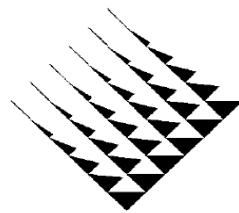


**INSTITUTO TECNOLÓGICO DE COSTA RICA  
ESCUELA DE INGENIERÍA ELECTRÓNICA**



**TEC**

---

Instituto Tecnológico de Costa Rica  
Escuela de Ingeniería Electrónica

**INFORME DE PROYECTO DE GRADUACIÓN PARA OPTAR POR EL TÍTULO DE  
INGENIERO EN ELECTRÓNICA CON EL GRADO ACADÉMICO DE  
LICENCIATURA**

“PROPUESTA PARA LA OPTIMIZACIÓN DE LA RED INALÁMBRICA DE AREA LOCAL (WLAN) EN LAS OFICINAS CENTRALES DE LA CORPORACIÓN DE SUPERMERCADOS UNIDOS MEDIANTE LA MEJORA EN LA CONFIGURACIÓN DE LOS PUNTOS DE ACCESO (ACCESS POINTS).”

**EMPRESA**

CORPORACIÓN DE SUPERMERCADOS UNIDOS (C.S.U.)

**ESTUDIANTE**

JORGE EDUARDO CALVO ROMÁN

**CARTAGO, 2003**

**INSTITUTO TECNOLOGICO DE COSTA RICA  
ESCUELA DE INGENIERIA EN ELECTRONICA  
PROYECTO DE GRADUACION**

**TRIBUNAL EVALUADOR**

Ing. Eduardo Interiano Salguero  
Profesor Asesor  
Escuela de Ingeniería en Electrónica  
I.T.C.R.

Firma: \_\_\_\_\_

*Sello*

Ing. Sergio Lewis Beckford  
Asesor por la empresa

Firma: \_\_\_\_\_

Corporación de Supermercados Unidos  
C.S.U

*Sello*

Los miembros de este tribunal dan fe de que el presente trabajo de graduación ha sido aprobado y cumple con las normas establecidas por las Instituciones involucradas en la ejecución de este proyecto.

Oficinas Centrales CSU, 24 de Julio del 2003

## **DEDICATORIA**

Dedico el presente trabajo a aquellas personas que he tenido la dicha de conocer y que han permanecido cerca de mí durante todo este tiempo, brindándome su amistad incondicional y el apoyo emocional en los momentos difíciles de mi vida, para mantenerme en la lucha y no desfallecer ante las adversidades en mi esfuerzo por conseguir tan anhelado título universitario.

## **AGRADECIMIENTO**

En primera instancia deseo dar gracias a Dios por haberme acompañando a lo largo de mis estudios y por haberme permitido alcanzar esta meta tan anhelada.

En segundo lugar, agradezco a mis padres Jorge Eduardo Calvo Calvo y Flor María Román Zeledón, por haberme regalado el don de la vida y por enseñarme todo aquello que no se aprende ni en la mejor universidad del mundo, la paciencia y la perseverancia.

Agradezco el apoyo, confianza y la transferencia de conocimiento brindado por parte mi asesor en la empresa, el Ing. Sergio Lewis Beckford, quien me permitió ampliar la visión acerca de los sistemas inalámbricos a corto plazo y el impacto a futuro de éstos en los negocios donde un acceso flexible del Internet es vital, así como lo es para la Corporación de Supermercados Unidos C.S.U.

Doy gracias a todas aquellas personas que laboran en el departamento de Tecnología de la Información por aceptarme y hacerme sentir como parte de la familia de CSU, así como por la ayuda brindada de alguna u otra manera. Gracias especiales a Mauricio y el resto de sus colaboradores en el departamento de Soporte Técnico. Asimismo, agradezco a Allan Jinesta por permitirme elaborar este proyecto en el departamento que está bajo su cargo .

Agradezco además al director de la Escuela de Ingeniería Electrónica el Ing. Luis Paulino Méndez por su comprensión así como a mi profesor asesor Ing. Eduardo Interiano por dirigirme acertadamente hacia la finalización exitosa de este proyecto. También al Ing. Pedro Murillo, Coordinador del Proyecto de Graduación por su labor.

## RESUMEN

En los últimos años la tecnología ha alcanzado logros sin precedentes, especialmente en el ambiente de las comunicaciones inalámbricas móviles. Vemos como hoy en día cada vez más y más personas se ven utilizando artefactos inalámbricos como por ejemplo los celulares, pues éstos vienen a ser de mucha ayuda en los quehaceres del trabajo o en bien en sus otras actividades diarias; esto ya que les permiten mantenerse en contacto con sus allegados desde cualquier parte de este mundo y a cualquier hora día.

Esta accesibilidad y facilidad de las comunicaciones inalámbricas en celulares, también han venido tomando fuerza en el mundo de las redes de datos, ya sean estas en áreas locales como en largas distancias. El mismo concepto de movilidad mencionado anteriormente, ha venido cautivando cada día a más empresas quienes ven en las *LAN* inalámbricas muchas ventajas en comparación con las “rígidas” redes *LAN* tradicionales, como lo es el hecho de: movilidad de los equipos, rápida instalación de nuevas terminales, capacidad de trasladarse a través de diferentes puntos de acceso sin perder conexión, uso en ubicaciones temporales, facilidad de administración entre otras facilidades.

Las redes *WLAN* son un complemento de las *LAN* tradicionales, particularmente cuando se realizan grandes soluciones industriales donde se requiere que las estaciones estén localizadas donde se genera la información. Anteriormente no se promovía el desarrollo de las *WLAN* por falta de un estándar industrial que lo rigiera, pero esto se ha venido a solucionar con la aparición y ratificación del estándar IEEE 802.11 para *WLAN*.

## ABSTRACT

*In the lastest years, the technology had reached many achievements specially in the wireless mobile communication field. We saw today how the use of wireless devices is rising everyday specially the use of celular phones. This is because of the versatibility it has in the job activities or any other daily activity, in keeping close the person with his/her family or co-workers at any time and any place over the world.*

*This facility offered by wireless communications in mobile phones, is also taking force in the field of data networks, either in local areas or long distances. The same conception mencioned latetly in mobility, has impressed the enterprises which expect more advantages in comparison with tradicional wired networks. Some of the advantages they saw in this technology is the fact that they offer equipment mobility, faster installation, roaming by the entire building without loosing internet connexion and the easy administration it provides.*

*Wireless LAN are a complement of tradicional wired networks, specially when you are doing big industrial solutions were it requires that the stations be located at the source. Previously the WLAN solutions weren't promoted because they didn't have a regulatory standard, but it was solved with the appearence of IEEE 802.11 standard for wireless LAN.*

## ÍNDICE GENERAL DE CONTENIDOS

DEDICATORIA.....	III
AGRADECIMIENTO .....	IV
RESUMEN .....	V
ABSTRACT .....	VI
INDICE DE FIGURAS .....	XI
CAPITULO 1: DESCRIPCIÓN DEL PROYECTO.....	15
1.1. DESCRIPCIÓN DE LA EMPRESA.....	15
1.2. DESCRIPCIÓN DETALLADA DEL PROBLEMA A RESOLVER Y SUS EFECTOS.....	17
1.3. OBJETIVO GENERAL.....	19
1.4. OBJETIVOS ESPECÍFICOS .....	20
CAPITULO 2: ANTECEDENTES DEL PROYECTO.....	21
2.1. ESTUDIO DEL PROBLEMA.....	21
2.2. SOLUCION PROPUESTA.....	22
CAPITULO 3: PROCEDIMIENTO METODOLOGICO .....	23
3.1. METODOLOGIA.....	23
CAPITULO 4: MARCO TEORICO DE LOS SISTEMAS DE RED INALAMBRICOS .....	26
4.1. MARCO TEORICO DE TECNOLOGÍAS LAN .....	26
4.1.1. Funcionamiento básico de una red LAN.....	26
4.1.2. Trama <i>Ethernet</i> 802.3 .....	28
4.1.3. Características de las redes LAN.....	29
4.2. MARCO TEORICO DE TECNOLOGÍAS WLAN.....	30
4.2.1. Funcionamiento básico de una WLAN.....	30
4.2.2. Trama 802.11.....	32
4.2.3. Características de las redes WLAN .....	35
4.2.4. Aspectos de seguridad de WLAN.....	36
4.2.4.1. Protocolo WEP ( <i>Wired Equivalent Protocol</i> ) .....	36
4.2.4.2. Protocolo <i>Secure Shell</i> (SSH).....	38
4.2.5. Factores que afectan la transmisión en redes WLAN.....	40
CAPITULO 5: MARCO TEORICO DE EQUIPOS PARA WLAN.....	42
5.1. EQUIPOS PARA WLAN .....	42
5.1.1. Punto de Acceso AP 350 .....	42
5.1.2. Punto de Acceso AP 1200 .....	45
5.1.3. <i>Client Adapter</i> —Adaptador de red .....	46
5.2. MODOS DE OPERACIÓN DE LOS PUNTOS DE ACCESO.....	46
5.2.1. Unidad Principal ( <i>ROOT UNIT</i> : Configuración por defecto).....	46
5.2.2. Unidad Repetidora ( <i>REPEATER UNIT</i> ) .....	47
5.2.3. Unidad Central ( <i>CENTRAL UNIT</i> ).....	47
5.3. LEDS INDICADORES DEL PUNTO DE ACCESO .....	47
5.3.1. Estado del conexión <i>Ethernet</i> ( <i>Ethernet Status</i> ).....	47
5.3.2. Estado de Operación de señales ( <i>Association Status</i> ) .....	47
5.3.3. Actividad del Tráfico ( <i>Radio Activity</i> ).....	48

CAPITULO 6: ANTENAS PARA LOS SISTEMAS DE RED INALAMBRICOS .....	49
6.1. CONCEPTOS Y PARÁMETROS.....	49
6.1.1. Antenas .....	49
6.1.2. Parámetros eléctricos. ....	50
6.1.2.1. Ganancia .....	50
6.1.2.2. Directividad.....	50
6.1.2.3. Patrón de radiación de una antena. ....	51
6.1.2.4. EIRP (Potencia radiada isotrópica efectiva).....	52
6.1.2.5. Ancho del haz de la antena.....	52
6.1.2.6. Polarización de antena.....	53
6.1.3. Parámetros físicos. ....	53
6.1.3.1. Alcance.....	53
6.1.4. Cables usados para conectar antenas.....	54
6.1.5. Pararrayos.....	55
6.2. TIPOS DE ANTENAS. ....	56
6.2.1. Antenas para adaptadores de red.....	56
6.2.1.1. Antena dipolo AIR-ANT3351.....	56
6.2.1.2. Antena omnidireccional de alta ganancia AIR-ANT1728. ....	57
6.2.1.3. Antena direccional de montaje en pared AIR-ANT3549. ....	58
CAPITULO 7: MARCO TEORICO DEL RECOLECTOR DE DATOS ( <i>LOCUST</i> ) ...	60
7.1. FUNCIONAMIENTO .....	60
7.2. DESCRIPCIÓN FÍSICA .....	60
7.2.1. Descripción de luces indicadoras.....	61
7.2.2. Descripción de funciones por teclas .....	62
7.3. MENUS.....	62
7.3.1. <i>Select AP</i> .....	63
7.3.2. <i>Select PER AP</i> .....	63
7.3.3. <i>Survey Mode</i> .....	64
7.3.4. <i>Scan for AP's</i> .....	64
7.3.5. <i>Spectrum</i> .....	65
CAPITULO 8: GUIA PARA LA INSTALACION DE AP 350 .....	66
8.1. INGRESAR AL PUNTO DE ACCESO AIRONET 350 POR PRIMERA VEZ ...	67
8.2. CREAR UN NUEVO PERFIL DE USUARIO A LA NIC.....	72
8.3. INGRESE A UNA SECCIÓN HTTP PARA CONEXIÓN EN MODO GRÁFICO CON AP.....	74
8.4. DESCRIPCIÓN DE CADA UNO DE LOS PARÁMETROS DEL PUNTO DE ACCESO .....	75
ASSOCIATIONS:.....	81
a) <i>Display Defaults</i> —Despliegue de parámetros por defecto .....	81
b) <i>Address Filters</i> — Filtros de Direcciones .....	82
c) <i>Protocol Filters</i> — Filtros para protocolos .....	84
d) <i>Port Assignments</i> — Asignación de Puertos .....	85
e) <i>VLAN</i> — Redes Virtuales.....	86
f) <i>Advanced</i> — Avanzadas.....	88
g) <i>Service Sets</i> — Fijación de Servicios .....	91



<b>EVENT LOG</b> .....	92
a) <i>Display Defaults</i> — Despliegue de parámetros por defecto .....	92
b) <i>Event Handling</i> — Manipulador de Eventos .....	94
c) <i>Notifications</i> — Notificaciones .....	98
<b>SERVICES</b> .....	101
a) <i>Console/Telnet</i> .....	101
b) <i>Time Server</i> — Servidor de reloj .....	103
c) <i>Cisco Services</i> — Servicios de Cisco .....	104
d) <i>Boot Server</i> — Servidor de arranque .....	120
e) <i>FTP</i> — Protocolo de Transmisión de Archivos .....	125
f) <i>Security</i> — Seguridad .....	126
g) <i>Routing</i> — Enrutamiento .....	128
h) <i>Web Server</i> — Servidor Web .....	129
i) <i>Accounting</i> — Contabilidad .....	131
j) <i>Name Server</i> — Servidor de Nombres .....	134
k) <i>SNMP</i> — Protocolo de manejo simple de la red .....	135
<b>NETWORK PORTS</b> .....	138
1) <i>Ethernet</i> .....	138
a) <i>Identification</i> — Identificación .....	141
b) <i>Hardware</i> .....	142
c) <i>Filters</i> — Filtros .....	144
d) <i>Advance</i> — Avanzado .....	145
2) <i>AP Radio</i> — Puerto de Radio .....	148
a) <i>Identification</i> — Identificación .....	153
b) <i>Hardware</i> .....	155
c) <i>Filters</i> — Filtros .....	159
d) <i>Advance</i> — Avanzado .....	161
<b>DIAGNOSTICS</b> .....	168
<b>EXPRESS SETUP</b> .....	170
<b>CAPITULO 9: GUIA PARA LA INSTALACION DE AP 1200</b> .....	174
9.1. DESCRIPCIÓN DE PARÁMETROS DEL PUNTO DE ACCESO AIRONET 1200 .....	175
<b>ASSOCIATIONS:</b> .....	178
<b>EVENT LOG</b> .....	179
<b>SERVICES</b> .....	179
<b>NETWORK PORTS</b> .....	190
<b>DIAGNOSTICS</b> .....	191
<b>EXPRESS SETUP</b> .....	192
<b>CAPITULO 10: CISCOWORKS FOR WIRELESS (WLSE)</b> .....	193
10.1. WLSE ( <i>WIRELESS LAN SOLUTION ENGINE</i> ) .....	193
10.2. VISIÓN GLOBAL DEL SISTEMA .....	194
10.3. CARACTERÍSTICAS DE APLICACIÓN QUE SIMPLIFICAN LA OPERACIÓN Y EL DESPLIEGUE .....	195
10.4. MEJORAS A NIVEL DE SEGURIDAD .....	198
10.5. MAXIMO RENDIMIENTO Y DISPONIBILIDAD .....	199

10.6. REPORTES Y PLANEAMIENTO.....	200
10.7. MODELOS DE ACCESO BASADO EN LA FUNCIÓN .....	201
10.6. RED ESTRUCTURADA INALÁMBRICA DE CISCO. ....	201
CAPITULO 11: <i>AIRONET CLIENT UTILITY</i> (ACU) VERSION 12.01T.....	203
11.1. INGRESO AL CLIENTE AIRONET.....	203
11.2. DESCRIPCIÓN DE PARÁMETROS DEL MENÚ DE EDICIÓN DE USUARIOS.....	204
a) <i>System Parameter</i> —Parámetros del Sistema: .....	204
b) <i>RF Network</i> —Red de Radiofrecuencia: .....	206
c) <i>Advanced (Infrastructure)</i> —Avanzado: .....	208
d) <i>Network Security</i> —Seguridad de la red: .....	209
11.3. ESTADÍSTICAS DEL CLIENTE AIRONET .....	211
11.4. DIAGNOSTICOS DE COBERTURA.....	216
CAPITULO 12: ANALISIS DE DATOS RECOLECTADOS.....	218
12.1. ENCUESTA APLICADA .....	218
12.2. DATOS RECOLECTADOS CON EL <i>LOCUST</i> .....	221
12.3. ANÁLISIS DE DATOS RECOLECTADOS.....	224
CAPITULO 13: RECOMENDACIONES.....	226
En cuanto al diseño físico y distribución del equipo de la <i>WLAN</i> : .....	226
En los parámetros del ACU de la versión 12.01T: .....	227
En los parámetros del AP: .....	228
En cuanto al <i>LOCUST</i> :.....	232
En cuanto al CiscoWorks for Wireless (WLSE): .....	232
Otras recomendaciones: .....	233
CONCLUSIONES .....	234
BIBLIOGRAFIA .....	236
APENDICES .....	237
A.1. FÓRMULAS UTILIZADAS PARA REALIZACIÓN DE CÁLCULOS.....	238
GLOSARIO .....	240
LISTA DE ABREVIATURAS.....	243
ANEXOS .....	245
B.1. EQUIVALENCIA ENTRE MODELO OSI PARA REDES INALÁMBRICAS VRS ALAMBRADAS .....	246
B.2. CONEXIONES NECESARIAS PARA CONFIGURAR AP .....	247
B.3. TIPOS DE COBERTURA DE UNA ANTENA.....	249
B.4. COMPARACIÓN ENTRE ESTÁNDARES DE COMUNICACIÓN INALÁMBRICOS .....	250

## INDICE DE FIGURAS

FIGURA 1.1 DESCRIPCIÓN GRÁFICA DEL PROBLEMA .....	18
FIGURA 4.1 EJEMPLOS DE ALGUNAS TOPOLOGÍAS EN REDES LAN .....	27
FIGURA 4.2 TRAMA <i>ETHERNET</i> 802.3 .....	28
FIGURA 4.3 ESPECTRO EXPANDIDO Y ESPECTRO DE BANDA ANGOSTA (SEÑAL NORMAL).....	31
FIGURA 4.4 CANALES SIN TRANSLAPE (1,6 Y 11). .....	32
FIGURA 4.5 TRAMA 802.11 .....	32
FIGURA 4.6 NIVELES DE SEGURIDAD OFRECIDOS PARA <i>WLAN</i> . .....	39
FIGURA 4.7 DISTORSIÓN POR <i>MULTIPATH</i> .....	40
FIGURA 5.1 PUNTOS DE ACCESO AIRONET 350 .....	42
FIGURA 5.2 PUNTOS DE ACCESO AIRONET 1200 .....	45
FIGURA 5.3 <i>DATA RATE</i> VRS COBERTURA.....	45
FIGURA 5.4 ADAPTADOR PCM350 CISCO .....	46
FIGURA 6.1 ANTENA DIPOLO AIR-ANT3351. ....	56
FIGURA 6.2 ANTENA MODELO AIR-ANT1728 PARA AP. ....	57
FIGURA 6.3 ANTENA DIRECCIONAL AIR-ANT3549 PARA AP. ....	58
FIGURA 7.1 VENTANA PRINCIPAL DEL <i>LOCUST</i> .....	62
FIGURA 7.2 VENTANA DE SUBMENÚ <i>SELECT AP</i> DEL <i>LOCUST</i> . ....	63
FIGURA 7.3 VENTANA DE SUBMENÚ <i>SELECT PER AP</i> DEL <i>LOCUST</i> . ....	63
FIGURA 7.4 VENTANA DE SUBMENÚ <i>SURVEY MODE</i> DEL <i>LOCUST</i> .....	64
FIGURA 7.5 VENTANA DE SUBMENÚ <i>SCAN FOR AP'S</i> DEL <i>LOCUST</i> .....	64
FIGURA 7.6 VENTANA DE SUBMENÚ <i>SPECTRUM</i> DEL <i>LOCUST</i> .....	65
FIGURA 8.1 CONFIGURACIÓN INICIAL EN AP VIRGEN .....	67
FIGURA 8.2 MENÚ DE CONFIGURACIÓN Ó <i>SETUP</i> .....	67
FIGURA 8.3 CONFIGURACIÓN DEL <i>EXPRESS SETUP</i> . ....	68
FIGURA 8.4 ICONO DE CLIENTE AIRONET EN EL ESCRITORIO .....	72
FIGURA 8.5 EDICIÓN DEL NUEVO PERFIL DE USUARIO .....	72
FIGURA 8.6 CONFIGURACIÓN DEL SSID EN EL PERFIL DE USUARIO. ....	73
FIGURA 8.7 ESCOGENCIA DEL PERFIL DEL USUARIO. ....	73
FIGURA 8.8 ICONO DEL EXPLORADOR DE INTERNET .....	74
FIGURA 8.9 INICIO DE SESIÓN HTTP Y PÁGINA PRINCIPAL DE <i>HOME</i> . ....	74
FIGURA 8.10 PÁGINA PRINCIPAL DE <i>MAP</i> . ....	75
FIGURA 8.11 PÁGINA PRINCIPAL DE <i>NETWORK PORTS</i> . ....	76
FIGURA 8.12 PÁGINA PRINCIPAL DE LA TABLA DE ASOCIACIÓN. ....	78
FIGURA 8.13 PÁGINA PRINCIPAL DE <i>SETUP</i> .....	78
FIGURA 8.14 PÁGINA PRINCIPAL DEL <i>EVENT LOG</i> . ....	79
FIGURA 8.15 PÁGINA DE AYUDA PARA AP'S .....	80
FIGURA 8.16 PÁGINA PRINCIPAL DE <i>DISPLAY DEFAULTS</i> EN APARTADO DE <i>ASSOCIATIONS</i> . ....	81

FIGURA 8.17	PÁGINA PRINCIPAL DE <i>ADDRESS FILTERS</i> EN APARTADO DE <i>ASSOCIATIONS</i> .	82
FIGURA 8.18	PÁGINA PRINCIPAL DE <i>PROTOCOL FILTERS</i> EN EL APARTADO DE <i>ASSOCIATIONS</i> .	84
FIGURA 8.19	PÁGINA PRINCIPAL DE <i>PORT ASSIGNMENTS</i> EN EL APARTADO DE <i>ASSOCIATIONS</i> .	85
FIGURA 8.20	PÁGINA PRINCIPAL DE <i>VLAN SETUP</i> EN APARTADO DE <i>ASSOCIATIONS</i> .	86
FIGURA 8.21	PÁGINA PRINCIPAL DE <i>ADVANCED</i> EN APARTADO DE <i>ASSOCIATIONS</i> .	88
FIGURA 8.22	PÁGINA PRINCIPAL DE <i>SERVICE SETS</i> EN APARTADO DE <i>ASSOCIATIONS</i> .	91
FIGURA 8.23	PÁGINA PRINCIPAL DE <i>DISPLAY DEFAULTS</i> EN APARTADO DE <i>EVENT LOGS</i> .	92
FIGURA 8.24	PÁGINA DE <i>EVENT HANDLING SETUP</i> .	96
FIGURA 8.25	PÁGINA DE <i>EVENT NOTIFICATION SETUP</i> .	98
FIGURA 8.26	PÁGINA DE <i>CONSOLE/TELNET SETUP</i> .	101
FIGURA 8.27	PÁGINA DE <i>TIME SERVER SETUP</i> .	103
FIGURA 8.28	PÁGINA DE <i>CISCO SERVICES SETUP</i> .	104
FIGURA 8.29	PÁGINA DE <i>MANAGE INSTALLATION KEYS</i> .	105
FIGURA 8.30	PÁGINA DE <i>MANAGE SYSTEM CONFIGURATION</i> .	107
FIGURA 8.31	PÁGINA DE <i>DISTRIBUTE CONFIGURATION</i> .	110
FIGURA 8.32	PÁGINA DE <i>DISTRIBUTE FIRMWARE</i> .	111
FIGURA 8.33	PÁGINA DE <i>HOT STANDBY</i> .	113
FIGURA 8.34	PÁGINA DE <i>CDP SETUP</i> .	115
FIGURA 8.35	PÁGINA DE <i>BOOT SERVER SETUP</i> .	121
FIGURA 8.36	PÁGINA DE <i>FTP SETUP</i> .	125
FIGURA 8.37	PÁGINA DE <i>SECURITY SETUP</i> .	126
FIGURA 8.38	PÁGINA DE <i>ROUTING SETUP</i> .	128
FIGURA 8.39	PÁGINA DE <i>WEB SERVER SETUP</i> .	129
FIGURA 8.40	PÁGINA DE <i>ACCOUNTING SETUP</i> .	131
FIGURA 8.41	PÁGINA DE <i>NAME SERVER SETUP</i> .	134
FIGURA 8.42	PÁGINA DE <i>SNMP SETUP</i> .	136
FIGURA 8.43	PÁGINA DE <i>ETHERNET PORT</i> .	138
FIGURA 8.44	PÁGINA DE <i>ETHERNET IDENTIFICATION</i> .	141
FIGURA 8.45	PÁGINA DE <i>ETHERNET HARDWARE</i> .	143
FIGURA 8.46	PÁGINA DE <i>ETHERNET PROTOCOL FILTERS</i> .	145
FIGURA 8.47	PÁGINA DE <i>ETHERNET ADVANCED</i> .	145
FIGURA 8.49	PÁGINA DE <i>AP RADIO IDENTIFICATION</i> .	153
FIGURA 8.50	PÁGINA DE <i>AP RADIO HARDWARE</i> .	155
FIGURA 8.51	PÁGINA DE <i>AP RADIO PROTOCOL FILTER</i> .	160
FIGURA 8.52	PÁGINA DE <i>AP RADIO ADVANCED</i> .	161
FIGURA 8.53	PÁGINA DE <i>NETWORK DIAGNOSTICS</i> .	168
FIGURA 8.54	PÁGINA DE <i>EXPRESS SETUP</i> .	170
FIGURA 9.1	PÁGINA PRINCIPAL DE <i>NETWORK PORTS PARA AP 1200</i> .	176

FIGURA 9.2	PÁGINA PRINCIPAL DE <i>SETUP PARA AP 1200</i> .....	177
FIGURA 9.4	PÁGINA DE <i>PROXY MOBILE IP GENERAL</i> .....	182
FIGURA 9.5	PÁGINA DE <i>AUTHENTICATOR CONFIGURATION</i> .....	183
FIGURA 9.6	PÁGINA <i>LOCAL SA BINDINGS</i> .....	185
FIGURA 9.7	PÁGINA DE ESTADÍSTICAS DEL <i>PROXY MOBILE IP</i> .....	187
FIGURA 9.8	PÁGINA <i>SUBNET MAP TABLE</i> .....	190
FIGURA 11.1	ICONO DE CLIENTE AIRONET EN EL ESCRITORIO.....	203
FIGURA 11.2	EDICIÓN DEL NUEVO PERFIL DE USUARIO.....	203
FIGURA 11.4	PARÁMETROS DE LA RED DE RADIOFRECUENCIA.....	206
FIGURA 11.5	PARÁMETROS AVANZADOS DE INFRAESTRUCTURA.....	208
FIGURA 11.6	PARÁMETROS DE SEGURIDAD DE LA RED.....	209
FIGURA 11.7	ESTADÍSTICAS DEL CLIENTE AIRONET 350.....	211
FIGURA 11.8	DESPLIEGUE DEL <i>STATUS</i> EN PORCENTAJE.....	216
FIGURA 12.1	ENCUESTA APLICADA A EMPLEADOS DE CSU.....	218
FIGURA 12.2	DATOS OBTENIDOS DE LA 1ER PREGUNTA DE LA ENCUESTA. .....	219
FIGURA 12.3	DATOS OBTENIDOS DE LA 2DA PREGUNTA DE LA ENCUESTA. .....	220
FIGURA 12.4	PRIMERA PLANTA DEL EDIFICIO CENTRAL DE CSU.....	221
FIGURA 12.5	SEGUNDA PLANTA DEL EDIFICIO CENTRAL DE CSU.....	222
FIGURA 12.6	TERCERA PLANTA DEL EDIFICIO CENTRAL DE CSU.....	223
FIGURA 12.7	POTENCIA VRS DISTANCIA.....	224
FIGURA B.1.1	EQUIVALENCIA EN EL MODELO OSI ENTRE RED INALÁMBRICA VRS ALAMBRADA.....	246
FIGURA B.2.1	OPCIONES DE CONEXIÓN DE LA ALIMENTACIÓN AL AP.....	247
FIGURA B.2.2	CONEXIÓN DE CABLE SERIE DB-9 A DB-9, PARA CONFIGURACIÓN DEL AP.....	247
FIGURA B.2.3	CONEXIÓN DE CABLE SERIE DB-9 A RJ-45, PARA CONFIGURACIÓN DEL AP.....	248
FIGURA B.3.1	COBERTURA HORIZONTAL DE UNA ANTENA.....	249
FIGURA B.3.2	COBERTURA VERTICAL DE UNA ANTENA.....	249
FIGURA B.4.1	COMPARACIÓN ENTRE ESTÁNDARES DE COMUNICACIÓN INALÁMBRICOS.....	250

## INDICE DE TABLAS

TABLA 5.1 ESPECIFICACIONES TÉCNICAS <i>AIRONET</i> 350 .....	44
TABLA 5.2 RESUMEN DE <i>LEDS</i> INDICADORES PARA <i>AIRONET</i> 350 .....	48
TABLA 6.1 TIPOS DE CABLES BAJOS EN PÉRDIDAS DE LA SERIE CISCO <i>AIRONET</i> .....	55
TABLA 6.2 CARACTERÍSTICAS DE LA ANTENA AIR-ANT3351. ....	57
TABLA 6.3 CARACTERÍSTICAS DE LA ANTENA AIR-ANT1728. ....	58
TABLA 6.4. CARACTERÍSTICAS DE LA ANTENA AIR-ANT3549. ....	59
TABLA 8.1 <i>EVENT DISPLAY SEVERITY LEVEL</i> — DESPLIEGUE DE NIVEL DE SEVERIDAD DE EVENTOS. ....	94
TABLA 10.1 AP'S Y <i>BRIDGES</i> SOPORTADOS POR WLSE .....	202

## **CAPITULO 1: DESCRIPCIÓN DEL PROYECTO**

### **Breve explicación del capítulo**

En este primer capítulo se hará una reseña acerca de información histórica acerca de la empresa en primera instancia. Posteriormente se hará una descripción detallada del problema que se desea resolver, así como de los objetivos que se esperan cumplir al finalizar el proyecto.

### **1.1. DESCRIPCIÓN DE LA EMPRESA**

La Empresa Corporación de Supermercados Unidos (C.S.U.) es el resultado de la evolución de lo que en un principio fue llamado la Cadena de Supermercados MAS X MENOS, la cual fue fundada el 5 de diciembre de 1960, siendo el primer tipo de supermercado de Autoservicio en el país.

Dicha Corporación es en la actualidad, una de las empresas más importantes en el negocio al detalle de Centroamérica y una compañía en plena expansión regionalmente.

En la actualidad abarca el siguiente número de supermercados, los cuales se encuentran distribuidos en distintas zonas del país y parte de Nicaragua:

- 22 Más X Menos
- 88 Palí (16 de ellos ubicados en Nicaragua)
- 3 Hipermás
- 2 Maxi Mercados
- 4 La Unión (todos ubicados en Nicaragua)

Teniendo como total 119 establecimientos.

Esta empresa en la actualidad cuenta con más de 7500 empleados distribuidos solamente en lo que son supermercados.

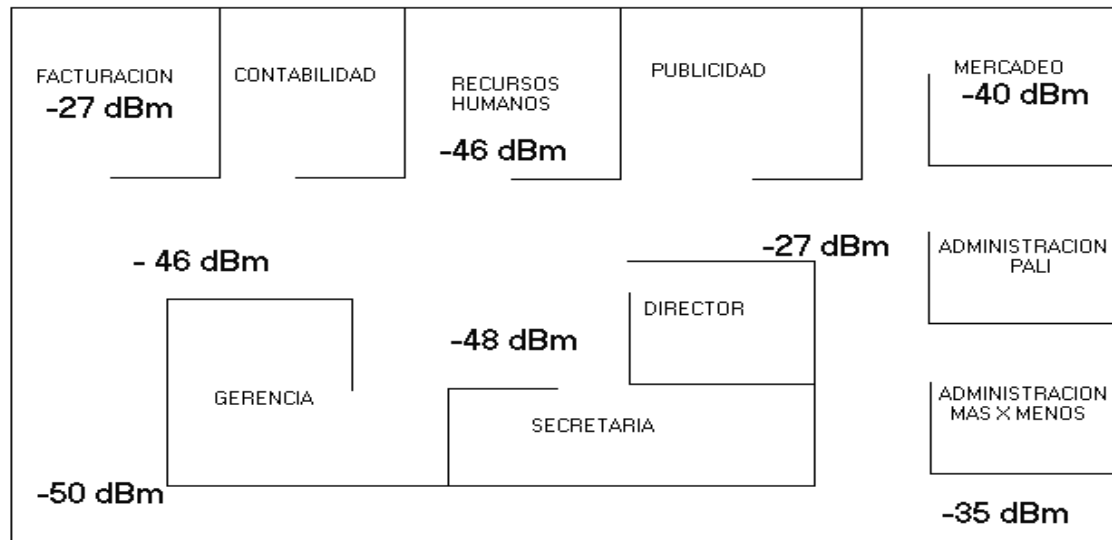
El Presidente de la Corporación es el señor Rodrigo Arguedas.



## 1.2. DESCRIPCIÓN DETALLADA DEL PROBLEMA A RESOLVER Y SUS EFECTOS

En la actualidad la empresa desea optimizar el rendimiento de la red inalámbrica que permite la conectividad a los empleados en producción tales como: oficinas de administración, contabilidad, jefaturas, recursos humanos, entre otras que se encuentran albergadas bajo un mismo edificio. El problema se presenta en algunas zonas del edificio donde la cobertura de los AP's es pobre. Ésto ocasiona que a los empleados que se desplazan con su respectiva *Laptop* por dichas áreas, se les vea reducida significativamente la velocidad de conexión. Lo anterior es parte de un mecanismo de autonegociación de velocidad que presentan los AP's en el cual se prefiere brindar una conexión confiable (es decir, con menor número de pérdidas de paquetes) sacrificando la velocidad de conexión a la red, conforme se aleja del AP.

La optimización de la red inalámbrica abarca la realización de un estudio preliminar para determinar en un plano del edificio las zonas más afectadas, así como las zonas donde el nivel de potencia es el adecuado. Este estudio preliminar incluye la recolección de datos mediante un analizador portátil para el estudio de las redes inalámbricas (*WLAN*) denominado *LOCUST*. Posteriormente se realizará el estudio correspondiente para determinar si se debe realizar cambios en cuanto a configuración de parámetros o reubicación de los 10 AP's que dan soporte al edificio en su totalidad, y finalmente se dejará plasmado el aporte del estudiante mediante la elaboración de una Guía de Configuración para Puntos de Acceso.



**Figura 1.1** Descripción gráfica del problema

La propuesta final que brinde el estudiante al Administrador de redes deberá ir acorde con las políticas de Administración propias de la empresa. Además se debe buscar que no se afecte el desempeño ni la seguridad de la misma, es decir, que cualquier cambio a favor de una óptima conexión nunca debe ponerse en riesgo que a la red interna puedan ingresar intrusos.

Se escogió que dicha investigación fuera llevada a cabo por un estudiante de Ingeniería Electrónica, ya que este tipo de tecnología es relativamente reciente en el mercado y se requiere de una persona que tenga una buena formación técnica en el área de las telecomunicaciones.

Con la finalización del proyecto se desea además, obtener una fundamentación técnica acerca de los parámetros de programación de los Puntos de Acceso, esto para buscar un perfil óptimo para la empresa donde se puedan aprovechar al máximo los recursos actuales para evitar que la Corporación tenga que invertir en segundos equipos que vengán a dar una solución parcial al problema.

### **1.3. OBJETIVO GENERAL**

Determinar las causas por las que no se ha logrado una optimización máxima del rendimiento de la red *WLAN* de la Corporación de Supermercados Unidos, y realizar una propuesta justificada para su futura implementación.

#### 1.4. OBJETIVOS ESPECÍFICOS

- a. Conocer las características más importantes a tomar en cuenta en una red inalámbrica de área local (*WLAN*).
- b. Conocer el funcionamiento del recolector de datos (*LOCUST*)
- c. Determinar los parámetros eléctricos para las antenas: Dipolo, Omnidireccional, Direccional; para montaje en AP.
- d. Estudiar la ubicación actual de los equipos dentro del edificio.
- e. Conocer el funcionamiento de la Tarjeta de Interfaz de Red (NIC's) en una red *WLAN*.
- f. Conocer los diferentes parámetros y órdenes que ofrecen cada uno de los 2 modelos de AP para su configuración.
- g. Determinar la influencia que conlleva la habilitación o no de los parámetros para la puesta en marcha del equipo.
- h. Realizar el levantamiento y análisis de datos con el *LOCUST*.
- i. Análisis de datos recolectados
- j. Realizar pruebas a los equipos configurados
- k. Elaboración del Manual de Instalación de AP

## **CAPITULO 2: ANTECEDENTES DEL PROYECTO**

### **Breve explicación del capítulo**

En el segundo capítulo de este documento se hará una descripción detallada del problema que presenta la empresa en el apartado **2.1: Estudio del Problema**. En la siguiente sección se desarrollará el modelo general de solución a aplicar por el estudiante de Ingeniería Electrónica.

### **2.1. ESTUDIO DEL PROBLEMA**

Casi un año después de la primera implementación de los equipos Aironet en CSU, se empiezan a presentar los primeros problemas en cuanto a velocidad y confiabilidad de la conexión de los usuarios a estos equipos.

El problema fue corregido agregando más AP's dentro del edificio y configurando algunos parámetros que éstos presentan. Aunque no se ha logrado satisfacer en su totalidad a todos estos usuarios insatisfechos con el rendimiento de su conexión inalámbrica.

El administrador de la red desea cuantificar los alcances logrados con la configuración realizada y está anuente a escuchar mejoras que puedan ser implementadas en su diseño inicial para lograr optimizar el funcionamiento de la misma. Lo que el encargado requiere en sí, es lograr una documentación donde se expliquen los efectos de la activación o no de los diferentes parámetros de configuración de los Puntos de Acceso, con el fin de buscarle el perfil idóneo para los requerimientos de la empresa.

## **2.2. SOLUCION PROPUESTA**

El estudiante propone realizar un levantamiento de datos con la ayuda del *LOCUST*, con el propósito de localizar las zonas de la red *WLAN* donde la cobertura es pobre, así como también las zonas donde existe buena cobertura. Los resultados obtenidos serán comparados con los datos teóricos obtenidos a partir del análisis que elabore el estudiante en base a los parámetros nominales de los equipos involucrados (antenas, adaptadores inalámbricos y los AP's). Es en base a éstos últimos que se realizará la documentación.

## **CAPITULO 3: PROCEDIMIENTO METODOLOGICO**

### **Breve explicación del capítulo**

En siguiente capítulo estará destinado a exponer la estrategia a utilizar por el estudiante para solventar el problema que se le plantea. El seguimiento de la estrategia permitirá seguir, metodológicamente, los aspectos involucrados en cada uno de los objetivos específicos planteados.

### **3.1. METODOLOGIA**

- a. Conocer las características más importantes a tomar en cuenta en una red inalámbrica de área local (*WLAN*).
  - a.1) Investigar el funcionamiento y dispositivos que constituyen una red *WLAN*.
  - a.2) Determinar los tipos de topologías más comunes en el diseño de redes *LAN*.
  - a.3) Determinar las limitaciones que afectan y presentan las *WLAN*.
  - a.4) Conocer aspectos de seguridad y administración de las *WLAN*.
  
- b. Conocer el funcionamiento del recolector de datos (*LOCUST*)
  - b.1) Buscar información sobre el dispositivo
  - b.2) Estudiar su funcionamiento
  
- c. Determinar los parámetros eléctricos para las antenas: Dipolo, Omnidireccional, Direccional; para montaje en AP.
  - c.1) Investigar en manuales los parámetros más importantes de los tipos de antenas a utilizar durante el proyecto.

- d. Estudiar la ubicación actual de los equipos dentro del edificio.
  - d.1) Recolección de datos con el *LOCUST*
  - d.2) Ubicar los principales obstáculos puedan estar afectando la cobertura del área donde fue colocado el APt.
  
- e. Conocer el funcionamiento de la Tarjeta de Interfaz de Red (NIC's) en una red *WLAN*.
  - e.1. Características de *PC WLAN Adapter Cisco*
  
- f. Conocer los diferentes parámetros y órdenes que ofrecen cada uno de los 2 modelos de AP para su configuración.
  - f.1) Conocer la lógica de programación para configurar los AP's.
  - f.2) Investigar las opciones de configuración presentadas para la configuración de los AP.
  
- g. Determinar la influencia que conlleva la habilitación o no de los parámetros para la puesta en marcha del equipo.
  - g.1) Llevar a cabo diversas pruebas para conocer las implicaciones en la configuración de los AP en diversos ambientes de trabajo.
  
- h. Realizar el levantamiento y análisis de datos con el *LOCUST*.
  - h.1) Levantamiento inicial de datos por las Oficinas Centrales.
  - h.2) Ordenamiento de los datos obtenidos
  
- i. Análisis de datos recolectados
  - i.1) Determinar las causas del inapropiado funcionamiento del equipo inalámbrico
  - i.2) Proponer soluciones al problema.



- j Realizar pruebas a los equipos configurados
- j.1) Probar nuevamente el rendimiento obtenido después de haber realizado la configuración propuesta por el estudiante.
  
- k. Elaboración del Manual de Instalación de AP.
- k.1) Recopilar las principales observaciones, conclusiones y recomendaciones en un documento para la empresa.

## **CAPITULO 4: MARCO TEORICO DE LOS SISTEMAS DE RED INALAMBRICOS**

### **Breve explicación del capítulo**

Este capítulo permitirá al lector adquirir el conocimiento teórico básico que le permita entender el funcionamiento tanto de los sistemas alambrados (*LAN*) como inalámbricos (*WLAN*) de Redes Locales. Para esto, se comienza a explicar el funcionamiento de las redes alambradas y posteriormente se comparan con las redes inalámbricas.

### **4.1. MARCO TEORICO DE TECNOLOGÍAS LAN**

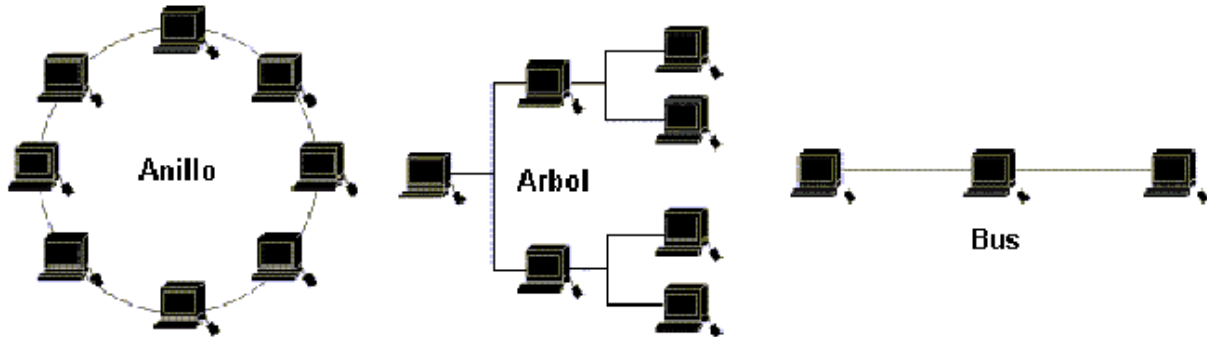
#### **4.1.1. FUNCIONAMIENTO BÁSICO DE UNA RED LAN**

Una red de área local (*LAN*) es una tecnología con alta velocidad y una tasa de error en transmisión de datos muy baja. Este tipo de tecnología es empleada generalmente para cubrir un área geográfica menor a los 100 metros de diámetro. Es muy utilizada para la interconexión de dispositivos tales como computadores, periféricos y otros. Esta tecnología ofrece como ventaja principal el acceso compartido de los dispositivos al medio, aunque esto puede convertirse a la vez en un problema si no se logra una adecuada configuración de los mismos. Las principales tecnologías *LAN* son la *Token Ring*, la *FDDI* y la *Ethernet*.

Para acceder el medio se cuenta con varias técnicas, las más usadas son la de **CSMA/CD (*Carrier Sense Multiple Access/Collision Detection*)** que consiste en que el dispositivo conectado a la red, antes de transmitir, escucha el canal para ver si hay alguna portadora, si no la detecta durante un periodo de tiempo específico el dispositivo inicia la transmisión.

Cuando dos dispositivos transmiten al mismo tiempo se produce una colisión la cual es detectada con este mismo método de acceso, la otra técnica es la denominada **Token Passing** o “pase de ficha” en la que el dispositivo puede acceder el medio sólo si se posee una pequeña trama de datos denominada ficha (*Token*), la cual circula por toda la red y sólo la posee un dispositivo a la vez.

La topología física de una red *LAN* es la forma en que se encuentran conectados los diversos dispositivos que conforman la red, desde esta perspectiva tenemos la topología de bus, de anillo, de estrella y de árbol, la Figura 4.1 nos muestra algunas de estas topologías.



**Figura 4.1** Ejemplos de algunas topologías en redes *LAN*

Existen dos técnicas de señalización: *Baseband* y *Broadband*, al menos en *Ethernet* la más usada es *Baseband*, este tipo de señalización digital consiste en tener una sola portadora de frecuencia, lo que implica que solo un canal de comunicación se usa al mismo tiempo y todas las estaciones conectadas deben de transmitir y recibir los mismos tipos de señales. La técnica analógica *Broadband* por su parte contiene varias portadoras y consiste en multiplexar (ó dividir en el tiempo) múltiples señales independientes dentro de un sólo cable, debido a esto se puede usar varios canales de comunicación al mismo tiempo y todas las estaciones conectadas pueden transmitir y recibir diferentes tipos de señales (voz, datos y video simultáneamente sobre el mismo medio de transmisión).

#### 4.1.2. TRAMA *ETHERNET* 802.3

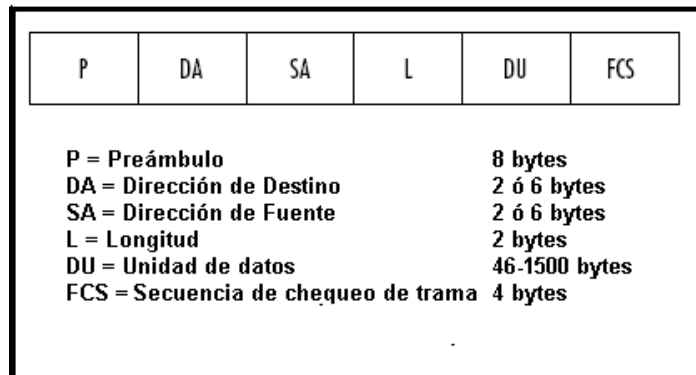


Figura 4.2 Trama *Ethernet* 802.3

- Preámbulo: Es la primera celda de la trama *Ethernet*. Presenta 8 *bytes* de longitud, con un patrón alternativo de 1's y 0's que le indica al dispositivo receptor que una nueva trama de datos está llegando.
- Dirección de Destino y de Fuente: Estos campos contienen la dirección MAC del dispositivo fuente y del destino.
- Longitud: Describe el número de *bytes* que contiene la celda de datos.
- Unidad de Datos: Esta celda contiene propiamente los datos a enviar o recibir.
- Secuencia de verificación de trama: Contiene un valor para realizar un control de error en la transmisión en la trama.

#### **4.1.3. CARACTERÍSTICAS DE LAS REDES LAN**

- Extensión de sus capacidades sin necesidad de hacer grandes cambios en la red.
- Está limitada a las áreas por donde pase el cableado.
- Puede manejar altas velocidades de transmisión y tiene una tasa reducida de error.
- Permite el uso de los recursos únicamente donde están ubicados físicamente los dispositivos.
- Puede usar diversos tipos de líneas de transmisión para intercambio de información, cada medio presenta sus propias características.
- Cualquier cambio en la ubicación física de la red requiere un nuevo cableado o una movilización del ya existente.
- Poseen una gran cantidad de sistemas de seguridad en redes.
- Las barreras físicas pueden impedir o dificultar su instalación.
- Si se trabaja con fibra óptica, los costos de instalación podrían ser altos.

