ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

DISEÑO Y PRUEBAS DE CAMPO DE UNA RED LAN INALÁMBRICA PARA LA EMPRESA ELÉCTRICA QUITO S.A. (CAMPUS EL DORADO) , EMPLEANDO EL ESTÁNDAR IEEE802.11G

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

ALVARO SANTIAGO CADENA PINARGOTE

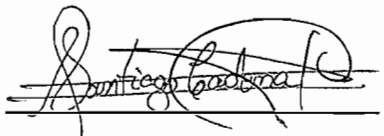
DIRECTOR: Ing. Fernando Flores

Quito, Agosto 2005

DECLARACIÓN

Yo Alvaro Santiago Cadena Pinargote, declaro que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional, puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.



Alvaro S. Cadena P.

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Alvaro Santiago Cadena Pinargote, bajo mi supervisión.

Ing. Fernando Flores
DIRECTOR DEL PROYECTO

AGRADECIMIENTOS

A mi tutor Ing. Fernando Flores por su constante apoyo en la realización de este proyecto.

A mis profesores, por haberme enseñado sus conocimientos y valores a lo largo de mi vida estudiantil.

A la Empresa Eléctrica Quito S.A., Ing. Miguel Araujo, Ing. Bolívar Ortiz, y todos quienes han depositado su confianza, apoyo y amistad.

DEDICATORIA

A Dios sobre todas las cosas, por haberme dado la oportunidad de existir como persona.

A mis padres por haberme dado la vida, ejemplo, amor y cuidado, así como a mis hermanos por su confianza y cariño.

A mi amada esposa Elizabeth, por su amor y comprensión.

A mi hija Jessica, mi muñequita preciosa el amor es para ti.

CONTENIDO

LISTA DE FIGURAS

RESUMEN

El presente trabajo implementa el diseño de una red LAN inalámbrica y sus respectivas pruebas de campo para la Empresa Eléctrica Quito S.A., campus el Dorado, empleando el estándar IEEE 802.11g.

Se realiza una introducción al estándar de comunicaciones inalámbricas IEEE 802.11g, se estudia cómo se produce la evolución en cuanto a cambios que se ha dado desde su estándar inicial IEEE 802.11, pasando por IEEE 802.11b, 802.11a y finalmente 802.11g.

Se determina como se encuentra el estado actual de la red del campus El Dorado, los requerimientos para la realización del diseño, y se describe un procedimiento de diseño y unas políticas de seguridad.

Se realiza el estudio e implementación de seguridad inalámbrica en el diseño de la red, posteriormente se determinan los productos existentes en el mercado y se selecciona un grupo de equipos.

Del diseño se procede a la realización de las pruebas de campo en el lugar con la finalidad de ajustar el mismo, establecer áreas de cobertura de una red de 54 Mbps, niveles de potencia, canales, y determinar correcciones.

En el diseño se considera la inclusión de opciones de seguridades necesarias para garantizar la operación de la red minimizando posibles ataques, como son implementación WEP, filtrado MAC, Autenticación LEAP por medio de servidor RADIUS.

PRESENTACIÓN

La incursión de la tecnología inalámbrica ha evolucionado de manera asombrosa en los últimos años, cada vez más empresas incluyen en su infraestructura de comunicaciones redes inalámbricas tanto a nivel de LAN o WAN.

Realizar un diseño inalámbrico involucra varios aspectos pero no es suficiente para implementar una red inalámbrica, y se ve la necesidad de realizar pruebas de campo, para evaluar el terreno y descubrir aspectos que son imposibles considerar en papel.

El aporte más importante a una institución es presentar soluciones y alternativas en cuanto a conectividad en Redes de Información, el avance de nuevas tecnologías así como de estándares es cada vez mayor.

Es por este motivo que se presenta el siguiente trabajo, desarrollado con la finalidad de establecer el diseño y realización de pruebas de campo para la red LAN inalámbrica para la Empresa Eléctrica Quito S.A., inicialmente como proyecto piloto para el campus El Dorado, que servirá de referente para implementación en las demás agencias de la empresa, siempre considerando la seguridad inalámbrica, la cual es un aspecto muy importante en la elaboración de diseños inalámbricos.

Capítulo 1
Introducción a la Red Inalámbrica

1. INTRODUCCIÓN A LA RED INALÁMBRICA

1.1 ESTADO DEL ARTE

El advenimiento vertiginoso de la tecnología, la necesidad de mayores velocidades de conexión, el crecimiento y la creciente necesidad de flexibilidad y escalabilidad en redes inalámbricas han impulsado el desarrollo de nuevas tecnologías inalámbricas como es IEEE 802.11 y el desarrollo de IEEE 802.11b, IEEE802.11a y últimamente el estándar IEEE 802.11g que presenta características combinadas de los 2 anteriores.

Cuando se precisa movilidad en las comunicaciones, el cable se convierte más en un inconveniente que en una ayuda.

Para salvar las restricciones impuestas en la utilización del cable, las conexiones inalámbricas se convierten en la alternativa.

1.1.1 CONSIDERACIONES GENERALES

En redes inalámbricas se deben considerar varios aspectos que afectan y caracterizan su funcionalidad como son:

- Movilidad

  El que se tenga un usuario el cual se pueda trasladar en tiempo real sin perder conectividad ofrece mayor productividad y posibilidades de servicio.

- Facilidad de instalación

  Instalar un usuario inalámbrico es más rápido ya que se evita tirar cable por muros y techos, lo cual no es muy conveniente en muchos casos.

- Flexibilidad

  Una red inalámbrica es más flexible en cuanto a la facilidad de crecimiento de usuarios para adherirse a la red.

- Reducción de costos

  Cuando se dan cambios frecuentes o el entorno es muy dinámico, el costo inicial de la red sin cable es significativamente más bajo.

  Además de tener mayor tiempo de vida y menor costo de instalación.

- Escalabilidad

La incorporación de nuevos estándares da la posibilidad de ser compatibles con estándares anteriores, por ello se define que una red puede ser escalable, así el estándar IEEE 802.11g es compatible con IEEE 802.11b

- Cobertura

Cobertura depende de las características de los equipos y de la arquitectura del sitio. La forma de asegurar cobertura en un lugar es realizando pruebas y verificando que se tienen adecuadas características como potencia de señal, áreas de cobertura, usuarios a ser atendidos, entre otros.

- Desvanecimiento por múltiples trayectorias

Este problema se produce al viajar la señal desde el transmisor al receptor, en el cual la señal se refleja por varias trayectorias y llega por distintos caminos, lo que provoca interferencias en el receptor y provoca un desvanecimiento de la señal.

Teniendo en consideración estos aspectos se entiende cómo una red inalámbrica tiene sus propias características, lo cual ayuda a obtener criterios para el diseño.

1.1.2 USO DE SISTEMAS INALÁMBRICOS

Hoy en día el uso de sistemas inalámbricos es cada vez mayor, existen empresas que se dedican a prestar este tipo de servicio, para garantizar al cliente un nivel de satisfacción de su red, es así que se tienen diversas aplicaciones:

- En hospitales: en el que los datos del paciente deben ser transmitidos de forma instantánea, sin pérdida de tiempo.
- En pequeños grupos de trabajo: que necesiten una puesta en marcha rápida de una red (por ejemplo, grupos de revisión del estado de cuentas, grupos de auditoria de empresas).
- En entornos dinámicos: se minimiza la sobrecarga causada por extensiones de redes cableadas, movimientos de éstas u otros cambios, por ejemplo en empresas privadas, en las cuales los cambios de áreas de trabajo son constantes.

- En centros de formación, universidades, corporaciones, etc., donde se usa red sin cable para tener fácil acceso a la información, intercambiar ésta y aprender.
- En viejos edificios es también más adecuada, ya que el tendido de cables deteriora paredes y acabados.

1.1.3 EVOLUCIÓN DE LOS SISTEMAS INALÁMBRICOS

Desde sus inicios los sistemas inalámbricos tuvieron gran impulso en el ámbito de las comunicaciones ya que ofrecen evidentes ventajas, lo que ha impulsado a empresas fabricantes el deseo de incursionar en este tipo de comunicaciones y adoptar estándares para su comercialización.

En junio de 1997 aparece el estándar IEEE 802.11 con una operación en el rango de frecuencias de 2.4 GHz. y con velocidades originales de 1 y 2 Mbps[1], con la presencia de 3 canales no interferidos para su uso y 11 en total [1].
A finales de 1999 la IEEE publica dos suplementos del estándar: IEEE 802.11a y el estándar IEEE 802.11b.
IEEE 802.11a determina velocidades de hasta 54 Mbps empleando OFDM (Orthogonal Frecuency Division Multiplexing), en la banda de los 5 GHz. permitiendo establecer comunicaciones a mayores velocidades: 6, 9, 12, 18, 24, 36, 48 y 54 Mbps., La regulación de canales para U.S.A., presenta la utilización de 8 canales totales en las bandas baja (U-NII lower band) y media (U-NII middle band), y presenta la utilización de 4 canales en la banda alta (U-NII upper band) [7]. IEEE 802.11b permite conseguir velocidades superiores al estándar de 802.11, operando en la banda de 2.4 GHz y alcanzando velocidades de hasta 11 Mbps.

En junio del 2003 aparece un estándar relativamente nuevo, IEEE 802.11g el cual permite velocidades de hasta 54 Mbps en la misma banda de IEEE 802.11b (2.4 GHz).
Se puede apreciar la evolución de estándares en la siguiente tabla comparativa.

Tabla 1.1 Evolución de estándares [4]

802.11	802.11a	802.11b	802.11g
Julio 1997	Septiembre 1999	Septiembre 1999	junio 2003
83.5 MHz	300 MHz	83.5 MHz	83.5 MHz
2.4-2.4835 GHz DSSS, FHSS	5.15-5.35 GHz OFDM 5.725-5.825Ghz OFDM	2.4-2.4835GHz DSSS	2.4-2.4835GHz DSSS OFDM
3 canales no interferidos	4 canales no interferidos	3 canales no interferidos	3 canales no interferidos
2, 1 Mbps	54, 48, 36, 24, 18, 12, 9, 6 Mbps	11, 5.5, 2, 1 Mbps	54, 36, 33, 24, 22, 12, 11, 9, 6, 5.5, 2, 1 Mbps
DQPSK (2 Mbps DSSS) DBPSK (1 Mbps DSSS) 4GFSK (2Mbps FHSS) 2GFSK (1Mbps FHSS)	BPSK (6, 9 Mbps) QPSK (12, 18 Mbps) 16-QAM (24,36 Mbps) 64-QAM (48,54 Mbps)	DQPSK/CCK (11, 5.5 Mbps) DQPSK (2 Mbps) DBPSK (1 Mbps)	OFDM/CCK (6,9, 12,18,24,36,48,54) OFDM (6,9,12,18, 24,36,48,54) DQPSK/CCK (22, 33, 11, 5.5 Mbps) DQPSK (2 Mbps) DBPSK (1 Mbps)
Compatible 802.11	No Compatible	Compatible Wi-Fi	Wi-Fi a 11Mbps o mas bajo

Últimamente el estándar 802.11i, tiene como meta otorgar a los estándares IEEE 802.11a, b y g características robustas de seguridad. Esto implica compatibilidad con el estándar 802.1x e integración con AES[1].

Así por otro lado se creó HIPERLAN (*High Performance Radio LAN*) para redes inalámbricas, publicado en 1996, el cual fue desarrollado por la ETSI (*European Telecommunications Standards Institute*). Especifica una operación a 5 Ghz con velocidades sobre los 20 Mbps. Luego se desarrolla HIPERLAN/2 para operar en la banda de los 5 Ghz con velocidad de 54 Mbps. Se diseña para llevar celdas ATM[2], paquetes IP y voz digital, para lo cual provee calidad de servicio (QoS) y garantía de ancho de banda [5].

[1] Advanced Encryption Standard
[2] Asynchronous Transfer Mode

1.1.4 TOPOLOGÍAS DE RED INALÁMBRICA

Una topología de red inalámbrica está fundamentada en la arquitectura IEEE 802.11 cuyo concepto es celdas WLAN, o BSS3. 802.11 soporta la formación de dos diferentes tipos de BSSs. El primero llamado "topología ad hoc", y el segundo es "topología de Infraestructura", como se verá mas adelante.

1.2 TIPOS DE SISTEMAS INALÁMBRICOS

Un sistema completo de comunicación inalámbrica constituyen equipos que permiten la conectividad entre computadores con un interfaz de aire, de acuerdo a la especificación de un estándar. Un sistema inalámbrico se agrupa de acuerdo al tipo de conectividad que presentan los equipos, así como tu topología sea esta de Infraestructura o Ad-Hoc.

1.2.1 CONECTIVIDAD DE USUARIO MÓVIL

En este esquema se tienen como equipos de conectividad, un usuario móvil por ejemplo una laptop, un punto de acceso AP que interactúa con la red cableada.

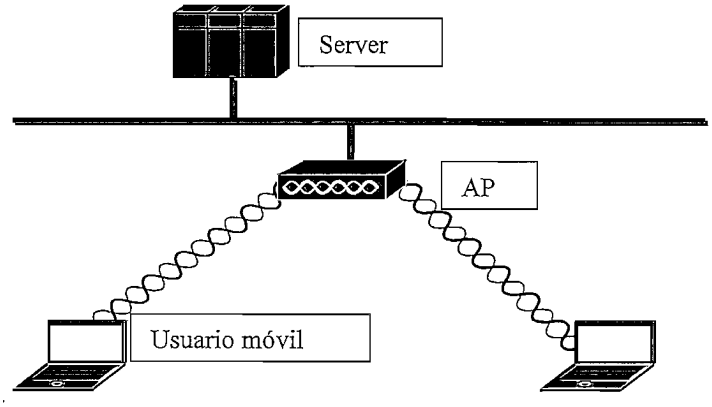


Figura 1.1.- Conectividad Usuario Móvil [10]

Este esquema se indica en la figura 1.1 y es comúnmente empleado en empresas privadas ya que el uso de usuarios móviles agilita las actividades y el recurso tiempo es primordial.

[3] Grupo de Servicios Básicos

1.2.2 CONECTIVIDAD DE LAN A LAN

En este esquema se comunican dos redes LAN entre edificios mediante antenas, es una estructura llamada *Building to Building* como indica la Figura1.2.

En su conectividad intervienen factores como propagación, línea de vista, atenuación, e interferencias.

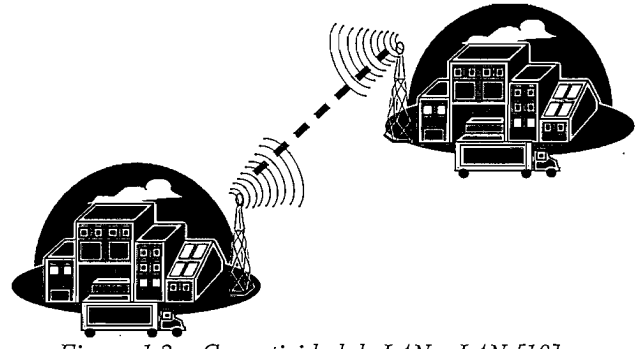


Figura 1.2.- Conectividad de LAN a LAN [10]

1.2.3 WLAN COMO UNA EXTENSIÓN DE UNA LAN CABLEADA

En este esquema se tienen diversos elementos de una red cableada como son servidores, equipos de trabajo, servidor de impresión, los cuales interactúan con la red inalámbrica mediante un AP. Este esquema se muestra en la Figura1.3 la cual es mayormente empleada en empresas corporativas de mayor tamaño, las cuales tienen entre su infraestructura estos elementos que requieren comunicarse e interactuar.

Si el ambiente es dinámico, y el crecimiento de usuarios se incrementa, es conveniente hacer una extensión de red cableada mediante medios inalámbricos.

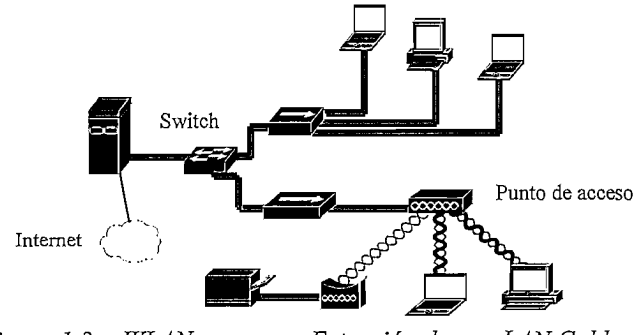


Figura 1.3.- WLAN como una Extensión de una LAN Cableada[10]

1.2.4 CONFIGURACIONES DE WLAN

La configuración determina la topología que va a tener la red, esta puede ser muy sencilla o elevar su complejidad. Tenemos las siguientes configuraciones

- Igual a Igual (peer to peer).
- Cliente y punto de acceso.
- Multipunto de acceso, roaming y extensiones.

La selección de este tipo de configuraciones depende de criterios y necesidades, como por ejemplo:

Rendimiento que se requiere, funcionalidad que va a tener, su ámbito de aplicación, seguridad requerida, capacidad de desplazamiento de los nodos, entre otros.

1.2.4.1 Configuración Igual a Igual

Constituyen dos ordenadores equipados con tarjetas adaptadoras para WLAN, de modo que pueden poner en funcionamiento una red independiente siempre que estén dentro del área que cubre cada uno.

Cada cliente tendría únicamente acceso a los recursos de otro cliente pero no a un servidor central.

Este tipo de redes no requiere administración o preconfiguración. El esquema descrito se indica en la Figura1.4.

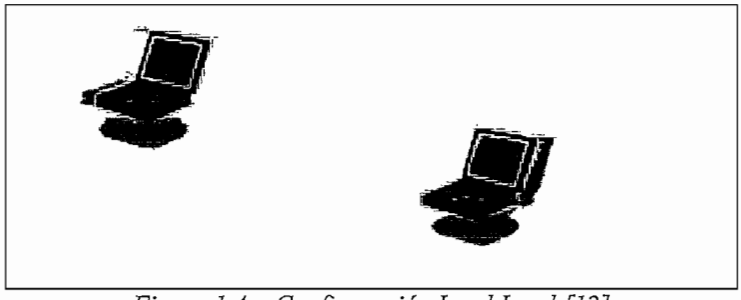


Figura 1.4.- Configuración Igual Igual [12]

1.2.4.2 Configuración Cliente - Punto de Acceso

Instalando un Punto de Acceso (AP) se puede doblar el rango al cuál los dispositivos se pueden comunicar, pues actúa como repetidor.

Cuando el punto de acceso se conecta a la red cableada, cualquier cliente tiene acceso a los recursos del servidor y además actúa como mediador en el tráfico de la red en la vecindad más inmediata.

La Figura 1.5 muestra esta configuración.

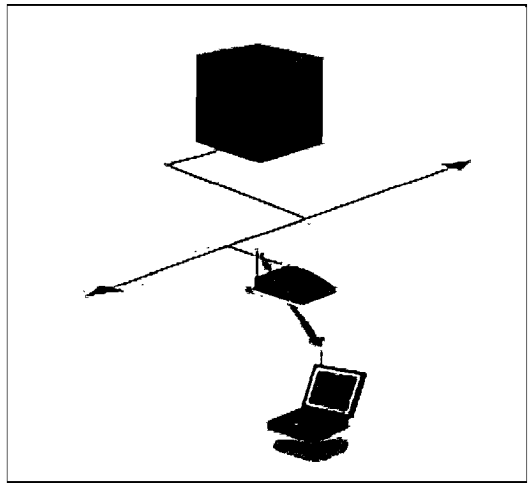


Figura 1.5.- Configuración Cliente - Punto de Acceso [12]

Cada punto de acceso puede servir a varios clientes, según la naturaleza y número de transmisiones que tienen lugar.

Existen muchas aplicaciones en el mundo real con entre 15 y 50 dispositivos cliente en un solo punto de acceso.

1.2.4.3 Configuración Multipunto de Acceso

Los puntos de acceso tienen un rango finito, del orden de 100m en interiores y 200m en exteriores, dependiendo del equipo y de otras condiciones. En zonas grandes como por ejemplo un campus universitario o un edificio es probablemente necesario más de un punto de acceso.

La meta es cubrir el área con celdas que solapen sus áreas, de modo que los clientes puedan moverse sin cortes entre un grupo de puntos de acceso. Esto es llamado "roaming". Este esquema es mostrado en la Figura 1.6.

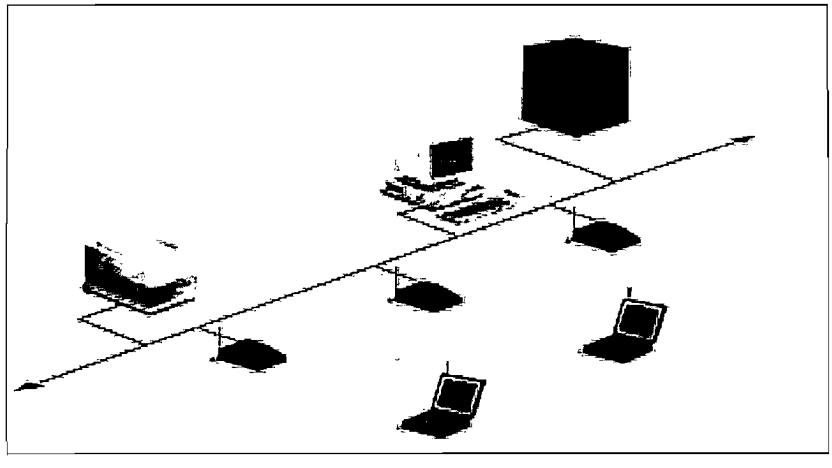


Figura 1.6.- Configuración Multipunto de Acceso [12]

1.2.4.4 Configuración con Puntos de Extensión

Para resolver problemas particulares de topología, el diseñador de la red puede elegir usar un Punto de Extensión (EP) para aumentar el número de puntos de acceso a la red, de modo que funcionan como tales pero no están enganchados a la red cableada como los puntos de acceso.

Los puntos de extensión funcionan como su nombre indica extendiendo el rango de la red retransmitiendo las señales de un cliente a un punto de acceso o a otro punto de extensión.

Los puntos de extensión pueden encadenarse para pasar mensajes entre un punto de acceso y clientes lejanos de modo que se construye un "puente" entre ambos, este esquema se indica en la figura 1.7.

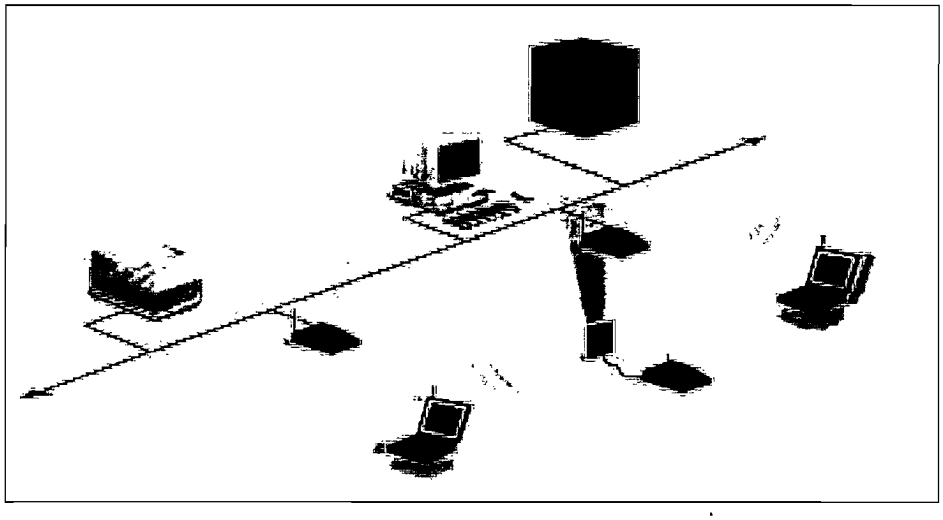


Figura 1.7.- Configuración con Puntos de Extensión [12]

1.3 ESTÁNDAR IEEE 802.11 PARA WLAN

La designación oficial del estándar es: *IEEE Standard for Wireless LAN Medium Access (MAC) and Physical Layer (PHY) Specifications.*

Tiene como finalidad definir un mecanismo de control de acceso al medio MAC y especificaciones de capa física para interconexión inalámbrica de estaciones fijas, móviles y portables dentro de una área local.

1.3.1 HISTORIA DEL ESTÁNDAR

LANs inalámbricas tienen una amplia gama de estándares y especificaciones para redes así como para WPAN tales como:

- IEEE 802.11
- HiperLAN
- Home RF SWAP
- Bluetooth

IEEE 802.11 es uno de los más populares, opera en la banda de 2.4Ghz con velocidades de 1 y 2 Mbps, con 3 medios físicos, DFIR, FHSS, y DSSS. En 1999 se publican dos suplementos al estándar, IEEE 802.11b y el IEEE 802.11a
IEEE 802.11b en la banda de 2.4Ghz con hasta 11Mbps y IEEE 802.11a en la banda de 5 GHz con hasta 54 Mbps, y posteriormente IEEE 802.11g, el cual opera en la banda de 2.4 GHz y permite conseguir velocidades de hasta 54 Mbps, garantizando compatibilidad con IEEE 802.11b.

1.3.2 TOPOLOGÍAS

Dentro del estándar 802.11 se definen las dos topologías Ad Hoc y de Infraestructura.

1.3.2.1 Descripción de Topología Ad Hoc

Una topología Ad Hoc es creada y administrada sin la necesidad de un control central o de un punto de acceso inalámbrico, la red se crea por los dispositivos que se adhieren al BSS, generalmente se forma una red de este tipo con la finalidad de intercambiar datos entre los dispositivos, por ejemplo transferir un archivo desde una computadora personal a otra.
En la modalidad Ad Hoc sólo hay dispositivos inalámbricos presentes, por lo que la señalización debe ser controlada por las estaciones.

Al área que sirve un BSS se le denomina el Área de Servicios Básicos (BSA), en el caso de existir solamente dispositivos inalámbricos dentro de un BSS éste se denomina IBSS[4]. Este esquema se lo aprecia en la Figura1.8

[4] Grupo de Servicios Básicos Independiente

1.3.2.2 Descripción de Topología Infraestructura

Una red inalámbrica con esta topología está formada por dispositivos de red que se interconectan entre sí por medio de un punto de acceso (AP), siendo éste el que interactúa con la red cableada y por tanto une las 2 redes, la red cableada con la inalámbrica.

Un AP tiene un área de cobertura lo cual determina al BSS, los dispositivos que se encuentren dentro del BSS se identifican, estarán en la capacidad de autenticarse, posteriormente asociarse, e intercambiar información con los demás equipos conectados al AP, este procedimiento se realiza mediante tareas de señalización de los AP por parte de las estaciones móviles.

El AP tiene la función de coordinar tanto la transmisión como la recepción de datos de las estaciones.

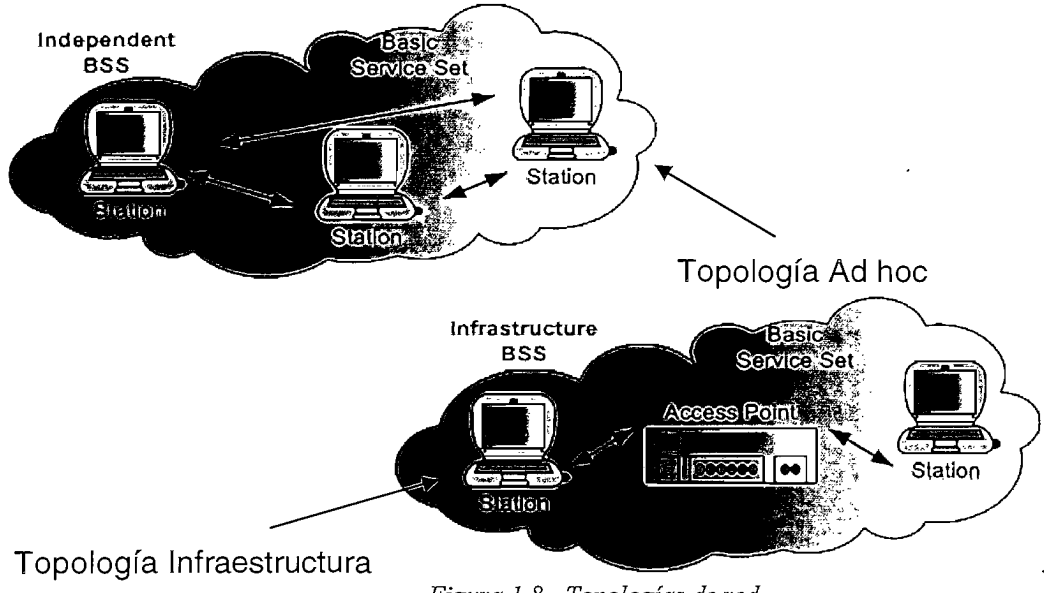


Figura 1.8.- Topologías de red

Los BSS definen el grupo de servicios básicos de un área de cobertura, y se identifica un identificador del grupo de servicios SSID (*Service Set Identifier*), que determina el dominio o nombre de la WLAN.

Al área que sirve un BSS se le denomina el Área de Servicios Básicos (BSA), en el caso de existir solamente dispositivos inalámbricos dentro de un BSS éste se denomina IBSS.

Dentro del estándar se define que los BSSs se pueden conectar a través del sistema de distribución (DS), lo que genera la formación de los ESS[5]

1.3.3 802.11 CAPA FÍSICA (PHY)

La capa física provee de servicios a la subcapa MAC de IEEE 802.11. Se definen diferentes capas físicas (PHY) como parte del estándar. La capa física tiene 2 subcapas cuyas principales funciones están dadas por Procedimiento de Convergencia de Capa Física (PLCP) y Capa Dependiente del medio físico (PMD).

Capas superiores son encapsuladas en capas inferiores como se muestra en la Figura 1.9.

