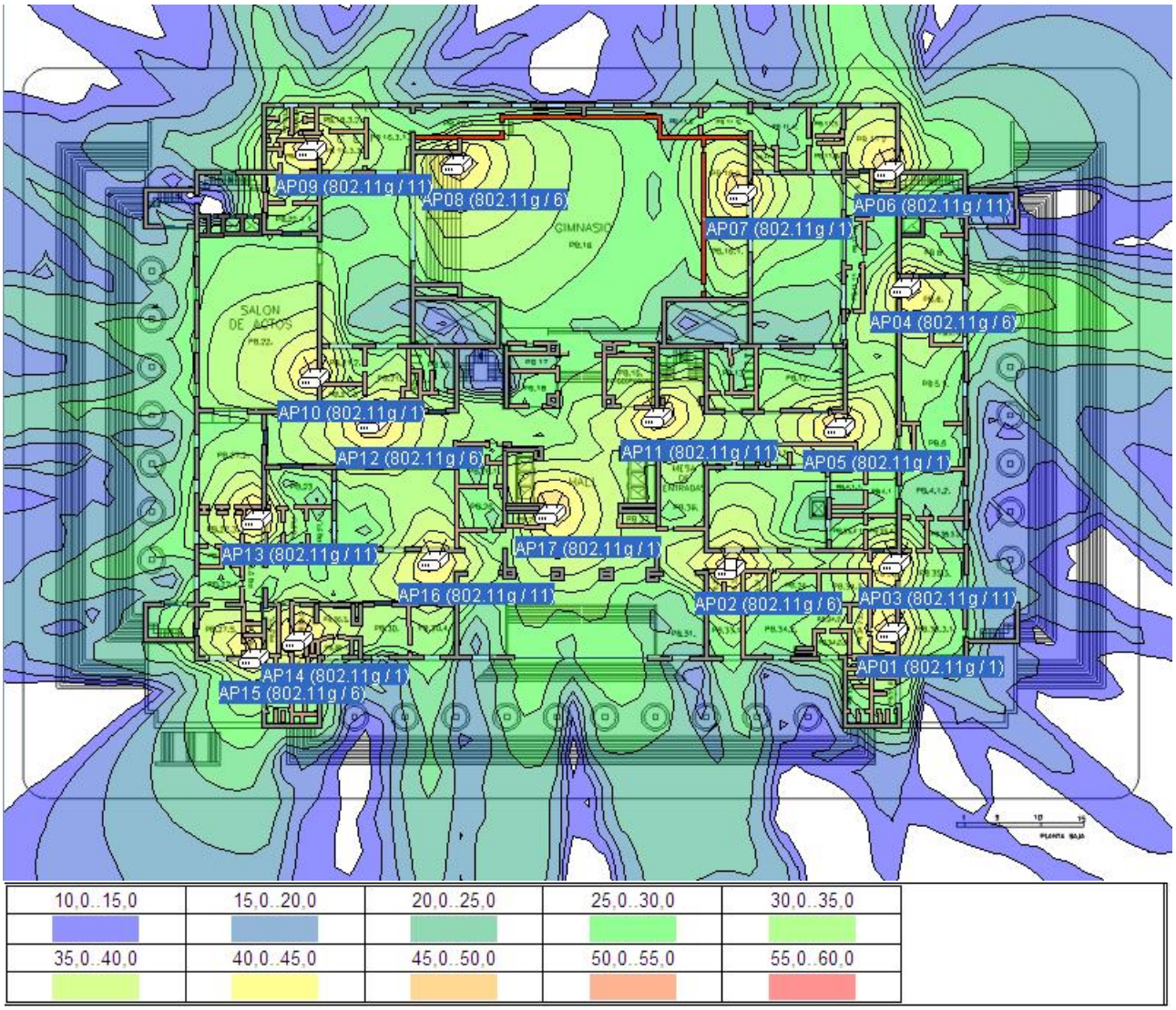


Figura 11.14: Relación señal ruido (dB)

Interferencia

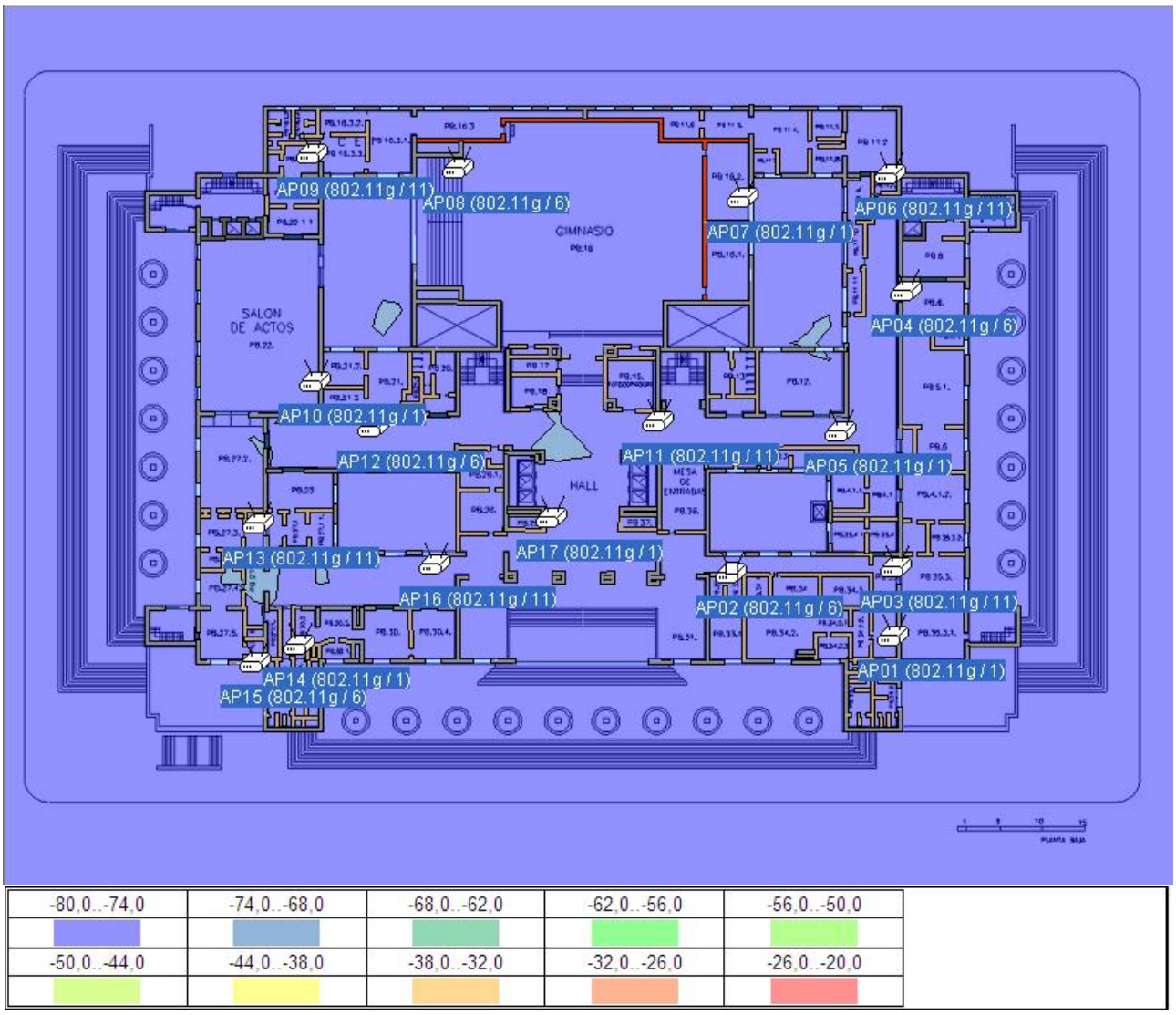


Figura 11.15: Interferencia (dBm)

Velocidad de datos

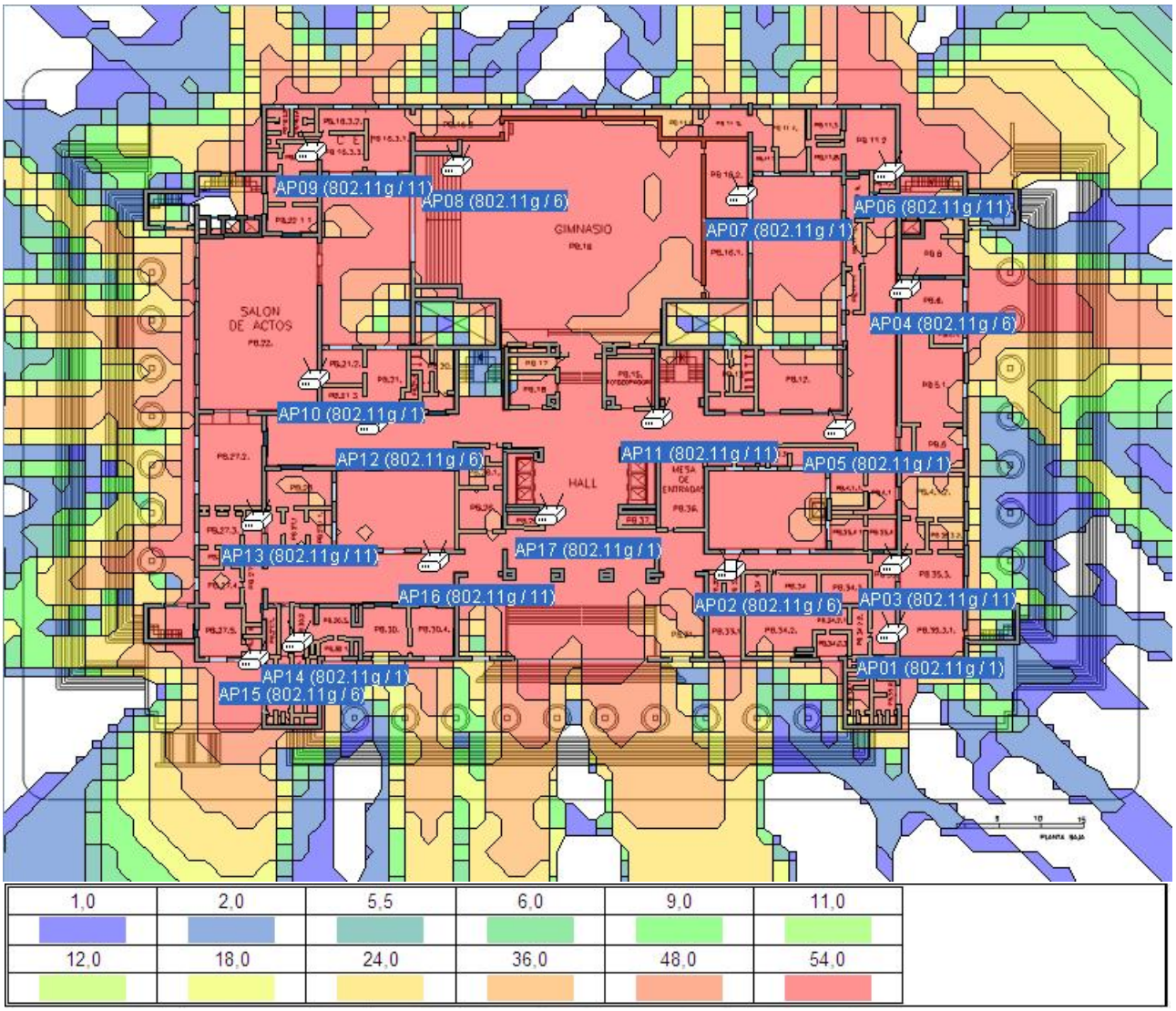


Figura 11.16: Velocidad de datos ($Mbps$)

Estado de RF

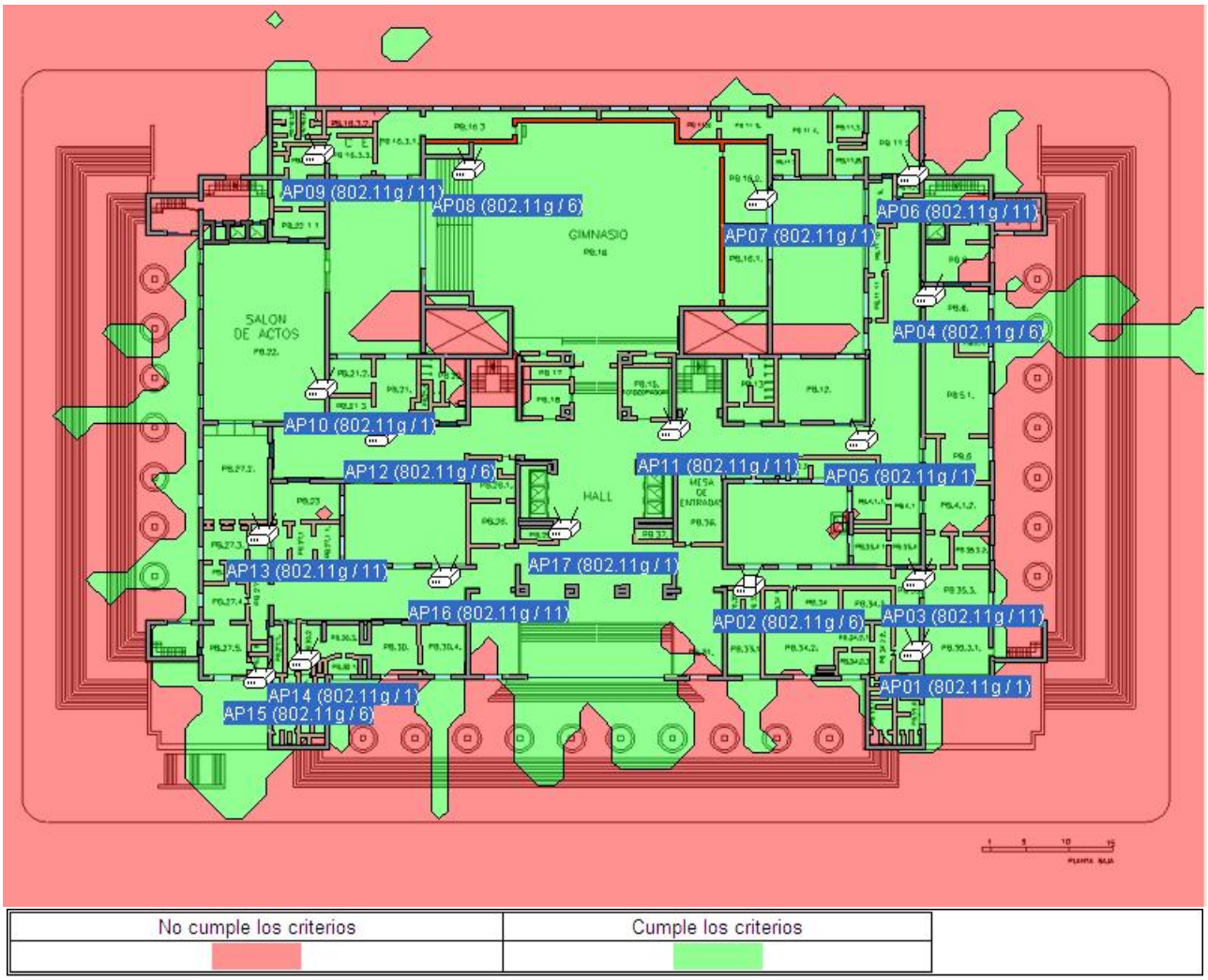


Figura 11.17: Estado RF

Motivo de fallo

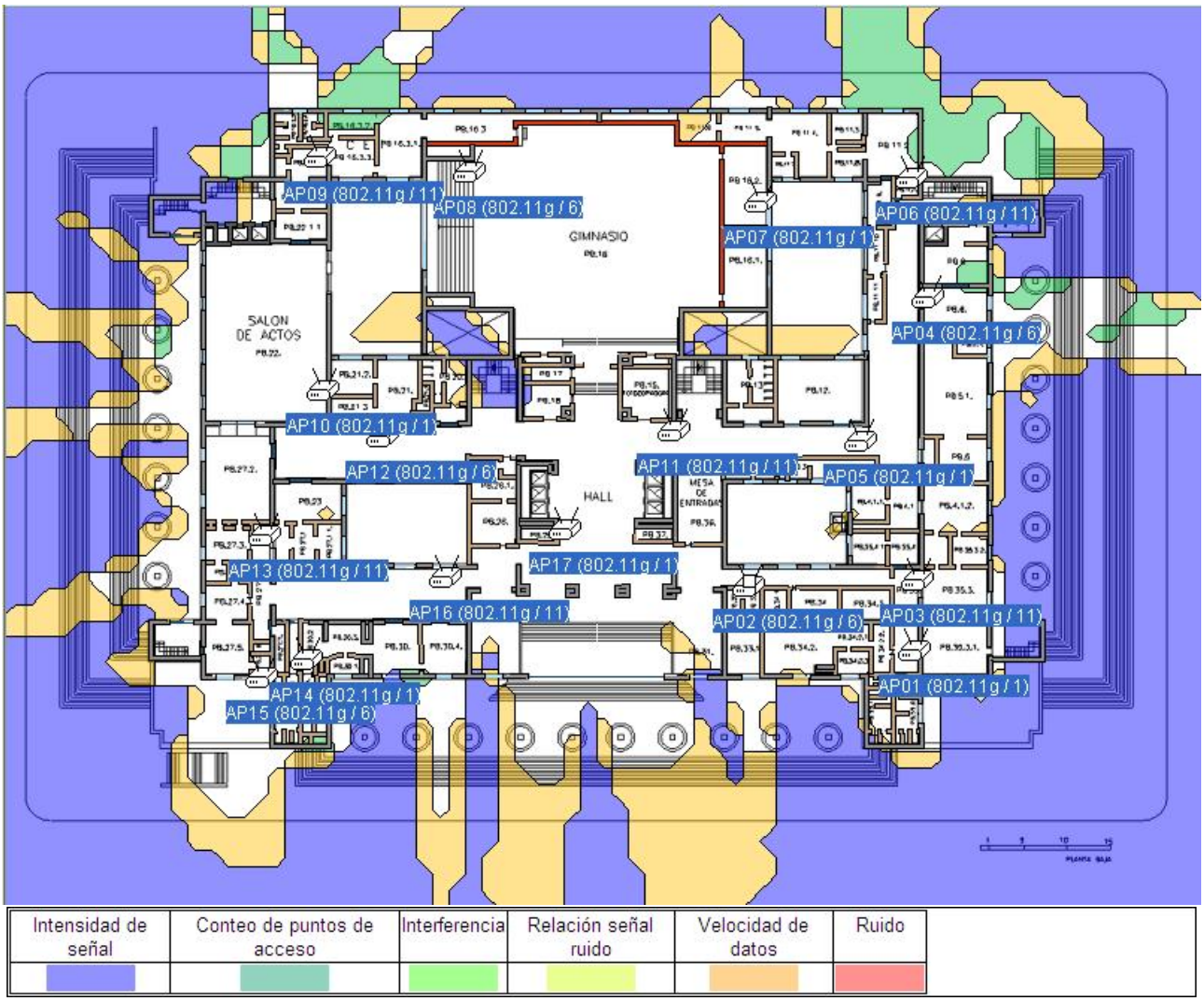


Figura 11.18: Motivo de fallo

11.2.4. Piso 1

Intensidad de señal

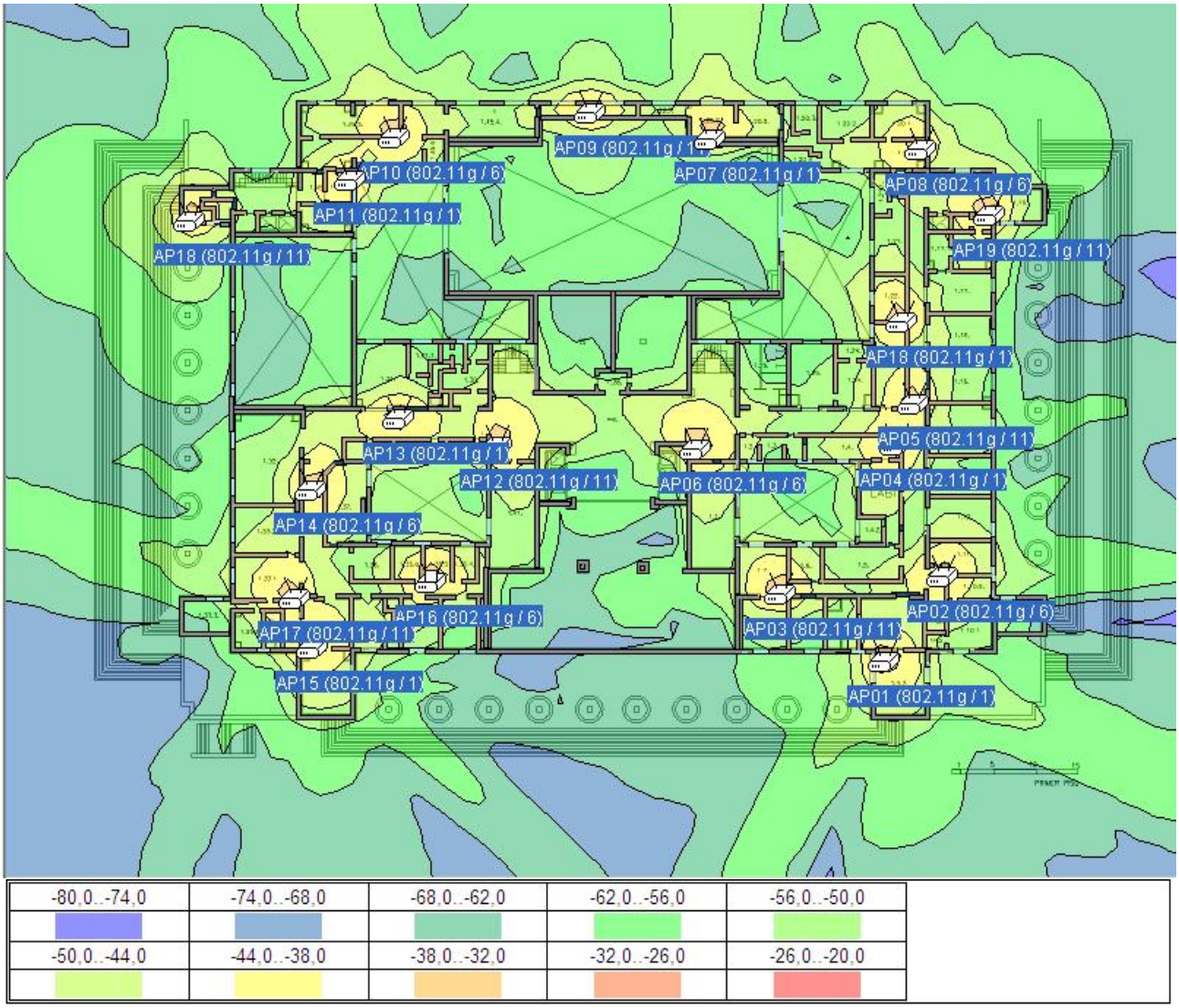


Figura 11.19: Intensidad de señal (dBm)

Relación señal ruido

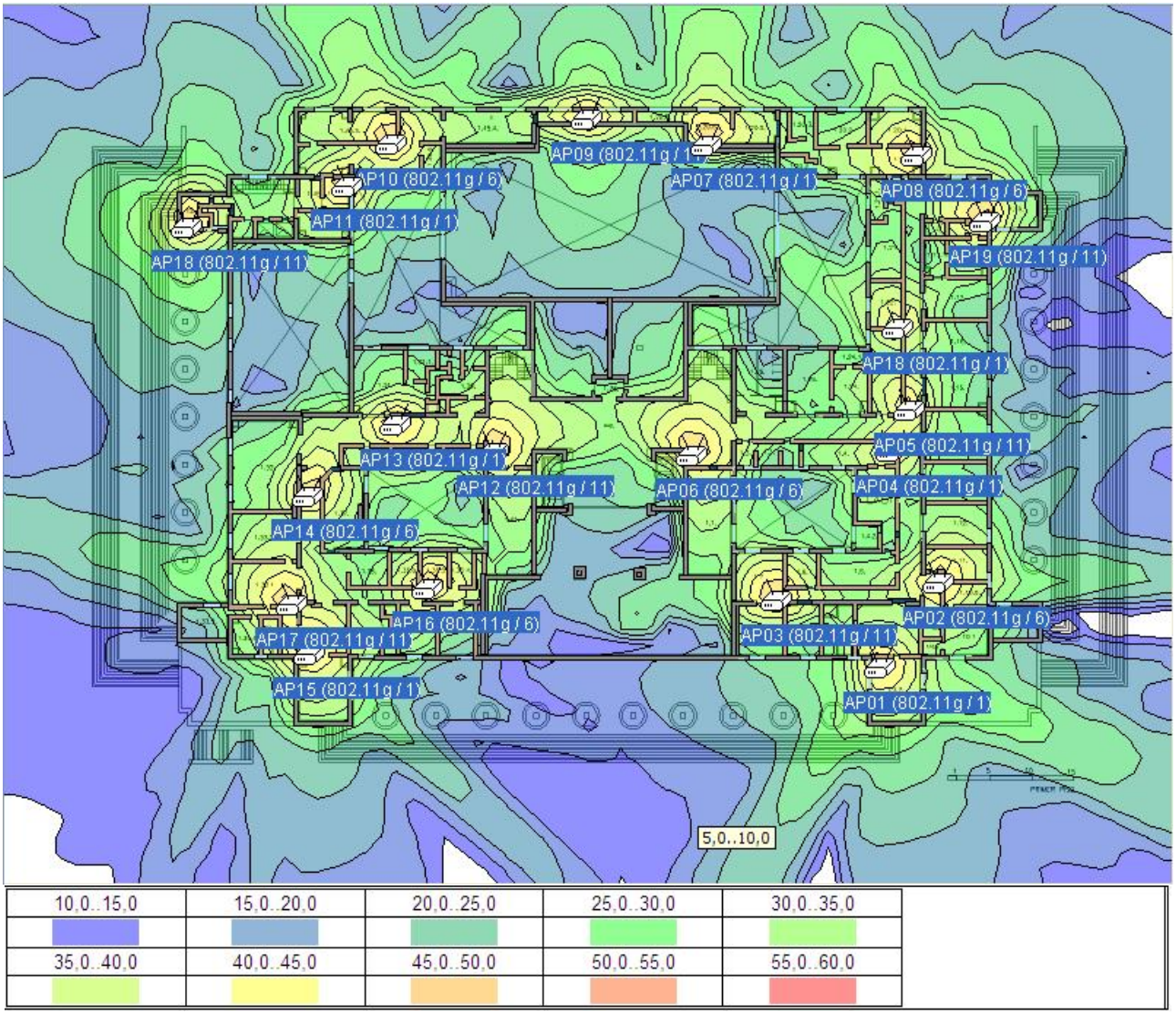


Figura 11.20: Relación señal ruido (dB)

Interferencia

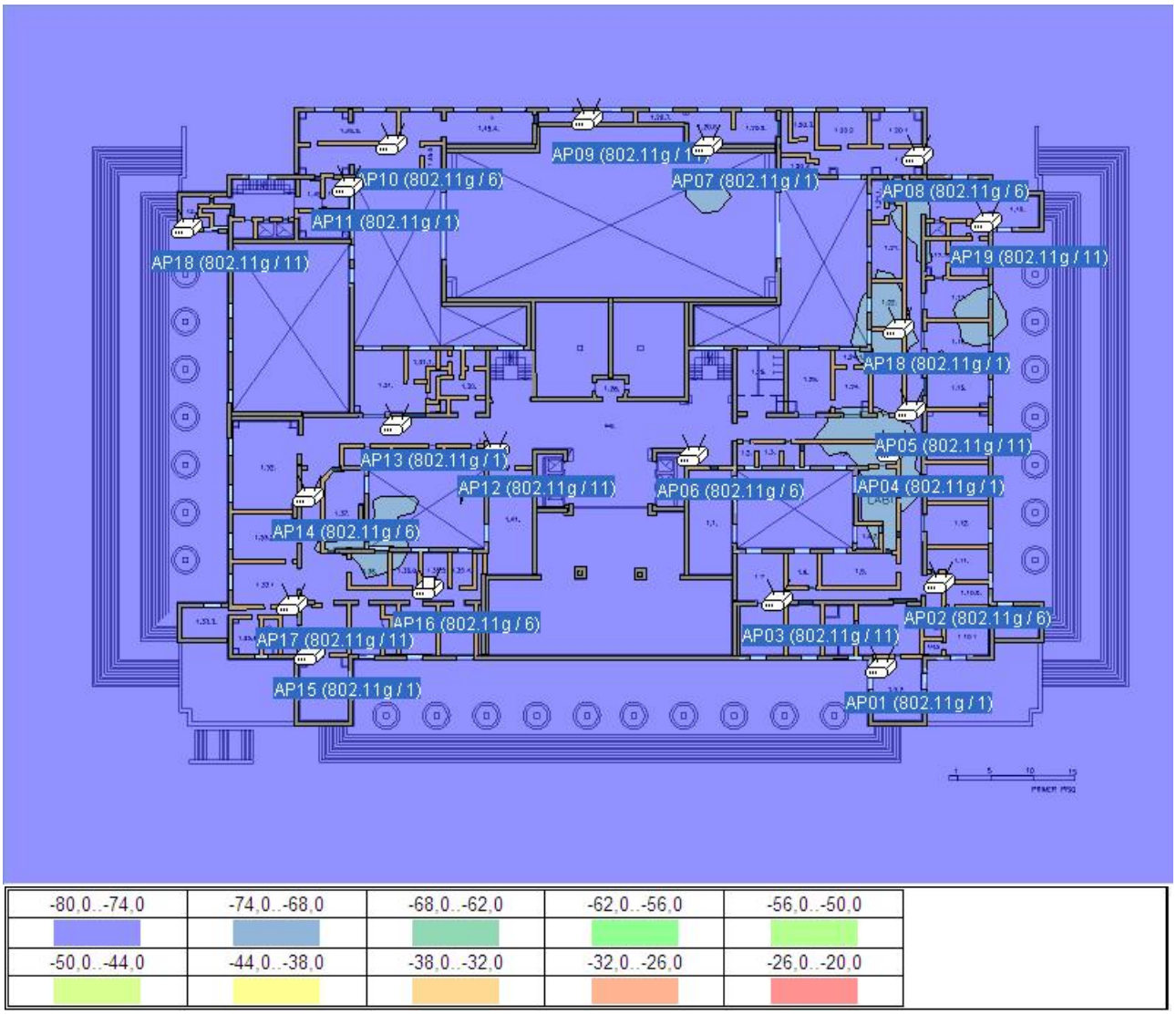


Figura 11.21: Interferencia (dBm)

Velocidad de datos

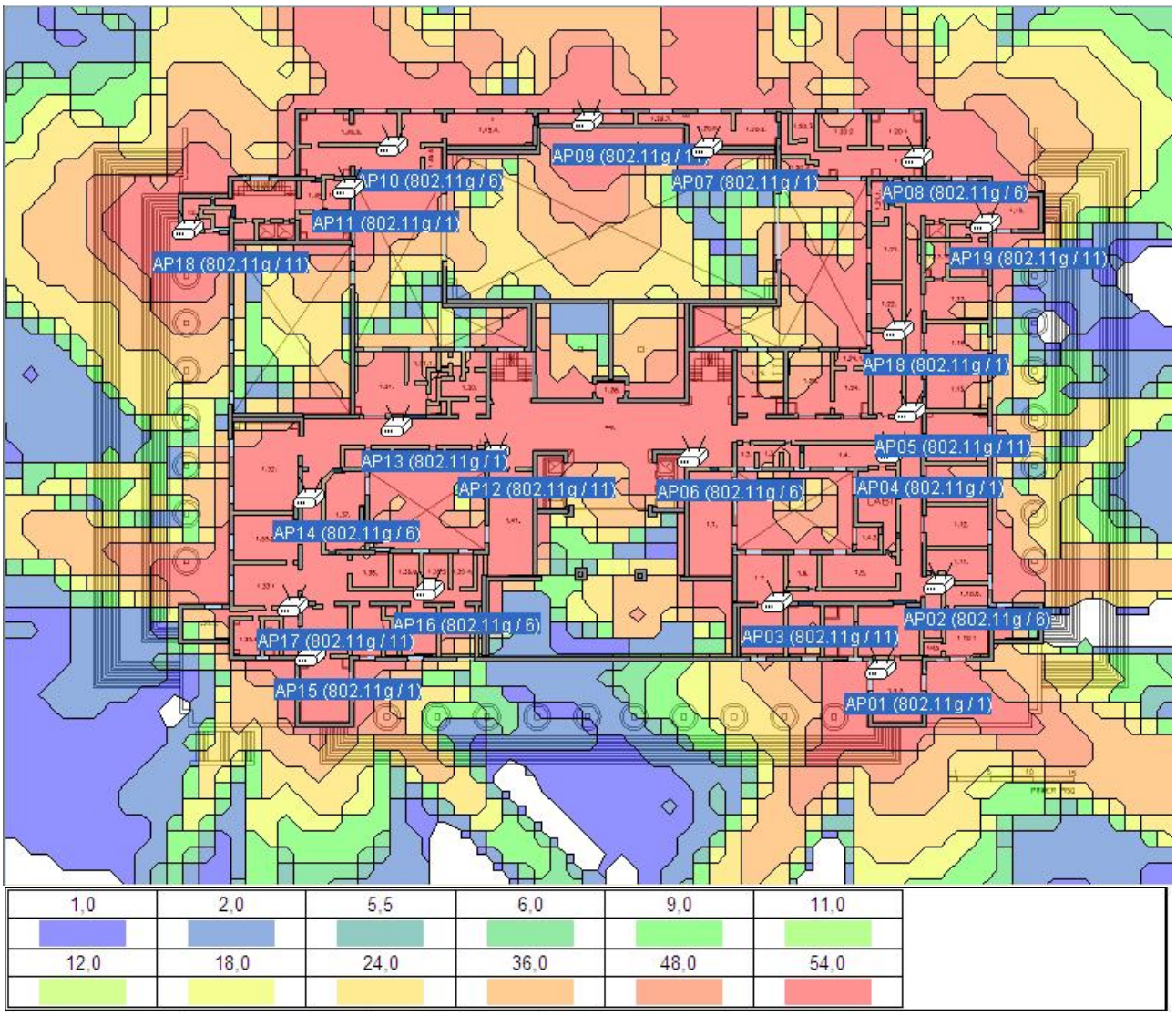


Figura 11.22: Velocidad de datos ($Mbps$)

Estado de RF

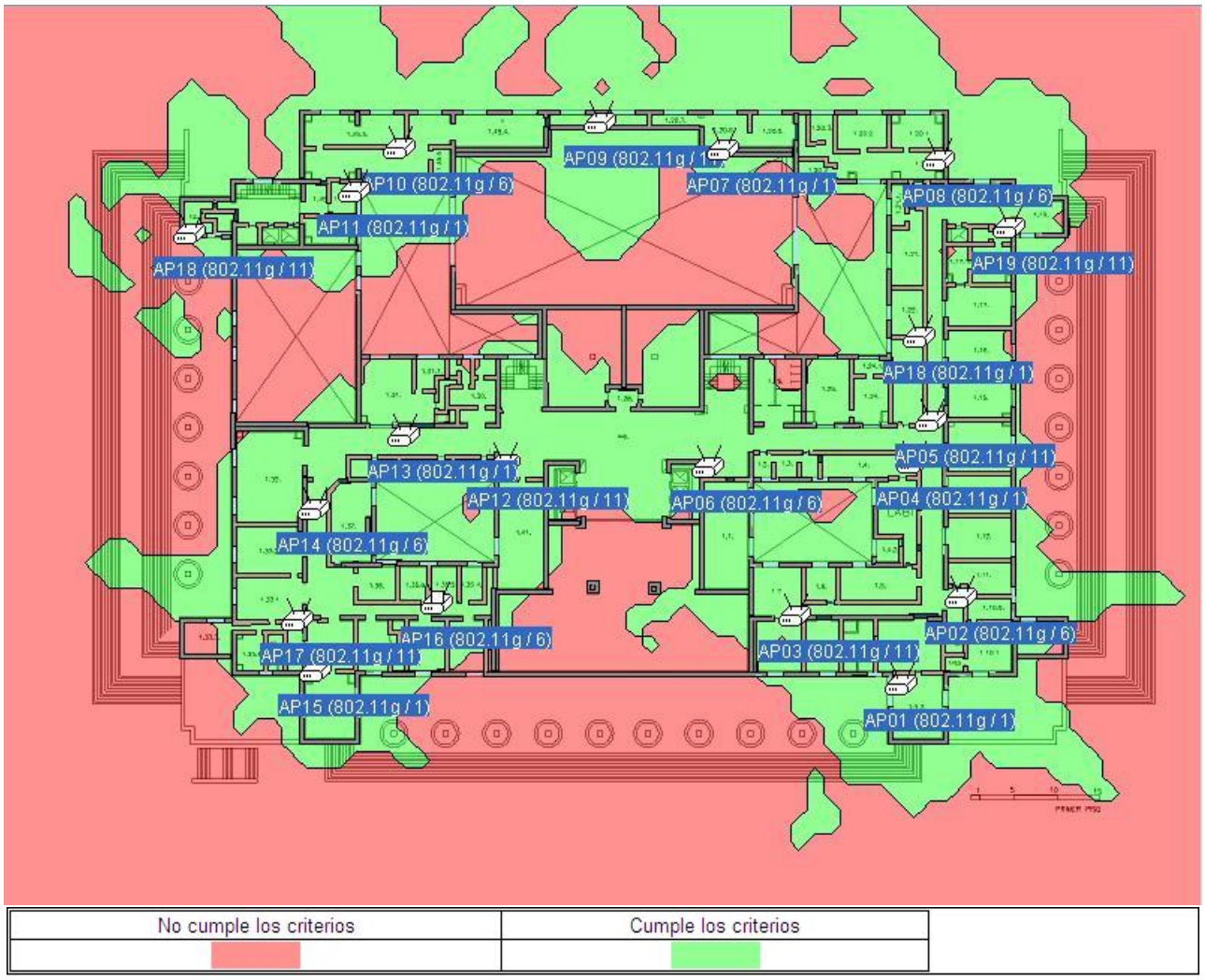


Figura 11.23: Estado RF

Motivo de fallo

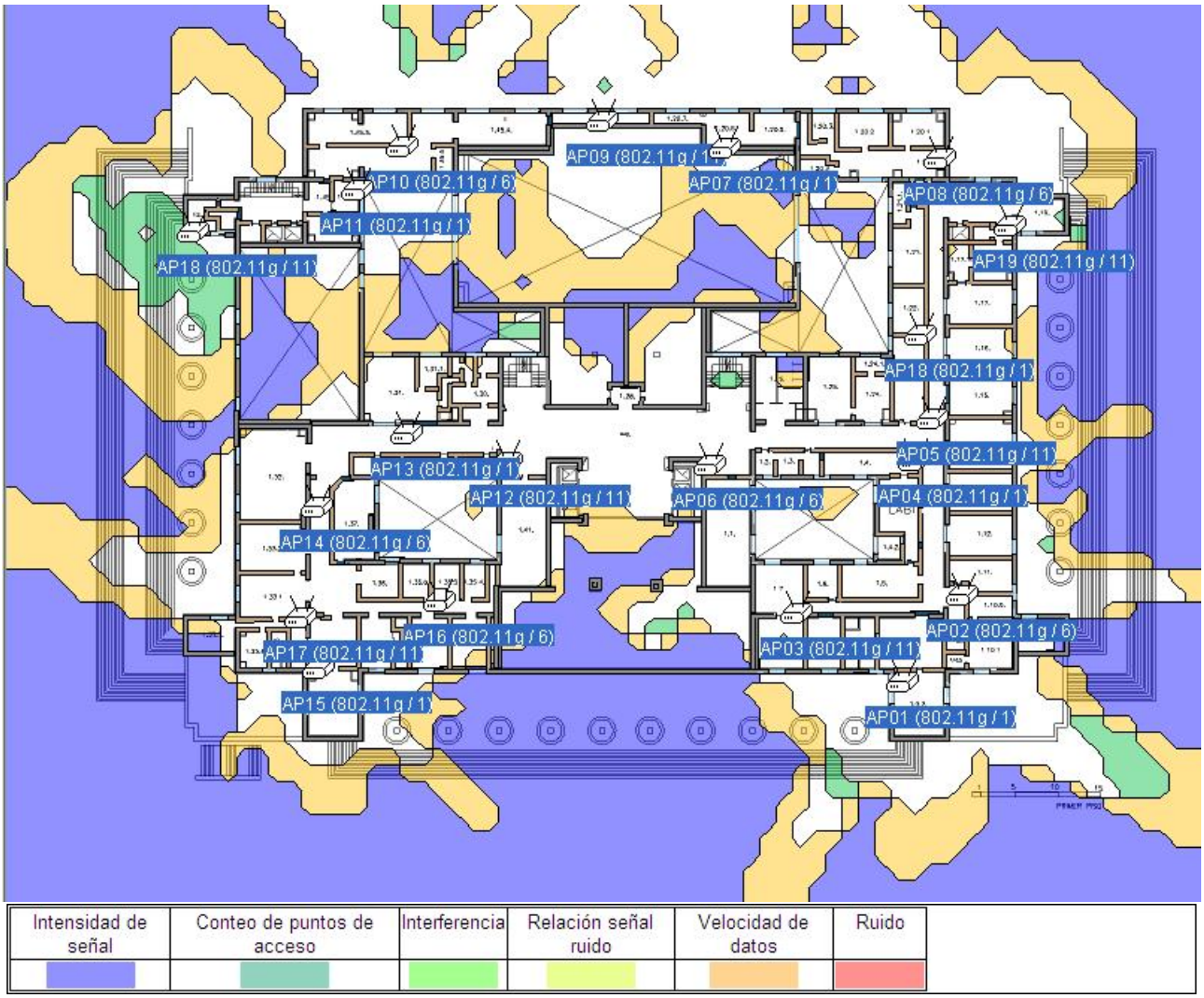


Figura 11.24: Motivo de fallo

11.2.5. Piso 2

Intensidad de señal

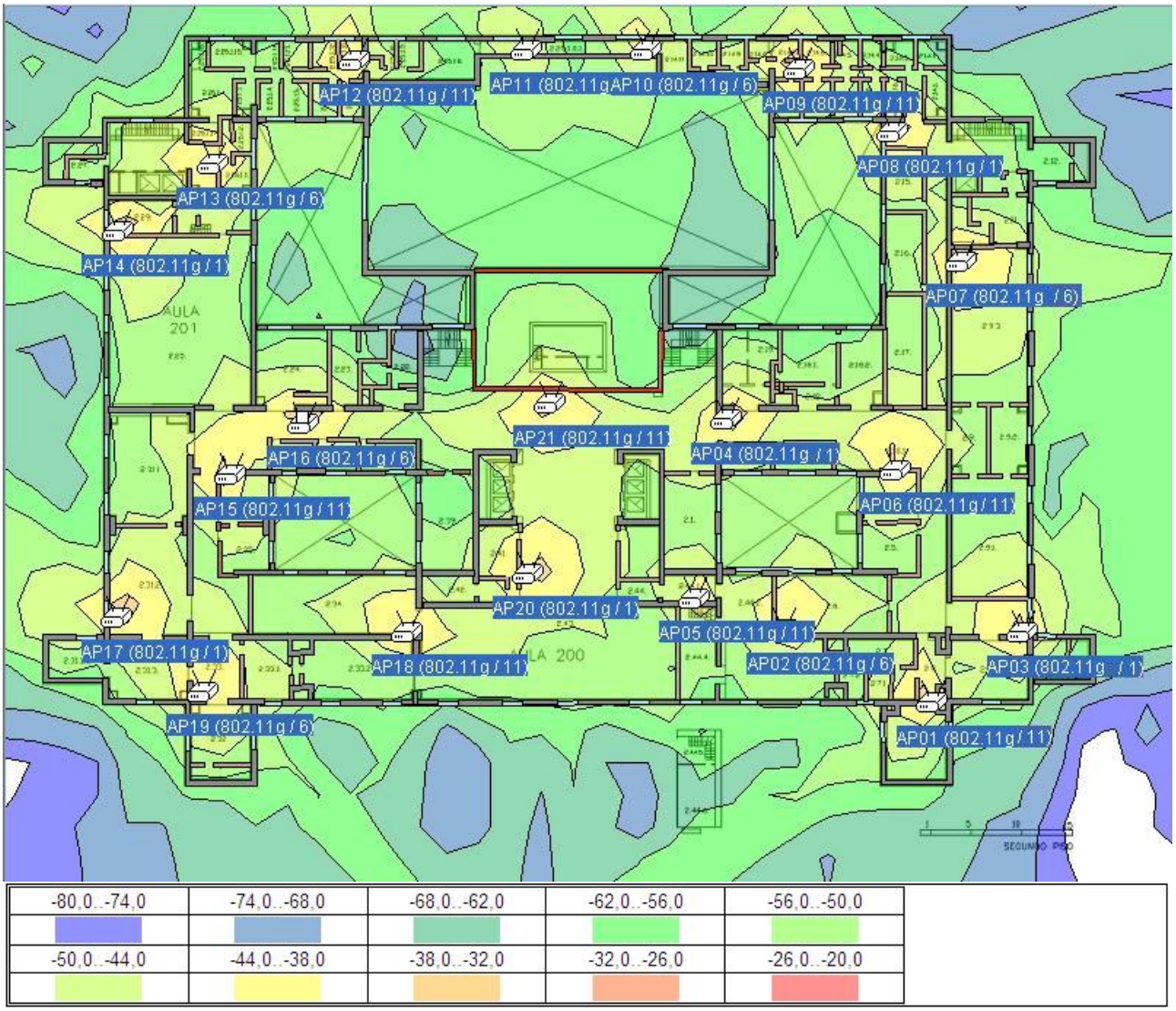


Figura 11.25: Intensidad de señal (dBm)