## 4.2. MARCO TEORICO DE TECNOLOGÍAS WLAN

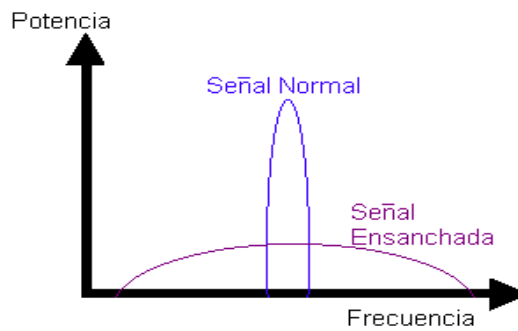
### 4.2.1. FUNCIONAMIENTO BÁSICO DE UNA WLAN

Las redes *Wireless LAN* (WLAN) son aquellas en las cuales el medio por el cual se propaga la señal de información **no** es constituido por las líneas de transmisión sino más bien que, la información ha sido modulada en señales de radiofrecuencia (RF) las cuales viajan a través del vacío desde el equipo emisor hasta el receptor. Esta tecnología ha nacido con el fin de reemplazar las LAN's, por un sistema más fácil de instalar y tan seguro como el anterior, si es bien configurado<sup>1</sup>.

Para realizar el proceso de transmisión de datos a través de ondas electromagnéticas se utiliza la banda de frecuencias denominada **ISM** comprendidas entre 2.40 GHz y los 2.48 GHz. Lo anterior presenta la ventaja que no es necesario tener licencia para operar dentro de dicha banda, adicionalmente, en ésta banda se utiliza la técnica de modulación en Espectro Expandido (*Spread Spectrum*) la cual tiene como ventajas fundamentales la creación de interferencias muy pequeñas (debido a que su amplitud es menor a la de Banda Angosta) así como también, de presentar una menor susceptibilidad al ruido ya que esparce la señal transmitida dentro de la Banda de radiofrecuencia que lo comprende.

---

<sup>1</sup> Ver gráfico de comparación de LAN vrs WLAN en el modelo OSI en [Anexo B.1.](#)



**Figura 4.3** Espectro expandido y espectro de banda angosta (señal normal).

Este espectro expandido recurre a dos tipos de transmisión para radiofrecuencia, la primera es denominada FHSS (*Frequency Hopping Spread Spectrum*) la cual está limitada a una velocidad de transferencia de datos entre 1 y los 2 Mbps, por lo cual está limitado a aplicaciones específicas; mientras que la DSSS (*Direct Sequence Spread Spectrum*) es la más utilizada, esto ya que permite trabajar a varias velocidades 1, 2, 5.5 o 11 Mbps. El acceso al medio utilizado por este último es la técnica llamada CDMA (*Code Division Multiplexing Access*) la cual permite que se den varias transmisiones en la misma frecuencia y al mismo tiempo gracias a la utilización de tres canales independientes de frecuencia que evitan que se traslapen y que crean vías distintas para el traslado de la información.

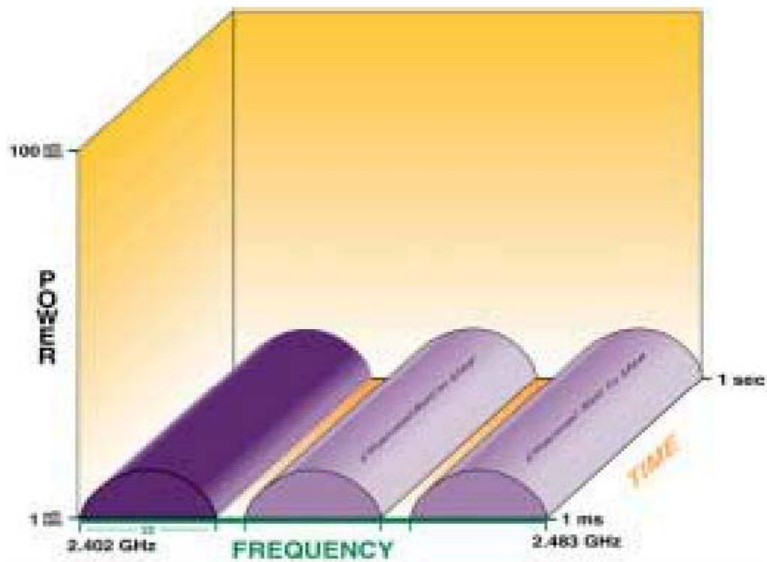


Figura 4.4 Canales sin transape (1,6 y 11).

#### 4.2.2. TRAMA 802.11

FC	D/ID	A1	A2	A3	SC	A4	FB	FCS
FC = Control de la trama	D/ID = Duración/ID	A1 = Dirección 1	A2 = Dirección 2	A3 = Dirección 3	SC = Control de secuencia	A4 = Dirección 4	FB = Cuerpo de la trama	FCS = Secuencia de control de la trama
2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0-2314 bytes	4 bytes

Figura 4.5 Trama 802.11

- Control de la trama: Contiene 10 subcampos:
  - a) Versión del protocolo: Tiene 2 bits de longitud. Su valor por defecto es 0.
  - b) Tipo: Tiene 2 bits de longitud y trabaja en conjunto con el campo de subtipo para identificar la función de la trama.



- c) Subtipo: Tiene 4 bits de longitud.
- d) Hacia el sistema de distribución: Presenta 1 bit de longitud y es colocado en 1 en todas las tramas enviadas por la estación asociada con el AP, para decir que la trama está destinada para la red detrás del AP.
- e) Desde el sistema de distribución: Presenta 1 bit de longitud y es colocado en 1 en todas las tramas salientes desde del DS.
- f) Más fragmentos: Presenta 1 bit de longitud y es colocado el 1 en todas las tramas que contienen otro fragmento del actual servicio de la unidad de datos MAC (MSDU) ó del Protocolo de Administración de Unidad de Datos (MMPDU).
- g) Reintentar: Presenta 1 bit de longitud y es colocado en 1 en todas las tramas que son retransmisiones de tramas anteriores.
- h) Administración de energía: Presenta 1 bit de longitud y se coloca en 1 para indicar que la estación estará en modo de ahorro de energía después de haber intercambiado satisfactoriamente una secuencia de trama. Estará en 0 cuando la estación se mantendrá en modo activo.
- i) Más datos: Presenta una longitud de 1 bit y se encuentra en 1 para decirle a la estación que está en modo ahorro de energía y que tiene al menos una trama para la estación conectada al AP.
- j) Protocolo *WEP*: Presenta 1 bit de longitud y es colocado en 1 si el cuerpo de la trama que ha sido procesada por el algoritmo *WEP*.

k) Orden: Presenta 1 bit de longitud y es colocado en 1 en cualquier trama que contenga datos utilizando la clase de servicio Estrictamente Ordenada. Éste último consiste en guardar paquetes de *broadcast* o *multicast* que asocian direcciones para tramas que han sido procesadas, evitando que se alcance un destino fuera de orden y que pueda crear problemas de comunicación.

- Duración/ID: Presenta una longitud de 16 bits. Lleva la identificación de la asociación de la estación con el AP.
  
- Campos de Dirección:
  - a) Identificadores de Servicio de Destino (BSSID): MAC del AP.
  
  - b) Dirección de destino (DA): La del destinatario final.
  
  - c) Dirección de la fuente (SA): La de la estación que envía en la *WLAN*.
  
  - d) Dirección del receptor (RA): La estación del destinatario inmediata.
  
  - e) Dirección del transmisor (TA): MAC de la estación que envía.
  
- Cuerpo de la trama: Constituye los datos contenidos dentro de la trama.
  
- Secuencia de Verificación de Errores: Valor asignado para la verificación de errores.

### **4.2.3. CARACTERÍSTICAS DE LAS REDES *WLAN***

- Posee las características y beneficios de una *LAN* cableada.
- Ideal para las empresas que cambian de infraestructura constantemente.
- Permite la movilidad de los usuarios a través de toda la empresa.
- Es ideal también para empresas que desean diseñar una red pero la infraestructura de su edificio no lo permite, por ejemplo: es una edificación muy antigua, es una ubicación temporal o porque el sitio es alquilado y no se permite hacer cambios de infraestructura.
- Usar señales de RF la banda ISM no requiere licencia.
- Pueden usarse para redes en un solo departamento o piso, o bien para enlazar varias *LAN* ubicadas en edificios distintos.
- Es posible tener computadoras donde antes era imposible, más que todo por razones de cableado.
- Seguridad equivalente a las redes cableadas, debido al protocolo *WEP*.
- Promueve la productividad, ya que se ha demostrado en estudios que los trabajadores pasan más tiempo conectados a la red.
- Mayor facilidad de configurar espacios temporales por motivos de reuniones.
- Mejora la imagen de la compañía e incrementa la ventaja competitiva.

#### 4.2.4. ASPECTOS DE SEGURIDAD DE WLAN

##### 4.2.4.1. Protocolo WEP (*Wired Equivalent Protocol*)

El estándar 802.11 para comunicaciones LAN inalámbricas introdujo el WEP en un intento de abordar los nuevos problemas en el ámbito de seguridad de los sistemas cableados a los inalámbricos. El objetivo principal de WEP es proteger la confidencialidad de los datos de los usuarios de escuchas indeseables. WEP es parte de un estándar internacional; ha sido integrado por los fabricantes en sus dispositivos 802.11 y hoy día su uso es común.

Desdichadamente, WEP no consigue alcanzar sus objetivos de seguridad, a pesar de emplear el conocido y supuestamente seguro cifrado RC-4, en fin, WEP adolece de varias vulnerabilidades severas de seguridad. Estas vulnerabilidades dan lugar a cierto número de ataques, tanto activos como pasivos, que permiten escuchar y alterar conexiones inalámbricas.

El WEP confía en una clave secreta  $k$  compartida entre los partícipes del grupo de comunicaciones para proteger el cuerpo del mensaje de una trama de datos.

El protocolo WEP fue diseñado para imponer tres metas de seguridad principales:

- a) **Confidencialidad:** El objetivo fundamental de WEP es evitar escuchas fortuitas.
- b) **Control de acceso:** Un segundo objetivo del protocolo es proteger el acceso a la infraestructura de red inalámbrica.

**c) Integridad de datos:** Su tercer objetivo es prevenir la manipulación de los mensajes transmitidos; por lo que se agrega el campo *checksum*.

La seguridad del protocolo *WEP*, “reside en la dificultad de obtener la clave pública por medio de ataques por fuerza bruta”.

Hoy día hay dos clases de implementación *WEP*:

- La clásica (de 40 bits): Esta longitud de clave no es lo suficientemente larga como para evitar ataques de fuerza bruta.
- La de 128 bits (que realmente emplean 104 bits): Esta extensión a la cantidad de bits convierte en casi imposibles los ataques por fuerza bruta incluso para el adversario con los mayores recursos, dada la tecnología actual.

A pesar de utilizar este último tipo de implementación, se recomienda que *WEP* no sea considerado como un protector total de la seguridad a nivel de enlace, y que se tomen medidas adicionales para asegurar el tráfico de red tales como el uso de otro protocolo que permita encriptar la información como lo es el *Secure Shell* (SSH).

#### 4.2.4.2. Protocolo *Secure Shell* (SSH)

SSH es un protocolo que provee un nivel criptográfico para el manejo del tráfico, el cual es muy seguro para reemplazar las sesiones de **Telnet**. Esta última es necesaria para realizar cambios en configuraciones de equipos de manera remota.

Utilizando SSH se puede realizar el registro de ingreso (*login*) a cualquier equipo remoto, evitando que tanto el nombre de usuario como la clave viajen hasta el equipo en texto claro (sin encriptación), teniéndose menor preocupación que algún *sniffer* pueda capturarlos y utilizarlos para ingresar al equipo.

Este *software* provee tanto un fuerte enlace *host-to-host* así como una autenticación de usuario para lograr una comunicación segura a través de una red no segura.

SSH opera de la siguiente manera:

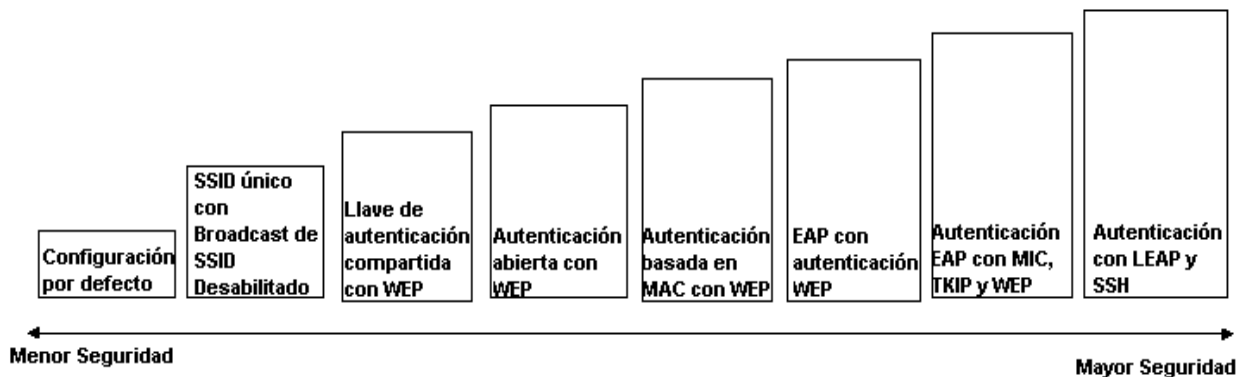
- a) El AP escucha la petición del servidor SSH en el puerto TCP número 22.
- b) Cuando se recibe la petición de un Cliente para conexión por SSH, el AP envía una llave pública, una cifra con detalles de especificación y el tipo de autenticación (clave) al Cliente.
- c) El Cliente genera una llave de sesión doblemente encriptada y la envía al AP por el mismo camino con la cifra escogida.
- d) El AP autentifica el Cliente basado en una identificación de usuario y clave cuando la característica de Usuario Administrador es habilitada.

Si la autenticación es válida, todo el tráfico que viaje entre el Cliente y el AP estará encriptado utilizando la llave de sesión.

El protocolo SSH se ejecuta en la capa de aplicación del modelo TCP/IP y es relativamente fácil de utilizar para los Clientes y se encuentra disponible para ejecutarse en computadoras con *Windows* y algunos tipos de *Unix*. Los Clientes SSH se encuentran disponibles para utilizarse en algunos *handhelds*.

El protocolo SSH se encuentra habilitado por defecto en los AP's. Cuando se tiene habilitado el Administrador de Usuarios en el AP, SSH utiliza los nombres de usuarios y claves establecidos por el Administrador de Usuarios. Los modelos recientes de computadoras tienen el Cliente SSH instalado. En caso de no estar instalado puede ser descargado desde el sitio [www.ssh.com](http://www.ssh.com).

A continuación se muestra los niveles de seguridad ofrecidos para redes *WLAN*. Como se puede apreciar en la Figura 4.6, el nivel más alto de seguridad es ofrecido por la autenticación mediante *LEAP* y el uso del protocolo SSH.



**Figura 4.6** Niveles de seguridad ofrecidos para *WLAN*.

#### 4.2.5. FACTORES QUE AFECTAN LA TRANSMISIÓN EN REDES *WLAN*

Las señales electromagnéticas se propagan en el espacio y son afectadas por un fenómeno llamado *Multipath* (Múltiples Rutas), el cual consiste en la creación de múltiples caminos por los cuales las señales reflejadas llegan al receptor. Éstas señales reflejadas llegan al receptor con una intensidad ó amplitud menor a la señal principal, además de presentar un atraso en el tiempo.

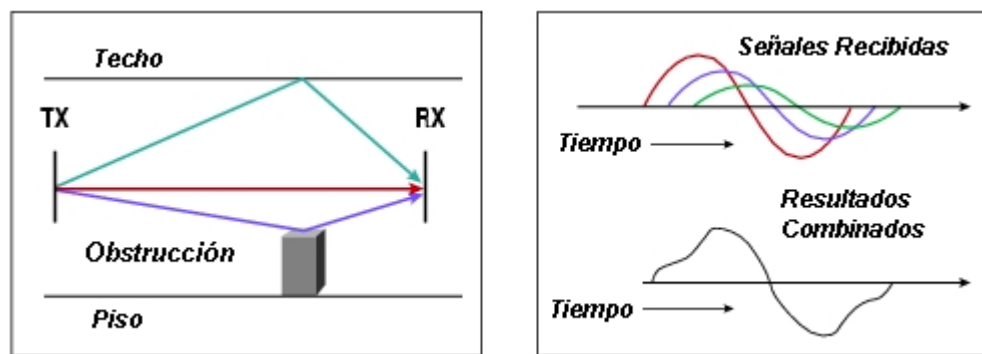


Figura 4.7 Distorsión por *Multipath*

Existen cinco efectos que perturban la propagación de las ondas electromagnéticas, ellos son:

- a) **La reflexión**, este fenómeno se produce cuando una onda electromagnética es reflejada en parte o en su totalidad por un objeto cuyas dimensiones son mayores que la longitud de onda ( $\lambda$ ) de la señal propagada.
- b) **La dispersión**, al igual que la reflexión se produce cuando la onda electromagnética choca con algún objeto, solo que con dimensiones cercanas a longitud de onda ( $\lambda$ ) de la señal propagada, logrando que ésta se disperse.



**c) La difracción**, el cual ocurre cuando la onda electromagnética se topa con un objeto impenetrable lo que causa que al receptor lleguen únicamente señales reflejadas por lo tanto señales de menor potencia.

**d) La refracción**, éste se presenta cuando una señal pasa de un medio a otro con diferente densidad, lo que ocasiona un cambio en la velocidad de propagación de la onda.

**e) La interferencia**, éste se presenta cuando dos o más ondas electromagnéticas se combinan de tal forma que el funcionamiento del sistema no es el esperado.

Básicamente hay dos tipos de interferencia: la denominada **Co-Channel** la cual se presenta cuando otro enlace RF está usando el mismo canal de frecuencia y la interferencia **Adjacent Channel** (Canal adyacente) la cual se da cuando otro enlace RF está usando un canal adyacente al que se está utilizando.

## CAPITULO 5: MARCO TEORICO DE EQUIPOS PARA WLAN

### Breve explicación del capítulo

En este capítulo se hará mención de los principales equipos utilizados e involucrados en el desarrollo del proyecto. Se hará énfasis en sus principales características y parámetros de configuración que ofrecen.

**Nota:** Los gráficos con el despliegue de equipos son únicamente utilizados como ilustración y no necesariamente constituyen los parámetros recomendados.

### 5.1. EQUIPOS PARA WLAN

#### 5.1.1. PUNTO DE ACCESO AP 350



**Figura 5.1** Puntos de Acceso Aironet 350

Los Puntos de Acceso Cisco *Aironet* Series 350 soporta tasas de datos de hasta 11 Mbps, es compatible con IEEE 802.11b. La corriente eléctrica fluye internamente a través de *Ethernet* 10/100, simplificando y reduciendo los costos totales de instalación y propiedad.

Se han fabricado dos versiones: estándar y robusta.

- El AP estándar viene en caja de plástico, trabaja en temperatura operativa estándar y usa antenas integradas.
- El AP robusto ofrece un margen de temperatura de operación mayor, conectores de antena externos para antenas auxiliares y caja de metal para mayor durabilidad en trabajo bajo condiciones severas (Esta versión es la que interesa para el proyecto).

Ambos presentan la característica de [diversidad de antena](#), mejorando el efecto ocasionado por *multipath*.

La potencia de transmisión de la radiofrecuencia puede ser regulada por el usuario (1, 5, 20, 30, 50, 100 mW) para satisfacer los requerimientos específicos de cobertura y minimizar la interferencia. Cuenta con dos conectores RP-TNC para colocación de antenas removibles que puedan aumentar el alcance y la confiabilidad.

Todos los *Access Points* Cisco *Aironet* Series 350 ofrecen la funcionalidad de balance de carga. Pueden utilizarse hasta tres *Access Points* para lograr una capacidad pico de 33 Mbps en una única área de cobertura.

**Tabla 5.1** Especificaciones técnicas *Aironet 350*

<b>Descripción</b>	<b>Especificaciones</b>
Tasas de datos soportadas	1, 2, 5.5, y 11 Mbps
Estándar de Red	IEEE 802.11b
Enlace	10/100BaseT <i>Ethernet</i> Autosensible
Banda de Frecuencia	2.4 a 2.497 GHz
Medio Inalámbrico	DSSS ( <i>Direct Sequence Spread Spectrum</i> )
Protocolo de Acceso de Medios	CSMA/CA
Canales operativos	América del Norte: 11
Canales sin translaje	Tres (canales 1,6 y 11)
Sensibilidad de recepción	1 Mbps: -94 dBm ; 2 Mbps: -91dBm 5.5 Mbps: -89 dBm ; 11 Mbps: -85 dBm
<i>Delay Spread</i>	1 Mbps: 500 ns ; 2 Mbps: 400 ns 5.5 Mbps: 300 ns ; 11 Mbps: 140 ns
Configuraciones de potencia de transmisión disponibles	100 mW (20 dBm) ; 50 mW (17 dBm) 30 mW (15 dBm) ; 20 mW (13 dBm) 5 mW (7 dBm) ; 1 mW (0 dBm)
Alcance (Típico)	<b>Interior:</b> 40 m @ 11 Mbps ; 107 m @ 1 Mbps
Longitud de llave de encriptación ( <i>WEP</i> )	128-bit

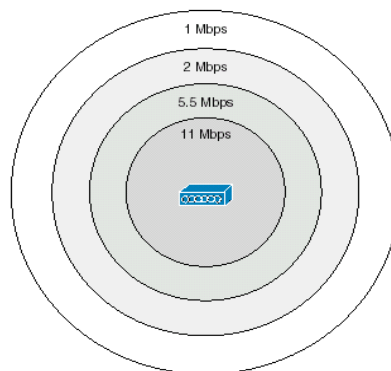
### 5.1.2. PUNTO DE ACCESO AP 1200



**Figura 5.2** Puntos de Acceso Aironet 1200

Los *Access Points* Cisco Serie 1200 imponen el estándar para las redes inalámbricas de área local de la próxima generación. Posee gran capacidad de actualización y compatibilidad con los estándares actuales. Este modelo soporta las tecnologías IEEE 802.11a (5 GHz) y 802.11b (2.4 GHz) en modos de operación sencillo y dual (ambos estándares funcionando juntos). En cuanto al resto de su funcionalidad y especificaciones técnicas es similar al *Aironet 350*.

Ambos AP's presentan las características de autonegociación de velocidad, lo cual consiste en que conforme el Cliente se aleje del AP, la velocidad de transmisión va a disminuir sin necesidad de interrumpir la conexión.



**Figura 5.3** Data Rate Vrs Cobertura

### 5.1.3. CLIENT ADAPTER—ADAPTADOR DE RED

Tienen a su cargo la tarea de proveer comunicaciones de datos inalámbricas entre dispositivos móviles o fijos, otros sistemas inalámbricos o infraestructuras de red cableada, los PCM poseen una antena integrada y los LMC no tienen antena integrada sino que más bien poseen conectores para adaptarle una antena de entre varios modelos, la Figura 5.4 nos muestra este tipo de dispositivo.



**Figura 5.4** Adaptador PCM350 Cisco

Las tarjetas Cisco *Aironet 350* tiene una potencia de salida en EEUU de 100 mW (autolimitadas a 30 mW )

## 5.2. MODOS DE OPERACIÓN DE LOS PUNTOS DE ACCESO

Existen 3 tipos comunes de configuraciones inalámbricas

### 5.2.1. UNIDAD PRINCIPAL (*ROOT UNIT*: CONFIGURACIÓN POR DEFECTO)

Un AP conectado directamente provee un punto de conexión para usuarios inalámbricos. Si existen varios AP el usuario puede desplazarse entre varias áreas de cobertura. Tan pronto el usuario se desplaza fuera del alcance del AP, ellos automáticamente establecen una asociación hasta el AP más próximo. Este proceso es transparente para el usuario. Deben estar configurados con el mismo SSID.

### **5.2.2. UNIDAD REPETIDORA (*REPEATER UNIT*)**

El AP puede ser configurado como repetidor con el propósito de extender su área de cobertura. El AP Repetidor comunica los usuarios con el AP conectado a la *LAN Ethernet*. Deben estar configurados con el mismo SSID y en el mismo canal.

### **5.2.3. UNIDAD CENTRAL (*CENTRAL UNIT*)**

Configuración utilizada en una red totalmente inalámbrica (sin conexión *Ethernet*), lo cual pone a funcionar al AP como un *hub*, conectando todas las estaciones entre sí.

## **5.3. LEDS INDICADORES DEL PUNTO DE ACCESO**

### **5.3.1. ESTADO DEL CONEXIÓN *ETHERNET* (*ETHERNET STATUS*)**

Indica si existe tráfico en el cable *LAN Ethernet*.

- Parpadeo Verde: El paquete es recibido o transmitido a través de cable *Ethernet*.
- Parpadeo Rojo: El cable no está conectado.

### **5.3.2. ESTADO DE OPERACIÓN DE SEÑALES (*ASSOCIATION STATUS*)**

- Parpadeo Verde: Operando normalmente pero no asociado de manera inalámbrica con dispositivo alguno.
- Verde Fijo: Opera normalmente y asociado de manera inalámbrica con al menos 1 dispositivo.

### 5.3.3. ACTIVIDAD DEL TRÁFICO (*RADIO ACTIVITY*)

Normalmente se encuentra apagado.

- Parpadeo Verde: Siempre que un paquete es recibido o transmitido sobre el radio de cobertura del AP.

**Tabla 5.2** Resumen de *leds* indicadores para *Aironet 350*

Mensaje	Indicador de Radio	Indicador de Estado	Indicador de <i>Ethernet</i>	Significado
Estado Asociado		Verde		Al menos un Cliente está asociado
		Parpadeo Verde		
En Operación	Parpadeo Verde	Verde		No hay Clientes asociados (revise conf, SSID y <i>WEP</i> )
		Verde	Verde	Transm/Recepc. de paquetes en <i>Ethernet</i>
	Parpadeo Verde	Verde		Número de reintentos máx. ó <i>Buffer</i> lleno
Error / Advertencia		Verde	Parpadeo Ambar	Error Transm/Recepc.
			Parpadeo Rojo	Cable <i>Ethernet</i> desconectado
Fallo	Rojo	Rojo	Rojo	Fallo de Sistema operativo.
Actualización de Sistema Operativo		Rojo		Cargando el nuevo Sist. Operativo



## **CAPITULO 6: ANTENAS PARA LOS SISTEMAS DE RED INALAMBRICOS**

### **Breve explicación del capítulo**

El capítulo mostrado a continuación presenta las características más importantes a tomar en cuenta para la escogencia de las antenas a utilizarse en los AP's.

### **6.1. CONCEPTOS Y PARÁMETROS**

#### **6.1.1. ANTENAS**

Una antena es un sistema conductor metálico capaz de radiar y recibir ondas electromagnéticas, se utiliza como la interfaz entre el transmisor y el espacio libre o el espacio libre y el receptor.

Existen una serie de parámetros característicos de cada antena que nos permiten comprender cuál se adapta mejor a una necesidad específica. Los parámetros eléctricos; por ejemplo, nos dan una idea de la capacidad que tienen las antenas para transmitir o recibir ondas electromagnéticas, los parámetros físicos por su parte nos permiten ubicar una antena en una posición o lugar específico de manera que se garantice un adecuado enlace entre el transmisor y el receptor.

Las antenas pueden encontrarse de diversos tipos, sin embargo, para efectos prácticos, nos referimos únicamente a tres tipos de antenas: los dipolos, la omnidireccional y las antenas direccionales de pared.

En los siguientes apartados se describen estos tipos de antenas y cuáles son aptas para cada dispositivo de red inalámbrica.

## **6.1.2. PARÁMETROS ELÉCTRICOS.**

A continuación se hace una descripción de los parámetros eléctricos más comunes en antenas, los cuales le permiten al usuario seleccionar antenas de acuerdo a su necesidad.

### **6.1.2.1. Ganancia**

Es la relación que existe entre la densidad de potencia radiada por la antena en una dirección particular y la densidad de potencia radiada al mismo punto por una antena de referencia, generalmente se usa como referencia una antena isotrópica (antena teórica que irradia la misma cantidad de energía en todas las direcciones), suele usarse los decibeles (dB) para expresar ésta cantidad.

Cuando se usa como referencia la antena isotrópica, la ganancia se expresa en dBi, en otras ocasiones se utiliza como referencia una antena dipolo, en este caso dicha magnitud se expresa en dBd sin embargo bastaría considerar que  $0 \text{ dBd} = 2.14 \text{ dBi}$ .

### **6.1.2.2. Directividad.**

Los diagramas de radiación de una antena nos permiten determinar hacia qué dirección y de qué manera se irradia la energía desde una antena hasta un punto específico, la directividad describe la capacidad que tiene una antena para irradiar energía hacia una dirección específica, de esta forma decimos que una antena es muy directiva cuando su haz de radiación principal es muy delgado y permite por lo tanto tener un alcance mayor, y por otro lado decimos que una antena es poco directiva cuando su haz de radiación principal es más ancho y por lo tanto permite tener una mayor cobertura.

Desde esta perspectiva encontramos dos clases de antenas las omnidireccionales que poseen una cobertura de 360° y las direccionales que poseen un ámbito limitado de cobertura normalmente expresado en grados. Al aumentar la ganancia de una antena aumenta también la cobertura de la antena, sólo que en cierta dirección por lo que el ángulo del ancho del haz disminuye.

Por ejemplo en las antenas omnidireccionales, cuando tenemos una con alta ganancia, implica que tenemos mayor área de cobertura en distancias más lejanas, como aspecto importante cabe destacar que en este caso el nivel de energía justo abajo de la antena es muy bajo.

Normalmente la directividad está relacionada con el tipo de enlace que se desee realizar, así por ejemplo cuando se trata de un enlace punto a punto se recomienda utilizar una antena con bastante directividad, sin embargo si lo que se desea es un enlace punto a multipunto una antena omnidireccional estará en capacidad de cubrir una zona mayor y por lo tanto más puntos de conexión inalámbrica.

### **6.1.2.3. Patrón de radiación de una antena.**

Es una herramienta de amplio uso en los sistemas de antenas, la cual permite visualizar la cantidad de energía y la dirección a la que se irradian los campos electromagnéticos.

Los diagramas de radiación están compuestos por lóbulos los cuales representan la energía radiada por la antena, el lóbulo que concentra la mayor cantidad de energía se define como el lóbulo principal, los demás se denominan lóbulos secundarios, la dirección a la que irradia el lóbulo principal se le denomina frente y la dirección opuesta a la que irradia este lóbulo principal se le conoce como espalda, por lo cual también recibe el nombre de relación frente-espalda

#### **6.1.2.4. EIRP (Potencia radiada isotrópica efectiva).**

Se define como una potencia de transmisión equivalente que tendría que radiar una antena isotrópica (“antena teórica” que irradia la misma cantidad de energía hacia todas las direcciones) para alcanzar la misma densidad de potencia en la dirección seleccionada hacia un punto determinado.

Sirve para tener una idea de la eficiencia con la que una antena transmisora entrega su potencia a una antena receptora. Para alcanzar un EIRP alto se debe tener una antena con dimensiones mayores a la longitud de onda a la que se está transmitiendo, cuando no es posible realizar esto debido a una longitud de onda muy grande, se debe compensar el sistema con una mayor potencia. Las letras EIRP significan *Effective Isotropic Radiated Power*.

#### **6.1.2.5. Ancho del haz de la antena.**

El ancho del haz consiste en la separación angular entre dos puntos de media potencia (esto es -3 dB) en el lóbulo de radiación principal de una antena. Entre más pequeño sea este ángulo, más directiva es una antena.

Al ser los lóbulos de radiación tridimensionales, suele expresarse esta cantidad como ancho del haz horizontal y vertical.

#### **6.1.2.6. Polarización de antena.**

Una onda electromagnética está compuesta por campos eléctricos y campos magnéticos, la polarización se refiere a la orientación del campo eléctrico al ser radiado por una antena; es decir cómo varía en magnitud y en dirección a través del espacio.

Una antena puede polarizarse en forma lineal (horizontal o vertical), circular o elíptica, se dice entonces que cuando una antena irradia una onda electromagnética polarizada horizontalmente, la antena posee una polarización horizontal. Las antenas que se usan para en las redes *WLAN* poseen polarización vertical.

#### **6.1.3. PARÁMETROS FÍSICOS.**

Los parámetros físicos son los que el ser humano puede visualizar sin necesidad de realizar cálculos para ello. Los más comunes en las antenas, son los que se detallan a continuación.

##### **6.1.3.1. Alcance.**

Cuando nos referimos al alcance del enlace nos referimos a la distancia que puede extenderse una comunicación sin que ésta se pierda o tenga demasiada interferencia, adicionalmente en algunos casos el alcance se relaciona con la velocidad de transmisión de un determinado sistema de comunicación.

Dependiendo del dispositivo que usemos o de la capacidad de las antenas, podemos encontrar alcances de tres tipos: corto, medio y largo alcance.

Normalmente esta característica se utiliza para equipos de un mismo tipo, así por ejemplo decimos que los puntos de acceso son un tipo de dispositivo que tiene antenas que poseen un alcance medio de 44 m para una velocidad de 11 Mbps y los *Bridges*, los cuales son otro tipo de dispositivo, poseen antenas que tienen un alcance medio de 3.3 Km a una velocidad de 11 Mbps, como se observa en ambos casos a pesar de que se maneja la misma velocidad de transmisión y de ser un alcance medio las diferencias en las distancias son considerables, esto debido a que son dispositivos para diferentes aplicaciones con diferentes potencias de transmisión y patrones de radiación.

#### **6.1.4. CABLES USADOS PARA CONECTAR ANTENAS.**

Al llevar a cabo las conexiones de las antenas con diversos tipos de cables se introduce un factor de pérdidas tanto en el sistema de recepción como en el de transmisión. Entre mayor sea la longitud del cable, mayores serán las pérdidas. Es normal expresar las pérdidas en dB y para determinar la influencia que tiene un tipo de cable en un sistema de antenas se suele expresar en dB/m (Decibeles por metro).

Un aspecto que se debe tomar en consideración siempre es que los cables deben de ser lo más cortos posibles para así evitar al máximo las pérdidas.

Normalmente se usan dos tipos de cable: uno de ellos se llama cable de interconexión el cual puede adaptarse a cualquier antena excepto a los dipolos, este cable posee una impedancia de  $50 \Omega$  y tiene altas pérdidas, es mejor usarlo para conexiones menores a los 3 m; el otro tipo de cable es el denominado bajo en pérdidas, el cual, como su nombre lo indica posee menos pérdidas que el cable de interconexión regular, y se usa cuando hay que colocar la antena a una distancia considerable del dispositivo de radiofrecuencia; aunque es un cable bajo en pérdidas debe siempre de usarse la distancia más corta posible.

Se debe tomar en cuenta que cada modelo de antena incluye un cable con una longitud específica, la cual se puede encontrar normalmente en las hojas de datos.

**Tabla 6.1** Tipos de cables bajos en pérdidas de la serie Cisco Aironet

Modelo Anterior	Nuevo Modelo	Longitud (m)	Pérdidas (dB/m)
AIR-420-003346-020	AIR-CAB020LL-R	6	1.3
AIR-420-003346-050	AIR-CAB050LL-R	15	3.4
AIR-420-003346-075	AIR-CAB100ULL-R	23	5
AIR-420-003346-100	AIR-CAB100ULL-R ó AIR-CAB150ULL-R	30	6.7

El cable utilizado en la actualidad por la compañía es el **AIR-CAB020LL-R**, el cual presenta una impedancia de 50  $\Omega$ , y un total de pérdidas incluyendo los conectores, de 7.8 dB.

#### 6.1.5. PARARRAYOS.

Cuando se usan antenas en instalaciones exteriores es necesario proteger estos sistemas de comunicación con pararrayos debido a que estos sistemas están expuestos a descargas eléctricas naturales o estáticas que podrían dañar permanentemente los equipos.

Estos dispositivos se colocan entre la conexión de la antena y la conexión al dispositivo RF y poseen una línea a tierra, de esta manera en caso de que una descarga eléctrica se presente, su trayectoria sería hacia la conexión a tierra y no hacia el equipo de RF como podría suceder en caso de no poseer éste sistema de protección.

## 6.2. TIPOS DE ANTENAS.

### 6.2.1. ANTENAS PARA ADAPTADORES DE RED.

Las antenas para este tipo de dispositivos son generalmente omnidireccionales, lo que significa que la cobertura horizontal, o bien el ancho del haz horizontal es de 360° y poseen la particularidad de que cuentan con un sistema de diversidad dual, el cual consiste en que el sistema de antenas mide continuamente las señales de radiofrecuencia entrantes y selecciona automáticamente la mejor situada para recibirlas.

#### 6.2.1.1. Antena dipolo AIR-ANT3351.

Su característica principal consiste en su fácil manejo y su capacidad de ampliar el alcance en las computadoras que usen adaptadores de Cliente tipo *PC Card*, además su sistema de diversidad dual le permite mejorar la comunicación.



**Figura 6.1** Antena dipolo AIR-ANT3351.



**Tabla 6.2.** Características de la antena AIR-ANT3351.

<b>Modelo</b>	<b>AIR-ANT3351</b>
<b>Aplicación</b>	Antena con diversidad para interiores.
<b>Ganancia</b>	2.2 dBi
<b>Alcance a 1 Mbps</b>	107 m
<b>Alcance a 11 Mbps</b>	31 m
<b>Ancho del haz</b>	360° H, 75° V
<b>Longitud del cable</b>	1.5 m
<b>Dimensiones</b>	Base (18 cm x 5 cm) Altura (20cm)
<b>Peso</b>	261 g

#### **6.2.1.2. Antena omnidireccional de alta ganancia AIR-ANT1728.**

La Figura 6.2 nos muestra este tipo de antena cuyas características principales consisten en su gran ganancia (5.2 dBi), respecto a las otras antenas para puntos de acceso y omnidireccionalidad, lo que hace que tenga un alcance medio.



**Figura 6.2** Antena modelo AIR-ANT1728 para AP.

A continuación se presenta la tabla 6.3, la cual resume las principales características de esta antena omnidireccional de gran ganancia.

**Tabla 6.3** Características de la antena AIR-ANT1728.

<b>Modelo</b>	<b>AIR-ANT1728</b>
<b>Aplicación</b>	Antena para interiores, alcance Medio, colocada en techo.
<b>Ganancia</b>	5.2 dBi
<b>Alcance a 1 Mbps</b>	151 m
<b>Alcance a 11 Mbps</b>	44 m
<b>Ancho del haz</b>	360° H, 75° V
<b>Longitud del cable</b>	0.91 m
<b>Dimensiones</b>	Longitud (22.86 cm) Diámetro (2.5 cm)
<b>Peso</b>	131 g

#### **6.2.1.3. Antena direccional de montaje en pared AIR-ANT3549.**

La Figura 6.3 nos muestra este tipo de antena cuyas características principales consisten en su alta ganancia (8.5 dBi), respecto a las otras antenas para Puntos de acceso y direccionalidad, lo que hace que tenga un gran alcance sin obstáculos, además por su forma y dimensiones es ideal para instalar en paredes, puede usarse adicionalmente como antena de puente de alcance medio en este caso a 1 Mbps se tendría un alcance de 3.2 Km y a 11 Mbps un alcance de 1.032 m.



**Figura 6.3** Antena direccional AIR-ANT3549 para AP.

A continuación se presenta la tabla 6.4, la cual resume las principales características de esta antena direccional de largo alcance.

**Tabla 6.4.** Características de la antena AIR-ANT3549.

<b>Modelo</b>	<b>AIR-ANT3549</b>
<b>Aplicación</b>	Antena para interiores, de largo alcance sin obstrucciones, normalmente se coloca en una pared.
<b>Ganancia</b>	8.5 dBi
<b>Alcance a 1 Mbps</b>	213 m
<b>Alcance a 11 Mbps</b>	61 m
<b>Ancho del haz</b>	60° H, 55° V
<b>Longitud del cable</b>	0.91 m
<b>Dimensiones</b>	12.4cm x 12.4cm
<b>Peso</b>	150 g

## **CAPITULO 7: MARCO TEORICO DEL RECOLECTOR DE DATOS (*LOCUST*)**

### **Breve explicación del capítulo**

El presente capítulo permitirá al lector conocer los menús ofrecidos por el *LOCUST* para lograr una correcta recolección de datos en el sitio donde se encuentra la red inalámbrica (*Site Survey*).

### **7.1. FUNCIONAMIENTO**

Este aparato receptor portátil, fue diseñado para realizar un barrido de las señales en RF y así lograr optimizar las redes *WLAN*. Este instrumento realiza mediciones de cobertura en redes CDMA y opera estrictamente bajo el estándar 802.11b, permitiendo determinar el Puntos de Acceso, PER (Razón de Pérdidas por Paquetes) y niveles de señales RSSI (*Received Signal Strength Indicator*). El *LOCUST* detecta y diferencia lo que son interferencias de banda angosta por *multipath* y sistemas con saltos de frecuencias.

### **7.2. DESCRIPCIÓN FÍSICA**

El *LOCUST* es un aparato portátil de tamaño relativamente pequeño. Cuenta con una pantalla LCD que constituye casi la tercera parte de su área frontal. Además, presenta una interfaz para el usuario por medio un teclado y luces indicadoras. Debe colocársele una pequeña antena omnidireccional y puede ser utilizado en conjunto con un GPS.

### 7.2.1. DESCRIPCIÓN DE LUCES INDICADORAS

**Receive:** Normalmente parpadea color amarillo constantemente cuando está rastreando estaciones o AP's.

**GPS power:** Debe presentar una luz verde sólo si se coloca un GPS.

**Logging:** Normalmente está apagado. Indica si se está utilizando la memoria *flash*.

## 7.2.2. DESCRIPCIÓN DE FUNCIONES POR TECLAS

**POWER:** Únicamente se utiliza una vez cuando se enciende o apaga el aparato.

**SETUP:** Nos lleva al menú de "Info Screen".

→**GPS:** ON/OFF (debe tenerse en OFF si no se tiene conectado un GPS)

→**Initiate Card:** Cumple la función de Reset

→**Display:** Presenta dos opciones

a) *AP's only* (Rastrea únicamente Puntos de Acceso)

b) *All STAs* (Rastrea todos los equipos de RF en esta banda)

**ESC:** Retrocede un nivel.

**ENT:** Avanza un nivel.

## 7.3. MENUS

El menú principal consiste en cinco apartados:

- *Select AP*
- *Select PER AP*
- *Survey Mode*
- *Scan for AP's*
- *Spectrum*

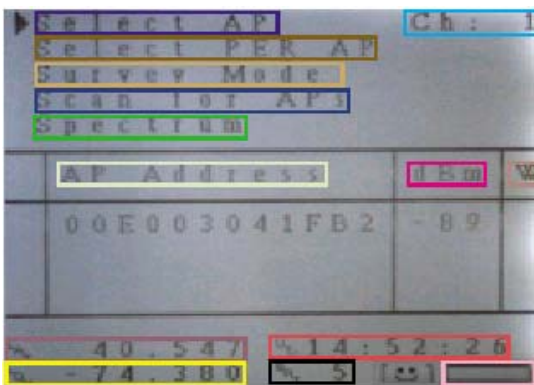


Figura 7.1 Ventana Principal del LOCUST

### 7.3.1. SELECT AP

Para ingresar a este submenú se debe presionar la tecla *ENT* para seleccionar el Punto de Acceso que se desea estudiar, en la ventana principal. Una vez escogido el AP se debe volver a presionar *ENT*.

Aquí se despliega información de potencia en dBm y la Correlación vrs *Chips*.

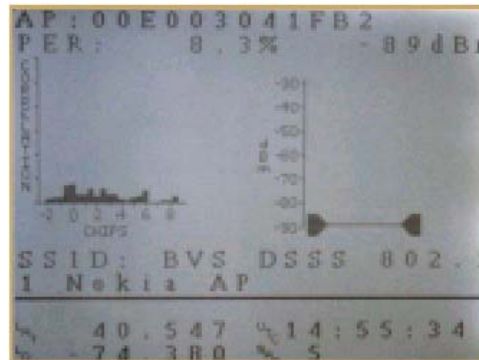


Figura 7.2 Ventana de submenú *Select AP* del LOCUST

Para volver al menú principal, presionar ESC.

### 7.3.2. SELECT PER AP

En este submenú se presenta la Razón de Pérdidas por Paquetes (PER) que presenta el AP escogido. Se rastrea principalmente cuatro diferentes velocidades: 1, 2, 5.5 y 11 Mbps; indicándose para cada uno el PER y el uso actual.

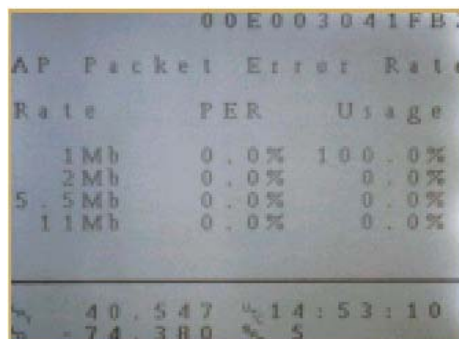
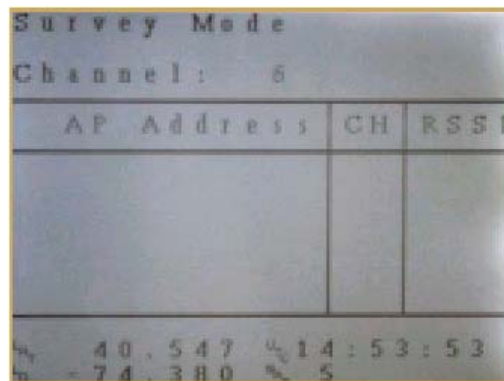


Figura 7.3 Ventana de submenú *Select PER AP* del LOCUST

Para volver al menú principal, presionar ESC.

### 7.3.3. SURVEY MODE

En esta opción rastrea 14 canales de manera simultánea, y se despliega los AP que se encuentran funcionando en cada uno de ellos. También se despliega su respectivo RSSI.



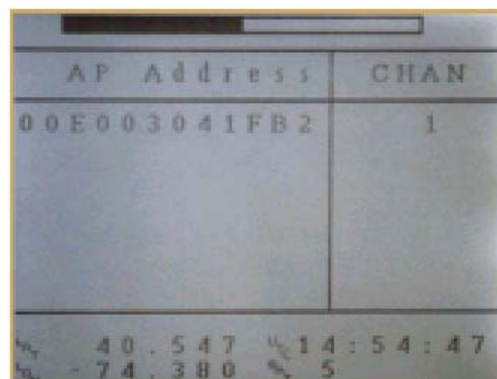
AP Address	CH	RSSI
------------	----	------

Figura 7.4 Ventana de submenú *Survey Mode* del *LOCUST*

Para volver al menú principal, presionar ESC.

### 7.3.4. SCAN FOR AP'S

Realiza un barrido en frecuencia buscando Puntos de Acceso



AP Address	CHAN
00E003041FB2	1

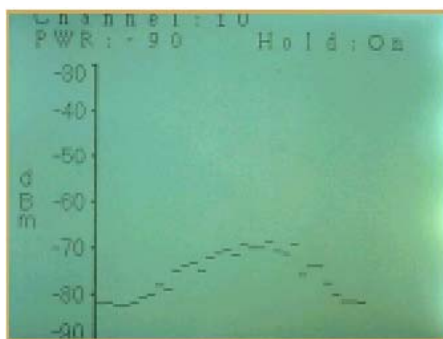
Figura 7.5 Ventana de submenú *Scan for AP's* del *LOCUST*



Para volver al menú principal, presionar ESC

### 7.3.5. SPECTRUM

Despliega en tiempo real todo el RSSI a lo largo de un ancho de banda de 22 MHz. El pico de potencia es indicado numéricamente tan pronto como el canal a sido rastreado.



**Figura 7.6** Ventana de submenú *Spectrum* del *LOCUST*

Para volver al menú principal, presionar ESC

## CAPITULO 8: GUIA PARA LA INSTALACION DE AP 350

### Breve explicación del capítulo

En este capítulo se hará referencia a la configuración paso a paso, para lograr el acceso a la configuración del AP 350 mediante el navegador en modo gráfico.

Posteriormente se hará dar un paseo por los principales menús que contiene el AP y se dará una referencia teórica acerca de los principales parámetros que presenta el mismo. Los gráficos mostrados han sido tomados de la configuración por defecto que presenta el AP de fábrica.

### Antes de comenzar

- 1) Asegúrese de tener conectado, al menos una antena al conector PRIMARY del AP. Esto es muy importante.
- 2) Debe realizarse la conexión del cable al puerto de *Ethernet*, para proveer la energía al AP. Para esto vea la **Opción 3** del Diagrama de Conexión del *Power Injector*, en la [Figura B.2.1](#) de los Anexos. Nota: No incluya el *Switch* para ésta configuración inicial.
- 3) Conecte el cable serie DB-9 a DB-9, a la respectiva interfaz serie DB-9 del AP, así como al puerto COM de su computador, para realizar la configuración respectiva. Este cable utilizado debe ser un *rollover*. Ver [Figura B.2.2](#) en Anexos.
- 4) Ejecute algún *software* de acceso al puerto Serie. En su defecto, utilice el *Hyperterminal*, el cual viene incluido en las versiones más actuales de WINDOWS.