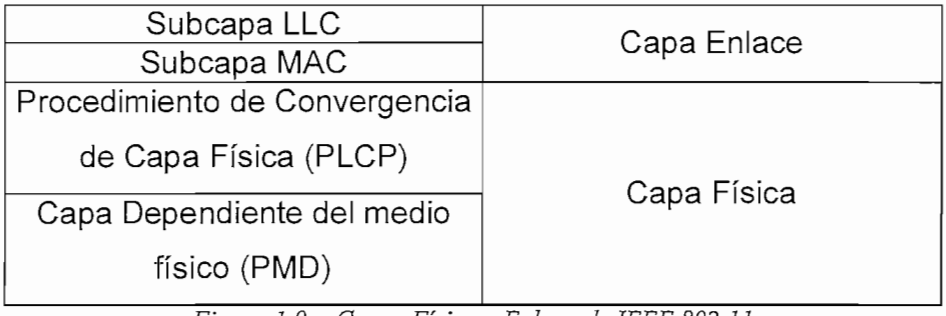


Figura 1.9.- Capas Física y Enlace de IEEE 802.11

1.3.3.1 802.11 Subcapa PLCP

PLCP tiene una función de convergencia a la capa física, adapta las mejores capacidades a la subcapa PMD (*Physical Medium Depend*). Define un método para adecuar las unidades de datos MPDUs (*MAC Protocol Data Units*) en un formato de trama adecuado para el envío y recepción de datos del usuario, e información de administración entre dos o más estaciones usando la subcapa PDM. La Figura 1.10 muestra como se forma la subcapa PLCP.

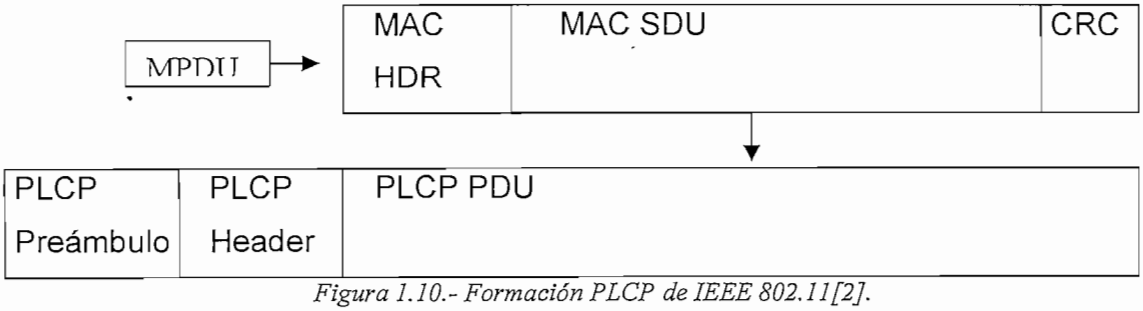


Figura 1.10.- Formación PLCP de IEEE 802.11[2].

[5] Grupo de Servicios Extendidos

Cada MPDU se encapsula en la trama PLCP que contiene 3 campos:
Preámbulo PLCP formado por los campos Sincronización y Delimitador de Inicio de Trama. Cabecera PLCP formado por Servicio, Longitud y CRC. El campo de PLCP PDU corresponde a la MPDU encapsulada como datos.

Preámbulo PLCP.

Está formado por 2 subcampos: Sincronización (Sync) y Delimitador de Inicio de Trama (SFD), es empleado para sincronización e inicio de trama, es transmitido a 1 Mbps.

- Sincronización (*Sync*).- Este campo es de 128 bits, es empleado para que el receptor desarrolle operaciones adecuadas para su sincronización.
- Delimitador de Inicio de Trama (SFD).- Este campo es provisto para indicar el inicio de trama.

Cabecera PLCP.

Contiene información acerca de velocidad de transmisión, inicialización, longitud de trama y CRC, contiene los campos Señalización (*Signal*), Servicio (*Service*), Longitud (*Length*), CRC (*FCS*).

- Señalización (*Signal*).- Este campo consta de 8 bits, es provisto para indicar el esquema de modulación empleado en transmisión y recepción. La velocidad conseguida será el valor de este campo multiplicado por 100 Kbps. Se define en DSSS PHY dos modulaciones obligatorias dadas por las siguientes palabras de 8 bits en este campo.

  a) 0Ah para 1 Mbps DBPSK
  b) 14h para 2 Mbps DQPSK

- Servicio (*Service*).- Este campo es de 8 bits y será reservado para uso futuro. El valor de 00h indicará que el dispositivo cumple con el estándar IEEE 802.11
- Longitud (*Length*).- Este campo es un entero de 16 bits sin signo que nos indica el número de microsegundos que se requieren para la transmisión.

- CRC (CCITT CRC-16).- Los campos Señalización, Servicio, Longitud son protegidos por un CRC de 16 bits, empleando el polinomio $x^{16}+x^{12}+x^5+1$.

Campo de Datos PDU-PLCP

Este campo es de longitud variable y contiene a la MPDU[6]. En un medio físico DSSS, el preámbulo PLCP, la cabecera PLCP, y el campo de datos MPDU forman la trama PLCP (PPDU), este esquema es mostrado en el formato de trama PLCP de la Figura 1.11.

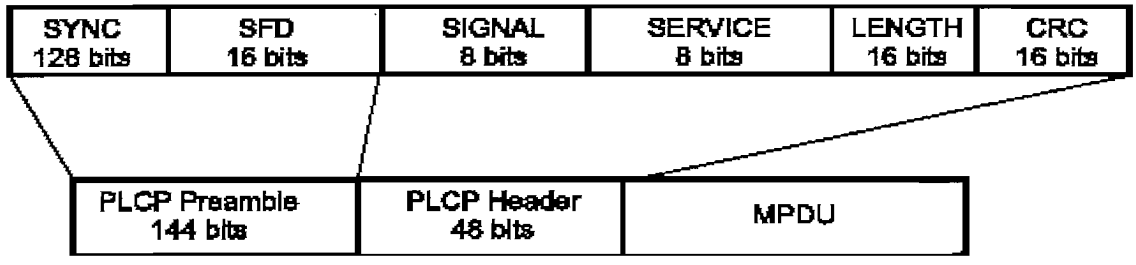


Figura 1.11.- Formato de la Trama PLCP 802.11 [2]

El preámbulo PLCP consta de 144 bits denominado Preámbulo grande (*Long Preamble*).

En el medio físico FHSS el formato de trama es el que se indica en la figura 1.12

Preambulo PLCP		Cabecera PLCP			PSDU
Sync	Start Frame Delimiter	PLW	PSF	Header Error Check	
80 bits	16 bits	12 bits	4 bits	16 bits	número de octetos variable

Figura 1.12.- Formato de trama en FHSS

En el medio físico Infrarrojo IR la trama es el que se indica en la figura 1.12

Preambulo PLCP		Cabecera PLCP				PSDU
SYNC	SFD	DR	DCLA	LENGTH	CRC	
57-73 slots	4 slots	3 slots	32 slots	16 bits	16 bits	numero variable de octetos

Figura 1.13.- Formato de trama PCLP IR

[6] Corresponde a la trama MAC, como datos para PLCP

1.3.3.2 Subcapa PMD

Esta subcapa PMD, tiene funciones que definen las características y métodos de transmisión y recepción de datos a través de un medio inalámbrico entre dos estaciones.

Los servicios de capas inferiores se proveen a la subcapa MAC de una estación mediante puntos de acceso al servicio SAP indicados en la figura 1.14 que se encuentran entre las subcapas PMD, PLCP y MAC y son administradas por una subcapa de administración MLME.

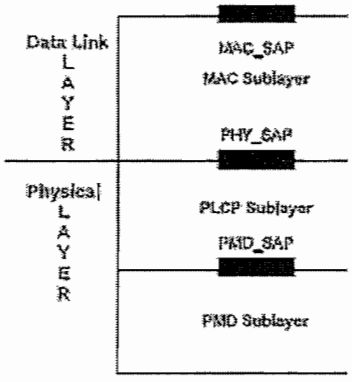


Figura 1.14.- Puntos de acceso al servicio SAP de 802.11[2]

Dentro del estándar se definen mecanismos para conseguir el acceso al medio físico, estas técnicas de acceso pueden ser por medio de Infrarrojos DFIR , FHSS (*Frequency Hopping Spread Spectum*) y DSSS (*Direct Sequence Spread Spectum*).

1.3.3.3 Infrarrojos

Este medio inalámbrico referido a capa física requiere la existencia de línea de vista entre los dos puntos, es usado en ambientes interiores ya que no atraviesa paredes, por este requerimiento no ha sido muy difundido. Logra velocidades de 1 y 2 Mbps, denominadas *basic access rate* y *enhanced access rate* respectivamente.

La modulación empleada por esta capa física es modulación 16-PPM[7] para 1 Mbps y 4-PPM para lograr 2 Mbps.

[7] Modulación por posición de pulsos

Para lograr 1 Mbps se utilizan palabras de 4 bits a 16 bits que se codifican con el código de Gray[8], esto genera palabras de 16 bits con quince ceros y un uno. Para lograr 2 Mbps se utilizan palabras de 2 bits a 4 bits que se codifican con el código de Gray, esto genera palabras de 4 bits con tres ceros y un 1 [5].

1.3.3.4 Salto de Frecuencia (FHSS)

La técnica de modulación Salto de Frecuencia (*Frecuency Hopping Spread Spectrum*) asigna frecuencias que van cambiando de acuerdo a un patrón de saltos, es así que tanto el transmisor como el receptor deben estar sincronizados para lograr una transmisión exitosa. Presenta velocidades de 1 y 2 Mbps, emplea un generador de números pseudo-aleatorios para cambiar a un canal de transmisión.

Tiene 72 canales en la banda de 2.4 GHz. con un ancho de 1MHz cada uno. El tiempo de utilización de un canal de frecuencia es variable, pero no mayor a 400 ms, es empleado en WPAN[9] con tecnología Bluetooth que permite la conexión inalámbrica de monitores, teclados, escáneres y cualquier periférico sin la necesidad de llenar de cables el sitio de trabajo. Las WPAN´s llegan a velocidades de 1 Mbps.

1.3.3.5 Secuencia Directa (DSSS)

*La t*écnica de modulación de espectro disperso en secuencia directa (*Direct Sequence Spread Spectrum*) emplea dos técnicas de modulación, modulación de intercambio de fase con dos estados DBPSK(*differential binary phase shift keying*) y modulación de intercambio de fase en cuadratura con 4 estados DQPSK (*differential quadrature phase shift keying*) para lograr velocidades de 1 y 2 Mbps respectivamente, emplea 11 chips para representar un bit mediante la secuencia de Barker (vea sección 1.3.6).

---

[8] Codificación con el menor número de transiciones posibles

[9] Redes inalámbricas de área personal.

1.3.4 802.11 SUBCAPA MAC

La subcapa MAC permite el control del acceso al medio mediante mecanismos que garantizan que el acceso al medio físico sea el adecuado para la transmisión de datos.

Dentro de la arquitectura MAC se definen Funciones de Coordinación que determinan cuando una estación en un BSS puede transmitir y cuando puede recibir información.

Se disponen de 2 funciones: Función de Coordinación Distribuida (DCF) y Función de Coordinación Puntual (PCF).

1.3.4.1 Función de Coordinación Distribuida DCF

Esta función de coordinación permite la transmisión de datos asíncronos de unidades de datos MAC empleando el método del mejor esfuerzo [3]. Al emplear DCF se opera en modo de contención empleando el protocolo CSMA/CA acceso múltiple con detección de portadora con prevención de colisiones, y es empleado generalmente en redes Ad Hoc, aunque puede ser empleado en redes de infraestructura.

1.3.4.2 Función de Coordinación Puntual PCF

En este tipo de coordinación se tiene un control centralizado desde una estación base sobre toda su área de cobertura (celda) [5]. La estación base pregunta a las estaciones si tienen datos que transmitir mediante un sondeo. Como la estación base asigna los permisos de transmisión se evitan las colisiones.

La utilización del medio está controlada por el AP por lo que no existe la lucha por el canal.

1.3.4.3 Tipos de Tramas

Existen tres tipos de tramas a nivel MAC que son: tramas de Administración, tramas de control, y tramas de datos, estos son especificados de acuerdo al campo de control de la trama, que consta en la cabecera MAC.

1.3.4.4 Cabecera MAC

La cabecera MAC contiene campos que proporciona información acerca de control de la trama que indica, duración, direccionamiento y control de secuencia. Como se muestra en la Figura 1.15.

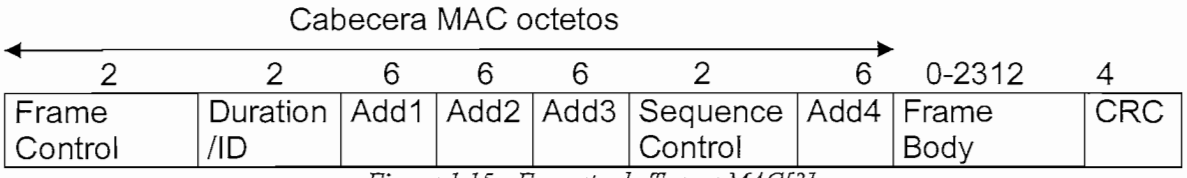


Figura 1.15.- Formato de Trama MAC[3]

1.3.4.4.1. Campo Control de Trama (Frame Control)

El campo de control de la trama especifica el tipo de paquete, para identificar tramas de datos, tramas de control y tramas de gestión.

Consiste de los subcampos mostrados en la Figura 1.16: Protocol Versión, Type, Subtype, To DS, From DS, More Fragments, Retry, Power Management, More Data, Wired Equivalent Privacy (WEP), y Order, que se encuentran especificados en la tabla 1.2.

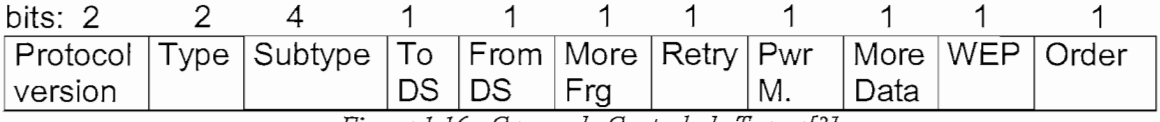


Figura 1.16.- Campo de Control de Trama[3]

Tabla 1.2.- Campos de control de trama [2]

Campos	Descripción
Protocol Versión	Versión del protocolo
Type	Tipo de trama, administración, control o de datos
Subtype	RTS, CTS, etc.
To DS	Trama dirigida al Sistema de Distribución
From DS	Trama desde el Sistema de Distribución
More Fragments	Indica que hay más fragmentos
Retry	Marca que es una trama de retransmisión
Power Management	Administración de potencia de STAs.
More Data	Indica que el emisor tiene más tramas que enviar

Wep	Indica que en el cuerpo de la trama se ha utilizado WEP (*wired equivalency protocol*).
Order	Indica que la secuencia de tramas debe procesarse en orden estricto.

1.3.4.5 Campo Duración

Especifica cuanto tiempo ocupará el canal la trama y su confirmación de recepción. Mediante este campo se maneja el mecanismo de NAV (Vector de asignación a la Red) con tramas de control.

NAV es un indicador, mantenido por cada estación, de períodos de tiempo cuando la transmisión no se ha iniciado debido a que el medio inalámbrico está ocupado.

1.3.4.6 Campos de Direcciones

Estos campos corresponden a las direcciones que intervienen en la comunicación, 2 de ellas son de BSSID (*basic service set identification*) origen y destino, y las 2 restantes son de estaciones.

1.3.4.7 Campo Control de Secuencia

El control de secuencia consta de dos subcampos: Número de Secuencia y Número de Fragmento. El número de secuencia identifica de manera única un MSDU[10] o MMPDU[11], mientras que el número de fragmento lo identifica cuando la trama ha sido fragmentada.

1.3.4.8 Campo Cuerpo de Trama

El cuerpo de la trama contiene la información de la subcapa LLC de nivel superior, la cual se encapsula como datos para la trama MAC.

El Cuerpo de la trama es un campo de longitud variable que contiene información específica de la trama, el tamaño mínimo del cuerpo de la trama es 0 octetos, mientras que el máximo valor es definido por MSDU + ICV + IV, donde ICV e IV son campos definidos de WEP.

[10] MAC Service Data Units
[11] MAC Management Data Units

1.3.4.9 Trailer (CRC)

El trailer contiene una secuencia de comprobación CRC, es un campo de 32 bits, es calculado sobre todos los campos de la cabecera MAC y garantiza el cuerpo de la trama, utiliza un generador polinomial G(x) de grado 32. [2]

1.3.5 SERVICIOS 802.11

IEEE 802.11 explícitamente no especifica el detalle de implementación del DS, en su lugar, IEEE 802.11 especifica servicios[2].

Los servicios son asociados con diferentes componentes de la arquitectura. Hay dos categorías de servicios de IEEE 802.11: Servicios de estación (SS) y servicios del sistema de distribución (DSS). Ambas categorías de servicios son usadas por la subcapa MAC de IEEE 802.11.

1.3.5.1 Servicios del Sistema de Distribución (DSS)

Este servicio está dado por el punto de acceso (AP) y se encarga de administrar estaciones en la celda y su comunicación con estaciones de otras celdas. Se tienen 5 servicios de distribución:

Asociación.- Sirve para establecer la conexión entre el punto de acceso y la estación, se presenta cuando una estación se une a una celda o cuando la estación se enciende, el punto de acceso puede aceptar o denegar la petición de asociación.

Disociación.- Se produce cuando una estación sale del área de una celda o cuando se apaga una estación.

Reasociación.- Se produce cuando la estación cambia de una celda y se asocia a otra.

Distribución.- Es usada por el sistema de distribución en el envío de tramas de estaciones STAs o entre STAs y portales, distribuye las tramas sean locales o sean de otro BSS.

Integración.- Maneja el direccionamiento y el formato de traducción al estándar requerido, cuando las tramas deben ser enviadas por una red que no es 802.11.

1.3.5.2 Servicios de Estación (SS)

Su ámbito es dentro del área de cobertura (celda), son los siguientes:

Autenticación.- Sirve para permitir el acceso de estaciones autorizadas, se especifica el proceso de autenticación con el protocolo WEP que será descrito con detalle mas adelante.
Desautenticación.- Se produce cuando una estación abandona la red, se da el proceso contrario a una autenticación.
Privacidad.- Este servicio permite privacidad de los datos que viajan en la red, para esto se utiliza tipos de encripción.
Entrega de datos.- Es el servicio esencial de transmisión y recepción de los datos.

1.3.6 ESTÁNDAR IEEE 802.11b

La necesidad de mayores velocidades en comunicaciones inalámbricas fue incrementándose, es así que en 1999 el IEEE aprueba el estándar 802.11b que extiende la velocidad hasta 11 Mbps a una frecuencia de 2.4 GHz, aunque también permite el funcionamiento a 5.5, 2 y 1 Mbps.

Para que IEEE 802.11b llegue a la velocidad de 11 Mbps se desarrolló una nueva capa física para adherirla al estándar, ésta es HR/DSSS (*High Rate - Direct Sequence Spread Spectrum*). Luego de su aprobación fue ampliamente difundido es así que hoy en día es el estándar con mayor producción en el mercado.
Para proveer altas velocidades, se emplean 8-chips con esquema de modulación CCK que aplica 4 y 8 bits por símbolo para alcanzar 5.5 y 11Mbps respectivamente. La tasa de chips es a 11 MHz, la cual es la misma que la descrita en DSSS de 802.11.

Se provee un esquema adicional que es opcional denominado Packet Binary Convolutional Coding (HR/DSSS/PBCC), que permite velocidades de 2, 5.5 y 11 Mbps.

Otro modo opcional que permite velocidades de 2, 5.5, y 11 Mbps es el uso de un preámbulo mas corto, lo cual incrementa el throughput[12].

- **Chips.**

Son producidos por un generador de código que produce los "code bits" que se insertan a la señal original de datos para ser modulados para ampliar el espectro de la señal como lo muestra la Figura 1.17.

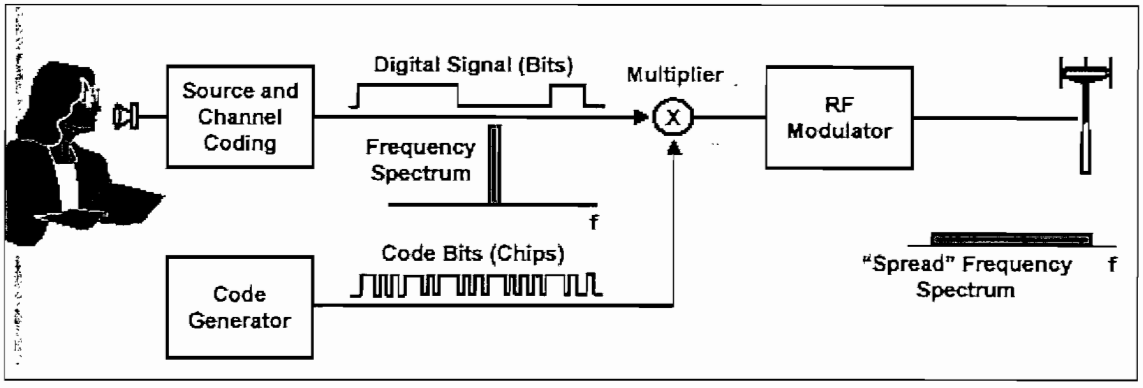


Figura 1.17.- Inserción de Chips

Los "code bits" son llamados chips y, la secuencia producida es llamada código de Barker (11 chips) +1, –1, +1, +1, –1, +1, +1, +1, –1, –1, –1.

1.3.6.1 Formato de la Trama PLCP de IEEE 802.11b

Se definen dos preámbulos y cabeceras diferentes [6] : el preámbulo y cabecera obligatorios, lo cuales operan con la especificación actual DSSS de 1 y 2 Mbps (descritas en IEEE Estándar 802.11, edición 1999), y un Preámbulo corto y cabecera opcional.

- **Preámbulo Grande 802.11b**

El formato de trama con preámbulo grande se muestra en la Figura 1.18.

[12] Velocidad Efectiva de Datos

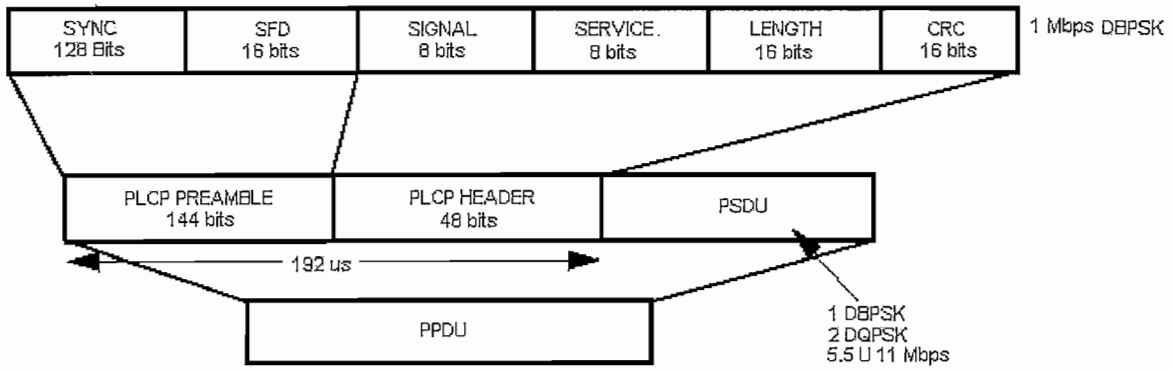


Figura 1.18.- Formato de Trama PLCP Grande 802.11b [6]

El preámbulo PLCP contiene los siguientes campos: sincronización (Sync) y delimitador de inicio de trama (SFD). La cabecera PLCP contiene los siguientes campos: Señalización (SIGNAL), Servicio (SERVICE), Longitud (LENGTH), y CRC-16. Cada uno fue descrito anteriormente. El formato no difiere de 802.11. Las excepciones son en la codificación del campo Señalización y el uso del campo Servicio:

- Señalización (*Signal*).- Este campo consta de 8 bits, es provisto para indicar el esquema de modulación empleado en transmisión y recepción. La velocidad conseguida será el valor de este campo multiplicado por 100 Kbps. Se definen dos modulaciones adicionales dadas por las siguientes palabras de 8 bits.
  a) 0Ah para 1 Mbps
  b) 14h para 2 Mbps
  c) 37h para 5.5Mbps
  d) 6Eh para 11Mbps
- Servicio (*Service*).- Consta de 8 bits, b0 a b7, donde b0 se transmite primero como lo indica la Figura 1.19.

b0	b1	b2	b3	b4	b5	b6	b7
Reservado	Reservado	bit de reloj 0 = no 1 = si	Modulación 0 = CCK 1 = PBCC	Reservado	Reservado	Reservado	bit exten longitud

Figura 1.19.- Campo Servicio de PLCP 802.11b [6]

Se definen tres bits en este campo para la extensión de alta velocidad. El bit b7 será usado para indicar que el campo longitud ha sido modificado. El Bit b3 será usado para indicar cual técnica de modulación se empleará CCK <0> ó PBCC <1>. El Bit b2 se empleará para indicar la frecuencia de transmisión. Los bits b0, b1, b4, b5, y b6 serán establecidos a 0.

- Longitud (*Length*).- Este campo es un entero de 16 bits sin signo que nos indica el número de microsegundos que se requieren para la transmisión. Existe ambigüedad en el número de octetos al sobrepasar 8Mbps por tanto existe una extensión del campo longitud al establecer el bit7 del campo Servicio.

➢ **Preámbulo Corto 802.11b**

El uso del preámbulo corto se denomina HR/DSSS/Short, permite la reducción de overhead[13], y por tanto mayor throughput[14].

El formato de la trama PLCP con preámbulo corto se muestra en la Figura 1.20, en la cual se indica como se forma el preámbulo, cabecera y cuerpo de la trama, de esta figura podemos observar los cambios que se han realizado.

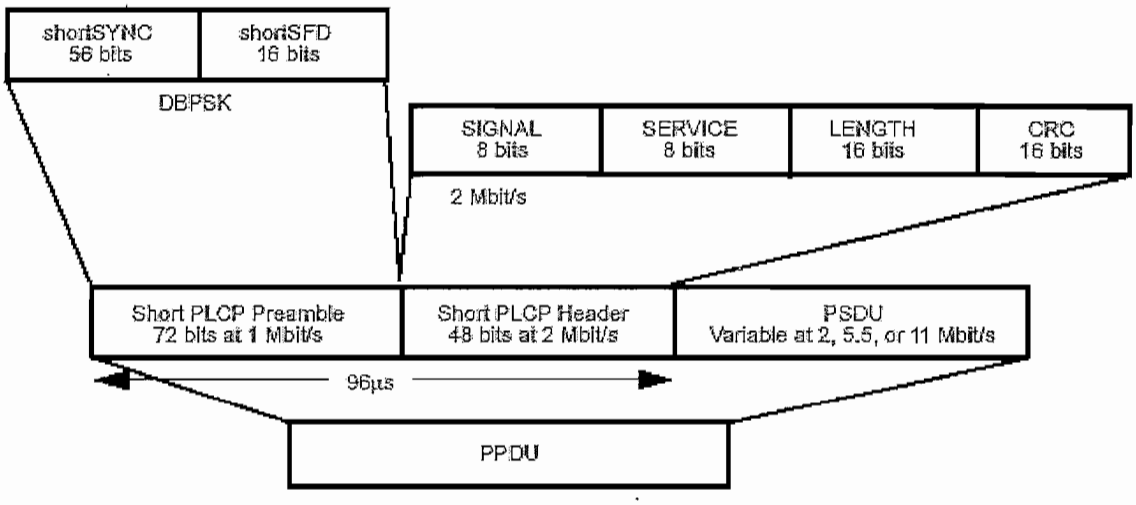


Figura 1.20.- Formato de Trama PLCP Corta 802.11b [6]

Los siguientes cambios se realizan respecto a 802.11:

[13] Sobrecarga por cabecera
[14] Velocidad efectiva de datos

- Campo Sincronización corto (shortSYNC).- Este campo consta de 56 bits, el cual provee al receptor mecanismos de sincronización.
- Campo Señalización.- provee tres tipos de velocidad provistas por las siguientes palabras de 8 bits.

a) 14h para 2 Mbits/s;
b) 37h para 5.5 Mbits/s;
c) 6Eh para 11 Mbits/s.

El preámbulo corto PLCP será transmitido usando los 1 Mbps en modulación DBPSK. La cabecera PLCP será transmitida modulando a 2 Mbps. La combinación del campo Señalización y Servicio indicarán la velocidad y modulación de la transmisión de la trama respectivamente.

1.3.7 ESTÁNDAR IEEE 802.11a.

IEEE 802.11a determina velocidades de hasta 54 Mbps. empleando OFDM (*Orthogonal Frecuency Division Multiplexing*), en la banda de los 5 GHz. permitiendo establecer comunicaciones a velocidades de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps., siendo mandatarias velocidades de 6, 12 y 24 Mbps en productos.
Opera mediante la división de la señal de radio en varias subportadoras ortogonales que son transmitidas simultáneamente a diferentes frecuencias al receptor con la finalidad de reducir interferencia.
La elaboración de estos productos es compleja, por lo cual su difusión en el mercado no ha sido tan popular como 802.11b.

1.3.7.1 OFDM

Esta técnica es adoptada de IEEE 802.11a, la cual emplea OFDM como su técnica de modulación y logra velocidades de 54Mbps en la banda de 5 GHz.
OFDM es una técnica de modulación de múltiples portadoras; y hasta recientemente no se podía emplear en la banda de 2.4Ghz.
Tiene como características principales que los datos son divididos en algunas sub-portadoras espaciadas cercanamente.
Provee buena confiabilidad en ambientes de múltiples caminos, para reducir problemas de desvanecimiento por múltiples caminos, y demás problemas que se

presentan en una comunicación inalámbrica OFDM presenta en su técnica de modulación, múltiples portadoras que se encuentran de tal suerte que sus componentes de frecuencia principales no se interfieren y con una adecuada frecuencia para recuperar la señal se toma en cuenta estas principales armónicas con lo que se consigue alcanzar mayores velocidades.