Relación señal ruido

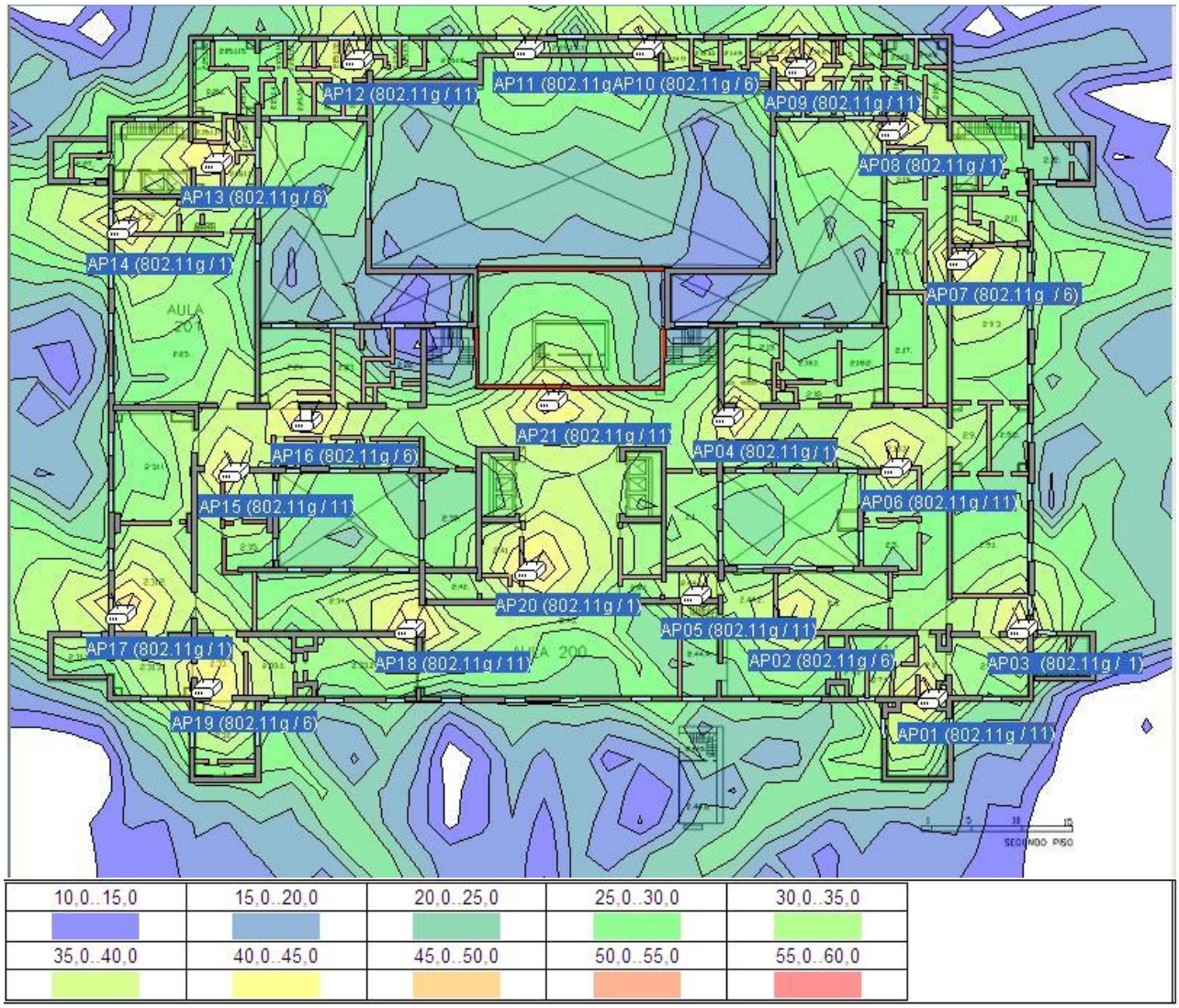


Figura 11.26: Relación señal ruido (dB)

Interferencia

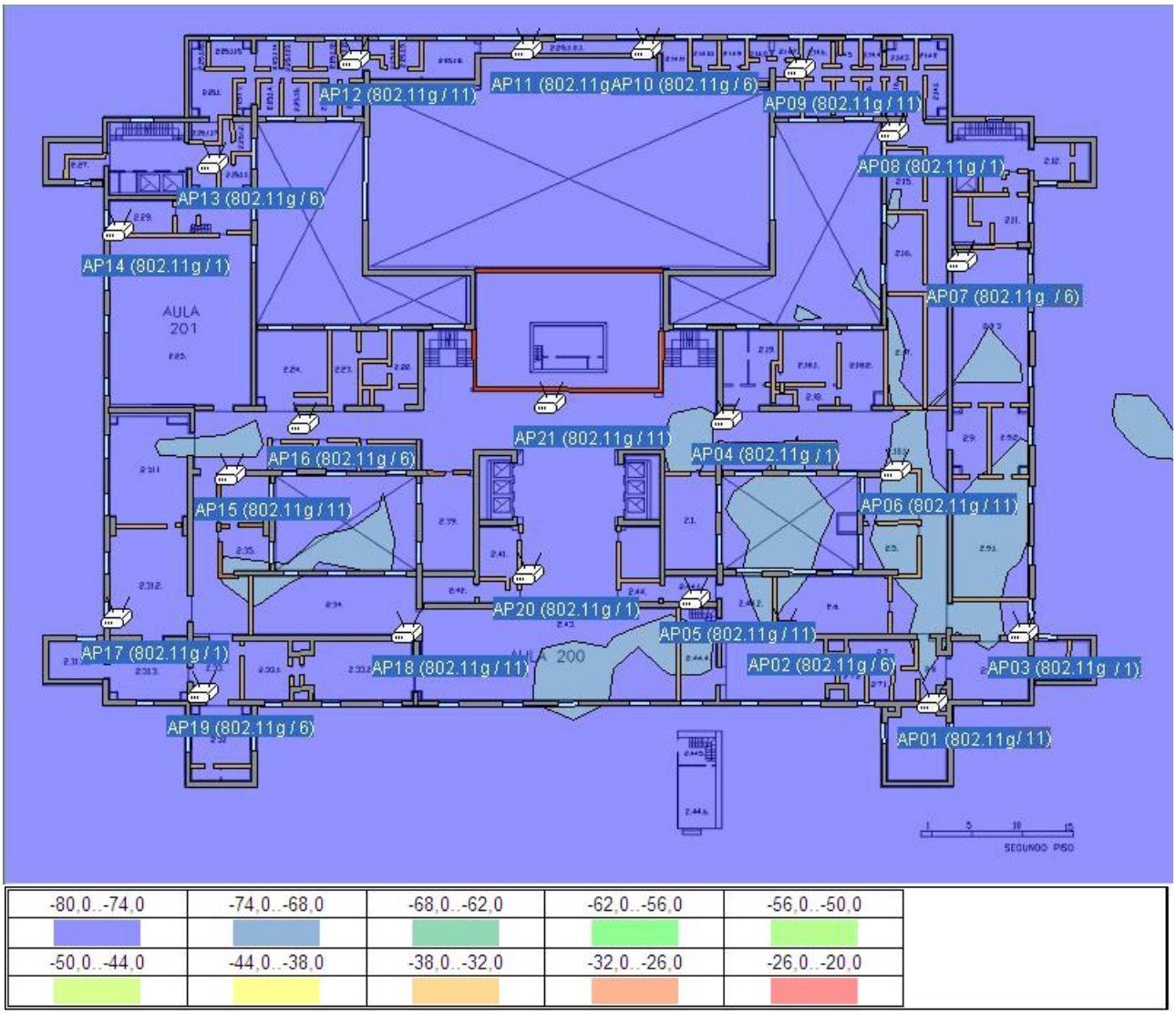


Figura 11.27: Interferencia (dBm)

Velocidad de datos

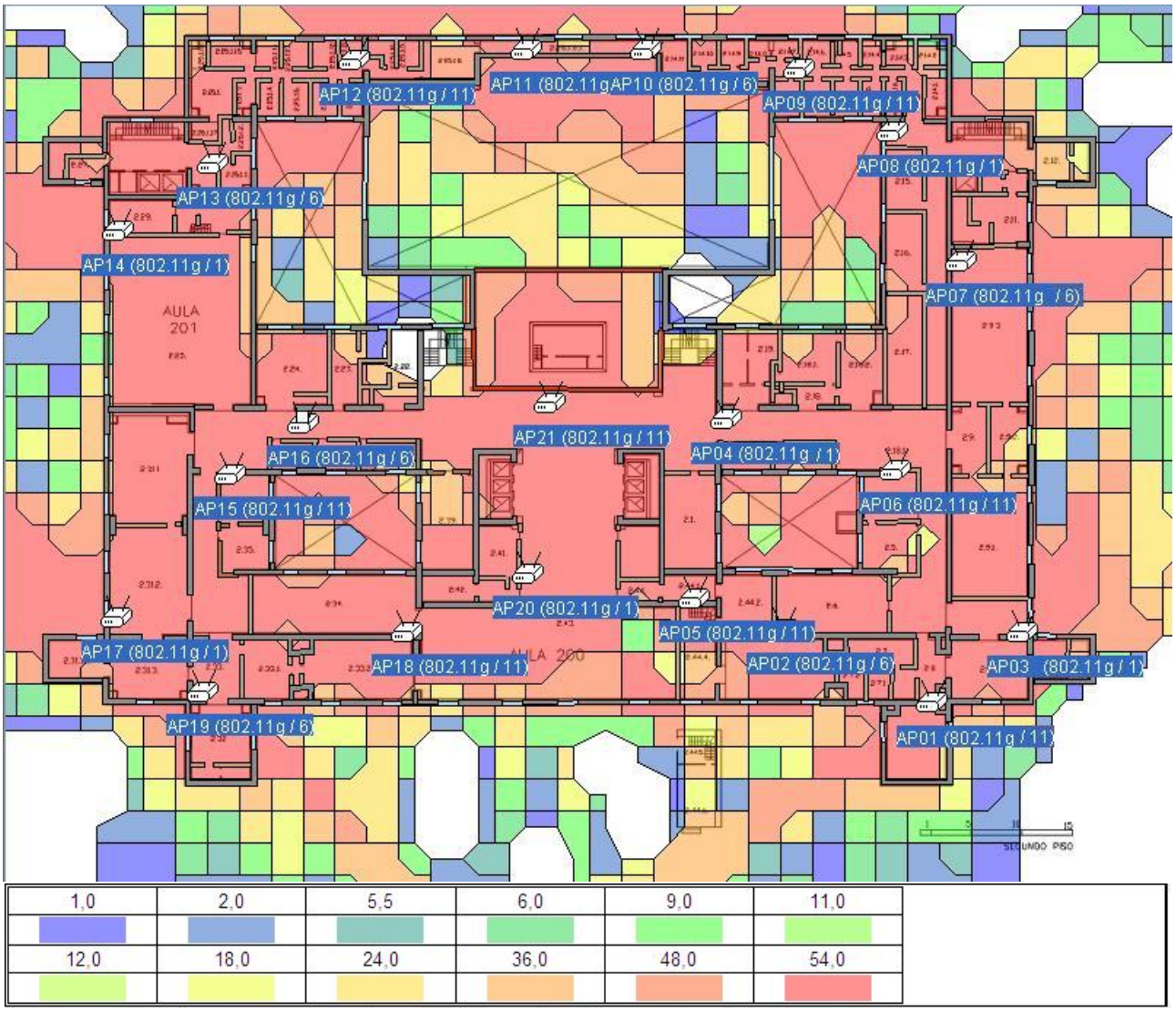


Figura 11.28: Velocidad de datos ($Mbps$)

Estado de RF

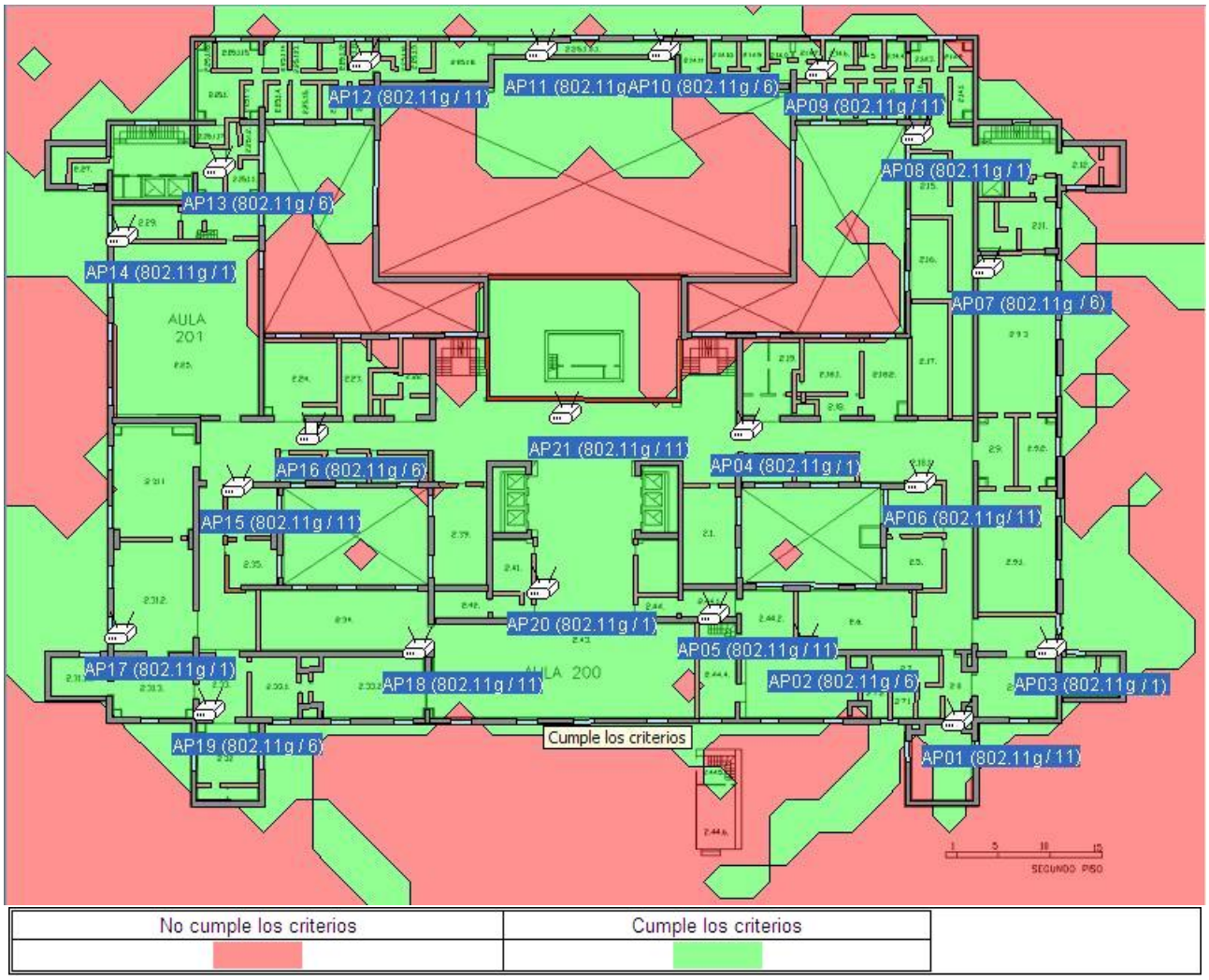


Figura 11.29: Estado RF

Motivo de fallo

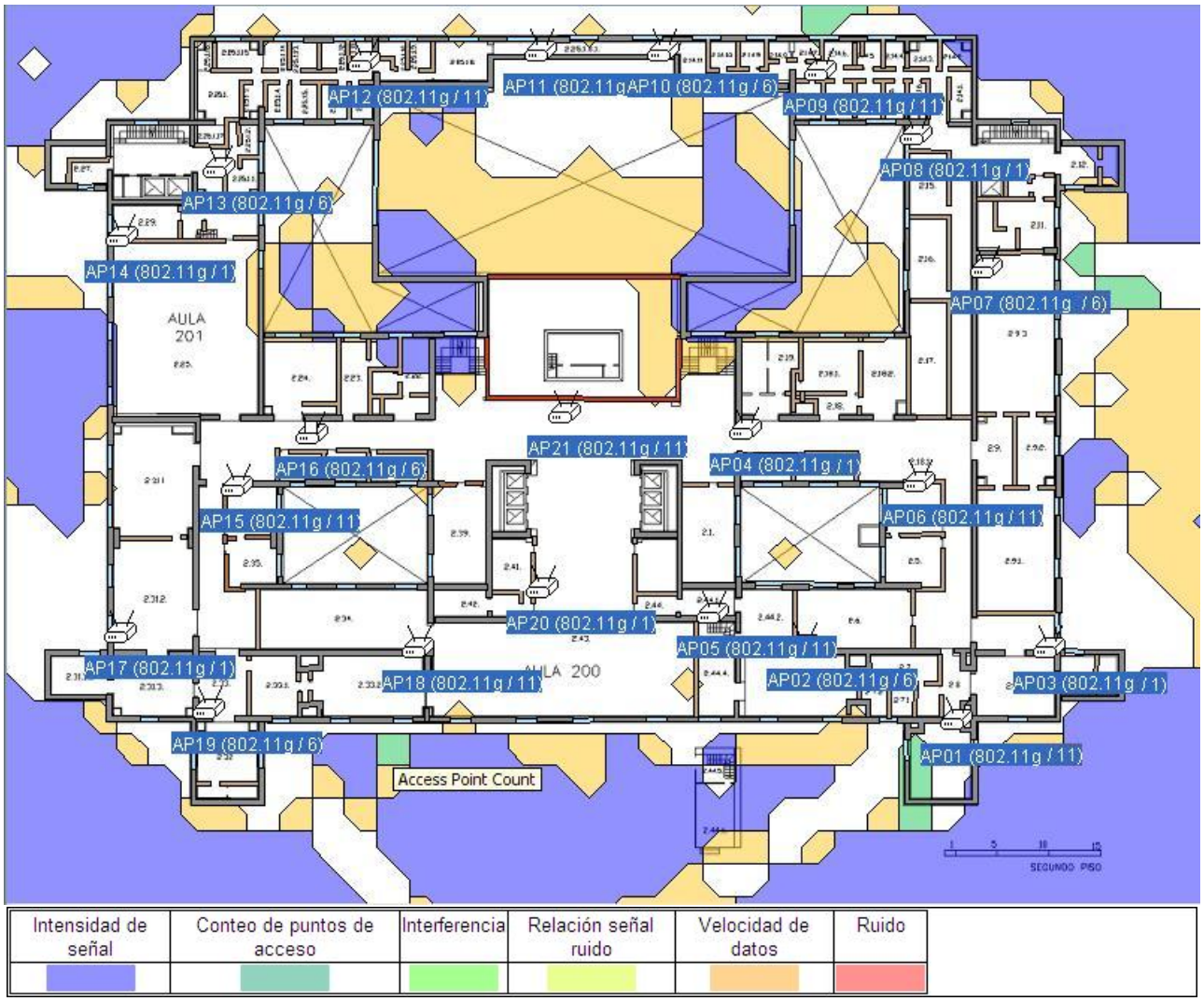


Figura 11.30: Motivo de fallo

11.2.6. Piso 3

Intensidad de señal

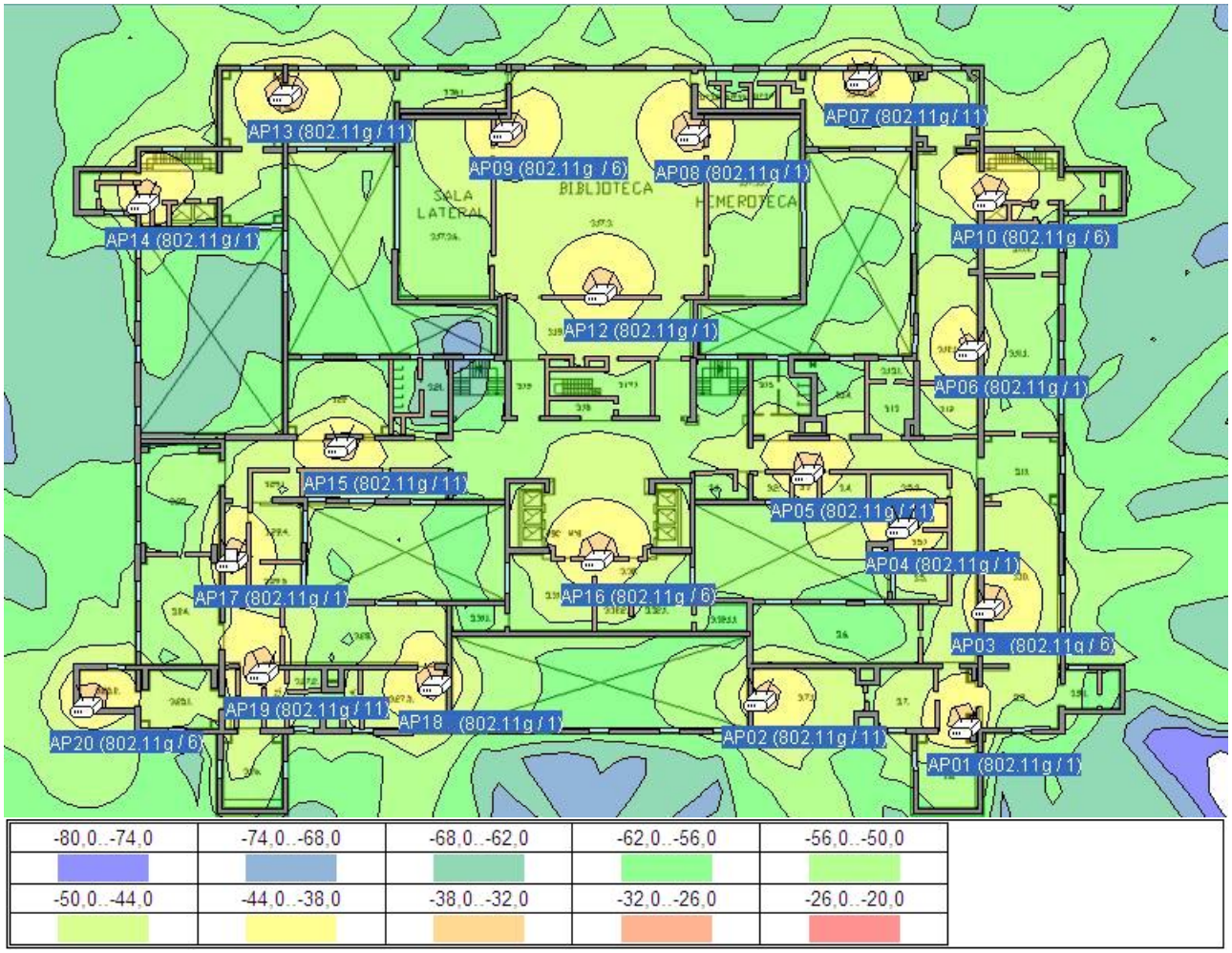


Figura 11.31: Intensidad de señal (dBm)

Relación señal ruido

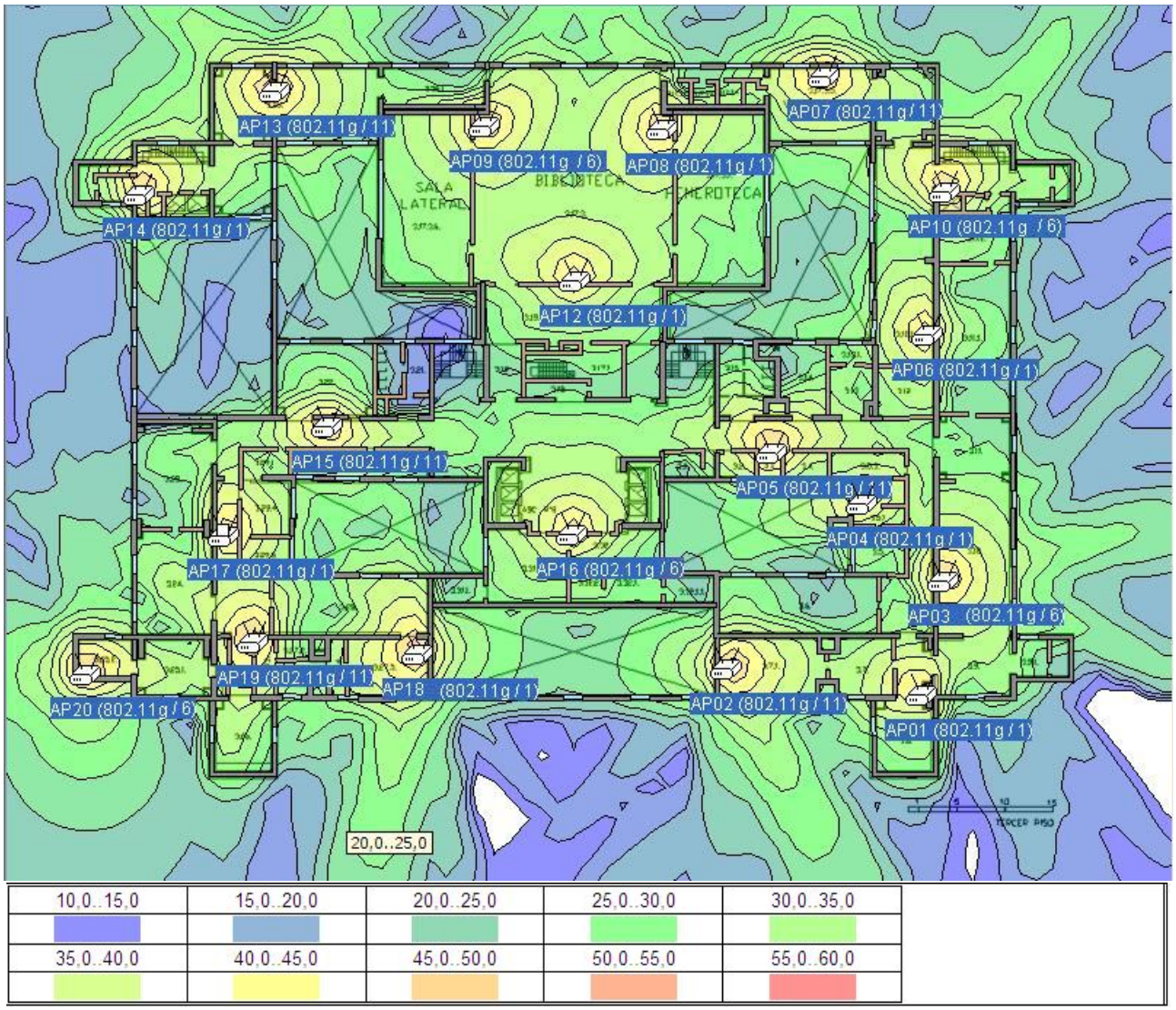


Figura 11.32: Relación señal ruido (dB)

Interferencia

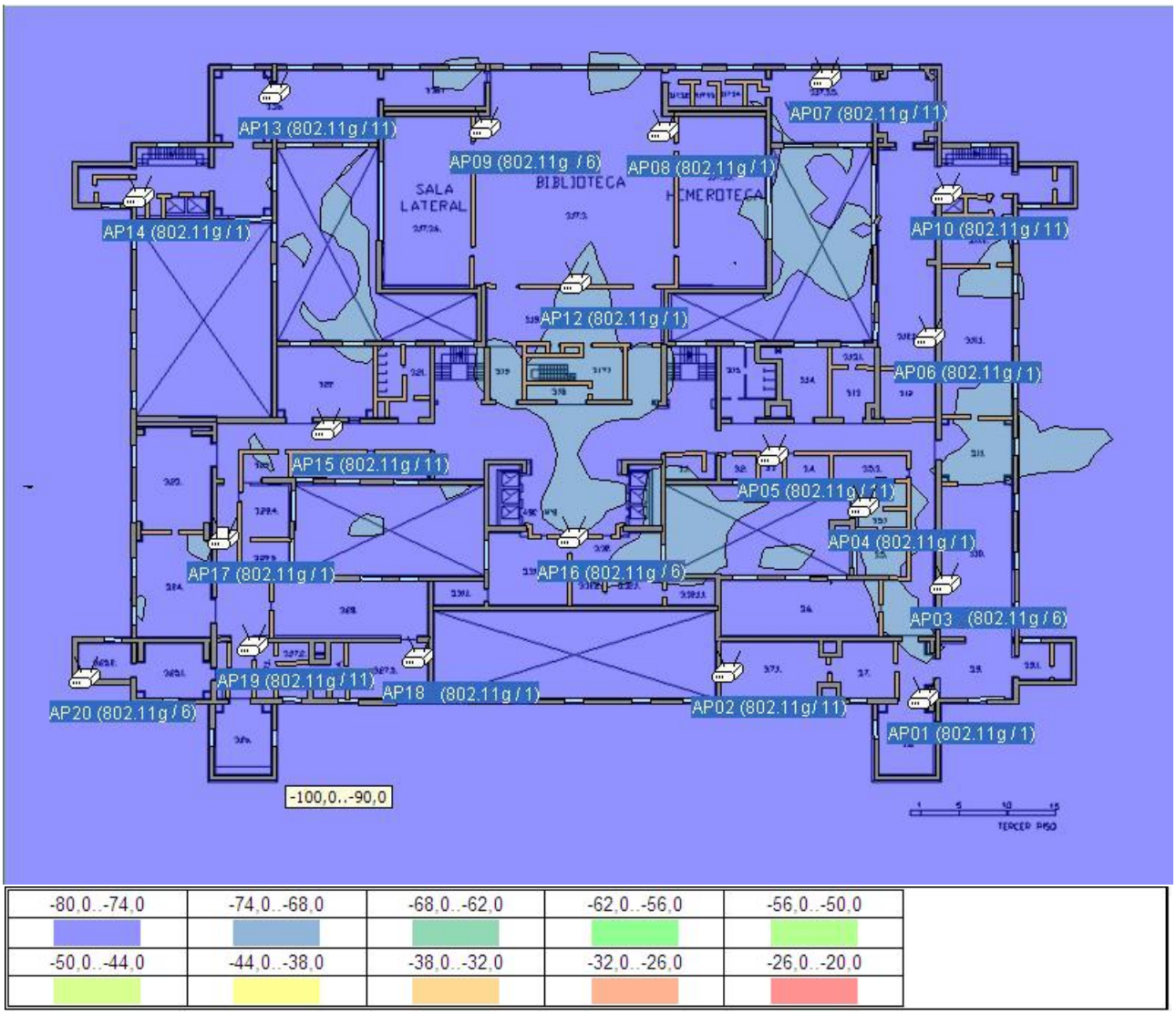


Figura 11.33: Interferencia (dBm)

Velocidad de datos

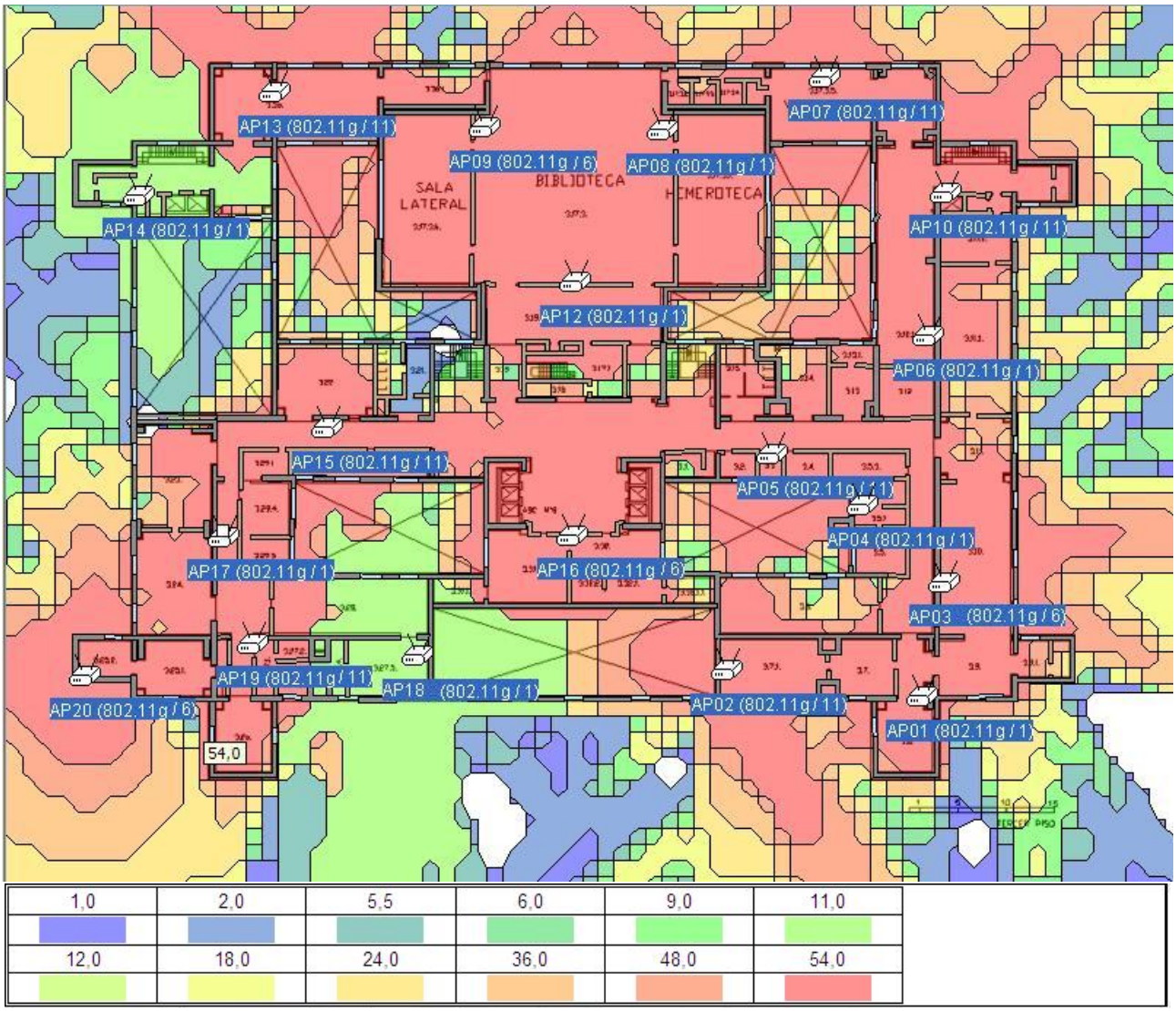


Figura 11.34: Velocidad de datos ($Mbps$)