## 8.1. INGRESAR AL PUNTO DE ACCESO AIRONET 350 POR PRIMERA VEZ

Una vez inicializado el Punto de Acceso , se obtiene ésta primera pantalla.

```

AP0001 [Cisco 350 Series AP 12.00T] Uptime: 00:00:51
-----
Associations
[Clnts: 0] of 1 [Rptrs: 0] of 0 [Brdgs: 0] of 0 [APs]: 1
-----
Events Time Severity Description
00:01:41 (Warning): Lost Authentication with Parent
00:01:28 (Warning): Ethernet Link Lost. Attempting to re-establish link to primary network.
00:01:16 (Info): Station 00022d8449ca roamed
00:01:16 (Warning): No DHCP OFFER's received, restarting the negotiation in the background
-----
Network Ports ==[Diagnostics]==
Device Status Mb/s IP Addr. MAC Addr.
[Ethernet] No Link 0.0 10.0.0.1 0040965c9433
[Rptr Radio] No Link 11.0 10.0.0.1 0040965c9433
-----
Home - [Network] - [Associations] - [Setup] - [Logs] - [Help]
(Auto Apply On) :Top, :Up, ^R, =, <ENTER>, or [Link Text]:

```

Figura 8.1 Configuración inicial en AP virgen

Para ingresar al modo de configuración se escribe **S** (de Setup), y se despliegan las siguientes opciones a configurar.

```

AP350-5c9433 Setup Uptime: 00:25:15
==[Express Setup]==
Associations
[Defaults Associations] [Address Filters] [Advanced]
[Port Assignments]
[Protocol Filters] [VLAN] [Service Sets]
Event Log
[Defaults Event] [Event Handling] [Notifications]
Services
[Console/Telnet] [Boot Server] [Routing] [Name Server]
[Time Server] [FTP] [Web Server] [SNMP]
[Cisco Services] [Security] [Accounting]
Network Ports ==[Diagnostics]==
[Id Ethernet] [Hw Ethernet] [Fltr Ethernet] [Adv Ethernet]
[Id Rptr Radio] [Hw Rptr Radio] [Fltr Rptr Radio] [Adv Rptr Radio]
-----
[Home] - [Network] - [Associations] - Setup - [Logs] - [Help]
[END]

```

Figura 8.2 Menú de configuración ó SETUP

**Nota Importante:** Antes de realizar cualquier cambio en el AP, debe realizarse lo siguiente:

- 1) En la sección de *Network Ports*, ingresar al *Ethernet Hardware*, digitando **Hw E**.
- 2) Una vez dentro, debe cambiar en el parámetro *Lost of Backbone Connectivity Action*, a **NO ACTION**.
- 3) Seleccionar **APPLY**.

El menú de *EXPRESS SETUP* es un menú adicional al de *SETUP* (teclea **E**), por esta razón se abre una nueva ventana.

AP350-5c9433	<b><u>Express Setup</u></b>	Uptime: 00:45:47
System [Name	][Prueba1	]
[Terminal Type	][teletype]	
MAC Address	: 00:40:96:5c:94:33	
Config. Server [Protocol	][NONE ]	
IP [Address	][172.20.17.175 ]	
IP [Subnet Mask	][255.255.255.0 ]	
Default [Gateway	][255.255.255.255]	
[Service Set ID (SSID)	][ab3 ]	
[Role in Radio Network	][Root Access Point ]	
[Optimize Radio Network For	][Throughput] [Hw Radio]	
Ensure Compatibility With:	[2Mb/sec Clients][X]	
	[non-Aironet 802.11][ ]	
[Security Setup]		
[SNMP Admin. Community	][ ]	
[Apply] [OK] [Cancel] [Restore Defaults]		
(Auto Apply On) :Bottom, :Down, :Back, ^R, =, <ENTER>, or [Link Text]:		

Figura 8.3 Configuración del *EXPRESS SETUP*

Ahora sí es posible empezar a realizar cambios en el AP.

Para cada uno de los parámetros se deben seguir los pasos para cada uno.

**Nota:** Las letras **o** (*OK*), **Ap** (*Apply*), **c** (*Cancel*), **re** (*Restore Defaults*); están reservadas para las instrucciones especificadas dentro del respectivo paréntesis.

Cambiar nombre del sistema (AP):

- 1) Ingrese la instrucción **na** (de *name*)
- 2) Aparecerá en su pantalla  
**Enter Name:** (escriba el nombre deseado aquí)
- 3) Presione **ENTER**

Cambiar el *terminal type* (tipo de terminal):

- 1) Presione **t** (de *terminal*)
- 2) Aparecerá en su pantalla  
**Please select an item from the following or hit <ENTER>**  
**Values: [teletype] [ANSI]** (Escoja alguno de los dos valores: *Teletype* o *ANSI* )
- 3) Presione **ENTER**

**Recomendación:** Escoja *teletype* para realizar la configuración la primera vez.

**OJO:** La *MAC address* o *dirección MAC*, no se puede cambiar ya que es un valor único y se encuentra escrito en la ROM del AP.

Cambiar la configuración del servidor:

- 1) Presione **pr** (de *protocolo*)
- 2) Aparecerá en su pantalla  
**Please select an item from the following or hit <ENTER>**  
**Values: [None] [BOOTP] [DHCP]** (Escoja alguno de los tres: Ninguno, Bootp o DHCP)
- 3) Presione **ENTER**

**Recomendación:** Utilice la opción *None* para configurar el AP por primera vez.

Cambiar la dirección IP:

- 1) Presione **ad** (de *address*)
- 2) Aparecerá en su pantalla

**Enter Address:X.X.X.X** (Escoja la dirección respetando el siguiente formato)

- 3) Presione **ENTER**

**Observación:** En este caso se escogió un IP dentro de la misma subred del Cliente (172.20.17.175).

**Nota:** Esta dirección debe encontrarse dentro de la misma subred del Cliente o Clientes (PC).

Cambiar la máscara de red:

- 1) Presione **su** (de *subnet mask*)
- 2) Aparecerá en su pantalla

**Enter Subnet Mask: X.X.X.X** (Escoja la submáscara respetando el siguiente formato)

- 3) Presione **ENTER**

Cambiar la dirección del *default gateway*:

- 1) Presione **g** (de *gateway*)
- 2) Aparecerá en su pantalla

**Enter Gateway:X.X.X.X** (Escoja la dirección respetando el siguiente formato)

- 3) Presione **ENTER**

Cambiar el *Service Set ID*:

- 1) Presione **ser** (de *Service Set ID*)
- 2) Aparecerá en su pantalla

**Enter Service Set ID (SSID):**

(Digite el que desee, diferente a **Tsunami**, el cual es el valor por defecto de Cisco)

- 3) Presione **ENTER**

**Nota:** El SSID que coloque al AP debe ser el mismo que el del Cliente.

Cambiar el Rol in Radio Network:

- 1) Presione **ro** (de *rol in radio network*)
- 2) Aparecerá en su pantalla

**Please select an item from the following or hit <ENTER>**

**Values: [Root Access Point] [Repeater Access Point] [Site Survey Client ]**

(Escoja el modo de operación de su AP en la red)

- 3) Presione *ENTER*

**Observación:** Para efectos de configuración por primera vez, es mejor utilizar la opción *Root Access Point*.

Cambiar la optimización de la radiofrecuencia (*Optimize Radio Network For*):

- 1) Presione **op** (de *Optimize Radio Network For*)
- 2) Aparecerá en su pantalla

**Please select an item from the following or hit <ENTER>**

**Values: [Throughput] [Range] [Custom]** (Escoja alguno de las 3 opciones)

- 3) Presione *ENTER*

Cambiar la compatibilidad:

- 1) Presione **2** (de *2Mb/sec Clients*) si lo que desea es compatibilidad con equipos Cisco ó **no** (*non-Aironet 802.11*)

**Recomendación:** Utilizar la opción de *2Mb/sec Clients*, ya que ofrece compatibilidad total con los equipos Cisco.

Una vez realizado las configuraciones necesarias, debe digitar AP (*APPLY*).

## 8.2. CREAR UN NUEVO PERFIL DE USUARIO A LA NIC

Para crear un nuevo perfil, se debe ir al ESCRITORIO y presionar en el ícono del Cliente de Cisco (ACU).



Figura 8.4 Icono de Cliente Aironet en el Escritorio

Una vez dentro del ACU, seleccionar **Profile Manager** para crear un nuevo Perfil.

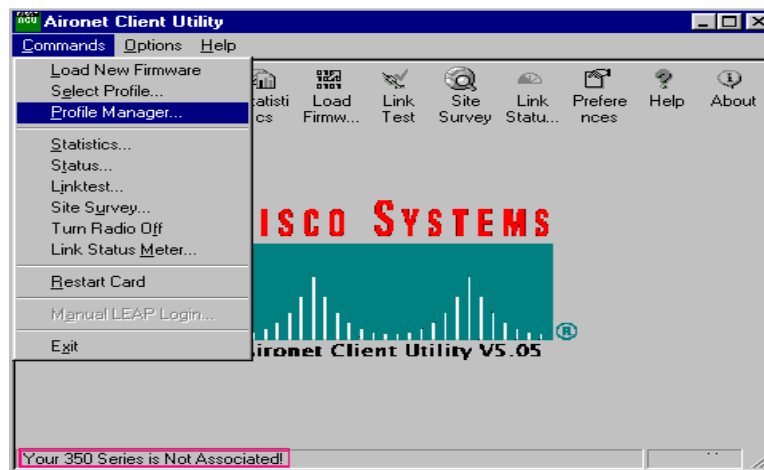
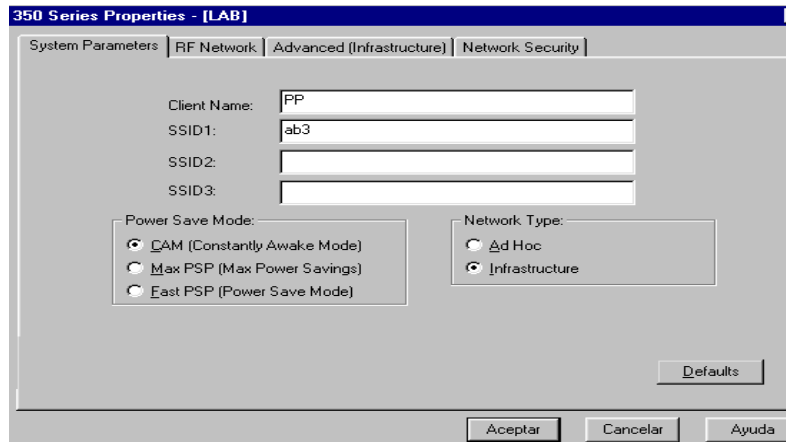


Figura 8.5 Edición del nuevo perfil de usuario

Note en la parte inferior de la ventana, la no asociación de su PC al AP, todavía. Se debe crear un nuevo perfil presionando ADD.

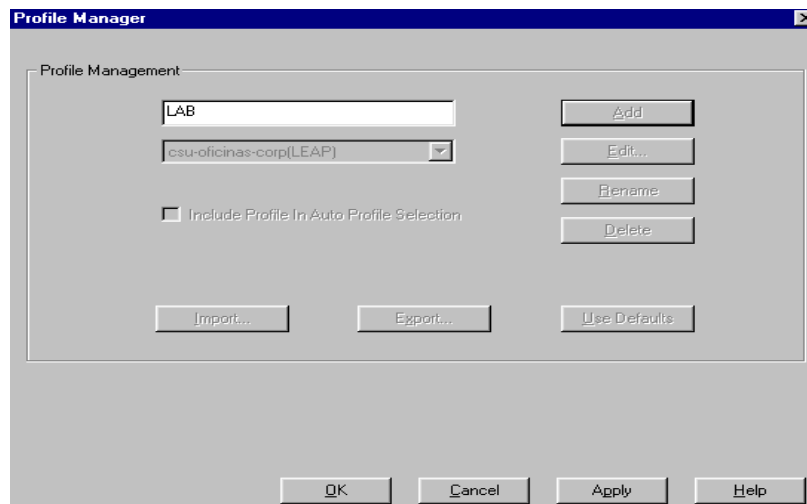




**Figura 8.6** Configuración del SSID en el perfil de usuario.

Luego presione OK.

En este paso se debe indicar el nombre del Cliente (PC) y un código correspondiente al SSID igual al ingresado al AP.



**Figura 8.7** Escogencia del perfil del usuario.

### 8.3. INGRESE A UNA SECCIÓN HTTP PARA CONEXIÓN EN MODO GRÁFICO CON AP

Se debe iniciar una sesión en el navegador, presionado el icono de *EXPLORER* ubicado en el ESCRITORIO.



Figura 8.8 Icono del Explorador de Internet

Debe iniciar una sesión Http en el navegador, escribiendo la dirección IP asignada al AP.

**Prueba1 Summary Status - Microsoft Internet Explorer**

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Adelante Detener Actualizar Inicio Búsqueda Favoritos Historial Correo

Dirección <http://172.20.17.175>

---

**Prueba1 Summary Status** **CISCO SYSTEMS**

**Cisco 350 Series AP 12.00T** Uptime: 01:26:52

Home Map Network Associations Setup Logs Help

**Current Associations**

<b>Clients: 1 of 2</b>	<b>Repeaters: 0 of 0</b>	<b>Bridges: 0 of 0</b>	<b>APs: 1</b>
------------------------	--------------------------	------------------------	---------------

**Recent Events**

Time	Severity	Description
01:26:44	<a href="#">Info</a>	Station [PP1000a8afaa14a] Reassociated
01:26:44	<a href="#">Info</a>	Station [PP1000a8afaa14a] Authenticated
01:26:44	<a href="#">Info</a>	Deauthenticating [PP1000a8afaa14a], reason "Not Authenticated"
01:26:41	<a href="#">Info</a>	Station 00022d8449ca roamed
01:25:21	<a href="#">Info</a>	Disassociating 00022d8449ca, reason "Not Associated"

**Network Ports** *Diagnostics*

Device	Status	Mb/s	IP Addr.	MAC Addr.
Ethernet	No Link	0.0	172.20.17.175	0040965c9433
AP Radio	Up	11.0	172.20.17.175	0040965c9433

Figura 8.9 Inicio de sesión HTTP y página principal de HOME

## 8.4. DESCRIPCIÓN DE CADA UNO DE LOS PARÁMETROS DEL PUNTO DE ACCESO

Como se puede notar, existen 7 submenús en la parte superior:

**Home:** También denominado *SUMMARY STATUS* (Resumen de Estados). Este corresponde a la pantalla desplegada anteriormente.

**Map:** Esta opción va a desplegar en siguiente menú, el cual permite una navegación rápida hasta el resto de los apartados, ya que presenta *links* (enlaces).

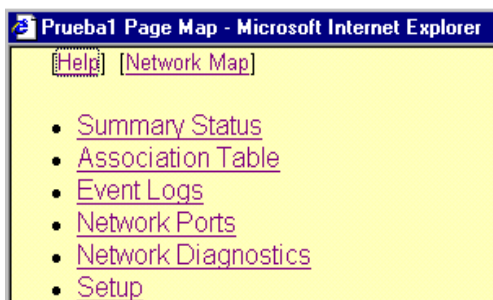


Figura 8.10 Página principal de MAP

**Network:** Como se puede observar en la opción de MAP, este menú es conocido como *Network Ports*. Se despliega la siguiente ventana, en la cual se observa detalladamente las estadísticas de recepción y transmisión, así como el SSID.

Pruebal **Network Ports**

Network Diagnostics VLAN Service Sets

Home Map Network Associations Setup Logs Help Uptime: 03:44:08

Name	Ethernet*	AP Radio
Status	No Link	Up
Max. Mb/s	0.0	11.0
IP Addr.	172.20.17.175	172.20.17.175
MAC Addr.	0040965c9433	0040965c9433
Radio SSID		ab3
<i>Receive</i>		
unicast pkts.	0	1528
multicast pkts.	0	0
total bytes	0	102872
errors	0	0
discards	0	0
forwardable pkts.	1374	563
filtered pkts.	0	0
<i>Transmit</i>		
unicast pkts.	0	450
multicast pkts.	44	1000
total bytes	5280	462310
errors	179	0
discards	0	0
forwarded pkts.	224	2099

Figura 8.11 Página principal de *Network Ports*

### Identificando Información y Estado:

- *Name* — Nombre: Despliega el nombre de la interfaz de la red. El asterisco junto al nombre identifica el puerto como el puerto primario para el AP.
- *Status* — Estado: Despliega 3 posibles estados de operación del puerto:
  - Up* (Arriba): El puerto se encuentra operando de manera apropiada.
  - Down* (Abajo): El puerto no está operando.
  - Error*: El puerto está operando pero presenta un error de condición.
- *Max Mb/s*: Máxima tasa de transmisión de datos en Megabits por segundo.
- *IP Addr* — Dirección IP del puerto: Cuando el AP está configurado en modo *Standby* el puerto *Ethernet* y el de Radio utilizan distintas direcciones IP.
- *MAC* (Control de Acceso al Medio): Es un identificador único asignado a la interfaz de red por el fabricante.
- *Radio SSID*: Identificador único que los Clientes necesitan para asociarse con el AP.

### Received ( Datos recibidos):

- *Unicast pkts*: El número de paquetes recibidos en una comunicación punto a punto.
- *Multicast pkts*: Número de paquetes recibidos que fueron enviados como transmisión para establecer nodos.
- *Total bytes*: Número total de *bytes* recibidos.
- *Errors*: Número de paquetes con errores.
- *Discards*: Número de paquetes descartados por el AP debido a errores ó congestión de la red.
- *Forwarded pkts*: Número de paquetes recibidos por el puerto que fueron aceptados o pasados a través de filtros.
- *Filtered pkts*: Número de paquetes que fueron detenidos por los filtros colocados a los puertos.

### Transmitted (Datos Transmitidos):

- *Unicast pkts*: El número de paquetes transmitidos en una comunicación punto a punto.
- *Multicast pkts*: Número de paquetes transmitidos que fueron enviados como transmisión para establecer nodos.
- *Total bytes*: Número total de *bytes* transmitidos.
- *Errors*: Número de paquetes con errores.
- *Discards*: Número de paquetes descartados por el AP debido a errores o congestión de la red.
- *Forwarded pkts*: Número de paquetes transmitidos por el puerto que fueron aceptados o pasados a través de filtros.

**Association:** Su nombre completo es ASSOCIATION TABLE (Tabla de Asociación). Presenta una lista de los dispositivos conectados a la red con sus respectivos enlaces. Se despliega el siguiente menú.

Pruebal **Association Table**

Network Diagnostics VLAN Service Sets

Home Map Network Associations Setup Logs Help

Uptime: 04:00:32

Client  Repeater  Bridge  AP  Infra. Host  Multicast  Entire Network

Press to Change Settings:

Association Table <span style="float: right;"><i>additional display filters</i></span>						
Device	Name	IP Addr./Name	MAC Addr.	VLAN	State	Parent
350 Series AP	Pruebal	172.20.17.175	0040965c9433			
350 Series Client	PP	172.20.17.174	000a8afaal4a		Assoc	[self]

Figura 8.12 Página principal de la Tabla de Asociación.

Este menú no presenta parámetro alguno para configuración.

**Setup:** El menú de SETUP (Configuraciones) es el que nos permitirá realizar los cambios deseados en el funcionamiento del AP.

Pruebal **Setup**

Cisco 350 Series AP 12.00T

Home Map Network Associations Setup Logs Help

Uptime: 04:04:44

[Express Setup](#)

Associations			
<a href="#">Display Defaults</a>		<a href="#">Port Assignments</a>	<a href="#">Advanced</a>
<a href="#">Address Filters</a>	<a href="#">Protocol Filters</a>	<a href="#">VLAN</a>	<a href="#">Service Sets</a>

Event Log		
<a href="#">Display Defaults</a>	<a href="#">Event Handling</a>	<a href="#">Notifications</a>

Services			
<a href="#">Console/Telnet</a>	<a href="#">Boot Server</a>	<a href="#">Routing</a>	<a href="#">Name Server</a>
<a href="#">Time Server</a>	<a href="#">FTP</a>	<a href="#">Web Server</a>	<a href="#">SNMP</a>
<a href="#">Cisco Services</a>	<a href="#">Security</a>	<a href="#">Accounting</a>	

Network Ports <span style="float: right;"><i>Diagnostics</i></span>				
<b>Ethernet</b>	<a href="#">Identification</a>	<a href="#">Hardware</a>	<a href="#">Filters</a>	<a href="#">Advanced</a>
<b>AP Radio</b>	<a href="#">Identification</a>	<a href="#">Hardware</a>	<a href="#">Filters</a>	<a href="#">Advanced</a>

Figura 8.13 Página principal de SETUP

**Logs:** También conocido como *Event Logs*. Esta tabla se está actualizando constantemente, monitoreando los eventos que ocurren a la red. Se despliega la siguiente ventana.

**Prueba1 Event Log**

Home Map Network Associations Setup Logs Help

Uptime: 04:09:16

Index:  Number of Events:  [Download Event Log](#)

Press to Change Settings: [Next](#) [Prev](#) [Apply New](#) [Purge Log](#)

Time	Severity	Description
01:56:39	Info	Station [PP1000a8afaa14a] Associated
01:56:39	Info	Station [PP1000a8afaa14a] Authenticated
01:56:19	Info	Deauthenticating [PP1000a8afaa14a, reason "Inactivity"
01:27:45	Info	Station [PP1000a8afaa14a] Associated
01:27:45	Info	Station [PP1000a8afaa14a] Authenticated
00:43:17	Info	Station [PP1000a8afaa14a] Associated
00:43:17	Info	Station [PP1000a8afaa14a] Authenticated
00:39:27	Info	Station [PP1000a8afaa14a] Associated
00:39:27	Info	Station [PP1000a8afaa14a] Authenticated
00:31:38	Info	Station [PP1000a8afaa14a] Associated
00:31:38	Info	Station [PP1000a8afaa14a] Authenticated
00:28:03	Info	Station [PP1000a8afaa14a] Associated
00:28:03	Info	Station [PP1000a8afaa14a] Authenticated

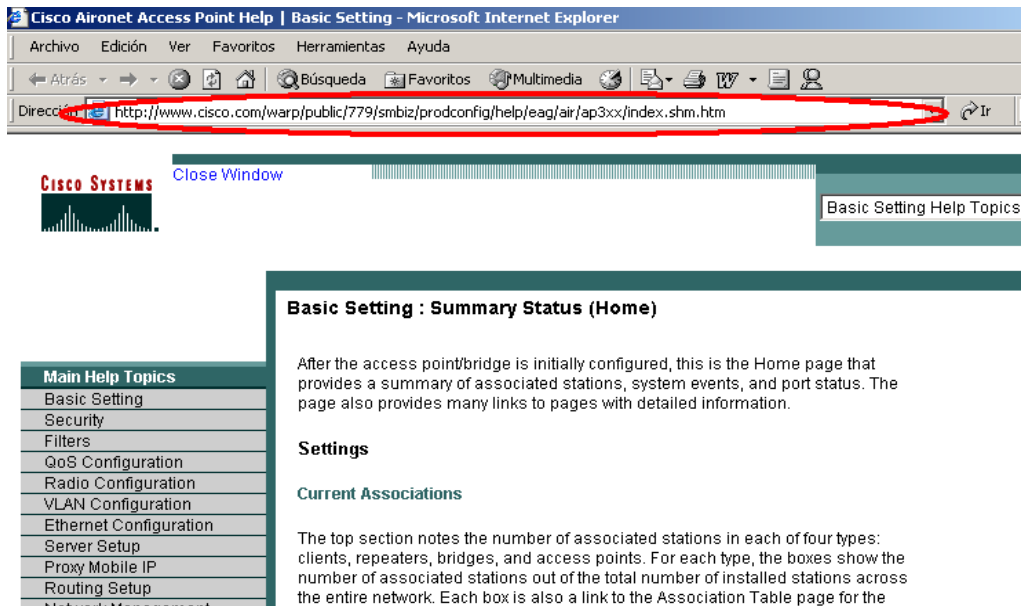
**Figura 8.14** Página principal del *Event Log*.

En el encabezado de esta página se encuentran los siguientes parámetros:

- *Time*—Tiempo: Representa el tiempo al cual ocurrió el evento.
- *Severity*—Severidad: Los eventos son clasificados en 4 niveles de severidad, dependiendo del impacto que tenga en las operaciones de la red:
  - Info* (Verde): Indica información de rutina, sin errores.
  - Warning* (Azul): Indica una condición potencial de error.
  - Alert* (Magenta): Indica que un evento que paso de estado de *Warning* (Advertencia) a un nivel superior de severidad.
  - Fatal* (rojo): Un evento que evita la operación de un puerto o dispositivo.

- *Description*—Descripción: Esta columna describe la naturaleza o la fuente de un evento. Si un dispositivo de la red es involucrado en el evento, su dirección MAC o IP aparece y provee un enlace directo a la página de la estación.

**Help:** Establece un enlace con la página oficial de la serie Aironet en Cisco.com



**Figura 8.15** Página de Ayuda para AP's



## ENFOQUE: MENÚ DE *SETUP* (CONFIGURACIONES)

Ver la ventana principal de menú de *Setup* en la [Figura 8.13](#).

En esencia este menú presenta 6 submenús:

### **Associations:**

Esta tabla de Asociación del sistema presenta todos los posibles dispositivos inalámbricos conectados a la *LAN* alamburada.

Este submenú presenta 7 opciones de configuración:

#### A) **DISPLAY DEFAULTS**—DESPLIEGUE DE PARÁMETROS POR DEFECTO

Pruebal **Association Table Filters**

Cisco 350 Series AP 12.00T

Map Help Uptime: 00:14:53

**Stations to Show:**

<input checked="" type="checkbox"/> Client	<input checked="" type="checkbox"/> Repeater	<input checked="" type="checkbox"/> Bridge	<input checked="" type="checkbox"/> AP
<input type="checkbox"/> Infra. Host	<input type="checkbox"/> Multicast	<input type="checkbox"/> Entire Network	

**Fields to Show:**

<input checked="" type="checkbox"/> System Name	<input checked="" type="checkbox"/> IP Address	<input checked="" type="checkbox"/> VlanID	<input type="checkbox"/> SSID	<input checked="" type="checkbox"/> Device
<input type="checkbox"/> Class	<input checked="" type="checkbox"/> State	<input checked="" type="checkbox"/> Parent	<input type="checkbox"/> SW Version	

**Packets To/From Station:**

<input type="checkbox"/> Total	<input type="checkbox"/> Alert
--------------------------------	--------------------------------

**Bytes To/From Station:**

<input type="checkbox"/> Total	<input type="checkbox"/> Alert
--------------------------------	--------------------------------

**Primary Sort:**

Device  System Name  IP Addr./Name  MAC Address  VLAN  SSID  Class  Parent

**Secondary Sort:**

Device  System Name  IP Addr./Name  MAC Address  VLAN  SSID  Class

OK Cancel Restore Defaults

Figura 8.16 Página principal de *Display Defaults* en apartado de *Associations*.

- *Stations to Show* — Tipos de estaciones a mostrar: Mediante las cajitas de selección se puede escoger los dispositivos que se desea se muestren en la Tabla de Asociación.

- *Fields to Show* — Campos a mostrar de las estaciones: Mediante cajitas de selección se escogen los parámetros de estado más importante de los dispositivos escogidos, que desean desplegarse.
- *Primary Sort* — Clasificación primaria: Escogencia del parámetro de despliegue en la primera columna (de izquierda a derecha) de la Tabla de Asociación.
- *Secondary Sort* — Clasificación secundaria: Escogencia del parámetro de despliegue en la segunda columna (de izquierda a derecha) de la Tabla de Asociación.

## B) ADDRESS FILTERS — FILTROS DE DIRECCIONES

Pruebal **Address Filters**

**Cisco 350 Series AP 12.00T**

Map Help Uptime: 00:18:31

**New MAC Address Filter:**

Dest MAC Address:

Allowed  Disallowed

The default settings for multicast and unicast destination MAC addresses transmitted from each network interface are specified on the Advanced Setup page for that network interface.

**Existing MAC Address Filters:**

Lookup MAC Address on [Authentication Server](#) if not in Existing Filter List?  yes  no

Is MAC Authentication alone sufficient for a client to be fully authenticated?  yes  no

**Figura 8.17** Página principal de *Address Filters* en apartado de *Associations*.

Los filtros de direcciones MAC permiten o no, el envío de paquetes *Unicast* o *Multicast*, ambos enviados desde o dirigidos hacia una dirección MAC específica.

Pueden crearse filtros que pasen tráfico a todas las direcciones MAC excepto aquellas que se especifiquen (**Allowed**), ó bien crear filtros que bloqueen el tráfico de todas las direcciones MAC excepto aquellas que sean especificadas (**Disallowed**).

- *New MAC address filter* — Nueva dirección MAC para filtro: Ingresa la nueva dirección MAC a ser filtrada.
- *Existing MAC address filters* — Filtros de direcciones MAC existentes: Lista de direcciones existentes que van a ser filtradas.
- *Lookup MAC address on Authentication Server if not in Existing Filter List?* — Buscar direcciones MAC en el Servidor de Autenticación si no existe lista de filtros?:

**YES:** Ir a buscar la lista en el servidor.

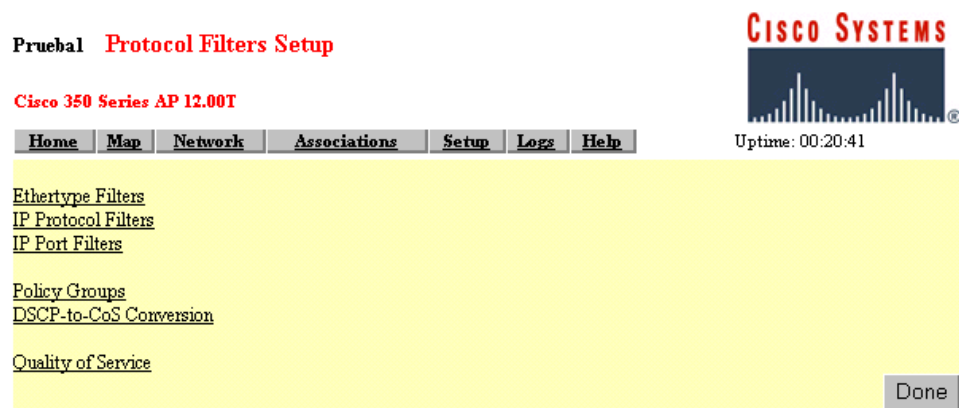
**NO:** No realiza acción alguna.

- *Is MAC Authentication alone sufficient for a client to be fully authenticated?* — Es suficiente la autenticación por MAC para que un Cliente sea totalmente autenticado?:

**YES:** Si es suficiente para lograr una autenticación.

**NO:** Debe chequear otros dispositivos de seguridad para ser autenticado, tal como *LEAP*.

### c) *PROTOCOL FILTERS* — FILTROS PARA PROTOCOLOS



**Figura 8.18** Página principal de *Protocol Filters* en el apartado de *Associations*.

Los filtros de protocolos previenen el uso de protocolos específicos a través del AP. Se puede configurar filtros de protocolos y habilitar cada filtro para una o más VLAN's. Se puede filtrar protocolos para dispositivos inalámbricos, usuarios en la red ó ambos. Sirve tanto para el puerto de *Ethernet* como para el de Radio.

- *Ethertype Filters* — Filtrado de protocolos tipo *Ethernet*
- *IP Protocol Filters* — Filtrado de protocolos IP
- *IP Port Filters* — Filtrado por puertos IP
- *Policy Grups* — Filtrado por grupos de políticas
- *DSCP-to-CoS Conversion*: Conversión del punto de valor diferenciado de código de servicio (DSCP) a Valor de Clase de Servicio (CoS).
- *Quality of Service* — Calidad de Servicio.

## D) PORT ASSIGNMENTS — ASIGNACIÓN DE PUERTOS

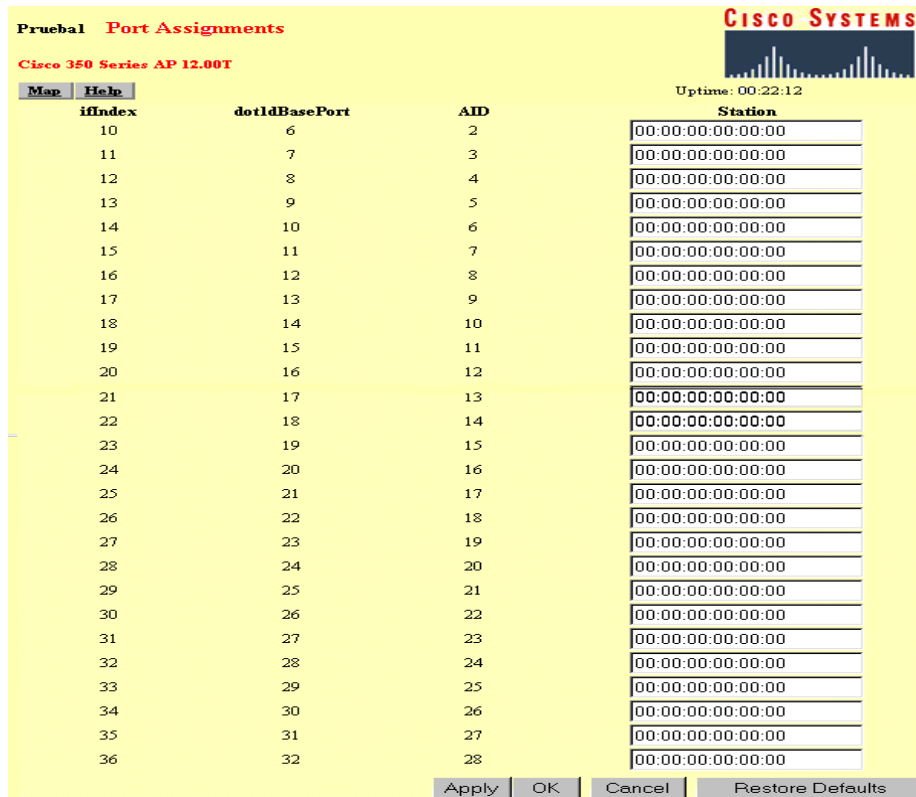


Figura 8.19 Página principal de *Port Assignments* en el apartado de *Associations*.

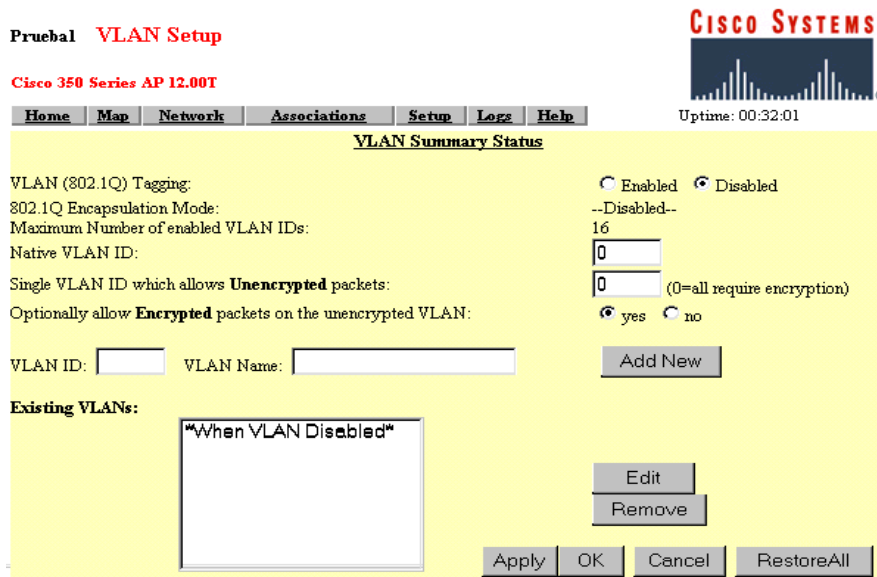
Este menú permite asignar un puerto de red específico al AP. Cuando se asignan puertos específicos, la topología de la red se mantiene constante aún cuando es reiniciado.

En este menú se despliega la siguiente información:

- *ifIndex* : Lista de puertos asignados en el estándar de índice de interfaz MIB-II (RFC 1213-MIB.my).
- *dot1dBasePort* : Lista de puertos designados en el índice de la interfaz en el *Bridge* MIB (RFC 1493; BRIDGE-MIB.my).

- *AID* : Lista de puertos de los controladores del identificador de asociación de radio 802.11.
- *Station* : Ingrese la dirección MAC del dispositivo al cual se desea asignar el puerto, en el campo de entrada de la estación del puerto. Cuando se hace *click* en **Apply** o **OK**, el puerto es reservado para esa dirección MAC.

### E) VLAN — REDES VIRTUALES



**Figura 8.20** Página principal de *VLAN Setup* en apartado de *Associations*.

Este menú permite realizar la configuración de redes virtuales (VLAN).

Se presentan los siguientes parámetros:

- *VLAN Summary Status* — Estado resumido de VLAN: Presionando este enlace se lleva a la página donde se enlistan todas las VLAN existentes en el AP, así como su respectiva información de configuración.

- *VLAN (802.1Q) Tagging* — Etiquetamiento de las VLAN's según estándar 802.1Q: Determina si el protocolo de IEEE 802.1Q está siendo utilizado para etiquetar paquetes provenientes de las VLAN's. Este último es utilizado para conectar múltiples *Switches* y *Routers* así como también para definir topologías de VLAN's.
- *802.1Q Encapsulation Mode* — Modo de encapsulado 802.1Q: Indica si está en uso el etiquetado IEEE 802.1Q. Este campo es siempre utilizado deshabilitado (**disable**), sin embargo se encuentra habilitado (**enable**) cuando:
  - Está habilitado el etiquetado de VLAN (802.1Q)
  - Una VLAN es especificada como VLAN ID nativa.
- *Maximun Number of Enables VLAN IDs* — Número máximo de identificadores de VLAN habilitados: Es un parámetro de estado, el cual provee el número máximo de VLAN's que pueden residir en el AP.
- *Native VLAN ID* — Identificador de VLAN nativa: Especifica el número de AP nativos.
- *Single VLAN ID which allows unencrypted packets* — Único identificador de VLAN que permite paquetes descriptados: Identifica el número de VLAN en el cual los paquetes descriptados pueden pasar entre el AP y el *Switch*.
- *Optionally allow Encrypted packets on the unencrypted VLAN* — Permitir paquetes encriptados opcionalmente en la VLAN descriptada: Determina si el AP pasa paquetes encriptados en una VLAN descriptados. Este parámetro permite que el dispositivo que se asocia al AP permita tanto asociaciones *WEP* como no-*WEP*.

- *VLAN ID* — Identificador de la VLAN: Único número que identifica a la VLAN. Este debe ser el mismo que el configurado en el *Switch*.
- *VLAN Name* — Nombre de la VLAN: Único nombre configurado en la VLAN del AP. Este parámetro es único y no es utilizado por el AP o el *Switch*, como parámetro para determinar los datos del destino.
- *Existing VLAN's* — VLAN's existentes: Enlista las VLAN's configuradas satisfactorias en el AP. Cuando es configurada la VLAN, aparece en la lista por nombre y número de identificación. Puede ser editado o removido.

## F) ADVANCED — AVANZADAS

**Pruebal Association Table Advanced**

Cisco 350 Series AP 12.00T

Uptime: 00:41:54

Handle Alerts as Severity Level: External Information

Maximum number of bytes stored per Alert packet: 0

Maximum Number of Forwarding Table Entries: 8192

Rogue AP Alert Timeout (minutes): 30

Aironet Extended Statistics in MIB (awcTpFdbTable):  Enabled  Disabled

Block ALL Inter-Client Communications ("PSPF"):  Yes  No

**Default Activity Timeout (seconds) Per Device Class:**

Unknown Class	300
Multicast Addresses	28800
Infrastructure Hosts	1800
Client Stations	1800
Repeaters	28800
Access Points	28800
Across-Bridge Hosts	1800
Non-Root Bridges	28800
Root Bridges	28800

Apply OK Cancel Restore Defaults

Figura 8.21 Página principal de *Advanced* en apartado de *Associations*.



- *Handle Alerts as Severity Level* — Manipular Alertas como Nivel de Seguridad: Este parámetro determina el nivel de severidad al cual cada estación reportará un registro de evento. Se pueden escoger los siguientes cuatro niveles:
  - *Fatal Severity Level (System, Protocol, Port)* — Nivel de severidad Fatal: Indica un evento que evita la operación del puerto o el dispositivo. Para resumen de la operación, el puerto o el dispositivo deben estar en *Reset*. Estos eventos aparecen en color rojo en el *Event Log*.
  - *Alert Severity Level (System, Protocol, Port)* — Nivel de severidad de Alerta: Este mensaje indica que se necesita tomar acciones para corregir las condiciones. Estos eventos aparecen en color magenta en el *Event Log*.
  - *Warning Severity Level (System, Protocol, Port)* — Nivel de severidad de Advertencia: Indica que un error o fallo puede haber ocurrido. Estos eventos aparecen en color azul en el *Event Log*.
  - *Information Severity Level (System, Protocol, Port)* — Nivel de severidad de Información: Notifican algunos de los eventos no fatales. Estos eventos aparecen en verde en el *Event Log*.
  
- *Maximun number of bytes stored per Alert packet* — Número máximo de *bytes* guardados por cada paquete de alerta: Este es utilizado solamente cuando el rastreo de paquetes está habilitado. Si se utiliza 0 (por defecto) el AP no guarda ningún *byte* por paquete de alerta por estación, y únicamente registra el evento.

- *Maximun Number of Forwarding Table Entries* — Máximo número de envío de entradas de la tabla: Determina el número máximo de dispositivos que pueden aparecer en la Tabla de Asociación.
- *Rogue AP Alert Timeout (minutes)* — Tiempo fuera de alertas del AP: Cuando el AP lo detecta, el mismo envía un mensaje de alerta las registra del sistema. Este parámetro especifica el aumento del tiempo en minutos que el AP transmite un mensaje de alerta. Cuando el tiempo es alcanzado, el AP detiene el envío de mensajes.
- *RFC 1493 802.1D Statistics in MIB (dot1dTpFdbTable)* — Estadísticas del RFC 1493: Utilice este parámetro para habilitar o deshabilitar el almacenamiento detallado de las estadísticas 1493 802.1D en la memoria del AP. Cuando se deshabilitan las estadísticas extendidas, se conserva la memoria y el AP puede incluir más dispositivos en la Tabla de Asociación. Por tal razón es recomendable tenerlo deshabilitado.
- *Aironet Extended Statistics in MIB (awcTpFdbTable)* — Estadísticas extendidas del Aironet: Utilícese para habilitar o deshabilitar el almacenamiento de estadísticas para Aironet extendidas en la memoria del AP. Cuando se deshabilita se puede conservar la memoria y el AP puede incluir más dispositivos en la tabla de Asociación.
- *Block ALL Inter-Client Communications (PSPF)* — Bloquear todas las comunicaciones entre Clientes: El PSPF (*Publicly Secure Packet Forwarding*) evita que Clientes asociados a un AP compartan archivos con otros Clientes en la red inalámbrica. Esto provee acceso a Internet a los Clientes sin proveer otras capacidades a la LAN. Con el PSPF habilitado, el Cliente no se comunica con otro Cliente mediante la red inalámbrica. Esta característica es útil para redes públicas como aquellas instaladas en aeropuertos o campus colegiales.

- *Default Activity Timeout (seconds) Per Device Class* — Tiempo de actividad por defecto por clase de dispositivo: Este parámetro determina la cantidad de segundos que el AP le sigue la huella al dispositivo inactivo dependiendo de su clase. Un valor de 0, dice que el AP le sigue la huella a un dispositivo infinitamente, sin importar cuando tiempo lleva inactivo. Un valor de 300 es igual a 5 minutos.

### G) SERVICE SETS — FIJACIÓN DE SERVICIOS

Esta página permite crear, editar o remover la configuración del SSID.



Figura 8.22 Página principal de *Service Sets* en apartado de *Associations*.

- *Device* — Dispositivo: Este es un campo de información que muestra el dispositivo para el cual ha sido configurado en la página de “Aplicar”.
- *SSID for use by Infrastructure Stations (such as Repeaters)* — SSID para el uso de estaciones de infraestructura: Esta configuración identifica el SSID para ser utilizado por los repetidores para asociarse con el AP. El SSID debe ser mapeado para la VLAN ID nativa con el propósito de facilitar las comunicaciones entre los dispositivos de infraestructuras y los AP en modo *non-root*.

- *Disallow Infrastructure Stations on any other SSID* — No permitir estaciones de infraestructura en otros SSID: Evita que repetidores o *Bridges* se asocien a otro SSID que no sea el de Infraestructura. El parámetro por defecto es **NO**, por lo que para invocar esta herramienta se debe poner en **YES**.
- *Service Set ID (SSID)* — Fijación de Servicios de Identificación: Un SSID es un identificador único que el Cliente utiliza para asociarse con el AP o la VLAN a la que da soporte el AP. Se puede configurar hasta 16 SSID en cada AP, y éste puede estar compuesto de caracteres alfanuméricos de 2 hasta 32 caracteres de longitud.
- *Existing SSID's* — SSID's Existentes: Este campo contiene la lista de SSID's que han sido creados en el AP. El número entre paréntesis a la izquierda de cada SSID indica la VLAN a la cual ese SSID pertenece.

## Event Log

### A) *DISPLAY DEFAULTS* — DESPLIEGUE DE PARÁMETROS POR DEFECTO

**Prueba1 Event Display Setup**

Cisco 350 Series AP 12.00T

Map Help

CISCO SYSTEMS  
Uptime: 00:06:11

How should time generally be displayed? Wall-Clock Time

How should Event Elapsed (non-wall-clock) Time be displayed? Since Boot

Severity Level at which to display events immediately on the console: External Information

Severity Level at which to display events on the console log: External Information

Severity Level at which to display events on the GUI log: External Information

Apply OK Cancel Restore Defaults

**Figura 8.23** Página principal de *Display Defaults* en apartado de *Event Logs*.

- *How should time generally be displayed?* — Cómo debería ser desplegado el tiempo: Este menú permite determinar si el evento en el *Event Log*, son desplegados como actualización de tiempo del sistema (*system uptime*) o como reloj de pared (*wall-clock time*). Si se necesita seleccionar el *system uptime*, los eventos son desplegados tanto desde el *reboot* o desde la última vez que fue desplegado el *Event Log*. Si selecciona *wall-clock time*, los eventos son desplegados en el formato **YY:MM:DD HH:MM:SS**. Si el tiempo no ha sido configurado en el AP, el tiempo que aparece es el tiempo de actualización desde su selección.
- *How should Event Elapsed (non-wallclock) Time be displayed?* — Cómo debería ser desplegado el tiempo de eventos transcurridos: Escójase para desplegar un evento en el tiempo desde la última vez que el AP hizo *reboot* o desde la última vez que ocurrió un evento.
- *Severity Level at which to display events* — Nivel de severidad al cual desplegar los eventos: Cuando ocurre un evento, éste puede ser desplegado inmediatamente en la consola, en el *console log* o en el *GUI log*, para propósitos de lectura solamente. Este evento puede ser grabado.

**Tabla 8.1** *Event Display Severity Level* — Despliegue de nivel de severidad de eventos.

<b>Nivel de Severidad</b>	<b>Descripción</b>
<i>*Silent*</i>	El parámetro <i>*Silent*</i> Direcciona el AP para que no despliegue ningún evento inmediato en la consola, el <i>console log</i> o el <i>log GUI</i> .
<i>System Fatal</i> <i>Protocol Fatal</i> <i>Port Fatal</i>	El parámetro fatal indica un evento que previene la operación del puerto o dispositivo. Para la operación, el puerto o dispositivo usualmente debe ser en <i>Reset</i> . <i>System</i> — Se refiere al AP como un todo. <i>Protocol</i> — Se refiere a una comunicación específica del protocolo en uso.  <i>Port</i> — Referente al puerto <i>Ethernet</i> o interfaz de radio del AP.
<i>System alert</i> <i>Protocol alert</i> <i>Port alert</i> <i>External alert</i>	El parámetro de alerta indica los eventos a los cuales el administrador especifica las peticiones para ser informado. <i>System</i> — Se refiere al AP como un todo. <i>Protocol</i> — Se refiere a una comunicación específica del protocolo en uso.  <i>Port</i> — Referente al puerto <i>Ethernet</i> o interfaz de radio del AP. <i>External</i> — Referido al dispositivo en la red que no es el AP.
<i>System warning</i> <i>Protocol warning</i> <i>Port warning</i> <i>External warning</i>	El parámetro de <i>Warning</i> indica que ha ocurrido un fallo. <i>System</i> — Se refiere al AP como un todo. <i>Protocol</i> — Se refiere a una comunicación específica del protocolo en uso.  <i>Port</i> — Referente al puerto <i>Ethernet</i> o interfaz de radio del AP. <i>External</i> — Referido al dispositivo en la red que no es el AP.
<i>System information</i> <i>Protocol information</i> <i>Port information</i> <i>External information</i>	El parámetro de configuración indica una normal que no es fatal, por ejemplo: el puerto ha sido apagado, la velocidad ha cambiado, etc. <i>System</i> — Se refiere al AP como un todo. <i>Protocol</i> — Se refiere a una comunicación específica del protocolo en uso.  <i>Port</i> — Referente al puerto <i>Ethernet</i> o interfaz de radio del AP. <i>External</i> — Referido al dispositivo en la red que no es el AP.