Un pico de amplitud de una subportadora es alineado al valor nulo de otra subportadora, lo cual implica ortogonalidad. Y así si el receptor detecta la señal portadora a este pico de amplitud no existirá interferencia desde otras subportadoras. Este esquema se muestra en la Figura 1.21

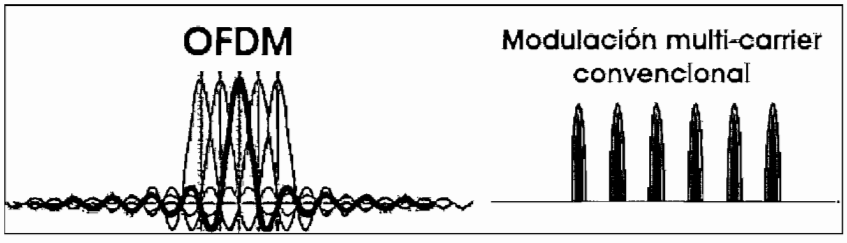


Figura 1.21.- Ortogonalidad en OFDM

OFDM es una clase de modulación multicarrier (*MCM*) que combina transmisión paralela de datos con FDM y permite un sobrelapamiento del espectro en sub-canales. Esto puede ser visto como una técnica de multiplexación. El principio de OFDM es transmitir un flujo de datos a alta velocidad, sobre múltiples flujos de datos paralelos a baja velocidad.

Los flujos de datos de baja velocidad son modulados en subportadoras ortogonales para prevenir ICI (*Inter Carrier Interference*).
Modulaciones digitales como *Phase Shift Keying* (PSK) o *Quadrature Amplitude Modulation* (QAM), son usualmente usadas en cada subportadora; sin embargo, no tienen que ser las mismas técnicas de modulación para todas las subportadoras. Estas modulaciones operan señales digitales de banda base. El resultado de la señal OFDM será convertida digital-a-analógica y modulada en otra señal portadora de radio frecuencia (RF).

1.3.7.2 Formato de la Trama PLCP de IEEE 802.11a

El formato de la trama de 802.11a tiene un formato diferente al de 802.11 el cual ayuda a comprender como funciona este estándar.

Para alcanzar varias velocidades hasta llegar a 54Mbps, las 52 subportadoras son moduladas usando BPSK/QPSK, 16 QAM, ó 64QAM [7]. Se emplea codificación convolucional del tipo FEC a una tasa de codificación 1/2 , 2/3, o ¾, denotado como R.

El formato de la trama PLCP de IEEE 802.11a es mostrado en la Figura 1.22 y consta del Preámbulo PLCP OFDM, Cabecera PLCP OFDM, PSDU, bits de cola (tail bits), y bits de relleno (pad bits). La cabecera PLCP contiene los campos: longitud, velocidad, un bit reservado, un bit de paridad, y el campo Servicio.

En términos de modulación los campos Longitud, Velocidad, bit reservado, bit de paridad constituyen un símbolo OFDM que forma el campo Señalización, éste es transmitido usando una combinación de modulación BPSK con una tasa de codificación convolucional R=½. El campo Servicio de la cabecera PLCP y el campo PSDU (conjuntamente con 6 tail bits "cero" y pad bits), forman el campo Datos (DATA), que son transmitidos a una tasa descrita en el campo Velocidad y constituyen múltiples símbolos OFDM. Los bits de cola (tail bits) del campo Señalización habilitan la decodificación inmediata luego de los campos Velocidad y Longitud, después de la recepción de los bits de cola (tail bits). Los campos Velocidad y Longitud son requeridos para la decodificación del campo Datos (DATA).

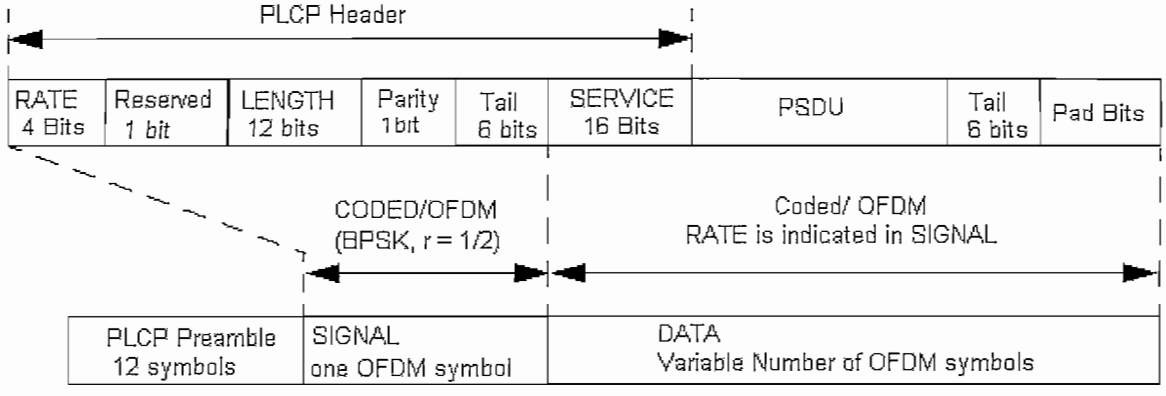


Figura 1.22.- Formato de la Trama PLCP 802.11a [7]

Los 12 símbolos del preámbulo PLCP son usados para sincronización, están formados por 10 símbolos de corta duración, y 2 símbolos de larga duración precedidos de un intervalo de guardia.

Cualquier dato recibido después de los indicados en el campo Longitud de Datos son considerados pad bits (para rellenar un símbolo OFDM) y deberán ser descartados.

1.3.7.3 Preámbulo PLCP 802.11a

Este campo consta de 12 símbolos conformados por 10 símbolos de corta duración seguidos por 2 símbolos de larga duración, precedidos por un tiempo de guardia, estos símbolos sirven de entrenamiento al receptor para el procedimiento de decodificación.

1.3.7.4 Velocidades 802.11a.

Las velocidades que son establecidas en IEEE 802.11a se encuentran relacionadas al tipo de modulación empleada y a la tasa de codificación empleada, de las velocidades mostradas en la Tabla 1.3, las velocidades de 6, 12, y 24 son obligatorias:

Velocidad (Mbps)	Tipo de Modulación
6	BPSK
9	BPSK
12	QPSK
18	QPSK
24	16-QAM
36	16-QAM
48	64-QAM
54	64-QAM

Tabla 1.3.- Velocidades de 802.11a.[7]

1.3.7.5 Parámetros Relacionados a Tiempo.

Los parámetros de tiempo definidos en IEEE 802.11a son establecidos de acuerdo a la Tabla 1.4.

Parámetro	Valor
Subportadoras para datos	48
Subportadoras piloto	4
Subportadoras totales	52
Espaciamiento de frecuencia = Δf	0.3125 Mhz
Período de FFT = T_{FFT}	32 μs ($1/\Delta f$)
Preámbulo PLCP = Tpreamb.	16μs = Tcorto+Tgrande
Señalización = Tseñaliz	4μs (T_{GI}+ T_{FFT})
Intervalo de Guardia T_{GI}	0.8μs($T_{FFT}/4$)
T_{GI} de Entrenamiento T_{GI2}	1.6 μs($T_{FFT}/2$)
Símbolos	4 μs(T_{GI}+T_{FFT})
Entrenamiento corto Tcorto	8μs(10 x $T_{FFT}/4$)
Entrenamiento grande Tgrande	8μs(T_{GI2} + 2 x $T_{FFT}/4$)

Tabla 1.4.- Parámetros de tiempo 802.11a [7]

El parámetro T_{FFT} hace referencia a la Transformada Rápida de Fourier, la cual es empleada para transportar las señales del dominio de tiempo al dominio de la frecuencia y viceversa mediante la transformada Inversa Rápida de Fourier.

1.4 SEGURIDAD INALÁMBRICA

Las redes inalámbricas al tener como medio de transmisión el aire se encuentran expuestas a retos inherentes que en estos tiempos son un desafío para los investigadores los cuales estudian nuevas soluciones cada día.

Para tratar de garantizar seguridad en un medio inalámbrico es común el emplear mecanismos denominados AAA *AUTHENTICATION, AUTHORIZATION, ACCOUNTING,* este acrónimo hace referencia al hecho de tener un control de la red en Autenticación (identificar quien es), Autorización (Saber que permisos se tiene sobre los recursos de la red), y Accounting (es decir, llevar un seguimiento, qué se ha hecho y que se está haciendo en la red).

Existen mecanismos para minimizar los riesgos que se tienen en una red inalámbrica, los cuales se mencionarán a continuación.

1.4.1 AUTENTICACIÓN Y ASOCIACIÓN

Se tienen dos procesos para garantizar conectividad en una red LAN inalámbrica. Estos procesos se producen en el orden en el cual se mencionan, autenticación y asociación.

1.4.1.1 Autenticación.

Es el proceso por el cual un nodo inalámbrico (tarjeta inalámbrica, cliente USB, adaptador PCI) es identificado por la red (punto de acceso), y al cual el nodo está tratando de conectarse.

Este proceso se lo hace con la finalidad de garantizar que el nodo sea quien dice ser, e identificarlo antes de conectarlo.

El nodo envía una trama de petición de autenticación al AP y éste puede aceptar o negar su petición y notifica al nodo con una trama de respuesta.

1.4.1.2 Asociación

Luego que el nodo ha sido autenticado, el cliente pasa a ser asociado, este estado significa que el nodo puede pasar datos al AP.

Cuando el cliente es conectado envía una petición de asociación al cual, el AP notifica con una permisión o una negación de la asociación. Este proceso se indica en la Figura 1.23.

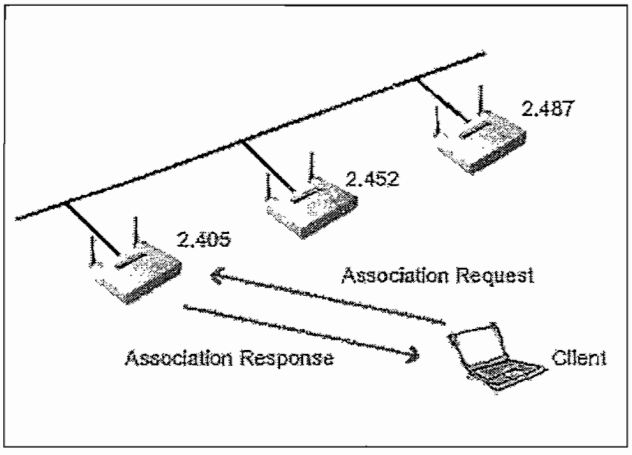


Figura 1.23.- Proceso de Asociación

Como se puede observar en la Figura 1.23, los puntos de acceso trabajan en un rango de canales establecidos.

1.4.2 ESTADOS DE AUTENTICACIÓN Y ASOCIACIÓN

Existen tres estados posibles en los que puede encontrarse un dispositivo debido al proceso anterior.

1.4.2.1 No autenticado & No asociado

En este estado el nodo se encuentre totalmente fuera de la red, desconectado incapaz de pasar datos al AP. Existe una tabla de conexión dentro del AP, en ésta se mostrará como, No autenticado.

1.4.2.2 Autenticado & No asociado

El cliente ha pasado la autenticación pero no se ha asociado, por lo que es incapaz de pasar o recibir datos del AP. Se mostrará en su tabla como Autenticado. Es raro que se dé este estado en el AP, lo mas común es que pase rápidamente, en milisegundos este estado, por lo que generalmente se mostrará No autenticado ó Asociado en su tabla de conexión.

1.4.2.3 Autenticado & Asociado

En este estado el nodo se encuentra totalmente conectado a la red mediante el AP y es capaz de transmitir y recibir datos del AP.
En su tabla de conexiones del AP se mostrará como , Asociado.

1.4.3 MÉTODOS DE AUTENTICACIÓN

Dentro del estándar IEEE 802.11 se define dos métodos de autenticación:
Sistema de Autenticación Abierta *(Open System Authentication)* y Autenticación de Llave Compartida *(Shared Key Authentication)* [13].

1.4.3.1 Sistema de Autenticación Abierta (OSA)

Se denomina sistema de autenticación nula (Null Authentication) y viene por defecto en los equipos. Un nodo podrá asociarse a un AP siempre y cuando éste

tenga el correcto SSID[15] el cual permite emparejar tanto a cliente y AP para completar el proceso de autenticación, este esquema se muestra en la Figura 1.24.

1. Se hace una petición de autenticación desde el cliente al AP.
2. El AP envía su notificación y el cliente queda.conectado.

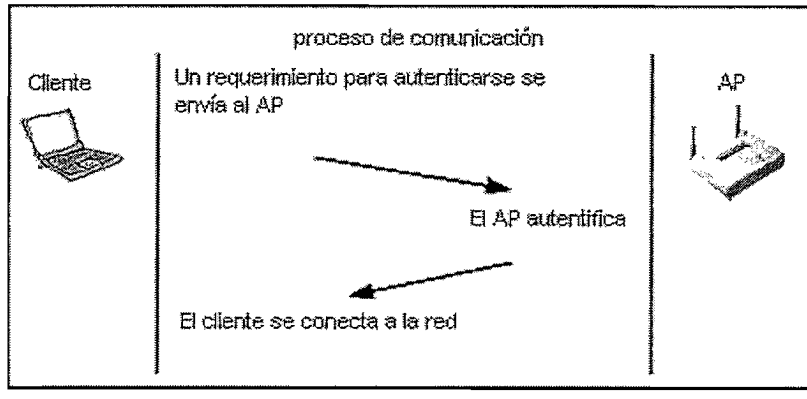


Figura 1.24.- Sistema de Autenticación Abierta[13].

Este proceso puede funcionar con WEP (Wired Equivalence Protection) que estudiaremos mas adelante, es de fácil configuración y viene por defecto en equipos.

1.4.3.2 Autenticación de Llave Compartida (SKA)

Este método de autenticación requiere de WEP. El proceso requiere de llaves que son ingresadas tanto en el cliente como en el AP.

1. El cliente envía una petición de requerimiento al AP.
2. El AP envía un texto claro, sin cifrar al cliente llamado reto, desafío (Challenge).
3. El cliente responde el reto cifrando con la llave el texto y lo envía nuevamente.
4. El AP descifra el texto y comprueba la identidad del AP.
5. El cliente se conecta a la red.

El proceso con llave compartida se muestra en la Figura 1.25.

[15] Identificador de Grupo de servicios.

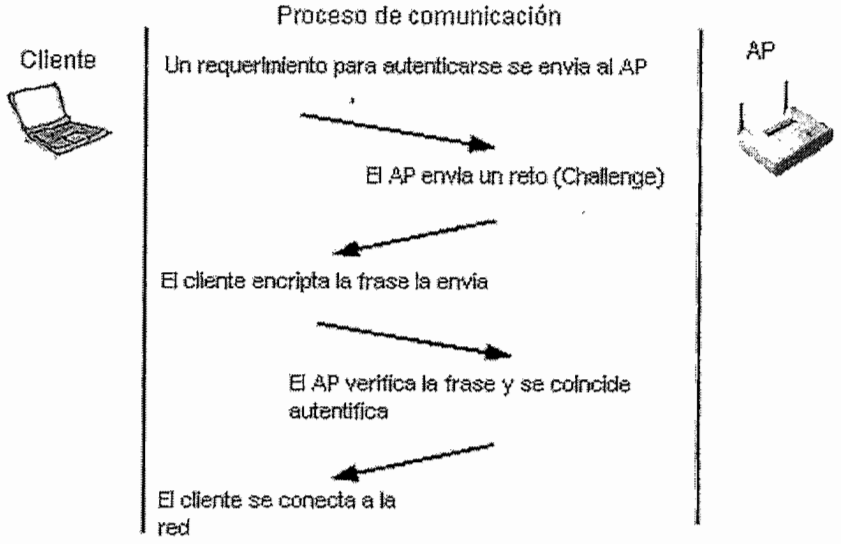


Figura 1.25.- Autenticación con Llave Compartida[13]

El uso de SKA a simple vista es mas seguro pero no en realidad, el hecho de enviar un texto plano y enviar el texto cifrado puede ser causa de un ataque.
Los dos textos pueden ser capturados por un sniffer y mediante un programa obtener la llave de encripción, e introducirse en la red.
Ninguno de estos métodos es 100% seguro por lo que se ha visto la necesidad de otros mecanismos y esfuerzos en seguridad por lo que han surgido estándares que tratan de aumentar seguridad en comunicaciones inalámbricas.
Entre los protocolos mas relevantes se encuentran 802.1x y EAP (Extensible Authenticaction Protocol), VPNs, y AAA que es un acrónimo (Authentication, Authorization, Accounting), los cuales se mencionan a continuación.

1.4.4 ENCRIPCIÓN WEP

La Encripción es un mecanismo por medio del cual se oculta la información de los datos. Encripción WEP fue ideado con el propósito conseguir un nivel de seguridad similar al que se obtiene inherentemente de una red cableada.
Los datos que no son encriptados se denominan texto plano (*plaintext*) denotados por ***P*** [2]. Los datos encriptados se denominan texto cifrado (*ciphertext*) denotados por ***C.*** El proceso de Encripción de un texto plano se denotará por la letra ***E***. El

proceso de recuperación del texto cifrado se denomina desencripción denotada por ***D.*** WEP basa su funcionamiento en una llave secreta ***k*** compartida entre las partes que intervienen en la comunicación para proteger el cuerpo de la trama de datos.

La Encripción de la trama procede de la siguiente manera:

Checksum: Primero, se computa un checksum ***c(M)*** en el mensaje ***M***. Se concatena los dos y se obtiene el texto plano ***P = (M,c(M))***, el cual será usado como entrada en la etapa de Encripción. Note que ***c(M)*** así como ***P***, no dependen de la llave secreta ***k***.

Encripción: En esta etapa, se encripta el texto plano ***P*** usando RC4[16]. Se escoge un vector de inicialización denotado por $\mathcal{V}$. El algoritmo RC4 genera un flujo de datos ***(keystream),*** que es una secuencia randómica de bytes como una función de $\mathcal{V}$ y la llave ***k***, denotado por ***RC4(v,k)***. Luego se realiza una operación XOR lógica (denotada por $\oplus$) entre el *texto plano* y el *keystream* para obtener el *texto cifrado*:

$$C = P \oplus RC4(v,k)$$

Transmisión: Finalmente, se transmite el vector de inicialización y el texto cifrado sobre el enlace de radio. Simbólicamente esto puede ser representado de la siguiente manera:

$$A \rightarrow B: \mathcal{V}, (P \oplus RC4(v,k)) \text{ donde } P = (M,c(M))$$

Este procedimiento se denota gráficamente en la Figura 1.26.

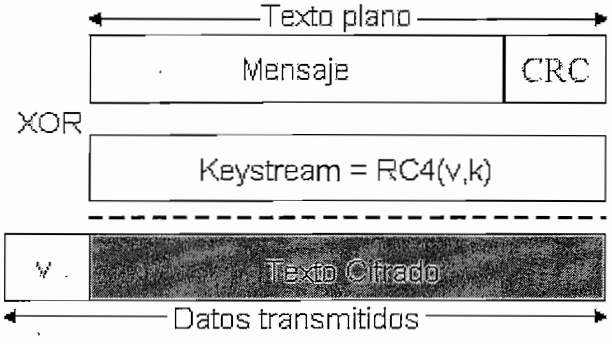


Figura 1.26- Encripción WEP

[16] Encripción Simétrica con llave de 40 bits.

Características de seguridad se encuentran especificadas en IEEE 802.11, como WEP.

En un sistema inalámbrico sin embargo existen vulnerabilidades y la posibilidad de ataques siempre estará presente.

Es así que día a día se tienen mejoras, la evolución de los estándares trata de garantizar más seguridad en cuanto a conexiones seguras.

1.4.4.1 Problemas de Seguridad en IEEE 802.11

Como se mencionó anteriormente el protocolo WEP es usado como base para redes inalámbricas 802.11. WEP usa un algoritmo de encripción RC4 con llave de longitud variable para proteger el tráfico. Dentro del estándar IEEE 802.11, se especifica que el protocolo WEP tiene una llave de 40 bits. Sin embargo hoy en día se tiene llaves de 104 bits y 128 bits. Con la adición de IV de 24 bits, la actual llave usada en RC4 tiene 152 bits (128 + 24) [9].

Algunos especialistas en seguridad computacional han descubierto problemas que permiten a usuarios maliciosos comprometer la seguridad de redes inalámbricas. Esto incluye ataques pasivos para descifrar tráfico basándose en análisis estadísticos, ataques activos para inyectar nuevo tráfico desde estaciones móviles no autorizadas (basados en conocer el texto plano), y ataques activos para descifrar tráfico (basados en suplantar el punto de acceso).

Los problemas de WEP que se han detectado incluyen lo siguiente:

1. El uso de llaves estáticas en WEP.- muchos usuarios en la red inalámbrica potencialmente comparten una idéntica llave por largos períodos de tiempo, es una vulnerabilidad de la red bien conocida. Si una computadora (con llave WEP), como *una laptop* es robada, esta llave podría comprometer a largo plazo la red. Otro caso es, si muchas estaciones usan la misma llave, gran cantidad de tráfico circulará por la red y puede estar rápidamente disponible para un ataque.
2. El campo IV de WEP, es un campo de 24 bits enviado en claro (sin cifrar) como parte del mensaje. Esta cadena de caracteres de 24 bits, usada para inicializar la llave generada por RC4, es relativamente pequeña cuando se trata de fines criptográficos. La reutilización del mismo IV produce los mismos flujos de

datos de llaves para la protección de datos, y el tamaño de IV implica que se repitan luego de poco tiempo en una red con bastante tráfico. El estándar 802.11 no especifica como establecer o cambiar valores de IV, tarjetas inalámbricas del mismo fabricante pueden generar secuencias de IVs iguales, o posiblemente usar un IV constante, por tanto hackers pueden interceptar el tráfico de red, determinar los flujos de datos de llaves, y usarlos para descifrar los textos encriptados.

3. El campo IV es una parte de la llave de encripción de RC4. El hecho que un atacante conozca los 24 bits de cada llave de un paquete, combinado con artificios del esquema de RC4, permite que ataques analíticos tengan éxito, y que se recupere la llave, después de interceptar una cantidad relativamente pequeña de tráfico.

4. WEP proporciona integridad sin criptografía. Sin embargo, se tiene el uso de mecanismos de CRC en la subcapa MAC de 802.11 para el chequeo de la integridad de paquetes, y el uso de paquetes ACK (acknowledge) con el correcto checksum. La combinación de este checksum no cifrado con datos cifrados es peligroso e introduce vulnerabilidades, como es el caso de WEP. Hay un ataque activo que permite al atacante descifrar cualquier paquete modificando el paquete y CRC sistemáticamente, enviándolo al punto de acceso y notando cuando se recibe el paquete de ACK.

Note que solamente uno de los 4 problemas listados depende de una debilidad en el algoritmo de criptografía. Por tanto, estos problemas no se mejoran por la sustitución del método de encripción. Por ejemplo, el tercer problema listado arriba es consecuencia de una debilidad en el cifrado RC4 lo que se entiende como un diseño pobre del protocolo, y es por este motivo que nuevas mejoras se han introducido.

1.4.5 802.1x CON EAP

Este es un estándar relativamente nuevo en seguridad hace referencia a un control de acceso a la red basada en puertos (*port-based network access control*) lo que permite conectividad en capa 2 si el proceso de autenticación es exitoso.

El proceso de autenticación se muestra en la Figura 1.27 en el cual interviene un servidor de autenticación.

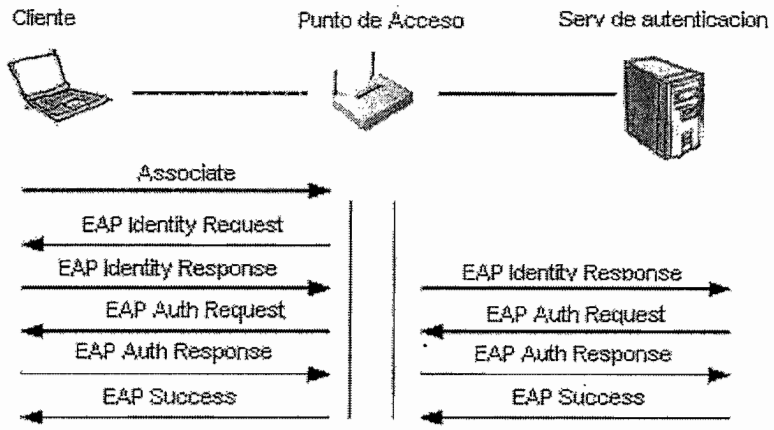


Figura 1.27.- Proceso de Autenticación en EAP[13]

1. El cliente realiza una petición de asociación al AP.
2. El AP pide al cliente que se identifique con un *EAP Identity Request*
3. A este requerimiento el cliente envía una respuesta *EAP Identity Response*, identificándose a la red.
4. Esta respuesta de identificación es enviada al Servidor de Autenticación.
5. El servidor envía a un requerimiento para validar su autenticación (*EAP Auth Request*).
6. El (*EAP Auth Request*) es enviado al cliente por medio del AP
7. El cliente envía una respuesta de autenticación al AP y éste a su vez al Servidor (*EAP Auth Response*).
8. Una vez que el Servidor de Autenticación a recibido el EAP Auth Response, autentica al cliente enviándole un EAP-Success por medio del AP.

➢ Como se puede observar se tienen dos etapas claramente definidas, la etapa de identificación del cliente en la red, y la etapa de autenticación.

1.4.6 WPA (*Wi-Fi Protected Access)*

Aparece a finales del 2002 y sirvió como base al estándar IEEE 802.11i, pretende garantizar mayor seguridad en los estándares de capa física 802.11a, 802.11b y 802.11g. Emplea el protocolo TKIP (*Temporal Key Integrity Protocol*) en el cifrado de datos, el cual cambia cada cierto tiempo la clave de cifrado que se empleará

entre el cliente y el punto de acceso. TKIP amplia la longitud de clave WEP de 40 a 128 bits y es generada de forma dinámica para cada usuario por sesión, siendo ésta una clave temporal y de un período fijo de duración. TKIP aplica un código de integridad MIC de mensajes (*Message Intergrity Code*) para garantizar la integridad del mensaje. WPA emplea 802.1x como mecanismo de autenticación. Envía un mensaje de autenticación MAC junto con la información transmitida. Con WPA se puede seguir usando WEP ya que lo hace más robusto.

1.4.7 IEEE 802.11i

Es un estándar nuevo aprobado en junio de 2004, el cual pretende mejorar la seguridad en redes inalámbricas. Emplea AES como algoritmo de cifrado con claves de 128, 192 y 256 bits.

El grupo de trabajo de IEEE de 802.11i define una red de seguridad robusta RSN por sus siglas en inglés la cual permite la creación de asociaciones de redes de seguridad robustas.

Estas asociaciones de todos los dispositivos, estaciones y APs, se realizan sobre una autenticación/ asociación fuerte denominada RSNA.

Las estaciones pueden ser RSN si son capaces de crear RSNAs, caso contrario son pre-RSN.

En el proceso de autenticación /asociación, puede ir incluido un handshake de 4 vías, si este handshake de 4 vías no está incluido en el proceso mencionado se consideran a las estaciones como pre-RSNAs.

RSN utiliza 802.1x para su autenticación y servicio de administración de claves, incorpora en su arquitectura dos componentes: puerto 802.1x y servidor de autenticación (AS).

Permite dos tipos de administración de claves: manual por parte del administrador y automática en una RSNA.

Los algoritmos de encripción son CCMP (obligatorio) y TKIP opcional.

1.4.8 SERVICIOS BÁSICOS DE SEGURIDAD EN REDES WLAN

En un sistema de comunicaciones inalámbrico se debe garantizar seguridad en la transmisión de datos. En esta sección se describen los componentes de

seguridad de 802.11. En IEEE 802.11 se identifican servicios que proporcionan un ambiente de operación seguro. Estos servicios básicos son Autenticación, Confidencialidad e Integridad [9], que son provistos por el protocolo WEP (*Wired Equivalent Privacy*) para proteger el enlace de datos durante la transmisión inalámbrica.

1.4.8.1 Autenticación.

Es el primer objetivo de WEP para proporcionar un servicio de seguridad, para verificar la identidad de las estaciones clientes en la comunicación. Esto proporciona un control de acceso a la red mediante la negación de acceso a clientes que no tienen permiso de autenticación apropiado, por tanto no están permitidas para acceder a la red.

1.4.8.2 Confidencialidad

El servicio de confidencialidad o privacidad fue la segunda meta de WEP, fue desarrollado para proporcionar "privacidad lograda por la red cableada". La intención fue prevenir que la información sea comprometida por ataques garantizando que solamente las personas permitidas puedan ver los datos.

1.4.8.3 Integridad

Otro objetivo de WEP fue el desarrollo de un servicio de seguridad que garantice que los mensajes no sean modificados durante el envío entre los clientes inalámbricos y el punto de acceso. Este servicio garantiza que los datos, tanto entrantes como salientes de la red no sean corrompidos.

1.4.9 REQUERIMIENTOS DE SEGURIDAD Y ATAQUES

Como se ha mencionado la industria inalámbrica WLAN de 802.11 está creciendo y actualmente está en un significante momento. Todos los indicadores sugieren que numerosas organizaciones desarrollarán tecnología WLAN.

Sin embargo, existen situaciones en las cuales 802.11 WLANs no ha sido totalmente positivo. Se tienen numerosas publicaciones y *papers*, que describen ataques en redes inalámbricas 802.11 que exponen a las organizaciones riesgos

de seguridad. Esta sección describe de manera general estos riesgos y ataques en confidencialidad, integridad y disponibilidad de la red.

La Figura 1.28 proporciona una visión general de ataques producidos que ayuda al entendimiento de los mismos.

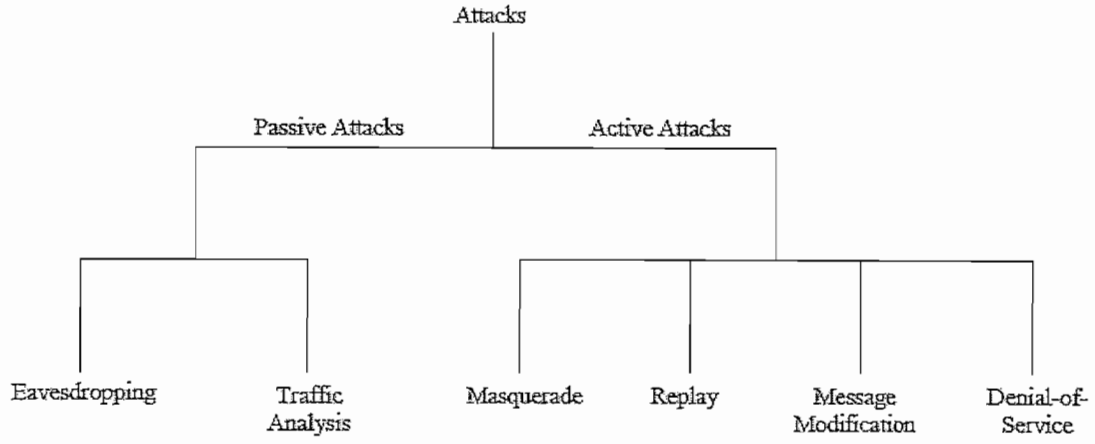


Figura 1.28.- Tipos de Ataques Contra la Seguridad [9]

Los ataques típicos de seguridad se clasifican en dos grandes grupos: ataques pasivos y ataques activos, que a su vez son divididos en otro tipo de ataques.