Estado de RF

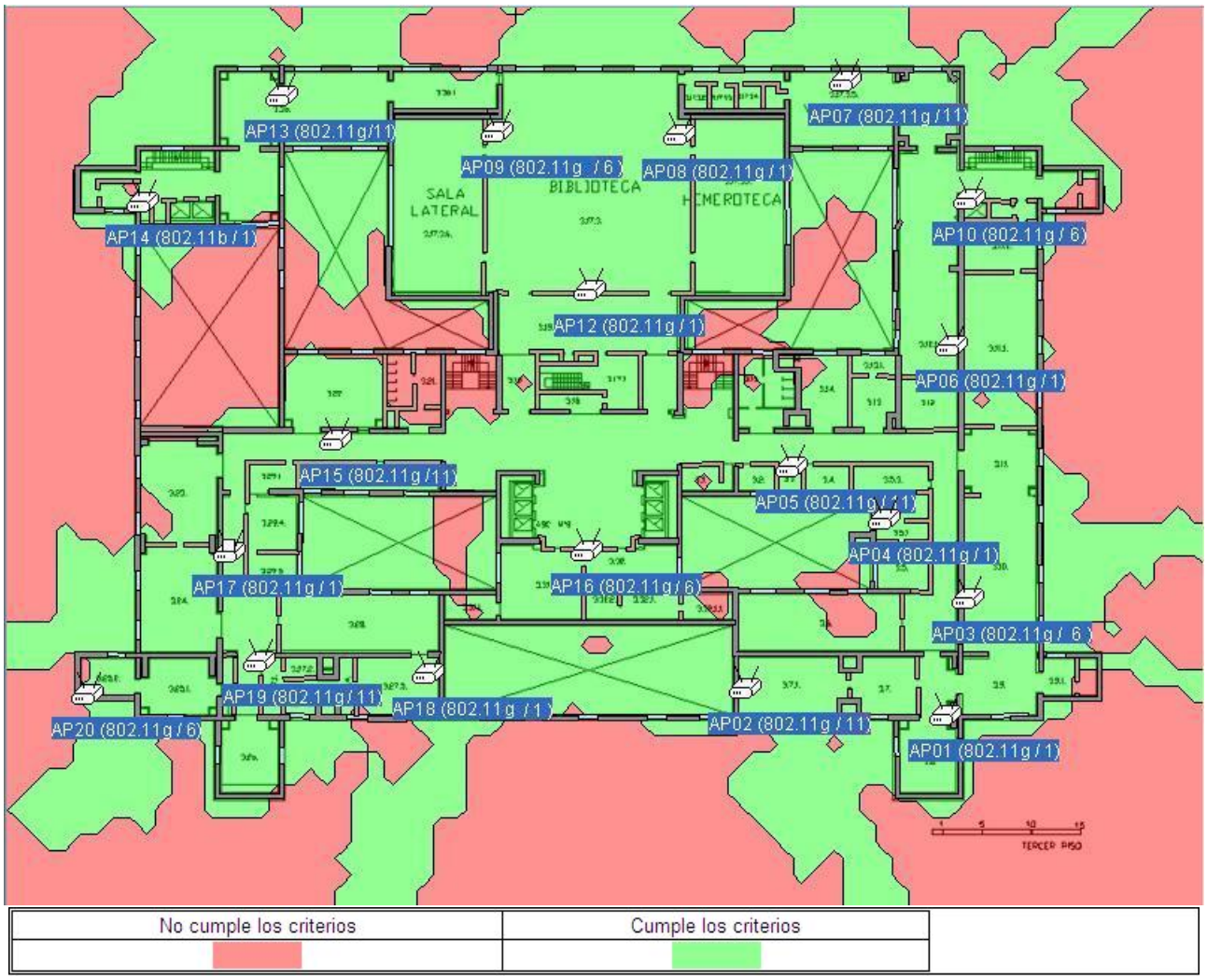


Figura 11.35: Estado RF

Motivo de fallo

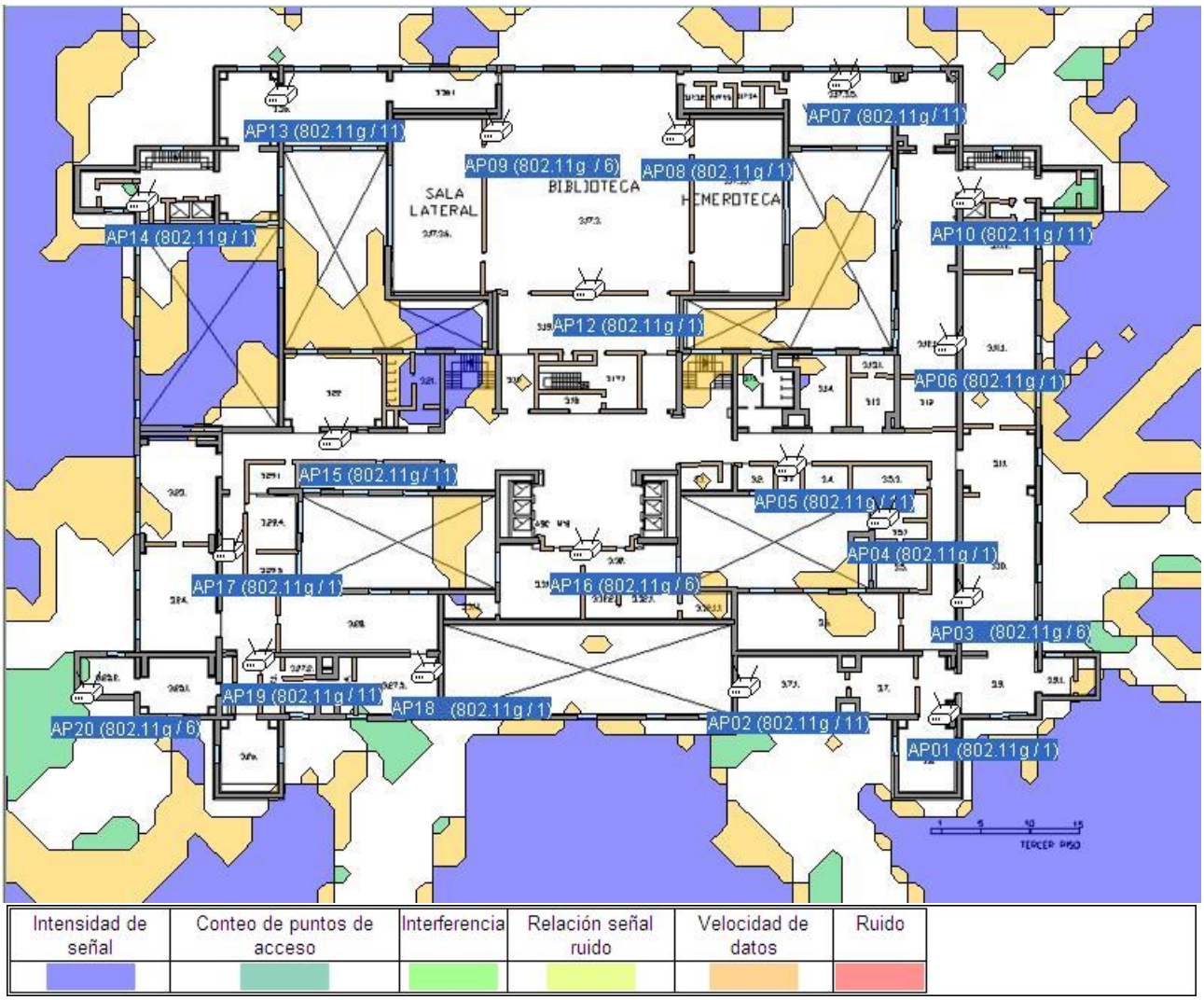


Figura 11.36: Motivo de fallo

11.2.7. Piso 4

Intensidad de señal

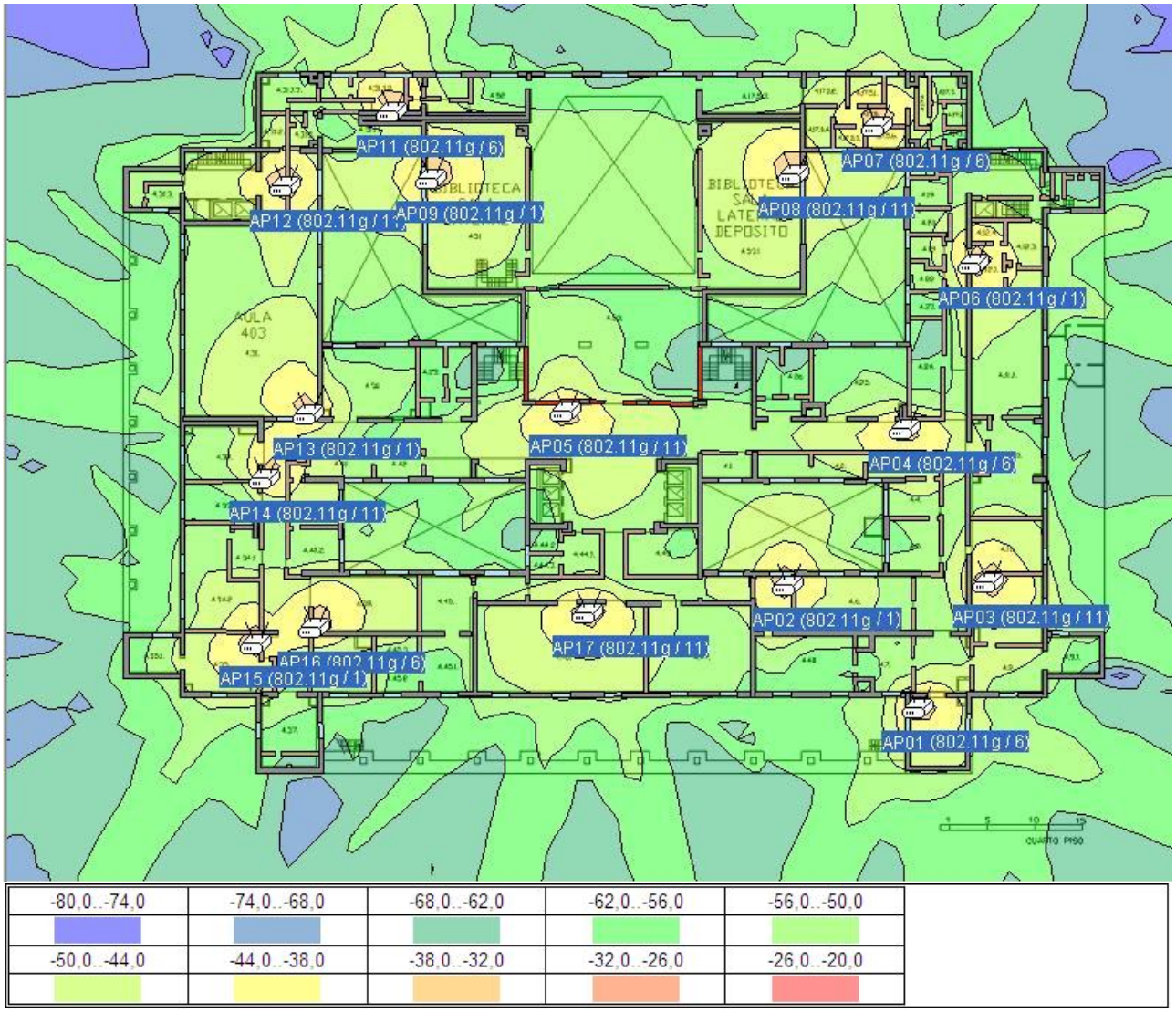


Figura 11.37: Intensidad de señal (dBm)

Relación señal ruido

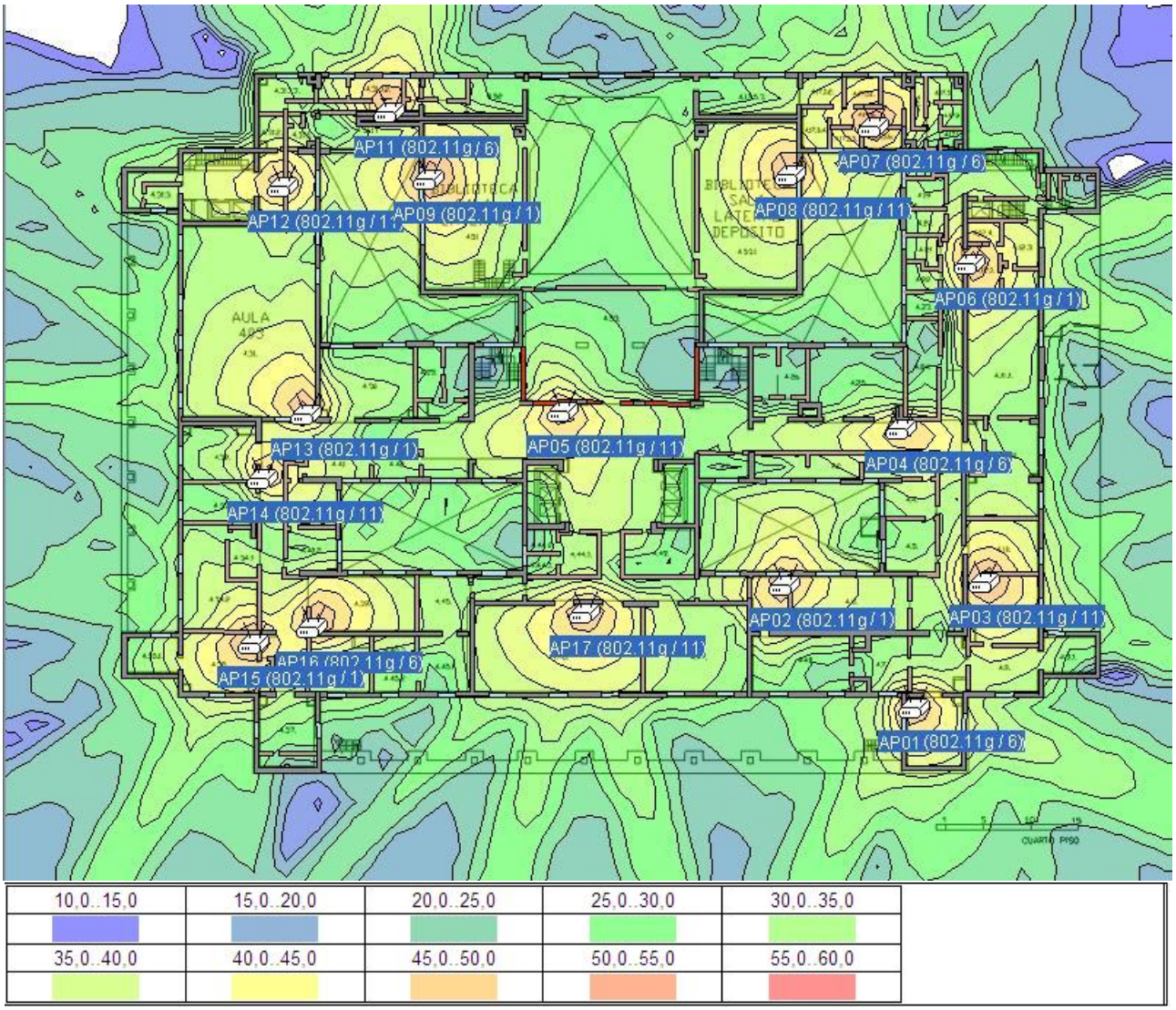
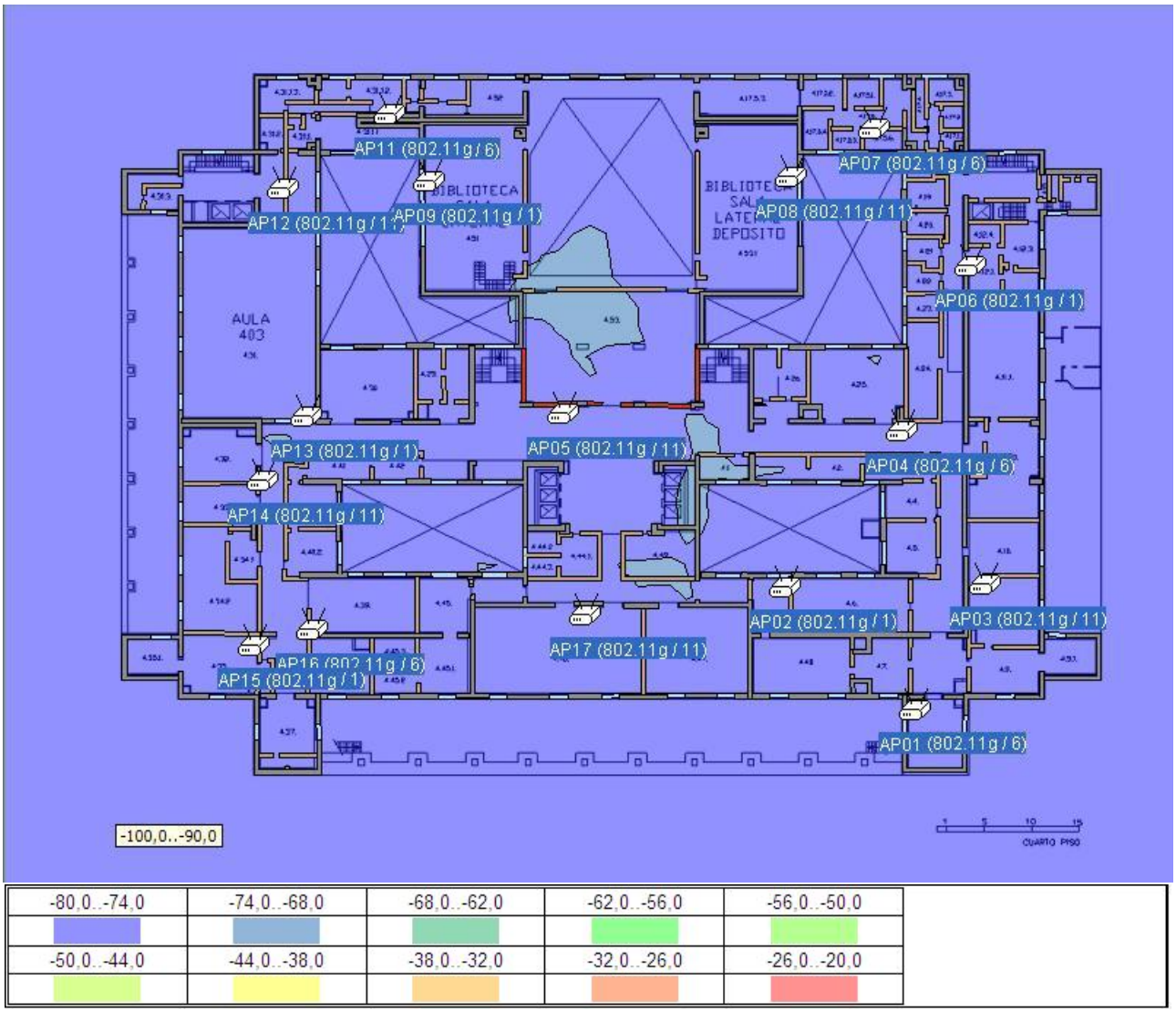


Figura 11.38: Relación señal ruido (dB)

Interferencia



-80,0..-74,0	-74,0..-68,0	-68,0..-62,0	-62,0..-56,0	-56,0..-50,0
-50,0..-44,0	-44,0..-38,0	-38,0..-32,0	-32,0..-26,0	-26,0..-20,0

Figura 11.39: Interferencia (dBm)

Velocidad de datos

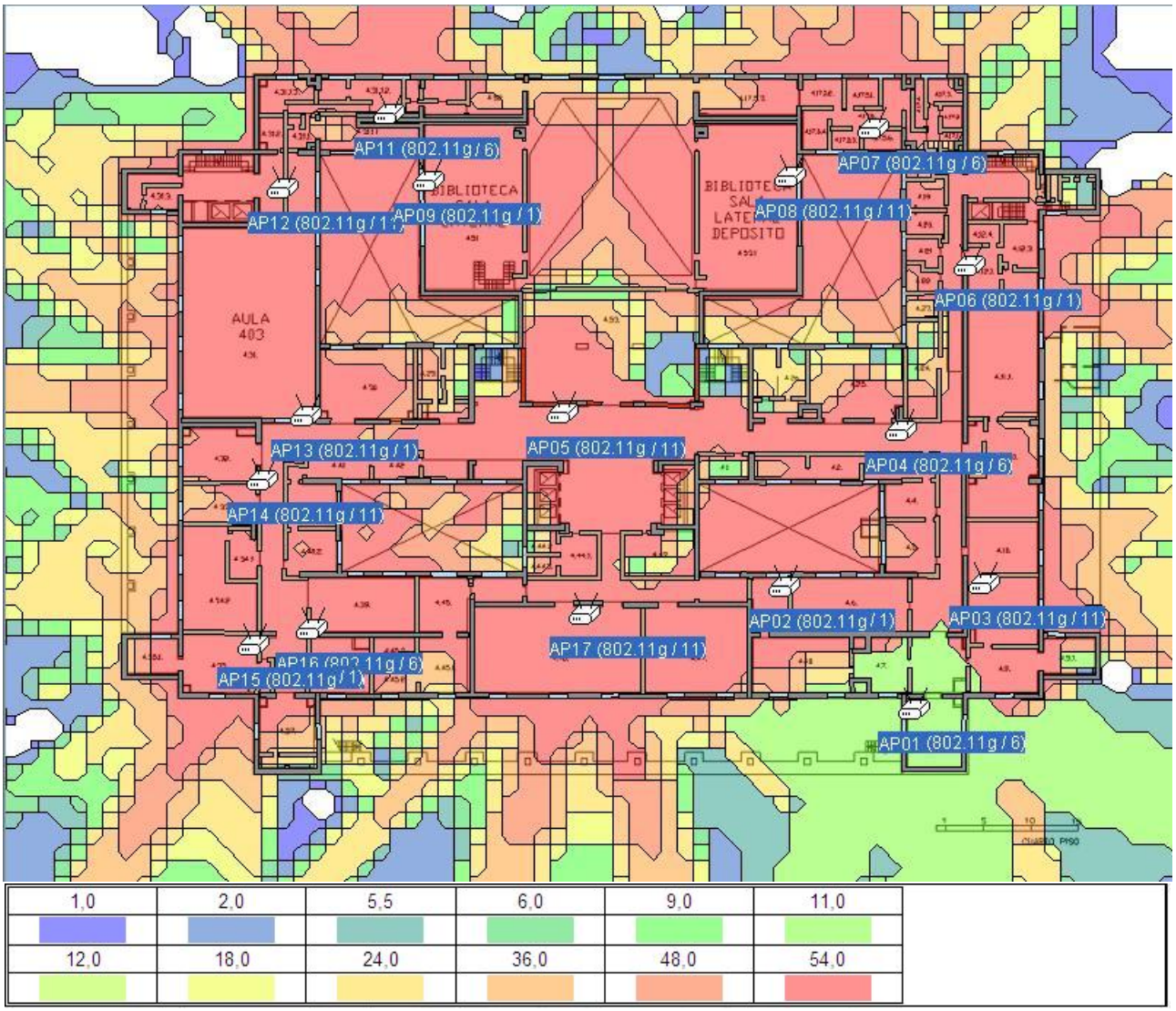


Figura 11.40: Velocidad de datos ($Mbps$)

Estado de RF

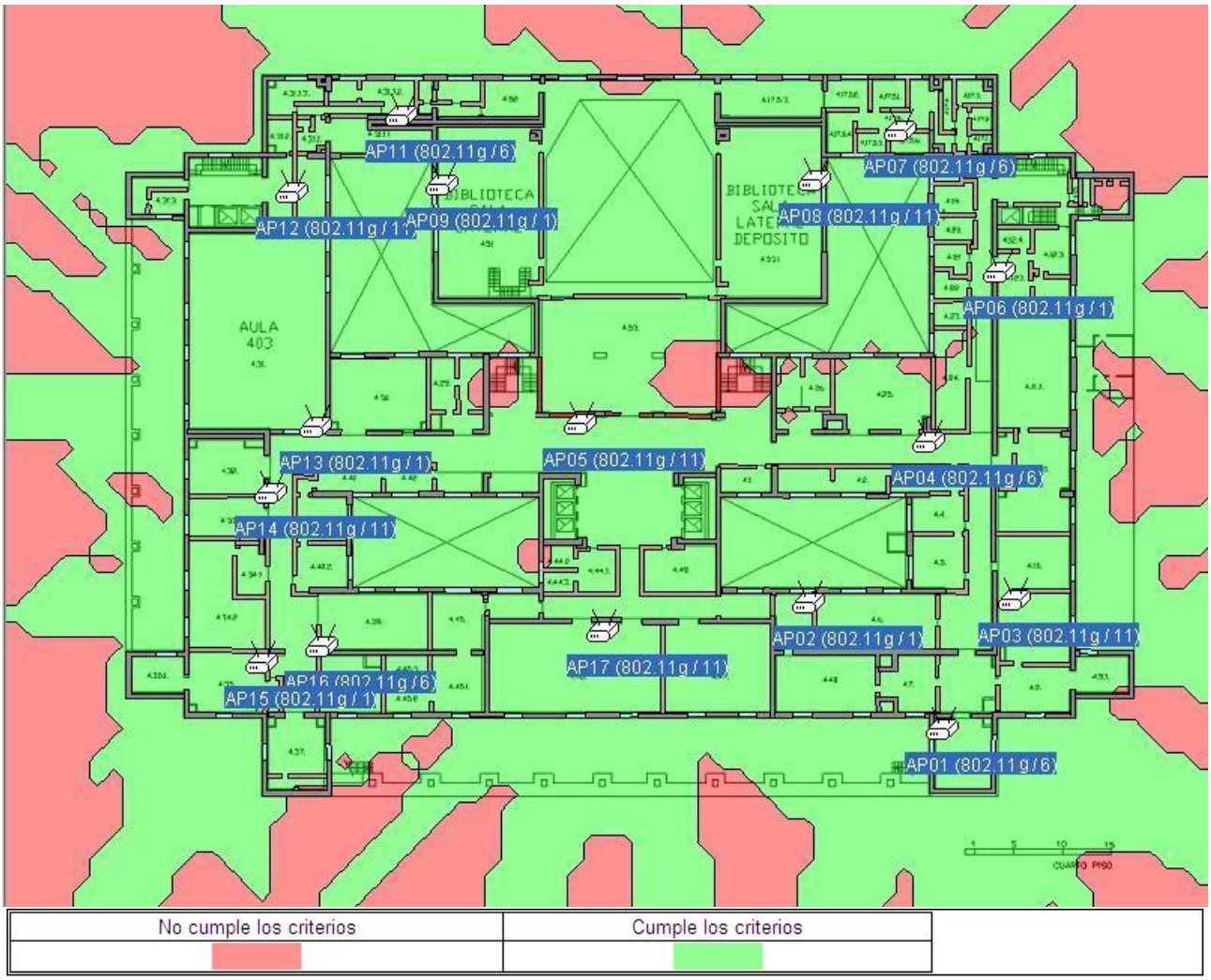


Figura 11.41: Estado RF

Motivo de fallo

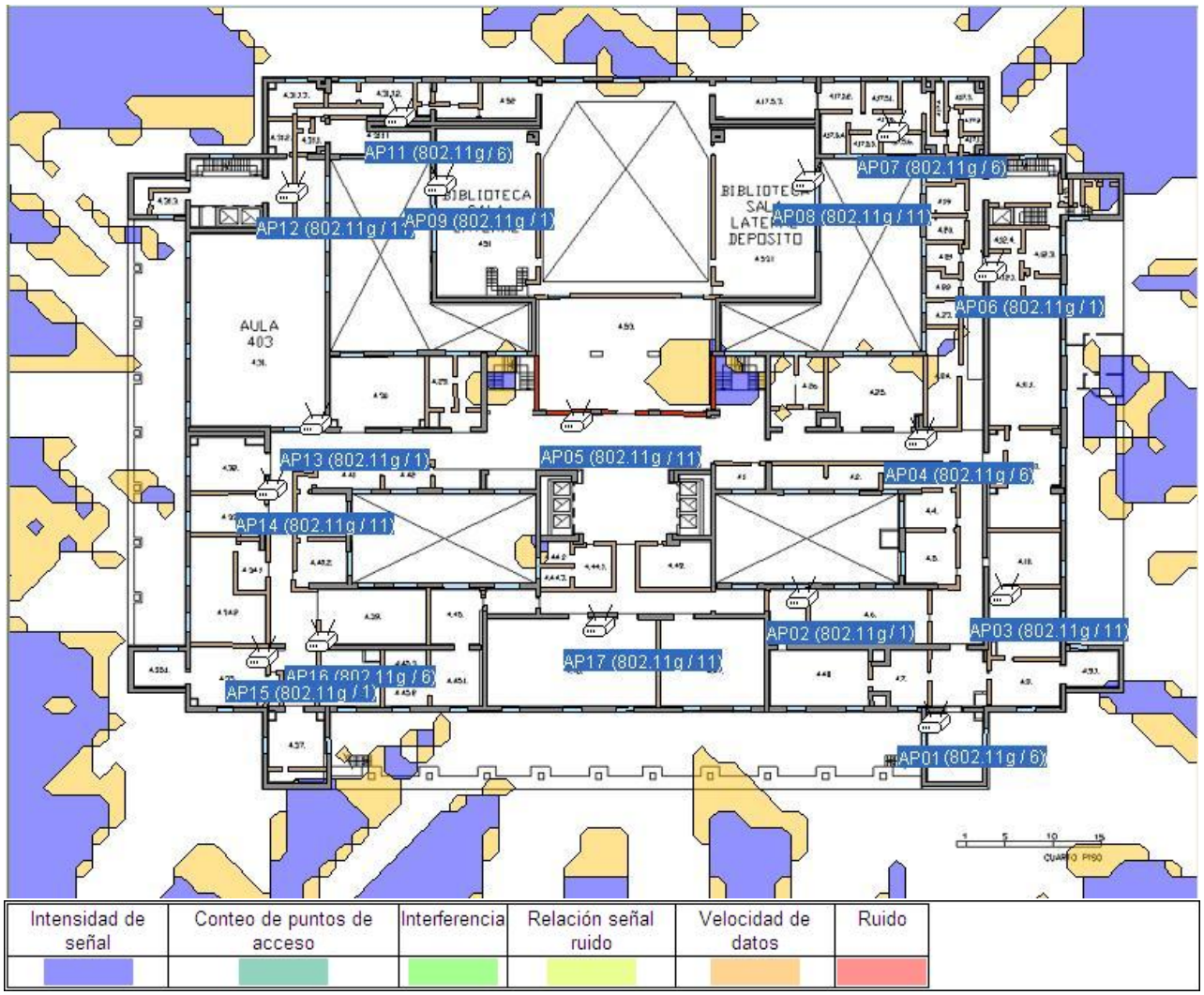


Figura 11.42: Motivo de fallo

11.2.8. Piso 5

Intensidad de señal

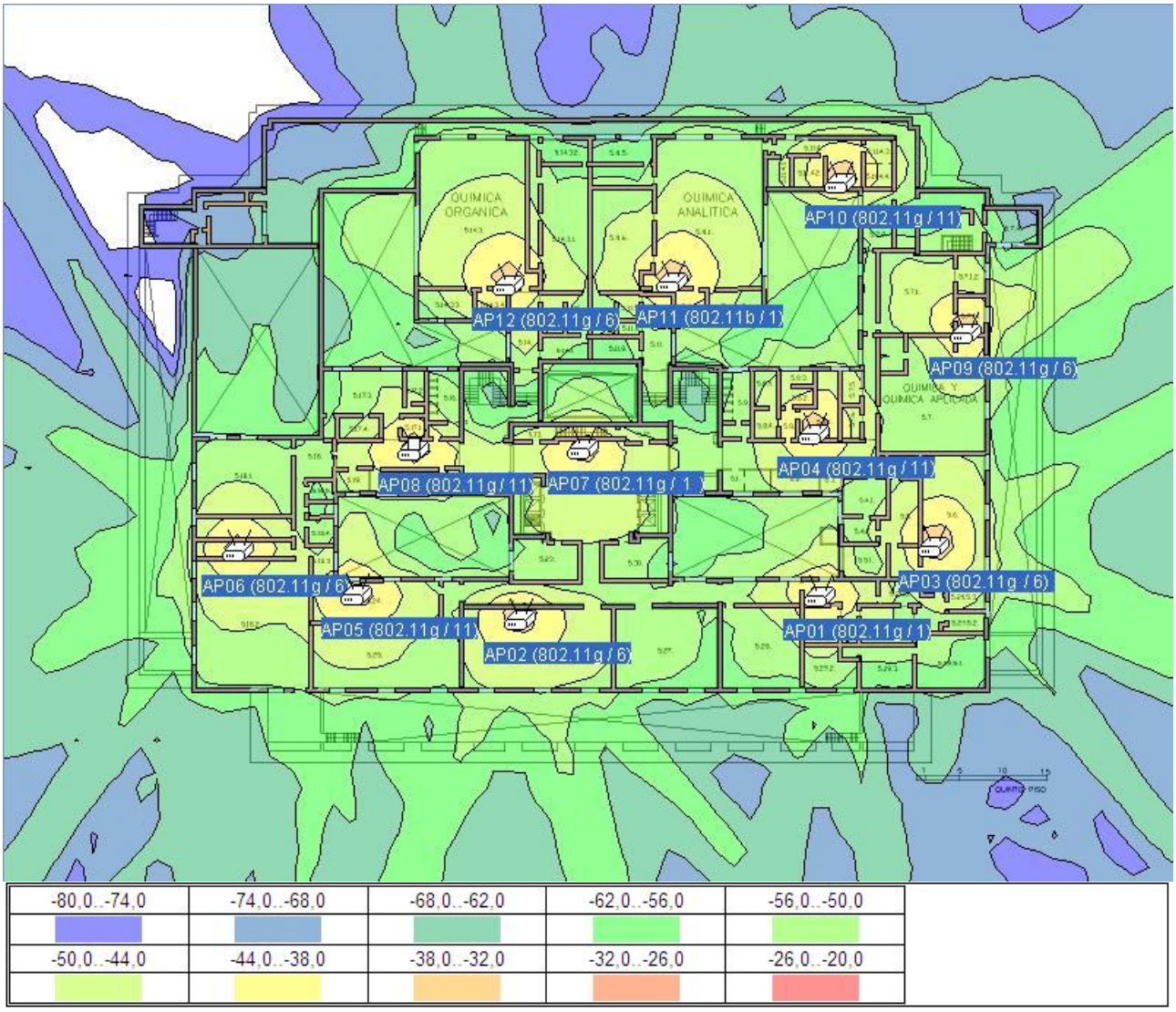


Figura 11.43: Intensidad de señal (dBm)

Relación señal ruido

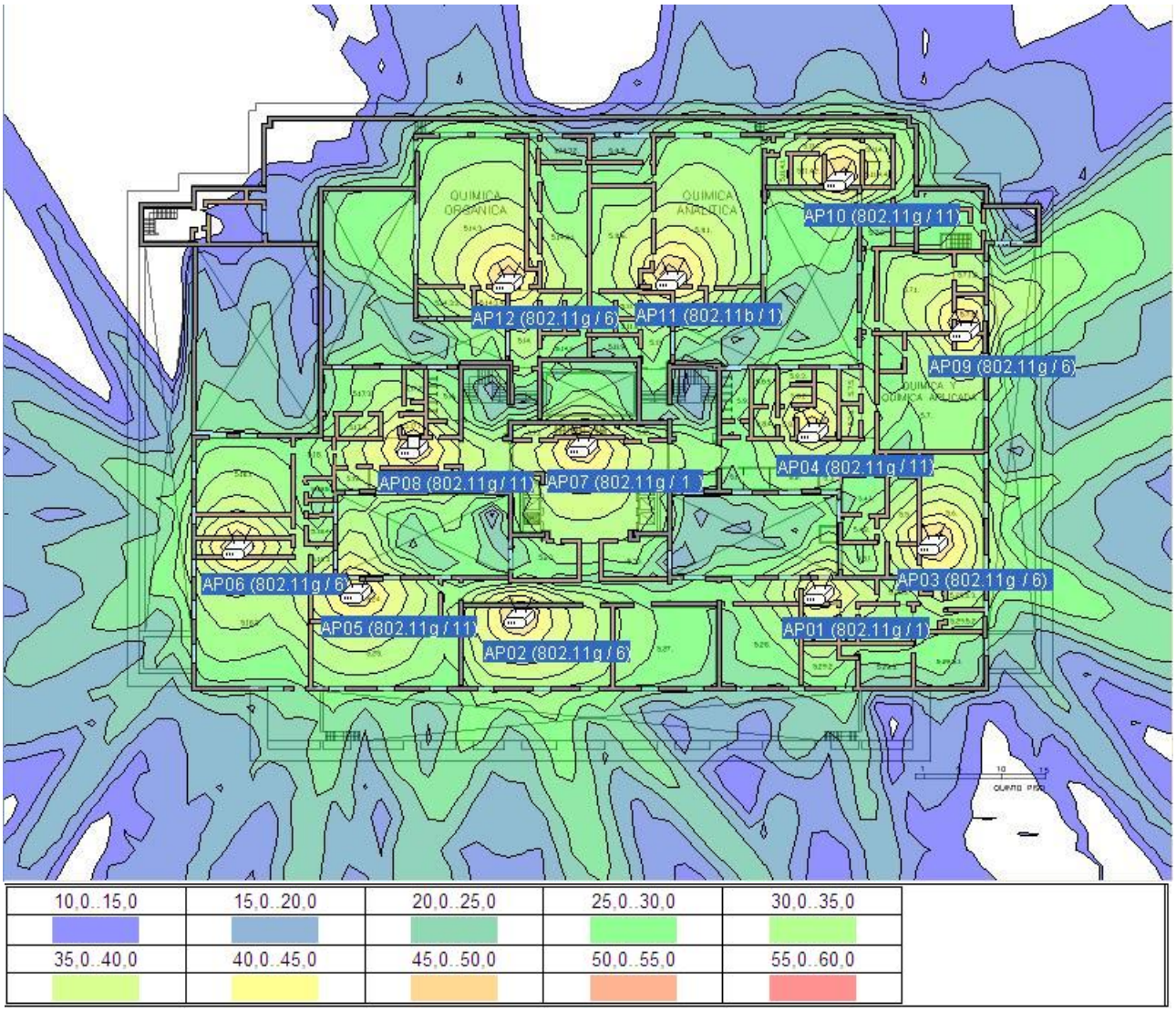


Figura 11.44: Relación señal ruido (dB)

Interferencia

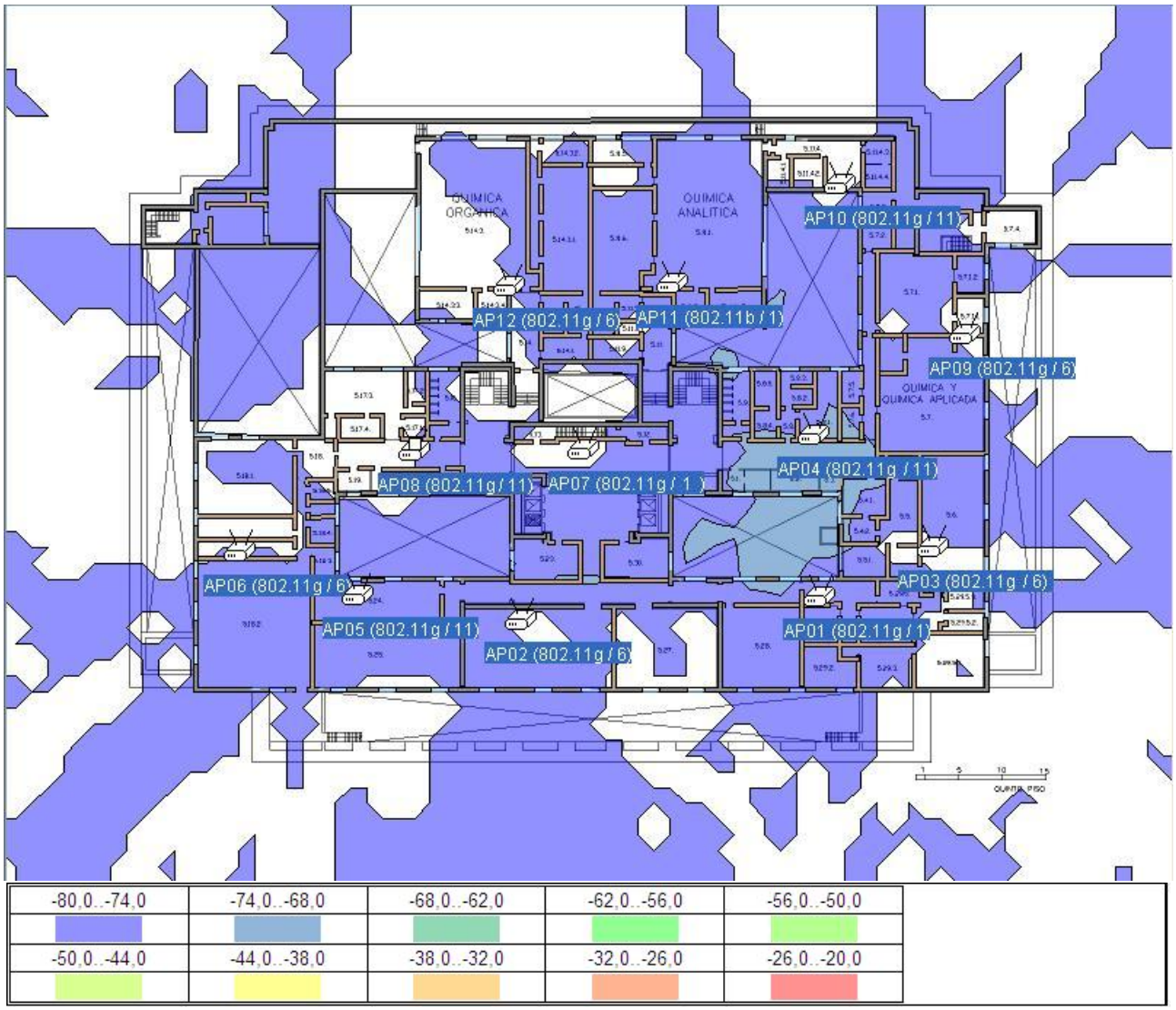


Figura 11.45: Interferencia (dBm)

Velocidad de datos

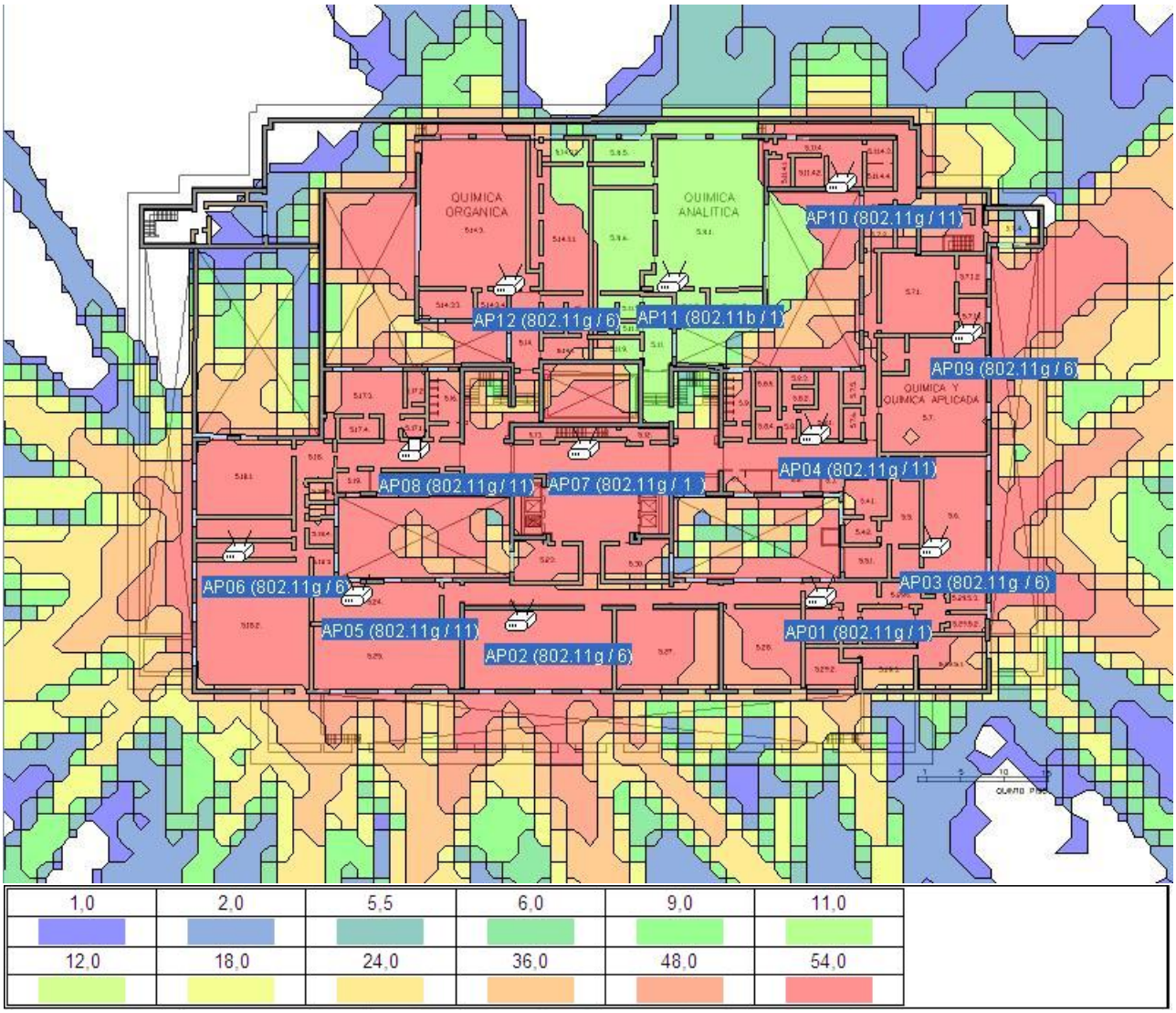


Figura 11.46: Velocidad de datos ($Mbps$)