Éstas selecciones afectan el despliegue de eventos solamente. Son utilizados para filtrar información y no para removerla del *Event Log*. Para quitar la información, debe hacer *click* en **Purge Log**.

## **B) EVENT HANDLING — MANIPULADOR DE EVENTOS**

Esta página es utilizada para determinar como notificar eventos: *fatal*, *alert*, *warning* y *information*. Se puede escoger solo contar los eventos, desplegarlos en la consola pero no guardarlos después de desplegarse.

## Prueba1 Event Handling Setup

Cisco 350 Series AP 12.00T

[Map](#) [Help](#)



Disposition of Events (by Severity Level)		Total Events
System Fatal	Notify	0
Protocol Fatal	Notify	0
Network Port Fatal	Notify	0
System Alert	Notify	0
Protocol Alert	Notify	0
Network Port Alert	Notify	0
External Alert	Notify	0
System Warning	Record	0
Protocol Warning	Record	0
Network Port Warning	Record	0
External Warning	Record	0
System Information	DisplayConsole	0
Protocol Information	Record	8
Network Port Information	Count	91
External Information	DisplayConsole	0

Handle Alerts as Severity Level:

Maximum number of bytes stored per Alert packet:

Maximum memory reserved for Detailed Event Trace Buffer (bytes):

Download Detailed Event Trace Buffer: [Headers Only](#) [All Data](#)

Figura 8.24 Página de Event Handling Setup

- *Disposition of Events* — Disposición de los Eventos: Los parámetros de eventos controla la manera en que los eventos son manejados por el AP: contados, desplegados en el registro, grabados o anunciados en una notificación.
- *Count* — Contador: Lleva la cuenta de eventos totales ocurridos en esta categoría, pero no los graba.
- *Display Console* — Despliegue de la consola: Provee un despliegue sólo para lectura del evento pero no lo graba.



- *Record* — Grabar: Graba el evento y lo despliega.
- *Notify* — Notificar: Graba el evento, lo despliega y menciona a quién debe notificar para resolver el problema.
- *Handle Alerts A severity Level* — Maneja las alertas de un nivel de severidad: Este parámetro le indica un nivel de severidad para la alerta de la estación.
- *Maximum number of bytes stored per Alert packet* — Número máximo de *bytes* guardados por paquetes de alerta: Ingrese el número de *bytes* que el AP debe guardar para cada paquete. Si usted quiere ver el contenido entero de cada paquete, ingrese **1600**. Si solamente se desea ver el encabezado, ingrese **64**.
- *Maximum memory reserved for Detailed Event Trace Buffer (bytes)* — Memoria máxima reservada para el *buffer* de rastreo de eventos detallados en *bytes*: Ingrese el número de *bytes* reservados para el *Buffer* de rastreo detallado de eventos. Este último es una herramienta para rastrear el contenido de paquetes entre las estaciones especificadas en la red.  
Después de reservar el espacio en el *Buffer*, debe navegar hasta la página de *Station* del dispositivo y seleccionar *Alert* de la caja de verificación en las columnas de *To Station* (hacia la estación) y el *From Station* (desde la estación).
- *Download Detailed Event Trace Buffer* — Descargue detallado del *Buffer* de rastreo de eventos: Utilice este enlace para ver los encabezados o todos los datos en el *Buffer*. El número de *bytes* guardados por paquete es controlado en la Tabla de Asociación Avanzada de Configuración.
- *Clear Alert Statistics* — Limpiar Estadísticas de Alerta: Este botón, borra los mensajes de alerta.

- *Purge Trace Buffer* — Purgado del *Buffer* de rastreo: Este botón elimina los rastros de paquetes del *Buffer* de eventos.

### c) NOTIFICATIONS — NOTIFICACIONES

Utilice esta página para habilitar y configurar la notificación de eventos a destinos externos para el AP, tal y como el servidor SNMP o sistema *Syslog*.

**Nota:** Para que notificación de eventos sea enviada a un destino externo, los eventos deben ser configurados para notificar en la página *de Event Handling Setup*.

**Figura 8.25** Página de *Event Notification Setup*

- *Should Notify-Disposition Events generate SNMP Traps?* — Deberían notificarse la disposición de eventos *SNMP Traps*: Seleccionar **SI** para enviar notificaciones de eventos al servidor SNMP.

**Nota:** para que las notificaciones sean enviadas al servidor SNMP, el parámetro SNMP debe estar habilitado en la página *SNMP Setup*, y se debe ingresar *el SNMP trap* y el *SNMP trap community*.

- *SNMP-Trap Destination* — Destino del *Trap* SNMP: Ingrese la dirección IP o el nombre del *host* del servidor que se encuentra corriendo el *software* de *SNMP Management*.
- *SNMP-Trap Community* — Comunidad del *Trap* SNMP: Escriba el nombre de la comunidad SNMP (*SNMP community name*).
- *Should Notify-Disposition Events generate Syslog Messages?* — ¿Debería notificar la disposición de eventos generados por mensajes de *Syslog*?: Seleccionar **SI** para enviar notificación de eventos al servidor de *Syslog*.
- *Should Syslog Messages use the Cisco EMBLEM format* — Deberían usar los mensajes *Syslog* el formato *EMBLEM* de Cisco: Cuando este parámetro está habilitado, el AP genera *EMBLEM* estándares.
- *Syslog Destination Address* — Dirección de destino del *Syslog*: Escriba la dirección IP o el nombre del *host* del servidor corriendo *Syslog*.
- *Network Default Syslog Destination* — Red de destino del *Syslog* por defecto: Provee la dirección de destino de los servidores DHCP o BOOTP. Esta dirección es utilizada por defecto si el campo de *Syslog Destination Address* está vacío.
- *Syslog Facility Number* — Número de *Syslog*: Número para notificaciones para el *Syslog*. El parámetro por defecto es **16**, el cual corresponde al código local 0.

- *IEEE SNMP Traps Should Generate the Following Notifications* — Los paquetes *Trap SNMP* deben generar las siguientes notificaciones: Se puede designar como se manejan los *Traps SNMP* de los siguientes eventos de los Clientes:
  - *Client Authentication Failure* — Fallo de autenticación del Cliente.
  - *Client Deauthentication* — Incorrecta validación del Cliente.
  - *Client Disassociation* — Desasociación del Cliente.

Usted puede colocar las siguientes opciones para cada evento:

- No Trap nor Event Log*: El evento no registrado.
- Event Log Only*: El evento es generado y enviado al registro de eventos.
- IEEE Trap Only*: El evento es enviado a la comunidad SNMP.
- Both IEEE Trap and Event Log*: El evento es enviado al registro de eventos.

## Services

### A) CONSOLE/TELNET

**Prueba1 Console/Telnet Setup**

Cisco 350 Series AP 12.00T

Uptime: 00:24:05

Map Help

Baud Rate: 9600

Parity: None

Data Bits: 8

Stop Bits: 1

Flow Control: SW Xon/Xoff

Terminal Type: teletype

Columns (64-132): 80

Lines (16-50): 24

Telnet:  Enabled  Disabled

Apply OK Cancel Restore Defaults

**Figura 8.26** Página Console/Telnet Setup

- *Baud rate* — Tasa de baudios: La velocidad de transmisión de datos es expresada en bits por segundo. Seleccionar desde 110 hasta 115 200, dependiendo de la capacidad de la computadora para abrir el sistema de administración del AP.
- *Parity* — Paridad: Un proceso de detección de errores basado en la adición de un bit de paridad para hacer un total de número de bits ODD ó EVEN. El parámetro por defecto es **NONE**, sin utilizar bit de paridad.
- *Data Bits* — Bits de datos: El parámetro por defecto es 8.
- *Stop Bits* — Bits de parada: El parámetro por defecto es 1.

- *Flow Control* — Control de flujo: Define la forma en la cual la información es enviada entre partes del equipo para prevenir la pérdida de datos cuando llega mucha información al mismo tiempo al dispositivo. El parámetro por defecto es **Xon/Xoff**.
- *Terminal Type* — Tipo de terminal: El parámetro predefinido es **ANSI**, el cual ofrece características gráficas como botones de video inversos y enlaces subrayados. No todos los emuladores soportan ANSI, por lo que el parámetro por defecto es **Teletype**.
- *Columns* — Columnas: Define el ancho del despliegue de la terminal del emulador dentro del rango de caracteres desde 64 hasta 132 caracteres. Se debe ajustar el valor para obtener el óptimo despliegue del emulador de la terminal.
- *Lines* — Líneas: Define la altura del despliegue desde la terminal emuladora dentro del rango de 16 hasta 50 caracteres. Ajustando el valor se puede obtener el óptimo despliegue para el emulador.
- *Enable Telnet* — Habilitar *Telnet*: El parámetro por defecto es **SI**. Debe seleccionar **NO** para prevenir acceso por *Telnet* al sistema de administración.

## B) TIME SERVER —SERVIDOR DE RELOJ

**Prueba1 Time Server Setup**

Cisco 350 Series AP 12.00T

Uptime: 00:26:26

Simple Network Time Protocol (SNTP):  Enabled  Disabled

Default Time Server:

Current Time Server:

GMT Offset (hr): (GMT - 05:00) Eastern Time (US & Canada)

Use Daylight Savings Time:  yes  no

Manually set date (YYYY/MM/DD):

Manually set time (HH:MM:SS):

Apply OK Cancel Restore Defaults

Figura 8.27 Página de *Time Server Setup*

El AP permite tres métodos de reporte de tiempo. Un correcto reporte del tiempo puede ayudar en la resolución de problemas.

Se mencionan los siguientes métodos:

- a) No colocar el tiempo en absoluto: El sistema iniciará a rastrear el tiempo basado en la duración desde el encendido. Este es utilizado solamente en instalaciones simples.
- b) Colocar el tiempo manualmente: Este método funciona bien pero, no garantiza mantener el tiempo si se va el fluido eléctrico. Si esto último pasa, el AP volverá a rastrear el tiempo basado en la duración desde el encendido (método anterior).
- c) Configurar el tiempo via *Simple Network Time Protocol* (SNTP): Es el mejor para grandes empresas. Este será configurado en el inicio de encendido del AP, y podrá mantener el mismo tiempo que el resto de dispositivos conectados a la red. El tiempo SNTP puede ser proveído por la internet, un servidor local o un receptor GPS.

### c) CISCO SERVICES — SERVICIOS DE CISCO

Esta página es quien describe cómo realizar actualizaciones de la versión del Sistema Operativo en el AP, cómo distribuirlo a los otros AP, cómo distribuir la configuración a otros AP's y cómo descargar, cargar y borrar la configuración del AP.

En un AP pueden ser actualizados los siguientes componentes del Sistema Operativo: Administración del Asistema Operativo (*Management System Firmware*), páginas Web del Sistema Operativo (*Web Pages Firmware*) y el Sistema Operativo del puerto de Radio (*Radio Firmware*).

Estos a su vez, pueden ser actualizados uno por uno o bien, todos los AP's a la vez.

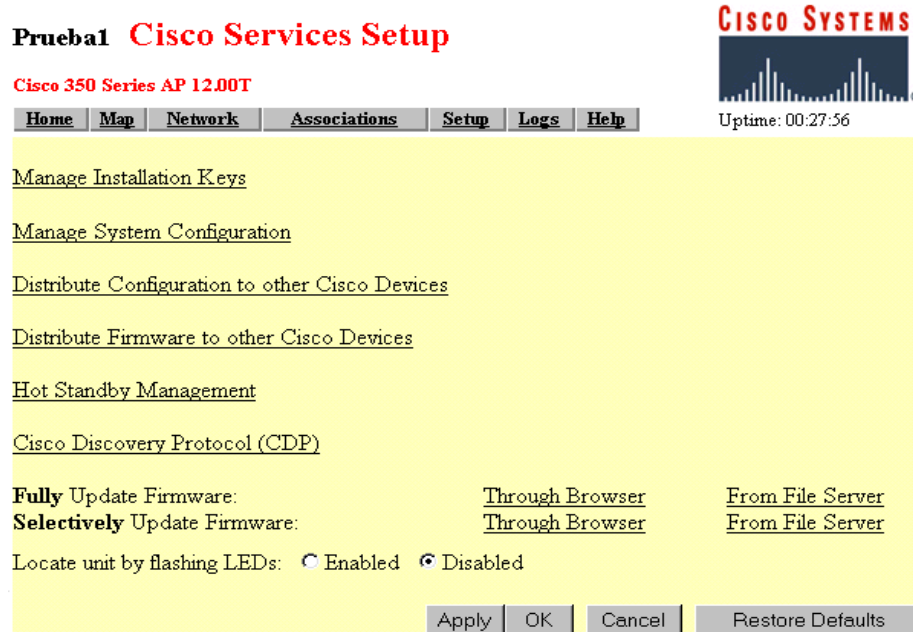


Figura 8.28 Página de *Cisco Services Setup*

c.1) *Manage Installation Keys* — Llaves Administrativas de Instalación: Este parámetro se utiliza para leer las especificaciones acerca de la licencia del *software* así como para instalar una nueva licencia.



## Prueba1 **Manage Installation Keys**

Cisco 350 Series AP 12.00T

[Map](#) [Help](#)



**Current License:**

MAC Address:	00:40:96:54:f9:0a
Serial Number:	XXXXXXXXXXXX
Device Type:	350 Series AP
Number of Associations:	2007
Features Enabled:	Long WEP, Antenna Diversity

**Install a new License using one of the following methods:**

Type in new License:

Select a new License File:

**Figura 8.29** Página de *Manage Installation Keys*

- *Current License* — Licencia actual: Esta sección es un resumen de la información acerca de la licencia de *software* instalada en el dispositivo.
  - *MAC Address* — Dirección MAC: Identificador único asignado por el fabricante.
  - *Serial Number* — Número de serie: Número de serie del producto.
  - *Device Type* — Tipo de dispositivo: Nombre completo del producto.
  - *Number of Associations* — Número de asociaciones: Máximo número de estaciones que pueden asociarse a este dispositivo.
  - *Features Enabled* — Características habilitadas: Aquí se enlistan las características del *software* que fueron habilitadas en su dispositivo. Aunque existen muchas opciones, las 2 más comunes son:

-*Antenna Diversity* — Diversidad de antena: Dos antenas para mejorar la recepción y transmisión de datos.

-*Long WEP* — *WEP* Largo: Sistema de seguridad por encriptación.

- *Install a New License Using One of the following methods* — Instalar una nueva licencia utilizando uno de los siguientes métodos: Esta sección selecciona uno de los dos métodos para actualizar la licencia del *software* de AP.

- *Type in New License* — Escribir una nueva licencia: Ingrese manualmente la llave alfanumérica completa de la licencia.

- *Select a New License File* — Seleccionar un nuevo archivo de licencias: Este método permite navegar en el disco duro o en la unidad de red para buscar el archivo que contiene la llave de licencia.

*c.2) Manage System Configuration* — Administrar Sistema de Configuración: Utilice este enlace para reiniciar el dispositivo, bajar el archivo de configuración o borrar las configuraciones programadas desde la fábrica.

## Prueba1 System Configuration Setup

Cisco 350 Series AP 12.00T



Home Map Network Associations Setup Logs Help Uptime: 00:46:18

"WARM" RESTART SYSTEM NOW "COLD" RESTART SYSTEM NOW

[Download Non-Default System Configuration Except IP Identity](#)

Reset System Factory Defaults Except IP Identity

[Download Non-Default System Configuration](#) [Download All System Configuration](#)

Reset All System Factory Defaults

Additional System Configuration File:  Examinar...

Read Config File from Server Browser Update Now Done

Figura 8.30 Página de *Manage System Configuration*

- *Download System Configuration Except IP Identity* — Descargar la configuración del sistema excepto la identidad IP: Si su navegador es el *Internet Explorer*, haga *click* en este botón para guardar el archivo de inicio (.ini) que contiene el archivo de configuración, excepto la dirección IP del dispositivo. Si su navegador es el *Netscape*, haga *click* en el botón de la derecha y seleccionar *Save Link as* en el menú.
- *Download Non-Default System Configuration* — Descargar la configuración del sistema que no esté por defecto: Utilice este enlace para descargar configuración del sistema que no esté por defecto.
- *Download All System Configuration* — Descargar toda la configuración del sistema: Si su navegador es el *Netscape* utilice el botón derecho del ratón para activar este botón y seleccionar *Save link as* en el menú. La configuración actual con la dirección IP del dispositivo es guardada. Si se realiza *click* en el enlace con el botón izquierdo del ratón, el *Netscape* desplegará el archivo de texto pero no abrirá la ventana para guardar.

- *Additional System Configuration File* — Archivo de configuración adicional del sistema: Escriba la ruta y el nombre del archivo de configuración que desea cargar al dispositivo. Si usted no está seguro de la ruta exacta debe navegar hasta encontrarla. Cuando la ventana de *File Upload* aparece, vaya al directorio que contiene el archivo de configuración y para luego seleccionar el archivo. Cuando el nombre del archivo aparece en este campo, se debe actualizar el navegador.
  
- Botones de Acción:
  - *“Warm” Restart System Now* — Reinicio del sistema en caliente: Un reinicio en caliente inicia el proceso de *reboot* del dispositivo.
  
  - *“Cold” Restart System Now* — Reinicio del sistema en Frio: Un reinicio en frío es equivalente a remover y volver a aplicarle nuevamente la alimentación de potencia para el dispositivo.
  
  - *Reset System Factory Defaults Except IP Identity* — Limpia los parámetros por defecto de fábrica excepto la Identidad IP: Se borran todas las configuraciones excepto:
    - La dirección IP del dispositivo, la máscara de red, la compuerta por defecto y el protocolo de *reboot*.
    - Los usuarios de la lista de Administración de Usuarios.
    - El nombre de la Comunidad Administradora de SNMP.
  
  - *Reset All System Factory Defaults* — Limpia todos los parámetros a los configurados por defecto desde la fábrica: Esto incluye la identidad IP, exceptuando:
    - Los usuarios de la lista de Administración de Usuarios.
    - El nombre de la Comunidad Administradora de SNMP.

- *Read Config File From Server* — Leer archivo de configuración desde el servidor: Permite enviar la configuración desde el servidor hasta el dispositivo.
- *Browser Update Now* — Actualizar navegación: Envía el archivo de configuración que usted nombró en el campo de *Additional System Configuration File* hacia el dispositivo.
- *Done* — Listo: Este botón lo envía de vuelta a la página de *Cisco Services Setup*.

*c.3) Distribute Configuration to other Cisco Devices* — Distribuir la configuración a otros dispositivos Cisco: Utilícese para enviar la configuración de un dispositivo a otros dentro de la misma red. De esta manera, se envía la configuración completa del sistema excepto la información de identidad IP y la lista de usuarios. Esto se aplica para los dispositivos que:

- Se encuentran corriendo una versión igual o superior a 10.05
- Puedan detectar el *multicast* IP utilizado por el dispositivo de distribución (los dispositivos como los *routers* pueden bloquear los paquetes de *multicast*).
- Tengan los servidores de *Web* habilitados para navegación externa.
- Tengan habilitado el Administrador de Usuarios (*User Manager*), conteniendo en sus Listas de usuarios uno con el mismo nombre, clave y capacidades como el que realiza la distribución (persona registrada en el dispositivo de distribución).

## Prueba1 Distribute Configuration

Cisco 350 Series AP 12.00T

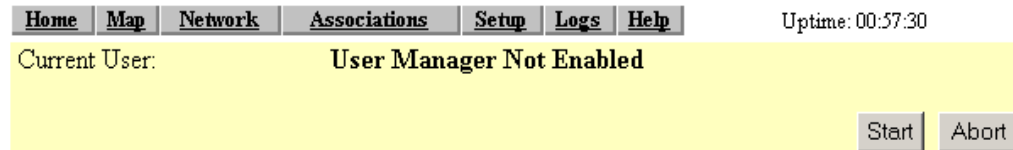


Figura 8.31 Página de *Distribute Configuration*

- *Current User* — Usuario actual: Este es el usuario que se ha registrado para distribuir la configuración. Si el Administrador de Usuarios está habilitado en los dispositivos de la red, la Lista de Usuarios de esos dispositivos debe contener un usuario con el mismo nombre, clave y capacidades como el que realiza la distribución.
- *Action Buttons* — Botones de acción:
  - *Start* — Inicio: La configuración, excepto la identidad IP y la lista de usuarios, es distribuida a los dispositivos de la red.
  - *Abort* — Abortar: Cancela la distribución.

c.4) *Distribute Firmware to other Cisco Devices* — Distribuir sistema operativo a otros dispositivos Cisco: Utilice este enlace para enviar una nueva versión de sistema operativo a otro dispositivo *Aironet* de la red, que presenten lo siguiente:

- Se encuentren corriendo una versión igual o superior a 10.05
- Puedan detectar el *multicast* IP utilizado por el dispositivo de distribución (los dispositivos como los *routers* pueden bloquear los paquetes de *multicast*).
- Tengan los servidores de *Web* habilitados para navegación externa.

- Tengan una configuración de la Compuerta por Defecto distinta a la 255.255.255.255.
- Tengan habilitado el Administrador de Usuarios (*User Manager*), conteniendo en sus Listas de Usuarios uno con el mismo nombre, clave y capacidades como el que realiza la distribución (persona registrada en el dispositivo de distribución).

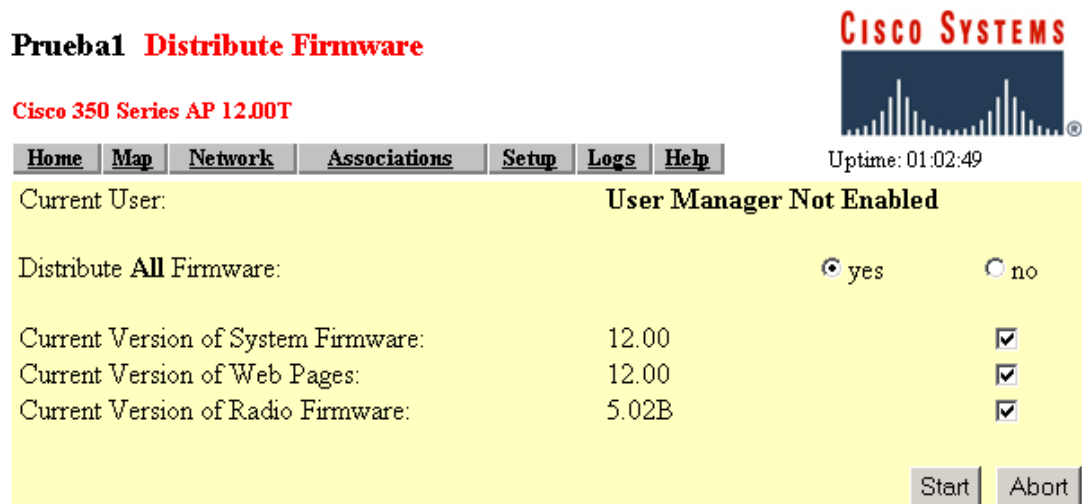


Figura 8.32 Página de *Distribute Firmware*

- *Current User* — Usuario actual: Este es el usuario que se ha registrado para distribuir la configuración. Si el Administrador de Usuarios está habilitado en los dispositivos de la red, la Lista de Usuarios esos dispositivos debe contener un usuario con el mismo nombre, clave y capacidades como el que realiza la distribución.
- *Distribute All Firmware* — Distribuir todo el Sistema Operativo: Distribuir todo el Sistema Operativo de una sola vez. Verificar que aparece **YES** y que todas las cajitas de selección para cada componente han sido escogidas. Para distribuir los componentes del sistema operativo individualmente, seleccionar **NO** y activar solamente los componentes del sistema operativo que desea distribuir.

- *Current Versión of System Firmware* — Versión actual del Sistema Operativo: Aquí aparece la versión del Sistema Operativo en el dispositivo de distribución.
- *Current Versión On Web pages* — Versión actual en páginas de Internet: Presenta la versión del sistema de administración de las páginas de Internet en el dispositivo de distribución.
- *Current Versión of Radio Firmware* — Versión actual de Sistema Operativo de interfaz de radio: Versión de Sistema Operativo que utiliza el puerto de radio.
- *Action Buttons* — Botones de acción:
  - *Start* — Inicio: La configuración, excepto la identidad IP y la lista de usuarios, es distribuida a los dispositivos de la red.
  - *Abort* — Abortar: Cancela la distribución.

#### c.5) *Hot Standby Management* — Administración del “*Hot Standby*”

Utilice este enlace para fijar el dispositivo en “*standby*”. Los Clientes asociados al *AP standby* pierden su conexión durante el proceso de configuración del “*Hot Standby*”. Para configuración preliminar, navegue hasta la página de *AP Radio Identification* en el AP configurado en modo “*standby*” y realice lo siguiente:

- En la página de *Summary Status*, haga *click* en *Setup*.
- En la página de *Setup*, realice *click* en *Identification*, en la fila de *AP Radio*.
- Seleccionar **NO** en la opción de *Adopt Primary Port Identity*. Entonces el AP reinicia. Luego el puerto de radio presenta su propia identidad (ahora las direcciones IP y MAC son distintas a las del puerto *Ethernet*).



Estas direcciones deben ser diferentes para poder navegar hasta el AP en “Standby” a través del puerto de radio.

- Haga *click* en *Apply* y el AP se reiniciará.
- Navegue hasta la página de *Hot Standby*. El modo de “*Hot Standby*” designa a un dispositivo como respaldo para otro AP. El dispositivo en *standby* es colocado cerca del AP que soporta y es configurado exactamente igual (exceptuando la dirección IP).

**Prueba1 Hot Standby**

Cisco 350 Series AP 12.00T

Uptime: 01:05:22

Service Set ID (SSID)	<input type="text" value="ab3"/>
MAC Address For the Monitored AP:	<input type="text" value="00:00:00:00:00:00"/>
Polling Frequency:	<input type="text" value="1"/> (Seconds)
Polling Tolerance Duration:	<input type="text" value="5"/> (Seconds)
Current State:	Hot Standby is not running.
Current Status:	Hot Standby unit is OK.

Figura 8.33 Página de *Hot Standby*

- *Service Set ID (SSID)* — Servicio de fijación de ID: El SSID es un identificador único que el dispositivo utiliza para asociarse con el AP o la VLAN. El SSID ayuda a distinguir entre múltiples dispositivos inalámbricos y VLAN's en la misma vecindad.
- *MAC Address for the monitored AP* — Dirección MAC para el AP monitoreado: Ingrese la dirección MAC del dispositivo monitoreado.
- *Polling Frequency* — Encuesta de frecuencia: Ingrese el número de segundos entre cada pregunta que el dispositivo *standby* envía al AP monitoreado.

- *Polling Tolerance Duration* — Duración de la tolerancia de la encuesta: Ingrese el número de segundos que el dispositivo *standby* debería esperar para obtener una respuesta del AP monitoreado, antes que este asuma que el dispositivo monitoreado no está funcionando.
  
- *Current State and Status* — Estado actual: Estos parámetros son informales y determinan si el “*Hot Standby*” está funcionando, así como su estado.
  
- *Action Buttons* — Botones de acción:
  - Start Hot Standby Mode* — Iniciar Modo “*Hot Standby*”: El dispositivo realiza un *reboot* y se convierte en Cliente asociado para el AP Asociado.
  - Stop Hot Standby Mode* — Detener Modo “*Hot Standby*”: El modo “*Hot Standby*” es detenido.
  - Apply* — Aplicar: Después de ingresar nuevos valores o parámetros, haga *click* en *Apply* para activar las nuevas entradas.
  - OK*: Aplica la nueva configuración.
  - Cancel* — Cancelar: Cancela todas las entradas o configuración de puertos, retornando los parámetros a la configuración guardada anteriormente.
  - Restore* — Restaurar: Cambia todas las configuraciones realizadas a la configuración por defecto de la fábrica.

c.6) *Cisco Discovery Protocol (CDP)* — Protocolo de descubrimiento Cisco:

Utilice este enlace para ajustar los parámetros CDP del dispositivo. El CDP es un protocolo de descubrimiento de dispositivos que corren en todos los equipos Cisco.

Cada dispositivo envía mensajes de identificación a una dirección *multicast*, y cada dispositivo monitorea los mensajes enviados por el *CiscoWorks2000*.

Utilice la página *CDP Setup* para ajustar los parámetros del dispositivo CDP. CDP está habilitado por defecto.

**Prueba1 CDP Setup**

Cisco 350 Series AP 12.00T

Map Help

Cisco Systems  
Uptime: 01:07:07

Cisco Discovery Protocol (CDP):  Enabled  Disabled

Packet hold time:  Seconds

Packets sent every:  Seconds

Individual Interface Enable:

01: Ethernet

Apply OK Cancel Restore Defaults

Figura 8.34 Página de *CDP Setup*

- *Cisco Discovery Protocol (CDP)* — Protocolo de descubrimiento Cisco: Seleccionar *Disable* para deshabilitar CDP en el dispositivo. CDP está habilitado por defecto.
- *Packet Hold Time* — Tiempo de espera del paquete: El número de segundos que otros dispositivos deberían considerar como válida la información del CDP. Si otros dispositivos no reciben otro paquete desde el dispositivo antes que este tiempo termine, ellos deberían asumir que el dispositivo ya no existe. El valor por defecto es 180. Este valor debería ser siempre más grande que el valor de los paquetes enviados a cada campo.
- *Packets Sent Every* — Paquetes enviados cada: Cantidad en segundos entre cada paquete CDP que el dispositivo envía. El valor por defecto es 60. Este valor debería ser siempre menor que el tiempo de espera del paquete.
- *Individual Port Enable* — Habilitación del puerto individual:

- *Ethernet*: Cuando se selecciona, el dispositivo envía paquetes CDP a través del puerto *Ethernet* y lo monitorea para paquetes CDP desde otros dispositivos.
- *AP Radio Internal* — AP Radio Interno: Cuando se selecciona, el dispositivo envía paquetes CDP a través de su puerto interno de radio y monitorea para paquetes CDP desde otros dispositivos.
- *AP Radio Module* — Módulo de AP Radio: Cuando se selecciona, el dispositivo envía paquetes CDP a través de su puerto de módulo de radio y monitorea para paquetes CDP desde otros dispositivos.

**Nota:** Un archivo MIB está disponible para el uso de CDP. Este puede ser descargado desde [www.cisco.com](http://www.cisco.com), el archivo **MIB-AP450Vxxxxxx.exe**.

- *Action Buttons* — Botones de acción:
  - *Apply* — Aplicar: Activa el nuevo parámetro configurado.
  - *OK*: Aplica una nueva configuración.
  - *Cancel* — Cancela: Cancela todos los cambios de los parámetros y retorna a la configuración previamente guardada.
  - *Restore Defaults* — Restaura valores por defecto: Cambia las configuraciones a los parámetros por defecto.
- *Fully Update Firmware* — Actualización total de Sistema Operativo:  
Permite realizar actualizaciones del sistema operativo de una sola vez.

*Through Browser* — A través del navegador: Con este método se puede navegar en el disco duro ó en las unidades de red mapeadas para encontrar el sistema operativo deseado y los archivos de página *Web*, y actualizar todos los componentes del sistema operativo al mismo tiempo.

-*Current Firmware Versión* — Versión actual del Sistema Operativo: Existen 3 niveles para la versión:

-*System Firmware* — Sistema Operativo del sistema.

-*Web pages* — Páginas *Web*.

-*Radio Firmware* — Sistema Operativo de interfaz de radiofrecuencia.

-*Retrieve All Firmware Files* — Recuperar todos los archivos del *firmware*: Realice un *click* para guardar el actual Sistema operativo y las páginas *Web* desde una unidad local o disco.

-*New File for All Firmware* — Nuevo archivo para todo el Sistema Operativo: Utilice esta sección para navegar en su disco duro o mapear las unidades de red para encontrar un nuevo archivo de sistema operativo.

-*Action Buttons* — Botones de acción:

*Browse Update Now* — Actualizar navegador: Después de ingresar el nombre del archivo para el nuevo sistema operativo, realice *click* aquí para cargar e instalar el nuevo sistema operativo. Cuando la actualización está completa, el dispositivo automáticamente reinicia.

*Done* — Listo: Actualiza y guarda la configuración realizada.

*From File Server* — Desde servidor de archivos: Con este método se ingresa el archivo de información para actualizar todos los componentes del sistema operativo.

-*Current Firmware Versión* — Versión actual del Sistema Operativo: Existen 3 niveles para la versión:

-*System Firmware* — Sistema Operativo del sistema.

-*Web pages* — Páginas Web.

-*Radio Firmware* — Sistema Operativo para la radiofrecuencia.

-*New File for All Firmware* — Nuevo archivo para todo el Sistema Operativo: Utilice esta sección para navegar en su disco duro o mapear las unidades de red para encontrar un nuevo archivo de sistema operativo.

-*File Server Setup* — Configuración del Servidor de Archivos: Utilice este enlace para ir a la página de *FTP Setup*.

-*Action Buttons* — Botones de acción:

*Update from Server* — Actualizar desde Servidor: Después de ingresar el nombre del archivo para el nuevo sistema operativo, realice *click* aquí para cargar e instalar el nuevo sistema operativo. Cuando la actualización está completa, el dispositivo automáticamente reinicia.

*Save To Server* — Guardar en Servidor: Realice *click* aquí para guardar el Sistema operativo y las páginas *Web* en su servidor.

*Done* — Listo: Actualiza y guarda la configuración realizada.

*Cancel* — Cancelar: Cancela todas las configuraciones realizadas y la restaura a la configuración previamente guardada.

- *Selectively Update Firmware* — Actualización selectiva del Sistema Operativo:

Permite realizar actualizaciones del sistema operativo de manera selectiva de cada uno de sus cuatro componentes de sistemas operativos existentes (sistema de administración, página *Web* y ambos puertos de radio).

Through Browser — A través del navegador: Con este método se puede navegar en el disco duro ó en las unidades de red mapeadas para encontrar el sistema operativo deseado y los archivos de página *Web*, y actualizar todos los componentes del sistema operativo al mismo tiempo.

-*Current Firmware Versión* — Versión actual del Sistema Operativo: Existen 3 niveles para la versión:

-*System Firmware* — Sistema Operativo del sistema.

-*Web pages* — Páginas *Web*.

-*Radio Firmware* — Sistema Operativo para radiofrecuencia.

-*New File for All Firmware* — Nuevo archivo para todo el Sistema Operativo: Utilice esta sección para navegar en su disco duro o mapear las unidades de red para encontrar cada uno de los archivos que componen el sistema operativo.

-*Action Buttons* — Botones de acción:

*Browse Update Now* — Actualizar Navegador: Después de ingresar el nombre del archivo para el nuevo sistema operativo, realice *click* aquí para cargar e instalar el nuevo sistema operativo. Cuando la actualización está completa, el dispositivo automáticamente reinicia.

*Done* — Listo: Actualiza y guarda la configuración realizada.

From File Server — Desde Servidor de Archivos: Con este método se ingresa el archivo de información para actualizar los componentes del sistema operativo individualmente.

-*Current Firmware Versión* — Versión actual del Sistema Operativo: Existen 3 niveles para la versión:

-*System Firmware* — Sistema Operativo del sistema.

-*Web pages* — Páginas Web.

-*Radio Firmware* — Sistema Operativo para radiofrecuencia.

-*New Firmware Files* — Nuevos archivos para el Sistema Operativo: Utilice esta sección para navegar en su disco duro o mapear las unidades de red para encontrar los archivos deseados del sistema operativo.

-*File Server Setup* — Configuración del Servidor de Archivos: Utilice este enlace para ir a la página de *FTP Setup*.

-*Action Buttons* — Botones de Acción:

*Update from Server* — Actualizar desde Servidor: Después de ingresar el nombre del archivo para el nuevo sistema operativo, realice *click* aquí para cargar e instalar el nuevo sistema operativo. Cuando la actualización está completa, el dispositivo automáticamente reinicia.

*Save To Server* — Guardar en Servidor: Realice *click* aquí para guardar el Sistema operativo y las páginas *Web* en su servidor.

*Done* — Listo: Actualiza y guarda la configuración realizada.

*Cancel* — Cancelar: Cancela todas las configuraciones realizadas y la restaura a la configuración previamente guardada.

#### **D) *BOOT SERVER* — SERVIDOR DE ARRANQUE**

Esta página permite configurar el dispositivo para la asignación automática de direcciones IP por parte de los Servidores de *boot* o DHCP.



## Prueba1 Boot Server Setup

Cisco 350 Series AP 12.00T



Uptime: 00:34:08

**Map** **Help**

Configuration Server Protocol:

Use previous Configuration Server settings when no server responds?  yes  no

Read ".ini" file from file server?

Current Boot Server: 0.0.0.0

Specified ".ini" File Server: 0.0.0.0

BOOTP Server Timeout (sec):

DHCP Multiple-Offer Timeout (sec):

DHCP Requested Lease Duration (min):

DHCP Minimum Lease Duration (min):

DHCP Client Identifier Type:

DHCP Client Identifier Value:

DHCP Class Identifier:

Figura 8.35 Página de *Boot Server Setup*

- *Configuration Server Protocol* — Configuración del Protocolo del Servidor: Se debe seleccionar el método de asignación de dirección IP. Presenta las siguientes opciones:
  - *None* — Ninguna: La red no tiene sistema de asignación automática de IP.
  - *BOOTP* : La red utiliza el Protocolo *Boot*, en el cual la asignación de direcciones IP están basadas las direcciones MAC de los clientes.
  - *DHCP*: Con el Protocolo DHCP, las direcciones IP son prestadas por un periodo de tiempo. Este último puede ajustarse en esta misma página.

- *Use Previous Configuration Server Settings When No Server Responds* — Utilice la configuración anteriormente fijada en el servidor cuando no exista respuesta del servidor: Seleccionar **YES** para que el dispositivo guarde la más reciente respuesta del servidor de inicio. De esta manera el dispositivo utilizará la configuración más reciente si el servidor no está disponible.
  
- *Read.ini File from File Server* — Archivo Read.ini desde el Servidor de Archivos: Utilice esta configuración para que el dispositivo utilice la configuración del archivo .ini en el servidor de BOOTP o DHCP, o bien, en el servidor de archivos por defecto. Se tienen las siguientes opciones:
  - *Always* — Siempre: El dispositivo siempre carga la configuración desde el archivo .ini en el servidor.
  - *Never* — Nunca: El dispositivo nunca carga la configuración desde el archivo .ini en el servidor.
  - *If specified by Server* — Si es especificado desde el servidor: El dispositivo carga la configuración desde el archivo .ini en el servidor si la respuesta del servidor DHCP o BOOTP especifica que el archivo .ini está disponible. Ésta es la configuración por defecto.

El botón de *LoadNow* le dice al dispositivo que lea el archivo .ini inmediatamente.

El Servidor actual de inicio se encuentra especificado bajo este menú que responde a la petición de inicio. Si aparecen ceros significa que el dispositivo no está utilizando BOOTP/DHCP o que ningún servidor responde a la petición del BOOTP/DHCP.

- *Current Boot Server* — Servidor actual de Inicio: Este es el servidor que responde a la petición de inicio. Si aparecen solamente ceros, el dispositivo no está utilizando o no responden a peticiones de BOOTP/DHCP.

- *Specified ".ini" File Server* — Servidor de archivos **.ini** especificado: Enlista las direcciones IP de los servidores donde el archivo **.ini** está especificado. Si todos son ceros significa que no existe servidor de archivos que provea un archivo **.ini**.
- *BOOTP Server Timeout (sec)* — Tiempo fuera del Servidor de BOOTP (seg): Ingrese la cantidad de tiempo (en segundos) que el dispositivo espera recibir una respuesta desde un servidor de BOOTP.
- *DHCP Multiple-Offer Timeout (sec)* — Tiempo fuera de oferta múltiple DHCP (seg): Ingrese la cantidad de tiempo (en segundos) que el dispositivo espera recibir respuesta cuando existen múltiples servidores DHCP.
- *DHCP Request Lease Duration (min)* — Duración del préstamo de petición DHCP (min): Ingrese la cantidad de tiempo (en minutos) que el dispositivo acepta el préstamo de la dirección IP del servidor DHCP.
- *DHCP Minimum Lease Duration (min)* — Duración mínima de préstamo DHCP (min): Ingrese el mínimo aumento de tiempo (en minutos) que el dispositivo acepta un préstamo de dirección IP. El dispositivo ignora préstamos menores a este periodo.
- *DHCP Client Identifier Type* — Tipo de identificador de Cliente DHCP: El servidor DHCP puede configurarse para que envíe respuestas de acuerdo al identificador de clases especificado por el AP en el paquete de petición DHCP. Si la mayoría de los Clientes que utilizan el AP son del mismo tipo de dispositivo, se puede seleccionar el tipo de dispositivo para ser incluido en el paquete de petición de DHCP. Para esto existe la siguiente lista de opciones:

- *Ethernet(10Mb)*: Valor por defecto
  - *Experimental Ethernet*
  - *Amateur Radio AX.25*
  - *Proteon ProNET Token Ring*
  - *Chaos*
  - *IEEE 802 Networks*
  - *ARCNET*
  - *Hyperchannel*
  - *Lanstar*
  - *Autonet Short Address*
  - *LocalTalk*
  - *LocalNet*
  - *Other Non Hardware*: Seleccionar esta opción para incluir un único valor de valor en el campo de Identificador de Cliente DHCP.
- *DHCP Client Identifier Value* — Valor identificador de Cliente DHCP: Utilice este parámetro para incluir un identificador único en el paquete de petición DHCP. Este campo contiene la dirección MAC del AP por defecto. Si selecciona *Other-Non Hardware*, se puede ingresar hasta 255 caracteres alfanuméricos. Si usted cualquier otra opción, se puede ingresar hasta 12 caracteres hexagesimales.
  - *DHCP Class Identifier* — Identificador de clase DHCP: El servidor DHCP puede ser configurado para enviar respuestas de acuerdo al grupo al que el dispositivo pertenezca. Utilice este campo para ingresar el nombre del grupo. El servidor DHCP utiliza el nombre del grupo para determinar la respuesta para enviar al dispositivo. El identificador de clase del dispositivo DHCP es el del fabricante.

## E) FTP —PROTOCOLO DE TRANSMISIÓN DE ARCHIVOS

Antes de cargarse el archivo de configuración desde el servidor, se debe ingresar la configuración FTP para el servidor. Se utiliza esta página para asignar la configuración FTP para el dispositivo. Todos los archivos de transferencia no navegables son gobernados por los parámetros en esta página.

**Prueba1 FTP Setup**

Cisco 350 Series AP 12.00T

Map Help Uptime: 00:38:02

File Transfer Protocol: FTP

Default File Server:

FTP Directory:

FTP User Name: anonymous

FTP User Password: \*

Apply OK Cancel Restore Defaults

Figura 8.36 Página de *FTP Setup*

- *File Transfer Protocol* — Protocolo de transferencia de archivos: Utilice el menú para seleccionar FTP ó TFTP. El FTP es el protocolo estándar que soporta la transferencia de datos entre computadores locales y remotos. El TFTP es relativamente lento y bajo en seguridad, que requiere un nombre de usuario o palabra clave (*password*).
- *Default File Server* — Servidor de archivos por defecto: Ingrese la dirección IP del Servidor donde el dispositivo debe ir a buscar los archivos FTP.
- *FTP Directory* — Directorio FTP: Ingrese el directorio en el servidor donde los archivos FTP están localizados.

- *FTP User Name* — Nombre de usuario FTP: Ingrese el nombre del usuario asignado a su servidor FTP. Si selecciona TFTP, se puede dejar este campo en blanco.
- *FTP User Password* — Clave FTP: Ingrese la clave asociada al nombre de usuario. Si selecciona TFTP, se puede dejar este campo en blanco.

## F) SECURITY—SEGURIDAD

Esta página permite configurar y administrar las características de seguridad. Es utilizada solamente cuando las VLAN's está deshabilitadas. Para habilitar las características de seguridad, se debe ir a la página de *User Information* y debe crear un usuario con capacidades de Administrador, Identidad, Cargar Sistemas Operativos y de Escrituras.

**Prueba1 Security Setup**

Cisco 350 Series AP 12.00T

Home Map Network Associations Setup Logs Help

CISCO SYSTEMS  
Cisco's Home  
Uptime: 00:39:43

[Login](#)  
[User Manager](#)  
[Change Current User Password](#)  
[User Information](#)

[Authentication Server](#)

If VLANs are *not* enabled, set Radio Data Encryption through the link below. If VLANs are enabled, Radio Data Encryption is set independently for each enabled VLAN through [VLAN Setup](#).

[Radio Data Encryption \(WEP\)](#)

Done

Figura 8.37 Página de *Security Setup*

- *Login* — Registro: Despliega una ventana de registro, donde el usuario puede registrarse si no lo ha hecho todavía.
- *User Manager* — Administrador de Usuarios: Este enlace habilita o no las características de seguridad.
- *Change Current User Password* — Cambiar Clave Actual del Usuario: Despliega la ventana de *User Information*. Esta última también despliega las capacidades asignadas al usuario.
- *User Information* — Información del Usuario: Este enlace agrega, remueve y asigna capacidades a los usuarios del sistema. Para habilitar el nivel de seguridad de usuario del sistema, utilice este enlace para agregar un usuario con capacidades de Administrador, Identidad, Cargar Sistema Operativo y Escritura; luego vaya a la pantalla de *User Manager* para habilitar las características de seguridad.
- *Authentication Server* — Servidor de Autenticación: Utilice el enlace de *Authentication Server* si necesita ingresar los parámetros de configuración.
- *VLAN Setup* — Configuración de VLAN: Este enlace lo lleva a la página de *VLAN Setup* donde usted fija la encriptación de datos para VLAN's en el AP. Las VLAN's deben estar habilitadas para utilizar este enlace, de otra manera utilice la página de *Radio Data Encryption (WEP)*.
- *Radio Data Encryption (WEP)* — Encriptación de datos de radiofrecuencia: Este enlace lo lleva a la página de *Radio Data Encryption*, donde se puede colocar cuatro llaves de encriptación y habilitar el *WEP*.

## G) ROUTING — ENRUTAMIENTO

Utilice esta página para configurar la comunicación del AP con el sistema de enrutamiento de la red. Utilícese para especificar la compuerta por defecto y para crear una lista de parámetros de enrutamiento de la red.

**Prueba1 Routing Setup**

Cisco 350 Series AP 12.00T

Map Help

Uptime: 00:43:58

Default Gateway: 255.255.255.255

New Network Route:

Dest Network:

Gateway:

Subnet Mask:

Add

Installed Network Routes:

Remove

Apply OK Cancel Restore Defaults

Figura 8.38 Página de *Routing Setup*

- *Default Gateway* — Compuerta por defecto: Ingrese la dirección IP de la compuerta por defecto de la red en este campo. La entrada de 255.255.255.255 indica que no existe compuerta.
- *New Network Route* — Nueva ruta de la red: Se puede definir rutas de redes adicionales para el dispositivo. El campo de entrada incluye:
  - *Dest network* — Red de destino: Ingrese la dirección IP de la red de destino.
  - *Gateway* — Compuerta: Ingrese la dirección IP de la compuerta utilizada para alcanzar la red de destino.
  - *Subnet Mask* — Máscara de Subred: Ingrese la máscara de subred asociada con la red de destino.



- *Installed Network Routes* — Rutas de Red Instaladas: La lista de rutas instaladas proveen la dirección IP de la red de destino, la compuerta y la máscara de subred para cada ruta instalada.

## H) **WEB SERVER** — **SERVIDOR WEB**

Utilice esta página para habilitar la navegación en la administración del sistema. Especifique la localización de los archivos de ayuda e ingrese los parámetros lograr una administración del sistema personalizada.

**Prueba1 Web Server Setup**

Cisco 350 Series AP 12.00T

Uptime: 00:53:03

Map Help

Allow Non-Console Browsing?  yes  no

HTTP Port:

Default Help Root URL:

Extra Web Page File:  Load Now

Default Web Root URL:

Apply OK Cancel Restore Defaults

**Figura 8.39** Página de *Web Server Setup*

- *Allow Non-Console Browsing* — Permitir Navegación sin consola: Seleccionar **YES** para permitir la administración del sistema. Si selecciona **NO**, la administración del sistema es accesible solo a través de la consola y las interfaces de *Telnet*.
- *HTTP Port* — Puerto HTTP: Este parámetro determina el puerto a través del cual el dispositivo proveerá acceso al *Web*.