1.4.9.1 Ataques Pasivos.

Un ataque en el cual se gana una parte de acceso a la red pero no modifica su contenido, puede realizarse un análisis de tráfico, se tienen 2 tipos de ataques relacionados.

- *Eavesdropping*.- El atacante realiza un monitoreo de la transmisión y puede ver el contenido de los mensajes. Un ejemplo de este ataque es una persona escuchando la transmisión de datos entre dos estaciones de trabajo en una red LAN, o entre un dispositivo inalámbrico y una estación base.

- Análisis de Tráfico.- El atacante, usa un modo mas discreto, gana inteligencia monitoreando la comunicación de dos entidades de la red. Gran cantidad de información es contenida entre dos partes que intervienen en la comunicación.

1.4.9.2 Ataques Activos.

Estos ataques son realizados por una entidad no autorizada que realiza modificaciones de un mensaje, flujo de datos o archivos. Es posible detectar este tipo de ataques, pero es más difícil ser prevenidos. Ataques activos pueden tomar cuatro formas: Enmascaramiento, reemplazo, modificación de mensajes, y negación del servicio.

- Enmascaramiento.- Un atacante se hace pasar por un usuario autorizado y por tanto gana privilegios que no eran autorizados.
- Reemplazo (*Replay*).- El atacante monitorea la transmisión y retransmite mensajes como un usuario legítimo.
- Modificación de mensajes.- El atacante altera un mensaje legítimo borrándolo, adhiriendo, cambiando o reordenándolo.
- Negación de Servicio.- El atacante imposibilita el uso normal de las comunicaciones o facilidades de su administración

Las consecuencias de estos ataques provocan pérdidas a la propiedad de información, costos legales, y pérdidas del servicio en la red.

1.4.10 OTROS RIESGOS DE SEGURIDAD

Con la presencia de un mayor número de dispositivos inalámbricos, más usuarios ven la manera de conectarse remotamente a sus propias organizaciones. Centros de conferencia, por ejemplo, proporciona a su red inalámbrica conexión a Internet durante las conferencias. Hoteles, aeropuertos, otros desarrollan redes 802.11 para sus clientes, siempre añadiendo capacidades de seguridad.

Sin embargo al ser redes públicas están disponibles para todos, incluso usuarios maliciosos, si estas redes usan mayor ganancia de antenas igualmente dan facilidades a ciertos ataques.

Por estas conexiones a sus propias redes o redes improvisadas, usuarios pueden crear vulnerabilidades para su propia compañía y sistemas, a menos que se tengan ciertos pasos y procedimientos para proteger a usuarios y a ellos mismos.

Se puede considerar protección a recursos públicos usando un protocolo que aplique niveles de seguridad como TLS *(Transport Layer Security)*, el grupo IETF (*Internet Engineering Task Force*) estandardizó la versión de SSL *(Secure Sockets Layer)* . Sin embargo, en la mayoría esto es innecesario debido a que la información es pública. Para recursos privados, se debería considerar el uso de soluciones VPN[17] para asegurar que sus conexiones sean seguras y eviten ataques *eavesdropping* y acceso no autorizado a sus recursos.

Finalmente, como en cualquier red, la ingeniería social es una situación concerniente que no puede ser controlada. Por tanto una empresa debe considerar todos los aspectos de seguridad en redes cuando se desarrolle redes inalámbricas, capacitar a usuarios sobre los riesgos que están presentes.

1.5 ESTÁNDAR IEEE 802.11g

Posterior a 802.11b y 802.11a surge el desarrollo del estándar IEEE 802.11g publicado en junio del 2003 que define la operación de hasta 54 Mbps al igual que 802.11a pero a la frecuencia de 2.4 GHz.

Oficialmente es designado como:
Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band.

IEEE 802.11g especifica un interfaz para soporte sobre aire entre un cliente inalámbrico y una estación (AP) ó entre dos clientes inalámbricos, el cual provee de 1 a 54 Mbps en la banda de 2.4Ghz garantizando compatibilidad con IEEE 802.11b; IEEE 802.11g incorpora a su estándar una capa física adicional ERP con técnicas de modulación combinadas, como DSSS, HR-DSSS, CCK (*Complementary Code Keying)* a velocidades de 1, 2, 5.5 y 11 Mbps en la banda de 2.4Ghz, adicionalmente 802.11g adopta OFDM (*Orthogonal Frequency*

[17] Red privada virtual

Division Multiplexing) de IEEE 802.11a para alcanzar hasta 54Mbps en la banda de 2.4 Ghz.

1.5.1 EL CAMINO HACIA IEEE 802.11g

Para lograr un sistema inalámbrico de alta velocidad en la banda de 2.4 GHz los investigadores pasaron por el desarrollo de esquemas que permitieron desde 1999 hasta hoy en día tener la suficiente base teórico-práctica para conseguir velocidades de hasta 54Mbps.

La formación de capa física para la transmisión de datos se da por medio de la formación de Unidades de Datos (MAC PDUs) que se encapsulan en tramas PLCP y es aquí donde se determinan esquemas de modulación, tipos de tramas, y velocidades que se emplearán.

Es por este motivo que se analizó el formato de la trama PLCP de IEEE 802.11 y los cambios que se fueron produciendo a este estándar, así como los esquemas de modulación que se han empleado, ya que, como se puede entender, el desarrollo de IEEE 802.11g fue el resultado de combinar y modificar técnicas anteriores como son DSSS de IEEE 802.11, preámbulo corto de IEEE 802.11b, OFDM de IEEE 802.11a, y esquemas opcionales que permiten otras velocidades como 22 y 33Mbps por ejemplo.

1.5.2 Formato ERP-PBCC a 22 y 33 Mbps en 802.11g

Dentro del estándar 802.11g se define dos modos de modulación que permiten alcanzar 22 y 33 Mbps empleando PBCC (*Packet Binary Convolutional Code*) como esquema de modulación.[8]

En el codificador PBCC, primero los datos entrantes son codificados previamente para ser transmitidos al canal. Se emplea una matriz generadora G.

$$G = \begin{bmatrix} 1+D^4 & D & D+D^3 \\ D^3 & 1+D^2+D^4 & D+D^3 \end{bmatrix}$$

Como el sistema es basado en tramas PPDU), el codificador debería estar con todos los elementos de memoria en cero, al comienzo de cada PPDU. El

codificador debe estar en un estado conocido al final de cada PPDU para prevenir que los bits de datos cercanos al final de la PPDU sea decodificados de forma incorrecta. Ésto se logra adheriendo un octeto lleno de ceros al final de la PPDU previa a la transmisión y descartándolo en la recepción de la PPDU.

Un diagrama de bloques del codificador se muestra en la figura 1.29. Consiste de dos caminos con cuatro elementos de memoria cada uno. Para cada par de bits de entrada se generan tres salidas. La salida de cada código convolucional se expresará en un diagrama de constelación 8-PSK; Cada salida de 3 bits es usado para producir un símbolo. Con esto se consigue un throughput de dos bits de información por símbolo. En ERP-PBCC-22 y ERP-PBCC-33, Los bits de datos a la entrada son divididos en pares de bits. En cada par, el primer bit se coloca en la entrada superior del codificador convolucional, y el segundo bit se coloca en la entrada inferior.

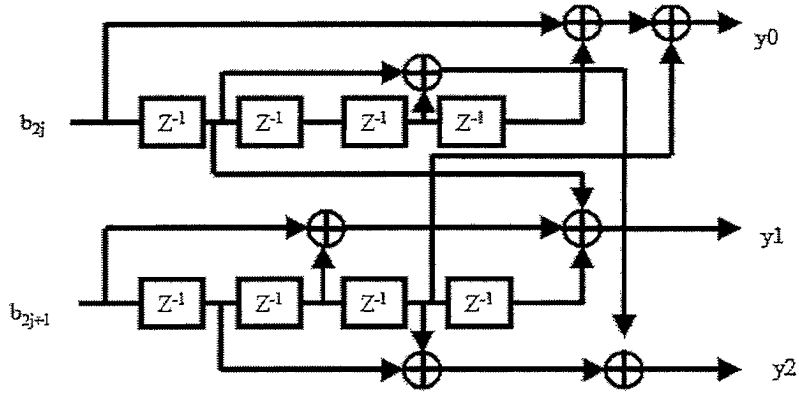


Figura 1.29.- Codificador Convolucional de ERP-PBCC 22/33 Mbps [8]

El diagrama de constelación 8-PSK para las salidas del codificador se indican en la figura 1.30

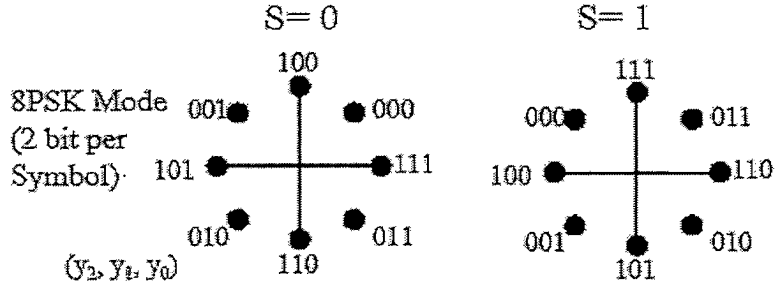


Figura 1.30.- Diagrama de Constelación en ERP-PBCC 22/33 Mbps.

El modo ERP-PBCC lograr 33 Mbit/s usando un reloj de 16.5 MHz para la parte de datos del paquete. Se adhiere una conmutación extra entre el preámbulo y la parte de datos. Cuando el reloj de 11 MHz pasa a 16.5 MHz, se usa el esquema de conmutación de la figura 1.31.

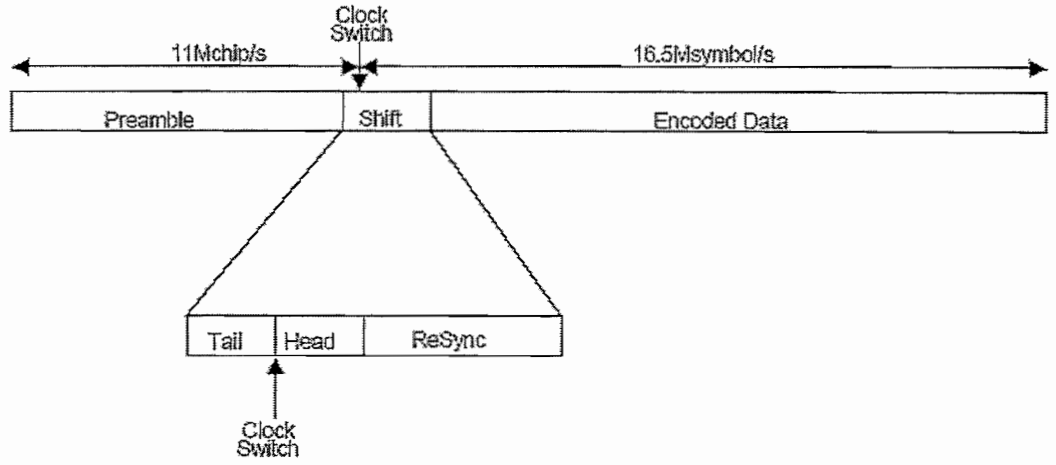


Figura 1.31.- Conmutación de reloj 33Mbps

El campo Tail es 3 ciclos de reloj a 11 Mchip/s y el campo Head es 3 ciclos de reloj a 16.5 Msymbol/s (QPSK). El campo resync es 9 ciclos de reloj a 16.5 Msymbol/s. El tiempo total de conmutación es 1 µs. Los bits de tail son 1 1 1, los bits de Head son 0 0 0, y los bits de resync son 1 0 0 0 1 1 1 0 1. La modulación es BPSK, la cual se sincroniza en fase con el símbolo previo. [8]

1.5.3 CAPA FÍSICA DE VELOCIDAD EXTENDIDA (ERP) DE 802.11g

La nueva capa física definida se conoce con el nombre de Capa Física de Velocidad Extendida (*Extended Rate Physical*).[8]

El estándar IEEE 802.11g define esta capa física de velocidad extendida ERP, con opciones de modulación: usa DSSS para lograr velocidades de 1 y 2 Mbps, usa modulaciones CCK y PBCC(opcional) para lograr velocidades de 5.5, y 11 Mbps. La capa física ERP provee velocidades adicionales de 6, 9, 12, 18, 24, 36, 48, y 54 Mbps. Tanto en transmisión como en recepción las velocidades 1, 2, 5.5, 11, 6, 12, y 24 Mbps son obligatorias.

Se definen dos modos de modulación opcionales: ERP-PBCC con velocidades de 22 y 33 Mbps. Un modo de modulación conocido como DSSS-OFDM es también incorporado que permite velocidades de 6, 9, 12, 18, 24, 36, 48, y 54 Mbps.

1.5.3.1 Formato de la Trama PLCP de IEEE 802.11g.

Para conseguir velocidades mayores, el preámbulo corto PLCP de 802.11b ya no es opcional, sino obligatorio. Una estación con capa física ERP deberá soportar tres diferentes formatos de preámbulo y cabecera.

El primer formato es de Preámbulo Grande y cabecera, apropiado para el uso con los modos de 1, 2, 5.5, y 11 Mbps y compatible con BSSs que usen estos modos. Esta PPDU provee interoperabilidad con estaciones a velocidades de 1, 2, 5.5, y 11 Mbps; la modulación opcional DSSS-OFDM a todas las velocidades de OFDM; y la modulación ERP-PBCC opcional.

El segundo formato es de Preámbulo Corto y cabecera.

El preámbulo corto soporta las velocidades 2, 5.5, y 11 Mbps tanto como DSSS-OFDM y ERP-PBCC.

El tercer formato es de preámbulo ERP-OFDM y cabecera especificadas según IEEE 802.11a con ciertas modificaciones.

La capa física ERP tiene dos formatos de PPDU opcionales, descritas en DSSS-OFDM de 802.11g y en preámbulo corto de 802.11b, para soportar las velocidades opcionales de DSSS-OFDM.

1.5.3.2 Preámbulo Grande 802.11g

El uso de preámbulo grande es el mismo de 802.11b, es adecuado para obtener las velocidades de 1, 2, 5.5, y 11 Mbps, y compatible con BSSs que usen estos modos, para incluir velocidades adicionales, se hacen los siguientes cambios al formato PLCP de 802.11b

El uso de un bit en el campo Servicio para indicar cuando el modo opcional ERP-PBCC es usado.

El uso de 2 bits adicionales en el Campo servicio para evitar ambigüedad en el uso de ERP-PBCC a 22 o 33 Mbps.

Adicionalmente tres velocidades opcionales en el octeto del campo Señalización de la siguiente manera:

1) DCh para 22 Mbps ERP-PBCC
2) 21h para 33 Mbps ERP-PBCC
3) 1Eh para velocidades DSSS-OFDM.

La Figura 1.32 muestra el campo Servicio de IEEE 802.11g, 3 bits b0, b1, y b4 son reservados y establecidos a 0. El bit b2 es usado para establecer la frecuencia de transmisión, el bit b3 es usado para indicar si se usará o no ERP-PBCC a 22 o 33 Mbps, b5, b6 y b7 son usados para evitar ambigüedad en los esquemas ERP-PBCC 11 a ERP-PBCC 33, el bit b7 también es usado para indicar el uso de CCK a 11Mbps definido en 802.11b, en el cual b3, b5 y b6 son establecidos a cero.

b0	b1	b2	b3	b4	b5	b6	b7
Reserved	Reserved	bit de reloj 0 = no 1 = si	Modulación 0 = no ERP PBCC 1 = ERP PBCC	Reserved	bit exten longitud ERP PBCC	bit exten longitud ERP PBCC	bit exten longitud

Figura 1.32.- Campo Servicio de 802.11g [8]

1.5.3.3 Preámbulo Corto 802.11g

El preámbulo corto definido en 802.11b ya no es opcional, Para la capa física ERP es obligatorio. El preámbulo corto es adecuado para velocidades de 2, 5.5 y 11 Mbps, los bits del campo Servicio en Preámbulo Corto y Campo Velocidad son los mismos que los definidos para Preámbulo Grande.

1.5.3.4 ERP-OFDM

El formato de preámbulo, y cabecera para unidad de datos PLCP con ERP-OFDM son descritas de igual manera que IEEE 802.11a.

Para las modalidades de ERP-OFDM, el campo Datos que contiene el campo Servicio, PSDU, TAIL bits, y PAD bits serán iguales.

El uso de todas las capacidades de capa física es igual a OFDM de 802.11a con las siguientes diferencias:

- El uso del plan de frecuencias asignado es diferente en el rango de 2.4–2.4835GHz.
- Una precisión de frecuencia de ± 25ppm[18] en lugar de ±20ppm definida en 802.11a.
- Un nivel máximo de potencia en señal de entrada de –20dBm en lugar de -30dBm definidos en 802.11a.

[18] Partes por millón

- El espacio corto entre tramas (SIFS) es de 10 μs en lugar de 16μs de 802.11a.

1.5.4 DSSS-OFDM de 802.11g

Dentro del estándar se denomina DSSS-OFDM al esquema de modulación en el cual combina DSSS con OFDM.

Ambos, Preámbulo Grande y Preámbulo Corto de 802.11g son usados con DSSS-OFDM.

Para todos, velocidades y preámbulos DSSS-OFDM, el campo Señalización definido en IEEE 802.11b será establecido al valor de 3Mbps. Esto es que los 8 bits del campo tendrán el valor 1Eh. Para DSSS-OFDM este valor indica que estaciones que no tengan la capacidad de ERP, lean el campo longitud y no utilicen el medio durante ese tiempo. La formación de la trama de datos que forman la unidad de datos (PPDU) en DSSS-OFDM se muestra en la Figura 1.33.

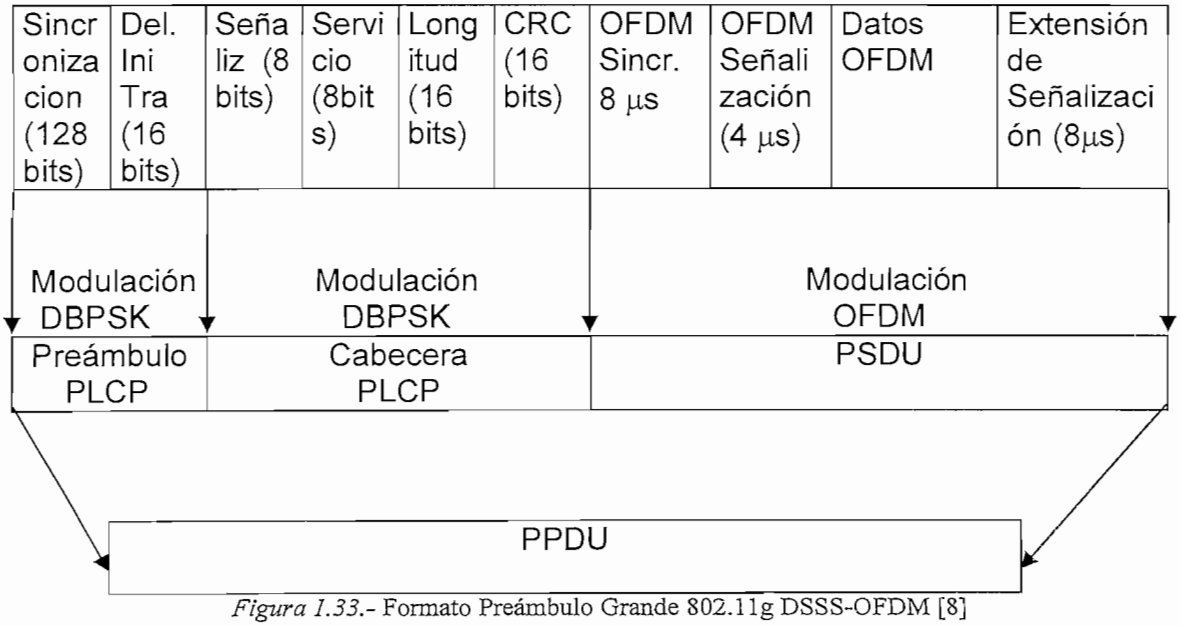


Figura 1.33.- Formato Preámbulo Grande 802.11g DSSS-OFDM [8]

Tanto el preámbulo como la Cabecera PLCP son modulados con DBPSK, mientras que el campo de datos (PSDU) son modulados con OFDM.

1.5.5.3.1 Formación del campo PSDU de DSSS-OFDM

La PSDU está compuesto de 4 secciones principales: Sincronización OFDM, Señalización OFDM, Datos OFDM y Extensión de señalización, como lo muestra la Figura 1.34.

Campo Sincronización OFDM.- Este campo es una secuencia de entrenamiento grande utilizada para adquisición de parámetros de recepción por el demodulador OFDM, consta de 2 símbolos de entrenamiento grandes (3.2 μs) precedidos por un intervalo de guardia (1.6μs). Contiene 52 subportadoras moduladas con DBPSK.

Campo Señalización OFDM.- Este campo provee información al receptor sobre la longitud y velocidad del campo de datos OFDM. Este campo es idéntico al Campo Señalización definido en IEEE 802.11a.

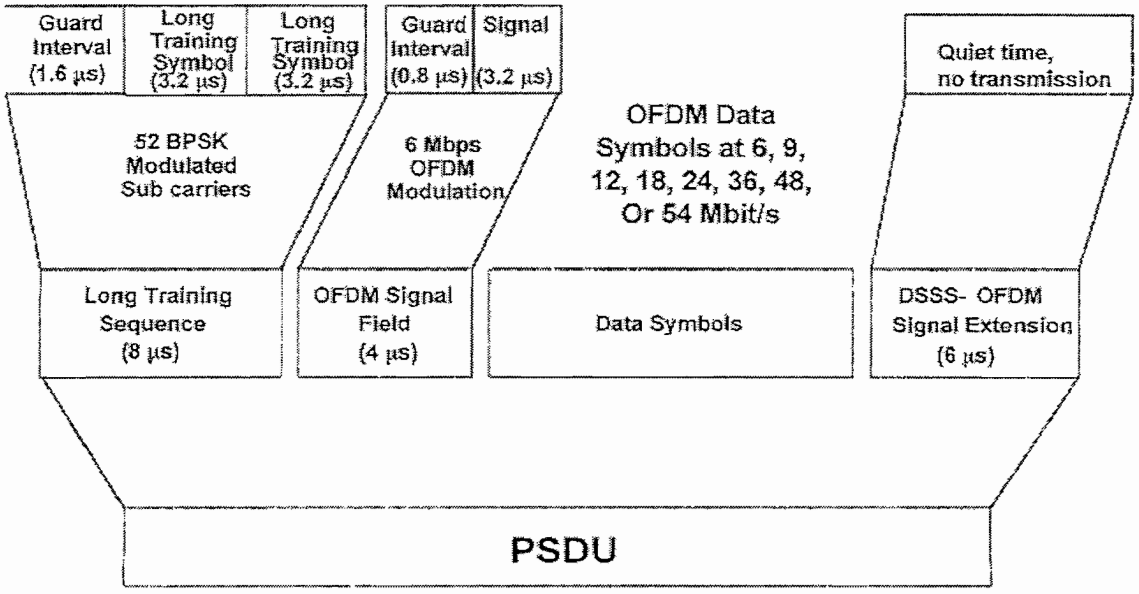


Figura 1.34.- Formación del Campo PSDU de DSSS-OFDM [8]

El campo de Extensión de Señalización ubicado luego del campo de datos es un tiempo en el cual no se transmite, este tiempo es empleado para que el demodulador logre la decodificación de los códigos convolucionales empleados en la modulación.

1.5.5 ERP-CCK (Complementary Code Keying)

El estándar define compatibilidad con la operación de CCK definida en IEEE 802.11b

CCK consta de un conjunto de 64 palabras código de ocho bits usadas para codificar datos a velocidades de 5.5 y 11Mbps en la banda de 2.4GHz. Las palabras código tienen un propósito matemático que permiten ser distinguidos correctamente por el receptor en presencia de ruido e interferencia.

CCK funciona solamente en conjunción con tecnología DSSS que se encuentra especificada en el estándar original de IEEE 802.11. Éste no funciona con FHSS.

CCK aplica fórmulas matemáticas a los códigos DSSS, permitiendo a los códigos representar gran cantidad de información por ciclo de reloj. El transmisor puede enviar múltiples bits de información por cada código DSSS, lo que permite lograr velocidades de hasta 11 Mbps, vea anexo 1.

Por lo estudiado del Estándar IEEE 802.11g se puede apreciar la evolución que se ha presentado en el estándar IEEE 802.11 el cual ha servido de base para el desarrollo y mejoras de nuevos estándares que permiten altas velocidades en comunicaciones inalámbricas.
Es así que hoy en día existen productos que hablan de velocidades de hasta 108 Mbps, las cuales no se encuentran establecidas dentro del estándar aprobado por la IEEE, ya que es IEEE 802.11g el último estándar aprobado hasta la fecha como especificación para medio físico.

1.6 VENTAJAS Y DESVENTAJAS DE 802.11g

Como todos los estándares no es la excepción, el estándar 802.11g tiene tanto sus ventajas como sus desventajas

1.6.1 VENTAJAS

- Facilidad de Instalación. Existen productos en el mercado con muchas facilidades como: administración por Web sencilla y facilidad en la instalación de los equipos y de las tarjetas.

- Movilidad. Las redes tienen un rango de aproximadamente 10 metros alrededor de donde está ubicado el punto de acceso, rango que puede variar de acuerdo a las características del sitio, atenuación, interferencia, desvanecimiento, paredes y otras consideraciones que disminuyen la intensidad de la señal.

- Facilidad de configuración para el usuario. La persona que se va a conectar a la red solo tiene que poner la llave de acceso en caso de que se tenga alguna seguridad configurada, si la red está en tipo de autenticación abierta no será necesario configurar nada, sin embargo esto puede contraer riesgos de seguridad, ya la tarjeta detecta la red automáticamente. Siempre debe existir un compromiso entre las facilidades automatizadas que presentan los equipos y la seguridad que se desea tener.

1.6.2 DESVENTAJAS

- Interferencias.- Se pueden ocasionar por teléfonos inalámbricos que operen a la misma frecuencia, por redes inalámbricas cercanas o incluso por otros equipos conectados de manera inalámbrica a la misma red.

- Velocidad. Las redes cableadas típicamente alcanzan la velocidad de 100 Mbps mientras que las redes inalámbricas estandarizadas alcanzan cuando mucho 54 Mbps, si hablamos propiamente de estándares inalámbricos, existen productos que no cumplen estándares de Jure, es decir establecidos por Ley, sino que establecen (o imponen) sus estándares, y permiten alcanzar velocidades superiores, se habla de hasta 108Mbps en conexiones inalámbricas, por otro lado actualmente se tiene en redes cableadas el

desarrollo de velocidades de hasta 1000Mbps, y por ende un compromiso velocidad-flexibilidad.

- Seguridad. En una red cableada es necesario tener acceso al medio que transmite la información mientras que en la red inalámbrica el medio de transmisión es el aire. Por más que el estudio de seguridad inalámbrica es imperante, no existe sistema 100% seguro, por lo que se tienen mecanismos que pretenden mitigar en parte estas vulnerabilidades. Es por ello que otos estándares han aparecido y continuamente se presentan mejoras.

1.6.3 COMPARACION CON 802.11b Y 802.11a.

En la tabla 1.5 se observa una comparación en cuanto a ventajas y desventajas de 802.11g.

	802.11g	**802.11b**	**802.11a**
Velocidad	Igual que *11a* y mayor que *11b*	Inferior a *11a,g*	Igual que *11g* y mayor que *11b*
Compatibilidad	Si	Si	No
Problemas de Interferencia	Si	Si	No
Rango de cobertura	similar a *11a* Menor que *11b*	Mayor que 11a y 11g	similar a *11a* Menor que *11b*
Costo	Inferior que *11a* y mayor que *11b*	Inferior a *11a,g*	*Superior a 11b,g*
Actualización *(Upgrade de firmware)*	Disponible en puntos de acceso, para incorporar 11a	No	No requiere

Tabla 1.4.- Cuadro Comparativo de 802.11g [7]

1.6.4 OTROS ESTÁNDARES.

Se encuentra en desarrollo el estándar 802.11n. Dos son las tecnologías que compiten actualmente para que el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) lo convierta en el próximo estándar. El primero es WWiSE (WorldWide Spectrum Efficiency) que es apoyado por Texas Instruments, Broadcom, Conexant, STMicro, Airgo y Bermai. WWiSE cree que 802.11n necesita ser capaz de usar el canal con 20Mhz de ancho, el mismo que 802.11b y 802.11g. emplear

MIMO (*Multiple Input, Multiple Output*) entre técnicas de antenas y el actualmente usado OFDM.

El segundo es TGn Sync, fundado por Agere Systems y apoyado por Cisco, Intel, Nokia, Nortel, Philips, Sony y otros. Como WWiSE, TGn Sync planea emplear el canal de 40Mhz y usar la tecnología MIMO.

Capítulo 2
Diseño de la Red Inalámbrica

2 DISEÑO DE LA RED INALÁMBRICA

Los problemas que se tiene actualmente en el campus para garantizar conectividad de red, disminuir problemas de conectividad, solucionar de manera ágil nuevos requerimientos en cuanto a puntos de red hacen del diseño inalámbrico la mejor alternativa.

La realización del diseño en 802.11g permitirá solucionar estos inconvenientes, garantizar conectividad de red donde se requiera, ofrecer mayores velocidades y garantizar compatibilidad con equipos portátiles que tienen el estándar 802.11b instalado en ellas por defecto. Ofrecerían las ventajas de ser portátiles y tener conexión a la red con movilidad dentro del campus.