Estado de RF

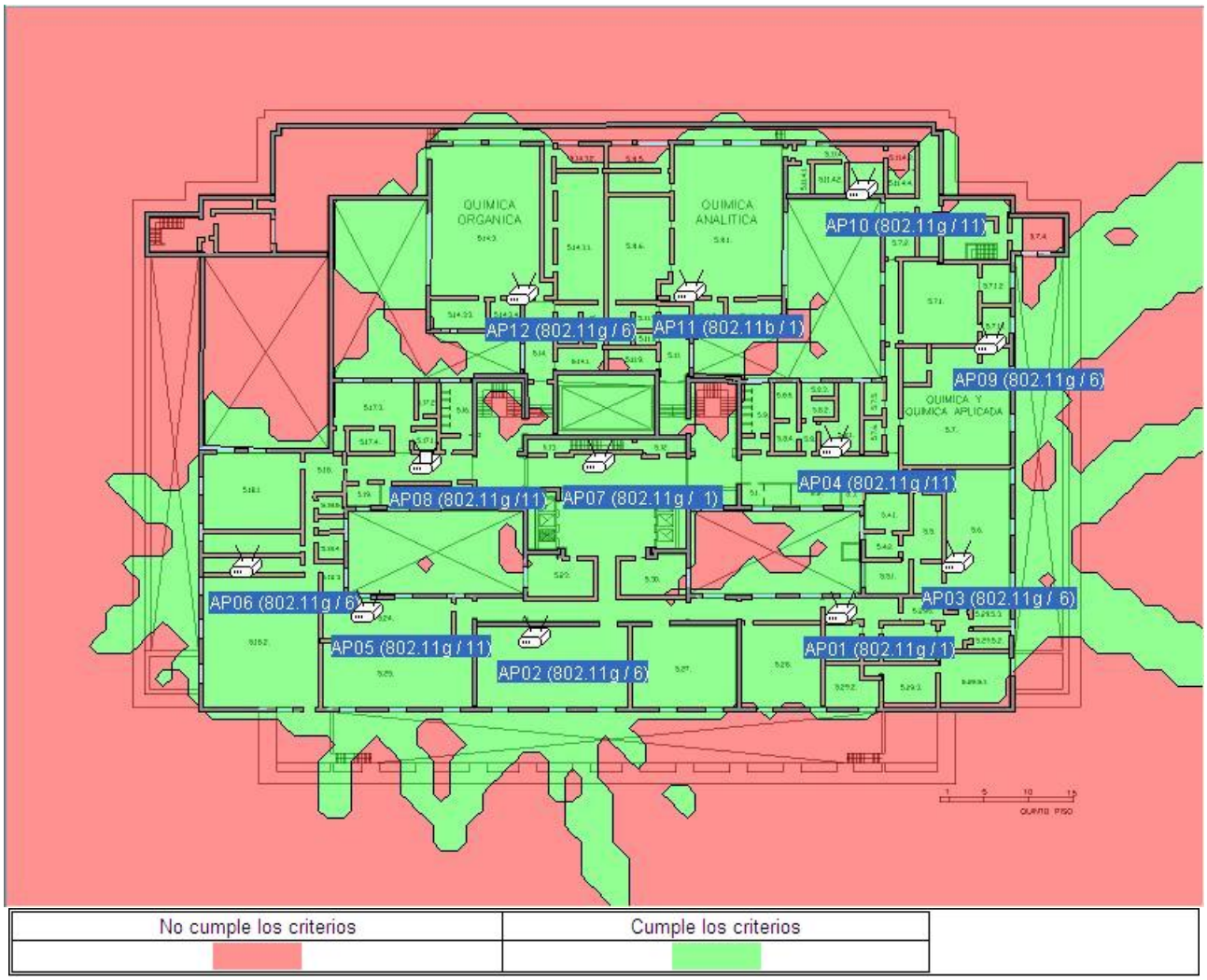


Figura 11.47: Estado RF

Motivo de fallo

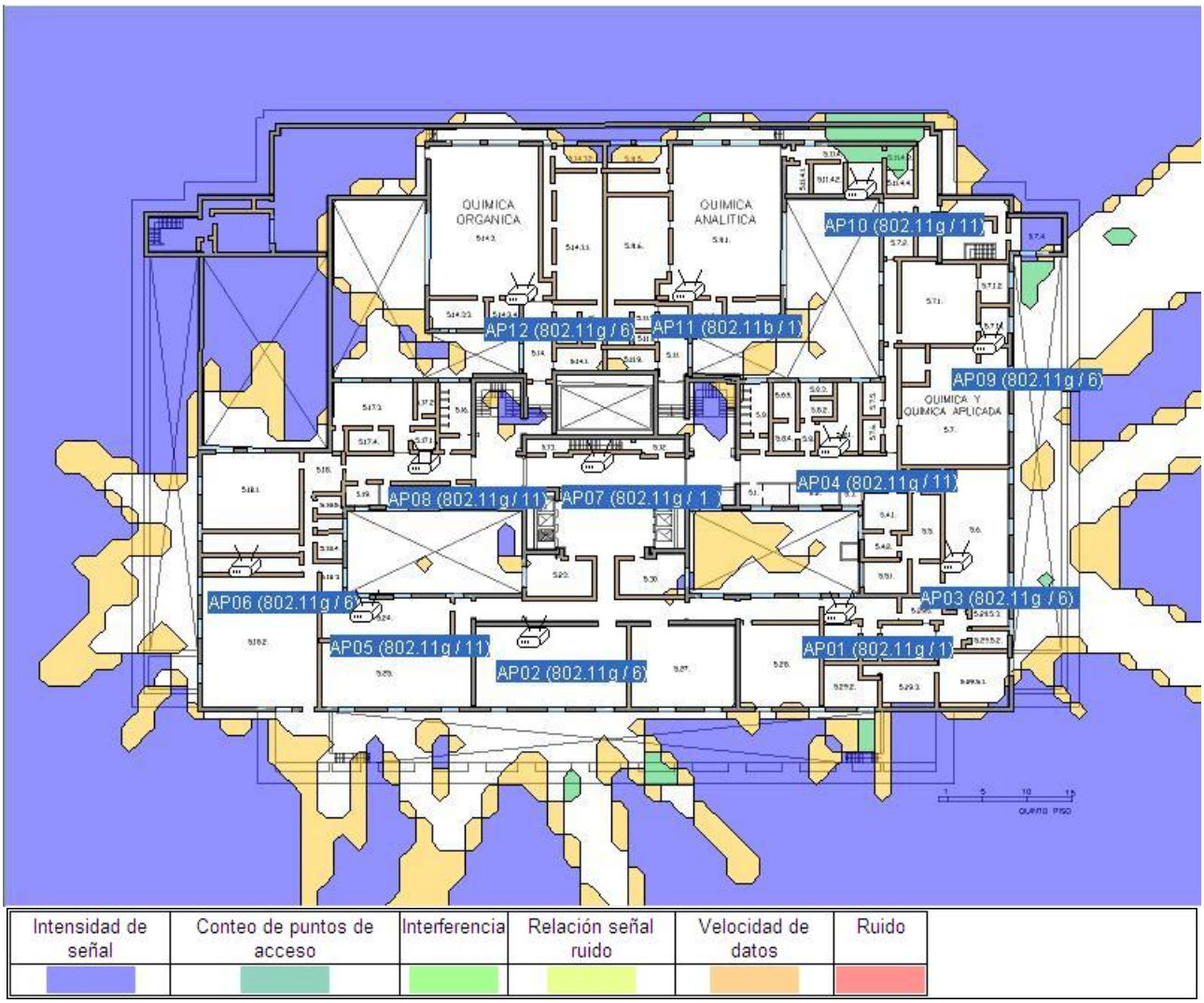


Figura 11.48: Motivo de fallo

Capítulo 12

Estudios de confiabilidad de hardware y de software

12.1. Introducción:

En la presente sección, se aplicarán métodos probabilísticos de falla, de uso común en productos electrónicos, para la estimación de la confiabilidad de la red propuesta. De esta forma, se contará con un modelo que indicará aproximadamente con que probabilidad y en que momentos la red estará fuera de servicio. De esta forma, además de observar cuan confiable será la red proyectada, en la sección siguiente se podrá proponer con los valores obtenidos un esquema de mantenibilidad de la red, y calcular la disponibilidad con la que funcionará la misma. Se comenzará con la breve explicación del modelo a utilizar, y se pasará inmediatamene a la aplicación del mismo a este caso particular, para la obtención de los parámetros de confiabilidad que el mismo nos proporciona.

12.1.1. Modelo de Confiabilidad:

Definamos primero el concepto de "tasa de fallas". Suponiendo que se está realizando un ensayo de confiabilidad, en el cual se tienen N_0 equipos funcionando a prueba, y que a lo largo del tiempo van quedando fuera de servicio por fallas. Llamamos tasa de fallas del equipo al siguiente valor:

$$\lambda(t) = \frac{dN_f}{N_s(t)dt} \tag{12.1}$$

Donde:

- $N_f(t)$: equipos que fallaron en el instante t.
- $N_s(t)$: equipos que todavía están en servicio en el instante t.

Además se cumple:

$$N_s(t) = N_0 - N_f(t) \tag{12.2}$$

Este valor nos indica la probabilidad de que un equipo cualquiera del grupo que se está ensayando falle, sabiendo que estamos en un instante mayor que t.

El comportamiento de cualquier tasa de fallas se puede generalizar a tres intervalos característicos. Uno al comienzo, llamado **"de fallas infantiles"**, que tiene en cuenta los posibles defectos de fabricación del producto. Uno intermedio o de **"fallas aleatorias"** que indica el comportamiento estocástico de las fallas en el equipo durante su vida útil. Y uno al final, llamado **"por degradación"** que manifiesta el incremento de fallas constante, mientras que los periodos restantes son crecientes a medida que nos alejamos del periodo de vida útil.

Para el presente proyecto, consideramos que el fabricante ha revisado ya la calidad del producto, y que nos encontramos todavía en el periodo de vida útil. Por esta razón consideramos de aquí en adelante un valor de tasa de fallas constante:

$$\lambda(t) = \lambda \tag{12.3}$$

Definamos ahora otro valor de utilidad: **la función de confiabilidad**:

$$R(t) = \frac{N_s(t)}{N_0} \tag{12.4}$$

En ella se nos está indicando la probabilidad de que el elemento dure un tiempo mayor a t. Para relacionarlo con la tasa de fallas, notemos que:

$$dN_s(t) = -N_s(t)\lambda dt \tag{12.5}$$

Dividiendo por N_0 y reacomodando la expresión, llegamos a que:

$$\frac{dR}{R(t)} = -\lambda dt \tag{12.6}$$

Integrando esta expresión, obtenemos finalmente que:

$$R(t) = e^{-\lambda t} \tag{12.7}$$

que nos da la función de confiabilidad para un equipo con tasa de fallas constante (dentro de su vida útil).

Veamos ahora lo que ocurre para un sistema como el nuestro, formado por varios equipos diferentes. Consideremos el caso para el cual la falla de uno solo de los componentes causa la falla total del sistema. Este caso se conoce como "configuración serie", ya que se asemeja a un circuito en serie, en el que la falla de un componente corta directamente el paso de la corriente. La probabilidad de que el sistema S falle en un instante mayor a t, es la siguiente:

$$R(t) = P(S) = P(S_1 \cap S_2 \cap ... \cap S_n) \tag{12.8}$$

donde los S_i, representan a los equipos individuales que se componen al sistema. Si estos equipos son estadísticamente independientes, se cumple entonces que:

$$R(t) = P(S) = P(S_1 - ... - S_n) = \prod_{i=1}^{n} P(S_i) = \prod_{i=1}^{n} R_i(t) \tag{12.9}$$

Si utilizamos ahora la expresión deducida anteriormente para $R(t)$, llegamos a que:

$$e^{-\lambda t} = \prod_{i=1}^{n} e^{-\lambda_i t} \tag{12.10}$$

Lo cual nos lleva a:

$$\lambda = \sum_{i=1}^{n} \lambda_i \tag{12.11}$$

es la tasa de fallas del sistema.

Definamos un valor, que se suele utilizar para expresar las características de confiabilidad de un componente. Se trata del "tiempo medio entre fallas".

$$MTTF = E(t) = \int_0^\infty t f(t) dt \tag{12.12}$$

que no es otra cosa que el tiempo medio que se espera que el componente dure sin fallar. Para calcularlo, notemos que la función de densidad de probabilidad se relaciona con la confiabilidad a través de la función de distribución de probabilidad $F(t)$, de la siguiente manera:

$$f(t) = \frac{dF}{dt} = -\frac{dR}{dt} \tag{12.13}$$

con lo cual nos queda que:

$$MTTF = -\int_0^\infty t dR = \lambda \int_0^\infty t e^{-\lambda t} dt = \frac{1}{\lambda} \tag{12.14}$$

Para el caso de los equipos formados por varios componentes reparables, se suele hablar de "Tiempo medio entre fallas"o $MTBF$[1], que en el período de vida útil es igual al $MTTF$ del equipo. Esta es la denominación que encontraremos en las hojas de datos de los equipos comúnmente.

12.1.2. Obtención del MTBF de la red inalámbrica:

Para el cálculo del MTBF en el caso del este proyecto, veamos de las expresiones anteriores, que indefectiblemente debemos contar con el valor de MTBF de cada uno de lo equipos que conforman la red, o que es lo mismo, la tasa de fallas de cada uno. Existen en general dos formas de calcular este parámetro para un equipo:

Estimación mediante una norma de confiabilidad de equipos:

En el primer caso, la técnica es poner una serie de equipos a funcionar e ir registrando los momentos en los que van apareciendo fallas. Se suelen aplicar técnicas de aceleramiento para realizar los ensayos en un tiempo razonable. En el segundo, se suele aplicar la norma MIL-HDBK-271, del departamento de defensa de los EE.UU. La misma permite la estimación de la

[1] Mean Time Between Failures

tasa de fallas de un equipo a partir de la detallada descripción de cada uno de sus componentes, y sus características funcionales. Otra norma reconocida que también se puede encontrar en equipos electrónicos es la Bellcore/Telcordia SR-332.

En nuestro caso, debemos indefectiblemente recurrir al fabricante del equipo, ya que la primera técnica de cálculo la realiza el mismo fabricante, y demanda obviamente una importante cantidad de recursos, mientras que para la segunda se requiere contar con los planos de los circuitos que conforman al mismo, lo cual es extremadamente difícil de conseguir ya que el fabricante no estará dispuesto a compartir con el público en general su costoso diseño. Es así que, en el mejor de los casos, el fabricante detalla un valor de MTBF en su hoja de datos, especificando de que manera obtuvo ese valor, y en que condiciones.

Lamentablemente, ninguno de los fabricantes de los equipos usados especifica valor alguno que hable sobre la confiabilidad de los equipos.

Ante la ausencia de información, el cálculo de confiabilidad de nuestro sistema se ve prácticamente imposibilitado. Sin embargo, se propone la realización de un cálculo de carácter estimativo, basado en los valores que otros fabricantes de equipos de similares características suministran. Este análisis es ciertamente cuestionable, pero se prefirió contar con esta aproximación en lugar a la ausencia total de datos.

Para la estimación del MTBF, se procedió a recolectar por la Web una cantidad de hojas de datos de equipos similares, que contengan este parámetro como información. Para el access point, se contó con los datos de AP-500, AP-600 y AP-1000 de Orinoco, junto con el PA A11 de Ericson. Los valores van de 100.000 horas a 150.000 horas, realizando un promedio de decidió por utilizar un valor de 125.000 horas para el Access Point. Para el switch se obtuvieron los datos del 3Com Superstack2 y PointScan 446. Los valores en este caso varían mucho, yendo de 50.000 a 700.000 horas. Un promedio nos da un valor de 235.000 horas. No se encontraron valores para el Media-Gateway pero se lo puede considerar un casi un switch, de hecho la línea 250, 350 y 450 de Avaya están construídos sobre la arquitectura de un switch, así que se usarán los mismo valores para él.

Equipo	**MTBF en horas**
Switches	375.000
Media-Gateway	375.000
Access Point	125.000

Cuadro 12.1: MTBF de los equipos utilizados.

12.1.3. Cálculo de la confiabilidad de la red:

Una vez que contamos con los valores del fabricante, ya podemos aplicar el modelo detallado al principio. Según el mismo, podemos calcular al tiempo medio entre fallas del sistema como:

$$MTBF = \frac{1}{\sum\limits_{equipos} \frac{1}{MTBF_i}} = \frac{1}{\sum\limits_{Switches} \frac{1}{MTBF_i} + \sum\limits_{Gateway} \frac{1}{MTBF_i} + \sum\limits_{AP} \frac{1}{MTBF_i}} \tag{12.15}$$

y utilizando los valores anteriores, llegamos a la siguiente expresión. Vale hacer la aclaración de que se está tomando la falla de un solo access point como una falla catastrófica o sea, que

la falla de un solo Access Point se considera una falla "de la totalidad "del sistema, esto es discutible y tiene que ver con la forma en la que uno quiera interpretar el problema, otra forma de verlo podría ser que el hecho de que falle un Access Point *por cada piso* sea una falla catastrófica, eso dividiría el numero de access points totales que se usaría en la siguiente fórmula por la cantidad de pisos, aumentando mucho el MTBF total. Nosotros hemos optado por poner el número total de Access Points y considerar la sola falla de uno de ellos como una falla crítica. Otro detalle es que al tener los switches y el Media-Gateway la misma MTBF el MG puede considerarse un switch más en la suma. El aporte que ofrece el Media-Gateway en este caso, al cálculo del MTBF total del sistema es mínimo, y sin embargo la sola falla de él implica dejar sin teléfonos IP a todo el sistema. Esto es también algo para tener en cuenta. Si bien ahora estamos calculando un MTBF general de "todo el sistema", se debería presentar los resultados de confiabilidad de este equipo solamente.

$$MTBF = \frac{1}{\sum_{equipos} \frac{1}{MTBF_i}} = \frac{1}{\frac{143}{MTBF} + \frac{22}{MTBF}} \tag{12.16}$$

Por lo que el valor total de $MTBF$ es de 1794 horas.

Usando también las expresiones antes descriptas, podemos calcular la función de confiabilidad del sistema como:

$$R(t) = e^{\frac{1}{MTBF}t} \tag{12.17}$$

12.1.4. Conclusión:

Llegamos entonces a una estimación de la confiabilidad de la red inalámbrica aplicando el modelo propuesto al principio. El valor de $MTBF$ al que arribamos, que es de $1794h$, es por cierto muy bajo. Esto se debe a la gran cantidad de componentes con relativamente alta tasa de fallas con la que se forma la red. En la próxima sección, deberemos plantear una estrategia de mantenibilidad eficiente, para lograr que estos bajos niveles de confiabilidad no incidan demasiado en la disponibilidad de la red.

12.2. Mantenibilidad de la red inalámbrica:

En esta parte del proyecto se propondrá una estrategia de mantenibilidad de la red inalámbrica adecuada a las necesidades de la facultad. Aplicando un modelo probabilístico, se calculará un parámetro de interés que indicará el tiempo medio de reparación de cualquier equipamiento que conforma la red, que pase a estado de mantenimiento. Finalmente, utilizando este parámetro y los calculados en la sección anterior para la confiabilidad del sistema, se procederá a estimar la disponibilidad con la que se podrá contar con los servicios de red no cableada.

Debido a que la red está conformada íntegramente por equipo electrónico, que responde exclusivamente a fallas de tipo aleatorio, se propone una estrategia de mantenimiento correctivo. Este tipo de mantenimiento incluye las tareas no programadas que son consecuencia de una falla en el sistema. El ciclo de mantenimiento incluirá:

- Identificación de la falla.
- Localización del equipamiento en falla.
- Desconexión y remoción.
- Envío a servicio técnico para reemplazo o reparación.
- Reinstalación del equipo.
- Verificación del funcionamiento.

Detallaremos a continuación las características particulares de cada uno de estos pasos:

Identificación de la falla: La detección principal de la falla será por quejas y reclamos de cualquier tipo de usuario de la red inalámbrica, ya sea alumno, profesor o empleado de la facultad. Ante la falta total de servicio en una celda, se identificará como falla de celda. Si la falla cubre varios PA conectados con el mismo switch, se identificará como falla de cluster. Para problemas más sutiles, como bajas velocidades o variación de cobertura, se podrá proceder a un pequeño recorrido por la zona afectada y la posterior comparación de los mapas de cobertura con los archivos de los ensayos iniciales cuando la red fue puesta en servicio. En caso de detectarse de esta forma problemas de hardware, se catalogará como falla de celda y se procederá en forma similar al caso anterior.

Localización del equipamiento en falla: En caso de falla de celda, se revisará el LED indicador de Port Ethernet del AP, para verificar la conexión. Si la conexión es correcta, se diagnosticará falla de PA. De no haber conexión de datos o de alimentación se verificará el link entre el AP. De estar el cable correctamente enchufado y en buen estado, se verificará el puerto del switch, para diagnosticar una falla en él. En caso de falla de cluster, se verificará inicialmente el LED de alimentación del switch. En caso de no estar presente se verificará tensión de la fuente, en caso de no funcionar correctamente, se diagnosticará una falla en la fuente de del switch.En caso de funcionar correctamente, verificará el link hacia el back-bone y en caso de estar correcto, se diagnosticará una falla en el switch.

Desconexión y remoción: Este punto implicará la desconexión del o los cables de datos y/o alimentación, y la extracción del equipo. En la mayoría de los casos esto será extremadamente fácil, ya que los racks y estantes son de fácil acceso y los conectores son todos normalizados y de inmediata conexión y desconexión. En algunos casos particulares, se deberá utilizar una escalera apoyada sobre la pared para acceder al equipo que se encuentra próximo al cielorraso.

Envío a servicio técnico para reemplazo o reparación: Se enviará el equipamiento de mal funcionamiento al soporte de la red inalámbrica. Este soporte sera creado según lo disponga el encargado de estos asuntos en la facultad, y podrá ser realizado sin problema por el actual soporte informático previamente capacitado en el tema. Se prevé el estudio de los equipos por personal del laboratorio abierto de electrónica (LABI) o por el mismo soporte técnico para observar el funcionamiento de los equipos a nivel de los componentes y determinar cuales son las partes que pudieran ser reparadas, la forma de

hacerlo, las herramientas necesarias, y cuando es necesario consultar directamente con el servicio técnico especializado del equipo en cuestión.

Reinstalación del equipo: Este punto implicará la reconexión del o los cables de datos y/o alimentación, y la puesta en marcha del equipo. Las características de accesibilidad, obviamente, son idénticas a las de la extracción de equipo. De ser necesario una reconfiguración, será realizada por el soporte técnico, quien seguirá nuevamente las instrucciones de la instalación y configuración.

Verificación del funcionamiento: La verificación se realizará siguiendo las mismas pautas utilizadas en los ensayos realizados a la red completa en el momento que se instaló la red, pero restringidos al área afectada por la falla detectada y reparada. De no pasar la prueba, se deberá volver a aplicar el procedimiento de mantenibilidad a las zonas que no estén funcionando correctamente.

12.2.1. Modelo de mantenibilidad:

En forma bastante similar a lo realizado en el punto anterior, delinearemos en este caso un modelo probabilístico aplicable a la mantenibilidad. Definamos entonces la función de mantenibilidad:

$$M(t) = \frac{N_{(t)}}{N_0} \tag{12.18}$$

donde:

- $N_{(t)}$: número de equipos reparados en el tiempo t.
- $N_0(t)$: número de equipos ingresados al servicio técnico.

No es muy difícil visualizar que la función de mantenibilidad no es otra cosa que la probabilidad de que un equipo esté reparado con un tiempo t de demora. Si definimos ahora la función de densidad y mantenibilidad como:

$$m(t) = \frac{dM}{dt} \tag{12.19}$$

podemos entonces definir un valor similar al MTBF pero con respecto al mantenimiento, calcularemos en este caso un parámetro llamado "tiempo medio de reparación" (MTR) que nos indicará el valor medio que lleva la reparación de un equipo cualquiera de la red que presenta una falla y es entregado al servicio técnico. El mismo se puede calcular como:

$$MTR = E(t) = \int_0^\infty tm(t)dt \tag{12.20}$$

En nuestro caso, por tratarse de un sistema conformado por varios equipos, el MTR puede ser calculado adecuadamente partiendo de los valores discretos de cada equipo, de la siguiente manera:

$$MTR = \sum m_i P_i \tag{12.21}$$

donde P_i es la probabilidad de que el equipo que halla fallado sea el i y el m_i es el tiempo medio que se tardará en repararlo. Con este último punto surge un pequeño problema; si contamos con un equipo de reemplazo, el tiempo de mantenimiento será muy bajo, causado simplemente por la extracción y reinstalación del equipo. Sin embargo, para los casos en que más de un equipo del mismo deje de funcionar al mismo tiempo, debemos tener en cuenta tiempos de reparación mas extensos, en los que habrá que seguir con todo el proceso de reparación propiamente dicho, por el soporte técnico. Cada equipo presentará entonces no solo su propio tiempo medio de reemplazo, sino también su tiempo medio de reparación propiamente dicho (sin reemplazo inmediato disponible). Nuestra expresión quedará entonces:

$$MTR = \sum m_i P_i + m_{SR_i} P_{SR_i} \tag{12.22}$$

Notemos que estamos considerando el caso de que no falten técnicos para reparar todos los equipos que van llegando, ya que el valor de tiempo de reparación no se modifica para los casos de múltiple falla. Esto no es una mala suposición, debido a que el soporte informático es numeroso, y no se esperan una mayor cantidad de equipos en reparación que técnicos disponibles. Calculamos ahora cada parámetro. La probabilidad de que falle solo un equipo del mismo tipo lo podemos calcular simplemente por:

$$P_i = \frac{n_i \lambda_i}{k} \tag{12.23}$$

recordemos que λ es la tasa de fallas de cada equipo. La constante k es el factor de proporcionalidad que lo obtenemos como:

$$k = \sum_{i=1} n_i \lambda_i \tag{12.24}$$

Para el caso de la probabilidad de que dos o más equipos del mismo tipo fallen en simultáneo (incluimos en este caso la falla mientras uno de los equipos estaba siendo reparado), vemos que:

$$P_{SR_i} = P\{\text{Fallan 2 equipos} \cup \text{Fallan 3 equipos} \cup ... \cup \text{Fallan} n_i \text{equipos}\} \tag{12.25}$$

donde n_i es la cantidad total de equipos de tipo i. Esta última expresión se puede desarrollar como:

$$\begin{aligned} P_{SR_i} &= P\{\text{Fallan 2 equipos}\} + P\{\text{Fallan 3 equipos}\} + ... + P\{\text{Fallan} n_i \text{equipos}\} \\ P_{SR_i} &= P_i P_i + P_i P_i P_i + ... + P_i^{n_i} \end{aligned} \tag{12.26}$$

Ahora estamos en condiciones de aplicar el modelo a nuestro caso particular y calcular el parámetro TMR deseado.

12.2.2. Tiempo medio de reparación:

El cálculo de MTR surge simplemente de aplicar el modelo propuesto anteriormente. Para ello, necesitamos previamente estimar los valores de tiempo medio de reparación para cada equipo. Siguiendo los lineamientos de la estrategia de mantenibilidad de cada uno de los componentes de la red inalámbrica, incluyendo todos los pasos necesarios, se estiman los siguientes valores para el tiempo de mantenimiento, incluyendo el caso de contar con el equipo de repuesto inmediato, o en caso de tener que repararlo directamente:

Equipo	m_i	m_{SRi}
Access Points	15 Min	1 Días
Switches	30 Min	0,5 Días
Gateway	30 Min	0,5 Días

Cuadro 12.2: Tiempos de reposición con con y sin repuestos disponibles .

Ahora ya podemos aplicar el modelo probabilístico de mantenibilidad propuesto, utilizando los valores estimados de tasa de falla λ y los valores de tiempos en el cuadro anterior. En la siguiente cuadro se resumen los valores utilizados, junto con los resultados obtenidos. Los valores temporales están expresados en horas.

i	n_i	λ_i	P_i	P_{SRi}	m_i	m_{SRi}	m_iP_i	$m_{SRi}P_{SRi}$
Access Point	143	1/125000	0.950	1.95	0.25	24	0.240	46,8
Switch	21	1/375000	0.046	0.002	0.5	12	0.023	0.024
Mediagateway	1	1/375000	0.0022	0	0.5	12	0.001	0

Cuadro 12.3: Especificaciones de los switches

Usando para estos cálculos un $K = 1{,}2026\ 10^{-3}$, llegamos entonces a la estimación del tiempo medio de reparación (MTR) de **47,1 horas o 1,96 días**

12.3. Disponibilidad de la red inalámbrica:

Definimos a la confiabilidad $A(t)$ de un sistema como la probabilidad de encontrar al sistema funcionando en un instante cualquiera t. Si el instante t se encuentra suficientemente alejado del instante en que hubo que realizar una reparación o se hizo su puesta en funcionamiento, la disponibilidad es independiente de t, y define lo que se conoce como disponibilidad a largo plazo:

$$\lim_{t\to\infty} A(t) \tag{12.27}$$

Considerando un período de tiempo extenso dado, en el que se realizan n reparaciones, vemos que el factor de utilización del sistema puede expresarse como:

$$T_f = \frac{T_f}{T_f + T_r} \tag{12.28}$$

donde:

T_f : Es el tiempo en el que el equipo estuvo funcionando.

T_r : Es el tiempo en el que el equipo estuvo fuera de servicio.

Dividamos ahora por n, tanto al dividendo como al divisor.

$$T_f = \frac{\frac{T_f}{n}}{\frac{T_f+T_r}{n}} \tag{12.29}$$

este valor tiende a D cuando n tiende a infinito, ya que estamos considerando el caso de toda la vida útil del sistema. Tomando entonces el límite para al expresión anterior, llegamos a la conclusión que:

$$D = \lim_{t\to\infty} F = \lim_{t\to\infty} T_f = \frac{\frac{T_f}{n}}{\frac{T_f+T_r}{n}} = \frac{MTBF}{MTBF + MTR} \tag{12.30}$$

es decir que podremos calcular la disponibilidad a largo plazo simplemente utilizando los valores del tiempo medio entre fallas y el tiempo medio de reparación respectivamente. Aplicando la expresión anterior llegamos a la conclusión de que:

Disponibilidad:	**97.44 %**

Cuadro 12.4: Disponibilidad

Es decir que la red inalámbrica propuesta, aplicando la estrategia de mantenibilidad propuesta, presenta una disponibilidad del **97.44 %**.

12.3.1. Conclusión:

Finalmente hemos descripto detalladamente los pasos a seguir para efectuar un mantenimiento eficaz de la red inalámbrica. El valor de disponibilidad obtenido es ciertamente bajo. Recordemos, sin embargo, que este cálculo se trata solamente de una estimación ya que no se contaron con los valores exactos de $MTBF$ de los equipos. Además los valores de TMR fueron también estimados según el criterio de los autores de este proyecto. Igualmente, este factor no es totalmente crítico para nuestro caso, ya que no se trata de un servicio tal como una línea de producción, una estación de radiodifusión prestando un servicio contratado, etc. donde las pérdidas ocasionadas por falta de servicio muchas veces son importantes, irrecuperables y muchas veces inaceptables.

Recordemos además que la confiabilidad fue calculada con un modelo de falla catastrófica serie, con lo cual cualquier falla es considerada una falla del sistema. En nuestro caso, este modelo es demasiado exigente, de ahí los valores bajos de $MTBF$ y D. Dicho de otra forma, en caso de una avería puede ser que cierto AP cubra igualmente el sector con menos potencia y velocidad de transmisión, o bien es posible reubicar temporariamente la notebook con PC Card en otro sitio cercano para encontrar servicio.

Capítulo 13

Evaluación Económica del Proyecto

En este punto se procederá a la identificación, medición y valoración de costos y beneficios del proyecto. Al no existir incertidumbre respecto a la selección de alternativas, se realizara la evaluación para la alternativa seleccionada.

Los costos de los proyectos de informática son relativamente simples de cuantificar no así los beneficios que se presentan como ahorro de costos con respecto a la situación base, siendo particularmente compleja la estimación de las horas hombre liberadas. Por otra parte este tipo de proyectos tiene costos y beneficios intangibles u ocultos los cuales se deberán describir en forma cualitativa.

13.1. Análisis del "Costo - Beneficio"

Cada vez que los aparatos productivos desean introducir un nuevo producto o servicio al mercado, las ciencias económicas presentan una gran batería de métodos muy precisos de evaluación económica de proyectos. Pero en el momento en que se empieza a hablar de proyectos sociales y/o educativos, surgen complicaciones para determinar los costos reales de implementación, especialmente los que se refieren a los costos indirectos, y aún más complicado es poder determinar, de una manera razonable y aproximada, los beneficios y utilidades del proyecto.

El análisis "Costo-Beneficio" permite analizar los desembolsos o gastos desde el punto de vista de maximizar los beneficios con respecto al costo para la comunidad para obtener los rendimientos financieros mas altos. El criterio difiere de la evaluación de una inversión privada, como el valor actual neto, el valor anual equivalente, o el flujo de efectivo descontado, en que intenta cuantificar los costos y beneficios sociales, beneficios tangibles e intangibles que no solo ocurren para el propietario del proyecto sino también para la comunidad como un todo.

13.1.1. Costos

En el Cuadro 13.1 se puede observar el detalle del "Flujo de Inversiones"[1].

[1]Todos los valores indicados están expresados en dólares estadounidenses, con una relación de cambio de U$S 1 = $ 3,8.

Tipo	Detalle	Costo Unitario	Mes 1		Mes 2		Mes 3		Mes 4		Mes 5		Mes 6		
			Cantidad	Costo	Cantidad	Costo	Cantidad	Costo	Cantidad	Costo	Cantidad	Costo	Cantidad	Costo	
IS	AP Aruba AP-61 Single Radio	320	39	12.480	27	8.640	48	15.360	28	8.960	0	0	0	0	
	AC Aruba 3600	12.240	1	12.240	0	0	0	0	0	0	0	0	0	0	
	Edge Switch Cisco SRW-2016	371	4	1.484	4	1.484	4	1.484	4	1.484	1	371	0	0	
	Media Gateway Avaya G450 y Server Avaya S8300	4.720	0	0	0	0	0	0	0	0	1	4.720	0	0	
	Firewall HP Proliant ML150 G5	725	0	0	0	0	0	0	0	0	2	1.450	0	0	
	Sistore MX NVS	3.836	0	0	1	3.836	1	3.836	1	3.836	0	0	0	0	
ES	Placa PCMCIA Encore ENPWI-G2 54Mbps Cardbus II	24	0	0	0	0	0	0	0	0	0	0	0	0	
	D-link 802.11g Wireless LAN USB Adapter	16	100	1.580	100	1.580	100	1.580	100	1.580	100	1.580	0	0	
	Placa de Red Wi-Fi D-link PCI 54Mbps Wireless	26	100	2.575	100	2.575	100	2.575	100	2.575	100	2.575	0	0	
	Teléfono IP Wireless Avaya 3641	202	0	0	0	0	0	0	0	0	0	0	300	60.720	
	Cámara IP DLINK DCS-3420	295	40	11.800	40	11.800	40	11.800	40	11.800	0	0	0	0	
BOM	Cable UTP Cat5e Int Furukawa Bobina 305m	54	3	162	3	162	3	162	3	162	0	0	0	0	Costo Total del Proyecto
	Bandeja Portacable Perforada 0,7 50x50mm X 3mts	13	275	3.575	275	3.575	275	3.575	275	3.575	0	0	0	0	
	Bandeja Portacable Curva Plana 90º 50x50mm	4	90	378	90	378	90	378	90	378	0	0	0	0	
MO	Mano de Obra según Planeamiento y Programación			3.715		3.715		3.715		3.715		4.380		1.265	
	Costo Mensual Total			**49.989**		**37.745**		**44.465**		**38.065**		**15.076**		**61.985**	**247.325**

Figura 13.1: Flujo de Inversiones (U$S)

Los cotos de la MO[2], el equipamiento y materiales de construcción indicado en el cuadro anterior, están basados en las tareas realizadas mensualmente obtenidas de la planificación y la programación del proyecto detallada en Sección 7.3, buscándose una distribución del flujo de inversiones constante, de forma tal de lograr que la inversión sea gradual.

13.1.2. Beneficios

En el Cuadro 13.2 se pueden observar los beneficios tangibles e intangibles calculados en un ciclo de vida de 5 años[3].

[2]Mano de Obra.

[3]El ciclo de vida se basa en valor adoptado por las empresas de telecomunicaciones en la práctica.

Tipo	Detalle	Ahorro					
		Año 1	Año 2	Año 3	Año 4	Año 5	
Tangibles	Mantenimiento de infraestructura de telefonía separada	30.316	30.316	30.316	30.316	30.316	
	Personal de seguridad	20.211	20.211	20.211	20.211	20.211	
	Operadora telefónica	6.063	6.063	6.063	6.063	6.063	
	Venta equipos viejos	2.772	0	0	0	0	
	Incremento de usuarios de internet	1.016	1.016	1.016	1.016	1.016	
	Incremento líneas telefónicas	633	633	633	633	633	
Intangibles	Mejora de la educación						
	Mejora estética edilicia						
	Mejora notable de telefonía						
	Aumento de la eficiencia de servicio de internet						
	Aumento en la velocidad de adquisición del un servicio						
	Aumento de seguridad						
	Incremento de la moral del personal debido a las nuevas herramientas de apoyo a la educación, investigación y los proyectos						
	Total Ahorro Anual	**61.010**	**58.238**	**58.238**	**58.238**	**58.238**	**Ahorro Total en el Ciclo de Vida** 293.963

Figura 13.2: Beneficios (U$S)

En el cuadro anterior, se puede observar que en los beneficios tangibles se indica el flujo de ahorro. Esta cuantificación se basa en las siguientes suposiciones:

Mantenimiento de infraestructura de telefonía separada: Debido a la integración del servicio de telefonía a la red de datos, se ahorra en tareas de mantenimiento de la red telefónica. Por lo tanto, se supone un ahorro de personal de mantenimiento de 5 técnicos con $12 (U$S 3,15) de honorarios por hora a un régimen de 8 horas de trabajo diaria.

Personal de seguridad: Debido a la integración de las nuevas herramientas de monitoreo y seguridad a la red de datos, se ahorra en personal seguridad. Por lo tanto, se supone

un ahorro de 4 personas de seguridad con \$10 (U\$S 2,63) de honorarios por hora a un régimen de 8 horas de trabajo diaria.

Operadora telefónica: Debido a la integración del servicio de telefonía a la red de datos, se ahorra el personal encargado de realizar la derivación a los internos de la facultad. Por lo tanto, se supone el ahorro de 2 personas con \$6 (U\$S 1,58) de honorarios por hora a un régimen de 8 horas de trabajo diaria.

Venta equipos viejos: Se supone una ganancia adicional de la venta de equipos que no se reutilizan por no cumplir con los requerimientos técnicos (switches Cisco 2924 y 3Com 4226) suponiendo que les resta una vida útil del %60.

Incremento de usuarios de internet: Se estima un ahorro en acceso cableado para cada nueva computadora suponiendo un incremento anual de usuarios del 10 %. Los costos del cableado se estiman basándose en que se debe cablear $10m$ promedio para conectar un nuevo usuario. El incremento anual del 10 % de usuarios se basa en que, según una nota del diario Clarín del 04/02/07, el 13 % de los inscriptos en la UBA eligen carreras de Ingeniería y teniendo en cuenta que existe una deserción del 60 % en el CBC resulta un incremento del 7,8 % anual. Para cubrir el peor caso se adopta para el calculo un 10 % de crecimiento de computadoras.

Incremento líneas telefónicas: Se estima un ahorro en acceso cableado para cada nuevo teléfono suponiendo un incremento anual de usuarios del 7,5 %. Los costos del cableado se estiman basándose en que se debe cablear $20m$ promedio para conectar un nuevo teléfono, mientras que el crecimiento anual se basa en utilizar la capacidad planificada en la Sección 9.5.1.

13.1.3. Flujo de Caja Descontada

El flujo de caja se calcula como diferencia entre los flujos de egresos y los de ingresos al final del ciclo de vida. Es necesario diferenciar entre el resultado contable y el resultado económico. En este último es necesario considerar el costo del capital, medido por la tasa de interés, lo que lleva al flujo de caja descontado.

$$FCD_i = \frac{FC_i}{(1+t_i)^i} = \frac{I_i - E_i}{(1+t_i)^i} \tag{13.1}$$

donde t_i es la tasa de interés, es el costo del capital previsto para el periodo i. Este valor dará un valor equivalente al valor del capital al inicio del proyecto de no haber depreciación o inflación. Si p_i es la tasa de inflación prevista para el periodo i, entonces deberá considerarse la siguiente modificación en la Ecuación 13.1:

$$FCD_i = \frac{I_i - E_i}{(1+t_i)^i(1+p_i)^i} \tag{13.2}$$

Para hallar el beneficio al final del ciclo de vida simplemente se contabilizan los flujos de caja descontados de cada periodo refiriéndolos al momento inicial de la siguiente forma:

$$VAN = B_n = E_0 + \sum_{i=1}^{N} FCD_i \tag{13.3}$$

Siendo E_0 la inversión inicial requerida para comenzar el proyecto, la cual será por tanto negativa. El beneficio del proyecto también es llamado VAN[4].