- *Default Help Root URL* — Localización por defecto de la ayuda: Permite especificarle al dispositivo donde buscar los archivos de ayuda. El botón de ayuda en cada página de administración del sistema abre una nueva ventana desplegando la ayuda para esta página. Los archivos de ayuda son proveídos en el CD en el directorio de **HELP**.

Se puede apuntar los archivos de ayuda a los siguientes lugares:

- *Internet*: Cisco mantiene actualizadas las ayudas para los dispositivos en su sitio *Web*. Para esto se requiere conexión cada vez que se necesita ayuda en línea.
  - *File Server* — Servidor de archivos: En redes multiusuarios, estos archivos pueden ser colocados en el servidor de archivos de la red. Para esto ingrese la dirección completa de los archivos en el campo de *Default Help Root URL*. Esta dirección debe ser similar a la siguiente:  
**[nombre del sistema][directorio]c:\wireless\help.**
  - *CD-ROM drive* — Unidad de CD: Para accesos ocasionales, se puede realizar consultas al CD directamente.
  - *Hard Drive* — Disco duro: Los archivos de ayuda pueden haber sido copiados al disco duro de la computadora que el usuario utiliza.
- *Extra Web Page File* — Archivo extra de página Web: Si se necesitan crear una alternativa para administrar el sistema, se puede crear páginas HTML y cargarlas en el dispositivo. Este campo es para especificar el nombre del archivo para la página HTML guardado en el Servidor de Archivos.

- *Default Web Root URL* — Localización por defecto de la dirección *Web*: Este parámetro apunta al sistema administrativo de la página HTML. Si se crea una página HTML, se debe cambiar este parámetro para apuntar páginas alternativas. El parámetro por defecto es **mfs0:/StdUI/**.

## 1) ACCOUNTING — CONTABILIDAD

Se puede habilitar la contabilidad en el AP para enviar información de contabilidad de la red sobre el dispositivo de Cliente inalámbrico para el servidor *RADIUS* de la red. El *Cisco Secure ACS* escribe el registro de contabilidad en el archivo de registro ó para una base de datos diaria.

Pruebal **Accounting Setup**

Cisco 350 Series AP 12.00T

Map Help Uptime: 00:54:46

Enable accounting:  Enabled  Disabled

Enable delaying to report STOP:  Enabled  Disabled

Minimum delay time to report STOP (sec):

Server Name/IP	Server Type	Port	Shared Secret	Retran Int (sec)	Max Retran	Enable Update	Update Delay (sec)
<input type="text"/>	RADIUS	1813	XXXXXXXXXXXXXXXXXXXX	5	3	<input checked="" type="checkbox"/>	600
Use accounting server for: <input type="checkbox"/> EAP authentication <input type="checkbox"/> non-EAP authentication							
<input type="text"/>	RADIUS	1813	XXXXXXXXXXXXXXXXXXXX	5	3	<input checked="" type="checkbox"/>	600
Use accounting server for: <input type="checkbox"/> EAP authentication <input type="checkbox"/> non-EAP authentication							
<input type="text"/>	RADIUS	1813	XXXXXXXXXXXXXXXXXXXX	5	3	<input checked="" type="checkbox"/>	600
Use accounting server for: <input type="checkbox"/> EAP authentication <input type="checkbox"/> non-EAP authentication							
<input type="text"/>	RADIUS	1813	XXXXXXXXXXXXXXXXXXXX	5	3	<input checked="" type="checkbox"/>	600
Use accounting server for: <input type="checkbox"/> EAP authentication <input type="checkbox"/> non-EAP authentication							

Apply OK Cancel Restore Defaults

Figura 8.40 Página de *Accounting Setup*

- *Enable Accounting* — Habilitar contabilidad: Habilítese para activar la contabilidad para la red inalámbrica.
- *Enable Delaying to Report Stop* — Habilitar retraso para reportar paradas: Seleccionar esta opción para atrasar el envío de un reporte de parada para el servidor cuando un Cliente se desasocia desde el AP. El retraso reduce la actividad de contabilidad para el cliente que se desasocia desde el AP y después rápido se desasocia.
- *Minimum Delay Time to Report Stop (sec)* — Retraso mínimo para reportar parada (seg): Ingrese el número de segundos que el AP espera antes de enviar un reporte de parada para el servidor cuando un Cliente se desasocia desde el AP. El retraso reduce la actividad de la contabilidad para el dispositivo que se desasocia del AP y luego se vuelve a asociar rápidamente.
- *Server Name/IP* — Servidor de nombres/IP: Ingrese el nombre o la dirección IP del servidor al cual el AP envía los datos contabilizados.
- *Server Type* — Tipo de servidor: Seleccione el tipo de servidor en el menú. El servidor de *RADIUS* es la única opción del menú. Tipos adicionales serán agregados en el futuro.
- *Port* — Puerto: Este parámetro especifica el puerto de comunicación utilizado por el AP y el servidor. El parámetro por defecto es 1813, el cual es el que se recomienda para AP's marca Cisco y el *Cisco Secure ACS*.
- *Shared Secret* — Secreto compartido: Ingrese el secreto compartido por el servidor de *RADIUS*. Este debe ser el mismo que el del AP.

- *Retran Int (sec)* — Interrupción para retransmisión (seg): Ingrese el tiempo en segundos que el AP debe esperar antes de darse por vencido de realizar el contacto con el servidor. Si el servidor no responde dentro de este tiempo, el AP intentará contactar el próximo servidor de contabilidad en la lista; si ha sido especificado. El AP utiliza los servidores de respaldo respetando el orden de la lista cuando el anterior servidor no responde en el tiempo especificado.
- *Max Retran* — Retransmisión máxima: Ingrese el número máximo de reintentos que el AP debe esperar para contactar al servidor antes de darse por vencido. Si el servidor no responde dentro de este tiempo, el AP intentará contactar el siguiente servidor especificado en la lista.
- *Enable Update* — Habilitar actualización: Permite actualizar mensajes para los Clientes inalámbricos. Con ésta opción activa el AP envía un mensaje de inicio de contabilidad cuando el dispositivo se asocia al AP, envía actualizaciones en intervalos regulares mientras que el Cliente inalámbrico es asociado al AP, y envía un mensaje de parada de contabilidad cuando el Cliente se desasocia del AP. Cuando este parámetro está deshabilitado el AP solamente envía el inicio y fin de los mensajes de contabilidad al servidor.
- *Update Delay* — Actualizar retraso: Ingrese el intervalo de actualización en segundos. Si se utiliza 360 (por defecto) el AP envía un mensaje de actualización de contabilidad para cada Cliente asociado cada 6 minutos.
- *Use Accounting Server For* — Utilice servidor de contabilidad para: Seleccionar los tipos de autenticación para los cuales se desea recolectar datos. Cuando se selecciona autenticación *EAP*, el AP envía datos de contabilidad al servidor cuando el Cliente que se autentifica utilizando Cisco Aironet *LEAP*, *EAP-TLS* ó *EAP-MD5*. Cuando se selecciona *non-EAP Authentication*, el AP envía datos al servidor cuando algún Cliente se autentifica con otro protocolo.

## J) NAME SERVER — SERVIDOR DE NOMBRES

Esta página es usada para configurar el AP para que funcione junto con el servidor DNS.

Pruebal **Name Server Setup**

Cisco 350 Series AP 12.00T

Map Help

CISCO SYSTEMS  
Uptime: 01:06:40

Domain Name System (DNS):  Enabled  Disabled

Default Domain:

Current Domain: corp.csu.co.cr

Domain Name Servers:

	Default	Current
1.	<input type="text" value="172.20.5.3"/>	172.20.20.1
2.	<input type="text" value="172.24.5.3"/>	172.20.20.2
3.	<input type="text"/>	

Domain Suffix:

Apply OK Cancel Restore Defaults

Figura 8.41 Página de Name Server Setup

- *Domain Name System* — Sistema de dominio de nombres: Si la red utiliza DNS, habilítese para que el AP utilice el sistema. Si no existe DNS, debe seleccionar *disabled*.
- *Default Domain* — Dominio por defecto: Ingrese el nombre de la red en este campo.

- *Current Domain* — Dominio actual: Escoja el dominio en el cual su AP está funcionando. El dominio actual debe ser distinto al del campo de entrada si, en la página de *Boot Server Setup*, se tiene DHCP o BOOTP configurado como el Protocolo del Servidor de Configuración. Se debe seleccionar **NO** para *fijar Use previous Configuration Server Setting when no server responds?*
- *Domain Name Servers* — Servidores de nombres de dominio: Ingrese la dirección IP para más de tres servidores DNS en la red. Las líneas actuales a la derecha del campo de entrada muestra los servidores que están actualmente en uso, los cuales deben ser especificados por el servidor DHCP o BOOTP.
- *Domain Name System Servers (Current)* — Servidores de nombre del dominio del sistema (Actuales): Éstos son los servidores que el dispositivo está utilizando en la actualidad.
- *Domain Suffix* — Sufijo del dominio: Ingrese una parte del nombre del dominio total que quisiera que no se desplegara.

#### **K) SNMP — PROTOCOLO DE MANEJO SIMPLE DE LA RED**

Esta página configura el dispositivo para que trabaje con el SNMP de la estación del Administrador del Sistema. Adicionalmente para habilitar el SNMP se debe crear un usuario que sea capaz de servir como comunidad SNMP. El nombre de la comunidad SNMP es el usuario. Cuando se ingrese el Nombre de la Comunidad Administrativa SNMP en la página de *Express Setup*, el usuario que se asocie con el nombre de la comunidad se crea automáticamente con las capacidades de escribir, SNMP y administración.

Prueba1 **SNMP Setup**

Cisco 350 Series AP 12.00T

Map Help Uptime: 01:09:22

CISCO SYSTEMS

Simple Network Management Protocol (SNMP):  Enabled  Disabled

System Description: Cisco 350 Series AP 12.00T

System Name:

System Location:

System Contact:

SNMP Trap Destination:

SNMP Trap Community:

[Browse Management Information Base \(MIB\)](#)

Apply OK Cancel Restore Defaults

Figura 8.42 Página de SNMP Setup

- *Simple Network Management Protocol (SNMP)*: Este parámetro debe estar habilitado para que el dispositivo utilice SNMP.
- *System Description* — Descripción del sistema: El tipo de dispositivo del sistema y la versión del Sistema Operativo se encuentran al final de la página.
- *System Name* — Nombre del sistema: Especifica el nombre del dispositivo.
- *System Location* — Ubicación del sistema: Ingrese la ubicación física del dispositivo, tal como el nombre del cuarto en el cual fue instalado.
- *System Contact* — Encargado del Sistema: Ingrese el nombre del encargado de la administración del sistema y que es responsable del dispositivo.




- *SNMP Trap Destination* — Destino del *Trap SNMP*: Es la dirección IP de la estación de la Administración SNMP. Si su red utiliza DNS, ingrese el nombre del invitado para resolver la dirección IP.
- *SNMP Trap Community* — Comunidad del *Trap SNMP*: Es requerido por la dirección del *Trap* de destino antes que los registros de *Traps* sean enviados por el dispositivo.
- *Browse Management Information Base (MIB)* — Navegar a la base de administración de la información: Este enlace lo lleva a la página de *Database Query*, la cual es usada para buscar y colocar los valores SNMP de muchos artículos de configuración.

## Network Ports

### 1) ETHERNET

Esta página presenta información importante para el puerto *Ethernet*.

Pruebal **Ethernet Port**

**CISCO SYSTEMS**  
  
Uptime: 00:07:57

[Home](#) [Map](#) [Network](#) [Associations](#) [Setup](#) [Logs](#) [Help](#)

Configuration		Set Properties	
Status of "fec0"	<b>No Link</b> (primary)	Maximum Rate (Mb/s)	0.0
IP Address	172.20.17.175	MAC Address	00409654f90a
Duplex	Full		
Statistics		Refresh	
Receive		Transmit	
	<i>Alert</i> <input type="checkbox"/>		<i>Alert</i> <input type="checkbox"/>
Unicast Packets	0	Unicast Packets	0
Multicast Packets	0	Multicast Packets	1
Total Bytes	0	Total Bytes	139
Total Errors	0	Total Errors	6
Discarded Packets	0	Discarded Packets	0
Forwardable Packets	84	by CoS (0-7): 0, 0, 0, 0, 0, 0, 0	
Filtered Packets	0	Forwarded Packets	8
Packet CRC Errors	0	Max Retry Packets	0
Carrier Sense Lost	0	Total Collisions	0
Late Collisions	0	Late Collisions	0
Overrun Packets	0	Underrun Packets	0
Packets Too Long	0		
Packets Too Short	0		
Packets Truncated	0		

Figura 8.43 Página de *Ethernet Port*

- *Configuration* — Configuración: Este apartado contiene un enlace al *Set Properties*, el cual lleva a la página de *Ethernet Hardware*.
- *Status of Fast Ethernet Controller (fec0)* — Estado del Controlador de *Ethernet* Rápido: Este campo despliega los 3 posibles estados del puerto.
  - Up* — Arriba: El puerto está operando apropiadamente.
  - Down* — Abajo: El puerto no está operando.
  - Error* : El puerto está en una condición de error.

- *Maximun Rate (Mb/s)* — Tasa máxima: Máxima tasa de transmisión de datos en Megabits por segundo.
- *IP Address* — Dirección IP: Dirección IP del Puerto.
- *MAC Address* — Dirección MAC: Identificador único asignado por el fabricante.
- *Duplex* — Dos vías: El puerto está en 1 o 2 vías.
- *Statistics: Receive* — Estadísticas: Recepción.  
Esta sección reporta el tráfico recibido a través del puerto *Ethernet*
  - *Unicast Packets* — Paquetes *unicast*: Número de paquetes recibidos en una comunicación punto a punto.
  - *Multicast Packets* — Paquetes *multicast*: Número de paquetes recibidos que son enviados como transmisión para fijar los nodos.
  - *Total Bytes* — *Bytes* totales: Número total de *bytes* recibidos.
  - *Total Errors* — Errores Totales: Número de paquetes a los que se les encontró algún error.
  - *Discarted Packets* — Paquetes descartados: Número de paquetes descartados debido a errores o congestión de la red.
  - *Forwardable Packets* — Paquetes enviados: Paquetes recibidos por el puerto que fueron aceptados o pasados a través de filtros.
  - *Filtered Packets* — Paquetes filtrados: Paquetes que fueron detenidos por los filtros configurados en el puerto.
  - *Packet CRC Errors* — Paquetes con errores CRC: Errores del tipo CRC que fueron detectados en los paquetes recibidos.

- *Carrier Sense Lost* — Pérdida de sensibilidad de portadora: Indica el número de desconexiones de la red *Ethernet*. Los eventos de pérdida de Sensibilidad de portadora son generalmente causados por la desconexión del cableado.
  - *Late Collisions* — Colisiones tardías: Error de paquetes que probablemente fueron causados por problemas de cableado. Este indicador también podría significar un fallo en tarjeta NIC.
  - *Overrun Packets* — Exceso de paquetes: Paquetes *Ethernet* que fueron descartados debido a que el dispositivo tuvo una sobrecarga de paquetes para manejar.
  - *Packets Too Long* — Paquetes muy largos: Paquetes de *Ethernet* que fueron más largo de máximo tamaño (1518 *bytes*).
  - *Packets Too Short* — Paquetes muy pequeños: Paquetes de *Ethernet* que fueron más pequeños que el mínimo (64 *bytes*).
  - *Packets Truncated* — Paquetes truncados: Paquetes corruptos o incompletos.
- *Statistics: Transmit* — Estadísticas: Transmisión.  
Esta sección reporta el tráfico transmitido a través del puerto *Ethernet*
    - *Unicast Packets* — Paquetes *unicast*: Número de paquetes transmitidos en una comunicación punto a punto.
    - *Multicast Packets* — Paquetes *multicast*: Número de paquetes transmitidos que son enviados como transmisión para fijar los nodos.
    - *Total Bytes* — *Bytes* totales: Número total de *bytes* transmitidos desde el puerto.
    - *Total Errors* — Errores totales: Número de paquetes a los que se les encontró algún error.
    - *Discarted Packets* — Paquetes descartados: Número de paquetes descartados debido a errores o congestión de la red.

- *Forwardable Packets* — Paquetes enviados: Paquetes enviados por el puerto que fueron aceptados o pasados a través de filtros.
- *Max Retry Packets* — Máximo reintento de envío de paquetes: Paquetes que fallaron después de haber sido reintentados varias veces.
- *Total Collisions* — Colisiones totales: Número de paquetes colisionados en este puerto.
- *Late Collisions* — Colisiones tardías: Error de paquetes que probablemente fueron causados por problemas de cableado. Este indicador también podría significar un fallo en tarjeta NIC.
- *Overrun Packets* — Exceso de paquetes: Paquetes que fallaron en el envío debido a que el dispositivo no pudo mantener el ritmo de transmisión del controlador de *Ethernet*.

#### A) IDENTIFICATION — IDENTIFICACIÓN

Pruebal **Ethernet Identification** CISCO SYSTEMS  
Uptime: 00:14:07

Cisco 350 Series AP 12.00T

[Map](#) [Help](#)

Primary Port?  yes  no Adopt Primary Port Identity?  yes  no

MAC Addr.:	00:40:96:54:f9:0a
Default IP Address:	<input type="text" value="172.20.17.175"/>
Default IP Subnet Mask:	<input type="text" value="255.255.255.0"/>
Current IP Address:	172.20.17.175
Current IP Subnet Mask:	255.255.255.0
Maximum Packet Data Length:	1504

Figura 8.44 Página de *Ethernet Identification*

- *Primary Port* — Puerto Primario: Determina tanto la dirección MAC como la IP. Por defecto, el puerto primario del Punto de Acceso es el *Ethernet*. Se debe seleccionar **NO** para configurar el puerto de radio como puerto primario.

- *Adopt Primary Port Identity* — Adoptar identidad de Puerto Primario: Si selecciona **NO**, es para especificar otra dirección MAC e IP al puerto *Ethernet*.
- *Default IP Address* — Dirección IP por defecto: Permite especificar la dirección IP del Punto de Acceso. Si se tiene inactivo el DHCP o BOOTP, la dirección especificada en este campo es la IP del Punto de Acceso. Si la opción de DHCP o BOOTP está activa, este campo muestra la dirección IP que ha sido asignada dinámicamente por alguno de estos servidores durante un tiempo limitado. Este campo también puede ser modificado en el Menú de *Express Setup* y en *AP Radio Identification*.
- *Default IP Subnet Mask* — Máscara de red por defecto: Si se tiene inactivo DHCP o BOOTP, este campo corresponde a la máscara de subred. Si se encuentra activo este campo provee máscara de subred sólo si no existen servidores que respondan a la petición del AP, y ésta es utilizada por el servidor. Este campo puede modificarse en el Menú de *Express Setup* y en *AP Radio Identification*.

## **B) HARDWARE**

Esta opción despliega la siguiente pantalla. Aquí se debe especificar el tipo de conector, velocidad de la conexión y la configuración *duplex* a utilizarse en el Puerto de *Ethernet*.

## Prueba1 Ethernet Hardware

Cisco 350 Series AP 12.00T

Map Help Uptime: 00:15:51

Speed: Auto  
CAM Size: 0  
Loss of Backbone Connectivity # of Secs (1-10000): 2  
Loss of Backbone Connectivity Action: No action  
Loss of Backbone Connectivity SSID: ab3

This system supports Ethernet-inline power from powered switches. Some models of such switches do not fully support Ethernet speed auto-negotiation. Because of this, selection of "Auto" for Ethernet speed will not take effect until the next Cold Boot of this system.

Apply OK Cancel Restore Defaults

Figura 8.45 Página de *Ethernet Hardware*

- *Speed* — Velocidad: El parámetro por defecto es **AUTO**, el cual es la mejor opción ya que la velocidad y los parámetros de *duplex* son negociados automáticamente entre la *LAN* y el AP. Se debe tener el cuidado que si se activa este modo de operación, el *hub*, *switch* o *router* al que se encuentra conectado lo soporte. De lo contrario debe especificarse de manera estática y con el cuidado de coincidir con los parámetros de velocidad de conexión, el tipo de conector y el modo *duplex*, especificados a la red.

### Ejemplo:

*10 Base-T / Half Duplex*: Conector a la red para 10 Mbps de velocidad sobre cable par trenzado, y operando en modo *Half-Duplex*.

- *Loss of Backbone Connectivity # of Secs (1-10000)* — Pérdida de conectividad al *Backbone* en # de segundos: Este parámetro especifica el aumento de tiempo que ha tenido el AP antes de tomar alguna acción cuando no se detecta conectividad al *Backbone*.
- *Loss of Backbone Connectivity Action* — Acción de Pérdida de Conectividad al Cable Principal: Determina la acción a tomarse una vez cumplido el tiempo de espera para que vuelva la conectividad. Pueden tomarse las siguientes posibles acciones:

- *No Action* — Sin acción: No se hace nada y se mantiene la conexión.
  - *Switch to repeater mode* — Conmutar a modo repetidor: El AP desasocia a todos sus Clientes y se convierte en repetidor mientras se encuentra suspendida la conexión del *backbone*. Para ello el AP intenta comunicarse con otro AP en modo *ROOT* utilizando el SSID. Si no logra establecer conexión, no vuelve a conectar Clientes.
  - *Shut the Radio Off* — Apagar el Radio: El AP se remueve a sí mismo de la red lograr asociar algún Cliente, hasta que se restablezca la conexión.
  - *Restrict to SSID* — Restringir al SSID: El AP se remueve a sí mismo y desasocia los Clientes, pero cuando se restablece el *Backbone* solamente permite a una persona con el mismo SSID para que vuelva a levantar el sistema.
- *Loss of Backbone Connectivity SSID* — Pérdida de conectividad SSID al *Backbone*: Este parámetro especifica el SSID usado por el AP si el parámetro de *Backbone Loss Conectivity* se configura como *Restrict to SSID* y si la conexión al *Backbone* sobrepasa el tiempo especificado en *Loss of Backbone Connectivity*.

**Nota:** Cuando la conexión al *Backbone* es restaurada, el AP carga los parámetros establecidos durante su operación normal.

### c) **FILTERS** — **FILTROS**

Los Filtros de protocolos evitan o permiten el uso de protocolos específicos a través del dispositivo. Estos se pueden configurar individualmente o por grupos. Utilice los Filtros de protocolos de radiofrecuencia *AP/Root* para crear y habilitar filtro para el puerto de radio. Utilice la página de Filtros de Protocolo *Ethernet* para crear y habilitar filtros de protocolos en esta interfaz.



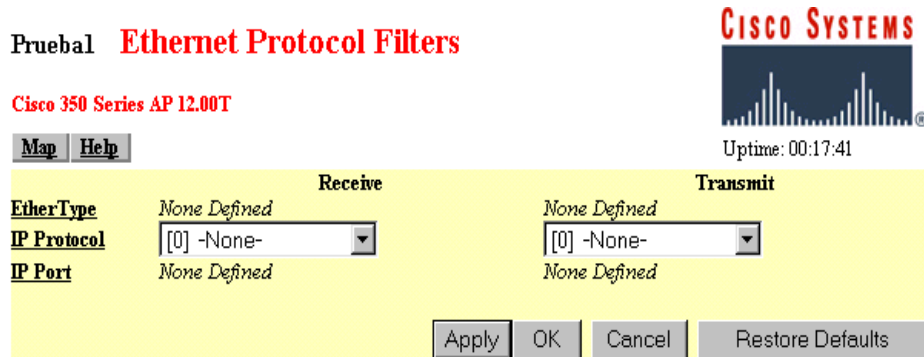


Figura 8.46 Página de *Ethernet Protocol Filters*

- *EtherType* — Tipo *Ethernet*: Seleccionar el filtro de protocolo que desea habilitar.
- *IP Protocol* — Protocolo IP: Seleccionar el filtro de protocolo que desea habilitar.
- *IP Port* — Puerto IP: Seleccionar el filtro de protocolo que desea habilitar.

#### D) ADVANCE — AVANZADO

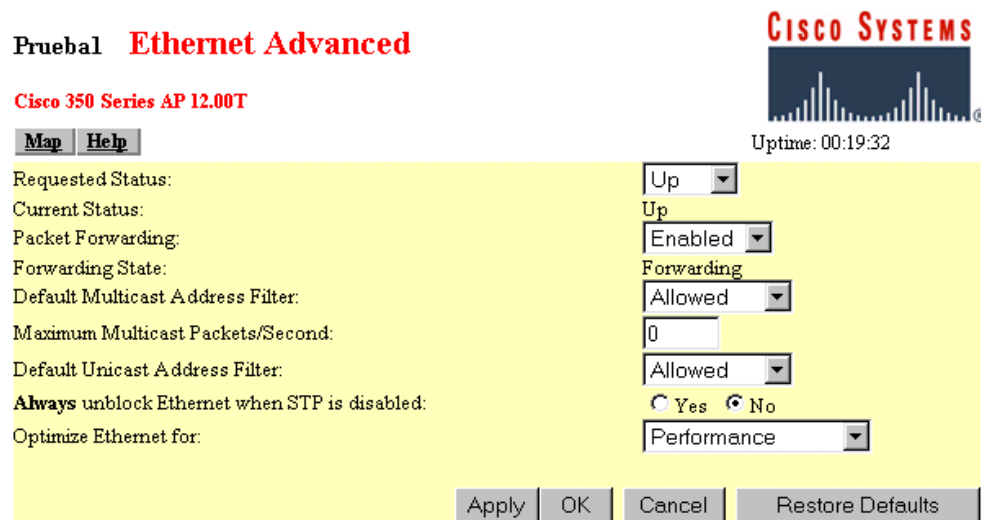


Figura 8.47 Página de *Ethernet Advanced*

Presenta el estado actual del puerto *Ethernet* y su estado de *Forwarding* (Envío). Existen los siguientes mensajes de condición: Arriba, Abajo y Error.

El estado de envío se encuentra establecido por defecto, sin embargo también existen otros cuatro estados:

- *Unknown* — Desconocido: No se puede determinar su estado.
  - *Disabled* — Deshabilitado: Las capacidades de envío están deshabilitadas.
  - *Blocking* — Bloqueado: El puerto se encuentra bloqueado para la transmisión. Este estado se despliega siempre que no existen Clientes asociados al Punto de Acceso.
  - *Broken* — Interrumpido: El estado reporta un fallo en el puerto.
- 
- *Requested Status* — Estado de petición: Este parámetro es utilizado para solución de problemas de la red. El estado de *Up* (arriba) permite que el puerto *Ethernet* funcione de manera normal. El estado de *Down* (abajo) deshabilita el puerto *Ethernet*.
  - *Packet Forwarding* — Envío de paquetes: Este parámetro está siempre habilitado en operación normal. Para solución de problemas, se debe deshabilitar este parámetro.

Existen 4 modos de operación adicionales:

- *Unknown* — Desconocido: No se puede determinar su estado.
- *Disabled* — Deshabilitado: Las capacidades de envío están deshabilitadas.
- *Blocking* — Bloqueado: El puerto se encuentra bloqueado para la transmisión.
- *Broken* — Interrumpido: El estado reporta un fallo en el puerto.

- *Default Unicast and Multicast Address Filters* — Filtros de dirección *unicast* y *multicast* por defecto: Los filtros de direcciones MAC permiten o no, realizar el envío de paquetes *multicast* o *unicast* a una dirección MAC específica. Puede crearse un filtro que permita el paso a todas las direcciones MAC excepto aquella a la que se les especifique.

**Nota:** Los paquetes *unicast* son aquellos dirigidos hacia algún dispositivo dentro de la red. Los paquetes *multicast* son los direccionados a varios dispositivos dentro de la red.

La opción de *Allowed*, permite que el AP se dirija a todo el tráfico excepto a la dirección MAC especificada en la página de filtros.


**Recomendación:** Para la mayoría de las configuraciones deben mantenerse en *Allowed* el parámetro de *Default Multicast Address Filter*. Si se elige *Disallowed*, se debe agregar la dirección de *broadcast* (ffffffff) para la lista de direcciones permitidas en la página de *Address Filters* antes de cambiar la configuración, de otra manera el AP será bloqueado.

- *Maximun Multicast Packets/Second* — Máximo de paquetes *multicast* por segundo: Este parámetro permite controlar el número de paquetes *multicast* que pueden pasar a través del puerto *Ethernet* por segundo. Si se ingresa 0, el AP permite el tráfico de un número ilimitado de paquetes *multicast*. Si se elige otro número, el dispositivo va a permitir el tráfico especificado de paquetes.
- *Default Unicast Address Filter* — Filtro de direcciones *unicast* por defecto: Especifica si el filtro *unicast* por defecto se encuentra permitido o no.
- *Optimize Ethernet for* — Optimizar puerto *Ethernet* para: Especifica el rendimiento del puerto *Ethernet*. Existen 2 opciones:

- *Performance (por defecto)* — Rendimiento: Limita que las estadísticas por estación sean retornadas.
- *Statistics Collection* — Colección de estadísticas: Permite que las estadísticas puedan retornar y de manera más detallada.

## 2) AP RADIO — PUERTO DE RADIO

Esta página indica las estadísticas referentes al Puerto de Radio en una tabla.



Uptime: 00:28:44

Pruebal **AP Radio Port**

[Home](#)
[Map](#)
[Network](#)
[Associations](#)
[Setup](#)
[Logs](#)
[Help](#)

Options: Detailed Config.  Detailed Stats.  Individual Rates  Apply

Configuration		Set Properties	
Status of "awc0"	Up	Maximum Rate (Mb/s)	11.0
IP Address	172.20.17.175	MAC Address	00409654f90a
SSID	ab3		
Operational Rates (Mb/s)	1.0B, 2.0B, 5.5, 11.0	Transmit Power (mW)	100

Statistics <span style="float: right;">Refresh</span>			
Receive		Transmit	
	<i>Alert</i> <input type="checkbox"/>		<i>Alert</i> <input type="checkbox"/>
Unicast Packets	269	Unicast Packets	138
Multicast Packets	0	Multicast Packets	145
Total Bytes	20080	Total Bytes	123144
Total Errors	0	Total Errors	0
Discarded Packets	0	Discarded Packets	0
Forwardable Packets	132	by CoS (0-7): 0, 0, 0, 0, 0, 0, 0	
Filtered Packets	0	Forwarded Packets	456
Packet CRC Errors	4	Max Retry Packets	0
Packet WEP Errors	0	Total Retries	3
Overrun Packets	0	Cancelled Assoc. Lost	0
Duplicate Packets	1	Cancelled AID	0
Lifetime Exceeded	0	Lifetime Exceeded	0
MIC Packets	0	MIC Packets	0
MIC Errors	0	MIC Errors	0
MIC Sequ. Errors	0		
MIC Auth. Errors	0		

Figura 8.48 Página de AP Radio Port

- *Options* — Opciones: Presenta 3 opciones: Configuración Detallada, Estadísticas Detalladas ó Tasas Individuales.
- *Configuration Information* — Información de configuración:
  - *Status of "awc0"* — Estado del "awc0": Presenta las siguientes opciones:
    - Up* — Arriba: El enlace está operando apropiadamente.
    - Down* — Abajo: El enlace no está operando.
    - Error*: El radio principal se encuentra en condición de error.
  - *Maximum Rate (Mbps)* — Tasa máxima: La tasa máxima de transmisión de datos en megabits por segundo. Las tasas de datos configuradas en *Basic* son seguidas de una *B*.
  - *IP Addr* — Dirección IP: Dirección IP del puerto de comunicación de radio.
  - *MAC Addr* — Dirección MAC: Identificador único asignado a la interfaz de red por el fabricante.
  - *SSID* : Identificador único que el Cliente utiliza para asociarse con el AP o VLAN. Este le ayuda al Cliente a distinguir entre múltiples redes inalámbricas en la misma cercanía y provee a los Clientes acceso a las VLAN's.
  - *Operational Rates* — Tasas operacionales: Transmisión de datos soportados y habilitados por el AP para comunicación con otros dispositivos.

- *Transmit Power (mW)* — Potencia de transmisión: Nivel de potencia de transmisión del radio. Ésta se puede reducir para reservar potencia o reducir la interferencia.
- *Receive Statistics* — Estadísticas de recepción:
  - *Unicast Packets* — Paquetes *unicast*: Número de paquetes recibidos en una comunicación punto a punto.
  - *Multicast Packets* — Paquetes *multicast*: Número de paquetes recibidos que son enviados como transmisión para fijar los nodos.
  - *Total Bytes* — Bytes totales: Número total de *bytes* recibidos.
  - *Total Errors* — Errores totales: Número de paquetes a los que se les encontró algún error.
  - *Discarded Packets* — Paquetes descartados: Número de paquetes descartados debido a errores o congestión de la red.
  - *Forwardable Packets* — Paquetes enviados: Paquetes recibidos por el puerto que fueron aceptados o pasados a través de filtros.
  - *Filtered Packets* — Paquetes filtrados: Paquetes que fueron detenidos por los filtros configurados en el puerto.
  - *Packet CRC Errors* — Paquetes con errores CRC: Errores del tipo CRC que fueron detectados en los paquetes recibidos.
  - *Packet Web Errors* — Errores de errores Web: Errores de encriptación recibidos a través de este puerto.
  - *Overrun Packets* — Exceso de paquetes: Paquetes *Ethernet* que fueron descartados debido a que el dispositivo tuvo una sobrecarga de paquetes que manejar.
  - *Duplicate Packets* — Paquetes duplicados: Paquetes que fueron recibidos dos veces debido a que el conocimiento se perdió y el transmisor volvió a transmitir el paquete.

- *Lifetime Exceeded* — Tiempo de vida excedido: Paquete fragmentado que es desechado debido a que tomó mucho tiempo para recibir el siguiente fragmento.
  - *MIC Packets* — Paquetes MIC: Total de paquetes recibidos a través del puerto de radio desde que el sistema inicializó, y que ha recibido una petición de validación de MIC con el algoritmo MMH.
  - *MIC Errors* — Errores MIC: Total de paquetes recibidos a través del puerto de radio desde que el sistema inicializó y que falló en la validación con el algoritmo MMH.
  - *MIC Sequ.Errors* — Errores de secuencia MIC: Paquetes que fueron recibidos tarde o fuera de orden debido a un mal estado del enlace de radio o una respuesta de ataque.
  - *MIC Auth. Errors* — Errores de autenticación MIC: La firma del MIC está mal debido a que la llave criptográfica está equivocada. La llave *WEP* necesitará reconfigurarse de nuevo.
- *Transmit Statistics* — Estadísticas de transmisión:
    - *Unicast Packets* — Paquetes *unicast*: Número de paquetes transmitidos en una comunicación punto a punto.
    - *Multicast Packets* — Paquetes *multicast*: Número de paquetes transmitidos que son enviados como transmisión para fijar los nodos.
    - *Total Bytes* — Bytes totales: Número total de *bytes* transmitidos.
    - *Total Errors* — Errores totales: Número de paquetes a los que se les encontró algún error.
    - *Discarded Packets* — Paquetes descartados: Número de paquetes descartados debido a errores o congestión de la red.
    - *Forwarded Packets* — Paquetes enviados: Paquetes transmitidos por el puerto que fueron aceptados o pasados a través de filtros.

- *Max Retry Packets* — Reintento máximo de paquetes: Número de reintentos máximos de peticiones de envío (RTS). Este número se puede cambiar en la página de *AP Radio Hardware*.
- *Total Retries* — Reintentos totales: Número de reintentos que ocurrieron a través del puerto de radio.
- *Cancelled Assoc.* — Asociación cancelada: Paquetes descartados debido a que el Cliente perdió asociación con el AP.
- *Cancelled AID* — AID cancelada: Paquetes descartados por el repetidor debido a que el Cliente se cambió a otro AP durante el intento de retransmisión.
- *Lifetime Exceeded* — Tiempo de vida excedido: Paquete fragmentado que es desechado debido a que tomó mucho tiempo para recibir el siguiente fragmento.
- *MIC Packets* — Paquetes MIC: Total de paquetes recibidos a través del puerto de radio desde que el sistema inicializó, y que ha recibido una petición de validación de MIC con el algoritmo MMH.
- *MIC Errors* — Errores MIC: Total de paquetes recibidos a través del puerto de radio desde que el sistema inicializó y que falló en la validación con el algoritmo MMH.
- *MIC Sequ.Errors* — Errores de secuencia MIC: Paquetes que fueron recibidos tarde o fuera de orden debido a un mal estado del enlace de radio o una respuesta de ataque.
- *MIC Auth. Errors* — Errores de autenticación MIC: La firma del MIC está mal debido a que la llave criptográfica está equivocada. La llave *WEP* recesitará reconfigurarse de nuevo.



## A) IDENTIFICATION — IDENTIFICACIÓN

La página de identificación contiene la ubicación básica y la información de identidad para los puertos internos y por módulos del AP.

Pruebal **AP Radio Identification**

Cisco 350 Series AP 12.00T

Map Help

Uptime: 00:32:46

Primary Port?  yes  no Adopt Primary Port Identity?  yes  no

MAC Addr.:	00:0b:5f:eb:e1:ce
Default IP Address:	<input type="text" value="10.0.0.2"/>
Default IP Subnet Mask:	<input type="text" value="255.255.255.0"/>
Current IP Address:	172.20.17.175
Current IP Subnet Mask:	255.255.255.0
Maximum Packet Data Length:	2304
Service Set ID (SSID):	<input type="text" value="ab3"/> <a href="#">more...</a>
LEAP User Name:	<input type="text"/>
LEAP Password:	<input type="password" value="*****"/>
Firmware Version:	5.02.02
Boot Block Version:	1.50

Apply OK Cancel Restore Defaults

Figura 8.49 Página de AP Radio Identification

- **Primary Port Settings:** Existen 2 opciones:
    - **Primary Port** — Puerto primario: Determina la dirección MAC e IP. Generalmente el puerto primario del AP es el puerto *Ethernet*, el cual está conectado directamente a la LAN, por lo cual el parámetro debe estar en **NO**. Si se escoge **SI**, el puerto primario va a ser el de radio.
    - **Adopt Primary Port Identity** — Adoptar identidad de puerto primario: Si se selecciona **SI**, el puerto adopta los parámetros de configuración para el puerto de radio (dirección IP y MAC). Si selecciona **NO** es para utilizar una dirección MAC e IP diferentes.
- Cuando el AP está activo como **ROOT** se adopta este parámetro para el puerto de radio. Cuando se encuentra configurado en modo *Standby*, debe seleccionarse como **NO**.

- *Default IP Address* — Dirección IP por defecto : En este parámetro se asigna una dirección IP al puerto de radio distinta a la del puerto *Ethernet*. Durante la operación normal el puerto de radio adopta la dirección del puerto *Ethernet*. Cuando el AP está en *Standby*, se debe configurar una dirección diferente al puerto de radio.
- *Default IP Subnet Mask* — Submáscara de red por defecto: Ingrese la máscara de subred para identificar la red a la cual pertenece la dirección IP asignada.
- *Service Set ID (SSID)* — Fijación de servicio de identificación: El SSID es un identificador único que permite asociar al Cliente con el AP o una VLAN. Pueden ser configurados cerca de 16 SSID's en un AP.
- *LEAP User Name* — Nombre de usuario *LEAP*: Utiliza el usuario configurado en este campo para validarse ante el servidor de autenticación de la red.
- *LEAP Password* — Clave *LEAP*: Utiliza la palabra clave configurada en este campo para validarse ante el servidor de autenticación de la red.
- *Firmware Versión* — Versión de Sistema Operativo: Indica el nivel del *software* que controla la red en la tarjeta de red para radio.
- *Boot Block Versión* — Versión del conjunto de inicio: Indica el nivel de la versión del *software* de *reboot* en la tarjeta de red para radio.

## B) HARDWARE

**Prueba1 AP Radio Hardware**

**Cisco 350 Series AP 12.00T**

**CISCO SYSTEMS**

Uptime: 00:35:04

[Map](#) [Help](#)

Service Set ID (SSID):  [more...](#)

Allow "Broadcast" SSID to Associate?:  yes  no

Enable "World Mode" multi-domain operation?:

Data Rates (Mb/sec):

1.0  2.0  5.5  11.0

Transmit Power:

Frag. Threshold (256-2338):  RTS Threshold (0-2339):

Max. RTS Retries (1-255):  Max. Data Retries (1-255):

Beacon Period (19-5000 Kusec):  Data Beacon Rate (DTIM):

Default Radio Channel:  In Use: 6

Search for less-congested Radio Channel?:  [Restrict Searched Channels](#)

Receive Antenna:  Transmit Antenna:

If VLANs are not enabled, set Radio Data Encryption through the link below. If VLANs are enabled, Radio Data Encryption is set independently for each enabled VLAN through [VLAN Setup](#).

[Radio Data Encryption \(WEP\)](#)

Figura 8.50 Página de AP Radio Hardware

Esta página de configuración contiene además un enlace a las páginas de *AP Radio Data Encryption* y *VLAN Setup*, con las cuales se puede configurar la encriptación de datos del puerto de radio. Si no existen VLAN's configuradas en su red debe utilizar solamente la página de enlace de *AP Radio Data Encryption (WEP)*.

- *Service Set ID (SSID)* — Fijador de servicios de identificación: El SSID es un identificador único que permite asociar al Cliente con el AP o una VLAN. Pueden ser configurados cerca de 16 SSID's en un AP.

- *Allow Broadcast SSID to Associate?* — Permitir asociación por *broadcast* de SSID: Este parámetro permite escoger aquellos dispositivos que no especifican un SSID y son permitidos para asociarse con un AP.

**YES:** Permite que el dispositivo que no especifica un SSID pueda asociarse con un AP. Estos son aquellos dispositivos que son de tipo “*Broadcasting*” en la búsqueda de un AP para asociarse. Este parámetro es el que se especifica por defecto.

**NO:** Especifica aquellos dispositivos que no especifican un SSID y que no son permitidos para asociarse a un SSID. Seleccionando esta configuración, el SSID utilizado por el Cliente debe asociarse exactamente al AP con el mismo SSID.

- *Enable World Mode* — Habilitar modo universal: Seleccionando **SI** de este menú, el AP agrega una portadora de canal para colocar información de la señal. El Cliente con este parámetro habilitado permite recibir la información colocada en la portadora y ajustar su configuración *automáticamente*.
- *Data Rates* — Tasa de datos: Permite escoger la velocidad de transmisión de datos que utiliza el AP. El AP siempre intenta transmitir a la mayor velocidad colocándose en *BASIC*. Existen tres opciones:
  - *Basic (por defecto)* — *Básico*: Permite la transmisión a ésta razón para todos los paquetes, sean éstos *unicast* o *multicast*.
  - *Yes*: El AP transmite solamente paquetes *unicast* a ésta razón, mientras que los *multicast* son enviados a alguna de las velocidades escogidas en *BASIC*.
  - *No*: El AP no transmite datos a ésta velocidad

**Nota:** Cuando se selecciona *Optimize Radio Network For Throughput*, en el menú de *Express Setup*, todas las cuatro velocidades son puestas en *BASIC*. Cuando se selecciona *Optimize Radio Network For Range*, en el menú de *Express Setup*, la velocidad de 1.0 Mbps es colocada en *BASIC* y el resto son colocados en **SI**.

- *Transmit Power* — Potencia de transmisión: Este parámetro determina el nivel de potencia para la transmisión de radiofrecuencia.
- *Frag Threshold* — Umbral de fragmentación: Este parámetro determina el tamaño al cual los paquetes son fragmentados, pudiéndose seleccionar dentro del rango de 256 hasta 2338 *bytes*.

**Recomendación:** Utilice un número bajo donde el área de comunicación es pobre o donde exista gran interferencia en radiofrecuencia.

- *RTS Threshold* — Umbral del RTS: Este parámetro el tamaño del paquete al cual el punto de acceso efectúa una petición de envío (RTS) antes de enviar un paquete. El tamaño del mismo puede variar desde 0 hasta 2339 *bytes*. Un valor bajo para este parámetro puede ser muy útil en áreas donde existen muchos Clientes asociados a un AP o donde los Clientes se encuentran muy lejos.
- *Max RTS Retries* — Reintentos máximos para RTS: Especifica en máximo número de veces que el AP realizar un RTS antes de detener el intento de enviar un paquete a través de la interfaz de radio. Puede ser escogido un valor entre 1 y 128.
- *Max. Data Retries* — Reintento máximo de Datos: Número máximo de intentos que realiza el AP antes de darse por vencido de enviar un paquete y desecharlo.

- *Beacon Period* — Periodo de señal: Aumento de tiempo entre señales, medido en unidades de kilomicrosegundos (1 kilomicrosegundo=1,024 microsegundos).
- *Data Beacon Rate (DTIM)* — Tasa de señales de datos: Este parámetro es siempre un múltiplo del periodo entre señales y determina qué tan seguido la señal contiene un mensaje indicador (DTIM). El DTIM dice en un Cliente configurado en modo de ahorro de energía, que un paquete está esperando por él.  
Si el periodo de señal es colocado en 100 (por defecto), y la señal de datos es colocado en 2 (por defecto), entonces el AP envía señales conteniendo un DTIM cada 200 Kμseg.
- *Default Radio Channel* — Canal de radio por defecto: El canal de radiofrecuencia especificado por defecto por Cisco es canal 6, para burlar el problema de interferencia. Sin embargo pueden ponerse a funcionar 3 canales a la vez (1, 6 y 11) sin tener problema de interferencia entre canales.
- *Search For Less Congested Radio Channel* — Buscar el canal menos congestionado : Cuando se selecciona **SI** en este parámetro, el AP revisa cual es el canal menos ocupado y lo utiliza. Si lo que se necesita es mantener un solo canal de transmisión estático, se debe seleccionar **NO**.
- *Restric Search Channels* — Restricción de canales de búsqueda: Puede seleccionarse y restringir a la hora de la búsqueda en los canales menos congestionados, entre cuáles canales debe escoger el AP para enviar información.

- *Receive Antenna and Transmit Antenna* — Antena de recepción y antena transmisión: Se presentan 3 opciones:

- *Diversity (por defecto)* — Diversidad: Este parámetro le dice al AP utilizar la antena que recibe la mejor señal. Si el AP cuenta con antenas no removibles, usted debe utilizar este parámetro.

- *Right* — Derecha: Si el AP tiene antenas removibles y se instala una antena de alta ganancia en el conector derecho del AP, usted puede utilizar este parámetro para recibir y transmitir.

- *Left* — Izquierda: Si el AP tiene antenas removibles y se instala una antena de alta ganancia en el conector izquierdo del AP, usted puede utilizar este parámetro para recibir y transmitir.

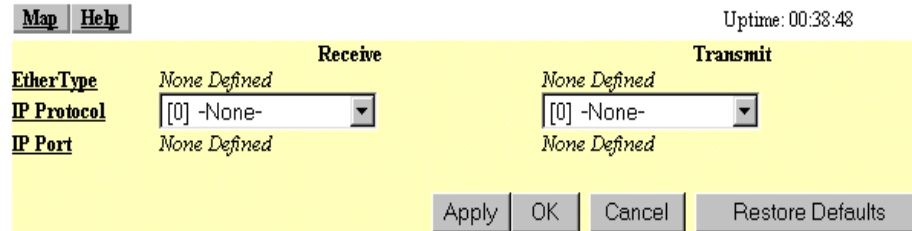
**Nota:** El AP transmite y recibe utilizando solamente una antena a la vez, por lo que no se puede incrementar la cobertura instalando antenas de alta ganancia en ambos conectores y apuntando en sentidos opuestos.

### **c) FILTERS — FILTROS**

Los filtros de protocolos evitan o permiten el uso específico de protocolos a través de un dispositivo. Pueden configurarse filtros de protocolos de manera individual o en grupos. Utilice los Filtros de protocolos para radiofrecuencia para crear y habilitar los filtros para el puerto de radio. Utilice la página de filtros de protocolos *Ethernet* para crear filtros de protocolos para el puerto *Ethernet*.

## Pruebal AP Radio Protocol Filters

Cisco 350 Series AP 12.00T



Map Help

Uptime: 00:38:48

	Receive	Transmit
<u>EtherType</u>	None Defined	None Defined
<u>IP Protocol</u>	[0] -None-	[0] -None-
<u>IP Port</u>	None Defined	None Defined

Apply OK Cancel Restore Defaults

Figura 8.51 Página de AP Radio Protocol Filter

- *EtherType* — Tipo *Ethernet*: Seleccionar el filtro del protocolo que desee activar.
- *IP Protocol* — Protocolo IP: Seleccionar el filtro del protocolo que desee activar.
- *IP Port* — Puerto IP: Seleccionar el filtro del protocolo que desee habilitar.