Para elaborar esta red inalámbrica empleando IEEE 802.11g en la banda de 2.4 GHz se deben realizar ciertos procedimientos que permitan una elaboración completa y detallada del diseño, en este capítulo se tratarán estos aspectos:

- El estado actual del la red.
- Consideraciones generales del diseño.
- Descripción y evaluación del sitio.
- Análisis de requerimientos.
- Políticas de seguridad en la red.
- Estudio de productos.
- Comparación de alternativas.
- Seleccionarlos en base a criterios técnico – económicos, y finalmente
- Determinar el diseño de la red en base a criterios establecidos, y criterios del autor.

2.1 ESTADO ACTUAL DE LA RED. CONSIDERACIONES GENERALES

El Campus El Dorado es propiedad de la Empresa Eléctrica Quito S.A., se encuentra ubicado en el Sector El Dorado en la parte Sur-Oriental de la ciudad de Quito, en el contorno de la calle Yaguachi.

El Campus presta el servicio a entidades departamentales como son Alumbrado Público, Operación y Mantenimiento Urbano de Redes, Acometidas, Departamento de Personal, Laboratorio de Medidores, Laboratorio de Transformadores, Departamento de Clientes Especiales, Seguridad Industrial, Departamento de Subestaciones, División de Talleres y Transportes, Operadores de Red, Construcción de Redes, Pérdidas Comerciales, Mecánica Automotriz y Mecánica Industrial.

Existen adicionalmente áreas como son de bodega de cables, bodega de materiales, que por su naturaleza no permiten un adecuado tendido de cableado.

2.1.1 DISTRIBUCIÓN POR EDIFICACIONES

En el campus se tiene diferentes edificaciones, las cuales se describen a continuación:

- Edificio Polifuncional.- alberga los siguientes departamentos: Alumbrado Público, Laboratorio de Medidores, Departamento de Clientes Especiales, Operadores de Red, Seguridad Industrial, Departamento de Subestaciones, División de Talleres y Transportes.

Cercano al Edificio Polifuncional se encuentran otras edificaciones:

- Departamento de Acometidas.
- Departamento de Personal.
- Operación y Mantenimiento Urbano de Redes.
- Mecánica Automotriz.
- Laboratorio de Transformadores, y
- Mecánica Industrial.

2.1.2 CABLEADO ESTRUCTURADO ACTUAL

De la infraestructura actual existente en el campus serán pocos los recursos que se reutilizarán, debido al no cumplimiento de normas de estandarización en cuanto a Cableado Estructurado, cabe recalcar que las aplicaciones que circulan por la red de datos actualmente se encuentran funcionando.

2.1.2.1 Cuarto de Equipos

El cuarto de equipos se encuentra en el tercer piso del Edifico Polifuncional, en la División de Talleres y Transportes.

En el cuarto de equipos se encuentra la interconexión a la Matriz de la Empresa Eléctrica Quito ubicada en el edificio Las Casas, su enlace es por medio de Fibra Óptica monomodo 8.3/125 µm.

2.1.2.2 Cableado Horizontal

En el cableado horizontal, la norma especifica la utilización de canaletas para llegar a las distintas áreas de trabajo, el uso de faceplates, jack RJ-45 y patchcords para la conexión de computadoras. Estos requerimientos no se tienen en el campus, por este motivo un diseño inalámbrico en lugar de la instalación de un cableado horizontal será beneficioso.

2.1.2.3 Cableado Vertical

La interconexión de edificios se realiza mediante cable UTP cat5e por tubería que interconecta el cuarto de equipos con los demás pisos del Edificio Polifuncional y de igual manera, el paso de cable UTP cat5e que interconecta mediante tubería el cuarto de equipos con los edificios adyacentes

2.1.3 EQUIPO ACTIVO EXISTENTE

Dentro del campus se encuentra presente equipo activo que por sus características técnicas se puede reutilizar, mientras que hay otro equipo que no servirá a la finalidad propuesta en el presente proyecto. En el cuarto de equipos se tienen convertidores de medio Fibra Óptica-FastEthernet 100 Mbps, y como switch principal un Catalyst Cisco 2950-24 , mostrado en la Figura 2.1

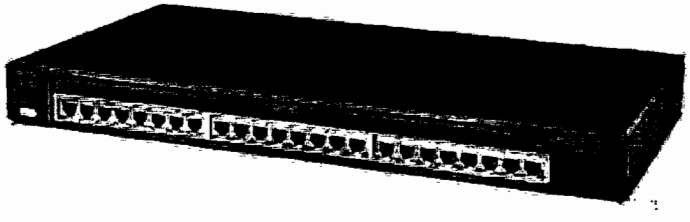


Figura 2.1.- Switch Cisco Catalyst 2950-24

El equipo existente en el campus es el resumido en la Tabla 2.1

Departamento	Equipo activo
Cuarto de Equipos	Switch Cisco Catalyst2950 24 puertos, 10/100 Mbps autonegociación, autosensing, administrable capa2.
Bodega de cables	Switch 3com Office Connect, 8 puertos, 10/100 Mbps.
Laboratorio de Medidores	Switch 3com Baseline no administrable, 24 puertos, 100Mbps.
Operación y Mantenimiento Urbano.	Switch 3com Baseline no administrable, 24 puertos, 100Mbps.
Clientes Especiales	Switch 3com Office Connect, 8 puertos, 10/100 Mbps
Alumbrado Público	Switch 3com Office Connect, 8 puertos, 10/100 Mbps
Acometidas	Hub 4 puertos, 1 up-link.
Personal	Switch 3com Office Connect, 8 puertos, 10/100 Mbps

Tabla 2.1.- Equipo activo por departamentos

2.1.4 APLICACIONES QUE SOPORTA LA RED

La Empresa Eléctrica Quito S.A. al ser una empresa pública que presta el servicio eléctrico a la ciudad, tiene sus necesidades como tal, en cuanto a aplicaciones que ayudan al normal desempeño de la misma.

➢ Aplicaciones adquiridas, entre las principales se tiene:

- El uso de correo electrónico mediante Lotus Notes v5.3
- Microsoft Office 2000.- en el uso de edición de documentos
- Internet Explorer v5.1 ó v6.0.- en el uso web.
- Chamaleon.- para el acceso a servidores en Unix de la empresa.
- Oracle Developer 6i.- En el desarrollo de formas Oracle para el desarrollo de sistemas de la empresa.

➢ Aplicaciones propias, entre las principales se tiene las desarrolladas por la División de Sistemas:

- SIDECOM (Sistema de Comercialización)
- Sistema de Recursos Humanos para control de personal
- Sistema de Talleres y Transportes
- Sistema de Distribución
- Sistema de Bodegas y
- La Intranet.

➢ Tipos de Tráfico.- El tráfico que circula por la red es de los siguientes tipos, los cuales ocupan un ancho de banda determinado:

- FTP.- (*File Transfer Protocol*) Es un protocolo empleado para el paso de información mediante la transferencia de archivos.
- SMTP.- (*Simple Mail Transfer Protocol*) el cual es empleado para transferencia de correo de la empresa mediante el Lotus Notes.
- Telnet.- Empleado para establecer conexiones con el servidor principal de la empresa (SP), u otros servidores Unix, y realizar transacciones tipo carácter.
- Http (*Hiper Text Transmission Protocol*).- Este tipo de tráfico es empleado para acceso a servidores web, por medio de cualquier navegador.
- Ping.- Empleado por los Administradores de Red para comprobar que existe comunicación entre dos extremos.

El tráfico total generado por El Dorado tiene un promedio de 200 kbps, y no supera el 1 Mbps, esto se puede comprobar desde un software de monitoreo de tráfico como el mrtg (*multi router traffic grapher*), el cual se encuentra configurado en la empresa, esto se puede observar en el gráfico de figura 2.2.

Máx Entrante:	317.1 kb/s (0.3%)	Promedio Entrante:	64.6 kb/s (0.1%)	Actual Entrante:	29.0 kb/s (0.0%)
Máx Saliente:	1239.4 kb/s (1.2%)	Promedio Saliente:	204.8 kb/s (0.2%)	Actual Saliente:	73.6 kb/s (0.1%)

Figura 2.2.- Tráfico de El Dorado

2.1.5 CONSIDERACIONES GENERALES DE DISEÑO

En un diseño de red inalámbrica se deben considerar varios factores que ayudan a garantizar un mejor desempeño de la red, entre estos se tiene: distorsión por múltiples trayectorias, dualidad de antenas, áreas de cobertura, velocidades de conexión, escalabilidad y usuarios a servir.

2.1.5.1 Distorsión por Múltiples Trayectorias.

Cuando una señal de radio frecuencia (*RF*) viaja de un lugar a otro entre un receptor y un transmisor, toma más de un camino, lo cual causa distorsión de la señal, produce una alteración de la señal degradándola, como lo muestra la Figura 2.3.

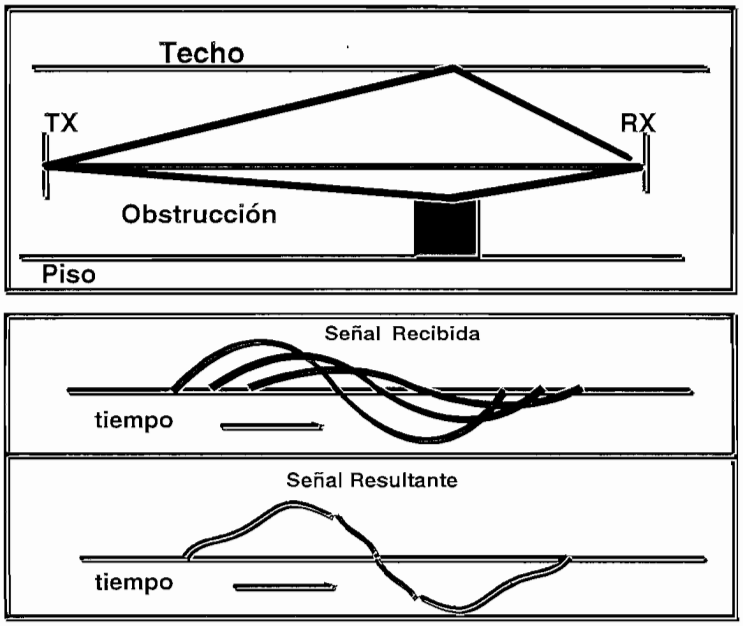


Figura 2.3.- Distorsión por Múltiples Trayectorias [10]

2.1.5.2 Diversidad de antenas.

En un ambiente de múltiples caminos, existen puntos nulos donde no existe señal, estos puntos se encuentran en el contorno del área que se quiere cubrir debido a obstáculos.

Es necesario moverse del punto nulo para recibir una señal correcta.

El concepto de antenas duales significa que, si una antena está en un punto nulo, la otra no la estará, por lo tanto se provee un mejor desempeño en ambientes de múltiples caminos, así lo muestra la Figura 2.4.

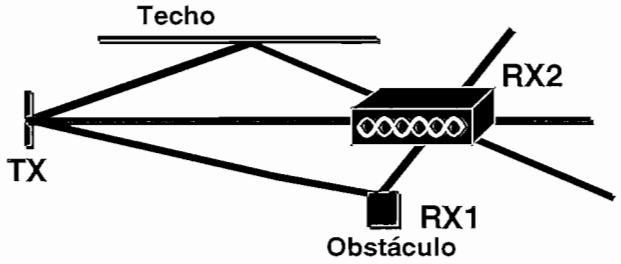


Figura 2.4.- Antenas Duales.

2.1.5.3 Áreas de Cobertura y Velocidades de Conexión

Este es un concepto contrapuesto al hablar de comunicaciones inalámbricas ya que, entre mayor sea el área de cobertura, menor será la velocidad a la cual se establece la conexión, así lo indica la Figura 2.5. En IEEE 802.11g se permiten velocidades de 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, y 54 Mbps, como se explicó anteriormente. En ocasiones no es solución el aumentar ganancia de antenas ya que se produce mayor interferencia con canales adyacentes.

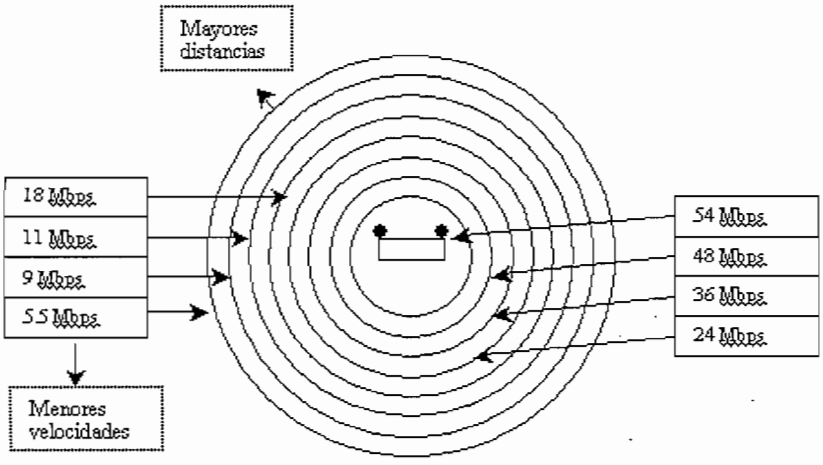


Figura 2.5.- Áreas de Cobertura y Velocidades de Conexión

2.1.5.4 Escalabilidad

Se puede emplear canales que no se interfieran con la finalidad de aumentar la velocidad de conexión, así por ejemplo se puede tener la utilización de 3 canales no interferidos en IEEE 802.11b, como lo muestra la Figura 2.6, logrando una velocidad de 33 Mbps.

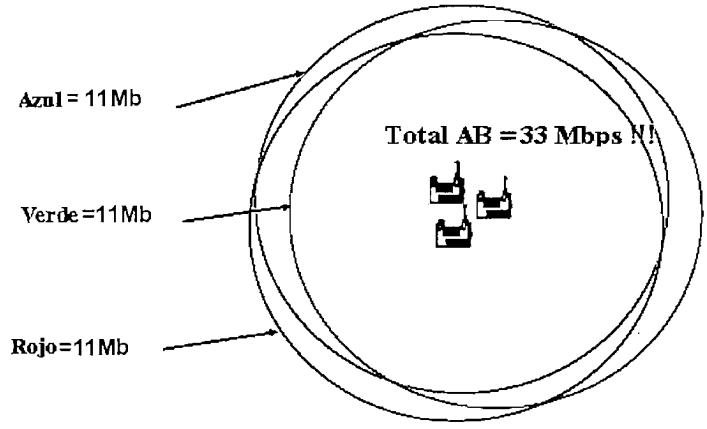


Figura 2.6.- Escalabilidad Inalámbrica [10]

2.1.5.5 Usuarios a Servir

La cantidad de usuarios a servir está determinada por las necesidades de la empresa, hay que considerar un crecimiento futuro, lo que permite definir un número total. Un punto de acceso sirve a determinada cantidad de usuarios, por lo cual se puede determinar la ubicación de los mismos para tratar de garantizar el mejor diseño.

2.2 ANÁLISIS DE REQUERIMIENTOS Y EVALUACIÓN DEL TERRENO.

En el presente proyecto se pretende rescatar recursos que se pueden reutilizar en el diseño de la red inalámbrica, y realizar adquisiciones, modificaciones y mejoras, esta sección especifica estos requerimientos.

2.2.1 ANÁLISIS DE REQUERIMIENTOS

En el campus El Dorado se generan Órdenes de Trabajo para la atención de diferentes tareas y atiende el personal operativo para el servicio de distribución de

energía eléctrica a la ciudad de Quito y sus alrededores, por tanto es imprescindible un adecuado funcionamiento de todos los componentes de comunicaciones, es por este motivo que en esta sección se estudiarán todos los requerimientos que se presentan en el sitio, tanto en el cuarto de equipos así como cantidad de usuarios.

2.2.1.1 En el Cuarto de Equipos

Como se mencionó anteriormente el Cuarto de Equipos está ubicado en el tercer piso del Edificio Polifuncional, el cual necesita equipamiento, para garantizar un mejor funcionamiento de red, minimizar daños, mejorar facilidades de administración y cumplir con normativas de cableado estructurado, para comodidad del lector el requerimiento en el cuarto de equipos se encuentra especificado en la sección 2.8.10.

2.2.1.2 Usuarios por Departamentos

El número de usuarios en las áreas de trabajo que requieren acceso a la red de datos, se encuentran distribuidas en los departamentos que se especifican en la Tabla 2.2.

Tabla 2.2.- Usuarios por Departamentos

Edificio Polifuncional

Primer piso	
Departamento	**Número de Usuarios**
Laboratorio de Medidores	11
Clientes Especiales	6
Operadores de Red	3

Segundo piso	
Departamento	**Número de Usuarios**
Seguridad Industrial	2
Departamento de Subestaciones	1

Tercer piso	
Departamento	**Número de Usuarios**
División de Talleres y Transportes	8
Alumbrado Público	5

Edificación (Mantenimiento Urbano)

Planta Baja	
Departamento	**Número de Usuarios**
Operación y mantenimiento urbano de redes.	9

Edificación (Acometidas)

Planta Baja	
Departamento	**Número de Usuarios**
Acometidas	9

Edificación (Personal)

Planta Baja	
Departamento	**Número de Usuarios**
Personal	2

Edificación (Construcción de redes)

Planta Baja	
Departamento	**Número de Usuarios**
Construcción de redes	3
Pérdidas Comerciales	3

Edificación (Mecánica Automotriz)

Planta Baja	
Departamento	**Número de Usuarios**
Mecánica Automotriz	2
Gasolinera	1
Mantenimiento Hidráulico grúas	1

Edificación (Taller Industrial)

Planta Baja	
Departamento	**Número de Usuarios**
Taller Industrial	1

Edificación (Laboratorio de Transformadores)

Planta Baja	
Departamento	**Número de Usuarios**
Laboratorio de Transformadores	2

Edificación (Bodegas)

Planta Baja	
Departamento	**Número de Usuarios**
Bodega de Distribución	1
Bodega de Instalaciones	2
Bodega Automotriz	1

Total de **usuarios = 73**

2.2.2 EVALUACIÓN DEL TERRENO

La superficie del campus es inclinada debido a la forma del terreno, mientras que las edificaciones del lugar se asientan en terreno plano, la construcción del Edificio Polifuncional se realizó mediante la elaboración de planos que se encuentran archivados en el departamento de Ingeniería Civil de la Empresa Eléctrica Quito S.A. (Las Casas)

Sin embargo estos planos fueron elaborados manualmente, por lo que no existe en medios magnéticos.

Las necesidades del transcurso de los años han implicado modificaciones arquitectónicas que no se especifican en los planos realizados, como construcción de nuevos pisos, edificaciones adjuntas y demás. Es por este motivo que se ha realizado el levantamiento de los planos y sus modificaciones en medios magnéticos, con la finalidad de tener información de los planos arquitectónicos actualizados, prever futuros crecimientos, y necesidades.

2.3 PROCEDIMIENTO DE DISEÑO

Para el Diseño de Red Inalámbrica se han seguido los siguientes pasos para garantizar un correcto desempeño.

2.3.1 PROCEDIMIENTOS A SEGUIR

1. Efectuar el levantamiento de los planos, con la finalidad de tener la infraestructura arquitectónica actual, y prever crecimiento futuro.
2. Realizar el análisis de requerimientos para dimensionar el equipamiento existente.

3. Determinar qué equipo se va a adquirir

3.1. Determinación del número de usuarios.

3.2. Análisis de equipos terminales, que son utilizados por los usuarios con la finalidad de determinar que interfaces se emplearán en las computadoras, (PC Cards por ejemplo).

4. Determinar la topología del diseño propuesto.

5. De los puntos de acceso determinar:

5.1. Áreas de cobertura

5.2. Capacidad máxima de usuarios que puede servir

5.3. Facilidades de administración y seguridad

6. Determinar la ubicación que deben tener los puntos de acceso para garantizar conectividad a los usuarios.

7. Determinar la distancia máxima y mínima entre usuarios y cuarto de equipos para determinar el número de corridas necesarias para el tendido del cableado, o realizar una medición de distancias mediante el método exacto para el cálculo de corridas.

8. Establecer todos los requerimientos adicionales al diseño como: canaletas, *faceplates*, *jacks*, *racks*, *patchpanel* y demás accesorios.

2.3.2 CONSIDERACIONES:

- Es necesario que luego de la elaboración del diseño se realicen las respectivas pruebas de campo para garantizar cobertura a todos los usuarios, y minimizar los puntos nulos de señal.
- La presencia de obstáculos pueden no haber sido considerados en el diseño pero estar presentes físicamente en el terreno.
- Consideraciones de seguridad son necesarias al tener como medio de transmisión el aire, por lo que el establecimiento de políticas de seguridad deben ser previstas.

2.4 POLÍTICA DE SEGURIDAD

La seguridad es un aspecto muy importante que se debe considerar en un diseño de red inalámbrica, en el capítulo anterior se mencionó algunos aspectos básicos de seguridad, sin embargo existen otras consideraciones a ser tomadas en cuenta

que en conjunto y bajo la aplicación de ciertas reglas constituyen las políticas de seguridad.

Es conveniente conocer todas las vulnerabilidades que puede tener un sistema para poder minimizar los riesgos y evitar ataques a la red, es por este motivo que en esta sección se describen los ataques que pueden suceder, soluciones que minimizan estas vulnerabilidades, y finalmente se especificará una política de seguridad que se sugiere sea establecida en conjunto con la implementación de la red inalámbrica.

Se puede mitigar riesgos a redes WLAN mediante la aplicación de medidas que dirijan y controlen ataques y vulnerabilidades específicas. Una correcta administración combinada con medidas técnicas y operacionales pueden reducir de manera los riesgos asociados.

Las siguientes líneas guía no previenen todas las penetraciones de adversarios, pero tratan de garantizar un ambiente de interconexión inalámbrica segura. Se describirá los pasos necesarios que se deben tomar en cuenta para mitigación de riesgos, reconociendo que es imposible remover todos. Adicionalmente, una política de seguridad no es una solución de tamaño fijo para todas las soluciones cuando se trate de seguridad. Algunas políticas serán tolerables a más riesgos que otras, ya que seguridad involucra costos, y el dinero que se utilice en equipamiento de seguridad no proporciona rentabilidad económica , y es un inconveniente su mantenimiento o en gastos operativos. Algunas políticas no pueden ser aceptadas, y se toman ciertos riesgos debido a un exceso en el contraste financiero.

Las medidas de administración para seguridad en redes inalámbricas comienzan por una *política* de seguridad comprensiva.

Una política de seguridad, y el cumplimiento de ella, es fundamental para otras medidas operacionales y técnicas relacionadas e implementadas. La Política de seguridad en la red WLAN será estructurada de la siguiente manera:

- Identificar quien puede usar tecnología WLAN.
- Identificar en que lugares el acceso a Internet es requerido.

- Describir el tipo de información que puede ser enviada sobre enlaces inalámbricos.
- Los estándares de seguridad para puntos de acceso, serán Filtrado MAC, Encripción WEP.
- Se empleará servidor de autenticación Radius
- Proporcionar líneas guía sobre reportes de pérdidas de dispositivos inalámbricos e incidentes de seguridad.
- Proporcionar una guía sobre el uso de encripción y administración de llaves.
- Definir la frecuencia y alcance de estas políticas.

Administradores de red deben estar completamente prevenidos de los riesgos de seguridad que una WLAN y dispositivos poseen. Ellos deben asegurar el cumplimiento de la política de seguridad y conocer que procedimientos tomar en el caso de presentarse un ataque. Finalmente, lo más importante es entrenar en estas medidas y prevenir a los usuarios.

Como políticas administrativas de seguridad física de equipos podemos citar:

- Describir quién puede instalar puntos de acceso y otro equipamiento inalámbrico.
- Proporcionar limitaciones en la localización de puntos de acceso por seguridad física.
- Describir las configuraciones de hardware y software de todos los dispositivos.
- Entrenamiento del personal para el uso de tecnología inalámbrica.

2.5 PRODUCTOS EXISTENTES EN EL MERCADO

El diseño de una red LAN inalámbrica se encuentra sujeto al tipo de producto que sea escogido para cubrir las necesidades requeridas, las capacidades de estos equipos, y los beneficios técnicos que proporcionen. Por este motivo, un estudio acerca de qué productos se tienen en el mercado es primordial, un análisis de sus características, permite lograr un conocimiento más amplio de los mismos.

Entre varias marcas se ha seleccionado a 2 que proporcionan equipos que cumplen con el estándar IEEE 802.11g que será empleado en el diseño. Estas empresas fabricantes seleccionadas son 3Com y Cisco.

2.5.1 PUNTO DE ACCESO 3Com 8250

Entre los puntos de acceso 3Com presenta productos de niveles personales y corporativos, el modelo 3Com Wireless LAN Access Point 8250, mostrado en la Figura 2.7 presenta características acordes a requerimientos empresariales.

Figura 2.7.- Punto de Acceso 3Com 8250

Características AP 8250

- Crea una LAN inalámbrica de clase empresarial que soporta hasta 253 usuarios simultáneos.
- Proporciona la opción de selección de canal (*Clear Channel Select).*
- Conexión automática a la red
- Negociación de velocidades de conexión automática
- Soporta PoE (*Power over Ethernet*).
- Diversidad de antenas
- Opción de antenas externas.
- Compatibilidad con IEEE 802.11b.
- Encriptación WEP de clave compartida de 40/64 bits y 128/54 bits,
- Encriptación avanzada WPA, AES de 256 bits
- El enlace dinámico de seguridad automáticamente asigna claves de encriptación de 128 bits, específicas para cada usuario en las sesiones inalámbricas.
- Autentificación 802.11x del servidor RADIUS.
- Administración dinámica de claves de sesión
- TKIP como mejora de seguridad
- ACLs a nivel de direcciones MAC.

- Asignación dinámica de VLAN, utilizada con autentificación RADIUS, les provee a los usuarios una VLAN adecuada, protegiendo el acceso a los recursos de la red.
- Soporte de gestión SNMP.
- Herramienta de Administración de Infraestructura Inalámbrica *(Wireless Infrastructure Device Manager)*
- Utilidad de descubrimiento de dispositivos en LANs Inalámbricas *(Wireless LAN Device Discovery)* mediante un navegador Web.
- Protocolo de acceso al medio CSMA/CA.
- Alcance operativo de hasta 100 metros (328 pies) de transmisión y recepción.
- Sistemas operativos Windows XP/2000 ME/SE98/95b+/NT 4.0

2.5.2 ADAPTADOR PCI INALÁMBRICO 3Com

En cuanto a Adaptadores PCI inalámbricos 3com proporciona su producto 3Com 11a/b/g Wireless PCI Adapter mostrado en la Figura 2.8.

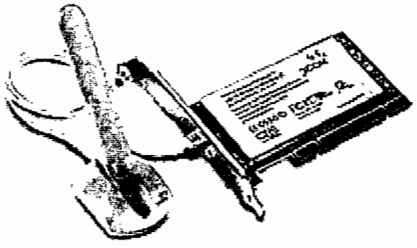


Figura 2.8.- 3Com 11a/b/g Wireless PCI Adapter

Características

- Soporta IEEE 802.11a, 11b, y 11g, compatibilidad Wi-Fi.
- Velocidades de hasta 54 Mbps o 108 Mbps en modo turbo.
- Soporta WPA, AES, y WEP.
- Autenticación MD5, 802.1x, y EAP

2.5.3 PC CARD INALÁMBRICAS 3Com

El uso de PC Card es adecuado para equipos portátiles (laptops), 3com ofrece PC Card entre los cuales se tiene el producto 3com Wireless 11a/b/g, mostrado en la Figura 2.9.

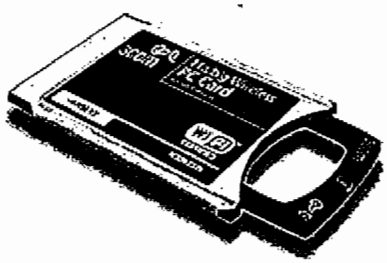


Figura 2.9.- 3Com PC Card 11a/b/g

Características

- Soporte de estándares IEEE 802.11a, 11b, y 11g.
- La certificación Wi-Fi.
- El Control de Acceso de Red IEEE 802.1x
- Protocolos EAP-TLS, PEAP, y EAP-TTLS.
- Encriptación avanzada AES de 152 bits,
- Encriptación RC4 por clave compartida WEP de 40/64, 128 y 154 bits
- Velocidades de hasta 54 Mbps en redes 802.11g o 802.11a.
- Balanceo Autónomo de Cargas (ALB).- se conecta al punto de acceso que proporciona el mejor señal.
- Cambio dinámico de velocidad
- Antena patentada XJACK de 3com.

2.5.4 PUNTO DE ACCESO CISCO

Entre los puntos de acceso, Cisco presenta productos de niveles personales y corporativos; el modelo Cisco Aironet de la serie 1200, mostrado en la Figura 2.10, presenta características acordes a requerimientos empresariales.

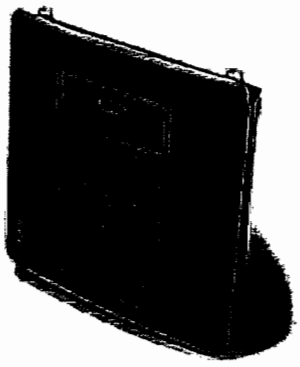


Figura 2.10.- Cisco Aironet 1200 Access Point

Características AP 1200

- Nivel empresarial de redes inalámbricas.

- Extiende aspectos de seguridad, escalabilidad, confiabilidad,
- Administración desde la red cableada a la WLAN.
- Diseño modular para un alto desempeño en puntos de acceso empleando 802.11g con configuración de antena simple o dual.
- Kit que permite el soporte de 802.11a,.
- Tiene soporte para 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA.
- Diversos tipos de autenticación EAP.
- Soporta IEEE 802.1X, TKIP (*Temporal Key Integrity Protocol)* para encripción WPA, y AES (*Advanced Encryption Standard*) para encripción WPA2, y el algoritmo de encripción RC4.
- Rangos de cobertura: Exteriores

Velocidad (Mbps)	54	48	36	24	18	12	11	9	6	5.5	2	1
Alcance (m)	34	61	69	99	122	145	149	168	198	201	210	213
Alcance (ft)	110	200	225	325	400	475	490	550	650	660	690	700

- Rangos de cobertura: Interiores

Velocidad (Mbps)	54	48	36	24	18	12	11	9	6	5.5	2	1
Alcance (m)	27	29	30	43	55	64	67	76	91	94	107	125
Alcance (ft)	90	95	100	140	180	210	220	250	300	310	350	410

2.5.5 ADAPTADOR PCI INALÁMBRICO CISCO

Los adaptadores PCI de Cisco Aironet IEEE 802.11a/b/g inalámbricos son los indicados en la Figura 2.11.