Al ser este un caso particular de proyecto, es decir no existen flujo de ingresos dado que es un proyecto social/educativo, el cálculo del FCD se realiza empleando el flujo de ahorro expuesto en el Cuadro 13.2, descontándose los costos y beneficios a la misma tasa de interés. De esta forma se puede observar los valores y el gráfico del FCD:

Años	***FCD (ti=1,3 %)***
0	0
0,5	-247.325
1,5	-187.098
2,5	-130.345
3,5	-74.320
4,5	-19.014
5,5	35.582
6,5	89.477

Cuadro 13.1: Flujo de Caja Descontada

[4]Valor Actual Neto

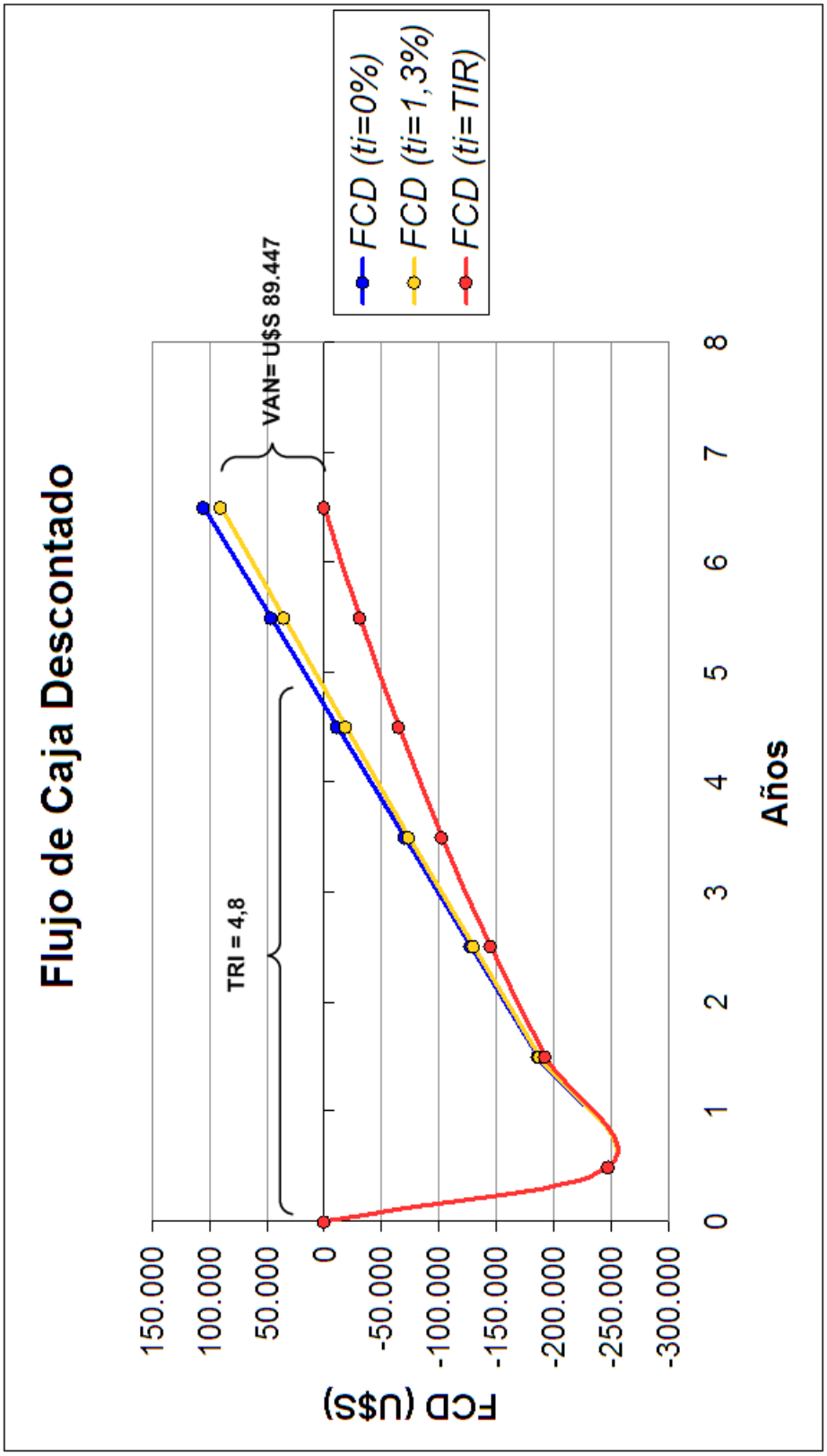


Figura 13.3: Flujo de Caja Descontada

Para el cálculo se utiliza la mayor tasa nominal anual en dólares estadounidenses, que es la que brinda el Banco de la Provincia de Buenos Aires, siendo la misma del 1,3 %. Adicionalmente, como el cálculo se realiza en dólares estadounidenses se supuso que la inflación es despreciable.

Del Cuadro 13.1 se puede obtener el VAN, obteniendo el mismo un valor:

VAN	U$S 89.477

Cuadro 13.2: VAN

13.1.4. TIR

Todo proyecto lleva implícito diversos riesgos. Por lo tanto, el proyecto debe producir un beneficio más atractivo que el que resultaría de colocar el capital a interés bancario. Por otro lado, como el beneficio B es función de la tasa de interés t_i, habrá una tasa de interés para la cual al final del proyecto resulta un beneficio nulo. Esta tasa de interés se conoce como tasa interna de retorno o TIR, de modo que:

$$VAN = B_n = E_0 + \sum_{i=1}^{N} FCD_i = E_0 + \sum_{i=1}^{N} \frac{FC_i}{(1+TIR)^i} = 0 \tag{13.4}$$

En este caso, el el TIR resulta:

TIR	11,22 %

Cuadro 13.3: TIR

En la medida en que la TIR se acerque al valor de la tasa de interés de mercado el proyecto se vuelve menos atractivo. Como puedo observarse del Cuadro 13.3 este no es el caso, ya que el mismo resuta muy superior a la tasa anual de interés (1,3 %). En la Figura 13.3 se puede observar el FCD para una tasa de interés $t_i = 11,22\,\%$, donde se comprueba que el cálculo es el correcto.

13.1.5. TRI

En muchos proyectos, con escenarios a largo plazo impredecibles, o con alta probabilidad de que el escenario a futuro cambie, toma importancia el TRI o Tiempo de Recupero de la Inversión. Este valor resulta de determinar el valor de k tal que:

$$VAN = B_n = E_0 + \sum_{i=1}^{k} FCD_i = E_0 + \sum_{i=1}^{k} \frac{FC_i}{(1+t_i)^i} = 0 \tag{13.5}$$

En este caso se puede obtener gráficamente de la Figura 13.3, resultando aproximadamente:

TRI	A los 4 meses del 4to año luego de realizada la inversión

Cuadro 13.4: TRI

13.1.6. Relación costo beneficio

Este criterio se basa en determinar la relación entre el valor actualizado de los ingresos netos, en relación al valor actualizado del total de los egresos; es decir, toma en cuenta el valor total comprometido en el proyecto. La $RCBN$[5] esta dada por la ecuación:

$$RCBN = \frac{\sum_{i=0}^{N} \frac{I_i - E_i}{(1+t_i)^i}}{\sum_{i=0}^{N} \frac{E_i}{(1+t_i)^i}} \tag{13.6}$$

$RCBN$ da una idea del rendimiento del proyecto. Obviamente, para aceptar el proyecto debe ser $RCBN > 0$. Para este caso,el $RCBN$ resulta:

RCBN	36,2 %

Cuadro 13.5: RCBN

[5]Relación Costo Beneficio Neto

Capítulo 14

Conclusiones

14.1. Objetivos alcanzados

El relevamiento de la red permite conocer el estado actual de la red con sus fortalezas y debilidades, otorgando la capacidad de analizar la evolución de la misma, comparando las distintas versiones de trabajos realizados en distintas oportunidades.

Una vez decidida la solución a implementar, se llevó a cabo un estudio de factibilidad y un planeamiento del proyecto asignando distribuyendo las tareas de implementación de forma uniforme de forma tal de lograr una inversión gradual. Luego se procedió al estudio de los estándares y protocolos que fueran necesarios para conocer a fondo los servicios de voz, vídeo y datos. En la sección de la ingeniería en detalle se definieron conceptos necesarios para construcción de la red planificada, y se prosiguió a validar la propuesta mediante las herramientas de simulación correspondientes. Permitiendo realizar un avance innovador en este aspecto con respecto a cualquier otro trabajo sobre la LAN de la FIUBA. Se concluye finalmente con los estudios de confiabilidad correspondientes y evaluación económica del proyecto.

Con respecto a la implementación real del proyecto, queda a criterio de las autoridades de la facultad, teniéndose en cuenta las posibles reducciones de costo y los beneficios a largo plazo planteadas en el Capítulo 13 en donde se presentó la evaluación económica del proyecto.

14.2. Fallos y recomendaciones para futuros diseños

Como recomendación principal, hacemos notar que de dilatarse el tiempo entre este estudio y una eventual implementación se deberá tener en cuenta por la presencia de nuevas tecnologías (principalmente 802.11n) y en menor medida por futuros cambios en la necesidad de tráfico. Sin embargo, las bases del presente proyecto se considera como modelo a seguir para este tipo de implementación, solo se recomienda recalcular las zonas de cobertura en función a la capacidad que los nuevos APs puedan dar y realizar un nuevo estudio del tráfico.

Se debe destacar que en el proyecto no se profundiza sobre la administración de los equipos, la cual no fue el objetivo de este informe debido a que esta información se encuentra detallada el los manuales y hojas de datos de los equipo.