## D) ADVANCE — AVANZADO

### Prueba! AP Radio Advanced

Cisco 350 Series AP 12.00T



Uptime: 00:40:17

[Map](#) [Help](#)

Requested Status: Up   
Current Status: Up  
Packet Forwarding: Enabled   
Forwarding State: Forwarding  
Default Multicast Address Filter: Allowed   
Maximum Multicast Packets/Second: 0

Radio Cell Role: Access Point/Root   
SSID for use by Infrastructure Stations (such as Repeaters): 0  
Disallow Infrastructure Stations on any other SSID:  yes  no  
Use Aironet Extensions:  yes  no  
Classify Workgroup Bridges as Network Infrastructure:  yes  no  
Require use of Radio Firmware 5.02B:  yes  no  
Ethernet Encapsulation Transform: RFC1042

Quality of Service Setup

If VLANs are not enabled, set the following three parameters on this page. If VLANs are enabled, the following three parameters are set independently for each enabled VLAN through [VLAN Setup](#).

Enhanced MIC verification for WEP: None   
Temporal Key Integrity Protocol: None   
Broadcast WEP Key rotation interval (sec): 0 (0=off)

To configure 802.11 Authentication, EAP, Unicast Address Filters, and the Maximum Number of Associations for this radio's Primary SSID (the default SSID), please use the link below.

[Advanced Primary SSID Setup](#) [more...](#)

Preferred Access Point 1: 00:00:00:00:00:00  
Preferred Access Point 2: 00:00:00:00:00:00  
Preferred Access Point 3: 00:00:00:00:00:00  
Preferred Access Point 4: 00:00:00:00:00:00

Radio Modulation: Standard   
Radio Preamble: Short

Figura 8.52 Página de AP Radio Advanced

- *Requested Status* — Estado de petición: Este parámetro es muy útil para reparar problemas en la red. Utilizando **UP** (por defecto), mantiene el AP en modo normal de funcionamiento. **DOWN** apaga el AP.
  
- *Packet Forwarding* — Envío de paquetes: Este parámetro se encuentra habilitado bajo operación normal. Para resolver problemas se debe deshabilitar para prevenir movimiento de datos entre la interfaz *Ethernet* y la de Radiofrecuencia.
  
- *Forwarding State* — Estado de Envío: Existen 4 posibles modos de operación en estado de envío:
  - *Unknown* — Desconocido: El estado no puede ser determinado.
  - *Disabled* — Deshabilitado: Capacidades de envío están deshabilitadas.
  - *Blocking* — Bloqueado: El puerto está bloqueado para transmisión. Este estado se da cuando no existen Clientes asociados.
  - *Broken* — Interrumpido: Reporta un fallo en el puerto de radio.
  
- *Default Multicast Address Filters* — Filtros de direcciones *multicast* por defecto: Los filtro de direcciones MAC permiten o no el envío de paquetes a una dirección MAC específica. Se puede crear filtros que permitan o nieguen, el tráfico a todas las direcciones MAC excepto aquellas que sean especificadas.

Se presentan 2 opciones para este parámetro:

- *Allowed* — Permitido: El AP envía todo el tráfico excepto a aquellos Clientes que han sido deshabilitados de la página de Filtros de dirección.
- *Disallowed* — No permitido: El AP descarta todo el tráfico excepto los paquetes enviados a los Clientes permitidos en la página de Filtros de dirección.

**Nota:** Si se desea descartar el tráfico de todas las direcciones MAC, excepto aquellas que usted especifique, debe asegurarse de ingresar su propia dirección MAC como permitida para evitar ser bloqueado por el AP.

- *Maximun Multicast Packets/Second* — Máximo de paquetes *multicast* por segundo: Con este parámetro se controlan el número de paquetes que pueden pasar através del puerto de radio por segundo. Si se ingresa 0, el AP permite un número ilimitado de paquetes de *multicast*. Si se especifica otro número mayor a 0, el dispositivo solamente permite el número especificado de paquetes *muticast* por segundo.
- *Radio Cell Role* — Papel del radio en la celda: Aquí se puede seleccionar el funcionamiento del AP dentro del área de cobertura o celda, determinando el modo de interacción con otros dispositivos inalámbricos.

Existen 3 opciones para este parámetro:

- *Root*: Utilice este parámetro si el AP está conectado a la red alambrada.
  - *Repeater/Non-Root*: El AP transfiere los datos entre un Cliente y otro AP. Se utiliza cuando el AP no esté conectado directamente a la red LAN alambrada.
  - *Client/Non-Root*: Utilice este parámetro para realizar diagnósticos, como por ejemplo cuando se necesita saber si el AP está teniendo comunicación con otro AP, sin necesidad de aceptar asociación de otros Clientes.
- *SSID for use by Infraestructura Stations (such as Repeaters)* — SSID utilizado por estaciones de infraestructura (tales como repetidores): Identifica el SSID a ser utilizado por repetidores o *Bridges* para que se puedan asociar al AP. Este SSID debe ser mapeado a la VALN ID con el propósito de facilitar la comunicación entre dispositivos de infraestructura y AP's en modo *Non-Root*.

- *Disallow Infrastructure Stations on any other SSID* — No permitir estaciones de infraestructura en otro SSID: Evita que repetidores o *Bridges* sean asociados a SSID's que no han sido especificados en la Infraestructura de SSID. Por defecto se encuentra en **NO** para invocar ésta condición.
  
- *Use Aironet Extensions* — Utilizar extensiones Aironet: Debe seleccionar si desea o no utilizar extensiones Cisco Aironet 802.11. Debe configurarse en **SI** (por defecto) para:
  - *Load Balancing* — Balanceo de la carga: Permite escoger entre las mejores condiciones de conexión a la red para proveer servicio a un Cliente, como por ejemplo: número de usuarios, relación de bits de error y fortaleza de la señal.
  - *Message Integrity Check (MIC)* — Verificación de la integridad del mensaje: Es una característica adicional de seguridad del *WEP* que previene ataques en paquetes encriptados llamados ataques *bit-flip*. El MIC agrega en los AP's y los Clientes asociados, unos bits adicionales a cada paquete para hacerlos menos vulnerables.
  
- *Temporal Key Integrity Protocol (TKIP)* — Protocolo de llave de integridad temporal: Es también conocido como la llave del *WEP*. Es una característica adicional de seguridad del *WEP* que evita que los intrusos utilicen un segmento no encriptado de los paquetes llamado Vector de Inicialización (IV) para calcular la llave *WEP*.
  
- *Repeater Mode* — Modo repetidor: Se debe configurar el uso de extensiones Aironet en **SI**, si el AP es configurado en modo repetidor o si se comunica con un repetidor.

**Nota:** Si se habilita ésta característica, el AP debe realizarse el *reboot* manualmente para que tengan efecto los cambios.

- *Classify Workgroup Bridges as Network Infrastructure* — Clasificar *Bridges* de grupo como redes de infraestructura: Se debe seleccionar **NO** para permitir que más de 20 *Bridges* se asocien al AP. La configuración **SI** (por defecto), limita el número de *Bridges* a menos de 20.

Tratar un *Bridge* como dispositivo de infraestructura significa que el AP envía paquetes de *multicast* de manera confiable, incluyendo los paquetes del Protocolo de Distribución de Direcciones (ARP) al *Bridge*.

El costo de rendimiento del envío de *multicast* confiables, limita el número de dispositivos de infraestructura que pueden ser asociados al AP. Para incrementar el número de *Bridges* que se puede asociar, el punto de acceso debe reducir la confiabilidad de los paquetes de *multicast* a los *Bridges*.

**Nota:** Esta característica funciona mejor en *Bridges* estacionarios, ya que en *Bridges* móviles pueden existir áreas de cobertura donde se pierda la comunicación.

- *Require Use of Radio Firmware x.xx* — Requiere el uso de Sistema Operativo del Radio: Este parámetro afecta el proceso de actualización del *firmware* cuando se carga uno más reciente al AP. Se debe seleccionar **SI** para forzar a la actualización de una versión compatible con sistema operativo actual. Seleccionando **NO** se evita realizar actualizaciones automáticas del *firmware*.
- *Ethernet Encapsulation Transform* — Transformar encapsulado *Ethernet*: Selecciona 802.1H o RFC1042 para colocar el tipo de encapsulado *Ethernet*. Los paquetes de datos que no son 802.2 deben ser formateados utilizando 802.1H o RFC1042. En general, los equipos Cisco Aironet utilizan 802.1H para proveer mayor interoperabilidad.
  - *802.2H (por defecto)*: Provee rendimiento óptimo para equipos Aironet.
  - *RFC1042*: Provee interoperabilidad con equipo inalámbrico que no pertenece a la familia Aironet, aunque no es lo óptimo.

- *Quality of Service Setup Link (QoS)* — Configuración de la calidad de servicio del enlace: Este parámetro está referido a la interfaz de radio.
- *VLAN Setup Link* — Configuración de enlace de VLAN: Permite el acceso a la página de configuración de VLAN.
- *Enhanced MIC verification for WEP* — Verificación mejorada de la MIC para WEP: Este parámetro habilita la Verificación de Integridad del Mensaje (MIC), el cual es una característica de seguridad que protege la llave de WEP. Para habilitarlo se debe seleccionar MMH del menú.

**Nota:** El MIC toma efecto solamente cuando en la página de *AP Radio Advanced*, el parámetro de *Use Aironet Extension* es **SI**; y además el WEP está habilitado y con encriptación completa.

Tome en cuenta que cuando se habilita este parámetro solamente los Clientes que soporten este parámetro se van a poder comunicar con el AP.

- *Temporal Key Integrity Protocol (TKIP)* — Protocolo temporal de integridad de la llave : Este parámetro habilita la llave de WEP, la cual defiende contra ataques utilizando el vector de inicialización (IV).

**Nota:** Tenga en cuenta que al habilitar este parámetro, solamente se podrán conectar al AP aquellos dispositivos que lo soporten.

- *Broadcast WEP key rotation interval (sec)* — Intervalo de rotación del *broadcast* para llave WEP: Esta opción habilita la rotación de la llave colocándole un intervalo tiempo para ello. En *broadcast* o *multicast*, el AP provee un *broadcast* dinámico de llave WEP. Ésta última alternativa es excelente para TKIP si en la red se encuentran dispositivos que no son Cisco o que no pueden ser actualizados con la última versión del *firmware* para Clientes.

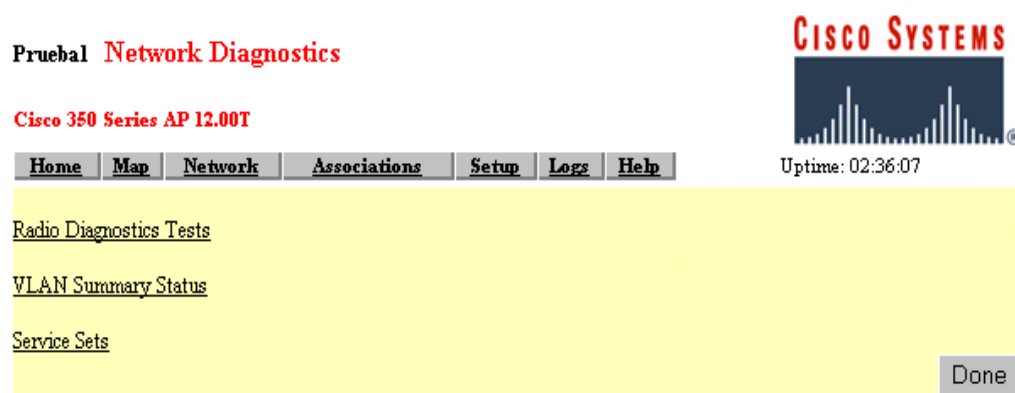
Para habilitar la rotación de la llave ingrese el intervalo en segundos para realizar cada *broadcast*. Para deshabilitar este parámetro ingrese 0.

**Nota:** Solamente los dispositivos que utilizan autenticación *LEAP*, *EAP-TLS* o *PEAP*, con este parámetro activo, pueden acceder al AP. El resto de dispositivos que utilicen autenticación *WEP* (con o sin llave abierta, o *EAP-MD5*) no podrán acceder el AP, con este parámetro activo.

- *Advanced Primary SSID Setup Link* — Configuración avanzada de enlace primario SSID : Este enlace permite configurar autenticación 802.11, *EAP*, filtros de dirección *unicast* y el máximo número de asociaciones para el radio primario SSID.
- *Preferred Access Points* — Punto de acceso preferido: Se utiliza para configurar una cadena de AP sin conexión *Ethernet*. La función del AP como repetidor funciona mejor cuando se asocia a un AP en específico.  
Si éste AP funciona como repetidor, debe ingresar la dirección MAC de los AP en modo *Root* a los cuales se desea asociar.  
Si la configuración del parámetro *Adopt Primary Port Identity* en la página de *Radio Identification*, es **NO**, se debe ingresar la dirección MAC tal y como aparece en la página de *Radio Identification*. Si el parámetro de *Adopt Primary Port Identity* es **SI**, se puede especificar la dirección MAC tal y como aparece en la página de *Express Setup*.
- *Radio Modulation* — Modulación del radio: Existen dos opciones:
  - *Standard (por defecto)*: Este es el tipo de modulación especificado por la IEEE 802.11.
  - *MOK*: Esta modulación fue utilizada antes de terminarse estándar 802.11 de alta velocidad y puede ser utilizada todavía en redes inalámbricas antiguas.

- *Radio Preamble* — Preámbulo de radio: El preámbulo es una sección de datos a la cabeza de los paquetes que contienen información del AP y el Cliente cuando se envían y reciben paquetes. Existen dos opciones para escoger el preámbulo:
  - *Long* — Largo: Un preámbulo largo asegura la compatibilidad entre AP y los modelos recientes de Adaptadores de Red (los PC4800 y PC4800A).
  - *Short* — Corto: Un preámbulo corto mejora el rendimiento del *throughput*. Los últimos modelos de Adaptadores de red requieren un preámbulo largo.

## **Diagnostics**



**Figura 8.53** Página de *Network Diagnostics*

a) *Radio Diagnostics Tests* — Prueba de diagnóstico de radio: Debe hacer *click* en este parámetro para acceder la página de diagnósticos para radiofrecuencia y poder realizar una prueba de portadora.

Esta prueba de portadora permite determinar cuáles frecuencias de radio contienen la mayor actividad de radio y el ruido que puede interferir con las señales de radio, desde y hacia el AP.

Utilice éste diagnóstico de la portadora para determinar cual es la mejor frecuencia para utilizar el AP.

Cuando realice esta prueba, debe estar seguro que los dispositivos inalámbricos de la red deben estar dentro del alcance de operación del AP.



**Nota:** El AP desconecta toda asociación con los dispositivos de red inalámbrica durante esta prueba de portadora.

*b) VLAN Summary Status* — Resumen de estados de VLAN's: Los siguientes enlaces están disponibles en esta página:

*b.1) VLAN Detailed Setup* — Configuración detallada de VLAN: Este enlace lleva a la página de *VLAN Setup*, desde la cual usted puede agregar, eliminar o editar la configuración de las VLAN's.

*b.2) ID(#)*: Este enlace lleva hasta la página de *VLAN Setup* para seleccionar el *VLAN ID* donde usted puede editar la configuración.

*b.3) Def. Pol.Grp (if set)*: Este enlace lleva a la página de *Policy Group* (Políticas de Grupo), donde se puede editar la configuración.

*c) Service Sets* — Fijación de servicios: Este enlace lleva a la página de *AP Radio Service Set Summary Status*. Aquí se encuentran los siguientes enlaces:

*c.1) Service Set Detailed Setup* — Configuración detallada de la fijación de servicios: Este enlace lleva a la página de *AP Radio Service Set*, desde la cual se puede crear, remover o editar la configuración del SSID.

*c.2) Idx(#)*: Este enlace lleva a la página de *AP Radio Primary SSID* del número seleccionado donde usted puede editar la configuración.

## Express Setup

**Prueba1 Express Setup**

**Cisco 350 Series AP 12.00T**

[Home](#) [Map](#) [Help](#) Uptime: 00:52:41

System Name:

MAC Address: 00:40:96:54:f9:0a

Configuration Server Protocol:

Default IP Address:

Default IP Subnet Mask:

Default Gateway:

AP Radio:

Service Set ID (SSID):  [more...](#)

Role in Radio Network:

Optimize Radio Network For:  Throughput  Range  Custom

Ensure Compatibility With:  2Mb/sec Clients  non-Aironet 802.11

Security Setup

SNMP Admin. Community:

Security Setup

SNMP Admin. Community:

**Figura 8.54** Página de *Express Setup*

Como se puede notar en la Figura 8.54, este menú presenta las siguientes opciones de configuración:

- *System Name* — Nombre del sistema: Aparece como título en las páginas del sistema de Administración y en la página de la Tabla de Asociación del Punto de Acceso. Este parámetro no es necesario colocarlo pero ayuda a identificar el Punto de Acceso en la red.

La dirección MAC del Punto de Acceso aparece debajo del Nombre del Sistema. Esta dirección es un número de serie asignado permanentemente al controlador *Ethernet* de Punto de Acceso. Ésta dirección no puede ser modificada.

- *Configuration Server Protocol* — Protocolo de configuración del servidor: Configure éste parámetro para asociar el método de la red para la asignación de la dirección del IP. Realice el *Click* en el enlace de *Configuration Server* para ir a la página de *Boot Server Setup*, la cual contiene la configuración detallada para poner a trabajar el Punto de Acceso con los servidores de BOOTP o DHCP para realizar la asignación automática de las direcciones IP.

Las posibles opciones de configuración para este parámetro son:

- a) *None* — Ninguna: Si la red no cuenta con un sistema automático de asignación de direcciones.
  - b) *BOOTP* — Protocolo de *Bootstrap*: Con esta configuración la dirección IP son codificados basados en las direcciones MAC.
  - c) *DHCP* — Protocolo de configuración dinámica de invitados: Si es activado este parámetro, se le presta direcciones IP a las estaciones que ingresen a la red por un periodo determinado de tiempo.
- *Default IP Address* — Dirección IP por defecto: Utilice este parámetro para cambiar la dirección IP del AP. Si no se tiene habilitado el DHCP o BOOTP en la red, la dirección IP que se especifica en este campo es la dirección IP del Punto de Acceso. Si se encuentra habilitado el DHCP o BOOTP, este campo provee la dirección IP en caso que ningún servidor con dirección IP responda a la dirección para el AP.
  - *Default IP Subnet Mask* — Submáscara de red por defecto: Ingrese la máscara de subred para que el IP pueda ser reconocido en la LAN. Si no se encuentra habilitado el DHCP o BOOTP, este campo corresponde a la máscara de subred. Si DHCP o BOOTP está habilitado, este campo provee la máscara de subred solamente si no existe ningún que reponda a la petición del AP.

- *Default Gateway* — Compuerta por defecto: Para especificar que no existe compuerta por defecto, ingrese 255.55.255.255.
- *Radio Service Set ID (SSID)* — Fijación de servicios de radio: El SSID es un identificador único que permite asociar al Cliente con el AP o una VLAN. Pueden ser configurados cerca de 16 SSID's en un AP.
- *Role in Radio Network* — Función en la red de radio: Aquí se selecciona la función que se desea asignar al AP en la red. Existen las siguientes opciones:
  - *Root Access Point*— AP como Principal: Utilice éste parámetro si el AP se encuentra conectada a la red LAN alamburada.
  - *Repeater Access Point* — AP como Repetidor: Funciona como un AP que transfiere datos entre un Cliente y otro AP, es decir, como un repetidor. Se configura cuando no se está conectado directamente a la red alamburada.
  - *Site Survey Client* — Cliente de Estudio del Sitio: Dispositivo que depende de un AP para su conexión a la red. Tenga en cuenta que si está activo, los Clientes no están permitidos para conectarse.
- *Radio Network Optimization (Optimize Radio Network For)* — Optimización de la red de radio: Se utiliza para personalizar la configuración de la interfaz de radio.
  - *Throughput*: Maximiza el volumen de datos manejados por el AP pero reduce el alcance de cobertura del AP.
  - *Range* — Alcance: Maximiza el alcance de cobertura del AP pero reduce el *throughput*.
  - *Custom* — Personalizado: El AP utiliza las configuraciones realizadas en la página de *AP Radio Hardware*.

- *Radio Network Compatibility (Ensure Compatibility With)* — Compatibilidad con la red de radio (Asegurar compatibilidad con): Este parámetro se utiliza para configurar automáticamente un AP para que sea compatible con otros dispositivos inalámbricos de la red.
  - *2Mb/sec clients*: Selecciona este parámetro si la red contiene dispositivos que operen a un máximo de velocidad de Mbps.
  - *Non-Aironet 802.11*: Seleccione esta configuración si existen dispositivos que no pertenezcan a la familia de Aironet.
  
- *Security Setup Link* — Enlace de configuración de seguridad: Este enlace te lleva a la página de *Security Setup*, en la cual se puede configurar algunos parámetros de seguridad del AP.
  
- *SNMP Admin. Community* — Comunidad de administración SNMP: Se debe ingresar el nombre de la comunidad en este lugar, para utilizar el Protocolo de Manejo Simplificado de la Red (SNMP). Este nombre aparece en la lista de usuarios autorizados para ver y hacer cambios en el sistema de manejo de los AP's.

## CAPITULO 9: GUIA PARA LA INSTALACION DE AP 1200

### Breve explicación del capítulo

En éste capítulo se hará referencia a la configuración del AP 1200.

Debido a que este presenta opciones de menú similares a las del AP 350, todas aquellas similitudes con el mismo serán **omitidas**. Se desea hacer recalcar aquellas principales ventajas y diferencia que presenta este AP respecto al AP 350. Una de estas diferencias más significativas consiste en que éste modelo presenta 2 módulos de Radio Frecuencia: uno **Interno** (*mini-PCI slot*) configurada por defecto a 2.4 GHz con antena integrada y otro **Externo** (*modified cardbus slot*) configurada por defecto a 5 GHz para uso con antenas externas. Este AP puede operar solamente con **una de las dos a la vez**, es decir, **no** puede ser configurada para utilizar 2 módulos a 2.4 GHz ó 2 módulos a 5 GHz; sin embargo, **si** pueden coexistir sin interferencia los módulos de 2.4 GHz y el de 5 GHz a la vez, ya que éste AP se ideó con el propósito de migrar los equipos funcionando bajo el estándar 802.11b (de 2.4 GHz) al 802.11a (de 5 GHz) el cual permite mayor tasa de transferencia de datos. Estos módulos son configurados separadamente.

### Antes de comenzar

- 1) Asegúrese de tener conectado, al menos una antena al conector PRIMARY del AP. Esto es muy importante.
- 2) Debe realizarse la conexión del cable al puerto de *Ethernet*, para proveer la energía al AP. Para esto vea la **Opción 3** del Diagrama de Conexión del *Power Injector*, en los Anexos. Nota: No incluya el *Switch* para esta configuración inicial.
- 3) Conecte el cable serie DB-9 hembra a RJ-45, a la respectiva interfaz serie RJ-45 del AP, así como el extremo del cable DB-9 al puerto COM de su computador, para realizar la configuración respectiva. Este cable debe ser un *rollover*. Ver [Figura B.2.3](#) en anexos.
- 4) Ejecute algún *software* de acceso al puerto Serie. En su defecto, utilice el *Hyperterminal*, el cual viene incluido en las versiones más actuales de WINDOWS.

## 9.1 DESCRIPCIÓN DE PARÁMETROS DEL PUNTO DE ACCESO AIRONET 1200

Los subcapítulos 8.1, 8.2, 8.3 del capítulo 8, correspondientes al ingreso al AP350 son los mismos para éste AP. [ir a capítulo 8.1](#); [ir a capítulo 8.2](#), [ir a capítulo 8.3](#).

Presenta los mismos submenús que el AP 350: [Home](#), [Map](#), [Network](#), [Association](#), [Setup](#), [Logs](#) y [Help](#).

El submenú de **Home** presenta las mismas opciones que el correspondiente al AP 350 ([Ver Figura 8.9](#)).

El submenú de **Map** es igual al del AP 350 y es utilizado para el mismo propósito que el correspondiente al AP 350 ([Ver Figura 8.10](#)).

El submenú de **Network** presenta las mismas estadísticas de recepción y transmisión que el AP 350, con la salvedad que especifica la interfaz de radiofrecuencia como *AP radio internal*.

## Prueba1 Network Ports

CISCO SYSTEMS



Network Diagnostics VLAN Service Sets

[Home](#) [Map](#) [Network](#) [Associations](#) [Setup](#) [Logs](#) [Help](#)

Uptime: 01:39:54

Name	Ethernet*	AP Radio: Internal
Status	No Link	Up
Max. Mb/s	0.0	11.0
IP Addr.	172.20.20.3	172.20.20.3
MAC Addr.	000c30cc041d	000c30cc041d
Radio SSID		ab3
<i>Receive</i>		
unicast pkts.	0	18
multicast pkts.	0	0
total bytes	0	1980
errors	0	0
discards	0	0
forwardable pkts.	682	597
filtered pkts.	0	0
<i>Transmit</i>		
unicast pkts.	0	19
multicast pkts.	0	2
total bytes	0	11809
errors	99	0
discards	0	0
forwarded pkts.	99	1757

Figura 9.1 Página principal de Network Ports para AP 1200

El menú de **Association** presenta la misma información que en el AP 350 ([Ver Figura 8.12](#)).

El menú de **Setup** del AP 1200, al igual que el del AP 350, permiten realizar los cambios deseados en el funcionamiento del AP; sin embargo presenta la diferencia de ofrecer una opción adicional en el submenú de *Services: Proxy Mobile IP*, la cual será explicada más adelante.



## Prueba1 Setup

Cisco 1200 Series AP 12.01T1



<a href="#">Home</a>	<a href="#">Map</a>	<a href="#">Network</a>	<a href="#">Associations</a>	<a href="#">Setup</a>	<a href="#">Logs</a>	<a href="#">Help</a>	Uptime: 02:07:10
<b>Express Setup</b>							
<b>Associations</b>							
<a href="#">Display Defaults</a>		<a href="#">Port Assignments</a>	<a href="#">Advanced</a>				
<a href="#">Address Filters</a>	<a href="#">Protocol Filters</a>	<a href="#">VLAN</a>	<a href="#">Service Sets</a>				
<b>Event Log</b>							
<a href="#">Display Defaults</a>		<a href="#">Event Handling</a>	<a href="#">Notifications</a>				
<b>Services</b>							
<a href="#">Console/Telnet</a>	<a href="#">Boot Server</a>	<a href="#">Routing</a>	<a href="#">Name Server</a>				
<a href="#">Time Server</a>	<a href="#">FTP</a>	<a href="#">Web Server</a>	<a href="#">SNMP</a>				
<a href="#">Cisco Services</a>	<a href="#">Security</a>	<a href="#">Accounting</a>	<a href="#">Proxy Mobile IP</a>				
<b>Network Ports</b>							
<i>Diagnostics</i>							
<b>Ethernet</b>	<a href="#">Identification</a>	<a href="#">Hardware</a>	<a href="#">Filters</a>	<a href="#">Advanced</a>			
<b>AP Radio: Internal</b>	<a href="#">Identification</a>	<a href="#">Hardware</a>	<a href="#">Filters</a>	<a href="#">Advanced</a>			

Figura 9.2 Página principal de *SETUP* para AP 1200

El menú de **Logs** presenta la misma información y parámetros que en el AP 350 ([Ver Figura 8.14](#)).

El menú de **Help** corresponde a la misma pantalla que se despliega en la ([Figura 8.15](#)), en el apartado de Configuración de AP 350.

Enfocándose ahora en el menú de *Setup* del AP 1200, se puede decir que presentan las mismas opciones que el AP 350 más una adicional: *Proxy Mobile IP* ([Ver Figura 9.3](#)).

Se presentan los mismos 6 submenús que en el AP 350:

## **Associations:**

Esta Tabla de Asociación del sistema presenta todos los posibles dispositivos inalámbricos conectados a la LAN alambrada.

En general, todos los submenús presentan las mismas opciones ofrecidas por el AP 350. Para ver la información correspondiente a cada parámetro vaya al apartado de [Associations](#) especificado en el Capítulo 8, o bien haga *click* en el enlace correspondiente a cada parámetro que se especifica a continuación:

- 1) **Display Defaults—Despliegue de parámetros por defecto:** Ver parámetros especificados en [Figura 8.16](#).
  
- 2) **Address Filters — Filtros de Direcciones:** Ver parámetros especificados en [Figura 8.17](#).
  
- 3) **Protocol Filters — Filtros para protocolos:** Ver parámetros especificados en [Figura 8.18](#).
  
- 4) **Port Assignments — Asignación de Puertos:** Ver parámetros especificados en [Figura 8.19](#).
  
- 5) **VLAN — Redes Virtuales:** Ver parámetros especificados en [Figura 8.20](#).
  
- 6) **Advanced — Avanzadas:** Ver parámetros especificados en [Figura 8.21](#).
  
- 7) **Service Sets — Fijación de Servicios:** Ver parámetros especificados en [Figura 8.22](#).

## **Event Log**

En general, todos los submenús presentan las mismas opciones ofrecidas por el AP 350. Para ver la información correspondiente a cada parámetro vaya al apartado de [Event Log](#) especificado en el Capítulo 8, o bien haga *click* en el enlace correspondiente a cada parámetro que se especifica a continuación:

1) **Display Defaults — Despliegue de parámetros por defecto:** Ver parámetros especificados en [Figura 8.23](#). También puede referirse a la [Tabla 8.1](#); la cual explica la información de severidad de los eventos.

2) **Event Handling — Manipulador de Eventos:** Ver parámetros especificados en [Figura 8.24](#).

3) **Notifications — Notificaciones:** Ver parámetros especificados en [Figura 8.25](#).

## **Services**

En general, todos los submenús presentan las mismas opciones ofrecidas por el AP 350. Se agrega un submenú denominado *Proxy Mobile IP*. Para ver la información correspondiente a cada parámetro vaya al apartado de [Services](#) especificado en el Capítulo 8, o bien haga *click* en el enlace correspondiente a cada parámetro que se especifica a continuación:

1) **Console/Telnet:** Ver parámetros especificados en [Figura 8.26](#).

2) **Time Server — Servidor de reloj:** Ver parámetros especificados en [Figura 8.27](#).

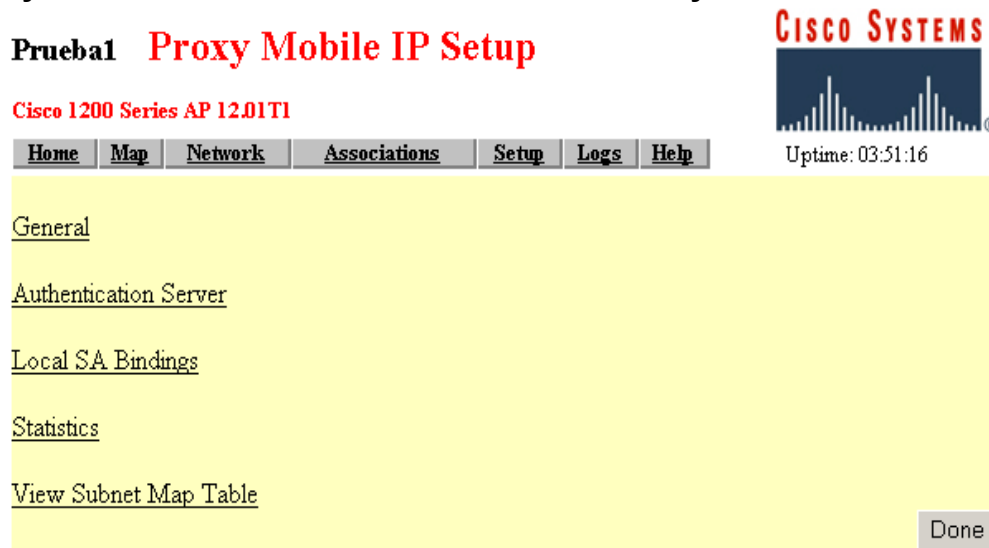
**3) Cisco Services — Servicios de Cisco:** Ver parámetros especificados en [Figura 8.28](#). Este presenta los submenús de:

- a) *Manage Installation Keys*—Llaves Administrativas de Instalación: Presenta los mismos parámetros que el AP 350 ([Ver Figura 8.29](#)).
- b) *Manage System Configuration* — Administrar Sistema de Configuración: Presenta los mismos parámetros que el AP 350 ([Ver Figura 8.30](#)).
- c) *Distribute Configuration to other Cisco Devices* — Distribuir la configuración a otros dispositivos Cisco: Presenta los mismos parámetros que el AP 350 ([Ver Figura 8.31](#)).
- d) *Distribute Firmware to other Cisco Devices* — Distribuir sistema operativo a otros dispositivos Cisco: Presenta los mismos parámetros que el AP 350 ([Ver Figura 8.32](#)).
- e) *Hot Standby Management* — Administración del “*Hot Standby*”: Presenta los mismos parámetros que el AP 350 ([Ver Figura 8.33](#)).
- f) *Cisco Discovery Protocol (CDP)* — Protocolo de descubrimiento Cisco: Presenta los mismos parámetros que el AP 350 ([Ver Figura 8.34](#)).

**4) Boot Server — Servidor de arranque:** Ver parámetros especificados en [Figura 8.35](#).

**5) FTP — Protocolo de Transmisión de Archivos:** Ver parámetros especificados en [Figura 8.36](#).

- 6) **Security** — **Seguridad**: Ver parámetros especificados en [Figura 8.37](#).
- 7) **Routing** — **Enrutamiento**: Ver parámetros especificados en [Figura 8.38](#).
- 8) **Web Server** — **Servidor Web**: Ver parámetros especificados en [Figura 8.39](#).
- 9) **Accounting** — **Contabilidad**: Ver parámetros especificados en [Figura 8.40](#).
- 10) **Name Server** — **Servidor de Nombres**: Ver parámetros especificados en [Figura 8.41](#).
- 11) **SNMP** — **Protocolo de manejo simple de la red**: Ver parámetros especificados en [Figura 8.42](#).
- 12) **Proxy Mobile IP** — **Dirección IP mobile del Proxy**:



**Figura 9.3** Página principal de *Proxy Mobile IP*

a) **General:** Esta página habilita el *proxy Mobile IP* en el AP e identifica las direcciones IP de los AP's autoritarios en la red inalámbrica.

**Prueba1 Proxy Mobile IP General**

Cisco 1200 Series AP 12.01T1

Home Map Network Associations Setup Logs Help

Uptime: 03:52:28

Enable Proxy Mobile IP:  yes  no

Authoritative AP 1:

Authoritative AP 2:

Authoritative AP 3:

Apply OK Cancel Restore Defaults

**Figura 9.4** Página de *Proxy Mobile IP General*

- **Enable Proxy Mobile IP**—Habilitar el Proxy Mobile IP: Este parámetro habilita la característica de *Proxy Mobile IP* en el AP. El parámetro por defecto es **NO**.  
Nota: Este parámetro también debe estar habilitado para el SSID que se intenta utilizar para dar soporte a esta característica. De otra manera, esta característica no funcionará.
- **Authoritative AP 1-3:** Estos parámetros identifican la dirección IP para más de 3 AP Autoritarios (AAP's) en la red inalámbrica. Al menos un AAP es requerido para habilitar el *proxy Mobile IP* de la red inalámbrica. La letra *n* representa el número del AP Autoritario. Este último es el dispositivo que se registra con el *Home Agent*. Una vez registrado con éste último, el AAP habilita un mapa de subred para los otros AP's. Este mapa de subred enlaza a los AP con el *Home Agent* para registrar un Cliente Móvil basado en la dirección IP del Cliente. Por ejemplo: si un Cliente Móvil aparece con la dirección IP perteneciente a la subred "30", en la subred "20", el AP debe registrarse con el *Home Agent* que da servicio a los Clientes Móviles de la subred "30".

- *View Subnet Map Tab*—Etiqueta para observar el Mapa de Subred: Haga *click* para ir a la pantalla con la tabla de Mapa de Subred, esto para poder ver la lista de direcciones IP de *Home Agents* y sus máscaras de red asociadas.

**b) Authentication Server—Servidor de Autenticación:** Esta página permite ingresar los parámetros de autenticación. El servidor de *RADIUS* de la red utiliza el *EAP* para proveer servicios de autenticación para los dispositivos de Clientes inalámbricos.

Pruebal **Authenticator Configuration**

Cisco 1200 Series AP 12.01T1

Map Help Uptime: 03:53:48

802.1X Protocol Version (for EAP Authentication): 802.1x-2001

Primary Server Reattempt Period (Min.): 0

Server Name/IP	Server Type	Port	Shared Secret	Retran Int (sec)	Max Retran
	RADIUS	1812	XXXXXXXXXXXXXXXX	5	3
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication <input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication					
	RADIUS	1812	XXXXXXXXXXXXXXXX	5	3
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication <input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication					
	RADIUS	1812	XXXXXXXXXXXXXXXX	5	3
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication <input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication					
	RADIUS	1812	XXXXXXXXXXXXXXXX	5	3
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication <input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication					

Note: For each authentication function, the most recently used server is shown in green text.

Apply OK Cancel Restore Defaults

**Figura 9.5** Página de *Authenticator Configuration*

- *802.1X Protocol Versión (For EAP Authentication)*— Versión de Protocolo 802.1X (para autenticación del *EAP*): Del menú, debe seleccionar el protocolo 802.1X a utilizar por la interfaz de radiofrecuencia del AP. Tome en cuenta que el *EAP* opera solamente cuando el *firmware* en el Cliente posee el mismo protocolo de administración que el AP.
  - *Draft 7*: Ninguna versión de *firmware* para radiofrecuencia con éste protocolo activo posee la capacidad de soportar el *LEAP*.

- *Draft 8*: Debe seleccionar esta opción si el Cliente posee activo el *LEAP* para la asociación con el AP que utilice las siguientes versiones de *firmware* para radio: 4.13, 4.16 ó 4.23.
  - *Draft 10*: Debe seleccionar esta opción si el Cliente que se asocia con el AP utiliza autenticación por Microsoft WindowsXP ó si el Cliente posee activo el *LEAP* para asociarse con el AP cuya versión de *firmware* para radio sea igual ó mayor a 4.25.
- *Primary Server Reattempt Period* —Periodo Primario de Reintento del Servidor: Especifique cuanto tiempo debe pasar antes de verificar que el servidor primario no fue accesado inicialmente.
  - *Server Name/IP*—Dirección IP ó nombre del servidor: Ingrese el nombre ó la dirección IP del servidor de *RADIUS*.
  - *Server Type*—Tipo de Servidor: Nombre del Servidor de *RADIUS* que es utilizado.
  - *Port*—Puerto: Ingrese el número de puerto que utilizará para autenticación el Servidor de *RADIUS*. El valor por defecto es 1812, el cual es utilizado por varios servidores de *RADIUS*; el 1645 es el puerto para los servidores de *RADIUS* Cisco (también conocido como *Access Control Server* ó ACS). Para este último se debe revisar la documentación para encontrar el parámetro correcto para el puerto.
  - *Shared Secret*—Secreto Compartido: Ingrese el secreto compartido utilizado por el servidor de *RADIUS*.
  - *Retran Int (sec)* — Intervalo de Retransmisión en segundos: Ingrese la cantidad de segundos que el dispositivo debe esperar antes de declarar un fallo por autenticación.



- *Max Retran* — Retransmisión Máxima: Ingrese el número máximo de intentos que el AP debe esperar antes de darse por vencido al contactar un servidor.
- *User server for*— Servidor de Usuarios para: En las cajas de verificación escoja el servidor para el tipo de autenticación a utilizar: *EAP*, por dirección MAC, Usuario ó MIP.

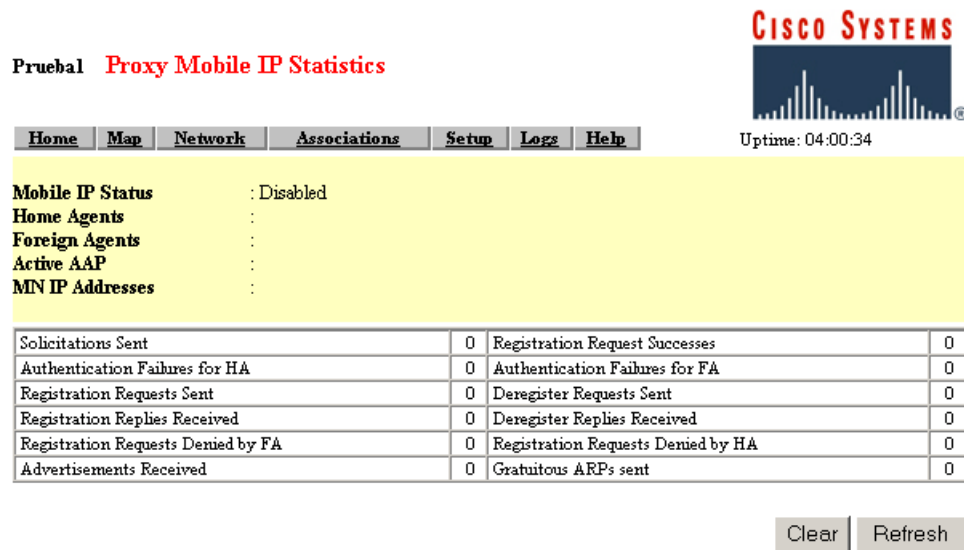
c) **Local SA Bindings**—**Local** : Utilice esta página para identificar un Cliente válido que esté disponible para establecer contacto con un agente extranjero en otro segmento de red.

Figura 9.6 Página Local SA Bindings

- *IP Address Range-Start* — Rango de dirección IP (inicio): Este campo contiene el inicio del rango de direcciones IP en el cual el Cliente debe residir para que sea válido.

- *IP Address Range-End* — Rango de dirección IP (final): Este campo contiene el final del rango de direcciones IP en el cual el Cliente debe residir para que sea válido.
- *Grup SPI* — Grupo SPI: Este campo especifica el índice de parámetros de seguridad del rango de direcciones IP ingresadas en los campos de los parámetros anteriores. El SPI es un número de 32 bits (8 dígitos hexagesimales) asignados al iniciador de peticiones de asociaciones de seguridad del punto final de IPsec receptor. En el paquete recibido, la dirección de destino, protocolo y el PI son utilizados para determinar la seguridad en la asociación. La seguridad en la asociación permite la autenticación del nodo ó la descricpción del según las políticas de seguridad configuradas para la asociación de seguridad.
- *Group Key* — Grupo de Llaves: Este campo contiene la llave de autenticación, similar a la llave WEP, que el grupo especificado en la seguridad de asociación utiliza para acceder el Agente Extranjero. Este grupo de llaves es de una longitud de 128 bits (32 dígitos hexagesimales).
- *Existing SA Bindings* — Envolturas existentes SA: Este campo muestra las envolturas de seguridad configuradas previamente. La información contiene el inicio y fin del rango de direcciones IP y su grupo asociado SPI y llaves de parámetros.

d) **Statistics—Estadísticas:** Esta característica no es soportada todavía.



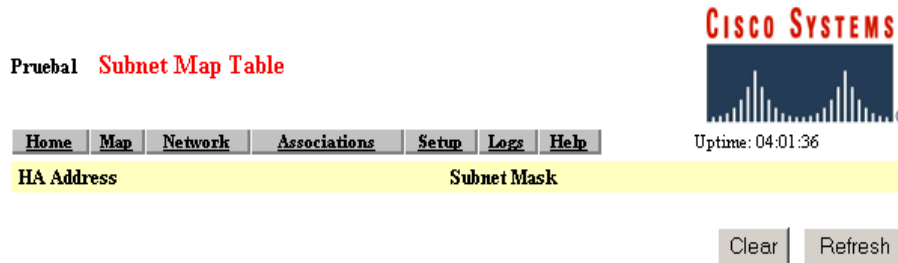
**Figura 9.7** Página de Estadísticas del *Proxy Mobile IP*

- *Mobile IP Status*— Estado de los IP Móviles: Este campo de información indica si el *proxy Mobile IP* está habilitado ó deshabilitado.
- *Home Agents*: Este campo presenta la información acerca de los *Home Agents* que el AP descubre en su propia subred. Si se descubre un *Home Agent*, su dirección IP es desplegada. Si no existen Agentes descubiertos, se despliega *Not Found*.
- *Foreign Agents* — Agentes Extranjeros: Este campo presenta la información acerca de los Agentes Extranjeros que el AP descubre en su propia subred. Si se descubre un Agente Extranjero, su dirección IP es desplegada. Si no existen Agentes descubiertos, se despliega *Not Found*.
- *Active AAP* — AAP Activo: Este campo muestra la dirección IP del AP autoritario activo.

- *MN IP Addresses*— Direcciones IP MN: Este campo muestra las direcciones IP de los nodos móviles, los cuales son Clientes que el AP está dando servicio.
- *Solicitations Sent*— Solicitudes Enviadas: Número de mensajes para solicitudes de los Agentes que el AP ha enviado. Si el AP no escucha avisos, este envía un mensaje de petición de conocimiento hacia cualquier agente. La solicitud fuerza a cualquier agente del enlace a enviar algún aviso.
- *Authentication Failures for HA* — Fallos de Autenticación para HA: Número de veces que el *Home Agent* rechaza las peticiones de registro, debido a los fallos de autenticación, tales como SPI inválido ó llave de grupo. Cuando un nodo móvil se mueve a una red distinta, el AP registra el nodo móvil a su *Home Agent*. Esta estadística indica que el número de fallos por registro causado por el fallo de un *Home Agent* ó Agente Extranjero para validarse entre sí ó al nodo móvil.
- *Registration Request Sent* — Petición de Registro Enviada: Cantidad de peticiones de registro enviadas por el AP hacia el nodo móvil.
- *Registration Request Denied by FA*—Petición de Registro Denegada por el FA: Cantidad de veces que un Agente Extranjero rechazado realiza una petición de registro. Cuando el nodo móvil se mueve hacia la red extranjera, el AP registra el nodo móvil como su *Home Agent*. Estas estadísticas indican el número de peticiones que fueron denegadas al Agente Extranjero. Las razones para denegar, incluyen: *Home Agent unreachable* (inalcanzable), *no resource found* (no se encontraron recursos), entre otras razones.
- *Advertisements Received* — Advertencias Recibidas: Número de advertencias IRDP recibidas por los agentes.

- *Registration Request Successes*— Peticiones de Registro Exitosas: Cantidad de veces que las peticiones de registro fueron exitosas.
- *Authentication Failure for FA* — Fallos de Autenticación por EA: Cantidad de veces que un Agente Extranjero rechazado hace peticiones de registro, debido a que el nodo móvil ó la autenticación del *Home Agent* falla.
- *Deregister Request Sent* — Peticiones no registradas enviadas: Cantidad de veces que el AP envia peticiones de salida de registro al *Home Agent*.
- *Deregister Replies Received* — No registro de respuestas recibidas: El número de veces que el AP recibió contestaciones de no registro del *Home Client*.
- *Registration Request Denied by HA* — Peticiones de registro denegadas por HA: Cantidad de veces que el *Home Agent* rechazado realiza peticiones de registro.
- *Gratuitous ARPs Sent* — ARP's Enviados: Cantidad de veces que se enviaron mensajes de ARP. Los ARP's son enviados por el *Home Agent* en nombre del nodo móvil para actualizar la Caché del ARP en los invitados locales. Cuando el nodo móvil retorna a su red principal, el *Home AP* envia el nombre del nodo móvil para verificar la dirección MAC y las direcciones IP. Además, el *Home Agent* también utiliza los ARP's para el nodo móvil en caso que existan otros nodos que no puedan escuchar al nodo móvil.

e) **View Subnet Map Table**—Ver Tabla de Mapeo de la Subred:



**Figura 9.8** Página *Subnet Map Table*

- *HA Address*—Direcciones HA: Direcciones IP de los *Home Agents*.
- *Subnet Mask* — Máscara de Subred: Direcciones de la máscara de subred para el correspondiente *Home Agents*.

### **Network Ports**

En general, todos los submenús presentan las mismas opciones ofrecidas por el AP 350. Para ver la información correspondiente a cada parámetro vaya al apartado de [Network Ports](#) especificado en el Capítulo 8, o bien haga *click* en el enlace correspondiente a cada parámetro que se especifica a continuación:

1) **ETHERNET**: Ver parámetros especificados en [Figura 8.43](#).

a) **Identification** — **Identificación**: Ver parámetros especificados en [Figura 8.44](#).

b) **Hardware**: Ver parámetros especificados en [Figura 8.45](#).

c) **Filters** — **Filtros**: Ver parámetros especificados en [Figura 8.46](#).

d) **Advance** — **Avanzado**: Ver parámetros especificados en [Figura 8.47](#).