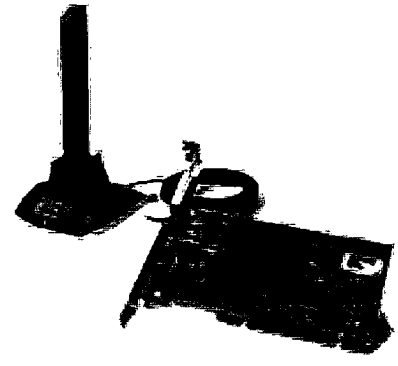


Figura 2.11.- Adaptador PCI Cisco Aironet 802.11a/b/g

Características

- Soporta IEEE 802.11b, 11g, y 11a, o modos combinados 802.11a/g o 802.11a/b/g, el adaptador cumple con Wi-Fi.
- Velocidades de hasta 54 Mbps en las bandas de 2.4 y 5 GHz
- Proporciona buen desempeño, seguridad y administrabilidad.
- La antena proporciona una ganancia de 1 dBi lo cual proporciona flexibilidad en la instalación y óptima ubicación para su desempeño.
- Comunicación de red segura mediante el componente de seguridad inalámbrica de Cisco (*Cisco Wireless Security Suite)* y soporte para WPA (*Wi-Fi Protected Access).*
- Utilidades, fácil configuración y administración.
- Características de Roaming

El sistema de clase empresarial *Cisco Wireless Security Suite* está basado en la arquitectura de 802.1X mostrada en la Figura 2.12, en el cual el adaptador PCI Cisco Aironet 802.11a/b/g es un componente instalado en el sitio del cliente.

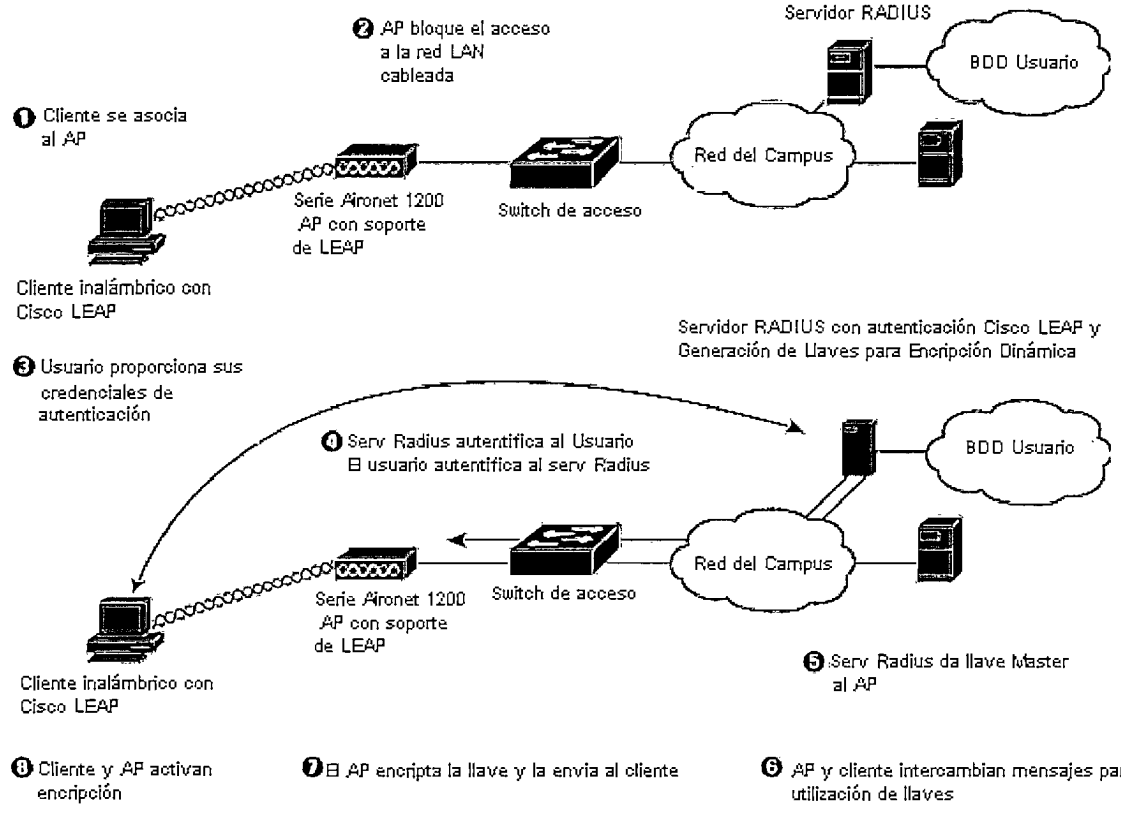


Figura 2.12.- Seguridad Basada en Arquitectura 802.1X de Cisco.

- Soporta autenticación EAP, en particular LEAP (propietaria de Cisco).
- Soporte de velocidades IEEE 802.11a/b/g,
- Protocolo de acceso al medio CSMA/CA
- Emplea como modulación DSSS:

• *Differential Binary Phase Shift Keying* (DBPSK) a 1 Mbps
• *Differential Quadrature Phase Shift Keying* (DQPSK) a 2 Mbps
• *Complementary Code Keying (*CCK) a 5.5 y 11 Mbps

- Adicionalmente modulación OFDM

• BPSK a 6 y 9 Mbps
• QPSK a 12 y 18 Mbps
• 16-Quadrature Amplitude Modulation (QAM) a 24 y 36 Mbps
• 64-QAM a 48 y 54 Mbps

- Puede trabajar en diferentes bandas de frecuencia:

• 2.40 a 2.4897 GHz
• 5.15 a 5.35 GHz (FCC UNII 1 y UNII 2)
• 5.725 a 5.85 GHz (FCC UNII 3)
• 5.15 a 5.35 GHz (ETSI)
• 5.470 a 5.725 (ETSI)
• 5.15 a 5.25 GHz (Japan)

2.5.6 ADAPTADOR PC CARD CISCO

El adaptador PC Card de Cisco es el indicado en la figura 2.13, es compatible con los estándares IEEE 802.11b IEEE 802.11a , y 802.11g,

Figura 2.13.- PC Card Cisco 802.11a/b/g.

Características Técnicas

- Controladores para la mayoría de los sistemas operativos, incluyendo Windows 95, Windows 98, Windows NT, Windows CE, Windows 2000, Windows XP, Macintosh, y Linux.
- Velocidades de conexión de hasta 54 Mbps, acorde al estándar que maneje el punto de acceso, si el punto de acceso solamente maneja IEEE 802.11b las velocidades se encontrarán limitadas a las velocidades soportadas por el punto de acceso (1, 2, 5.5 y 11 Mbps).
- Provee libertad, y flexibilidad en la WLAN. Laptops o PCs notebook, con tarjetas adaptadoras PCMCIA, se pueden mover libremente a través de un campus, mientras se mantiene la conectividad a la red.
- Posee el manejo de WEP con hasta 128 bits para seguridad de los datos.
- Posee leds identificadores del estado de la tarjeta, un led verde indica su estado, si existe enlace con el punto de acceso, si está en proceso de asociación, en modo Ad Hoc, de acuerdo a la duración de parpadeo o encendido permanente, un led naranja es el indicador de tráfico RF en la tarjeta. Estos componentes ayudan a detectar errores y facilitar soluciones.
- Posee una utilidad que se instala en el cliente que permite una administración más efectiva del enlace de comunicaciones.
- Permite el establecimiento de dualidad de antenas.
- Especificar un punto de acceso preferido de conexión así como puntos de acceso alternos.
- La tarjeta PC Card integra una antena la cual opera mejor en el modo de diversad, la que permite usar la mejor señal desde la antena derecha o izquierda.
- Permite la configuración de parámetros de seguridad, como WEP, mejoras TKIP,

  EAP, y sus protocolos propietarios como LEAP.

2.6 COMPARACIÓN DE ALTERNATIVAS

Entre los puntos de acceso de nivel empresarial que se han seleccionado como posibles soluciones para el diseño de la Red LAN Inalámbrica se tiene el punto de acceso 3Com con su producto AP 8250 y Cisco con su producto Aironet 1200.

2.6.1 COMPATIBILIDAD

El soporte de múltiples estándares lo cual proporciona soporte universal, completo acceso al manejo de redes inalámbricas IEEE 802.11a, 802.11b, y 802.11g.
Tanto los productos de Cisco como de 3Com cumplen con estas características, Cisco ofrece una forma de operación adicional en la cual se combina los estándares.

2.6.2 CERTIFICACIÓN Wi-Fi

Ayuda a asegurar que los adaptadores PCI puedan operar con productos de otros fabricantes que tengan compatibilidad de Wi-Fi.
Cisco y 3Com ofrecen estas características.

2.6.3 SEGURIDAD

Para manejar un nivel alto de seguridad en la red inalámbrica se tiene adicionalmente al uso de WEP, WPA y TKIP:

3Com con 802.1x con los protocolos EAP-TLS, PEAP, EAP-TTLS
Cisco con 802.1x con los protocolos anteriores y adicionalmente LEAP, lo cual es una ventaja ya que no se requiere el uso de certificados digitales

2.6.4 DESEMPEÑO Y CONFIABILIDAD

Alto desempeño corresponde al soporte de un buen funcionamiento a velocidades de hasta 54 Mbps en 802.11g o redes 802.11a. Sin embargo esta característica no puede ser apreciada hasta cuando la red se encuentra operativa y con plena carga.

2.6.5 CONMUTACIÓN AUTOMÁTICA DE VELOCIDAD

Referido al cambio automático de velocidad acorde a la potencia de la señal entre el transmisor y el receptor, lo cual garantiza la mejor conexión, tanto el equipamiento de 3Com como Cisco ofrecen esta característica en sus productos.

2.6.6 FACILIDAD DE USO

La creación de perfiles para administración en la red inalámbrica especifica una configuración del cliente, información sobre el estado de conexión.

Las opciones de configuración y administración permitidas se comparan establecen en la tabla 2.3

2.6.7 RANGO

El alcance operativo de Cisco es mayor que 3Com como se aprecia en la tabla 2.3

Estos y otros aspectos son comparados y resumidos en el cuadro comparativo de la Tabla 2.3.

Tabla 2.3.- Comparación de Puntos de Acceso

Descripción	**AP 3Com 8250**	**AP Cisco Aironet 1200**
Soporte de Usuarios	253	253
Selección automática de canal	Disponible	configurable
Conexión automática de velocidades	Disponible	configurable
Administración de energía	PoE	PoE o Cable
Encripción WEP	128 bits	128 bits
EAP	No	EAP, LEAP, LEAP-TLS
WPA	AES 256 bits	TKIP
WPA2	NO	AES
Protocolo de acceso al medio	CSMA/CA	CSMA/CA
autentificación 802.11x	RADIUS	RADIUS, deshabilitación de broadcast de SSID
Soporte de Tkip	Disponible	Disponible
Listas de control de acceso	Disponible	Disponible
Soporte de Vlan	Disponible	Disponible
Administración	*Wireless Infrastructure Device Manager*	*Aironet Desktop Utility* en el cliente
Utilidades	*Wireless LAN Device Discovery* (solo 3Com)	*Upgrade firmware Site survey*
Alcance operativo	hasta 100 metros, 328 pies	Hasta 213m, 700 pies
Sensibilidad receptor a 54 Mbps	54 Mbps: -73 dBm	54 Mbps: –72 dBm

Dimensiones alto/ancho/grosor	32/20/7 cm	4.22 / 16.67 / 18.37 cm
Sistemas operativos para adaptadores	Windows 95, Windows 98, Windows NT, Windows 2000, Windows Xp	Windows 95, 98, NT,Windows CE, Windows 2000, Windows Xp, Macintosh, y Linux

La siguiente tabla hace un cuadro comparativo en cuanto a adaptadores PCI, cuyas funcionalidades son iguales para adaptadores PC Card.

Tabla 2.4.- Comparación de Adaptadores Cliente

Descripción	**Adaptador PCI 3Com**	**Adaptador PCI Cisco**
Soporte de protocolos	IEEE 802.11a/b/g	IEEE 802.11a/b/g
Soporte Wi-Fi	Si	Si
Combinación de bandas	Disponible	Disponible
Configuración de seguridad	Si	Si
Encripción WEP	128 bits	128 bits
EAP	Si	EAP, LEAP, LEAP-TLS
WPA	AES 256 bits	TKIP
WPA2	NO	AES
Autentificación 802.11x	RADIUS	RADIUS, deshabilitación de broadcast de SSID
Manejo de usuarios	Perfil	Perfil
Soporte de Tkip	No	Disponible
Administración	Wireless Infrastructure Device Manager	ACU
Utilidades	Wireless LAN Device Discovery(solo 3Com)	Upgrade firmware Site survey, Cisco Wireless Security Suite
Sistemas operativos para adaptadores	Windows 95, Windows 98, Windows NT, Windows Windows 2000, Windows Xp	Windows 95, Windows 98, Windows NT, Windows CE, Windows 2000, Windows Xp, Macintosh, y Linux

2.7 SELECCIÓN DEL PRODUCTO

Para la selección del producto se deben considerar factores que determinan el tipo de solución que más se acople a las necesidades de la empresa así como a las capacidades adquisitivas en cuanto a equipamiento.

2.7.1 REQUERIMIENTOS MÍNIMOS GENERALES.

La Empresa Eléctrica Quito S.A. tiene como primordial recurso la información de bases de datos, e información confidencial que circula por la red, por este motivo se plantean los siguientes requerimientos mínimos de seguridad:

- Minimizar las vulnerabilidades y reducir los posibles ataques a la red mediante características de seguridad WEP con mejoras TKIP, WPA.
- Mecanismos de encripción y autenticación avanzados con el manejo de 802.1x con protocolos EAP.
- Filtrado MAC con ACLs en el punto de acceso.
- Filtrado de SSID.
- Facilidad de administración y configuración tanto de clientes como de puntos de acceso.
- Compatibilidad con Sistemas Operativos Windows, Linux.
- Buen alcance operativo con la finalidad de obtener un mayor rango de cobertura de los puntos de acceso.

2.7.2 CARACTERÍSTICAS TÉCNICAS

Del análisis de características y comparación de alternativas se concluye que la marca Cisco presenta características técnicas adicionales que permiten un nivel alto de seguridad sin el uso de certificados digitales, mejor rango operativo, filtrado MAC y de protocolos.

2.7.3 COSTO BENEFICIO

El beneficio otorgado por los equipos 3Com es inferior al otorgado por los equipos Cisco al plantear la solución requerida. Aspectos de seguridad son fundamentales en una empresa corporativa. El costo de los puntos de acceso 3Com8250

802.11g es inferior al de Cisco Aironet 1200, cuya diferencia está en alrededor de 200 USD, los adaptadores cliente de Cisco son más costosos que los de la línea 3Com, en aproximadamente 35 USD. El beneficio está en las características técnicas adicionales que brinda Cisco por un costo más elevado comparado con 3Com.

2.7.4 CONCLUSIÓN Y SELECCIÓN

Luego de analizar características y comparar alternativas se ha seleccionado a la marca Cisco con sus productos Aironet como el equipamiento más apropiado de nivel empresarial para equipamiento en el diseño de la red inalámbrica por características robustas de seguridad empresarial como son:

Manejo de LEAP para minimizar tráfico y garantizar seguridad ya que no es necesario el uso de Certificados ni Firmas Digitales que adicionan cantidad de procesamiento en los equipos.

Manejo de filtrado a nivel de protocolos y MAC.

Mejor rango operativo de cobertura.

2.8 INGENIERÍA DE DETALLE DEL DISEÑO PROPUESTO

En esta sección se detalla el procedimiento de ingeniería seguido para el diseño, en su total elaboración, es así que se describen los procedimientos mencionados anteriormente.

2.8.1 GENERALIDADES DE LA SOLUCIÓN

La instalación de la red inalámbrica propuesta para el Campus El Dorado de la Empresa Eléctrica Quito S.A. alberga alrededor de 73 usuarios, por lo que se puede clasificar como una red inalámbrica mediana con perspectivas de crecimiento.

En esta solución no se pretende incurrir en un gasto adicional para seguridad WLAN, por lo que adicionalmente al diseño de la red y la determinación de todo el equipamiento necesario para su funcionamiento se propondrá la configuración de WEP con clave de 128 bits con mejoras, Filtrado MAC, SSID ya que esto

involucra configuración de los equipos, lo cual se hará en la División de Sistemas de la EEQ, sin embargo se plantea al servidor RADIUS como mecanismo de protección y seguridad adicional , el cual tendría un costo de licencia aproximado de 2000 USD [5], éste costo no se incluye en el presupuesto.

2.8.2 DESCRIPCIÓN DEL ESCENARIO

La red planteada tendrá una topología de extensión de la red cableada, el diagrama de la topología de la red se muestra en la Figura 2.14, el trayecto de fibra entre Las Casas – El Dorado tiene una distancia aproximada de 4 km.

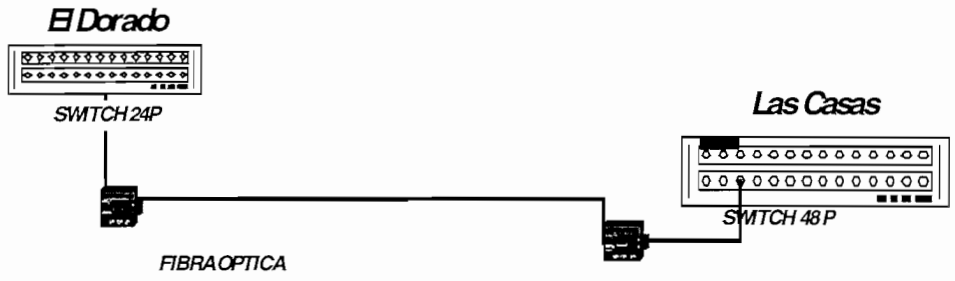


Figura 2.14.- Topología de la red EEQ hacia El Dorado

Los Servidores se encuentran en el Edificio de Las Casas (Matriz), aquí se encuentra la configuración del Servidor Proxy de la red y máscaras de subred.

El diseño de la red inalámbrica tendrá la topología que se indica en la figura 2.15

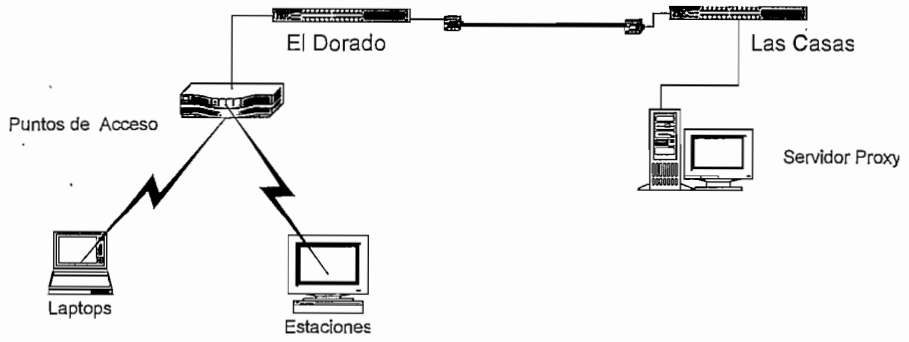


Figura 2.15.- Diagrama Topológico de la Red

2.8.3 LEVANTAMIENTO DE PLANOS

El proceso conlleva la obtención de los planos elaborados en papel y trasladarlos a medio magnético, para ello se ha realizado la visita al lugar, se realizó las respectivas actualizaciones en cuanto a infraestructura existente.

Los planos se encuentran especificados en el Anexo 2.

2.8.4 NÚMERO DE ADAPTADORES PCI INALÁMBRICOS

De acuerdo al número de usuarios existentes y visita en el lugar se ha determinado el número de usuarios que poseen computadoras de escritorio, en cuyo caso se utilizará adaptadores PCI inalámbricos. El número de adaptadores PCI se encuentran resumidos en la Tabla 2.4.

Tabla 2.4.- Adaptadores PCI por Edificaciones

Edificio Polifuncional

Primer piso	
Departamento	**Número de Usuarios**
Laboratorio de Medidores	9
Clientes Especiales	5
Operadores de Red	3

Segundo piso	
Departamento	**Número de Usuarios**
Seguridad Industrial	2
Departamento de Subestaciones	1

Tercer piso	
Departamento	**Número de Usuarios**
División de Talleres y Transportes	8
Alumbrado Público	5

Edificación (Mantenimiento Urbano)

Planta Baja	
Departamento	**Número de Usuarios**
Operación y mantenimiento urbano de redes.	6

Edificación (Acometidas)

Planta Baja	
Departamento	**Número de Usuarios**
Acometidas	9

Edificación (Personal)

Planta Baja	
Departamento	**Número de Usuarios**
Personal	2

Edificación (Construcción de redes)

Planta Baja	
Departamento	**Número de Usuarios**
Construcción de redes	2
Pérdidas Comerciales	3

Edificación (Mecánica Automotriz)

Planta Baja	
Departamento	**Número de Usuarios**
Mecánica Automotriz	2
Gasolinera	1
Mantenimiento Hidráulico grúas	1

Edificación (Taller Industrial)

Planta Baja	
Departamento	**Número de Usuarios**
Taller Industrial	1

Edificación (Laboratorio de Transformadores)

Planta Baja	
Departamento	**Número de Usuarios**
Laboratorio de Transformadores	2

Edificación (Bodegas)

Planta Baja	
Departamento	**Número de Usuarios**
Bodega de distribución	1
Bodega de Instalaciones	2
Bodega Automotriz	1

Total **Adaptadores PCI = 66**

2.8.5 NÚMERO DE ADAPTADORES PC CARDS

En base a la información que se encuentra en la división de sistemas se ha determinado la cantidad de adaptadores PC Card que se requieren para computadores portátiles, los cuales se detallan en la Tabla 2.5.

Tabla 2.5.- Adaptadores PC Cards por edificaciones

Edificio Polifuncional

Primer piso	
Departamento	**Número de Usuarios**
Laboratorio de Medidores	2
Clientes Especiales	1

Edificación (Mantenimiento Urbano)

Planta Baja	
Departamento	**Número de Usuarios**
Operación y mantenimiento urbano de redes.	3

Edificación (Construcción de redes)

Planta Baja	
Departamento	**Número de Usuarios**
Construcción de redes	1

Total adaptadores **PC Card (laptop) = 7**

2.8.6 PUNTOS DE ACCESO

Para determinar la ubicación de puntos de acceso se procede a determinar las áreas de cobertura que tienen los equipos así como la reutilización de frecuencias.

El área de servicio básico BSA (*Basic Service Area*) determina el área que cubre un punto de acceso. Para el diseño se ha considerado las áreas de cobertura que se presenta en las especificaciones técnicas del punto de acceso Cisco Aironet 1200.

2.8.6.1 Superposición de celdas.

Para extender las áreas de cobertura, se sitúan los puntos de acceso de la celda para formar el Área de Servicio Extendida denominada ESA (*Extended Service Area*). Para permitir que usuarios realicen el proceso de roaming sin pérdida de conectividad RF las celdas tienen un 10 a 15% de superposición [10]. Este esquema se indica en la Figura 2.16.

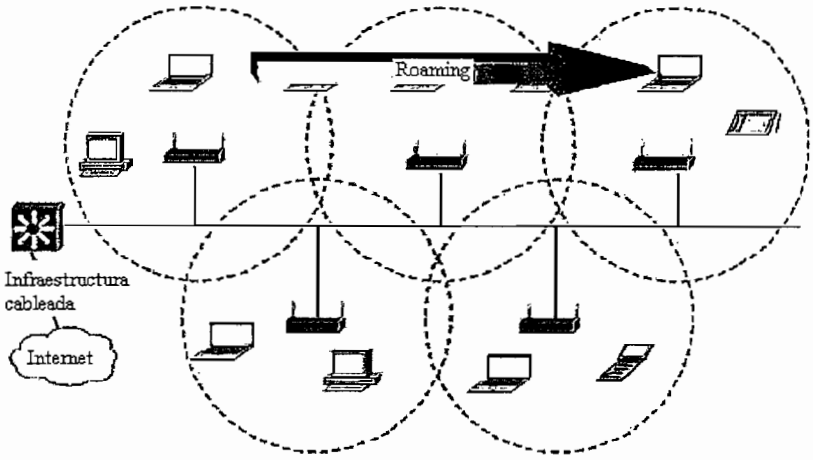


Figura 2.16.- Superposición de Celdas

En el diseño se ha considerado un rango de cobertura de 27 metros (90 ft) a 54Mbps cuya especificación consta en las características técnicas del AP 1200 Cisco Aironet para interiores, para una velocidad óptima y satisfacer concentración de tráfico.

De acuerdo a lo anterior y considerando una superposición de celdas del 10 - 15% se ha definido las ubicaciones que tendrán los puntos de acceso.

Este esquema es representado gráficamente en el anexo 2, en el cual se encuentra el diseño y la ubicación de los puntos de acceso.

2.8.6.2 Definición de ubicaciones

Los puntos de acceso se encuentran distribuidos para cubrir los lugares en los cuales se requiere conexión, se especifica la ubicación que tendrán los equipos en la Tabla 2.6. y su cobertura teórica se presenta gráficamente en el anexo 2.

Tabla 2.6.- Ubicación de puntos de acceso

Edificación	Cantidad	Ubicación	Identific
Edificio Polifuncional	5	Div. Talleres y Transportes	AP1
		Departamento de Alumbrado Público	AP2
		Clientes Especiales	AP3
		Laboratorio de medidores	AP4
		Operadores de Red	AP5
Departamento de Acometidas	1	Ingreso al Departamento de Acometidas	AP6

Operación y Mantenimiento Urbano de Redes	1	Jefatura del Departamento	AP7
Construcción de Redes y Pérdidas Comerciales	1	Construcción de Redes	AP8
Departamento de Personal	1	Ingreso al Departamento de Personal	AP9
Laboratorio de Transformadores, taller industrial	1	Jefatura de departamento	AP10
Mecánica Automotriz, Gasolinera y Grúas	1	Sección de grúas	AP11

2.8.7 PATCHCORDS

Los Patch Cords se emplearán en el closet de telecomunicaciones, conectarán el patchpanel con el switch Catalyst Cisco 2950-24 por lo que requiero de 11 patchcords de 3 pies.

2.8.8 NÚMERO DE CORRIDAS

El número de corridas que se requieren para la ubicación de los puntos de acceso determina la cantidad de cable UTP necesario.

Se puede considerar dos maneras de obtener el número de corridas, mediante un método exacto de distancias desde el closet de comunicaciones, hasta cada punto de acceso, o realizar un método aproximado para el cálculo de corridas.

La ubicación de los puntos de acceso, y su conexión al closet de telecomunicaciones, se indica en la figura 2.17.

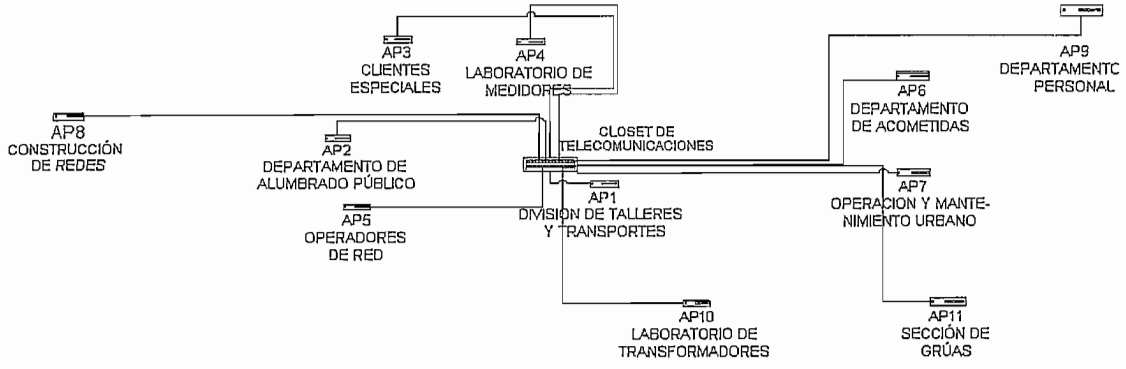


Figura 2.17.- Diagrama de Conexión de Puntos de Acceso

2.8.8.1 Método Exacto

Se determina la distancia que existe desde cada punto de acceso hasta el closet de comunicaciones, considerando una reserva de 2 metros para instalaciones, 0.50m en las ubicaciones de puntos de acceso y 2.50m en el closet de telecomunicaciones.

Los resultados al considerar este método se resumen en la Tabla 2.7, en el cual se muestran distancias y reservas.

Tabla 2.7.- Distancias del método exacto

Ubicación	Nombre	Distancia (m)	Reserva (m)
Div. Talleres y Transportes	AP1	8	3
Alumbrado Público	AP2	45	3
Clientes Especiales	AP3	40	3
Laboratorio de medidores	AP4	30	3
Operadores de Red	AP5	70	3
Dpto de Acometidas	AP6	55	3
Operación y mantenimiento urbano	AP7	40	3
Laboratorio de Transformadores	AP10	60	3
Sección de grúas	AP11	85	3

Para determinar el número de corridas se suma las distancias que no sobrepasen los 305 metros de una bobina.

Distancias que no sobrepasan 305 metros.

Ubicación	Nombre	Distancia
Div. Talleres y Transportes	AP1	8+3
Departamento de Alumbrado Público	AP2	45+3
Clientes Especiales	AP3	40+3
Laboratorio de medidores	AP4	30+3
Operadores de Red	AP5	70+3
Departamento de Acometidas	AP6	55+3
Total metros	**266**	

Para estas corridas se requiere 1 rollo de 305m

Operación y mantenimiento urbano	AP7	40+3
Laboratorio de Transformadores	AP10	60+3
Sección de grúas	AP11	85+3
Total metros	**194**	

Para estas corridas se requiere 1 rollo de 305m

De acuerdo a esto, el número total requerido es de **2 rollos.**

Existen distancias que sobrepasan los 100m como Construcción de Redes y Departamento de Personal indicadas en la tabla 2.8,

Tabla 2.8.- Distancias superiores a 100m

Ubicación	Nombre	Distancia (m)
Construcción de Redes	AP8	165
Ingreso al Departamento de Personal	AP9	149
Total	**314m**	

Para estos enlaces se tienen dos opciones implementar fibra óptica multimodo 62.5/125 μm ó enlaces inalámbricos con *bridges*.