Apéndice A

Planos

A.1. Primer Piso

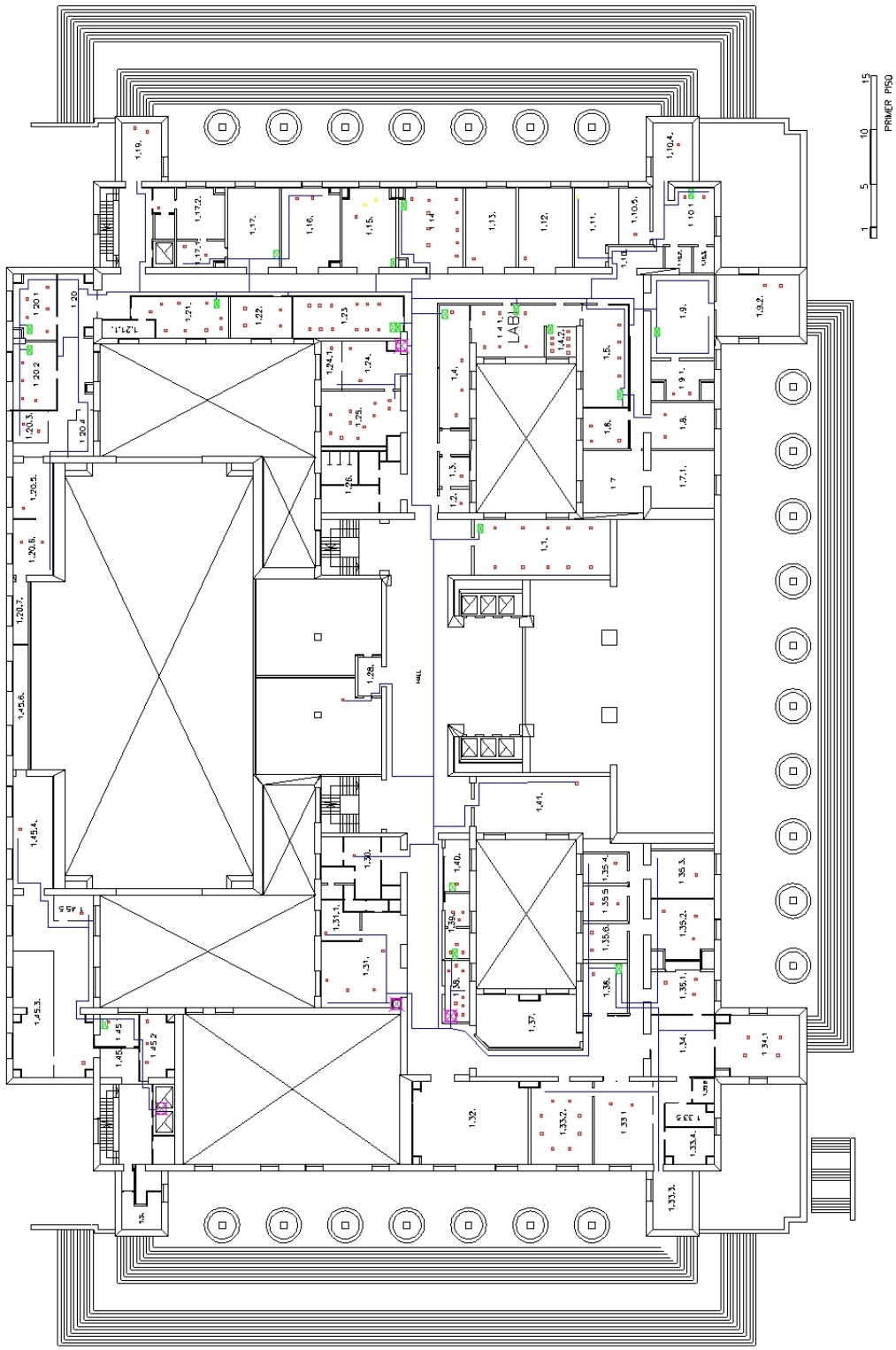


Figura A.1: Plano 1er Piso

A.2. Segundo Piso

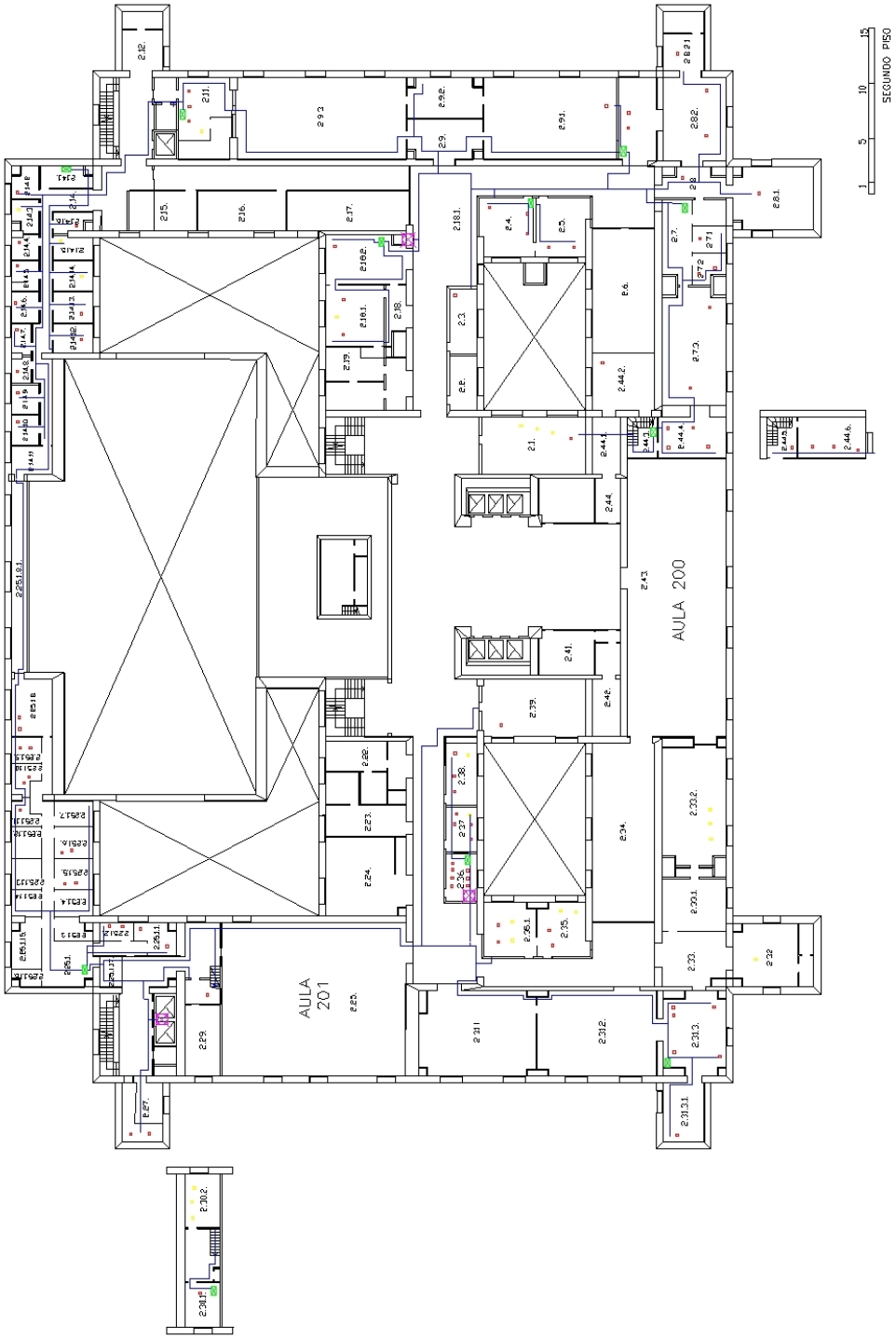


Figura A.2: Plano 2do Piso

A.3. Tercer Piso

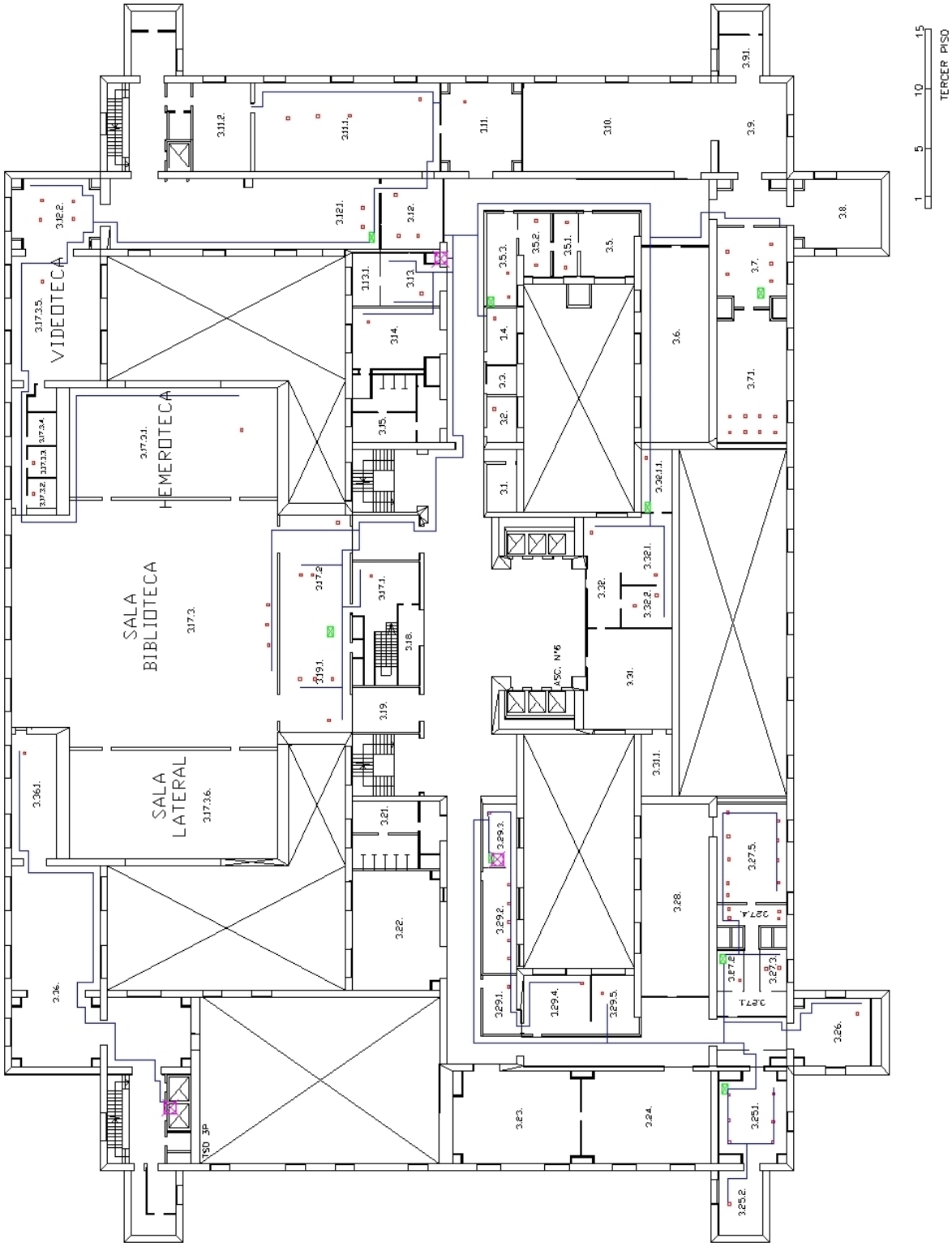


Figura A.3: Plano 3er Piso

A.4. Cuarto Piso

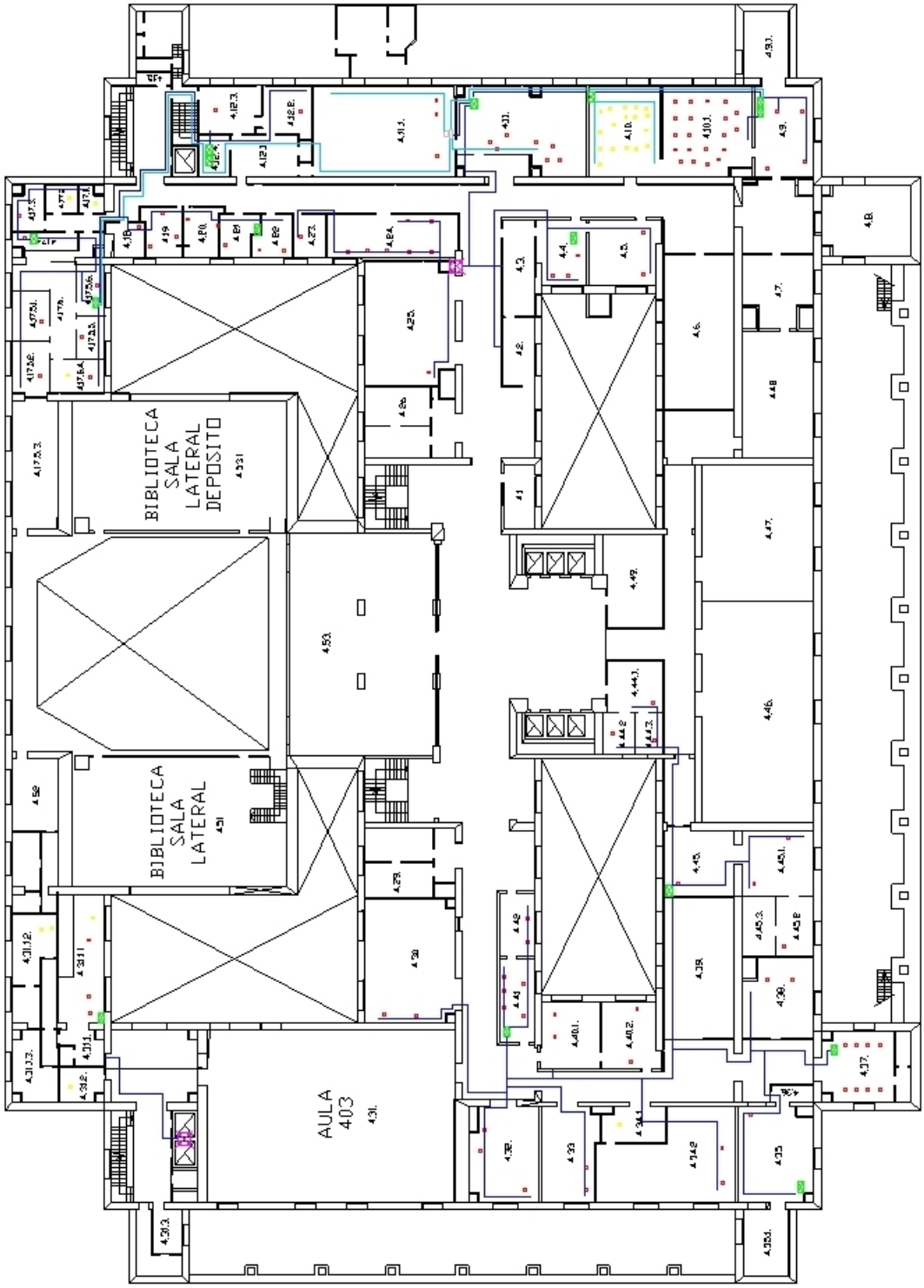


Figura A.4: Plano 4to Piso

A.5. Quinto Piso

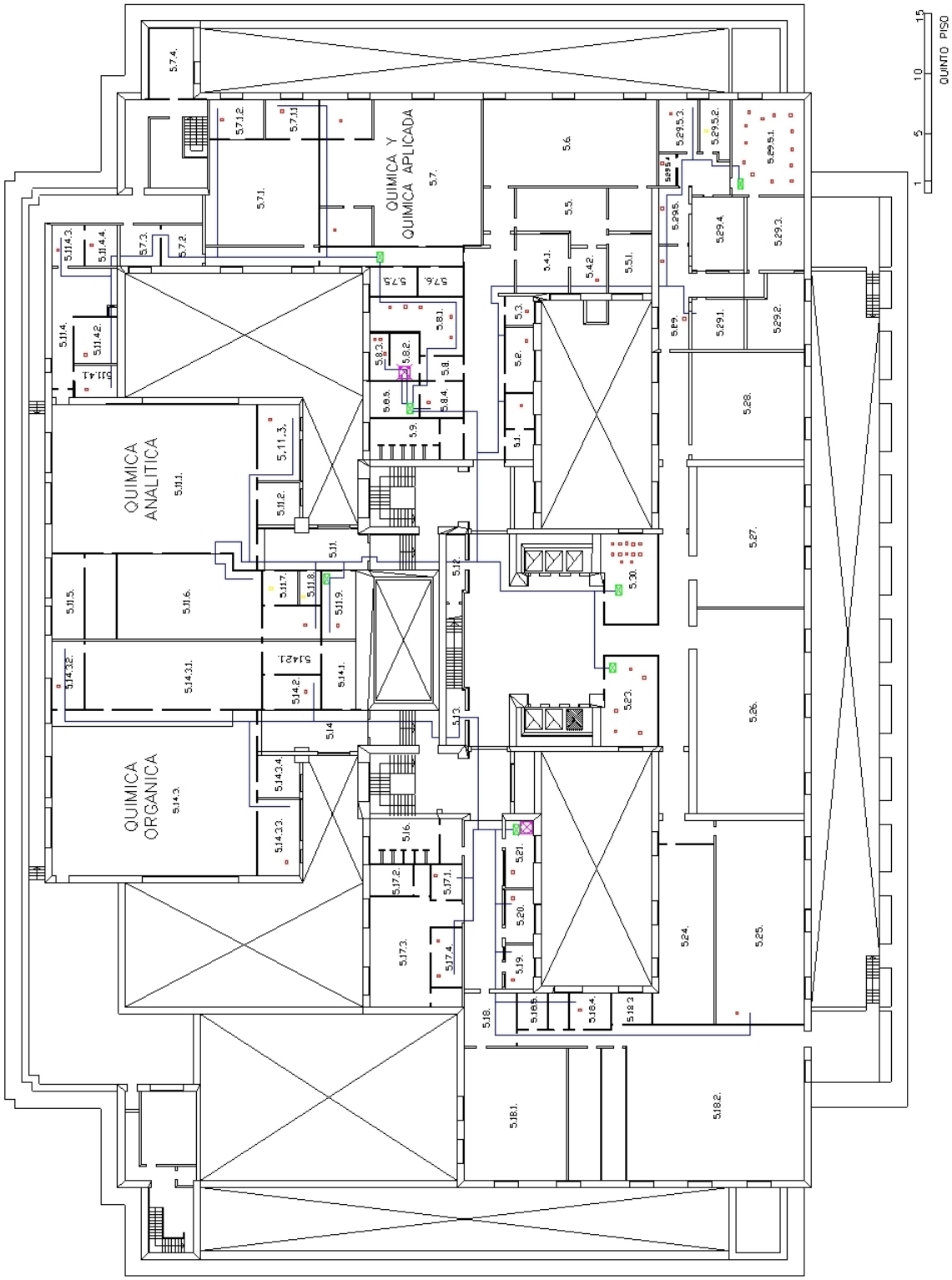


Figura A.5: Plano 5to Piso

A.6. Planta Baja

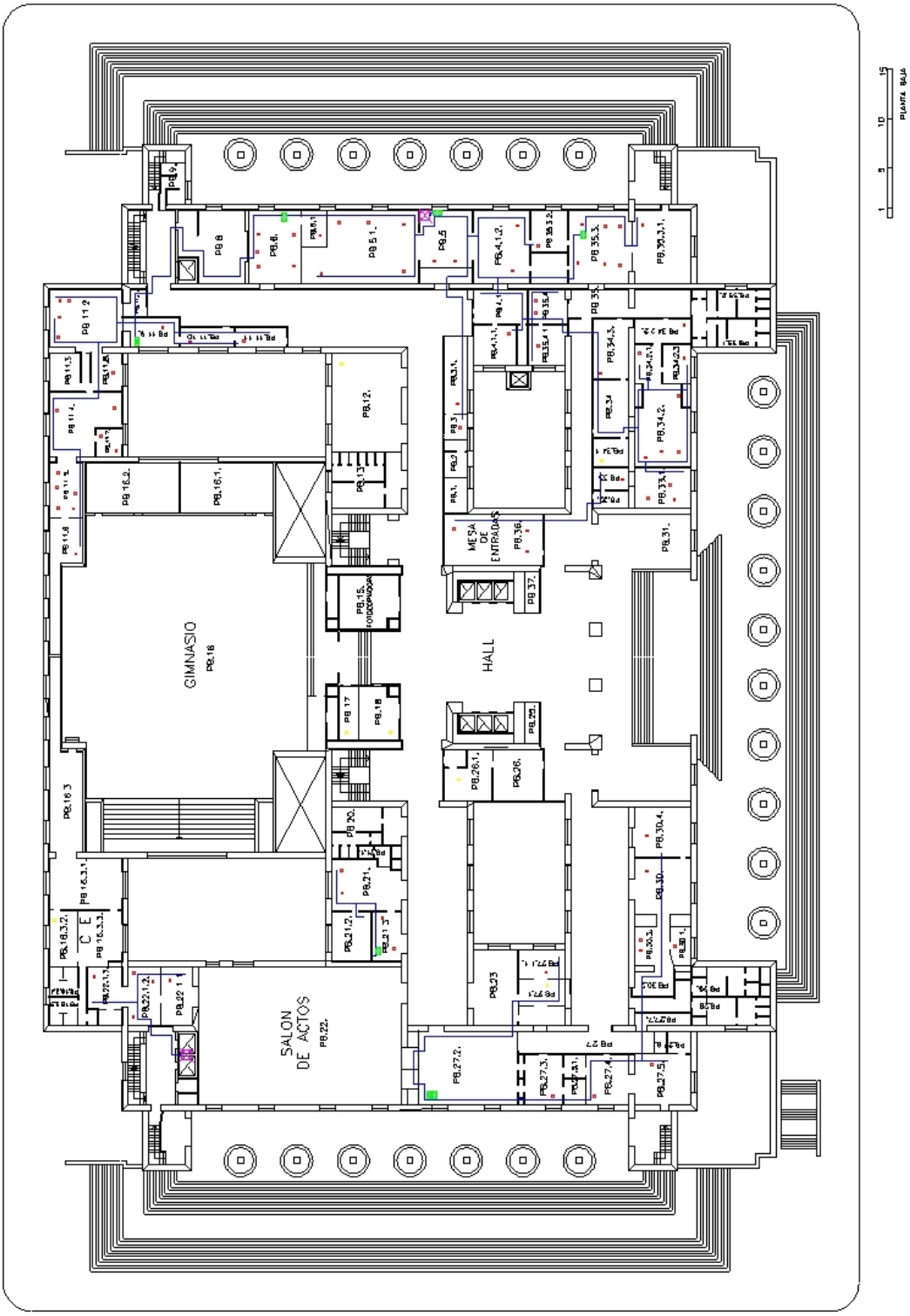


Figura A.6: Plano Planta Baja

A.7. Subsuelo

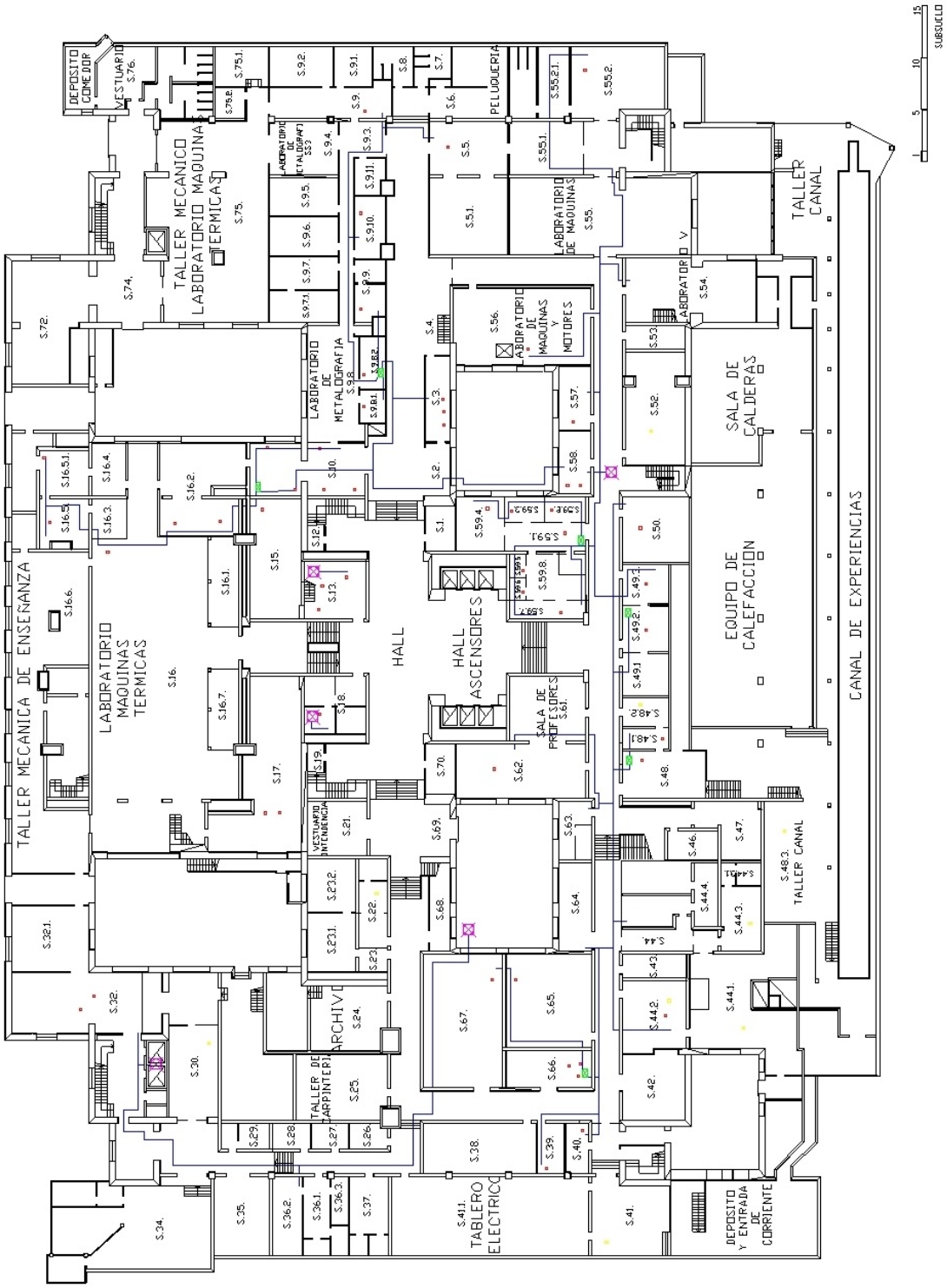


Figura A.7: Plano Subsuelo

A.8. Entre piso

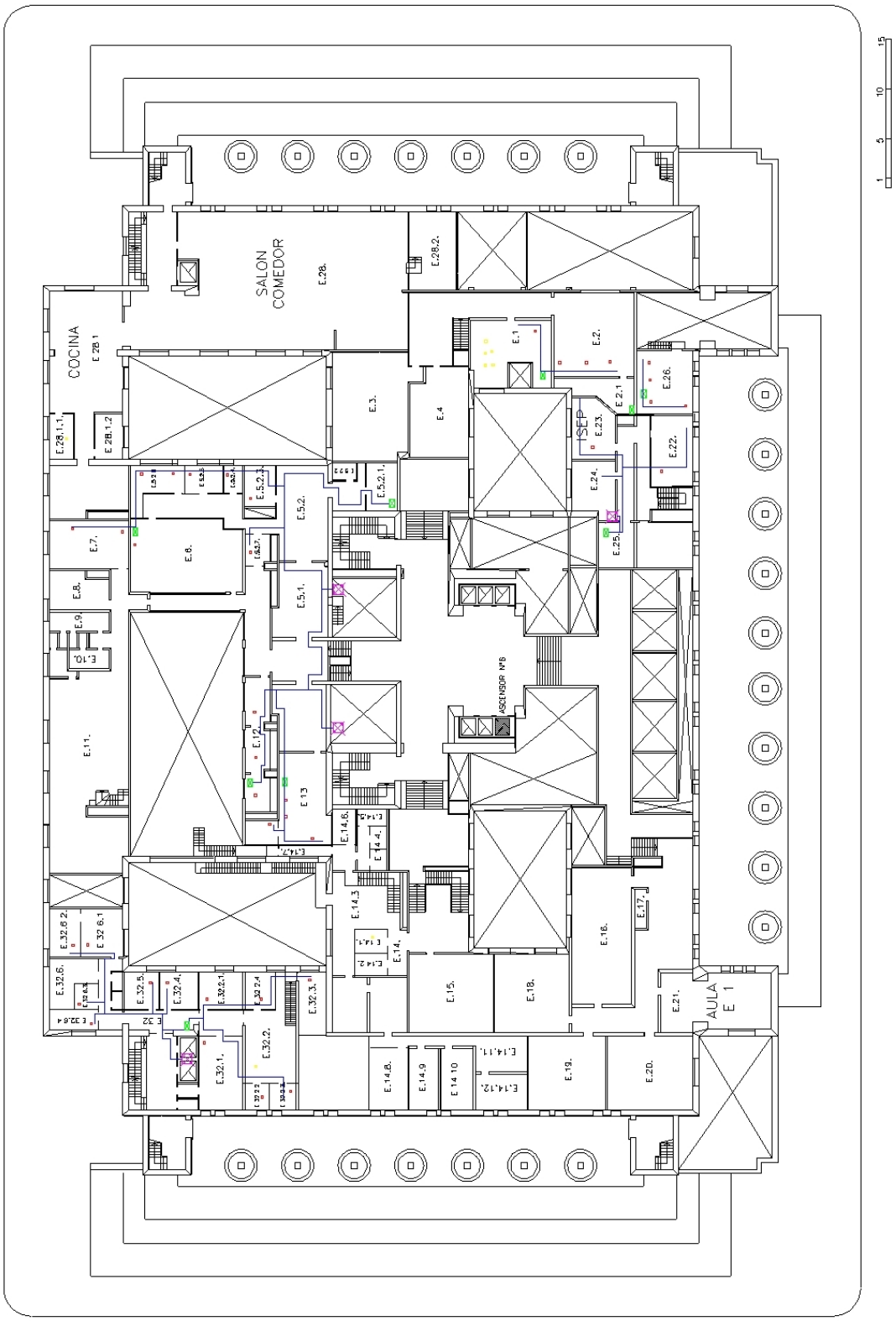


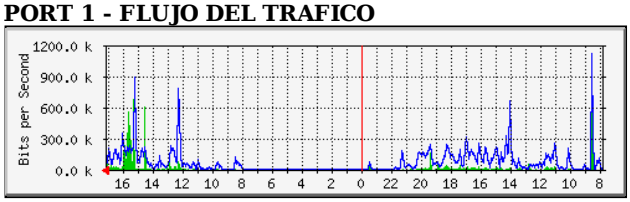
Figura A.8: Plano Entre Piso

Apéndice B

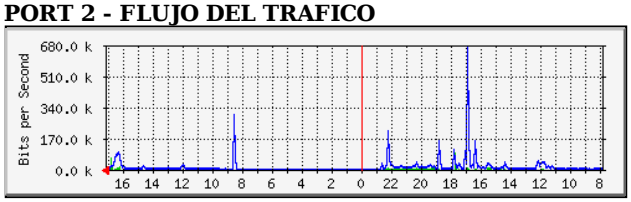
Monitoreo de Tráfico

SW ENTREPISO - FIUBA

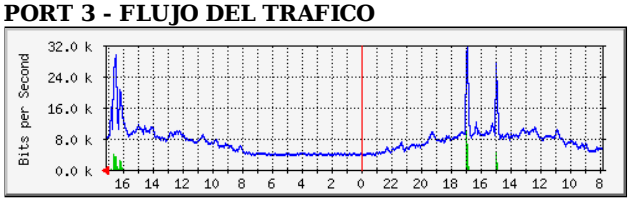
PORT 1 - FLUJO DEL TRAFICO



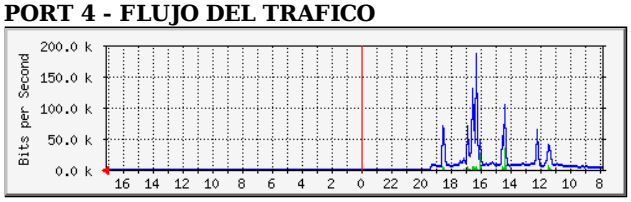
PORT 2 - FLUJO DEL TRAFICO



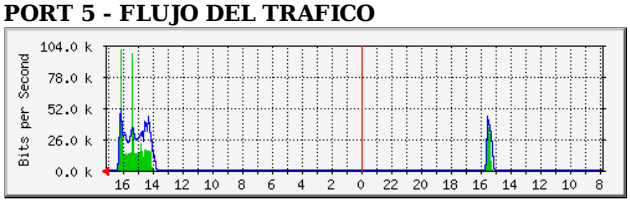
PORT 3 - FLUJO DEL TRAFICO



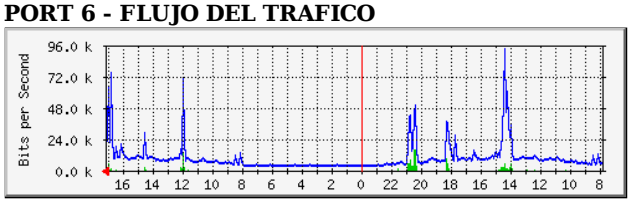
PORT 4 - FLUJO DEL TRAFICO



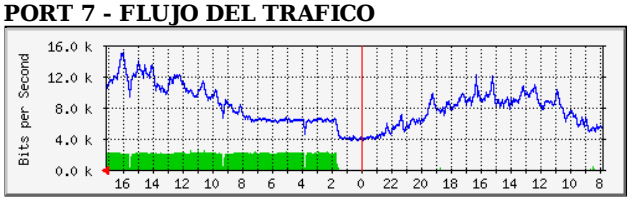
PORT 5 - FLUJO DEL TRAFICO



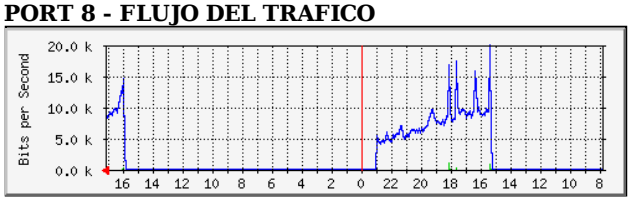
PORT 6 - FLUJO DEL TRAFICO



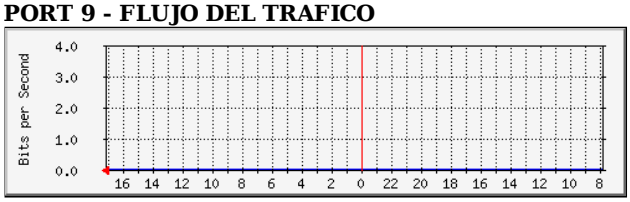
PORT 7 - FLUJO DEL TRAFICO



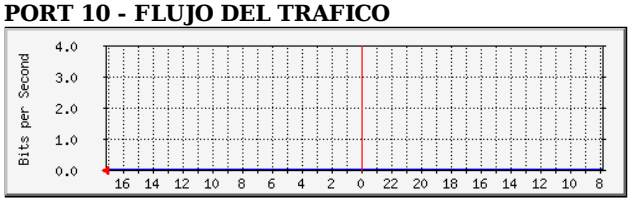
PORT 8 - FLUJO DEL TRAFICO



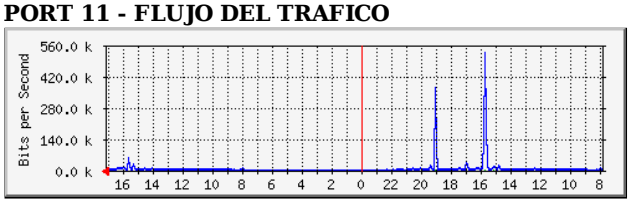
PORT 9 - FLUJO DEL TRAFICO



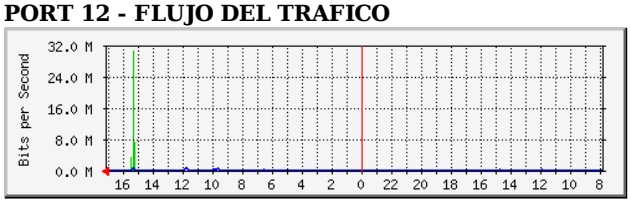
PORT 10 - FLUJO DEL TRAFICO



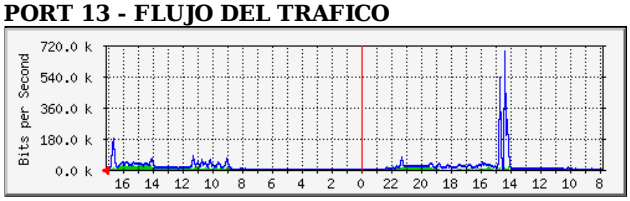
PORT 11 - FLUJO DEL TRAFICO



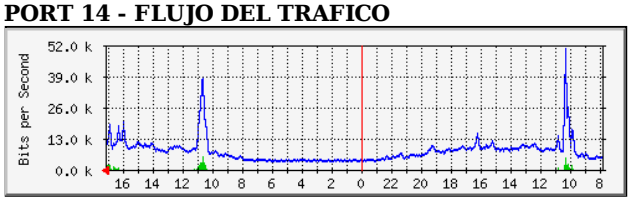
PORT 12 - FLUJO DEL TRAFICO



PORT 13 - FLUJO DEL TRAFICO



PORT 14 - FLUJO DEL TRAFICO

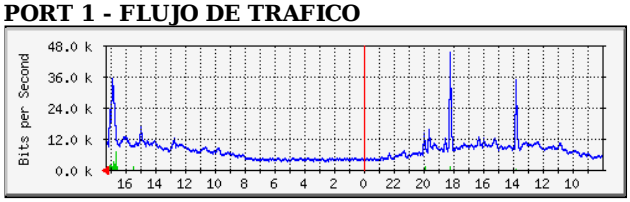


PORT 15 - FLUJO DEL TRAFICO

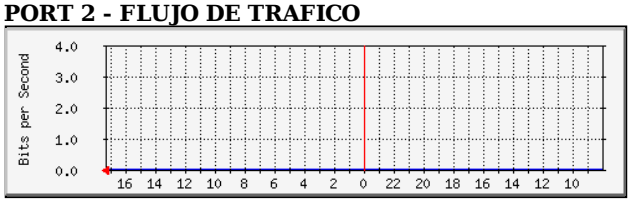
PORT 16 - FLUJO DEL TRAFICO

SW MECANICA - FIUBA

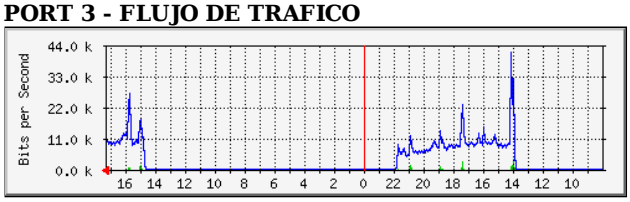
PORT 1 - FLUJO DE TRAFICO



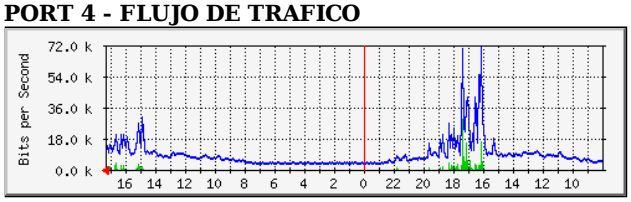
PORT 2 - FLUJO DE TRAFICO



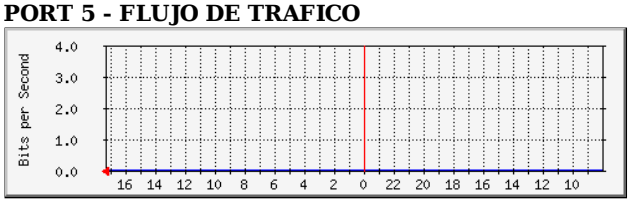
PORT 3 - FLUJO DE TRAFICO



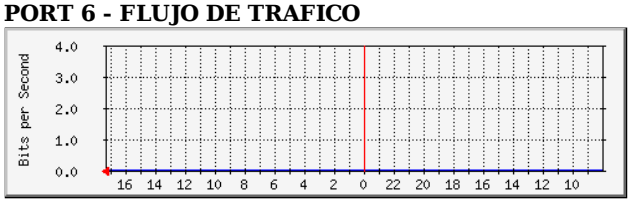
PORT 4 - FLUJO DE TRAFICO



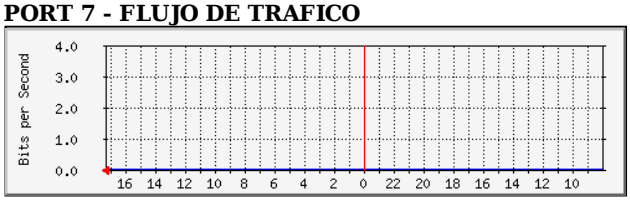
PORT 5 - FLUJO DE TRAFICO



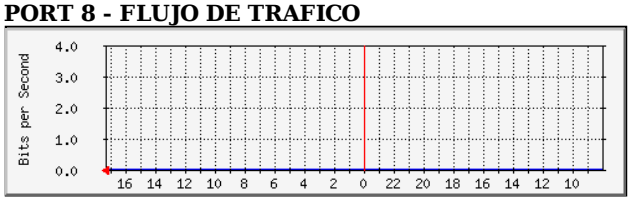
PORT 6 - FLUJO DE TRAFICO



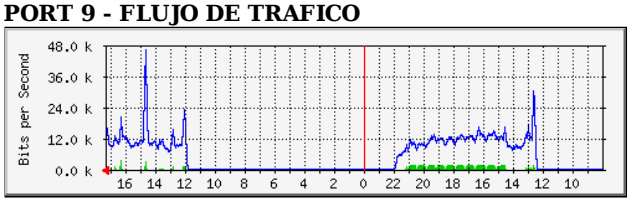
PORT 7 - FLUJO DE TRAFICO



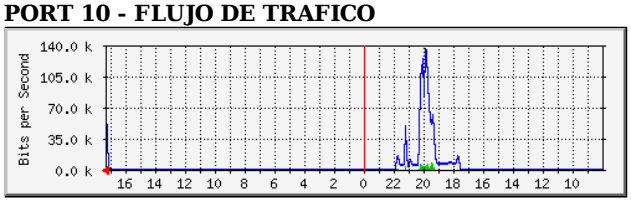
PORT 8 - FLUJO DE TRAFICO



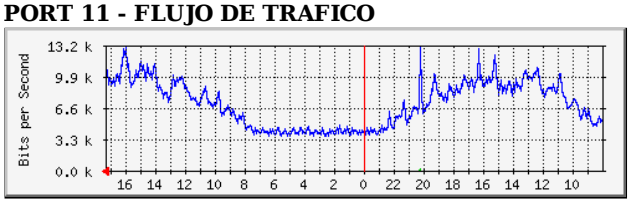
PORT 9 - FLUJO DE TRAFICO



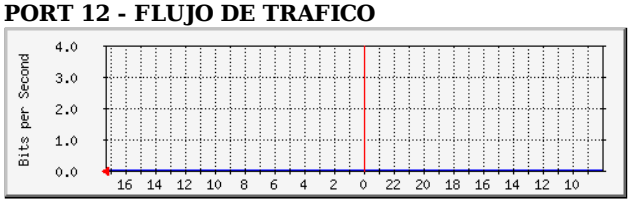
PORT 10 - FLUJO DE TRAFICO



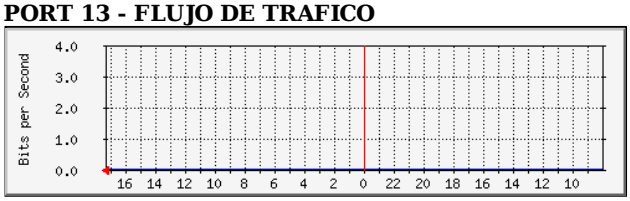
PORT 11 - FLUJO DE TRAFICO



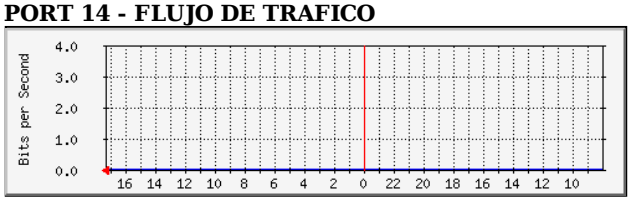
PORT 12 - FLUJO DE TRAFICO



PORT 13 - FLUJO DE TRAFICO



PORT 14 - FLUJO DE TRAFICO

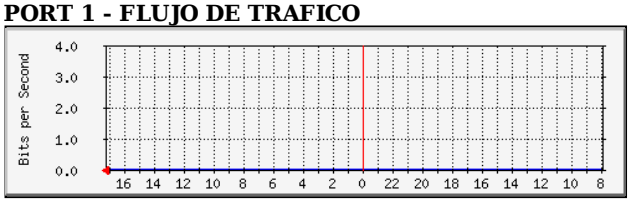


PORT 15 - FLUJO DE TRAFICO

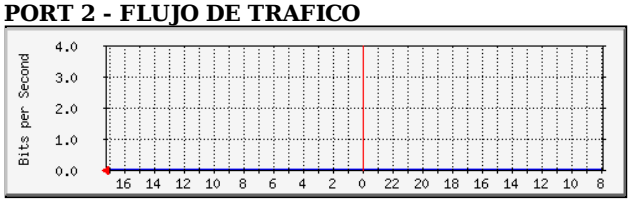
PORT 16 - FLUJO DE TRAFICO

SW ALUMNOS - FIUBA

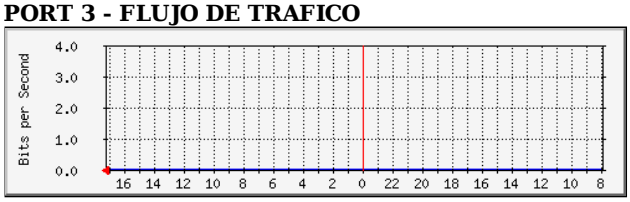
PORT 1 - FLUJO DE TRAFICO



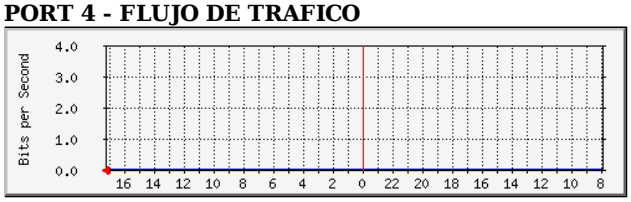
PORT 2 - FLUJO DE TRAFICO



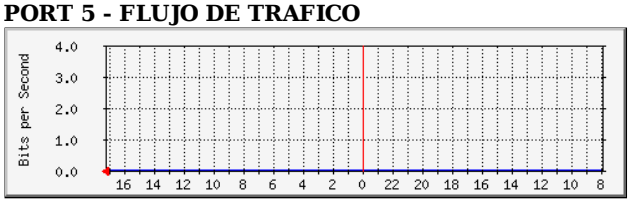
PORT 3 - FLUJO DE TRAFICO



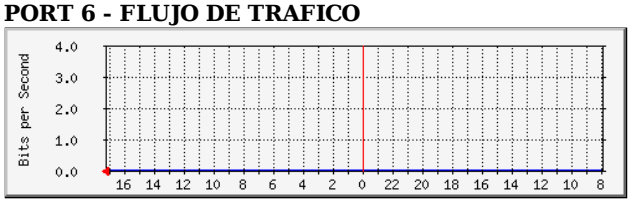
PORT 4 - FLUJO DE TRAFICO



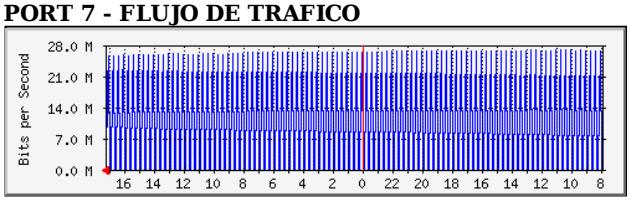
PORT 5 - FLUJO DE TRAFICO



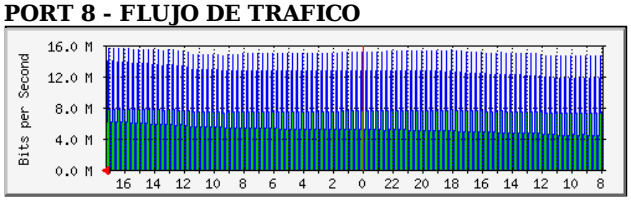
PORT 6 - FLUJO DE TRAFICO



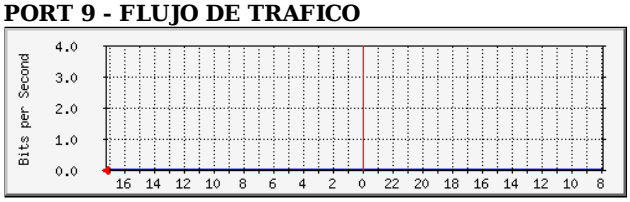
PORT 7 - FLUJO DE TRAFICO



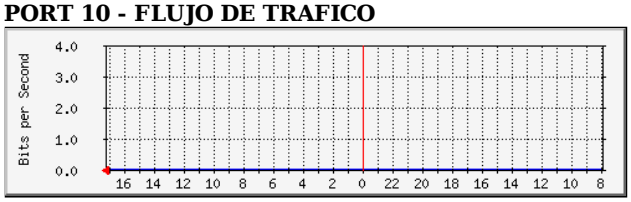
PORT 8 - FLUJO DE TRAFICO



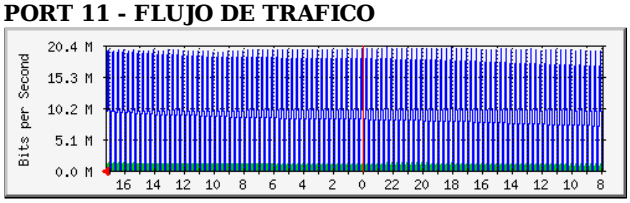
PORT 9 - FLUJO DE TRAFICO



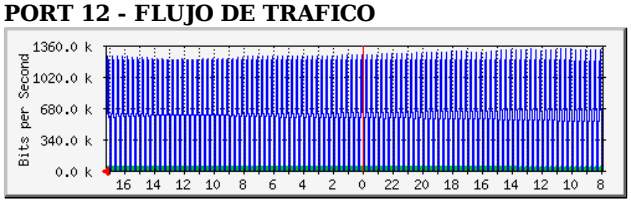
PORT 10 - FLUJO DE TRAFICO



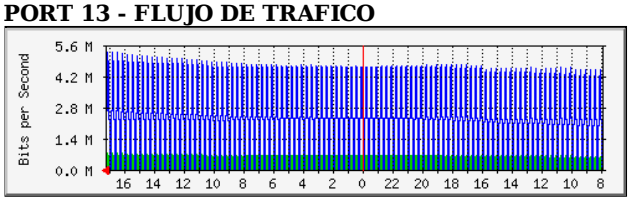
PORT 11 - FLUJO DE TRAFICO



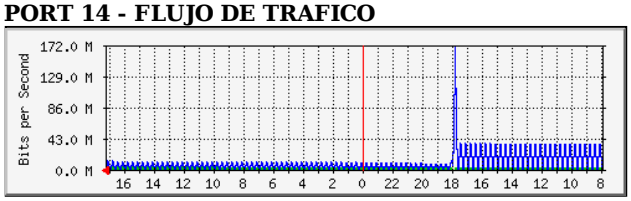
PORT 12 - FLUJO DE TRAFICO



PORT 13 - FLUJO DE TRAFICO



PORT 14 - FLUJO DE TRAFICO

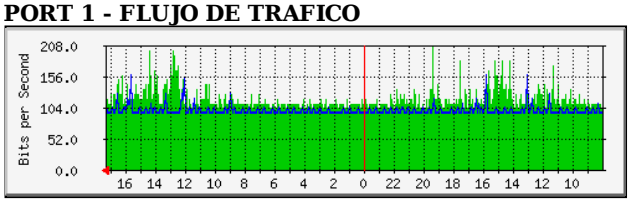


PORT 15 - FLUJO DE TRAFICO

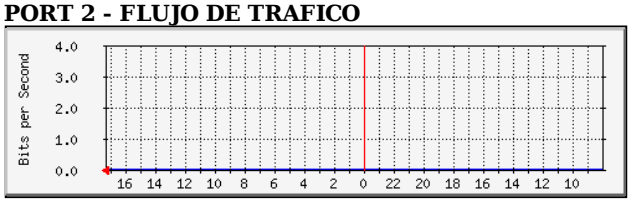
PORT 16 - FLUJO DE TRAFICO

SW DECANATO - FIUBA

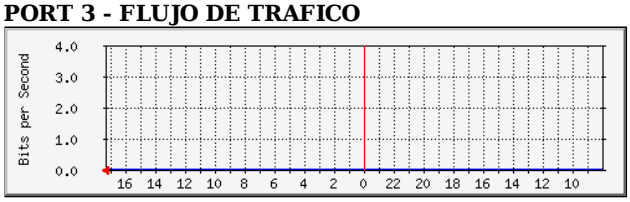
PORT 1 - FLUJO DE TRAFICO



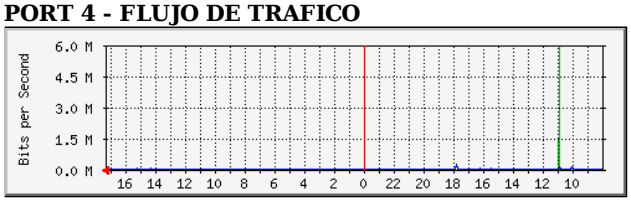
PORT 2 - FLUJO DE TRAFICO



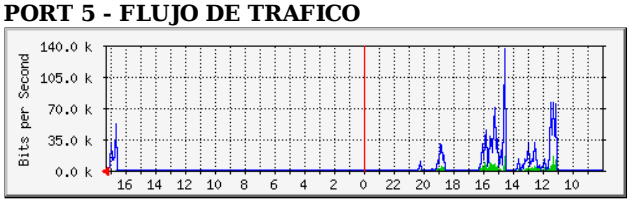
PORT 3 - FLUJO DE TRAFICO



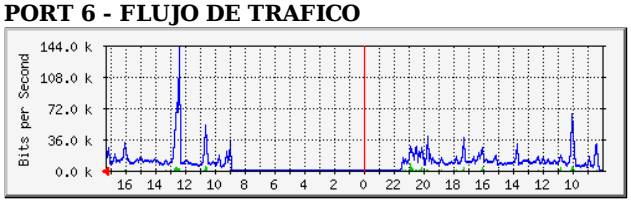
PORT 4 - FLUJO DE TRAFICO



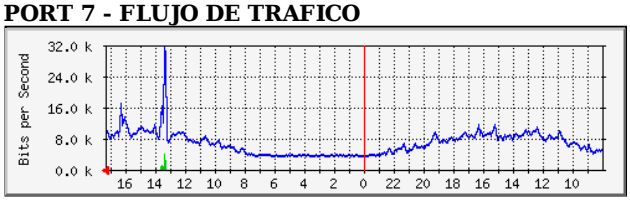
PORT 5 - FLUJO DE TRAFICO



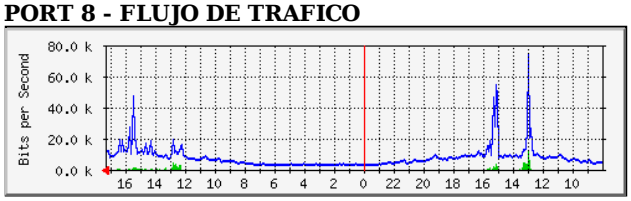
PORT 6 - FLUJO DE TRAFICO



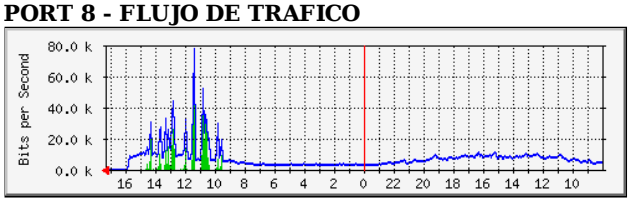
PORT 7 - FLUJO DE TRAFICO



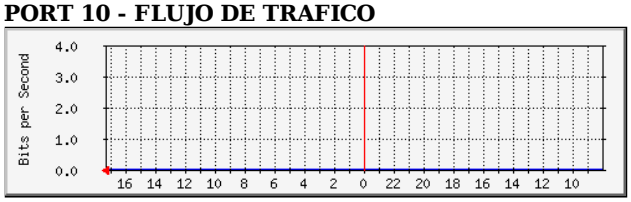
PORT 8 - FLUJO DE TRAFICO



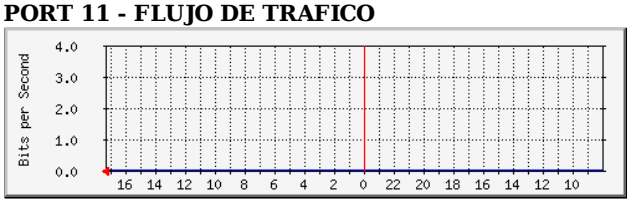
PORT 8 - FLUJO DE TRAFICO



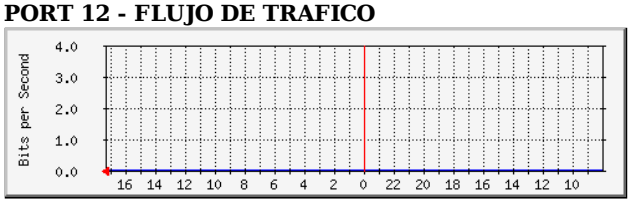
PORT 10 - FLUJO DE TRAFICO



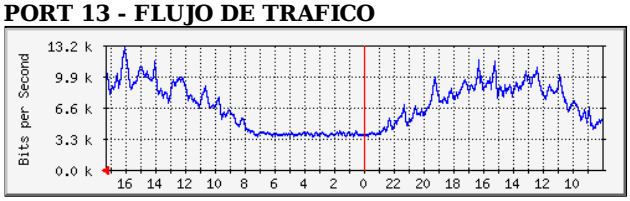
PORT 11 - FLUJO DE TRAFICO



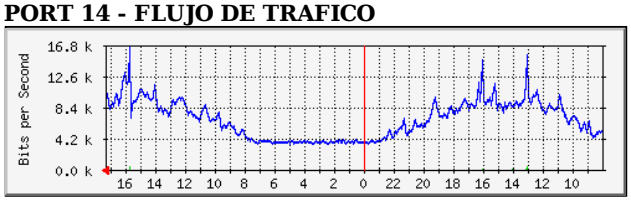
PORT 12 - FLUJO DE TRAFICO



PORT 13 - FLUJO DE TRAFICO



PORT 14 - FLUJO DE TRAFICO

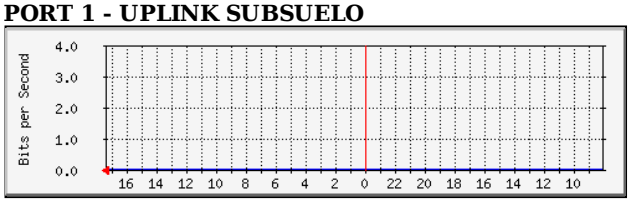


PORT 15 - FLUJO DE TRAFICO

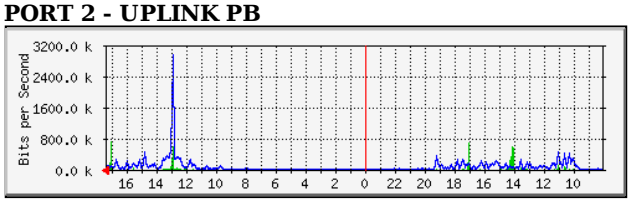
PORT 16 - FLUJO DE TRAFICO

CORE SW CDC - FIUBA

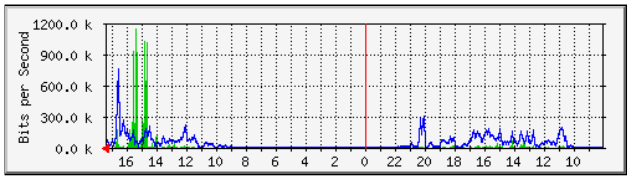
PORT 1 - UPLINK SUBSUELO



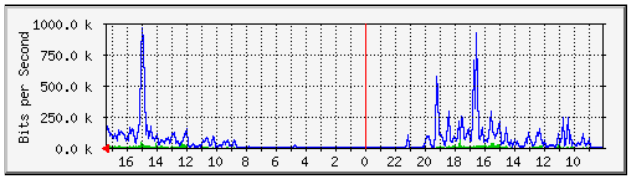
PORT 2 - UPLINK PB



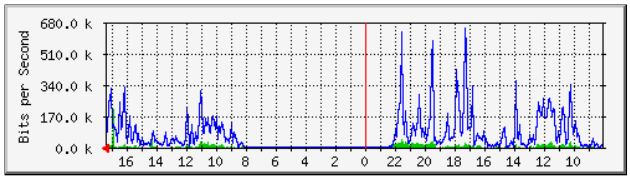
PORT 3 - UPLINK MATEMATICAS



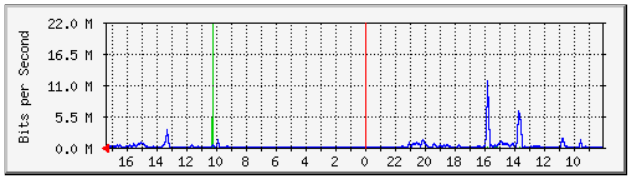
PORT 4 - UPLINK 205



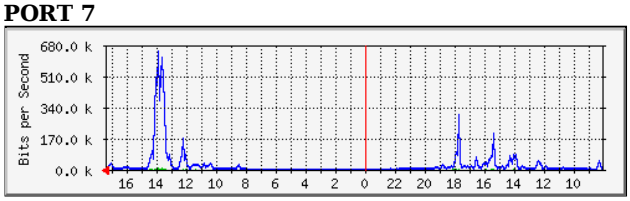
PORT 5 - UPLINK SECID



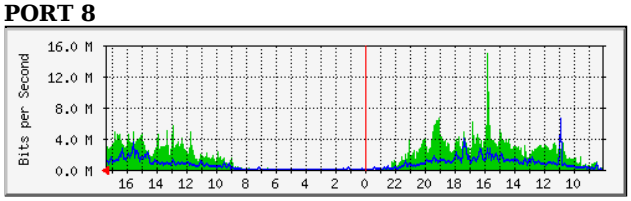
PORT 6 - UPLINK INTI



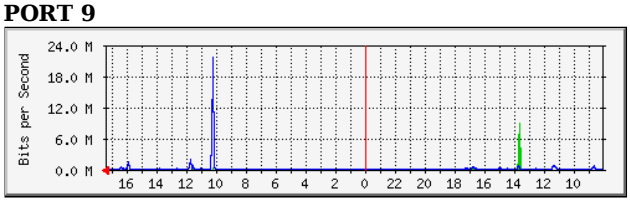
PORT 7



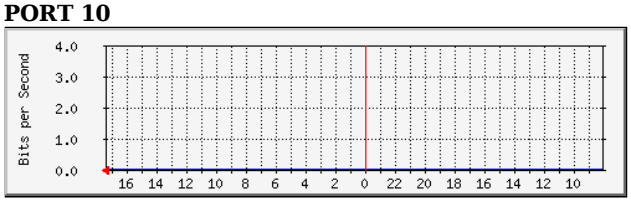
PORT 8



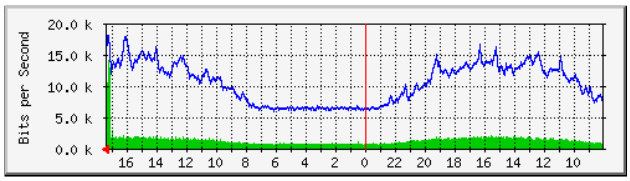
PORT 9



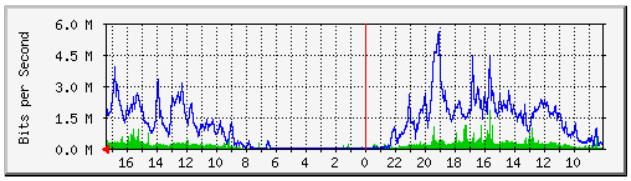
PORT 10



PORT 11 - UPLINK CORE L11 1

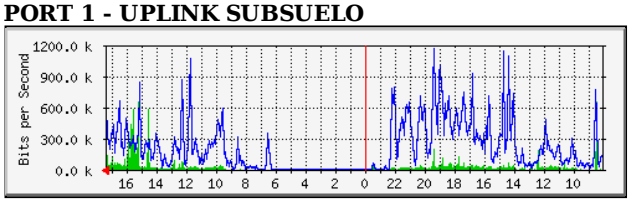


PORT 12 - UPLINK CORE L11 2

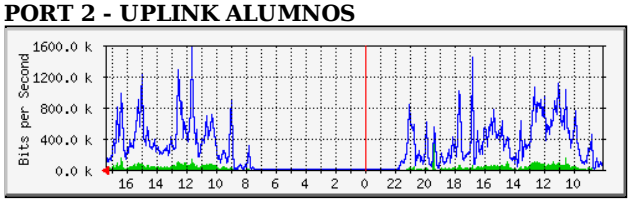


CORE SW L11 - FIUBA

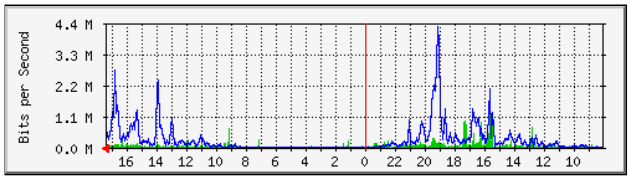
PORT 1 - UPLINK SUBSUELO



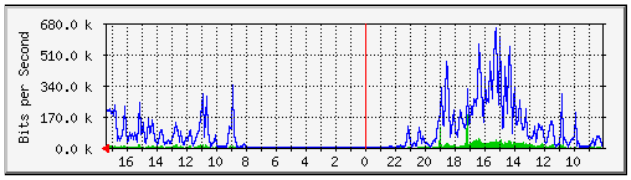
PORT 2 - UPLINK ALUMNOS



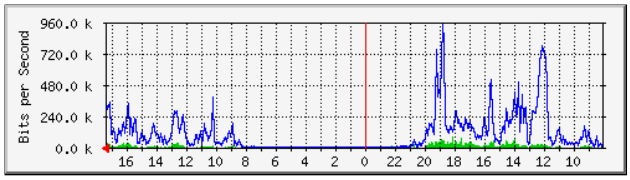
PORT 3 - UPLINK L11



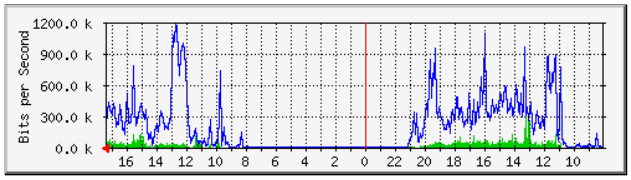
PORT 4 - UPLINK FISICA



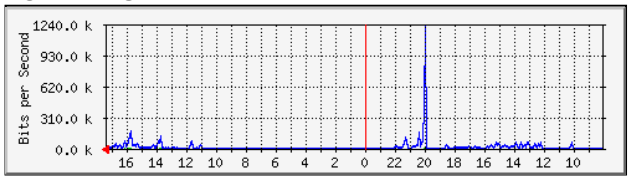
PORT 5 - UPLINK BIBLIOTECA



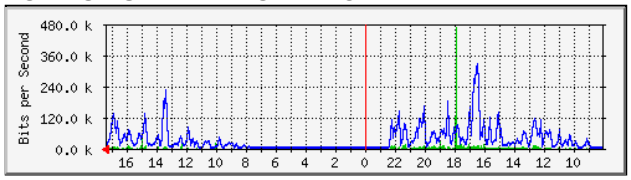
PORT 6 - UPLINK COMPUTACION



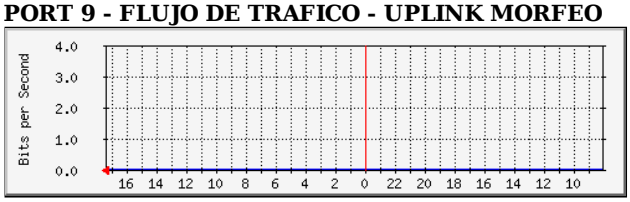
PORT 7 - UPLINK LAE



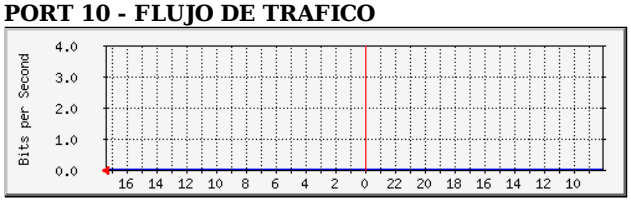
PORT 8 - UPLINK BIOMEDICA



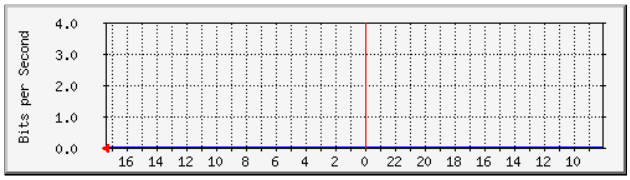
PORT 9 - FLUJO DE TRAFICO - UPLINK MORFEO