2) **AP RADIO** — **PUERTO DE RADIO**: Ver parámetros especificados en [Figura 8.48](#).

a) **Identification** — **Identificación**: Ver parámetros especificados en [Figura 8.49](#).

b) **Hardware**: Ver parámetros especificados en [Figura 8.50](#).

c) **Filters** — **Filtros**: Ver parámetros especificados en [Figura 8.51](#).

d) **Advance** — **Avanzado**: Ver parámetros especificados en [Figura 8.52](#).

### **Diagnostics**

En general, todos los submenús presentan las mismas opciones ofrecidas por el AP 350. Para ver la información correspondiente a cada parámetro vaya al apartado de [Diagnostics](#) especificado en el Capítulo 8.

a) **Radio Diagnostics Tests** — Prueba de Diagnóstico de Radio: Debe hacer *click* en este parámetro para acceder la página de diagnósticos para radiofrecuencia y poder realizar una prueba de portadora.

Esta prueba de portadora permite determinar cuáles frecuencias de radio contienen la mayor actividad, así como el ruido asociado que puede interferir con las señales de radio, desde y hacia el AP.

Utilice este diagnóstico de la portadora para determinar cual es la mejor frecuencia para utilizar el AP.

Cuando realice esta prueba, debe estar seguro que los dispositivos inalámbricos de la red deben estar dentro del alcance de operación del AP.

**Nota:** El AP desconecta toda asociación con los dispositivos de red inalámbrica durante esta prueba de portadora.

b) *VLAN Summary Status* — Resumen de estados de VLAN's: Los siguientes enlaces están disponibles en esta página:

b.1) *VLAN Detailed Setup* — Configuración detallada de VLAN: Este enlace lleva a la página de *VLAN Setup*, desde la cual usted puede agregar, eliminar o editar la configuración de las VLAN's.

c) *Service Sets* — Fijación de servicios: Este enlace lleva a la página de *AP Radio Service Set Summary Status*. Aquí se encuentran los siguientes enlaces:

c.1) *Service Set Detailed Setup* — Configuración detallada de la fijación de servicios: Este enlace lleva a la página de *AP Radio Service Set*, desde la cual se puede crear, remover o editar la configuración del SSID.

### **Express Setup**

Este apartado presenta las mismas opciones ofrecidas por el AP 350, con la ligera diferencia que la interfaz de radiofrecuencia se especifica como *Internal*. Para ver la información correspondiente a cada parámetro vaya al apartado de [Express Setup](#) especificado en el Capítulo 8.



## CAPITULO 10: CISCOWORKS FOR WIRELESS (WLSE)

### Breve explicación del capítulo

En este capítulo se hará un vistazo rápido al *CiscoWorks for Wireless* ó WLSE (*Wireless LAN Solution Engine*). Este *hardware/software* es en la actualidad el #1 en cuanto a la administración de redes inalámbricas Cisco, esto debido a la facilidad que ofrece para su operación así como por la versatilidad y capacidad en el manejo de equipos, permitiendo el manejo de hasta 2500 AP's. Además ofrece una capacidad para elaborar reportes, ejecutar *Jobs* calendarizados, actualizar *firmware*, entre muchas otras funciones.

### 10.1. WLSE (WIRELESS LAN SOLUTION ENGINE)

El WLSE es parte de la armazón de las redes inalámbricas estructuradas para desplegar, mantener y monitorear una segura y totalmente integrada infraestructura de LAN's inalámbricas a nivel empresarial. Esta armazón trae consigo inteligencia en la administración integrada del *CiscoWorks* con los AP's y *Bridges* de la serie *Aironet*, con el *software* del IOS, con la estructura de seguridad de las redes inalámbricas Cisco con los adaptadores de red y con el resto de los dispositivos de otros fabricantes que son compatibles con Cisco. Esto permite extender una *WLAN* a un mismo nivel de seguridad, escalabilidad y confiabilidad que los Clientes deben esperar de una *LAN* cableada.

## 10.2. VISIÓN GLOBAL DEL SISTEMA

El WLSE es una solución centralizada para administrar la infraestructura completa de la red *LAN* inalámbrica. Esta herramienta da al administrador la visibilidad necesaria dentro de la *WLAN* sin necesidad de sensores u otros dispositivos.

Algunas características como la configuración y la actualización del IOS en masa, reducen el tiempo y los recursos necesarios para la administración y reparación de averías cuando cientos de AP's están envueltos.

El WLSE monitorea la disponibilidad y el rendimiento de los AP's y *Bridges*, enviando notificaciones cuando las condiciones se presenten. La reparación de averías y la capacidad de herramientas de planeación incluyen grupos de utilización y reportes de asociaciones de los Clientes, mientras se despliega y opera de manera fácil con mecanismos para la configuración y actualización de *firmware* de los AP's y *Bridges* en grupos.

Si se desea, también el administrador ó encargado pueden definir configuraciones por defecto, que tomen su efecto cuando un nuevo AP se conecte a la red. Este equipo además, mejora la seguridad de la *WLAN* asegurando que todas las políticas de seguridad sean apropiadamente configuradas a través de todos los AP's y *Bridges*, y asegurando que el servicio de autenticación se esté desarrollando apropiadamente mediante el monitoreo de la respuesta de tiempo de los servidores de autenticación *EAP*.

Una segura interfaz basada en HTML prevee acceso a cualquier parte. La capa superior de la administración del red (NMS) y las operaciones de soporte de integración del sistema (OSS) es realizada mediante mensajes de *Syslog*, *SNMP traps*, *emails*, notificaciones y una interfaz SOAP/XML (*Simple Object Access Protocol/Extensible Markup Language*).

### 10.3. CARACTERÍSTICAS DE APLICACIÓN QUE SIMPLIFICAN LA OPERACIÓN Y EL DESPLIEGUE

El WLSE simplifica la operación de la *WLAN* al automatizar tareas repetitivas que consumen mucho tiempo. Estas características son:

- Agrupación Dinámica: Los grupos hacen que la red sea más fácil de entender y operar. Los dispositivos deben organizarse en grupos jerárquicos definidos por el administrador. Por defecto el AP y los *Bridges* son agrupados por la localización del SSID, tipo de dispositivo, versión del *firmware* y subred. Los grupos por nivel permiten diferentes perfiles de aplicación de políticas y encuesta para distintos grupos de dispositivos.
- Configuración en masa: Configurar un grupo con muchos dispositivos requiere no más que el esfuerzo de configurar un solo dispositivo. Las tareas de configuración pueden ser calendarizadas o ejecutadas por demanda. La configuración de parámetros puede ser verificada antes de ser aplicadas.
- Archivo de configuración: Este archivo guarda las últimas 4 versiones de configuración de cada dispositivo, permitiendo su utilización a futuro. Una búsqueda de configuraciones puede realizarse mediante el nombre ó dirección IP del AP.
- Auto-Configuración: Si se desea, los nuevos AP's pueden recibir automáticamente configuraciones definidas por el Cliente, las configuraciones por defecto se realizan mediante DHCP a través de una característica denominada "Auto-Config". Esta última permite al administrador mantener el control del ambiente. Configuraciones específicas son descargadas basados en el tipo de dispositivo y la subred para direcciones MAC autorizadas.

- Configuración de VLAN: El WLSE configura y monitorea las VLAN's especificadas en los AP's, permitiendo a los Clientes diferenciar las políticas y servicios, tales como seguridad y QoS para diferentes usuarios. El soporte de acceso público es posible a través del soporte de múltiples VLAN's sin encriptar.
- Actualización Centralizada del Firmware: El *firmware* de AP's y *Bridges* Cisco puede ser actualizado en masa. Este puede ser asignado a un específico dispositivo o grupo. Las tareas pueden ser calendarizadas o ejecutadas por demanda. Las imágenes de *software* pueden ser importadas desde el sitio Web de Cisco y el WLSE es utilizado como depósito central de las actualizaciones del *firmware*. Esta tarea puede realizarse utilizando tanto el protocolo HTTP ó SNMP. Opcionalmente el WLSE puede actualizar sitios remotos directamente o trabajar opcionalmente con un servidor TFTP.
- Herramienta de conversion Aironet Cisco para el software del IOS Cisco: Utilizando AP's de la serie 1200 que utilicen el sistema operativo **VxWorks**, se puede actualizar en masa el *software* del IOS. Como parte del proceso previo de la actualización, el formato del archivo **VxWorks** es trasladado al formato del *software* del IOS.
- Auto-Descubrimiento: El WLSE automáticamente descubre los AP's, *Bridges* y *Switches* de la serie Aironet, conectados al AP que se encuentra con el parámetro de CDP (*Cisco Discovery Protocol*). Este descubrimiento de la red puede ser calendarizado ó ejecutado por demanda. Si se desea, puede estar limitado por el rango de la subred y la dirección IP. Si el CDP está deshabilitado, una lista de direcciones IP y credenciales pueden ser importadas desde un archivo ó desde el *CiscoWorks* RME (*Resource Manager Essentials*). La sincronización del RME puede ser automática.

El WLSE recolecta estadísticas e información de administración para cada *AP* y *Bridge* Cisco en su inventario. El WLSE es también un dispositivo administrable con el CDP y además soporta el Cisco MIB-II.

- Sistema de Integración de Administración de la Red (NMS): Integración con la administración del sistema de red de tercer nivel (NMS) es proveído vía mensajes *Syslog*, *Traps SNMP* y la interfaz (SOAP/XML) *Simple Object Access Protocol/Extensible Markup Language*. La interfaz permite que los datos en los reportes del WLSE sean recuperados sin tener que lanzar esos reportes con la integración del *CiscoWorks*.
- Integración del *CiscoWorks*: Como parte de la familia de administración de la red *CiscoWorks*, este integra el LMS (*LAN Management Solution*) y las otras aplicaciones de *CiscoWorks* para maximizar la eficiencia ó convergencia de redes cableadas/inalámbricas. Una lista de direcciones IP y credenciales, por ejemplo, pueden ser importadas ó exportadas entre el WLSE y el RME, para una aplicación que provea un amplio manejo de la red para un amplio rango de dispositivos Cisco. Si se desea, el descubrimiento de dispositivos puede ser apagado en el WLSE y la sincronización del RME encendida en automático. El WLSE utiliza los mismos roles de usuarios por defecto que RME, pero permite la personalización.

El WLSE puede ser lanzado desde el escritorio de CMC (*Cisco Management Connection*) y viceversa ó lanzado desde el mapa de la topología del administrador de campus.

#### 10.4. MEJORAS A NIVEL DE SEGURIDAD

- Políticas de monitores de la seguridad: EL WLSE genera alertas para la seguridad de las desconfiguraciones en AP's y *Bridges* Cisco, reduciendo así las potencialidades de vulnerabilidades en seguridad y manteniendo predefinidos los parámetros del grupo de seguridad inalámbrica. Por ejemplo, cuando el WLSE encuentra un AP ó *Bridge* sin SSID en una lista de SSID válidos, una notificación de avería puede ser generada. Otros parámetros de seguridad monitoreados, incluyen la verificación que el SSID esté activado, que el WEP esté habilitado, que el *LEAP*, *PEAP* ó *RADIUS* estén habilitados y que el HTTP/*Telnet* esté deshabilitado.
- Interfaz Segura del Usuario: El WLSE posee una interfaz gráfica soportada en la capa SSL; el SSH (*Secure Shell*) es empleado para el máximo rendimiento y disponibilidad del acceso al *Telnet*. El WLSE monitorea de manera eficiente la infraestructura de *WLAN* para la utilización, *averías* y degradación del rendimiento mientras provee un amplio grupo de información apuntando siempre a la fuente del problema. Ambas interfaces del AP y *Bridges* (*Ethernet* y *Radio*) son verificadas.

## 10.5. MAXIMO RENDIMIENTO Y DISPONIBILIDAD

- Límites Personalizados: Los administradores pueden definir las fallas y los límites de rendimiento para monitorear atributos, y configurar acciones específicas y prioridades en las fallas. Una pantalla conteniendo la centralización de averías, conteniendo los detalles acerca de los dispositivos afectados, la severidad de la falla y una completa descripción es proveída. Las alarmas de las averías pueden ser filtradas y desplegadas por prioridad, para facilitar su localización.
- Estado de las averías: El *CiscoWorks* prevee una jerarquía de árbol de todos los AP's y grupos de usuarios. La codificación por color indica el estado de las averías y los iconos de grupo reflejan el estado más severo de sus miembros. Las averías pueden ser filtradas y desplegadas por prioridad para facilitar su observación.
- Notificación de Averías: La notificación de las averías es implementado a través de los mensajes de *Syslogs*, *Traps* SNMP y vía *email*.
- Monitoreo de Switches: Los *Switches* conectados al AP son monitoreados por su disponibilidad y utilización de los puertos, procesador y memoria.  
Un sólo WLSE posee la capacidad de administrar 2500 AP's ó *Bridges*. Redes más grandes son soportadas agregando dominios de administración.
- Respuesta de autenticación: La respuesta en el tiempo de autenticación de servidores, incluyendo el *Cisco Secure ACS (Access Control Servers)*, es monitoreado realizando autenticación de transacciones. El *LEAP*, *PEAP* y los tipos de autenticación genérica de *RADIUS* son soportados.

## 10.6. REPORTES Y PLANEAMIENTO

El WLSE ofrece una variedad de reportes predefinidos para los AP's y *Bridges*. Este incluye resumen de reportes basados en criterios tales como dirección IP, SSID, *firmware* y número de Clientes; mientras los reportes detallados muestran reportes mostrando información acerca de ítemes tales como número de Clientes; mientras que los reportes detallados muestran información acerca de ítemes tales como el estado de los puertos de *Ethernet* y *Radio*, errores, detalles de encriptación. Otros reportes incluyen reportes de autenticación de ACS (servidores, puertos y prioridad del servidor), asociación de los Clientes, entre otros. Todos los reportes están disponibles en ambos niveles del grupo y del AP ó *Bridge*. La utilización de grupos de reportes muestra el ancho de banda y la asociación de los Clientes al AP. Estos reportes son útiles para la capacidad del planeamiento al monitorear cuáles AP's consumen el mayor ancho de banda y poseen el mayor número de Clientes.

Debido a que los Clientes inalámbricos pueden estar en cualquier parte, los paquetes y los reportes de error ayudar con la resolución de problemas. Tanto el reporte actual como el de historia, pueden ser buscados tanto por la dirección MAC del Cliente y por el nombre, mostrando las asociaciones del AP para un determinado Cliente. Tanto los reportes detallados del Cliente (dirección MAC, dirección IP, estado, tipo y AP asociado) y los reportes de estadísticas (Errores, paquetes, fortaleza de la señal y calidad, etc) son proveídos. El administrador puede especificar tanto la adición y eliminación de frecuencias para los datos monitoreados mostrados en los reportes. Estos reportes pueden ser calendarizados y enviados via *email*. Los reportes pueden ser exportados en formatos CSV/XML/PDF y en SOAP/WML.



## **10.7. MODELOS DE ACCESO BASADO EN LA FUNCIÓN**

El WLSE posee un modelo flexible de acceso de usuarios basados en la función asignada. Las características de acceso en el WLSE son predefinidas por el administrador. Por ejemplo, el personal de *Help Desk*, puede limitarse a que solamente pueda ver los reportes y las averías. Los usuarios WLSE pueden validarse mediante varios módulos de autenticación tales como *TACACS+* (*Terminal Access Controller Access Control System Plus*), *RADIUS* (*Remote Dial-In User Service*); y el dominio de Microsoft NT. El WLSE permite encriptación total de 128 bits en las conexiones SSL entre el Cliente Web y las aplicaciones WLSE. Los usuarios autorizados pueden configurar, monitorear y generar reporte para la infraestructura LAN inalámbrica, aún a través de *Firewalls*. En adición al GUI basado en diseño WEB, el IOS de Cisco soporta acceso directo por consola mediante el CLI (*Command Line Interface*), *Telnet* ó *SSH* (*Secure Shell*) al WLSE para realizar la configuración y la resolución de problemas.

## **10.6. RED ESTRUCTURADA INALÁMBRICA DE CISCO.**

El portafolio de Cisco en cuanto a componentes de infraestructura inalámbrica, coloca a las empresas en un estándar de próxima generación y de máximo rendimiento, seguridad, confiabilidad y manejabilidad de las *WLAN*'s. El nuevo modelo estructurado de redes inalámbricas entrega nuevas características de IOS y nuevas capacidades de administración de la red que permiten una simplicidad, seguridad e inteligencia que asegura la convergencia entre las redes cableadas y las inalámbricas.

**Tabla 10.1** AP's y *Bridges* soportados por WLSE

<b>Modelos de AP's y <i>Bridges</i> soportados</b>	<b>Versión de Software</b>
Toda la serie Aironet 1100 de AP's	12.2(4)JA, 12.2(4)JA1, 12.2(8)JA, 12.2(11)JA
AIR-AP1200 y AIR-AP1220 AIR-AP1210 y AIR-AP1230	11.42T, 11.50T, 11.54T, 11.56, 12.02T1 12.2(8)JA, 12.2(11)JA
Toda la serie Aironet 350 de AP's	11.06a, 11.07a, 11.08T1a, 11.10T1a, 11.21, 11.23T, 12.00T, 12.01T1, 12.02T1
Toda la serie Aironet 340 de AP's	11.06a, 11.07a, 11.08T1, 11.10T1, 11.21, 11.23T, 12.00T, 12.01T, 12.02T

## CAPITULO 11: AIRONET CLIENT UTILITY (ACU) VERSION 12.01T

### Breve explicación del capítulo

Este capítulo muestra el procedimiento de ingreso al Cliente de Aironet instalado en una PC. Muestra además una explicación acerca de sus parámetros.

### 11.1. INGRESO AL CLIENTE AIRONET

Para ingresar al ACU debe realizar doble *click* sobre el icono en el Escritorio



Figura 11.1 Icono de Cliente Aironet en el Escritorio

Una vez dentro del ACU, seleccione **Profile Manager** para crear un nuevo Perfil.

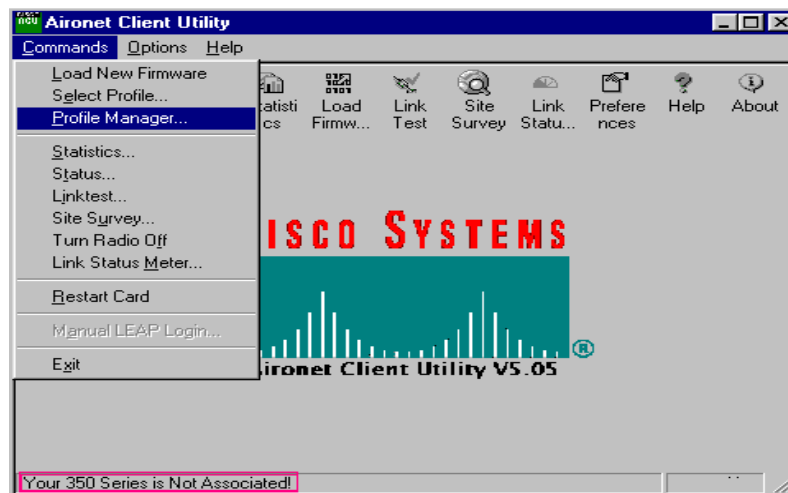
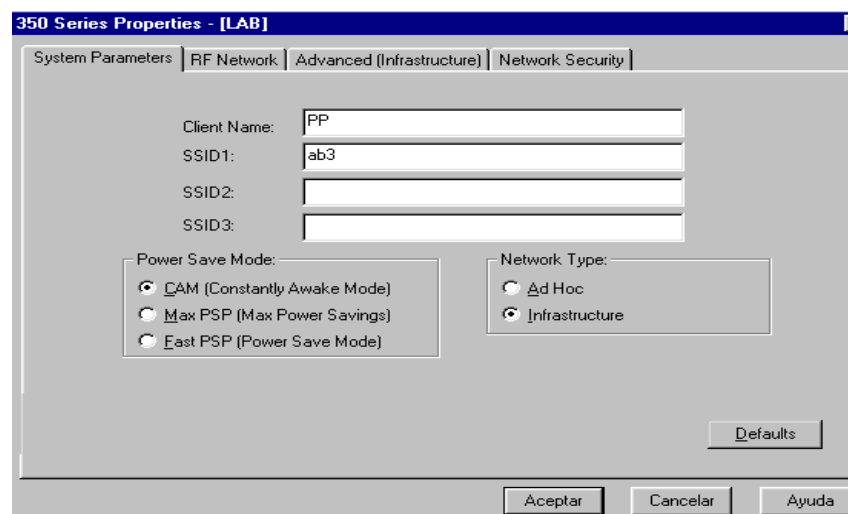


Figura 11.2 Edición del nuevo perfil de usuario

## 11.2. DESCRIPCIÓN DE PARÁMETROS DEL MENÚ DE EDICIÓN DE USUARIOS

Presenta los siguientes submenús: *System Parameter*, *RF Network*, *Advanced (Infrastructure)*, *Network Security*.

### A) *SYSTEM PARAMETER*—PARÁMETROS DEL SISTEMA:



The screenshot shows a window titled "350 Series Properties - [LAB]" with a tabbed interface. The "System Parameters" tab is active. It contains the following fields and options:

- Client Name: Text box containing "PP"
- SSID1: Text box containing "ab3"
- SSID2: Empty text box
- SSID3: Empty text box
- Power Save Mode: Radio buttons for:
  - CAM (Constantly Awake Mode)
  - Max PSP (Max Power Savings)
  - Fast PSP (Power Save Mode)
- Network Type: Radio buttons for:
  - Ad Hoc
  - Infrastructure
- Defaults: Button
- Aceptar, Cancelar, Ayuda: Buttons at the bottom

Figura 11.3 Parámetros del sistema .

- **Client Name:** Nombre del la PC ó dispositivo que contiene el Cliente ACU. Permite determinar rápidamente a cual dispositivo está conectado el AP sin necesidad de conocer la dirección MAC. Se permite un nombre menor a 16 caracteres ASCII.
- **SSID1:** Identificador de Servicio que identifica una red inalámbrica específica que desea acceder. Se permite un nombre menor de 32 caracteres ASCII, y es sensible a mayúsculas.  
**Nota:** Si está en blanco, el Cliente puede asociarse a cualquier AP que tenga habilitado el *Allow Broadcast SSID*.

- **SSID2:** SSID opcional que identifica otra red distinta y permite conectarse sin tener que configurar nuevamente el Cliente.

**Nota:** Si un perfil especifica más de un SSID, éste no puede ser incluido en la elección automática de perfil.

- **SSID3:** SSID opcional que identifica otra red distinta y permite conectarse sin tener que configurar nuevamente el Cliente.

**Nota:** Si un perfil especifica más de un SSID, éste no puede ser incluido en la selección automática de perfil.

- **Power Save Mode:** Configura el Cliente para su óptimo consumo de energía. Presenta 3 opciones:

-*CAM (Constantly Awake Mode):* Mantiene el Cliente con energía constante permitiendo el mayor *throughput*.

-*Max PSP (Max Power Savings):* Causa que el AP tenga que retener los mensajes hasta que el Cliente despierte y encuentre al AP para ver sus mensajes. De esta manera se ahorra la mayor cantidad de energía pero se reduce el *throughput*.

-*Fast PSP (Power Save Mode):* Conmuta entre los modos PSP y el CAM, dependiendo del tráfico por la red. Presenta un mayor *throughput* que el modo PSP.

- **Network Type:** Presenta dos opciones:

-*Ad Hoc:* Referido a redes punto a punto.

-*Infraestructure:* Indica que la red inalámbrica está conectada a la red *Ethernet* a través del AP.

## B) RF NETWORK—RED DE RADIO FRECUENCIA:

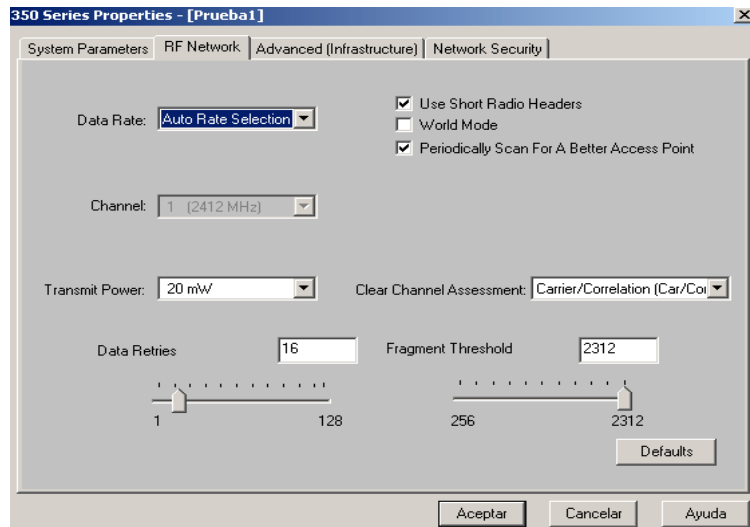


Figura 11.4 Parámetros de la red de Radiofrecuencia.

- **Use Short Radio Headers:** Los encabezados cortos mejoran el rendimiento del *throughput*; mientras que los encabezados largos aseguran la compatibilidad con los Clientes y AP's que no soportan encabezados cortos.
- **World mode:** Habilitando este parámetro el Cliente adoptará la máxima potencia de transmisión y rango de frecuencias del AP al cual está asociado. Para esto el AP debe tenerlo habilitado.
- **Periodically Scan For A Better AP:** Habilitando este parámetro el Cliente buscará un AP que presente la mayor fortaleza de la señal si al que se encuentra conectado presenta problemas y realiza conmutación entre ambos si encuentra alguno.
- **Channel:** Corresponde al canal en que se encuentra transmitiendo el AP. Debe estar configurado en automático.
- **Transmit Power:** Corresponde al nivel de potencia al cual el Cliente transmite.

- **Clear Channel Assessment:** Especifica el método a utilizar por el Cliente para determinar el canal al cual desea transmitir. Presenta 4 opciones:
  - Firmware Default (XXX)*: El mecanismo de *Clear Channel Assessment (CCA)* reportará si el canal está ocupado basado en el valor por defecto del *firmware* del Cliente.
  - Carrier/Correlation (Car/Cor)*: El mecanismo CCA reportará que el canal está ocupado si detecta una señal transmitida en DSSS (*Direct-Sequence Spread Spectrum*). Esta puede estar por encima ó debajo del límite de ED.
  - Energy Detect (ED)*: El mecanismo CCA reportará que el canal está ocupado si la detección de energía está por encima del límite de ED.
  - ED ó Car/Cor*: El mecanismo CCA reportará que el canal está ocupado si detecta una señal DSSS ó energía por encima del límite de ED.
- **Data Retries:** Especifica la cantidad de veces que un paquete es reenviado si la transmisión inicial no es exitosa. Puede ingresarse un número entre 1 hasta 128. El valor por defecto es 16 para Clientes de 2.4 GHz.
- **Fragment Threshold:** Define el límite de tamaño del paquete de RF, sobre el cual es partido ó segmentado. Si uno de estos paquetes segmentados presenta interferencia durante la transmisión, solamente este paquete deberá ser reenviado. El rendimiento del *throughput* es menor para paquetes segmentados ya que el paquete de encabezado para el arreglo de los paquetes, consume mucho ancho de banda. Puede ingresarse un valor entre 256 y 2312. Por defecto es 2312.
- **Data Rate:** Especifica la razón de transferencia o recepción de datos hacia el AP. Se recomienda seleccionar *Auto Rate* en el modo de infraestructura.

### c) ADVANCED (INFRASTRUCTURE) —AVANZADO:

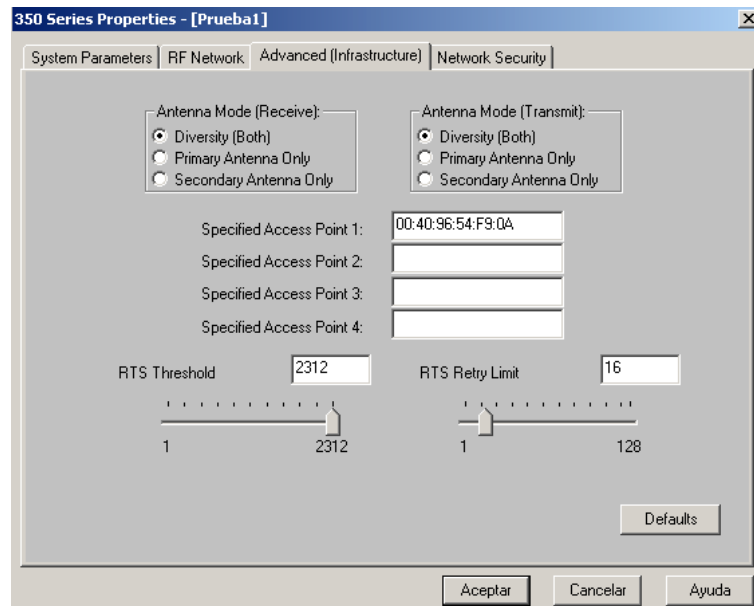


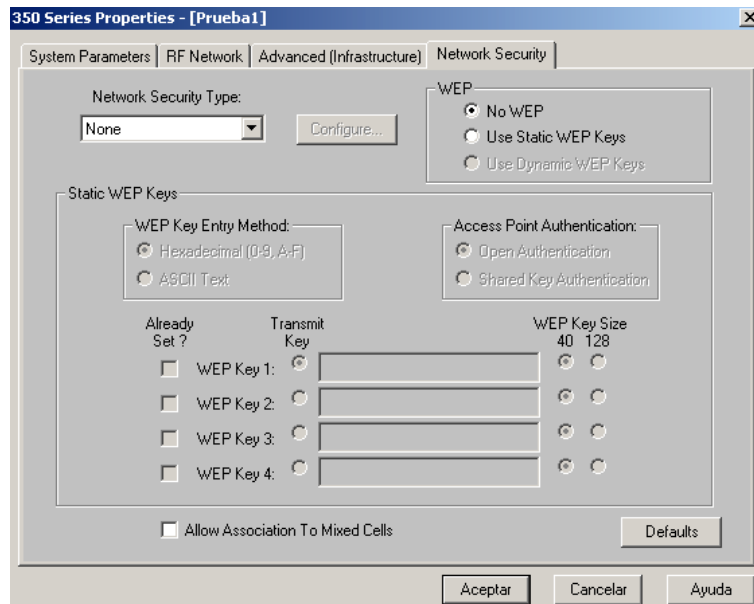
Figura 11.5 Parámetros Avanzados de Infraestructura.

- **Antena Mode (Receive):** Especifica la antena que el Cliente utiliza para recibir datos. Se recomienda utilizar el parámetro de *Diversity*.
- **Antena Mode (Transmit):** Especifica la antena que el Cliente utiliza para transmitir datos. Se recomienda utilizar el parámetro de *Diversity*.
- **Specified Access Point 1-4:** Especifica la dirección MAC de AP's preferidos para asociarse. Este parámetro debe ser utilizado solamente en AP's en modo repetidor.
- **RTS Threshold:** Especifica el tamaño del paquete de datos que utiliza el protocolo de RF para enviar peticiones de envío. Mientras menor sea el tamaño, se permite que exista mayor cantidad de peticiones lo cual hace más rápida la transmisión. Su valor oscila entre 0 y 2312.



- **RTS Retry Limit:** Especifica la cantidad de veces que el Cliente reenvia los paquetes RTS hasta que no reciba un CTS (*Clear to Send*) de un paquete enviado. Entre mayor sea este valor se disminuye el ancho de banda siempre que una interferencia es encontrada, ocasionando que el sistema se vuelva inmune a interferencias y colisiones. Puede escogerse un valor entre 1 y 128.

**D) NETWORK SECURITY—SEGURIDAD DE LA RED:**



**Figura 11.6** Parámetros de seguridad de la red.

- **Network Security Type:** Se presentan las siguientes opciones:

-None: No habilita ningún tipo de protocolo de autenticación como medio de seguridad de ingreso a la red.

-LEAP: Protocolo de autenticación basado en *EAP*, pero es propietario de Cisco.

-Host Based EAP: Permite el uso de cualquier tipo de autenticación 802.1X a la cual el sistema operativo puede soportar. Por ejemplo: *EAP-TLS*, *PEAP* y *EAP-SIM*.

- **WEP:** Permite o no la encriptación de datos que viajan por la red inalámbrica, utilizando entre los dispositivos, una misma llave compartida.

**Static WEP Keys:** Este apartado presenta los siguientes parámetros:

a) WEP Key Entry Method: Presenta 2 opciones:

**a.1) Hexagesimal (0-9, A-F):** Especifica que la llave WEP será ingresado en caracteres hexagesimales los cuales incluyen de 0-9, A-F y a-f.

**a.2) ASCII Text:** Especifica que la llave WEP será ingresada en texto ASCII, los cuales incluyen caracteres, números y signos de puntuación.

b) Access Point Authentication: Presenta 2 opciones:

**b.1) Open Authentication:** Habilita al Cliente, sin importar las configuraciones del WEP, a autenticar e intentar comunicarse con el AP. Este es el parámetro por defecto.

**b.2) Shared Key Authentication:** Habilita al Cliente a comunicarse solamente con los AP's que tienen la misma llave WEP. Esta opción está disponible solamente si selecciona *Use Static WEP Key*. En este tipo de autenticación el AP envía un paquete no encriptado conocido como "*Challenge Packet*" al Cliente, el cual lo encripta y lo envía de vuelta al AP. El AP intenta desencriptarlo y envía un paquete de respuesta de autenticación al Cliente indicando si tuvo o no éxito. Si tuvo éxito el usuario se considera como autenticado.

- **WEP Key 1, 2, 3, 4:** En estos espacio se ingresa la llave compartida para encriptar los mensajes mediante el uso del protocolo WEP..

- **Allow Association to Mixed Cells:** Indica si el Cliente puede asociarse a un AP que permita asociación basada en WEP y no-WEP.

### 11.3. ESTADÍSTICAS DEL CLIENTE AIRONET

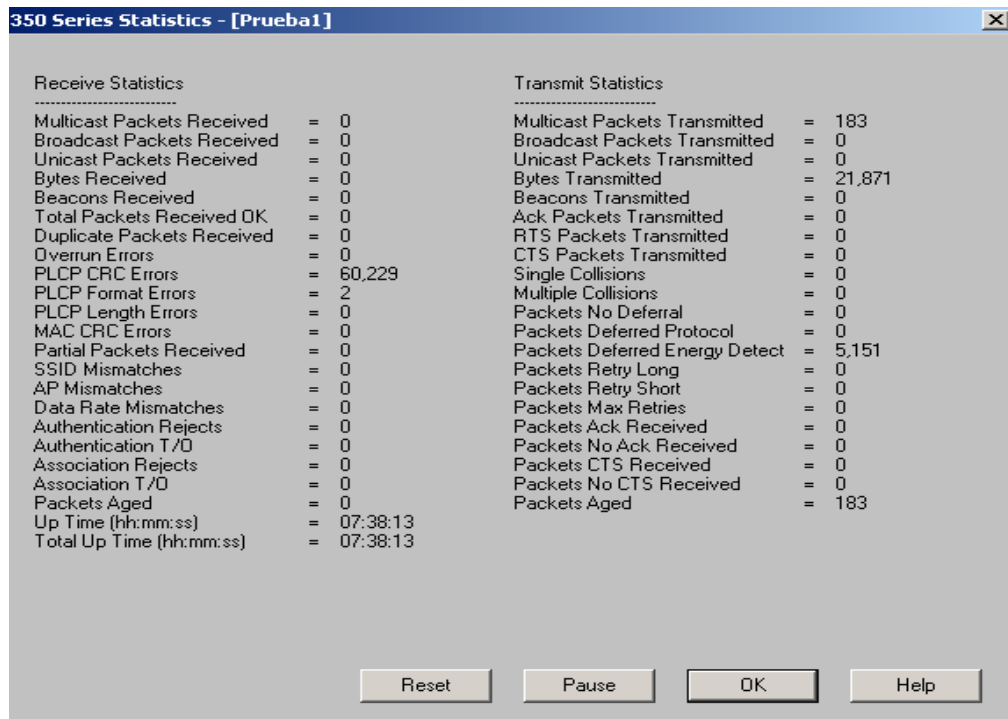


Figura 11.7 Estadísticas del Cliente Aironet 350.

#### Receiver Statistics — Estadísticas de Recepción:

- **Multicast Packets Received:** Número de paquetes de *multicast* que fueron recibidos exitosamente.
- **Broadcast Packets Received:** Número de paquetes de *broadcast* que fueron recibidos exitosamente.
- **Unicast Packets Received:** Número de paquetes de *unicast* que fueron recibidos exitosamente.
- **Bytes Received:** Número de *bytes* de datos que fueron recibidos exitosamente.

- **Beacons Received:** Número de paquetes de *beacon* que fueron recibidos exitosamente.
- **Total Packets Received OK:** Total de paquetes que fueron recibidos exitosamente.
- **Duplicate Packets Received:** Número de paquetes duplicados que fueron recibidos exitosamente.
- **Overrun Errors:** Número de paquetes recibidos cuando los *Buffer* de recepción no estaban disponibles.
- **PLCP CRC Errors:** Cantidad de veces que el Cliente inició la recepción de un encabezado de protocolo de convergencia 802.11 de Capa Física, pero el resto del paquete fue ignorado durante el ciclo de verificación de errores de redundancia (CRC).
- **PLCP Format Errors:** Cantidad de veces que un encabezado PLCP 802.11 fue recibido pero el resto del paquete fue ignorado debido a un valor desconocido en el encabezado.
- **PLCP Length Errors:** Cantidad de veces que un encabezado PLCP 802.11 fue recibido pero el resto del paquete fue ignorado debido a una longitud de encabezado no válida.
- **MAC CRC Errors:** Número de paquetes que tuvieron un encabezado PLCP 802.11 pero que contenían un error de CRC en la porción de datos del paquete.  
**Nota** Los errores de CRC pueden ser atribuidos a la colisión de paquetes causada por una densa población de Clientes, cobertura de AP's en un canal, alto índice de *multipath* ó la presencia de otras señales de 2.4 GHz.
- **Partial Packets Received:** Número de fragmentos que fueron descartados debido a que no se recibió el paquete entero.
- **SSID Mismatches:** Número de veces que el Cliente intentó asociarse a un AP pero no pudo debido a que el SSID no era el mismo que el del AP.
- **AP Mismatches:** Número de veces que el Cliente intentó asociarse a un AP pero no pudo debido a que el Cliente no había sido especificado en el AP.

- **Data Rate Mismatches:** Número de veces que el Cliente intentó asociarse al AP pero no pudo debido a que la tasa de transferencia de datos no fue soportada por el AP.
- **Authentication Rejects:** Número de veces que el Cliente intentó validarse al AP pero fue rechazado.
- **Authentication Time-out:** Número de veces que el Cliente intentó validarse al AP pero no pudo debido a que éste no respondió a tiempo (*Time Out*).
- **Packets Aged:** Número de paquetes recibidos satisfactoriamente pero fueron descartados por el Cliente debido a que no todos los fragmentos fueron recibidos dentro de los 10 segundos, ó el invitado no leyó los paquetes del adaptador dentro de los 10 segundos.
- **Packets MIC OK:** Número de paquetes que fueron recibidos satisfactoriamente con una válida Verificación de Integridad del Mensaje (MIC).
- **Packets No MIC:** Número de paquetes que fueron descartados debido a que no se encontró la MIC.
- **Packets Incorrect MIC:** Número de paquetes que fueron descartados debido a un incorrecto valor MIC.
- **Packets No MIC Seed:** Número de paquetes que fueron descartados debido a que no se recibió ningún MIC.
- **Packets Wrong MIC Sequence:** Número de paquetes que fueron descartados debido a que la secuencia de MIC estaba mala.
- **Up Time (hh:mm:ss):** Despliegue de tiempo (en horas:minutos:segundos) desde el último *Reset*. Si el Cliente ha estado ejecutándose por más de 24 horas, el tiempo se despliega como días, en horas:minutos:segundos.
- **Total Up Time (hh:mm:ss):** Despliegue del tiempo (en horas:minutos:segundos) que el Cliente ha estado recibiendo energía. Este conteo continúa a pesar de reiniciar y borrar la configuración del Cliente

*Transmit Statistics* — Estadísticas de Transmisión:

- ***Multicast Packets Transmitted:*** Cantidad de paquetes *multicast* que fueron transmitidos exitosamente.
- ***Broadcast Packets Transmitted:*** Cantidad de paquetes *broadcast* que fueron transmitidos exitosamente.
- ***Unicast Packets Transmitted:*** Cantidad de paquetes *unicast* que fueron transmitidos exitosamente.
- ***Bytes Transmitted:*** Número de *bytes* de datos que fueron transmitidos exitosamente.
- ***Beacons Transmitted:*** Número de paquetes de *beacon* que fueron transmitidos exitosamente (solamente en modo *ad hoc*).
- ***Ack Packets Transmitted:*** Número de paquetes de reconocimiento (Ack) que fueron transmitidos en respuesta a paquetes *unicast* recibidos exitosamente.
- ***RTS Packets Transmitted:*** Número de paquetes de petición de envío (RTS) que fueron transmitidos exitosamente.
- ***CTS Packets Transmitted:*** Número de paquetes *Clear-to-send* (CTS) que fueron transmitidos en respuesta a un paquete de RTS recibido.
- ***Single Collisions:*** Número de paquetes que han tenido que ser retransmitidos una vez debido a una colisión.
- ***Multiple Collisions:*** Número de paquetes que han tenido que ser retransmitidos más de una vez debido a una colisión.
- ***Packets No Deferral:*** Número de paquetes que estuvieron disponibles para ser transmitidos inmediatamente sin ser retrasados por una detección de energía o protocolo postergado.
- ***Packets Deferred Protocol:*** Número de paquetes que fueron retrasados debido a razones del protocolo 802.11 (como tiempo insuficiente para enviar el paquete).

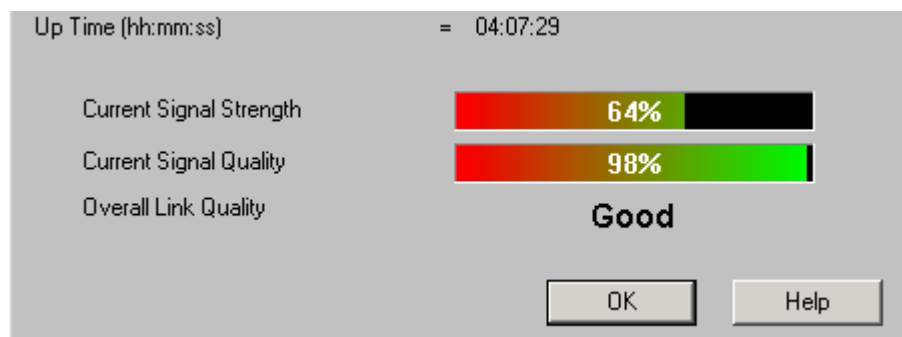
- **Packets Deferred Energy Detect:** Número de paquetes que fueron retrasados debido a que se detectó energía de radiofrecuencia. Esta condición es usualmente causada por otra transmisión en el medio ó fuente por alguna fuente de RF que causa interfeerencia (tal como un horno de microondas).
- **Packets Retry Long:** Número de paquetes de datos que fueron retransmitidos.  
**Packets Retry Short:** Número de paquetes de petición de envía (RTS) que fueron retransmitidos.
- **Packets Max Retries:** Número de paquetes que fallaron en la transmisión después de haber hecho un número exhaustivo de intentos.
- **Packets Ack Received:** Número de paquetes transmitidos que poseen su correspondiente paquete de reconocimiento (Ack) recibido existosamente.
- **Packets No Ack Received:** Número de paquetes transmitidos que no poseen su correspondiente paquete de reconocimiento (Ack) recibido satisfactoriamente.
- **Packets CTS Received:** Número de paquetes libre para el envío (CTS) que fueron recibidos en respuesta a un paquete RTS.
- **Packets No CTS Received:** Número de paquetes para los cuales no se recibió paquetes de CTS en respuesta a un paquete RTS.
- **Packets Aged:** Número de paquetes que fueron descartados por el Cliente debido a que no fueron transmitidos satisfactoriamente dentro de 5 segundos.

## 11.4. DIAGNOSTICOS DE COBERTURA

Para establecer la calidad general del enlace que garanticen la cobertura, se utilizan los mismos lineamientos dados por Cisco. Se establecen las siguientes categorías:

- *Excellent* — *Excelente*: Fortaleza de la señal con porcentajes mayor al 75%.
- *Good* — *Bueno*: Fortaleza de la señal mayor a 40%, pero menor a 75%.
- *Fair* — *Regular*: Fortaleza de la señal mayor a 20 %, pero menor a 40%.
- *Poor* — *Pobre*: Fortaleza de la señal menor a 20%.

Estos valores en porcentajes (%) son desplegados al seleccionar el botón de *Status*— Estado, en el menú principal del ACU.



**Figura 11.8** Despliegue del *Status* en porcentaje.

A partir de estos valores expresados en porcentajes, y conociendo que los límites de sensibilidad teóricos están dados por:

$$-95 \text{ [dBm]} \leq \text{Sensibilidad} \leq -45 \text{ [dBm]}$$

**donde** la Sensibilidad Mínima de Recepción corresponde a  $-95 \text{ [dBm]}$  y la Sensibilidad Máxima de Recepción ó Saturación corresponde a  $-45 \text{ [dBm]}$ .



Se puede realizar una interpolación de datos, para establecer la siguiente escala de categorías para los enlaces inalámbricos:

**-57,5 [dBm] < Excelente ≤ -45 [dBm]**

**-75 [dBm] < Bueno ≤ -57,5 [dBm]**

**-85 [dBm] < Regular ≤ -75 [dBm]**

**-95 [dBm] < Pobre ≤ -85 [dBm]**

Cabe destacar que óptimo rendimiento de la red inalámbrica no solamente depende de la fortaleza de la señal, sino también del Nivel de Ruido (S/N) que se encuentre en el ambiente, producto de la presencia de máquinas eléctricas (Generador Eléctrico), líneas de distribución de fluido eléctrico ó bien, el uso de otros equipos que utilicen la misma banda de frecuencia.

## CAPITULO 12: ANALISIS DE DATOS RECOLECTADOS

### Breve explicación del capítulo

En este capítulo se relata la situación actual que se vive en la empresa.

### 12.1. ENCUESTA APLICADA

Se pidió a los empleados de CSU a llenar una encuesta de manera voluntaria, la cual consistió en tres preguntas:

1. Considera que el servicio brindado por la red inalámbrica es:
  - a) Eficiente
  - b) Aceptable
  - c) Deficiente
  - d) No sabe
  - e) No responde
  
2. Le presenta algún problema la red inalámbrica:
  - a) Si
  - b) No
  
3. Explique cuál es su problema:

**Figura 12.1** Encuesta aplicada a empleados de CSU.

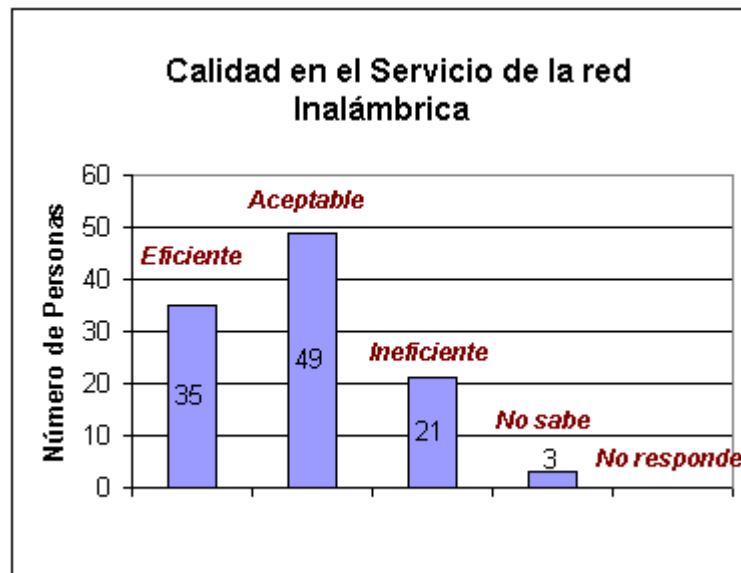
Del total de empleados de CSU, respondieron a la encuesta 108 personas.