El costo de de los 314m de fibra, cajas multimedia para fibra, fusión, certificación y 4 convertidores tiene un costo referencial de 2200 USD.

La segunda opción es implementarlos con enlaces inalámbricos de 4 de *bridges,* mástiles con sus propias antenas incorporadas . Este equipamiento tiene un costo aproximado de 2500 USD[19].

De lo anterior se selecciona la opción con fibra por ser más económica, ofrece seguridad y mayor velocidad.

2.8.8.2 Método Aproximado

Para determinar la cantidad de rollos de cable UTP que se empleará se siguen los siguientes procedimientos:

- Determinación de distancias

Distancia al punto más lejano (*Dmax*)

Distancia al punto más cercano (*Dmin*)

El punto más lejano lo tenemos desde nuestro closet de telecomunicaciones hasta un punto ubicado en Sección Grúas. Dmax: 85m

El punto más cercano se encuentra ubicado en la División de Talleres y Transportes cerca del closet de telecomunicaciones.

dmin: 8 m

- Sumar y dividir entre los 2, añadir un 10% de holgura, y 2.5m para la terminación.

[19] Valores proporcionados por EvolutioNet.

$$D' = \frac{D\max + D\min}{2}$$

$$D'' = D' + 10\% + 2.5$$

$$D'' = 46.5 + 4.65 + 2.5 = 53.65 \approx 54$$

- El número de corridas Q (para esto tomamos en cuenta que la caja tiene 305 m)

$$Q = \frac{305}{D''} = \frac{305}{54}$$

$$Q = 5.65 \approx 5$$

(Aproximamos por debajo debido a que no debemos tener corridas incompletas)

La cantidad de bobinas o rollos de cable R

$$R = \frac{\#\ salidas}{Q} = \frac{9}{5}$$

$$R = 1.8 \approx 2$$

(Para el número de salidas se toma en cuenta la suma de puntos de acceso)

De acuerdo a esto el número requerido es **2 rollos.**

Se puede observar que los métodos no difieren.

2.8.9 CUARTO DE EQUIPOS

- Dimensionamiento del rack

Existen diferentes racks en el mercado los cuales pueden ser de diversos tamaños y tipos, gabinetes, racks de piso, etc, como se indica en la figura 2.18.

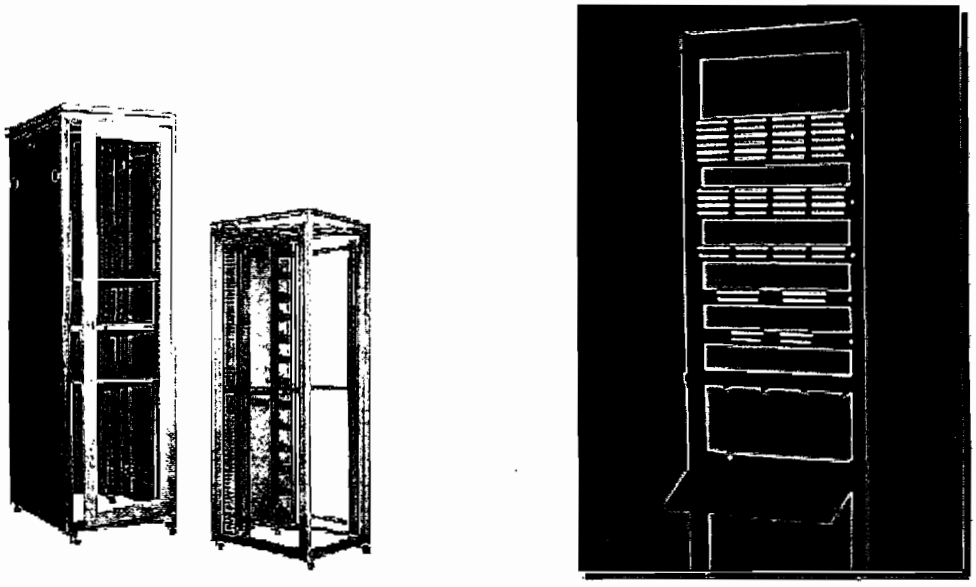


Figura 2.18.- Racks de Piso y Gabinetes

Para dimensionar el Rack se suma todos los patchpanel, switchs, organizadores, bandejas, supresores, de acuerdo a unidades HU resumidos en la Tabla 2.9

Tabla 2.9.- Dimensionamiento del Rack

Descripción	Cantidad	# de HU
Patch Panel	1	1
Switch	1	1
Organizadores		1
Supresores		1
Bandeja para convertidores		1
Espacio intermedio		1
Total		**6**

(HU: unidades de Rack)

1 HU = 1.75 pulgadas

6 HU *1.75 = 10.5 pulg.

Por lo tanto se requiere de 1 **Rack de 19 pulg. ancho por 10.5 pulg. de alto.** o superior.

- Patchpanel

Para la conexión del equipo activo se requiere un patchpanel de 16 puertos para Rack 19" cat5e o superior 1UR mostrado en la Figura 2.19.

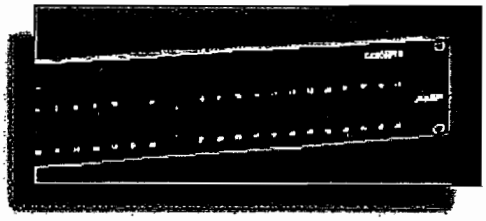


Figura 2.19.- Pathpanel para el Closet de Telecomunicaciones

- 1 Organizador vertical para Rack de piso 80*80
- 1 Organizador horizontal para Rack 19" 1 UR
- 11 Patchcords de 3 pies.
- 1 Supresor de energía de 8 tomas.

2.8.10 CANALETAS

Las distancias estimadas para utilización de canaletas vistas de pared que se emplearán en el tendido del cable UTP cat 5e hacia los puntos de acceso se resumen en la tabla 2.10.

Tabla 2.10.- Estimado de Canaletas

Ubicación	Nombre	Distancia (m)
Div. Talleres y Transportes	AP1	8
Departamento de Alumbrado Público	AP2	10
Clientes Especiales	AP3	5
Laboratorio de medidores	AP4	10
Operadores de Red	AP5	5
Departamento de Acometidas	AP6	15
Operación y mantenimiento urbano	AP7	15
Construcción de Redes	AP8	5
Ingreso al Departamento de Personal	AP9	3
Laboratorio de Transformadores	AP10	4
Sección de grúas	AP11	3
Total		**83**

2.8.11 RESUMEN DE REQUERIMIENTOS

La lista de requerimientos resumidos se presenta en la tabla 2.11.

Tabla 2.11.- Lista de Requerimientos

ITEM	DESCRIPCIÓN	Cantidad
1	Punto de acceso Cisco Aironet serie 1200 Manejo de IEEE 802.11g Banda 2.4 GHz Velocidades 1, 2, 5.5, 11, 24, 36, 48, 54 Mbps Seguridad WEP, WPA, TKIP, EAP, LEAP, LEAP-TLS Puerto Ethernet de uplink 10/100 Mbps autosensing Acceso Web, Consola, Telnet Cisco IOS Software versión 12.2(13)JA o superior. Protocolo CSMA/CA Antena omnidireccional por defecto.	11
2	Adaptador PCI Cisco Aironet 802.11a/b/g	66
3	Adaptador Cliente PC Card Cisco 802.11a/b/g	7

4	PATCH PANEL de conexiones de 16 puertos tipo RJ45 categoría 5e para distribución de cables tipo UTP de cuatro pares completo y armado	1
5	RACK estándar, tipo abierto de sistema estructurado de 19" de ancho por 42" de alto, con dos parantes verticales y bases de soporte	1
6	Bobinas de 305m cable UTP cat5e para instalación	2
7	Fibra óptica 4 hilos, multimodo 62.5/125μm para instalación aérea tipo ADSS en exteriores, elementos necesarios de conexión y fusión de 8 hilos	314m
8	Caja multimedia para fibra óptica	3
9	Convertidor de medio, fibra óptica multimodo con conectividad ST – RJ45 FastEthernet	4
10	Organizador vertical para Rack 80*80	1
11	Organizador horizontal para Rack 19" 1 UR	1
12	Supresor de energía de 8 tomas	1
13	Canaletas de 2m con capacidad para 2 cables UTP cat5e tipo panduit	42
14	Metros de manguera PVC 1"	368
15	Codos para canaleta con capacidad para 2 cables UTP cat5e de pared	20
16	Uniones para canaleta de 2m con capacidad para 2 cables UTP cat5e de pared	20
17	Patch cords de 3 pies cat5e	22

Con la finalidad de establecer con exactitud los requerimientos para el diseño de la red inalámbrica, es necesaria la realización de pruebas de campo en el lugar y con ello se presentará los costos de implementación de la red inalámbrica.

Capítulo 3
Pruebas de Campo

3 PRUEBAS DE CAMPO

Una vez realizado el diseño se procede a realizar las pruebas de campo para lo cual se utiliza equipos de la marca Cisco Aironet con sus componentes necesarios: punto de acceso Cisco Aironet de la serie 1200 802.11g, cliente el adaptador PC Card Cisco inalámbrico 802.11a/b/g modelo AIR-CB21AG-A-K9, en una laptop para facilidades de movilidad en cumplimiento con IEEE 802.11g, estos elementos permiten verificar la operación del sistema en diferentes puntos del campus.

En este capítulo se describe la realización de las respectivas pruebas de cobertura del punto de acceso, para determinar la potencia de señal, calidad de señal, y determinar sitios en los cuales se tenga señal nula.

Se realizan pruebas de velocidades de conexión que se logran en la red IEEE 802.11g, con la finalidad de optimizar el diseño de la red inalámbrica. De acuerdo a las pruebas en el lugar se determinará las correcciones que se impondrán al diseño, así como los requerimientos en cuanto a ubicaciones y por tanto corridas requeridas.
Finalmente se presenta el costo de implementación que involucra el diseño propuesto.

3.1 PRUEBAS DE COBERTURA

Para la realización de pruebas de campo se realiza la configuración de los parámetros de operación de la WLAN, para posteriormente realizar la revisión del sitio (*site survey*) en el campus, con lo que se puede determinar las características de operación de la red.
La configuración de la WLAN consta de dos etapas: La configuración de parámetros en el punto de acceso y la configuración de adaptadores inalámbricos en el cliente [5].

3.1.1 CONFIGURACIÓN DEL PUNTO DE ACCESO

El punto de acceso viene configurado con parámetros por defecto mostrados en la tabla 3.1

Tabla 3.1.- Parámetros por Defecto del AP 1200

Descripción	Valor por defecto
Nombre del Sistema	ap
Tipo Terminal (sobre el interfaz de consola)	teletype
Protocolo para configuración servidor	DHCP
IP	10.0.0.1
Máscara	255.0.0.0
Puerta de enlace	255.255.255.255
SSID	Tsunami
Rol en la red	Access Point/Root
Radio óptimo para	Default
Comunidad SNMP	Admin.

Se puede configurar al punto de acceso de tres maneras:

Configurar mediante Web.

Configurar mediante Consola

Configurar mediante Telnet.

La asignación de una dirección IP se estableció mediante acceso de consola, para ello se ejecuta desde un computador parámetros de comunicación 9600, 8, N, 1, desde HyperTerminal, como lo indica la figura 3.1.

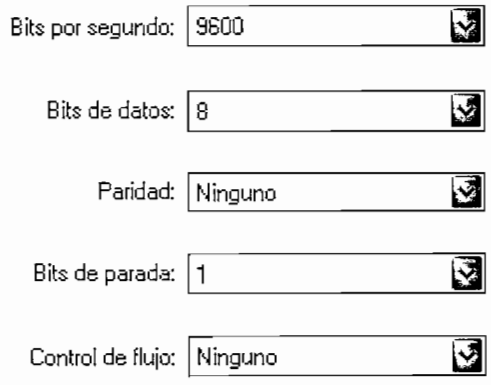


Figura 3.1.- Parámetros de Comunicación de HyperTerminal

Al presionar la tecla Enter aparece el prompt del punto de acceso en pantalla.
Username:
Escribimos *admin*, y como password por defecto *Cisco*, con lo cual ingresamos al modo privilegio.
ApEEQ1#
Ingresamos al modo de configuración global digitando:
ApEEQ1# configure terminal
Ingresamos al modo de configuración de interface BVI1 que maneja el interface FastEthernet0 digitando:
ApEEQ1 (config)# interface BVI1
Ingresamos una dirección IP con su respectiva máscara de subred mediante
ApEEQ1 (config-if)# ip address 132.147.160.12 255.255.255.252.0
Esta dirección IP así como su máscara se encuentra dentro del plan de direccionamiento IP de la EEQ.
ApEEQ1 (config-if)# end
ApEEQ1# write memory

Con ello se ha asignado la dirección IP al punto de acceso y grabado en memoria.
De aquí en adelante se empleará la configuración Web por facilidades de administración.
Para acceso mediante Web se digita en el navegador o *browser* de Microsoft Internet Explorer, la dirección IP del punto de acceso, a continuación se digita el nombre de usuario y contraseña, por defecto el nombre de usuario es admin y la contraseña es Cisco con lo cual se despliega la pantalla *Home* indicada en la figura 3.2.

La pantalla *Home* es la pantalla principal al ingreso en el punto de acceso, indica un resumen del estado del mismo, clientes asociados, su identificación en la red, sus interfaces de red, un registro de eventos.
Adicionalmente se puede ingresar a las opciones del menú que se indican a la izquierda para configuración.

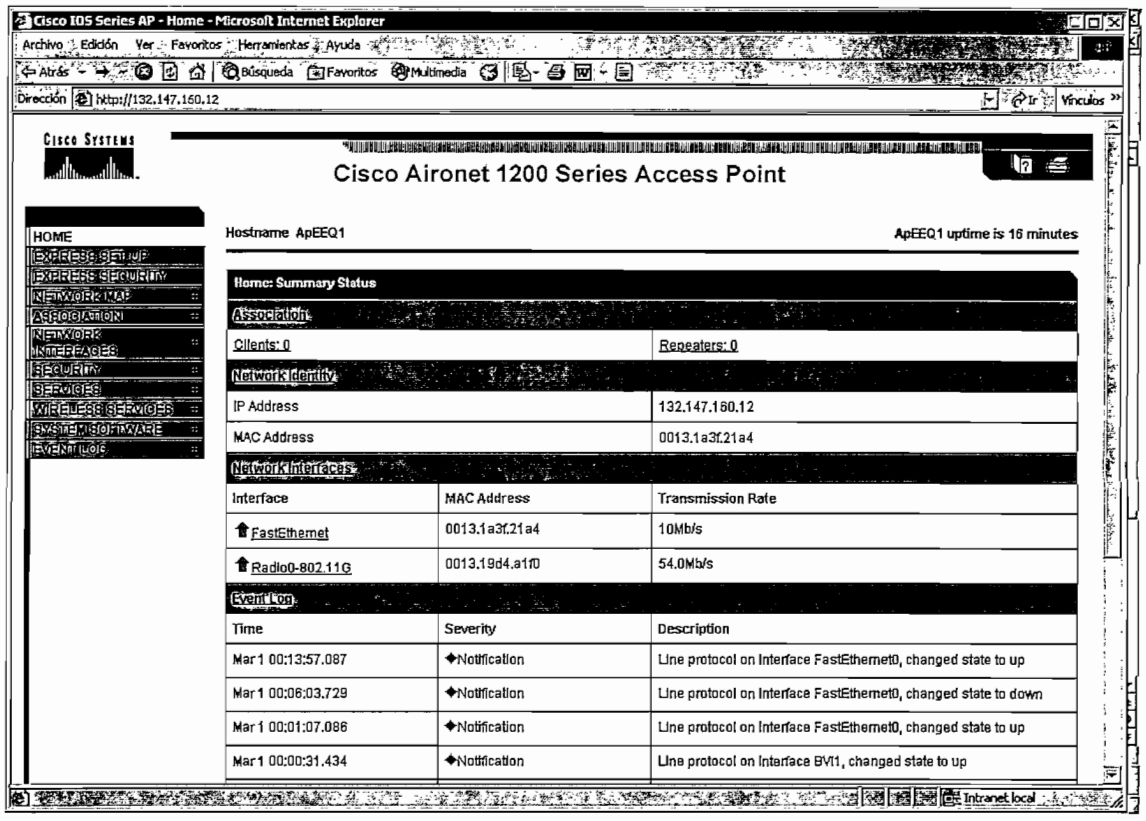


Figura 3.2.- Pantalla de Bienvenida AP1200

3.1.1.1 Parámetros Configurados

Los parámetros que se han configurado en el AP son los indicados en la tabla 3.2

Tabla 3.2.- Parámetros Configurados en el AP 1200

Parámetro	Asignación
Nombre	ApEEQ1
Protocolo para Configuración Servidor	IP estática
Dirección IP	132.147.160.12
Máscara	255.255.252.0
Puerta de enlace	132.147.161.20
SSID	EEQWLAN
Rol	Acces Point/Root
Comunidad SNMP	DefaultComunity

Para configurar todos estos parámetros se ingresa a *Express Setup* del menú principal, con lo que aparece la pantalla de la figura 3.3

Aquí se ingresan los cambios respectivos y se aplican mediante *Apply* ubicado en la parte inferior derecha de la página.

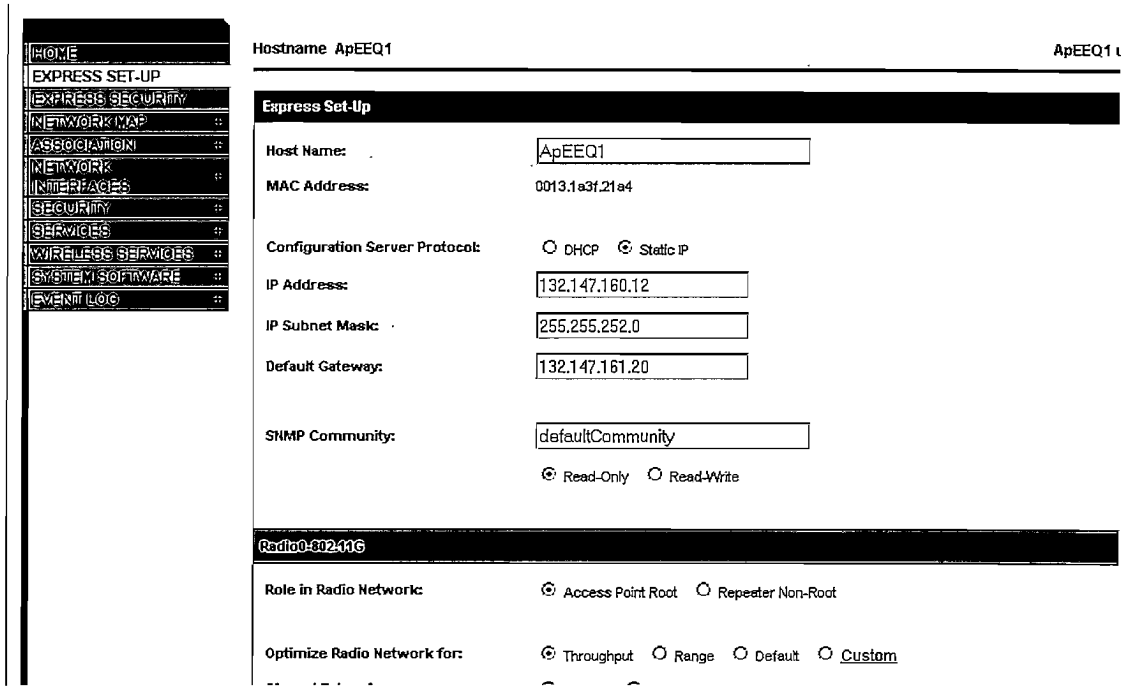


Figura 3.3.- Configuración Express Setup.

3.1.1.2 Configuración de Parámetros Adicionales

Como se ha tratado anteriormente la configuración de parámetros de seguridad como son WEP, filtrado MAC, deshabilitación de Broadcast SSID, Servidor RADIUS, deshabilitación de acceso Telnet en el punto de acceso se han considerado y configurado, pero por la finalidad que tiene el capítulo, se los presenta en el Anexo 3.

3.1.2 CONFIGURACIÓN DEL ADAPTADOR CLIENTE

Los adaptadores para tarjetas inalámbricas tienen disponibles controladores para todos los sistemas operativos Windows. El proceso de instalación se ha realizado sobre una portátil con Windows XP [5].

Se inserta físicamente el adaptador cliente PC Card Cisco 802.11a/b/g con la portátil apagada. Una vez que arranca el sistema operativo, es necesario suspender el proceso de *Detección de nuevo hardware*, el cual corre un asistente

predeterminado de Windows, es necesario ya que las utilidades de Cisco se instalan conjuntamente con los controladores.

Se ingresa el CD de instalación que viene con el adaptador cliente PC Card Cisco 802.11a/b/g.

Se corre el programa de instalación con lo cual aparece la pantalla de la figura 3.4

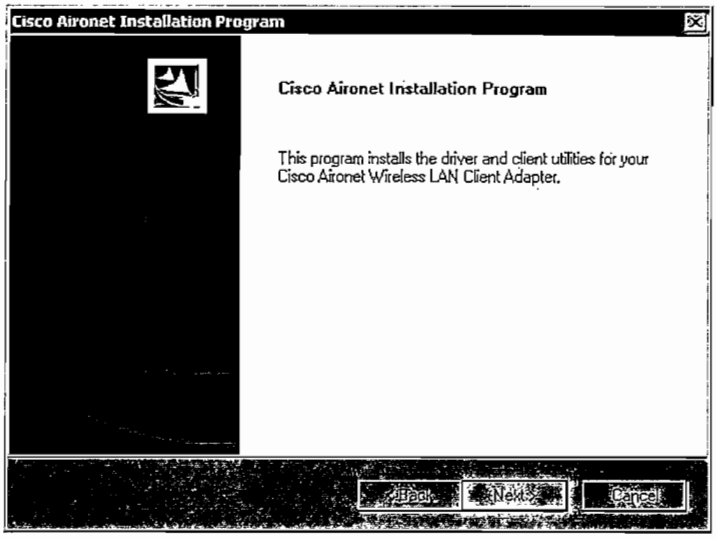


Figura 3.4.- Programa de Instalación de Cisco Aironet

Se puede descargar el controlador actualizado de http://cisco.com/public/sw-center/sw-wireless.shtml.

Una vez concluido los pasos de instalación, selección del modo de configuración y reinicio del equipo, se encuentra instalado el hardware, *drivers* y utilitarios de Cisco Aironet.

Es necesario la asignación de una dirección IP en el adaptador del cliente, para ello ingresamos en *Conexiones de red inalámbricas -> Propiedades-> Protocolo TCP/IP* del ícono de *Mis Sitios de Red* definido en el Sistema Operativo Windows XP, con lo cual se asigna una dirección IP, y se acepta los cambios, como lo indica la figura 3.5.

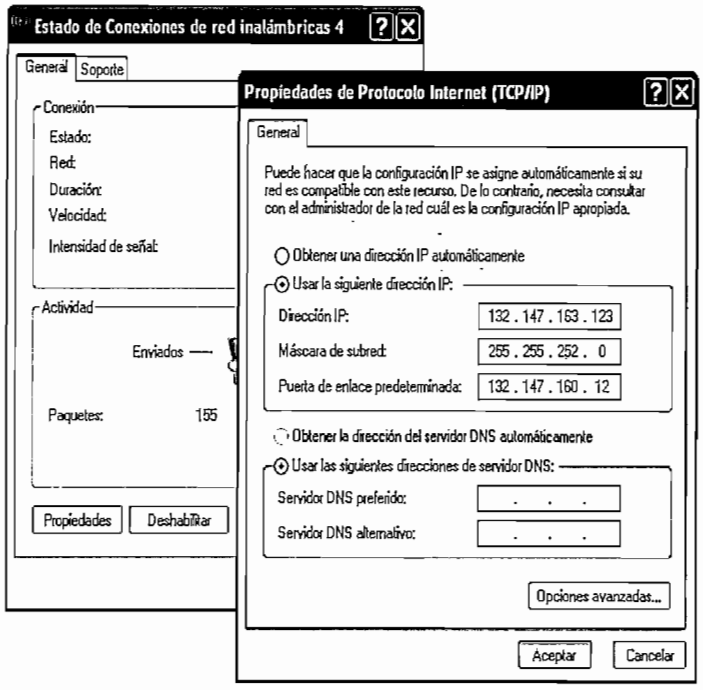


Figura 3.5.- Asignación de IP en el Cliente

Se verifica la actividad de la tarjeta mediante un ping a su dirección IP, como lo indica la pantalla de la figura 3.6

Figura 3.6.- Actividad de la Tarjeta Inalámbrica

Es necesario establecer la configuración de seguridad en el cliente para que se pueda *asociar* y autenticar en el punto de acceso. El procedimiento de configuración del cliente LEAP para Cisco del adaptador inalámbrico se indica en el anexo 3. Se observa la utilidad ADU *Aironet Desktop Utility* de Cisco indicado de la figura 3.7, el proceso que lleva la autenticación y el punto de acceso al cual se asocia el cliente,

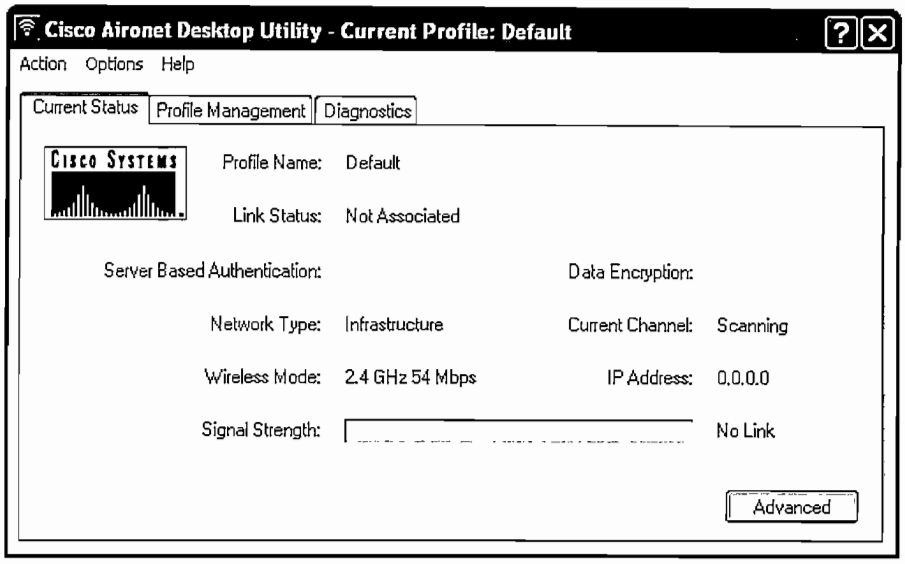


Figura 3.7.- Pantalla Principal de ADU.

Una vez configurado el cliente y llevado a cabo el proceso de asociación y autenticación se muestra la pantalla de la figura 3.8.

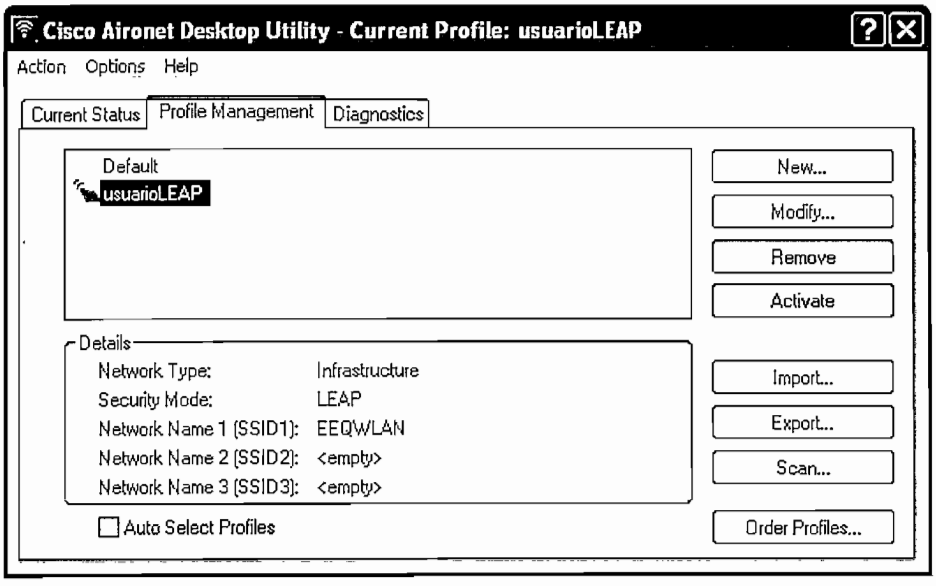


Figura 3.8.- Usuario LEAP Asociado y Autenticado

Se selecciona el perfil creado y se aplican los cambios. Una vez hecho esto el sistema empieza el proceso de autenticación en la red. Si se ha asociado al punto de acceso se indicará al ingresar en *Current Status* del menú principal del ADU. Adicionalmente es necesario verificar la Dirección MAC que tiene el adaptador cliente para establecer el filtrado MAC en el punto de acceso, para ello se ingresa

a *Diagnostics -> Adapter Information* del ADU, con lo cual aparece la pantalla de la figura 3.9.

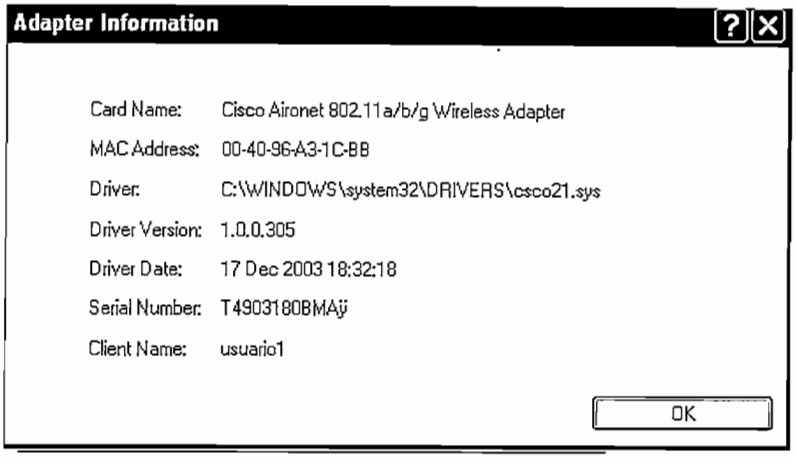


Figura 3.9.- Información del Adaptador Cliente

Desde el cliente se puede verificar que se encuentra deshabilitado el broadcast de SSID, al observar que no se encuentra presente entre las conexiones de red inalámbricas disponibles como lo indica la figura 3.10.