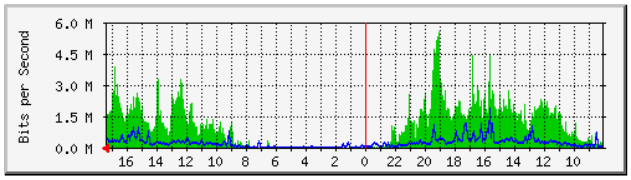
PORT 10 - FLUJO DE TRAFICO



PORT 11 - UPLINK CDC 1

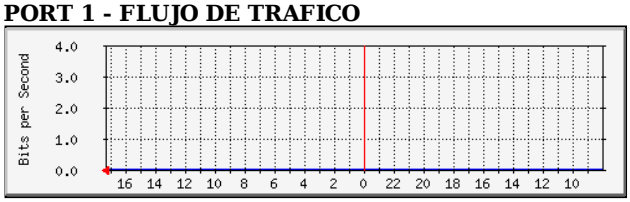


PORT 12 - UPLINK CDC 2

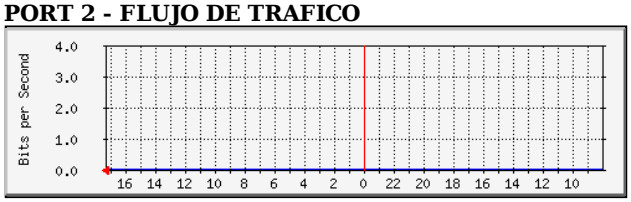


SW L11 - FIUBA

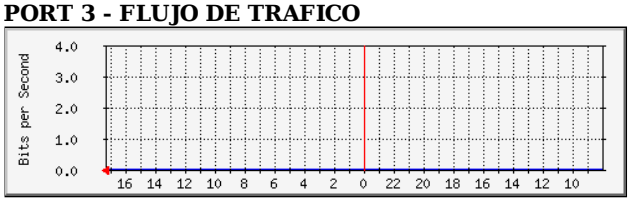
PORT 1 - FLUJO DE TRAFICO



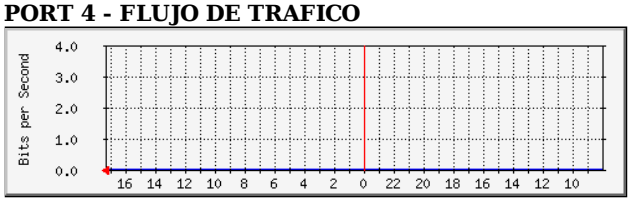
PORT 2 - FLUJO DE TRAFICO



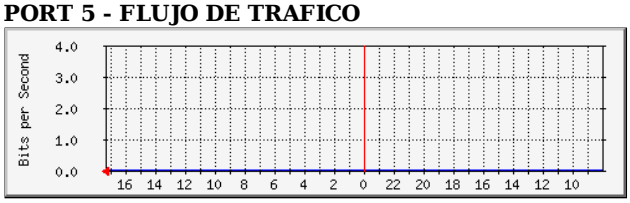
PORT 3 - FLUJO DE TRAFICO



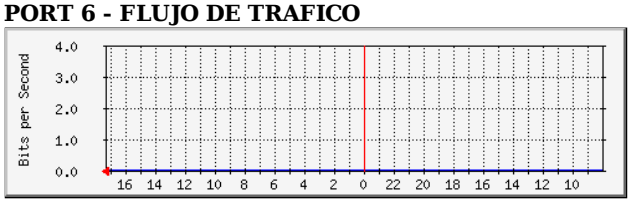
PORT 4 - FLUJO DE TRAFICO



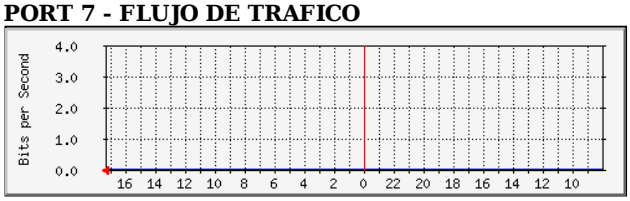
PORT 5 - FLUJO DE TRAFICO



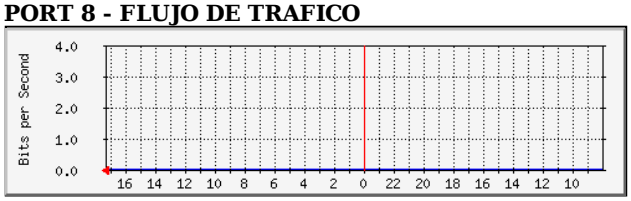
PORT 6 - FLUJO DE TRAFICO



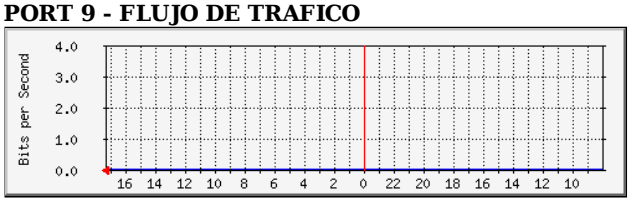
PORT 7 - FLUJO DE TRAFICO



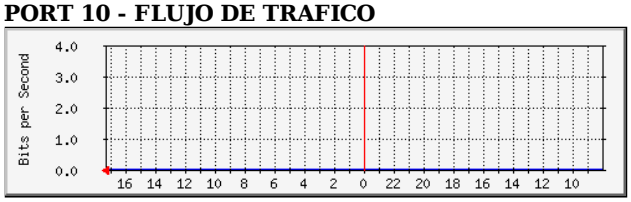
PORT 8 - FLUJO DE TRAFICO



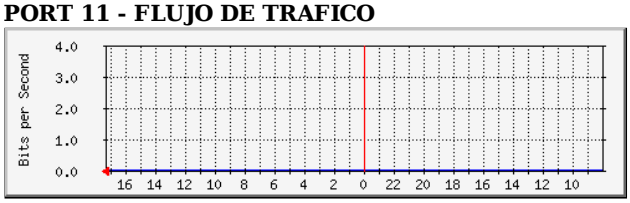
PORT 9 - FLUJO DE TRAFICO



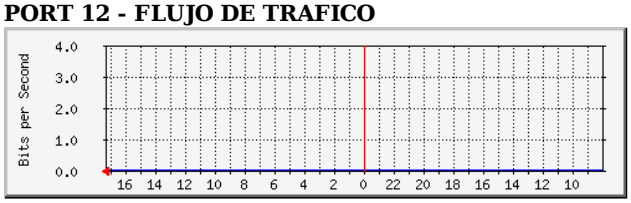
PORT 10 - FLUJO DE TRAFICO



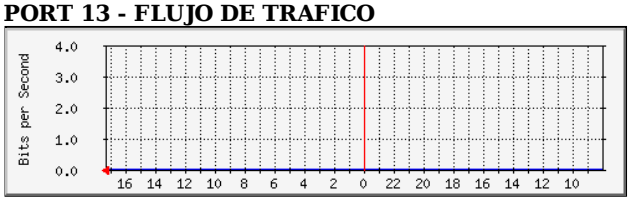
PORT 11 - FLUJO DE TRAFICO



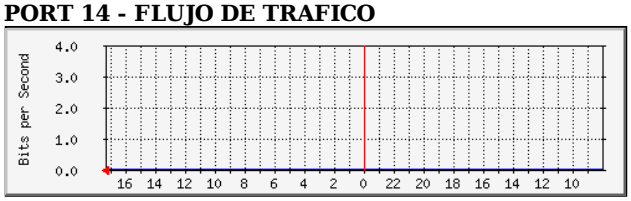
PORT 12 - FLUJO DE TRAFICO



PORT 13 - FLUJO DE TRAFICO



PORT 14 - FLUJO DE TRAFICO

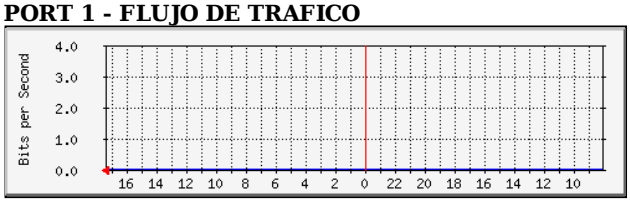


PORT 15 - FLUJO DE TRAFICO

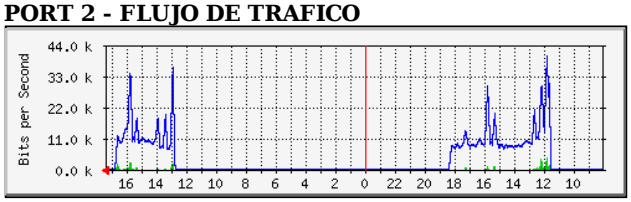
PORT 16 - FLUJO DE TRAFICO

SW MATEMATICAS - FIUBA

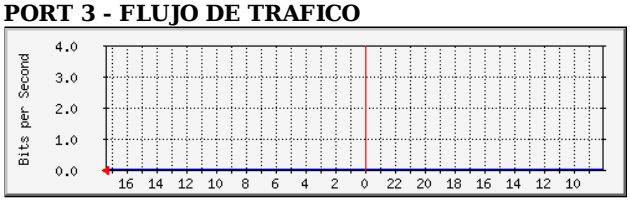
PORT 1 - FLUJO DE TRAFICO



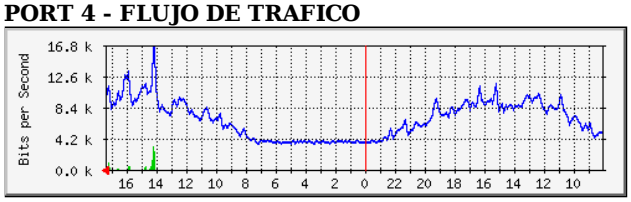
PORT 2 - FLUJO DE TRAFICO



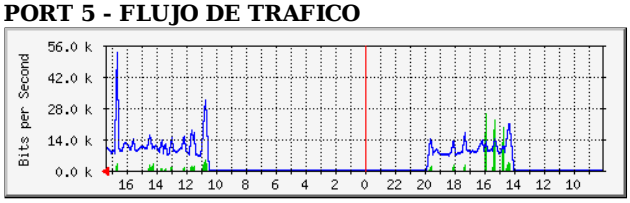
PORT 3 - FLUJO DE TRAFICO



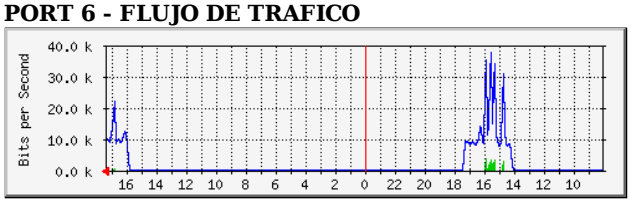
PORT 4 - FLUJO DE TRAFICO



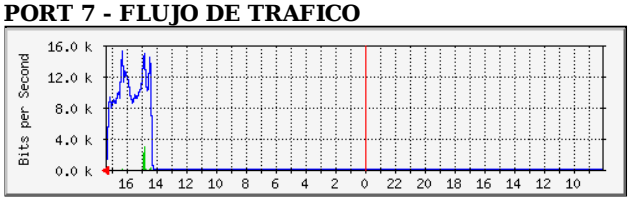
PORT 5 - FLUJO DE TRAFICO



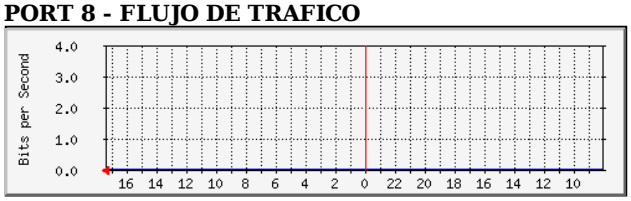
PORT 6 - FLUJO DE TRAFICO



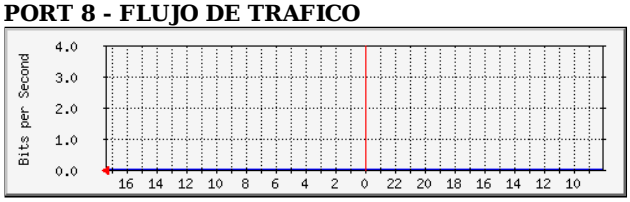
PORT 7 - FLUJO DE TRAFICO



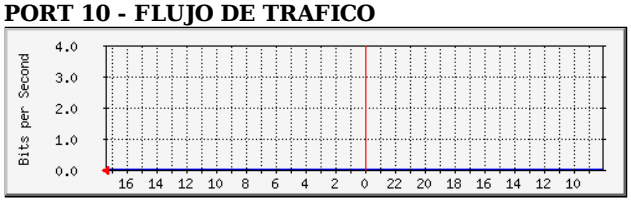
PORT 8 - FLUJO DE TRAFICO



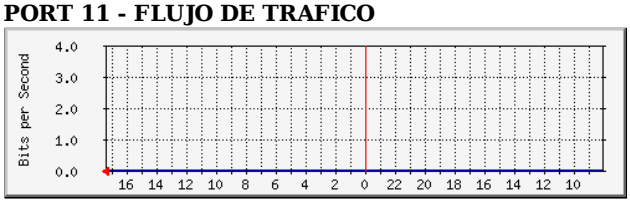
PORT 8 - FLUJO DE TRAFICO



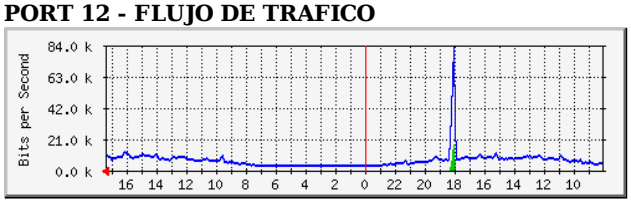
PORT 10 - FLUJO DE TRAFICO



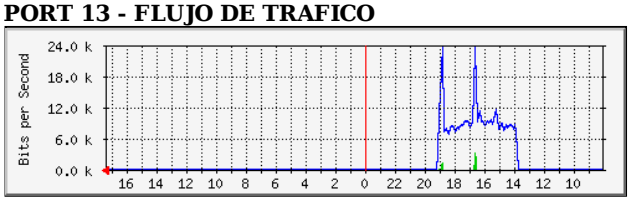
PORT 11 - FLUJO DE TRAFICO



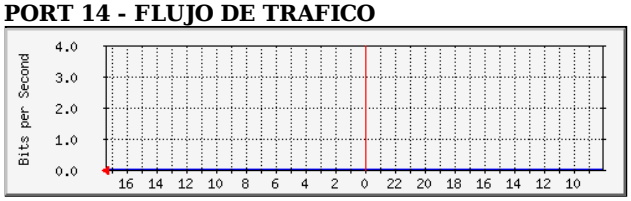
PORT 12 - FLUJO DE TRAFICO



PORT 13 - FLUJO DE TRAFICO



PORT 14 - FLUJO DE TRAFICO

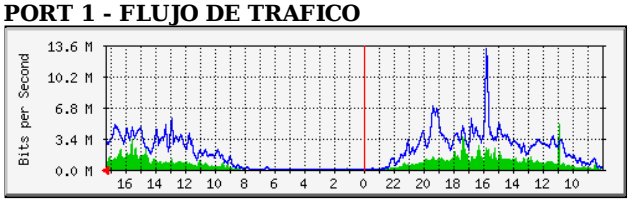


PORT 15 - FLUJO DE TRAFICO

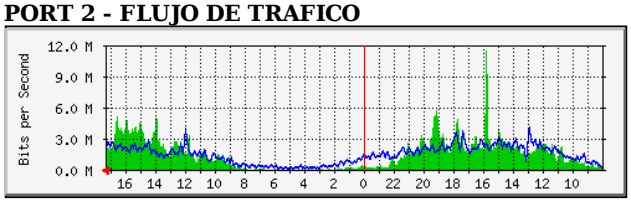
PORT 16 - FLUJO DE TRAFICO

SW MATRIX - FIUBA

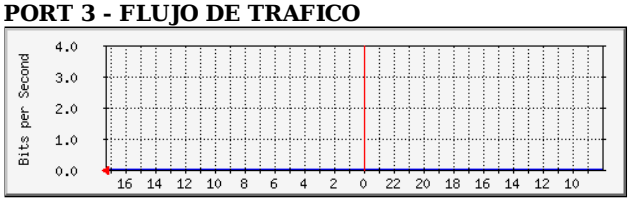
PORT 1 - FLUJO DE TRAFICO



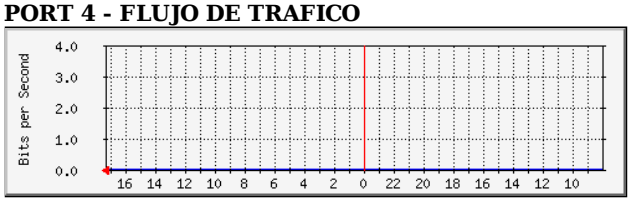
PORT 2 - FLUJO DE TRAFICO



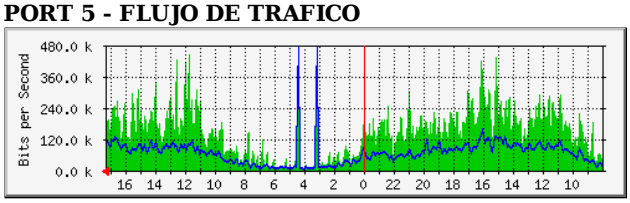
PORT 3 - FLUJO DE TRAFICO



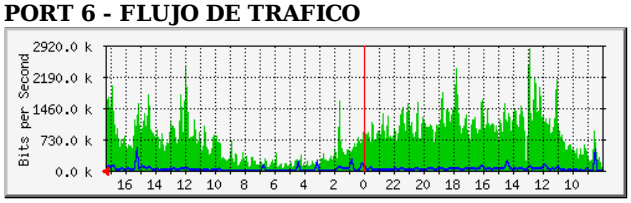
PORT 4 - FLUJO DE TRAFICO



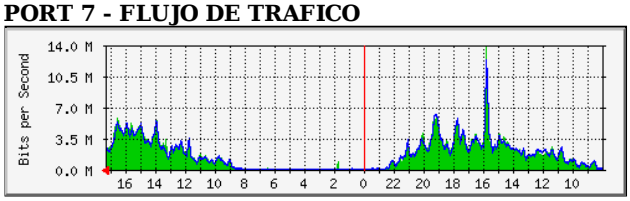
PORT 5 - FLUJO DE TRAFICO



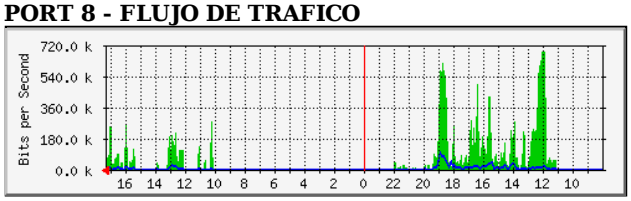
PORT 6 - FLUJO DE TRAFICO



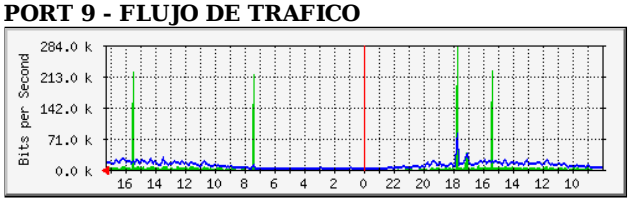
PORT 7 - FLUJO DE TRAFICO



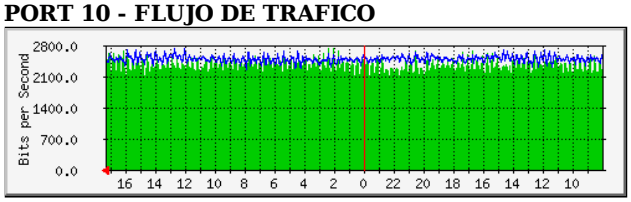
PORT 8 - FLUJO DE TRAFICO



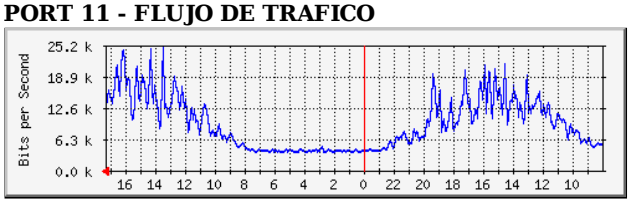
PORT 9 - FLUJO DE TRAFICO



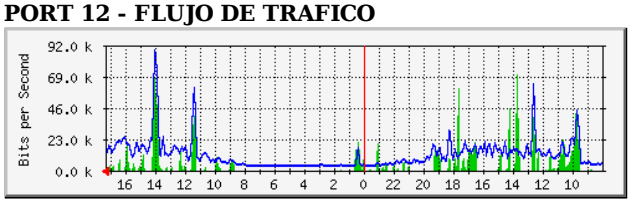
PORT 10 - FLUJO DE TRAFICO



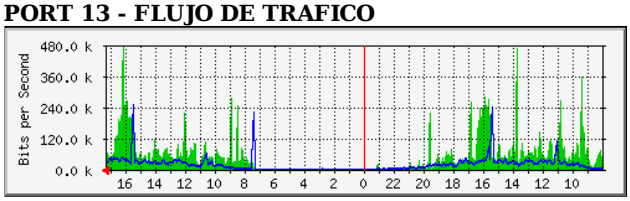
PORT 11 - FLUJO DE TRAFICO



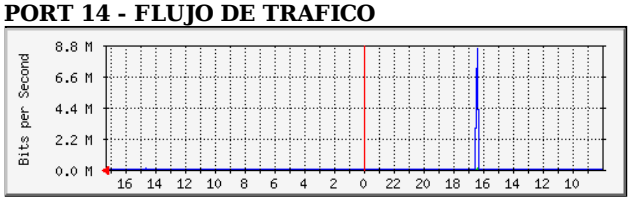
PORT 12 - FLUJO DE TRAFICO



PORT 13 - FLUJO DE TRAFICO



PORT 14 - FLUJO DE TRAFICO

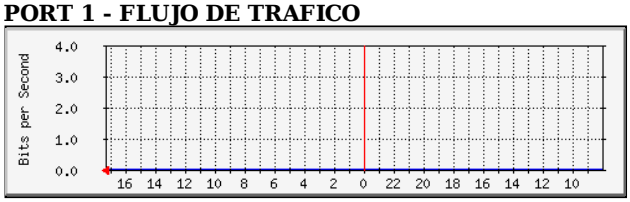


PORT 15 - FLUJO DE TRAFICO

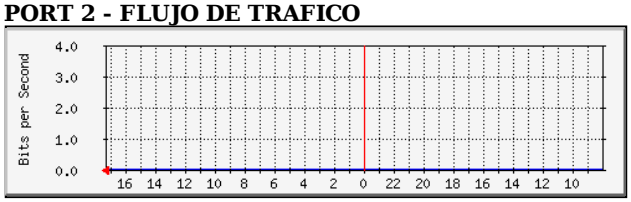
PORT 16 - FLUJO DE TRAFICO

SW MORFEO - FIUBA

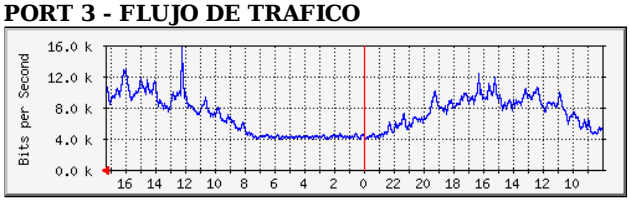
PORT 1 - FLUJO DE TRAFICO



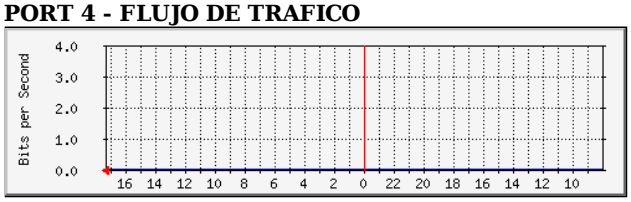
PORT 2 - FLUJO DE TRAFICO



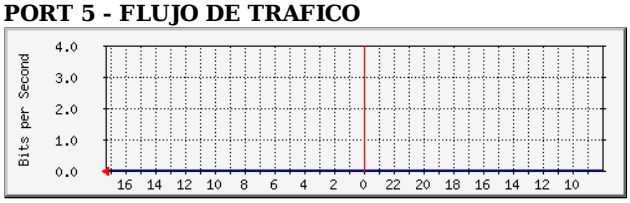
PORT 3 - FLUJO DE TRAFICO



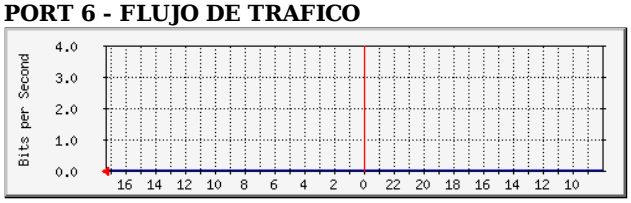
PORT 4 - FLUJO DE TRAFICO



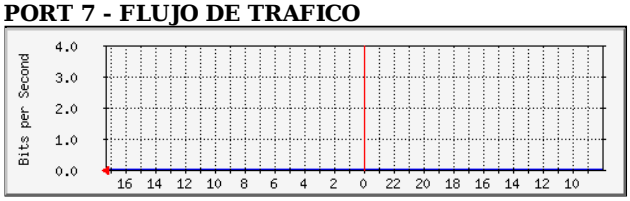
PORT 5 - FLUJO DE TRAFICO



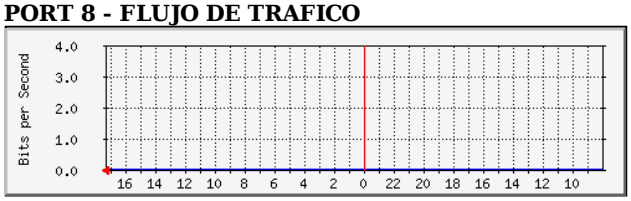
PORT 6 - FLUJO DE TRAFICO



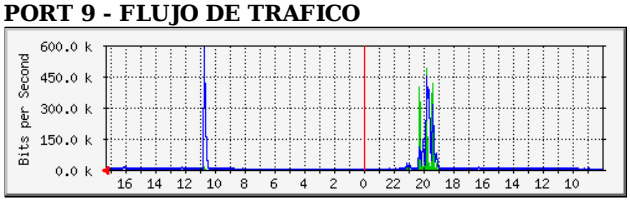
PORT 7 - FLUJO DE TRAFICO



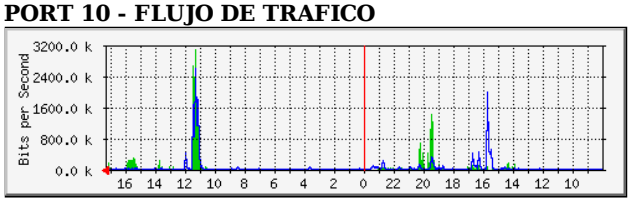
PORT 8 - FLUJO DE TRAFICO



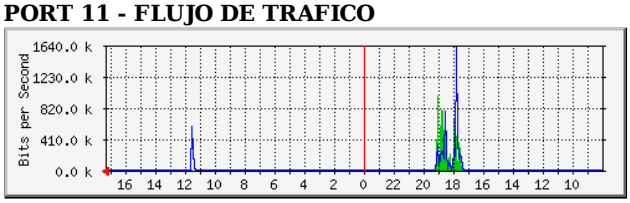
PORT 9 - FLUJO DE TRAFICO



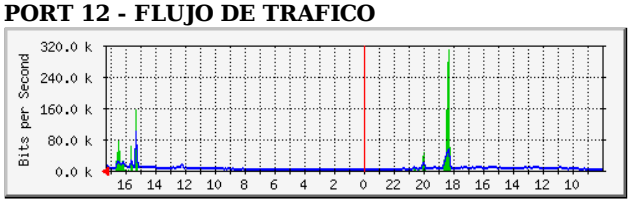
PORT 10 - FLUJO DE TRAFICO



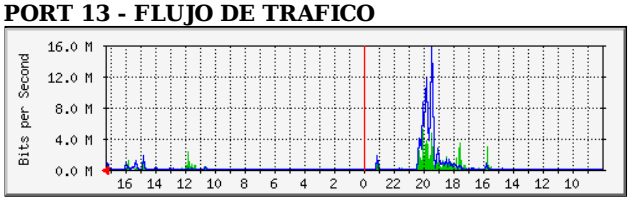
PORT 11 - FLUJO DE TRAFICO



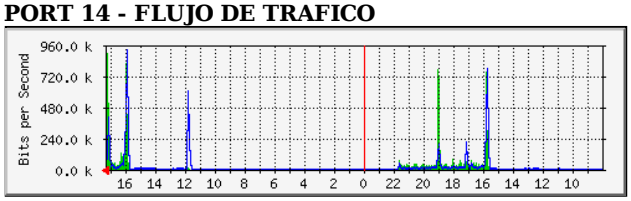
PORT 12 - FLUJO DE TRAFICO



PORT 13 - FLUJO DE TRAFICO



PORT 14 - FLUJO DE TRAFICO

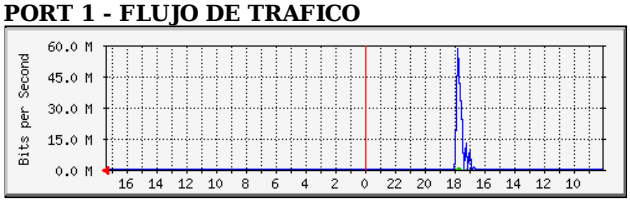


PORT 15 - FLUJO DE TRAFICO

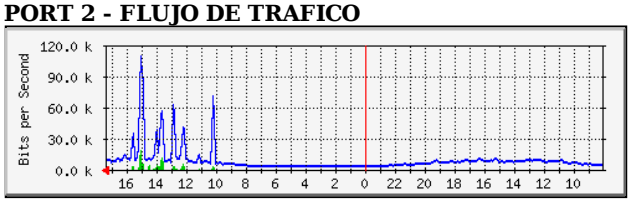
PORT 16 - FLUJO DE TRAFICO

SW 205 - FIUBA

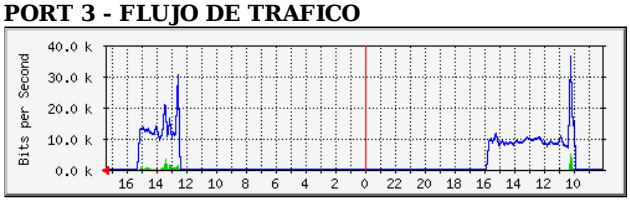
PORT 1 - FLUJO DE TRAFICO



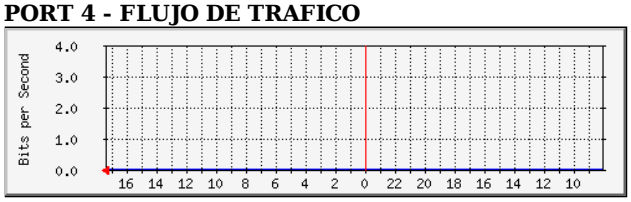
PORT 2 - FLUJO DE TRAFICO



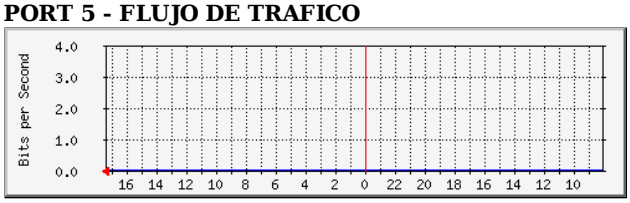
PORT 3 - FLUJO DE TRAFICO



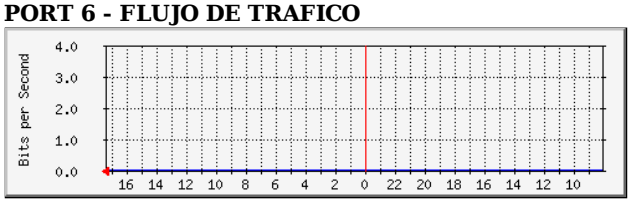
PORT 4 - FLUJO DE TRAFICO



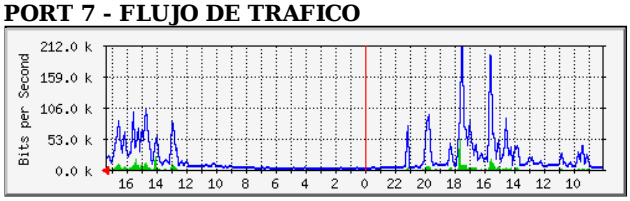
PORT 5 - FLUJO DE TRAFICO



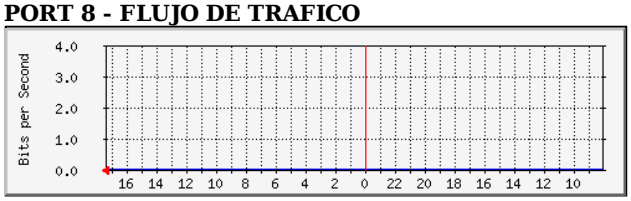
PORT 6 - FLUJO DE TRAFICO



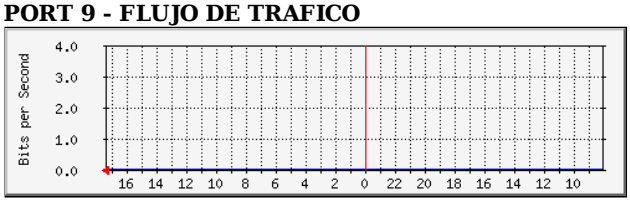
PORT 7 - FLUJO DE TRAFICO



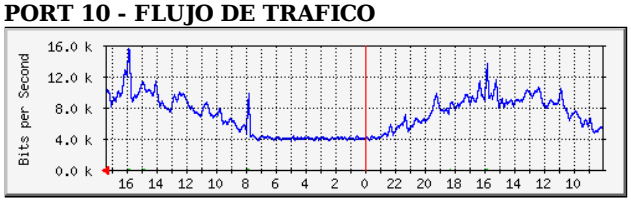
PORT 8 - FLUJO DE TRAFICO



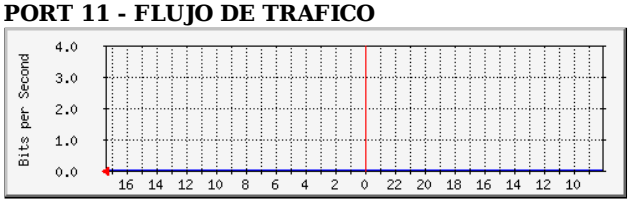
PORT 9 - FLUJO DE TRAFICO



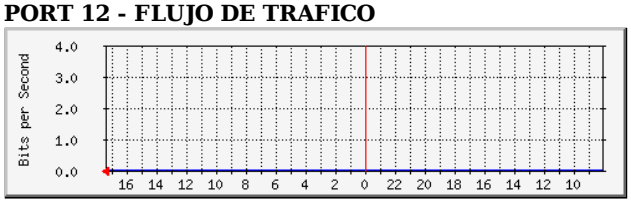
PORT 10 - FLUJO DE TRAFICO



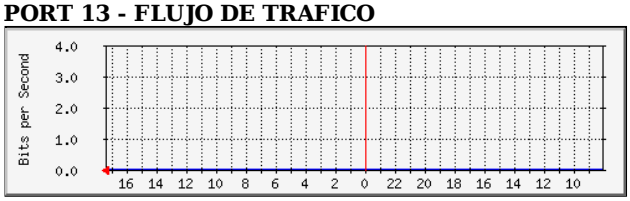
PORT 11 - FLUJO DE TRAFICO



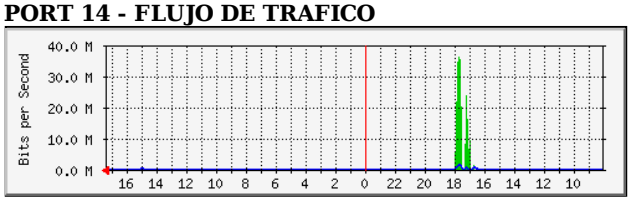
PORT 12 - FLUJO DE TRAFICO



PORT 13 - FLUJO DE TRAFICO



PORT 14 - FLUJO DE TRAFICO

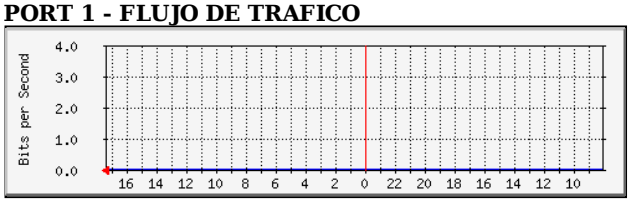


PORT 15 - FLUJO DE TRAFICO

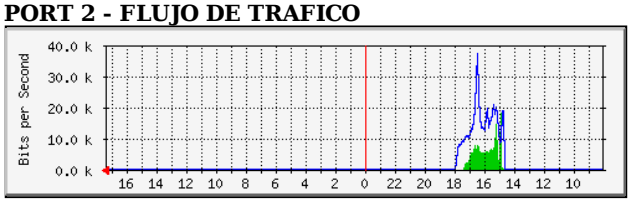
PORT 16 - FLUJO DE TRAFICO

SW FISICA - FIUBA

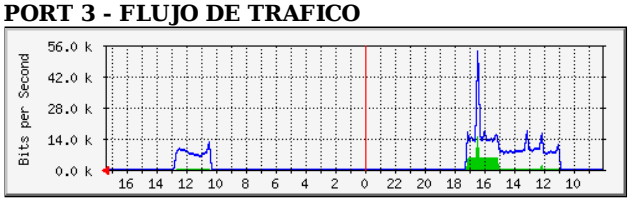
PORT 1 - FLUJO DE TRAFICO



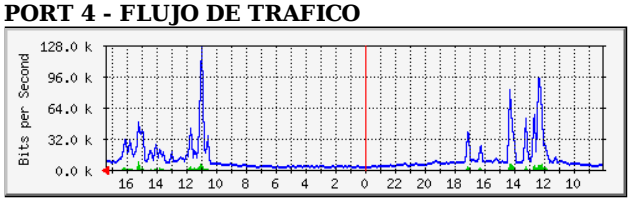
PORT 2 - FLUJO DE TRAFICO



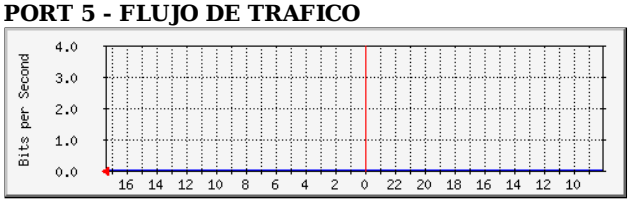
PORT 3 - FLUJO DE TRAFICO



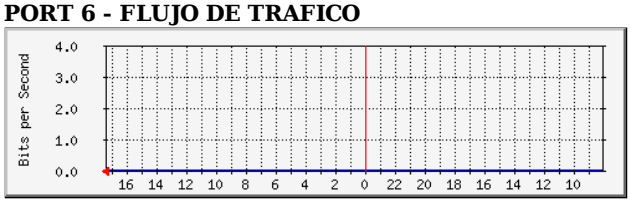
PORT 4 - FLUJO DE TRAFICO



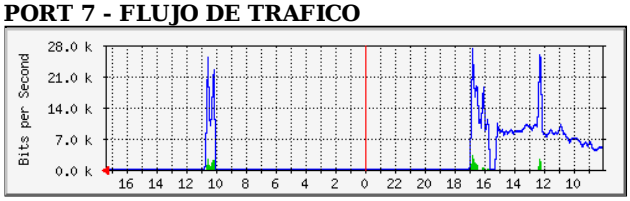
PORT 5 - FLUJO DE TRAFICO



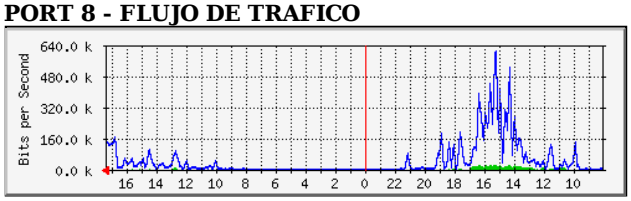
PORT 6 - FLUJO DE TRAFICO



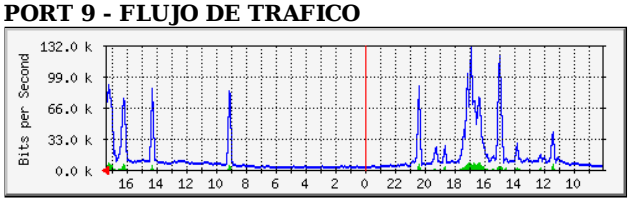
PORT 7 - FLUJO DE TRAFICO



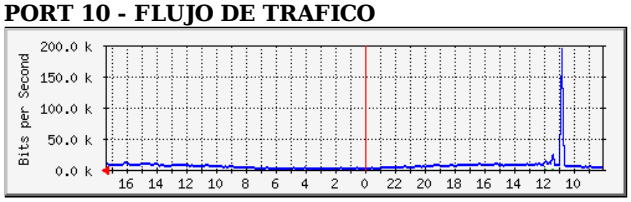
PORT 8 - FLUJO DE TRAFICO



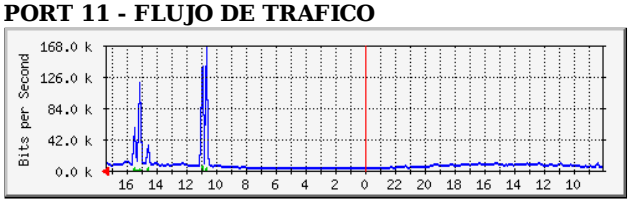
PORT 9 - FLUJO DE TRAFICO



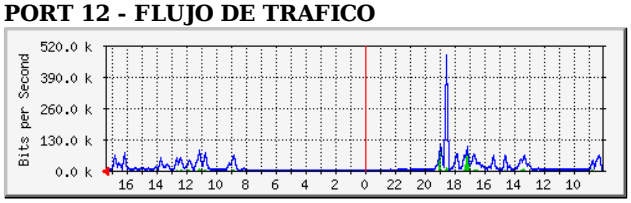
PORT 10 - FLUJO DE TRAFICO



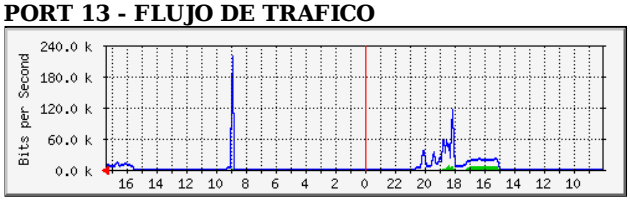
PORT 11 - FLUJO DE TRAFICO



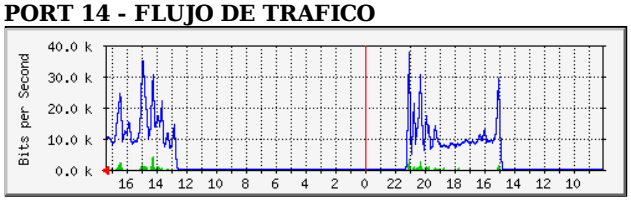
PORT 12 - FLUJO DE TRAFICO



PORT 13 - FLUJO DE TRAFICO



PORT 14 - FLUJO DE TRAFICO

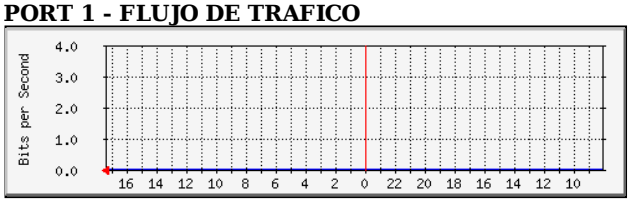


PORT 15 - FLUJO DE TRAFICO

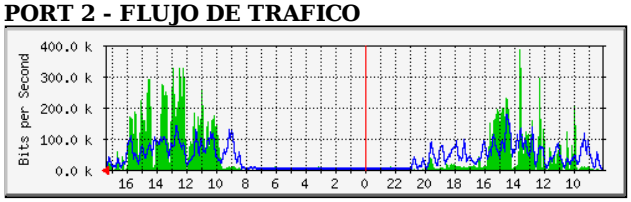
PORT 16 - FLUJO DE TRAFICO

SW BIBLIOTECA - FIUBA

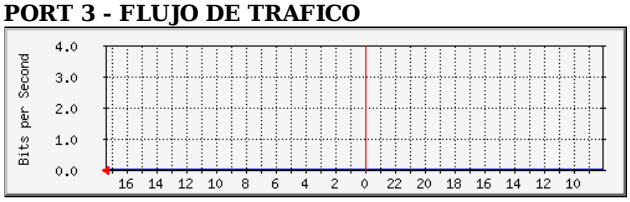
PORT 1 - FLUJO DE TRAFICO



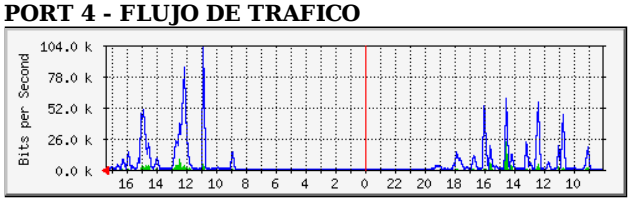
PORT 2 - FLUJO DE TRAFICO



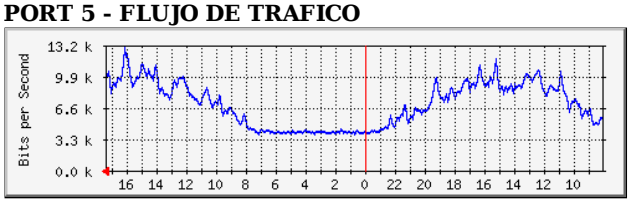
PORT 3 - FLUJO DE TRAFICO



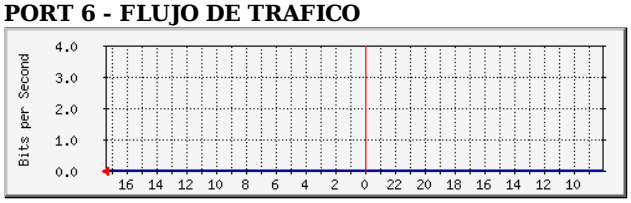
PORT 4 - FLUJO DE TRAFICO



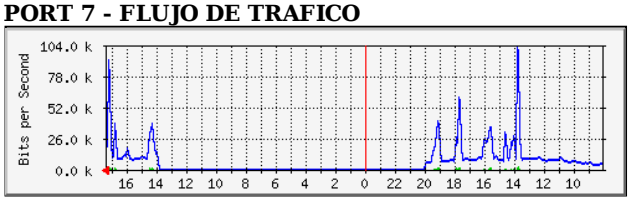
PORT 5 - FLUJO DE TRAFICO



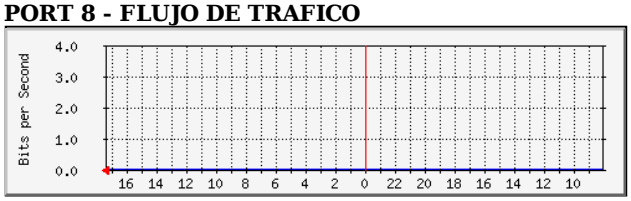
PORT 6 - FLUJO DE TRAFICO



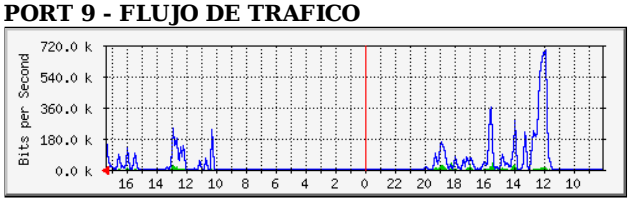
PORT 7 - FLUJO DE TRAFICO



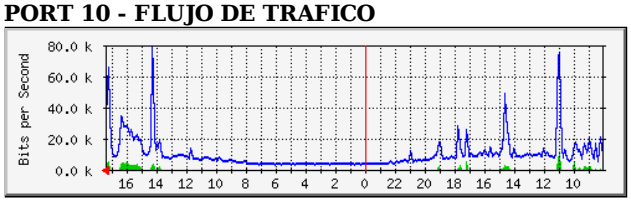
PORT 8 - FLUJO DE TRAFICO



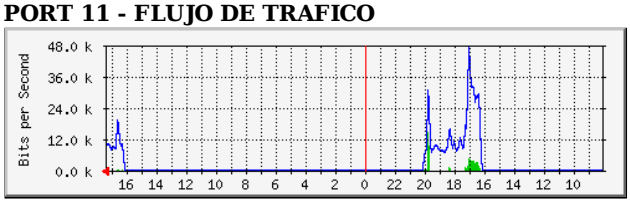
PORT 9 - FLUJO DE TRAFICO



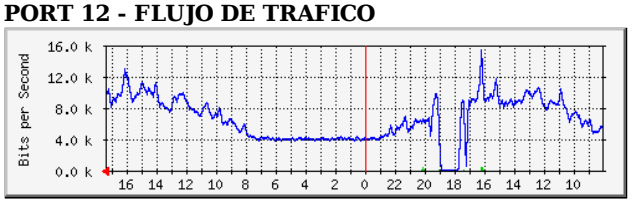
PORT 10 - FLUJO DE TRAFICO



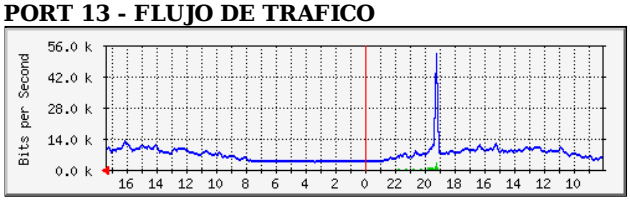
PORT 11 - FLUJO DE TRAFICO



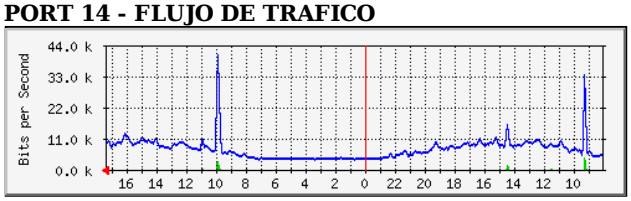
PORT 12 - FLUJO DE TRAFICO



PORT 13 - FLUJO DE TRAFICO