Los resultados fueron los siguientes:

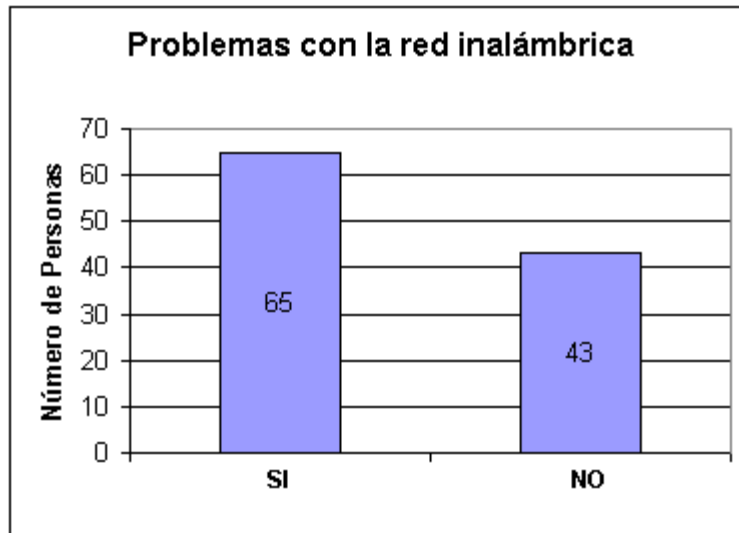
-La mayoría de los empleados de CSU considera que la calidad en el servicio proveído por la red inalámbrica se encuentra entre aceptable y excelente. Sin embargo es de preocuparse el hecho que gran cantidad de los encuestados la consideren ineficiente (Ver [Figura 12.2](#)).

-La mayoría de los empleados de CSU presenta problemas en sus conexiones con la red inalámbrica (Ver [Figura 12.3](#)).

-El principal problema que detallan los empleados es la falta de cobertura en distintas zonas del edificio.



**Figura 12.2** Datos obtenidos de la 1er pregunta de la encuesta.



**Figura 12.3** Datos obtenidos de la 2da pregunta de la encuesta.

## 12.2. DATOS RECOLECTADOS CON EL LOCUST

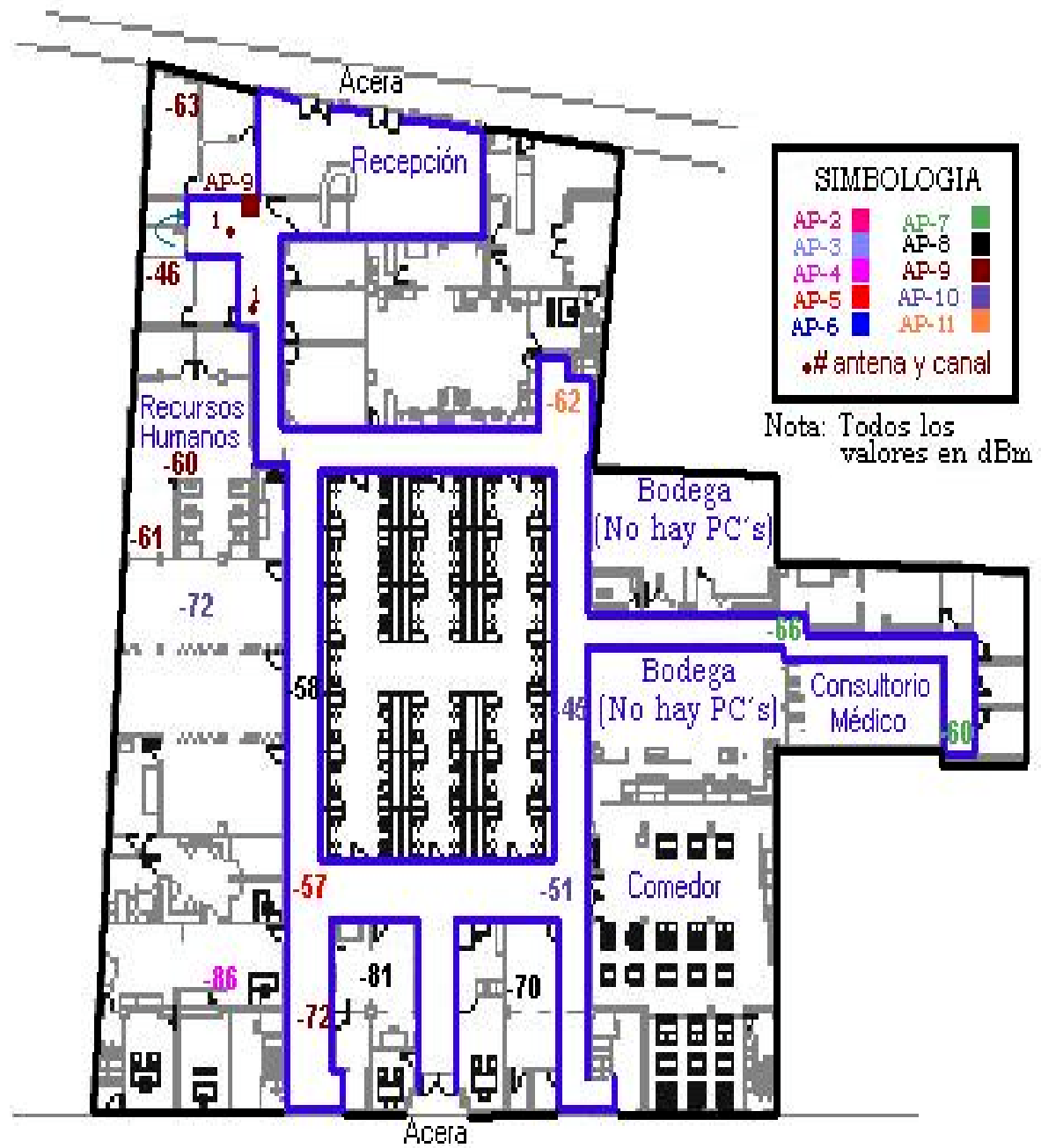


Figura 12.4 Primera Planta del Edificio Central de CSU

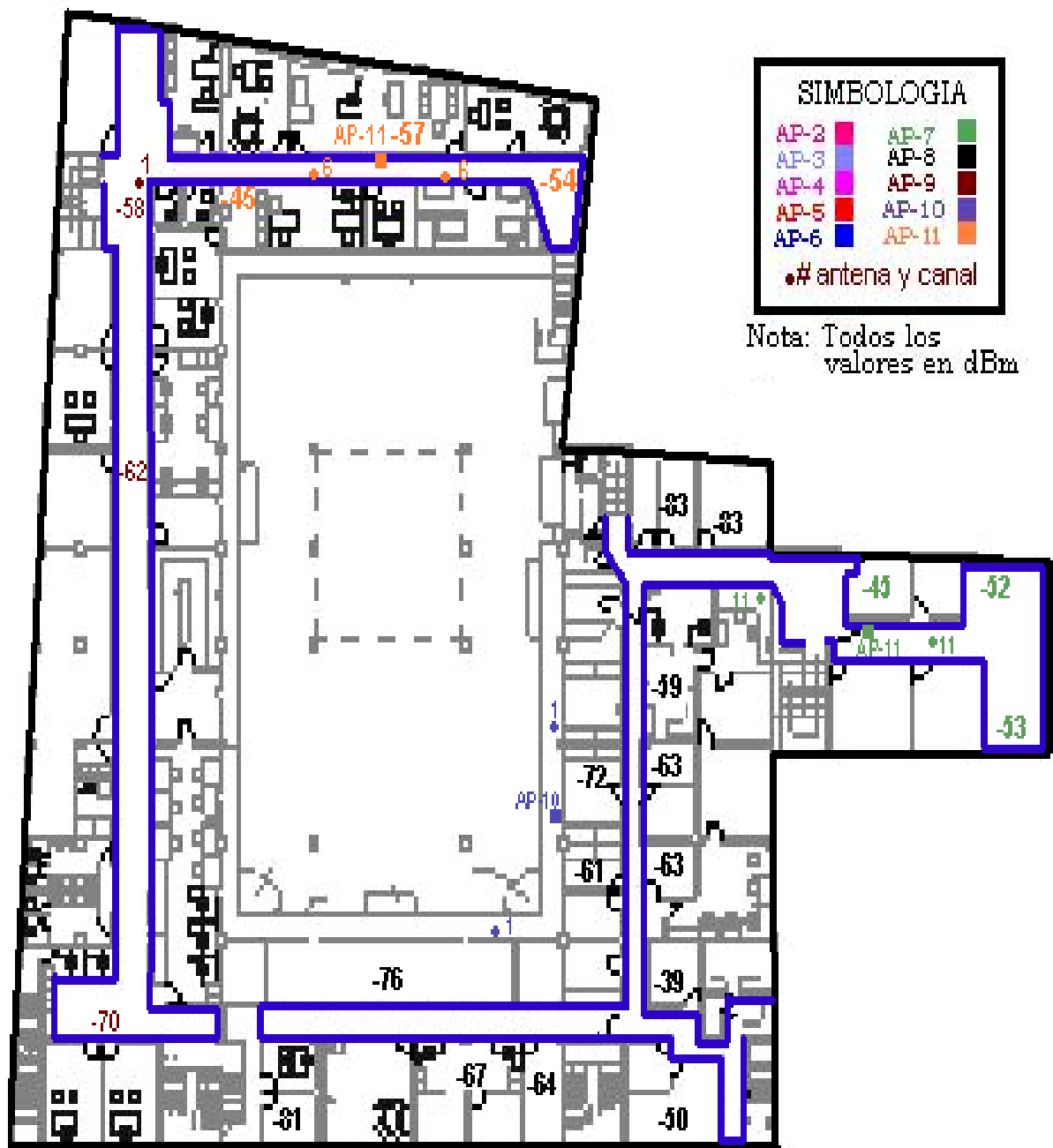


Figura 12.5 Segunda Planta del Edificio Central de CSU

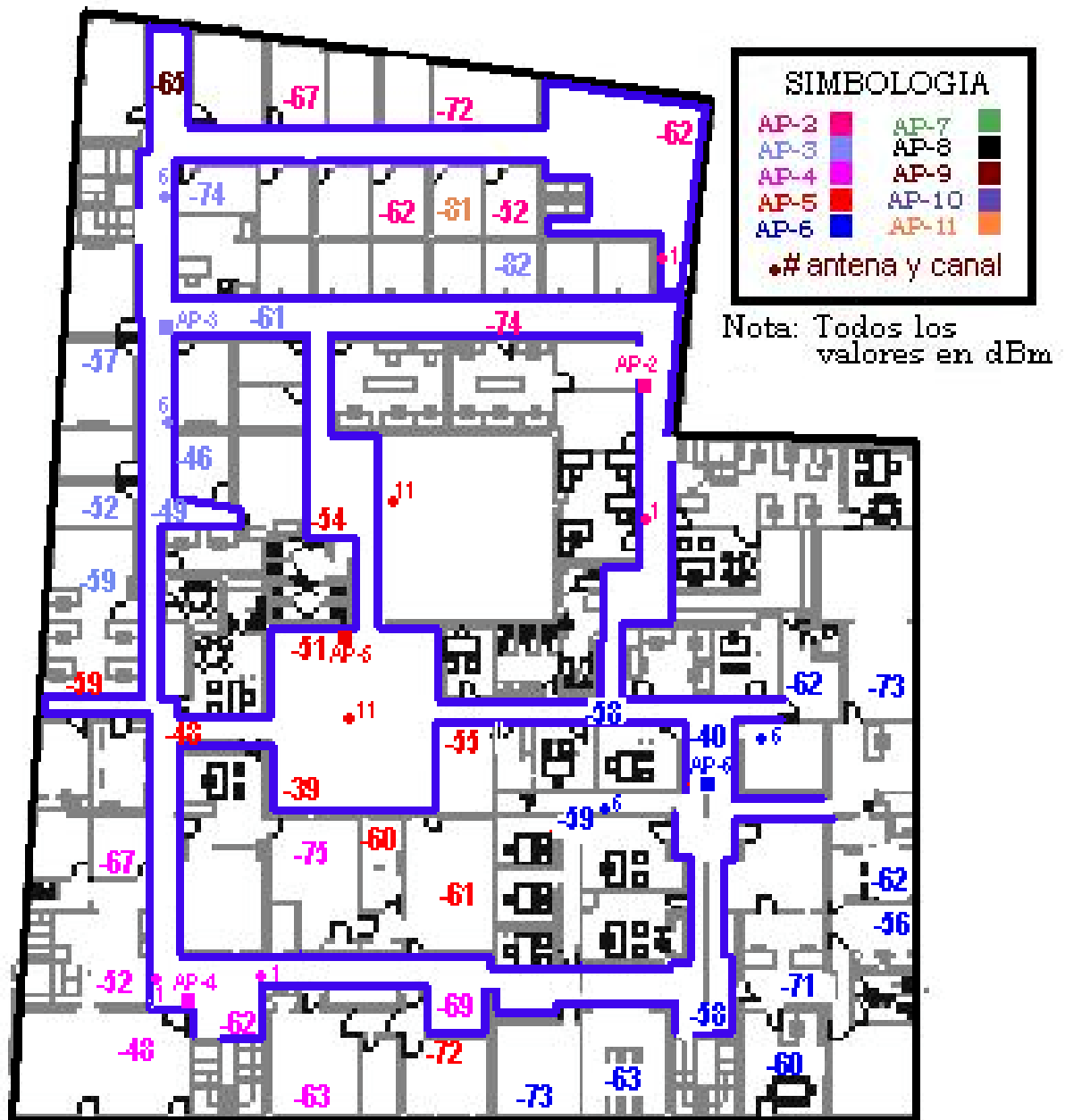


Figura 12.6 Tercera Planta del Edificio Central de CSU

### 12.3. ANÁLISIS DE DATOS RECOLECTADOS

Una vez analizada la distribución de las antenas en el edificio, se puede ver en las figuras [12.4](#), [12.5](#) y [12.6](#); como el nivel de potencia de la señal<sup>2</sup> presenta una fortaleza por encima del nivel mínimo del valor nominal propuesto por Cisco para una tasa de transferencia a 11 Mbps<sup>3</sup>, la cual se considera como el valor crítico para la transmisión. Esto se puede observar en la Figura 12.7.

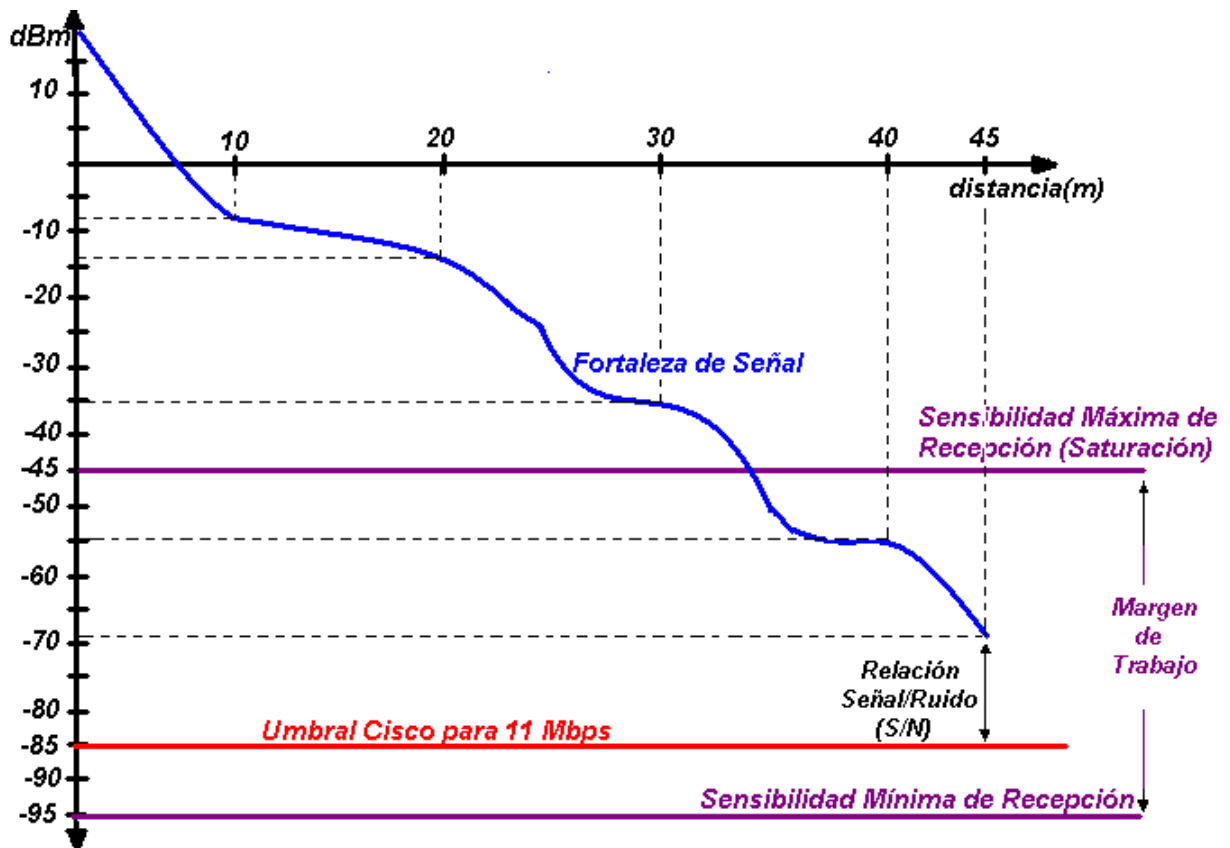


Figura 12.7 Potencia Vrs Distancia

<sup>2</sup> Medida en dBm

<sup>3</sup> Ver hojas de datos de Aironet 350 y 1200 en Anexos



El hecho de que la fortaleza de la señal esté por encima del Umbral Cisco para 11 Mbps, se garantiza que los paquetes de información enviados por cualquier estación de trabajo llegarán hasta el receptor con la potencia mínima necesaria para recorrer una distancia de por lo menos 45 mts a una tasa de transmisión de 11 Mbps. Este último valor corresponde al alcance típico recomendado por Cisco en sus hojas de datos.

Otro punto importante de recalcar es que, entre mayor sea la relación Señal/Ruido (S/R), más “clara” y mejor va a ser la comunicación entre los dispositivos que conforman la red.

En caso que los paquetes no tengan la suficiente potencia para llegar hasta el receptor, estarán por debajo del Nivel de Sensibilidad Mínima del AP ocasionando que éste no pueda decodificarlo debido a que los estados lógicos determinados por el tipo de modulación, no cuentan con la suficiente energía para ser “entendidos” por el AP.

Tal y como se puede notar en las figuras [12.4](#), [12.5](#) y [12.6](#), se aprecia que el nivel de potencia es insignificamente afectado por el hecho que la mayoría de los Departamentos en el edificio se encuentren divididos en cubículos de paredes prefabricadas delgadas y elaboradas con materiales sintéticos fácilmente penetrables por la señal de RF. De aquí se intuye que no son un factor determinante en las atenuaciones que se puedan presentar. Lo que sí es significativo en este aspecto son las paredes de concreto, los cuales atenúan en hasta 9 dBm la fortaleza de la señal transmitida.

Por lo tanto, el nivel de cobertura presentado en las Oficinas Centrales de CSU es bastante óptimo para la implementación de transmisiones con tasas de transferencia de 11 y 5.5 Mbps de manera confiable ya que; todas las mediciones realizadas presentan niveles de potencias mayores a los -85 dBm.

## CAPITULO 13: RECOMENDACIONES

### EN CUANTO AL DISEÑO FÍSICO Y DISTRIBUCIÓN DEL EQUIPO DE LA *WLAN*:

- Evitar colocar los AP's cerca de fuentes generadoras de ruido (o interferencia), tales como balastos, cables eléctricos, entre otros.
- Evitar colocar las antenas cerca de lugares con gran presencia de metales (tales como aceros, hierro, entre otros), ya que estos materiales son reflexivos y distorsionan la propagación de la señal RF. Inclusive son casi impenetrables para la señal de RF.
- Es necesario tomar en cuenta la distribución de las paredes de concreto en el edificio a la hora de la colocación de las antenas, ya que la señal de RF se debilita considerablemente (aproximadamente 9 dBm) cuando deben atravesarse para cubrir determinada área detrás de ellas. Por otra parte, la distribución de paredes constituidas por materiales prefabricados de poco grosor (tales como *fibrolit*, *plywood*, etc), pueden ser casi despreciadas en el diseño, ya que la señal de RF presenta una buena penetración en estos. (Ver datos en figuras [12.4](#), [12.5](#) y [12.6](#)).
- Utilizar las técnicas de diversidad de antenas para mejorar las pérdidas por múltiples rutas ([multipath](#)).
- Se debe aplicar la técnica de diversidad de antena correctamente ([Ver](#)).

## EN LOS PARÁMETROS DEL ACU DE LA VERSIÓN 12.01T:

- Debe habilitarse el parámetro **CAM** (*Constantly Awake Mode*) para proveer mayor *throughput* al enlace ([Ver Parámetro por Defecto](#)).
- Debe seleccionarse en *Auto-Rate*, el parámetro de **Data Rate**; con el propósito de proveer mayor *throughput* al enlace ([Ver Parámetro por Defecto](#)).
- Si todos los Clientes que se conectan a la red inalámbrica son Cisco, se debe habilitar el parámetro de **Use Short Radio Headers** para mejorar el *throughput* ([Ver Parámetro por Defecto](#)).
- El parámetro **World Mode** debe habilitarse tanto en el ACU como en el AP, para lograr que el Cliente adopte su máxima potencia de transmisión ([Ver Parámetro a activar](#)).
- El parámetro **Periodically Scan for A Better AP** debe habilitarse para que cuando el Cliente realice el *roaming*, siempre busque asociarse al AP que le ofrezca un mejor enlace (mayor potencia y confiabilidad) ([Ver Parámetro por Defecto](#)).
- El canal ó **Channel** en que trabaja el Cliente, debe configurarse como *Automático* para que el Cliente adopte el canal que utiliza el AP para dar cobertura a determinada zona de un edificio ([Ver Parámetro por Defecto](#)).
- Debe utilizarse la opción de **CAR/COR** (*Carrier/Correlation*) en el parámetro de **Clear Channel Assessment**, como método de detección para saber si el medio se encuentra ocupado para transmitir ([Ver Parámetro a Activar](#)).

- El valor del parámetro **Fragment Threshold** debe estar al máximo (2312) para evitar la fragmentación de paquetes lo más que se pueda, ya que cuando se transmite el encabezado de reparación, este consume mucho ancho de banda ([Ver Parámetro por Defecto](#)).
- En cuanto al modo de la Antena (**Transmit** y **Receive**), deben especificarse como **Diversity** para un mejor rendimiento ([Ver Parámetro por defecto](#)).
- El valor asignado al parámetro **RTS Threshold** debe ser lo más pequeño, para que se den una mayor cantidad de peticiones de acceso al medio por segundo ([Ver Parámetro a Activar](#)).
- El valor asignado al parámetro **RTS Retry Limit** debe ser lo más grande posible, ya que de esta manera la señal transmitida se vuelve más inmune al ruido o interferencias, esto porque se disminuye el ancho de banda de la señal ([Ver Parámetro a Activar](#)).

#### EN LOS PARÁMETROS DEL AP:

- Es necesario deshabilitar el *Telnet* para la administración de los equipos por razones de seguridad ([Ver Parámetro a Activar](#)). Es recomendable habilitar algún protocolo de encriptación como el SSH para mayor seguridad.
- Se debe configurarse el submenú de **User Manager** ya que SSH utiliza los nombres de usuarios y claves establecidos bajo este perfil cuando recibe una petición de un Cliente para establecer un enlace Punto a Punto con el AP, entre el cual se ejecute el protocolo SSH ([Ver submenú a configurar](#)).

- El parámetro ***Aironet Extended Statistics in MIB***, debe deshabilitarse para no guardar información de las Alertas en la memoria del AP ([Ver Parámetro a desactivar](#)).
- El parámetro ***Disallow Infrastructure Stations on any other***, debe configurarse como **NO**; para restringir que los dispositivos con diferentes SSID's puedan conectarse a la red ([Ver Parámetro a Activar](#)).
- El parámetro ***TFTP*** debe estar activo, ya que este es el protocolo que utiliza el *CiscoWorks for Wireless* para comunicarse con el AP ([Ver Parámetro por Defecto](#)).
- Es necesario deshabilitar el parámetro ***Search for Less Congested Channel***, ya que se busca que el canal que fue configurado al inicio, brinde cobertura a una determinada zona del edificio y se mantenga fijo independientemente de la cantidad de Clientes que estén conectados ([Ver Parámetro a Desactivar](#)).
- Las tasas de transferencias de 5.5 y 11 Mbps deben estar configuradas en ***Basic***, para que el rendimiento sea mayor a estas velocidades ya que permite el tráfico tanto de paquetes *unicast* como *multicast* ([Ver Parámetros a Configurar](#)).
- El parámetro ***Use Aironet Extensions*** debe configurarse en **SI**, para asegurar un balanceo de carga (*Load Balancing*) en caso de existir mucho tráfico en la red ([Ver Parámetro a Configurar](#)).

- Si la red está constituida solamente de equipo *Aironet* de Cisco, debe configurarse el parámetro de **Encapsulation** en **802.1H**, ya que es el tipo de encapsulado óptimo ([Ver Parámetro a Activar](#)). En cuanto a la NIC debe tenerse activo el parámetro *Use Short Radio Headers* para asegurar su compatibilidad ([Ver Parámetro a Activar](#)).
- Es necesario tener actualizadas las versiones de los sistemas operativos de todos los AP's y NIC's para lograr un mejor rendimiento de la red inalámbrica.
- Es necesario configurar un servidor NTP (*Network Time Protocol*) con el propósito de que cuando ocurran eventos, éstos queden registrados con la hora exacta en el *CiscoWorks for Wireless*.
- Es necesario tener un único usuario activo como administrador de redes.
- El CDP (*Cisco Discovery Protocol*) debe habilitarse para que el AP pueda reconocer cualquier nuevo dispositivo con el Cliente Cisco ([Ver Parámetro a Activar](#)).
- El parámetro *Role in Radio Network* debe estar en modo **Root** ([Ver Parámetro a Activar](#)).
- El parámetro de *Allow Broadcast SSID to Associate* debe configurarse como **NO**, esto para evitar que cualquier Cliente con un SSID (no necesariamente el de la red) configurado pueda ser aceptado por el AP.

Si todos los Clientes de la red son marca Cisco ó compatibles:

- El parámetro de *Radio Preamble* debe configurarse como **Short** (Corto), esto para ahorrar ancho de banda a la hora de realizar una transmisión entre equipos Cisco ya que no se envía el encabezado de reconstrucción del mensaje recibido, lo cual sí ocurre cuando se tiene configurado el **Long** ([Ver Parámetro a Activar](#)).
- El parámetro de *Radio Modulation* debe estar en **estándar**, ya que el **MOK** se utiliza para equipo muy antiguo ([Ver Parámetro por Defecto](#)).
- El parámetro *Ethernet Encapsulation Transform*, debe estar en **802.1H**, ya que es el recomendado por Cisco para sus equipos ([Ver Parámetro a Activar](#)).
- El parámetro *Use Aironet Extensions* debe estar en **Si**, para que el MIC (*Message Integration Check*) tome efecto y se ejecute en cada transmisión de datos. Debe configurarse además el *WEP* en **Full Encryption**, para lograr que esto funcione ([Ver Parámetro a Activar](#)).
- El parámetro *Disallow Infrastructure Stations on any other SSID* debe estar configurado como **Si**, esto para evitar que equipos con otro SSID puedan conectarse a la red ([Ver Parámetro a Activar](#)).
- El parámetro *Enhanced MIC Verification for WEP* debe estar en **MMH**, esto para poder chequear la integridad del mensaje una vez recibido ([Ver Parámetro a Activar](#)).

### EN CUANTO AL *LOCUST*:

- El levantamiento de los datos en el sitio debe realizarse cuando todas las posibles fuentes de ruido están activas, para poder obtener datos más acordes con la realidad.

### EN CUANTO AL *CISCOWORKS FOR WIRELESS (WLSE)*:

- Se recomienda adquirir el *CiscoWorks for Wireless*, con el propósito de lograr un manejo más centralizado y eficiente de toda la red inalámbrica de CSU.
- Debe configurarse parámetro **CDP** en el menú de **Services** del AP, para que el *WLSE* pueda descubrir automáticamente, todo aquel equipo nuevo que se conecte a la red ([Ver Parámetro a Activar](#)).
- Debe configurarse parámetro **SNMP** en el menú de **Services** del AP, para poder administrar los equipos inalámbricos desde el *WLSE* ([Ver Parámetro a Activar](#)).
- Debe configurarse parámetro **TFTP** en el menú de **Services** del AP, para lograr comunicación entre los equipos de la red inalámbrica y el *WLSE* ([Ver Parámetro a Activar](#)).
- Se debe crear un usuario en el *WLSE* con todos los privilegios de: escritura, SNMP, *firmware* y administración, en el menú de *User Administration*; para que sea utilizado por los Administradores de la Red de CSU, únicamente.



#### **OTRAS RECOMENDACIONES:**

- No es necesario pasar del estándar 802.11b (de 2.4 GHz) al estándar 802.11a (de 5 GHz), esto ya que a pesar que este último ofrece mejor *data rate* (54 Mbps), los equipos son muy caros en comparación a los primeros, ofrece una menor cobertura y no son compatibles con 802.11b.
- En un futuro, debe optarse por la migración de los equipos del estándar 802.11b al 802.11g, el cual ofrece un mejor precio y además es compatible con todos los equipos que se rigen bajo el estándar 802.11b ([Ver Figura B.4.1](#)).
- Se debe buscar que el máximo valor EIRP sea de +36 [dBm], con lo cual se podrá estar certificado ante la FCC ([Ver Anexos: Regulaciones según FCC](#)).
- No se debe encender un AP sin haber colocado primero la antena al conector de PRIMARY, ya que el equipo puede dañarse.

## CONCLUSIONES

- Los AP's 350 y 1200 poseen conectores RP-TNC, lo cual permite mayor maniobrabilidad a la hora del diseño ya que se puede llevar las antenas a lugares poco accesibles.
- Tanto las antenas direccionales como las omnidireccionales que se utilizan en el funcionamiento de la red inalámbrica dentro del edificio, están colocadas en la posición correcta, lo cual permite que la propagación de la onda de radiofrecuencia se desplace en el medio de manera adecuada.
- Los dispositivos inalámbricos Cisco Aironet poseen un sistema de movilización entre un punto de acceso a otro (si poseen el mismo SSID), sin sufrir ningún corte en la conexión llamado Vaganbundeó ó *Roaming*.
- El AP debe ir colocado lo más cerca de las antenas como sea posible, para evitar utilizar cables muy largos que ocasionen pérdidas mayores en la fortaleza de la señal.
- Entre mayor sea la longitud del cable utilizado entre el AP y la antena, mayor serán las pérdidas de potencia de la señal.
- La localización de dos antenas pertenecientes a un mismo AP deben estar cubriendo una misma área ó celda, y además deben colocarse con una pequeña diferencia de distancia entre sí (esto si el *antenna diversity* está activo en el AP).
- La cobertura del edificio de CSU cuenta con deficiencias en aquellos lugares donde su medición de potencia es menor a -80 dBm.

- La máxima penetración que puede lograr la señal sin degradarse considerablemente es de 1 a 2 paredes sólidas ó pisos de concreto.
- Las paredes de *block*, en general, limitan la penetración de la señal en hasta 3 ó 4 paredes sin degradar la señal.
- Las paredes de madera ó *plywood*, en general, no degradan la señal hasta después de atravesar 5 ó 6 paredes.
- Las paredes de metal delgado causan que la señal se refleje ó tenga una poca penetración.
- A nivel *Indoor*, un aumento en 9 dB en la potencia de transmisión duplica la distancia de cobertura.
- A nivel *Indoor*, una disminución en 9 dB en la potencia de transmisión disminuye a la mitad la distancia de cobertura.
- Si se siguen las recomendaciones se puede lograr un óptimo rendimiento de la red inalámbrica.

## BIBLIOGRAFIA

1. Stallings, W. ***Wireless communications and networks***. Prentice Hall.USA.
2. Berkley Varitronics Systems Inc. ***Wireless Products Catalog***
3. Cisco Systems Inc. ***WLAN Design***
4. Fuller, R.;Pfund,A.; Padjen, R.; Oullet, E.; Blankenship, T. ***Building a Cisco Wireless LAN***. Callisma

### Sitios

<http://www.ssh.com>

<http://www.cisco.com>

<http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eaglair/ap3xx/index.shm.htm>

## **APENDICES**



### **A.1.3. Conversión a dBm a partir de miliwatts (mW)**

$$X \text{ [dBm]} = 10 \log (P1[\text{mW}] / 1[\text{mW}]) \quad \text{donde: } P1 = \text{Potencia señal 1}$$

**X= Resultado**

Ejemplo:

$$10 \log (100 \text{ [mW]} / 1 \text{ [mW]}) = 20 \text{ [dBm]}$$

### **A.1.4. Obtención del EIRP (*Effective Isotropic Radiation Power*)**

$$\text{EIRP [dBm]} = P_{\text{TXap}} \text{ [dBm]} + P_{\text{ANT}} \text{ [dBi]} - P_{\text{CAB}} \text{ [dB]}$$

donde:  $P_{\text{TXap}}$  = Potencia de transmisión del AP.

$P_{\text{ANT}}$  = Potencia de antena.

$P_{\text{CAB}}$  = Pérdidas debidas al cable.

Ejemplo:

$$20 \text{ [dBm]} + 21 \text{ [dBi]} - 3.35 \text{ [dB]} = 37.65 \text{ [dBm]}$$

### **A.1.5. Conversión de dBd a dBi**

Se parte de la igualdad **0 dBd = 2.2 dBi**

Ejemplo:

$$3 \text{ [dBd]} = 5.2 \text{ [dBi]}$$

## **GLOSARIO**



- **LOCUST:** Verificador de cobertura para sistemas inalámbricos ó *IEEE 802.11b* *TESTER*.
  
- **Click:** Palabra del idioma inglés que tiene por significado seleccionar una determinada opción desplegada en pantalla y presionar una vez sobre ella el botón izquierdo del Ratón de la computadora.
  
- **Firmware:** Término del idioma inglés que hace referencia al sistema operativo de cualquier dispositivo de la red.
  
- **Multipath—Múltiples rutas:** Constituye como una de las causas principales por las que se dan los problemas de recepción en transmisiones en radiofrecuencia. Esto es debido a reflexiones que experimenta la señal en su recorrido hasta el receptor, lo cual ocasiona que la potencia de la señal original se divida tomando diferentes rutas hasta el receptor y por lo tanto se debilite.
  
- **Roaming—Vagabundeo:** Permite que el Cliente se desplace por un área cubierta de AP's de la misma red, sin que pierda conexión a la misma.
  
- **Cliente:** Dispositivo físico ó *software* instalado en un equipo remoto (*handheld*, PC), que permite establecer la comunicación entre el AP y el dispositivo. En este caso se le llama Cliente a la tarjeta de red inalámbrica que utilizan las PC's (ACU).
  
- **Nivel de penetración de la señal:** Cantidad de potencia proveniente de una señal de radiofrecuencia, que puede atravesar paredes u otros materiales. Este valor va a depender tanto de la frecuencia de la señal incidente como del valor de  $\lambda$  del material que la obstaculiza.

- **Antenna diversity —Diversidad de Antena:** Método utilizado para disminuir las pérdidas por [multipath](#). Esta técnica consiste en colocar dos antenas pertenecientes a un mismo equipo, dirigidas a cubrir una misma área determinada dentro de un edificio. La diversidad de antena puede ser comparada a un conmutador que selecciona una u otra antena, nunca ambas al mismo tiempo. La interfaz de radiofrecuencia en modo recepción, continuamente conmutará entre las antenas escuchando por un paquete válido. Después de escuchar el paquete de sincronización válido, esta interfaz evaluará la señal de sincronización del paquete en una antena, y luego conmutando a la otra para evaluar la mejor antena para que pueda recibir el resto del paquete.  
Durante la transmisión, la interfaz de radiofrecuencia seleccionará la misma antena utilizada la última vez que se comunicó. Si se da un fallo en la transmisión del paquete, el AP conmutará al otro puerto para transmitir por la otra antena.  
Debe tomar en cuenta que el AP no está diseñado para utilizar ambas antenas al mismo tiempo. Por lo tanto, a la hora del diseño con equipos en RF, se debe asegurar que ambas antenas cubran la misma área, con una pequeña diferencia de separación horizontal entre ellas.  
Esto ya que si la antena #1 está comunicándose con el dispositivo #1, mientras el #2 intenta comunicarse con el dispositivo #2, la comunicación fallará en este último ya que la antena #2 no está conectada (Debido a la posición del *Switch*).
- **Sensibilidad Mínima de Recepción:** Mínimo nivel de la potencia de una señal (en dBm ó mW) que el receptor necesita para decodificar la información. En el caso de los AP's y Clientes de la serie *Aironet*, este valor corresponde a -95 [dBm].
- **Sensibilidad Máxima de Recepción (saturación):** Máximo nivel de la potencia de una señal (en dBm ó mW) que el receptor necesita para decodificar la información. En el caso de los AP's y Clientes de la serie *Aironet*, este valor corresponde -45 [dBm].

## **LISTA DE ABREVIATURAS**

**AP:** Punto de Acceso ó *Access Point*

**AP's:** Plural de AP

**Tx:** Transmisor (emisor)

**Rx:** Receptor

**mW:** Unidad de medición de potencia denominada Miliwatts.

**dBm:** Unidad de medición de potencia denominada dBm.

**dBd:** Potencia en dB's referida a antena Dipolo teórica.

**dBi:** Potencia en dB's referida a antena Isotrópica (Omnidireccional) teórica.

**EIRP:** Abreviatura del idioma inglés referente a *Effective Isotropic Radiated Power* (Potencia Isotrópica Radiada Efectiva). Corresponde a la potencia efectiva ó total que sale de la antena. Este valor es utilizado como referencia por las agencias reguladoras FCC y ETSI para normar acerca de los límites de potencia permitidos en aplicaciones tales como los utilizados en la banda de ISM (banda en que operan los AP's).

**RSSI (*Received Signal Strength Indicator*):** Indicador de la fortaleza con que llega la señal al receptor. Este valor es desplegado en dBm, el cual corresponde a una unidad de potencia.

## **ANEXOS**

## B.1. EQUIVALENCIA ENTRE MODELO OSI PARA REDES INALÁMBRICAS VRS ALAMBRADAS

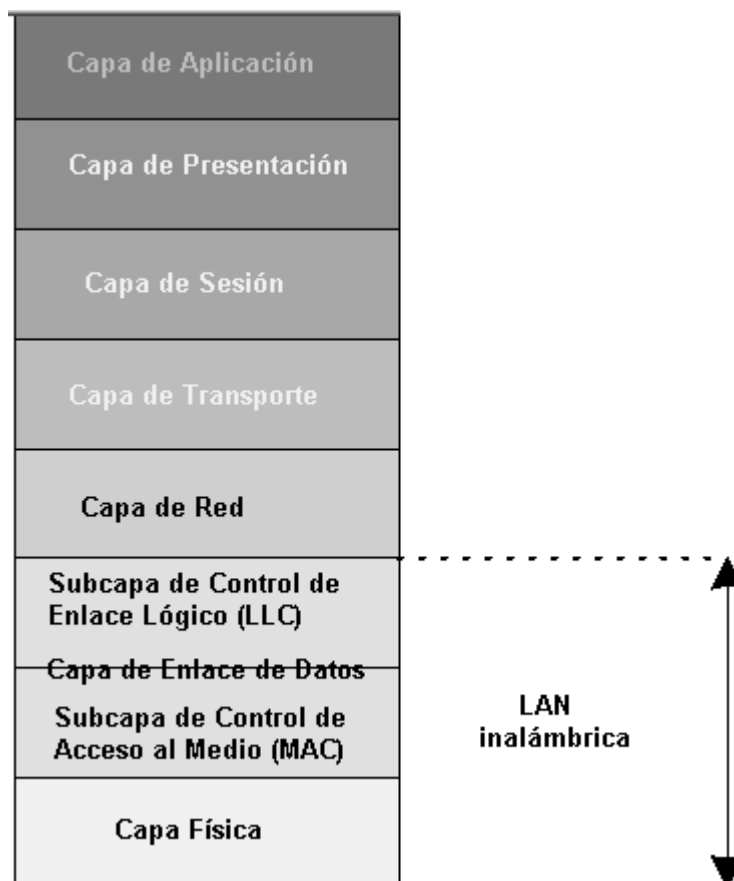


Figura B.1.1 Equivalencia en el Modelo OSI entre red Inalámbrica Vrs Alámbrada

## B.2. CONEXIONES NECESARIAS PARA CONFIGURAR AP

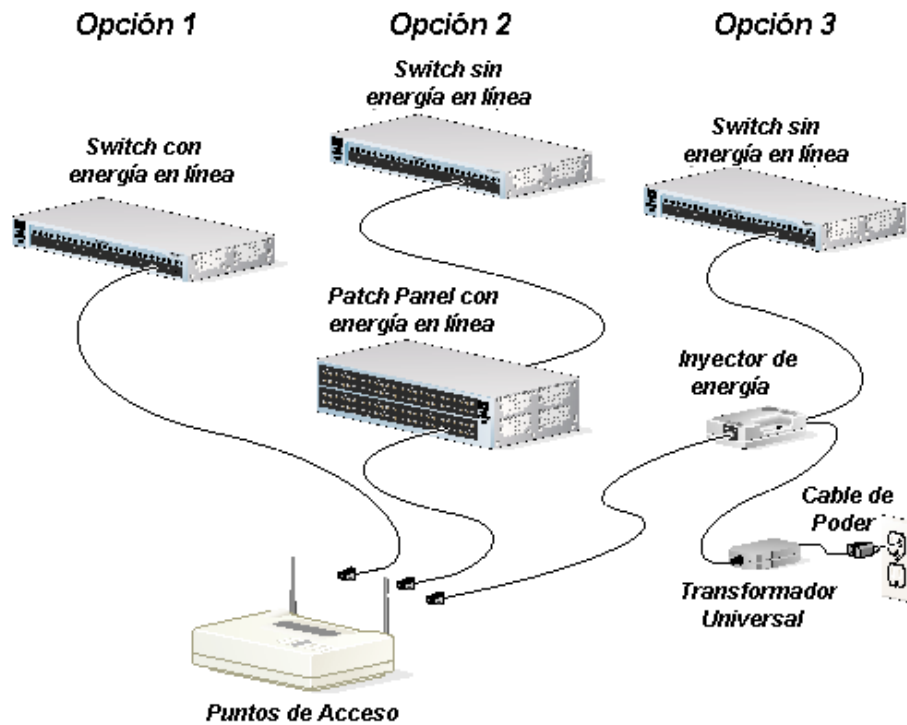


Figura B.2.1 Opciones de conexión de la alimentación al AP

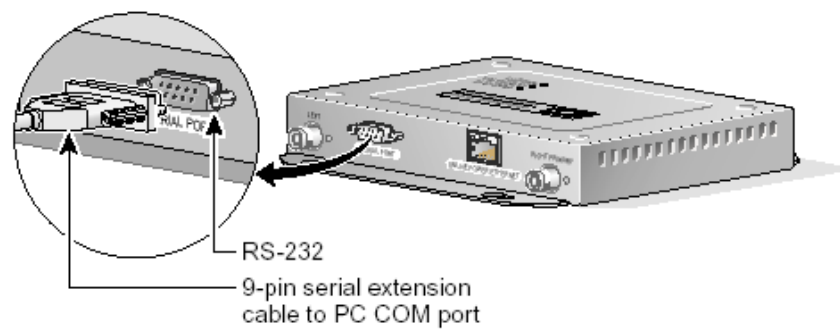
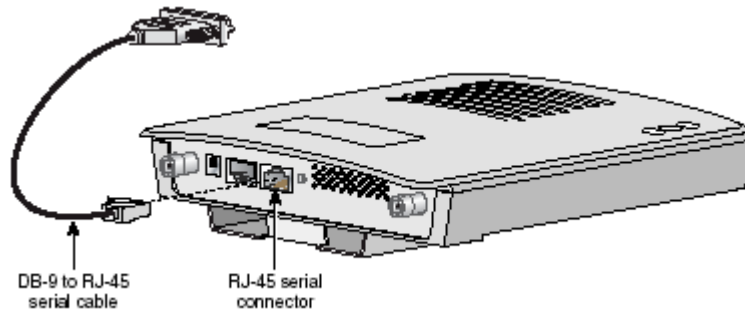


Figura B.2.2 Conexión de cable serie DB-9 a DB-9, para configuración del AP



**Figura B.2.3** Conexión de cable serie DB-9 a RJ-45, para configuración del AP



### B.3. TIPOS DE COBERTURA DE UNA ANTENA

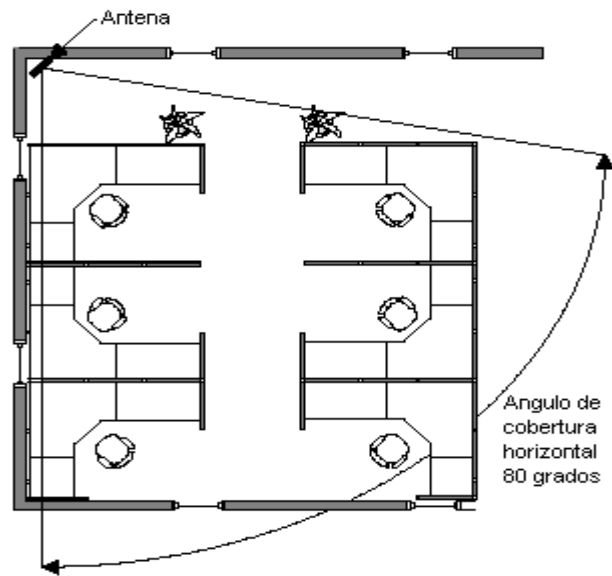


Figura B.3.1 Cobertura horizontal de una antena

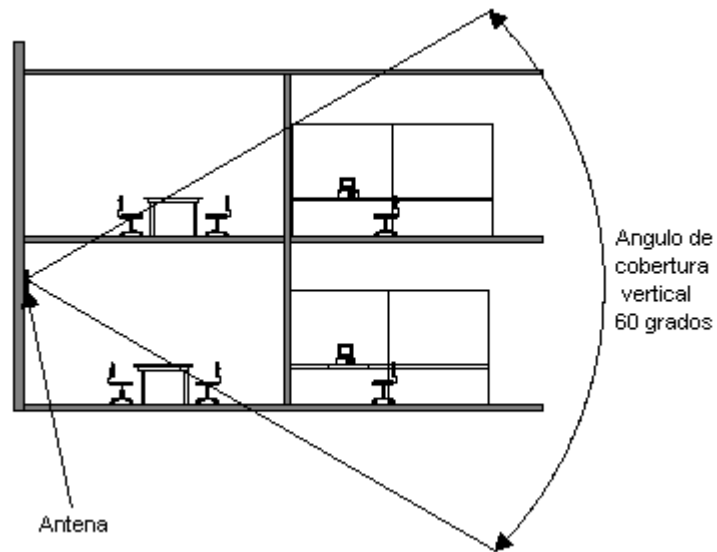


Figura B.3.2 Cobertura vertical de una antena

## B.4 COMPARACIÓN ENTRE ESTÁNDARES DE COMUNICACIÓN INALÁMBRICOS

<h1>Why Choose? A vs B vs G</h1> <h2>Wireless Technology Comparison Chart</h2>						
Wireless Standard	802.11b		802.11a		802.11g	
Popularity		Widely adopted. Readily available everywhere.		New technology.		New technology with rapid growth expected.
Speed	<b>11 Mbps</b>	Up to 11Mbps (note: cable modem service typically averages no more than 4 to 5Mbps).	<b>54 Mbps</b>	Up to 54Mbps (5X greater than 802.11b).	<b>54 Mbps</b>	Up to 54Mbps (5X greater than 802.11b).
Relative Cost		Inexpensive.		Relatively more expensive.		Relatively inexpensive.
Frequency	<b>2.4 GHz</b>	More crowded 2.4GHz band. Some conflict may occur with other 2.4GHz devices like cordless phones, microwave ovens, etc.	<b>5 GHz</b>	Uncrowded 5GHz band can coexist with 2.4 GHz networks without interference.	<b>2.4 GHz</b>	More crowded 2.4GHz band. Some conflict may occur with other 2.4GHz devices like cordless phones, microwave ovens, etc.
Range		Good Range. Typically up to 100-150 feet indoors, depending on construction, building materials, room layout.		Shorter range than 802.11b & 802.11g. Typically 25 to 75 feet indoors.		Good Range. Typically up to 100-150 feet indoors, depending on construction, building materials, room layout.
Public Access		The number of public "hotspots" is growing rapidly, allowing wireless connectivity in many airports, hotels, college campuses, public areas, and restaurants.		None at this time.		Compatible with current 802.11b hotspots (at 11Mbps). Also, it is expected that most 802.11b hotspots will quickly convert to 802.11g.
Compatibility	<b>OK</b> 802.11b	Widest adoption.	<b>OK</b> 802.11a	Incompatible with 802.11b or 802.11g.	<b>OK</b> 802.11b 802.11g	Interoperates with 802.11b networks (at 11Mbps). Incompatible with 802.11a.

Figura B.4.1 Comparación entre estándares de comunicación inalámbricos