PORT 14 - FLUJO DE TRAFICO

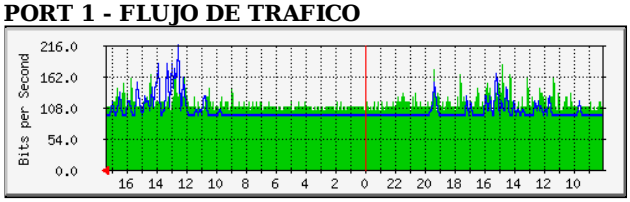


PORT 15 - FLUJO DE TRAFICO

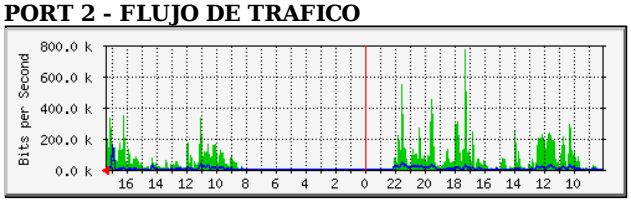
PORT 16 - FLUJO DE TRAFICO

SW SECID - FIUBA

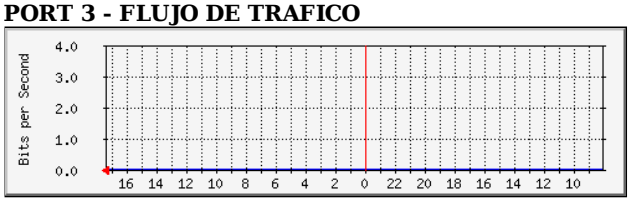
PORT 1 - FLUJO DE TRAFICO



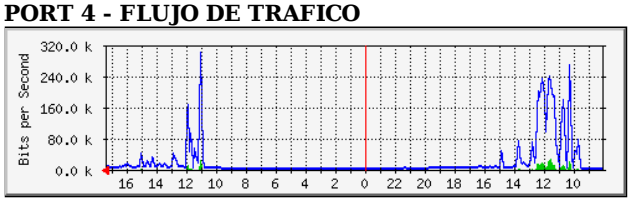
PORT 2 - FLUJO DE TRAFICO



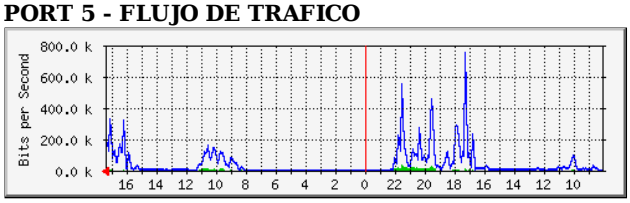
PORT 3 - FLUJO DE TRAFICO



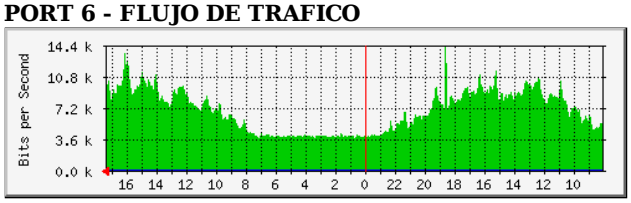
PORT 4 - FLUJO DE TRAFICO



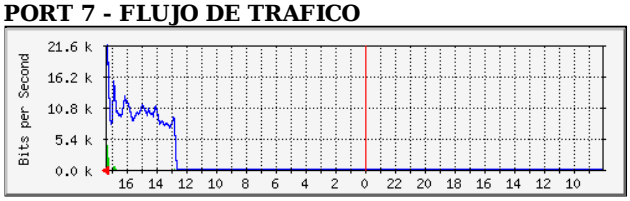
PORT 5 - FLUJO DE TRAFICO



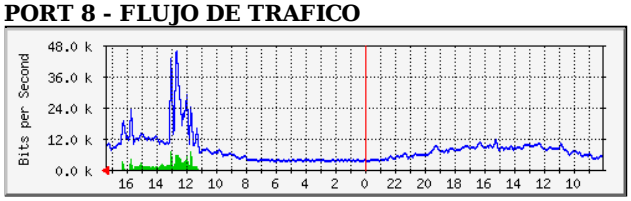
PORT 6 - FLUJO DE TRAFICO



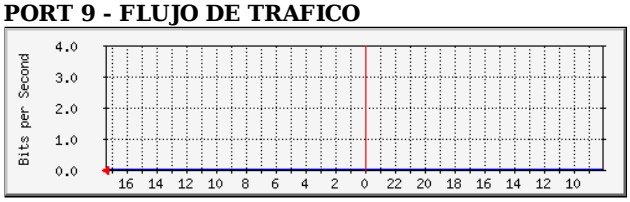
PORT 7 - FLUJO DE TRAFICO



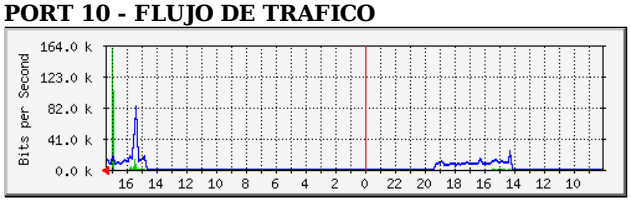
PORT 8 - FLUJO DE TRAFICO



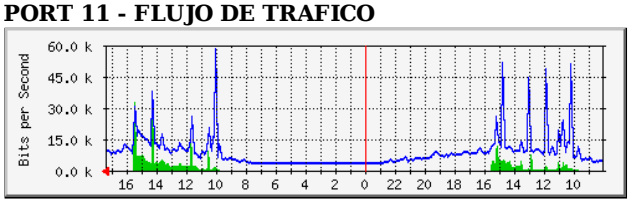
PORT 9 - FLUJO DE TRAFICO



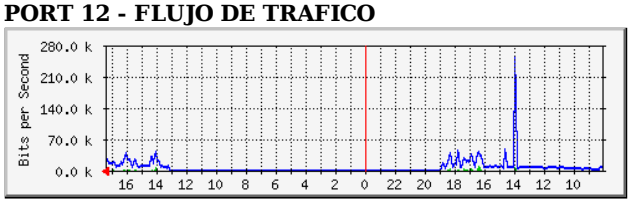
PORT 10 - FLUJO DE TRAFICO



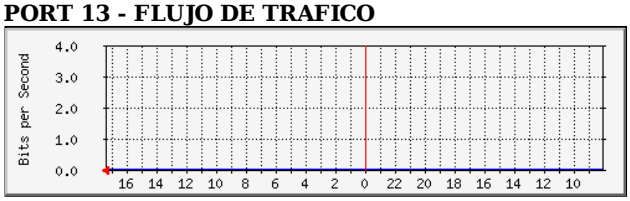
PORT 11 - FLUJO DE TRAFICO



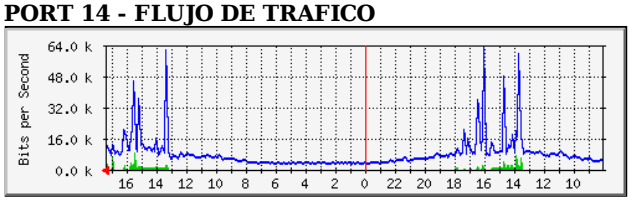
PORT 12 - FLUJO DE TRAFICO



PORT 13 - FLUJO DE TRAFICO



PORT 14 - FLUJO DE TRAFICO

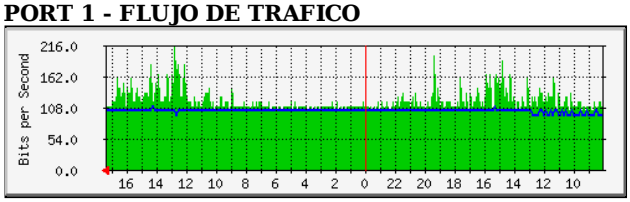


PORT 15 - FLUJO DE TRAFICO

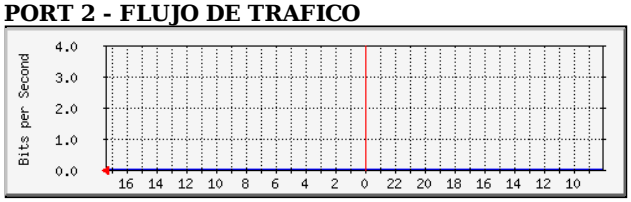
PORT 16 - FLUJO DE TRAFICO

SW COMPUTACION - FIUBA

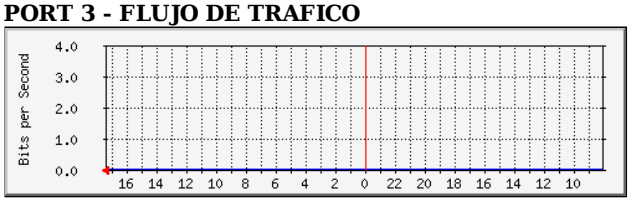
PORT 1 - FLUJO DE TRAFICO



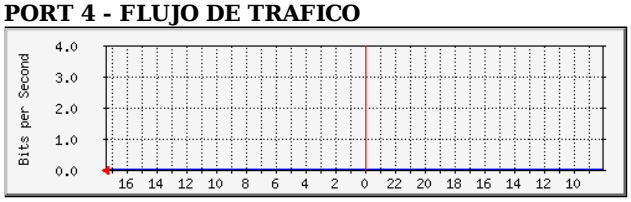
PORT 2 - FLUJO DE TRAFICO



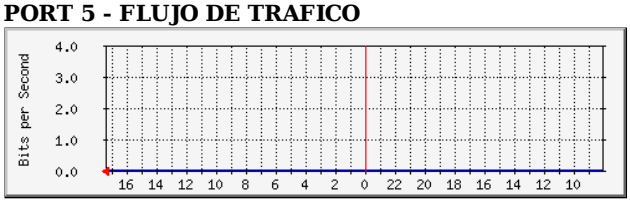
PORT 3 - FLUJO DE TRAFICO



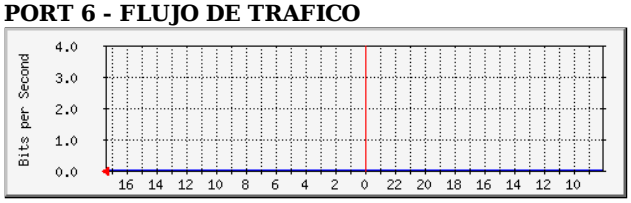
PORT 4 - FLUJO DE TRAFICO



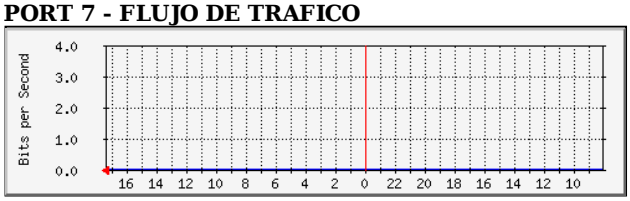
PORT 5 - FLUJO DE TRAFICO



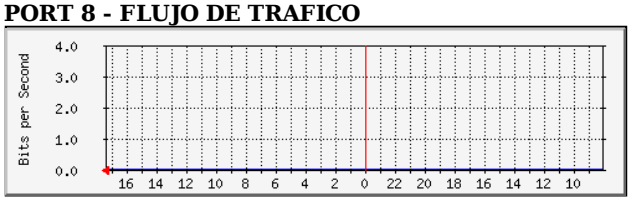
PORT 6 - FLUJO DE TRAFICO



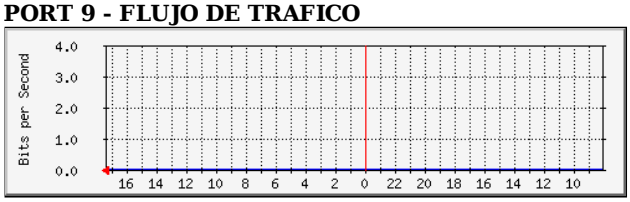
PORT 7 - FLUJO DE TRAFICO



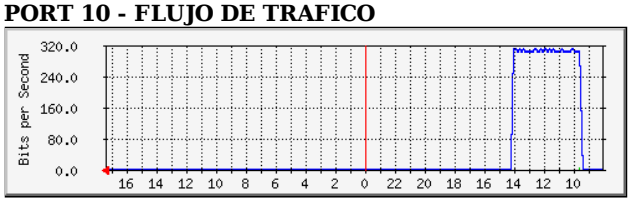
PORT 8 - FLUJO DE TRAFICO



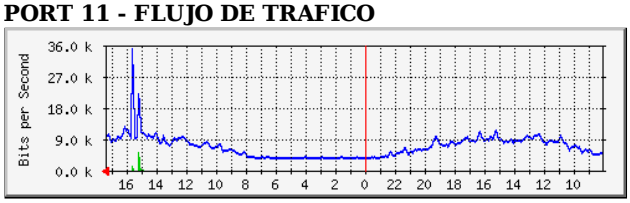
PORT 9 - FLUJO DE TRAFICO



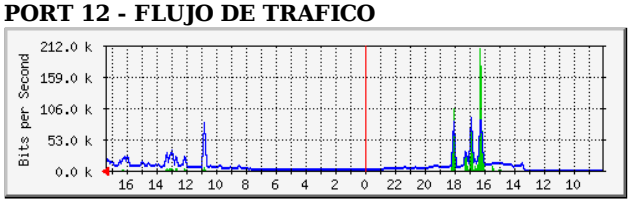
PORT 10 - FLUJO DE TRAFICO



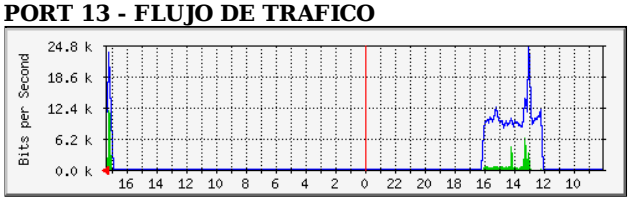
PORT 11 - FLUJO DE TRAFICO



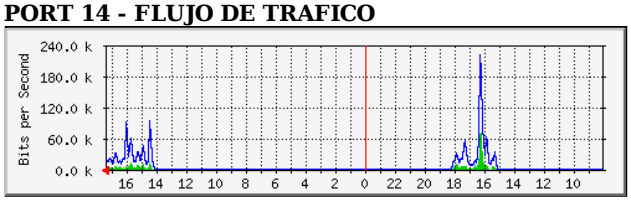
PORT 12 - FLUJO DE TRAFICO



PORT 13 - FLUJO DE TRAFICO



PORT 14 - FLUJO DE TRAFICO

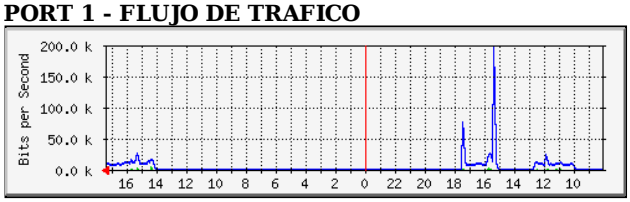


PORT 15 - FLUJO DE TRAFICO

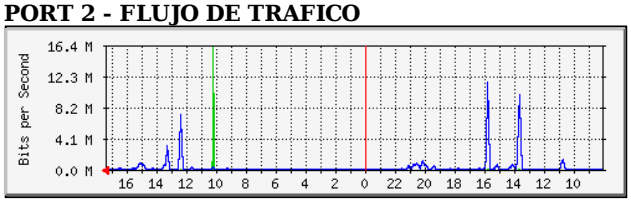
PORT 16 - FLUJO DE TRAFICO

SW INTI - FIUBA

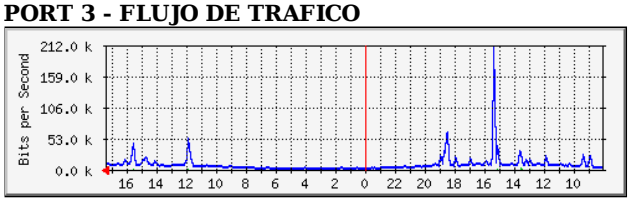
PORT 1 - FLUJO DE TRAFICO



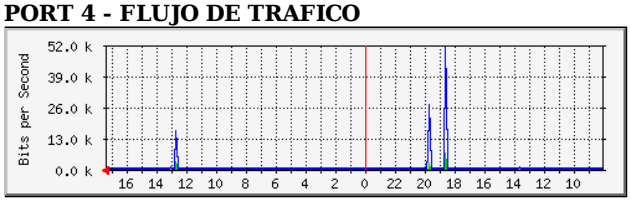
PORT 2 - FLUJO DE TRAFICO



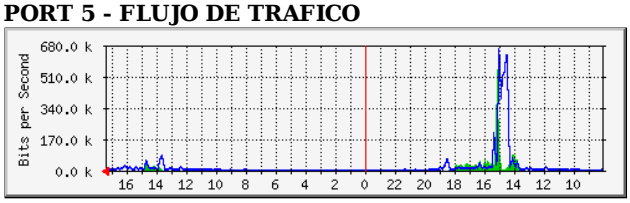
PORT 3 - FLUJO DE TRAFICO



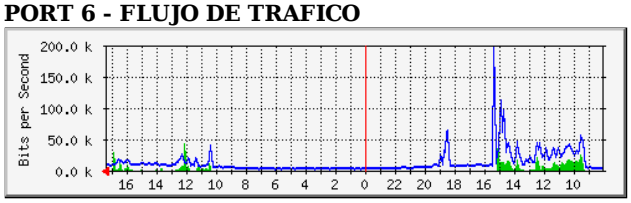
PORT 4 - FLUJO DE TRAFICO



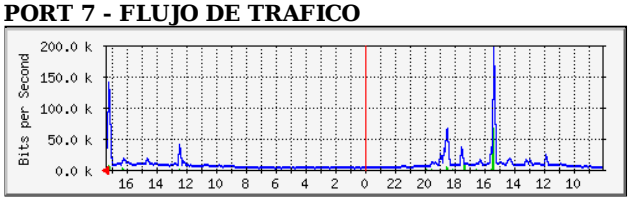
PORT 5 - FLUJO DE TRAFICO



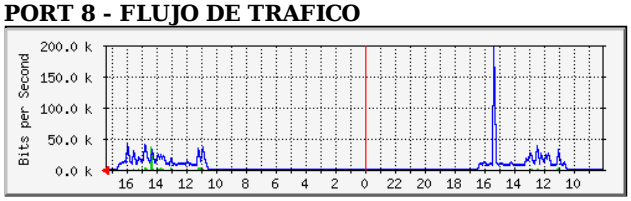
PORT 6 - FLUJO DE TRAFICO



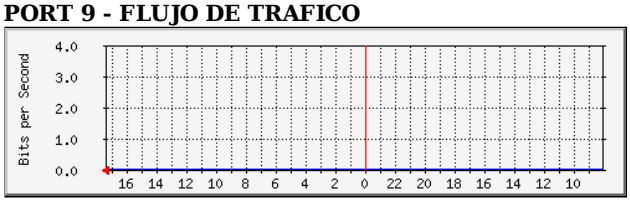
PORT 7 - FLUJO DE TRAFICO



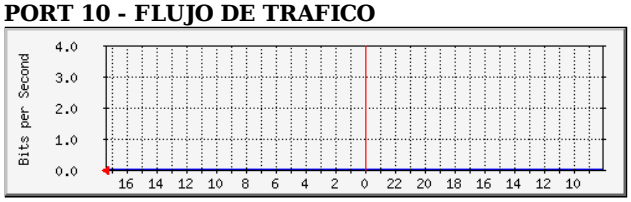
PORT 8 - FLUJO DE TRAFICO



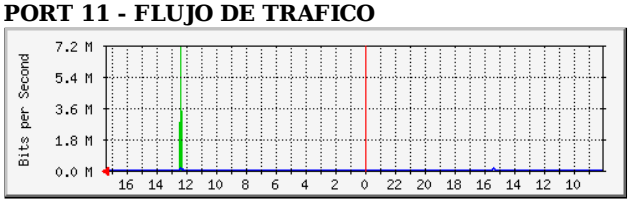
PORT 9 - FLUJO DE TRAFICO



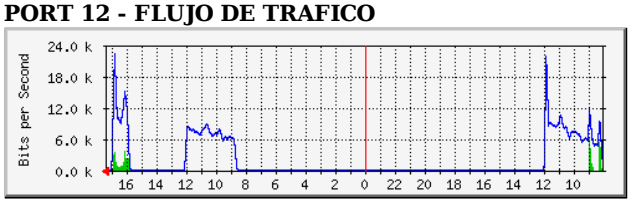
PORT 10 - FLUJO DE TRAFICO



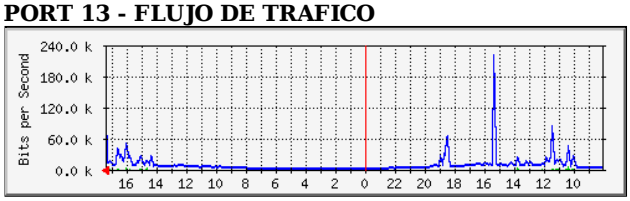
PORT 11 - FLUJO DE TRAFICO



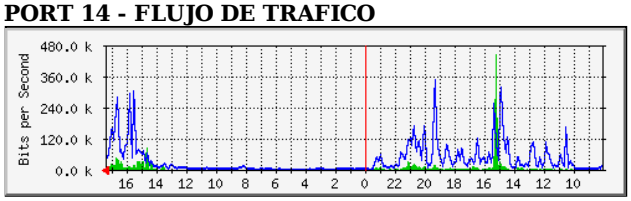
PORT 12 - FLUJO DE TRAFICO



PORT 13 - FLUJO DE TRAFICO



PORT 14 - FLUJO DE TRAFICO

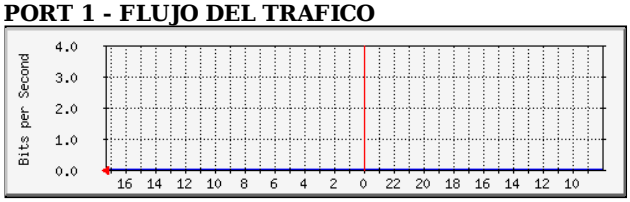


PORT 15 - FLUJO DE TRAFICO

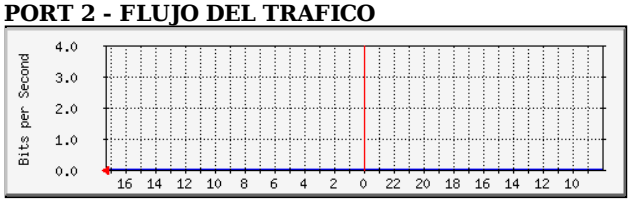
PORT 16 - FLUJO DE TRAFICO

SW BIOMEDICA - FIUBA

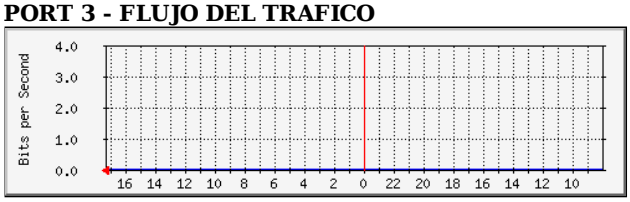
PORT 1 - FLUJO DEL TRAFICO



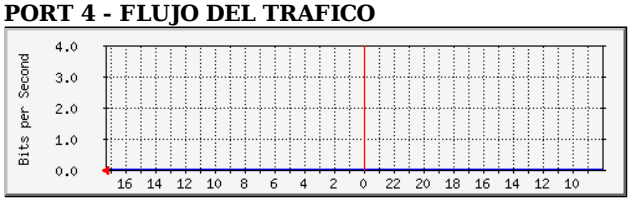
PORT 2 - FLUJO DEL TRAFICO



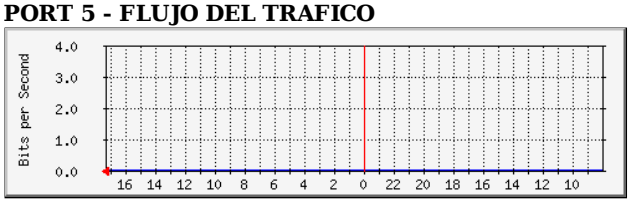
PORT 3 - FLUJO DEL TRAFICO



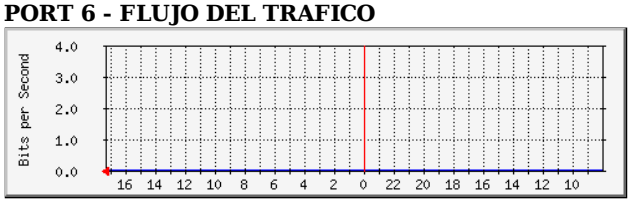
PORT 4 - FLUJO DEL TRAFICO



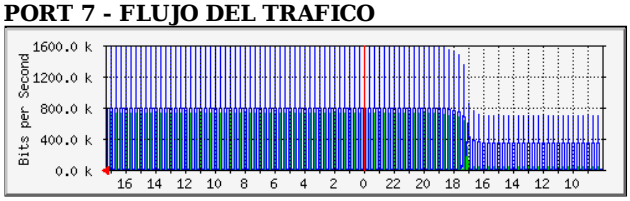
PORT 5 - FLUJO DEL TRAFICO



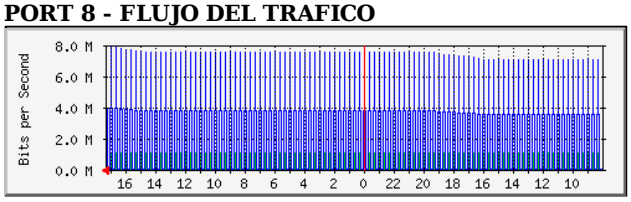
PORT 6 - FLUJO DEL TRAFICO



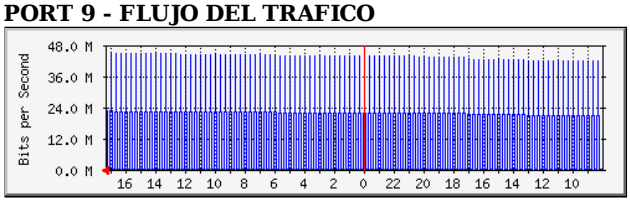
PORT 7 - FLUJO DEL TRAFICO



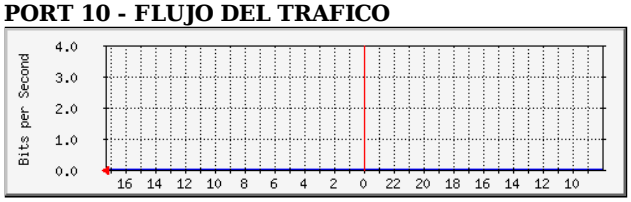
PORT 8 - FLUJO DEL TRAFICO



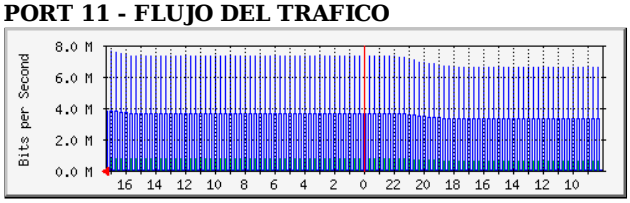
PORT 9 - FLUJO DEL TRAFICO



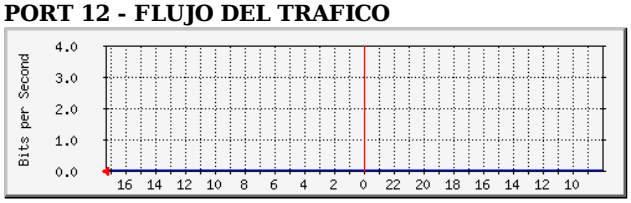
PORT 10 - FLUJO DEL TRAFICO



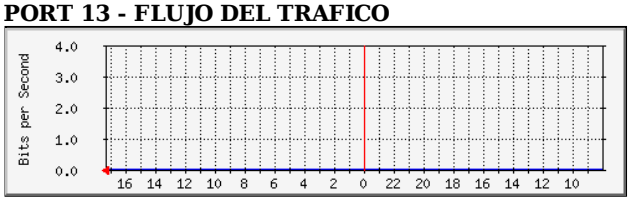
PORT 11 - FLUJO DEL TRAFICO



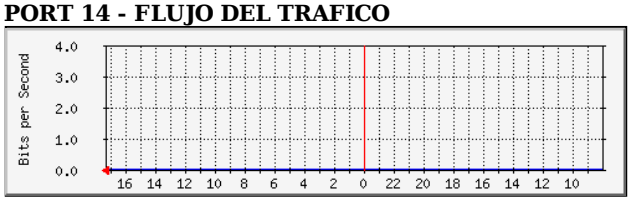
PORT 12 - FLUJO DEL TRAFICO



PORT 13 - FLUJO DEL TRAFICO



PORT 14 - FLUJO DEL TRAFICO

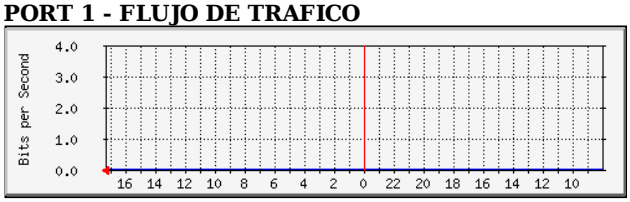


PORT 15 - FLUJO DEL TRAFICO

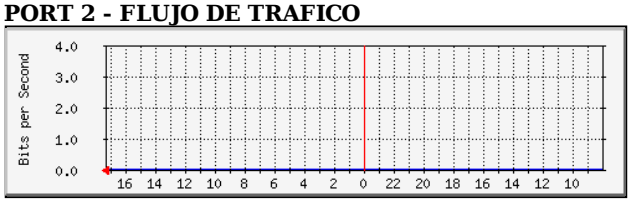
PORT 16 - FLUJO DEL TRAFICO

SW QUIMICA - FIUBA

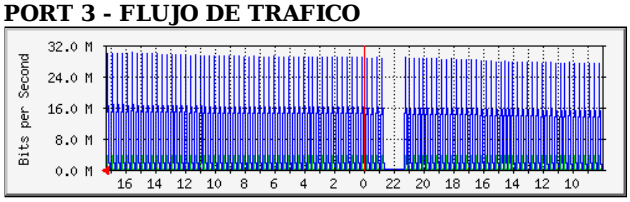
PORT 1 - FLUJO DE TRAFICO



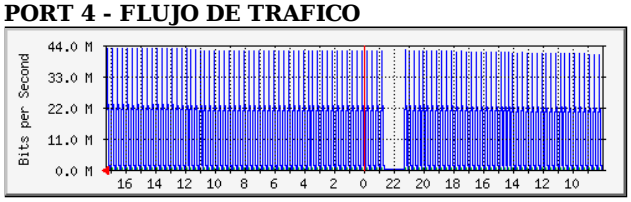
PORT 2 - FLUJO DE TRAFICO



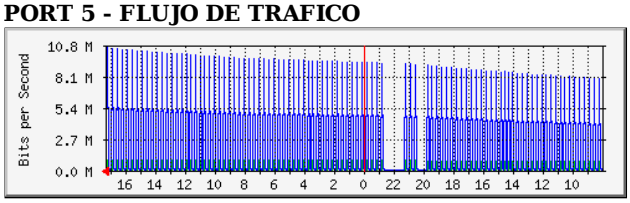
PORT 3 - FLUJO DE TRAFICO



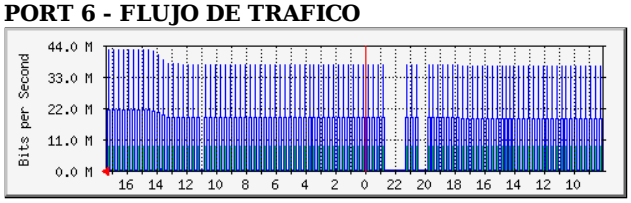
PORT 4 - FLUJO DE TRAFICO



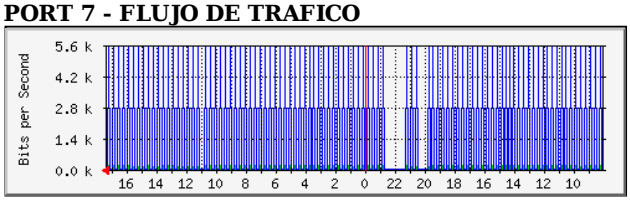
PORT 5 - FLUJO DE TRAFICO



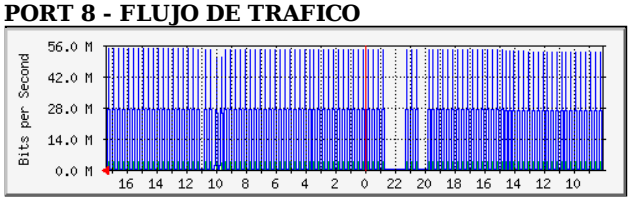
PORT 6 - FLUJO DE TRAFICO



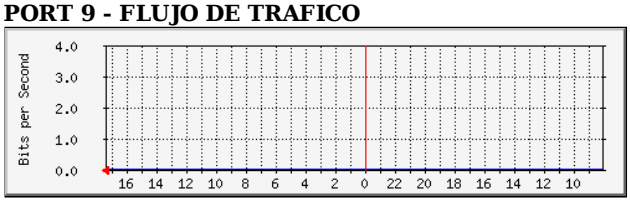
PORT 7 - FLUJO DE TRAFICO



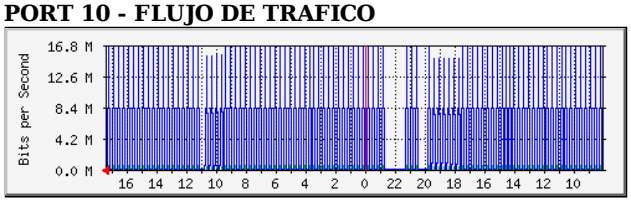
PORT 8 - FLUJO DE TRAFICO



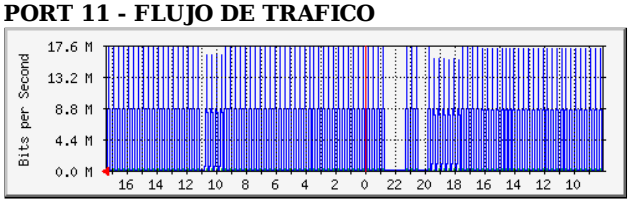
PORT 9 - FLUJO DE TRAFICO



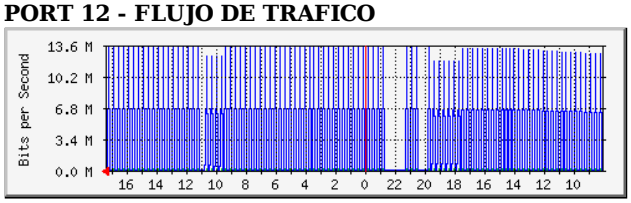
PORT 10 - FLUJO DE TRAFICO



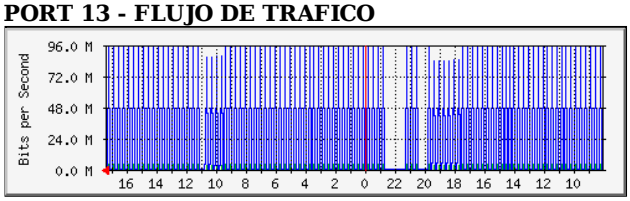
PORT 11 - FLUJO DE TRAFICO



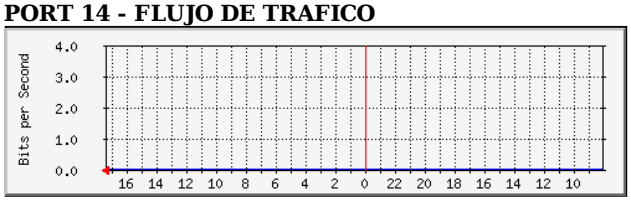
PORT 12 - FLUJO DE TRAFICO



PORT 13 - FLUJO DE TRAFICO



PORT 14 - FLUJO DE TRAFICO



PORT 15 - FLUJO DE TRAFICO

PORT 16 - FLUJO DE TRAFICO

Bibliografía

[BEL91] Bellamy J. *Digital Telephony*. New York: Wiley, 1991.

[COM00] Comer Douglas E. *Internetworking with TCP/IP Vol.1: Principles, Protocols, and Architecture (4th Edition)*. Prentice Hall Inc., 2000.

[G&H03] García, Enrique Villamil & García Hernández, Miguel J. *Introducción al Proyecto de Ingeniería*. Prentice Hall Inc., 2000.

[SKL01] Sklar, Bernard. *Digital Communications, Fundamentals and Applications*. Prentice Hall Inc., 2001.

[STA00] Stallings, William. *Data and Computer Communications*, Prentice Hall Inc., 2000.

[B&G92] Bertsekas, D. & Gallager, R. *Data Networks, 2nd edn.*. Prentice-Hall International Editions, 1992.

[SA&D] Kenneth E. Kendall, Julie E Kendall *Systems Analysis and Design (7th Edition)*Prentice Hall; 7 edition, 2007.

[MCS95] Couch, Leon W. *Modern Communications Systems*. Prentice-Hall, 1995.

[DCS87] Peebles, Peyton Z. *Digital Communications Systems*. Prentice-Hall, 1987.

[MCT89] Lee, William C. Y. *Mobile Cellular Telecommunications Systems McGraw-Hill*, 1989.

[SSS94] Dixon, Robert C.*Spread Spectrum Systems*. John Wiley & Sons, 1994.

[802.3] IEEE Std 802.3ae. *Ethernet Standard*, American National Standards Institute, 2002.

[568-B] ANSI/TIA/EIA-568-B. *Commercial Building Telecommunications Cabling Standard*. TIA e EIA, 2001.

[LAM80] Lam, S. *A carrier sence multiple access protocol for local networks. Computer Networks*,1980.

[C&B03] Castoldi, Fernando Ariel (74.367) & Bozzuto, Javier (71.726). *Infraestructura de la red de área local Fiuba*, 2003.

[M&G03] Mora, Santiago (76256) & Gallego, José Fransisco (76791). *Estudio de la red UBA*, 2003.

[CISSLA] Cisco Systems, Inc. *Cisco IOS IP SLAs Configuration Guide*. Release 12.4, 2008.

[TDUSO] Tendencias Digitales. *Indicadores de usos de Internet en Latinoamérica*. 2008.

[IEEES] IEEE Espectrum, The magazine of technology insiders, vol 46 number 1 *You next computer will probably be a Notebook*. 2009.

[LBA98] Jim Zyren and Al Petrick *Aplication Note on Link Budget Analysis*. 1998.