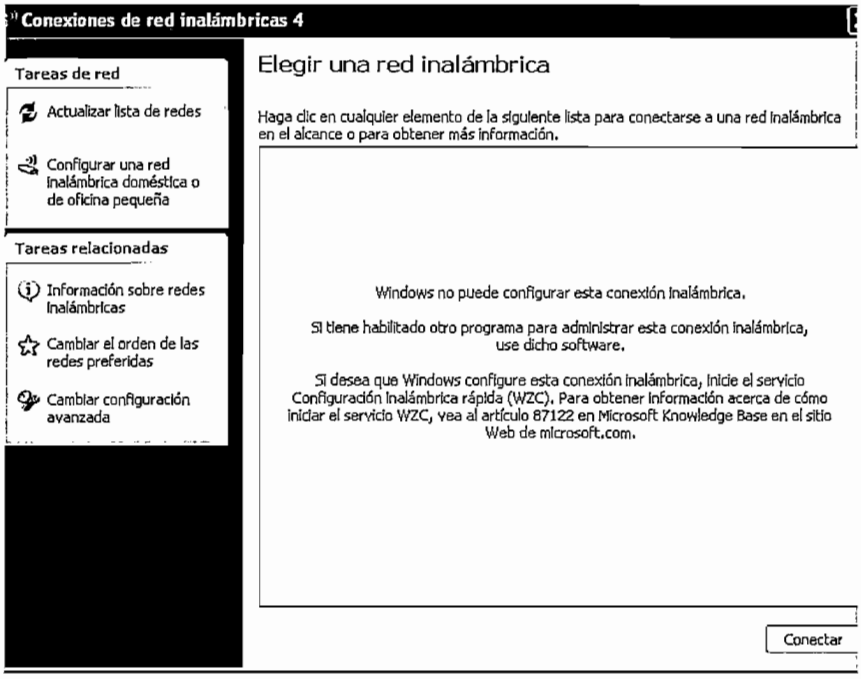


Figura 3.10.- Redes Inalámbricas Disponibles.

3.1.3 SEGURIDAD MEDIANTE SERVIDOR RADIUS

Con las configuraciones anteriores en el cliente se establece el Filtrado MAC, y encripción WEP de 128 bits, sin embargo se desea establecer un nivel más alto

de seguridad. Por este motivo se presenta la inclusión de autenticación por medio de servidor RADIUS.

En el presente proyecto se presenta las configuraciones del servidor en el punto de acceso y las configuraciones del servidor en el cliente inalámbrico. Vea anexo 2. Para la configuración del servidor de autenticación *Odissey Server* vea referencia 5.

3.1.4 SITE SURVEY

La ubicación de productos inalámbricos en la red puede ser influenciada por una serie de factores. En esta sección se analiza la influencia de estos factores y se proporciona una guía y herramientas para lograr una óptima ubicación.

El *site survey* y herramientas de prueba de enlace conjuntamente con las utilidades del cliente ayudan a determinar la mejor ubicación para los puntos de acceso y estaciones de trabajo en la red inalámbrica. Estas herramientas no son soportadas en Sistemas Operativos Linux [10].

Debido a la configuración de componentes, ubicación y ambiente físico, habrá una instalación que será la mejor posible. Antes de instalar un sistema, se recomienda desarrollar el *site survey* para determinar la utilización óptima de los componentes de red, maximizar rango, cobertura, y performance de la red.

Considerando la siguiente operación y condiciones ambientales:

- Velocidades – La sensibilidad y rango son inversamente proporcionales a la tasa de transmisión. La máxima cobertura se logra a la más baja velocidad soportada. Conforme se incrementa velocidades ocurre un decremento de sensibilidad en el receptor.
- Tipo de antena y ubicación – Una configuración apropiada de antena es un factor crítico para maximizar el rango de cobertura. Como regla general, el rango se incrementa en proporción al tamaño de la antena.

- Ambiente físico.- Áreas abiertas y libres de obstáculos proporcionan una mejor cobertura que áreas cerradas y con objetos. Un ambiente de trabajo con menos obstáculos provee un mayor radio.
- Obstrucciones.- Una obstrucción física como un archivador metálico o un pilar de acero puede disminuir el performance del adaptador del cliente. Evite ubicar las estaciones en ubicaciones con obstáculos metálicos entre antena transmisora y receptora.
- Material de edificaciones.- La penetración de radio es altamente influenciada por materiales de edificios. Por ejemplo, paredes de divisiones modulares permiten un rango más grande que bloques de concreto. Metal o construcciones de acero son un obstáculo para las señales de radio.

Adaptadores cliente son dispositivos de radio susceptibles a obstrucciones de RF y fuentes de interferencia que pueden reducir el throughput y rango.

Se recomienda instalar el adaptador cliente en áreas donde estructuras de acero, archivadores metálicos, libreros, y gabinetes no obstruyan las señales de radio hacia y desde el adaptador.
Instale el adaptador lejos de hornos microondas, los cuales operan a la misma frecuencia del cliente.

Pruebas de Enlace (*Advanced*)

La herramienta de pruebas es usada para determinar la cobertura de RF. Un ejemplo de ésta es la herramienta de *Current Status*, la cual gráficamente muestra el nivel de señal entre el adaptador cliente y un punto de acceso asociado como lo indica la figura 3.11 (disponible solo para sistemas operativos Windows).

Ingresando en *Advanced* se puede observar la pantalla de estado del usuario en la cual se muestra información de la conexión de una manera detallada. Esto se indica en la figura 3.12.

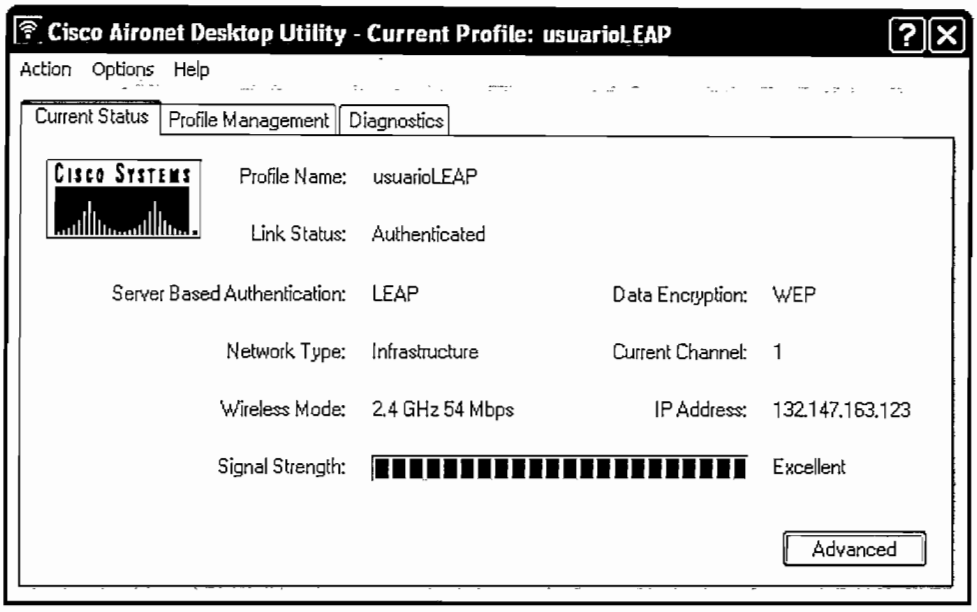


Figura 3.11.- Current Status del Usuario

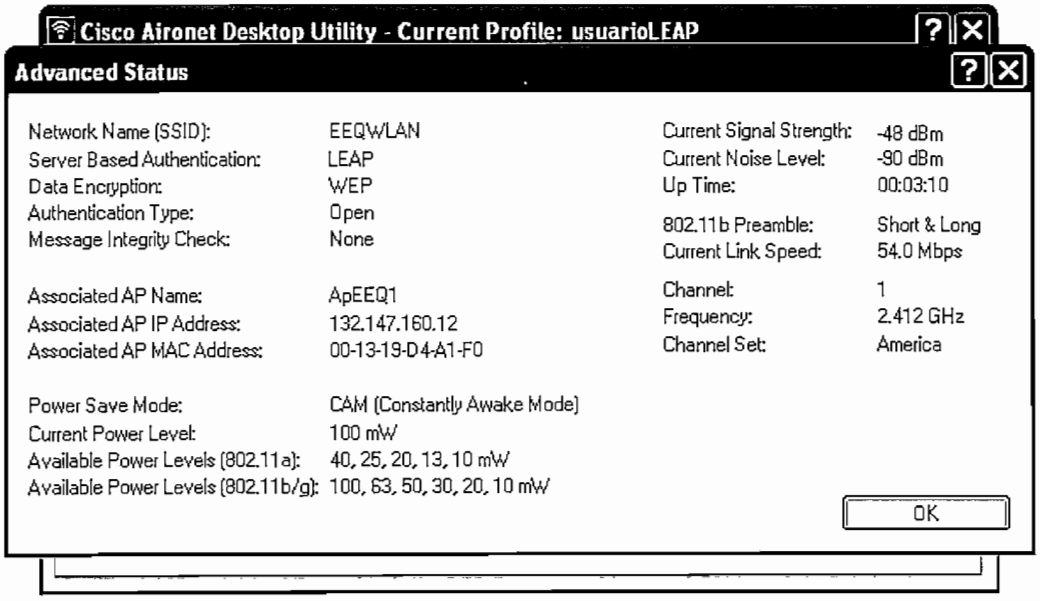


Figura 3.12.- Pantalla de Estado del Cliente

Ayuda mucho el mantener un ping hacia el punto de acceso en la realización del *site survey*, como se indica la figura 3.13

```
Haciendo ping a 132.147.160.12 con 32 bytes de datos:

Respuesta desde 132.147.160.12: bytes=32 tiempo<10ms TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo<10ms TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo<10ms TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo<10ms TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo<10ms TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo<10ms TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo<10ms TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo<10ms TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo<10ms TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo<10ms TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo<10ms TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo<10ms TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo<10ms TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo<10ms TTL=255
```

Figura 3.13.- Ping hacia el Punto de Acceso

Se debe tener la precaución de que todo el equipamiento esté operacional antes de arribar al lugar. El equipo debe estar configurado y listo para ser utilizado en el sitio del cliente. Una supervisión previa es necesaria para prever si se requiere equipamiento adicional como escaleras, pata de gallo, extensiones de energía eléctrica, etc.

3.1.5 *SURVEY* DE DOS ÁREAS Y COMPLETAR EL INTERIOR.

La manera más fácil de iniciar el *site survey* es establecer cuál es el área del establecimiento que necesita cobertura. Se escoge una esquina y se ubica el punto de acceso en la esquina como lo indica la Figura 3.14.

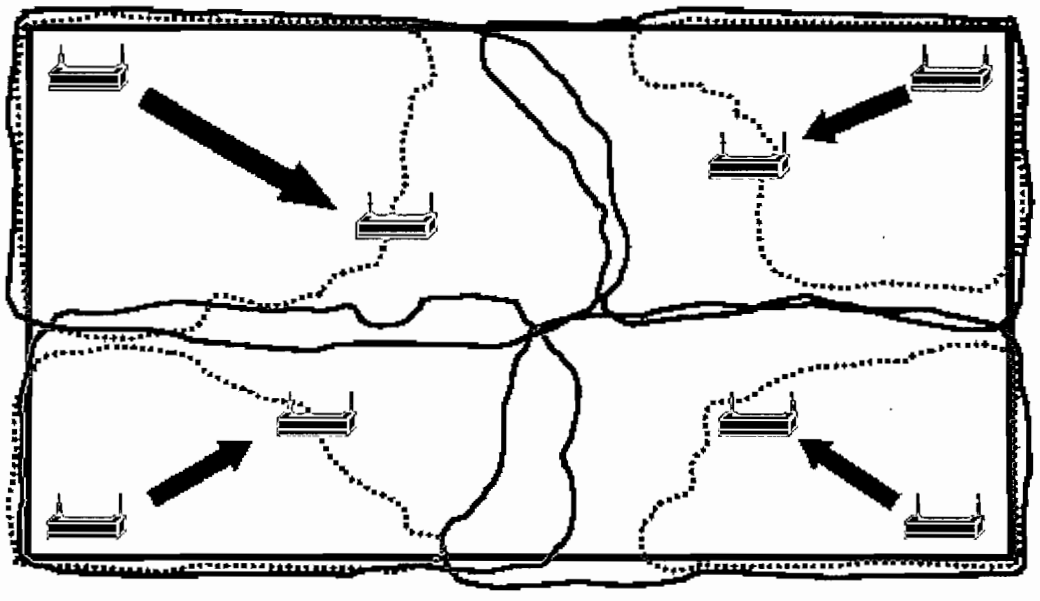


Figura 3.14.- Procedimiento de Site Survey

Se inspecciona el área de cobertura del punto de acceso y se toma nota de donde se encuentran puntos de cobertura pertenecientes al punto de acceso. Luego se

mueve hacia esos puntos. Si el punto de acceso se encuentra en una esquina, alrededor del 75% de la celda de cobertura estará desperdiciada en un área fuera de la edificación que no requiera cobertura [10].

Una vez que se ha movido el punto de acceso, se realiza nuevamente una inspección de las áreas de cobertura. Puede ser necesario mover varias veces el punto de acceso con la finalidad de obtener la mejor ubicación. Una vez decidido la mejor ubicación para ese punto de acceso, muévase a una diferente esquina del lugar y repita el proceso. En un simple almacén similar al mostrado en la Figura 3.14 se sugiere repetir el proceso unas cuatro veces. La inspección de cobertura de RF deberá entonces estar completada.

En un *site survey* más avanzado, repetir el proceso cuatro ocasiones puede solamente garantizar cobertura alrededor del perímetro del lugar, entonces puede ser necesario rellenar otros agujeros. Aquí es donde la experiencia y criterios entran en juego. Algunos ingenieros prefieren elegir el realizar el *survey* de perímetros y luego llenar el medio.

Las celdas de cobertura se pueden sobreponer en el *site survey* como lo indica la figura 3.15

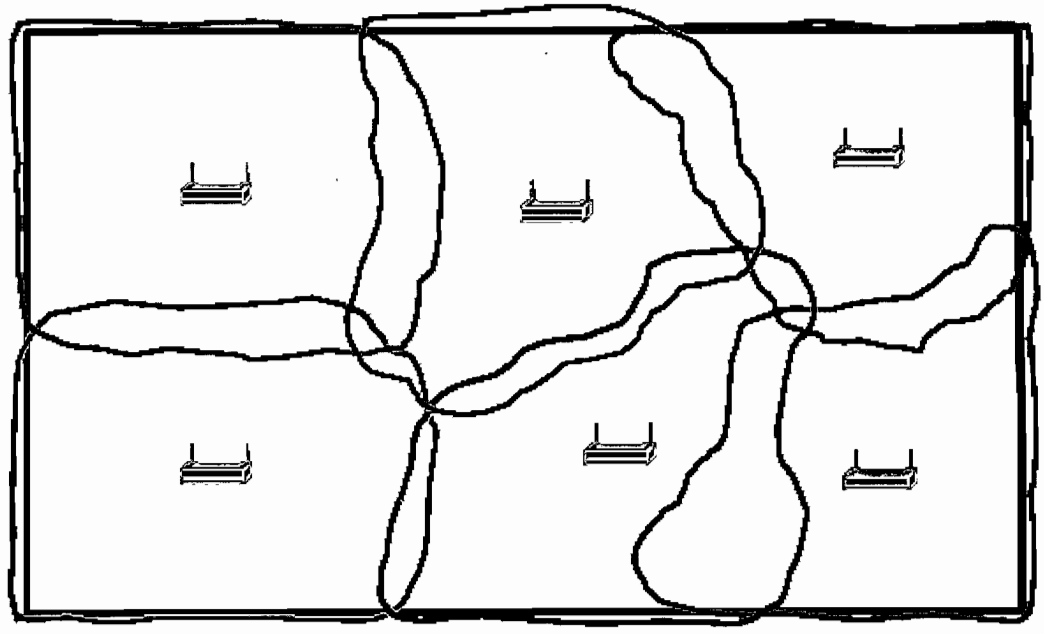


Figura 3.15.- Superposición de Celdas en el Site Survey

Para un *site survey* estándar el 15% de superposición es usualmente suficiente para proporcionar *handoffs* transparentes. Si se requiere el uso de repetidores, se podrá requerir un 50% de superposición con un punto de acceso conectado al cableado. Otra ventaja es realizar el *site survey* de los dos primeros puntos de acceso y encontrar las áreas de cobertura, como en la figura 3.16

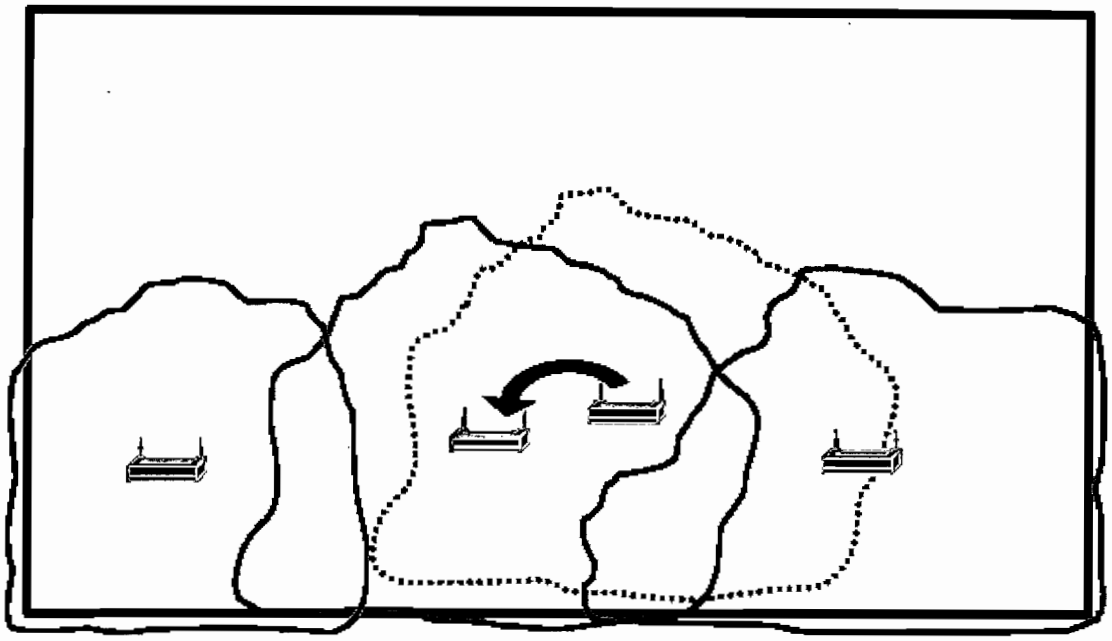


Figura 3.16.- Determinación de Áreas

Se coloca el AP en el centro de las celdas, se inspecciona su cobertura, luego se mueve el AP para emplear la celda completamente. Esto permite saber con certeza el tamaño de la celda. Se inspecciona la nueva ubicación y se determina la viabilidad y ajustes necesarios para continuar este proceso hasta que la localidad sea totalmente cubierta.

3.1.6 ANTENAS.

En ocasiones sucede que una celda de un punto de acceso se superpone demasiado con otra, o el caso contrario, que una celda no se superpone lo suficiente o lo deseado.

En este caso el nivel de señal, tamaño de celda y el tipo de antena son factores que influyen en el tipo de solución, una solución puede ser como la que se indica en la figura 3.17.

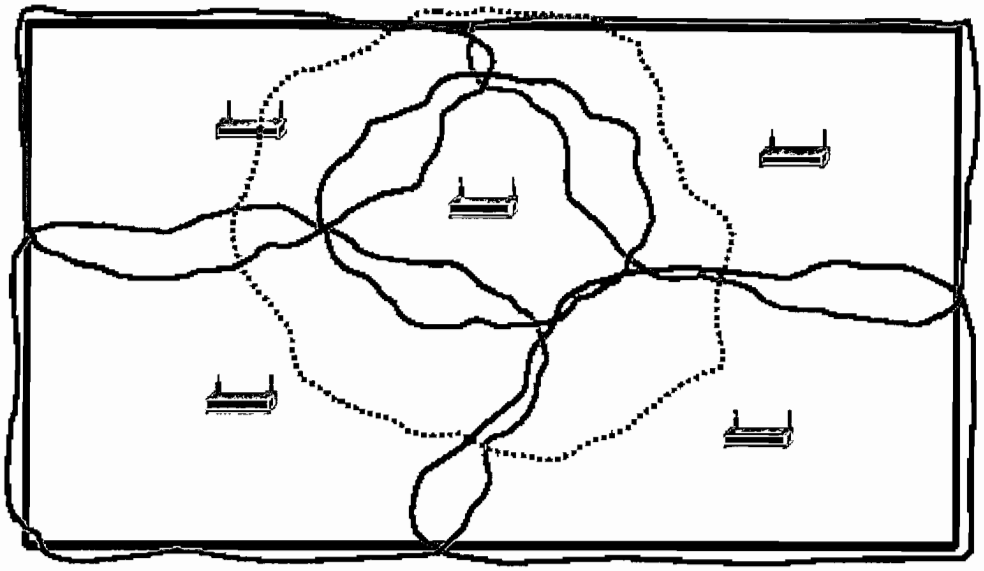


Figura 3.17.- Problemas de Superposición entre Celdas

Un ingeniero puede encontrarse en el caso de la figura 3.17, en este tipo de situaciones, los APs pueden proporcionar mucha cobertura, pero la cantidad de APs no proporcionan la cobertura deseada. En este punto la ingeniería en el sitio tiene algunas opciones. Se puede elegir, usar una antena diferente para obtener mayor cobertura desde los APs, o elegir, usar una antena más pequeña y adherir más puntos de acceso. Otra posibilidad es cambiar los niveles de potencia sobre uno o más APs para cambiar el tamaño de cobertura de la celda(s). Se puede usar una combinación de estas opciones para conseguir la cobertura deseada.

Finalmente la selección del tipo de antena, su patrón de radiación sea Omnidireccional, direccional, ganancia, y forma de instalación son determinantes para el diseño.

3.1.6.1 Tipo de Antenas

El tipo de antenas que ofrece la marca Cisco son fabricadas en cumplimiento con las regulaciones de la FCC[20] quien estandariza y norma el espectro de radio frecuencia [11].

Un sistema de antenas mostrado en la figura 3.18 comprende numerosos componentes, como son la antena, montaje de hardware, conectores, cable de antenas, y en algunos casos, un *lightning arrestor*[21].

---

[20] U.S. Federal Communications Commission

[21] Previene que energías alcancen el equipo de RF descargando a tierra.

Figura 3.18.- Sistema de Antenas

- **Antena Omnidireccional**

Una antena omnidireccional como lo indica la figura 3.19 está diseñada para proporcionar un modelo de radiación de 360 grados. Este tipo de antena se usa cuando se requiere cubrir en todas las direcciones de la antena.

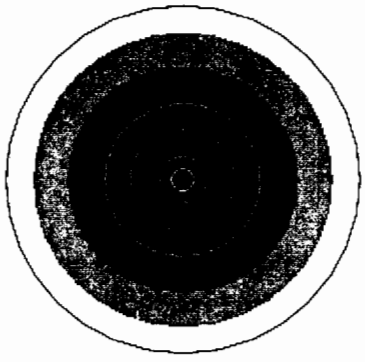


Figura 3.19.- Radiación Omnidireccional

- **Antena direccional Patch**

La antena no adhiere energía a la señal, solo direcciona la energía que recibe del transmisor, por este motivo tiene más energía en una dirección y menos en todas las demás. Como la ganancia de la antena se incrementa, el ángulo de radiación se decrementa, por lo que se obtiene mayor distancia de cobertura con un menor ángulo, entre este tipo de antenas se encuentra la antena Yagi, antena patch y antenas parabólicas tipo disco.

Estos patrones de radiación se indican en la figura 3.20.

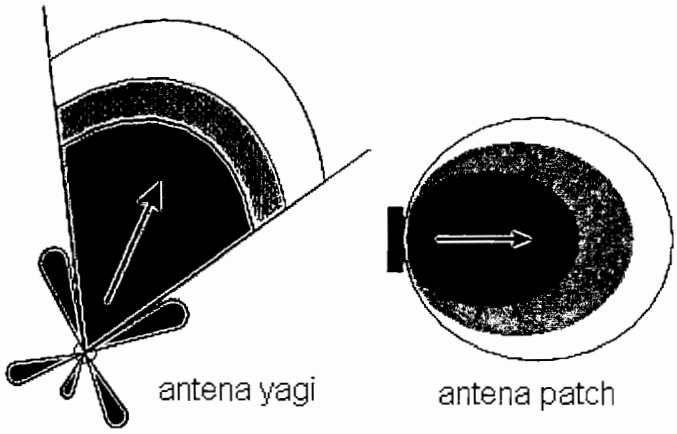


Figura 3.20.- Radiación Direccional

Entre la gama de antenas que *Cisco Systems* ofrece, y que son utilizables para el diseño inalámbrico se tiene el siguiente grupo de antenas:

- **AIR-ANT5959**

Proporciona características como diversidad, montaje en techo, tiene antena interior con diversidad para conector RP-TNC. Diseñada para aplicaciones WLAN en frecuencias de 2400 a 2500 MHz. La antena es omnidireccional y tiene una ganancia nominal de 2.2dBi, su perfil le permite pasar inadvertido en el techo. Viene con una grapa que le permite ser montado en cielo falso. Se indica en la figura 3.21.

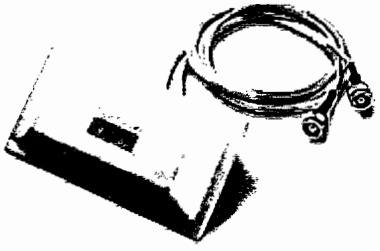


Figura 3.21.- Antena Cisco Aironet Modelo 5959

- **AIR-ANT4941**

Es una antena omnidireccional dipolo simple para conector RP-TNC. La antena proporciona cobertura omnidireccional en interiores y es diseñada para uso en la banda de frecuencia de 2.4 GHz. Tiene un radio de doblamiento de 90°. Pueden ser utilizados con todos los radios de que utilicen conectores tipo RP-TNC, y tiene una ganancia es de 2.2dBi, es mostrada en la figura 3.22.

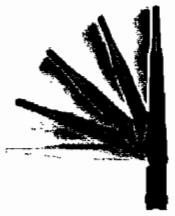


Figura 3.22.- Antena Cisco Aironet Modelo 4941

Su radiación vertical y sus dimensiones se indican en la figura 3.23.

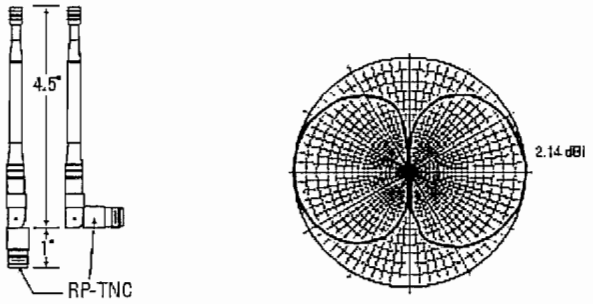


Figura 3.23.- Dimensiones y Radiación Vertical Cisco Aironet Modelo 4941

- **AIR-ANT1728**

Antena omnidireccional para interiores de montaje en techo, para conector tipo RP-TNC. Esta antena fue diseñada para aplicaciones WLAN con frecuencias de 2400 MHz a 2500 MHz. La antena tiene una ganancia nominal de 5.2dBi. Viene con una grapa que permite ser montada en el cielo falso. Se indica en la figura 3.24.

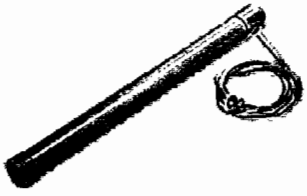


Figura 3.24.- Antena Cisco Aironet Modelo 1728

Sus dimensiones y patrón de radiación se indican en la figura 3.25.

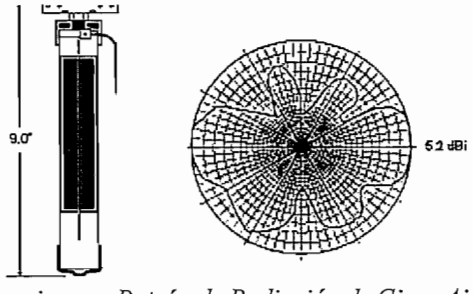


Figura 3.25.- Dimensiones y Patrón de Radiación de Cisco Aironet Modelo 1728

3.1.6.2 Regulaciones en el Ecuador

Las regulaciones de acuerdo a la SENATEL, específica que la potencia máxima para transmisión en la banda de 2,4GHz que puede implantarse en los radios es 250mw con una ganancia de antenas de 24 dBi, lo cual se encuentra en el Registro para uso de frecuencias de la Senatel. Como se puede observar las antenas que ofrece *Cisco Systems* no sobrepasan estos límites.

3.1.6.3 Antena Seleccionada

La antena seleccionada en el sitio ha sido especificada para lograr un mejor alcance de acuerdo a la infraestructura del sitio, Que permita cubrir los lugares requeridos de cobertura y, al realizar un diseño de alto desempeño a velocidad de hasta 54 Mbps que tenga una mayor ganancia.

El tipo de antena escogida para todos los puntos de acceso es la Antena Cisco modelo AIR.ANT1728 cuyas características se indicaron anteriormente.

3.1.7 RELACIÓN SEÑAL A RUIDO

Se puede determinar cómo se encuentra la relación señal a ruido en la transmisión, de los datos obtenidos del *site survey*, por ejemplo con características de conexión de la figura 3.26.

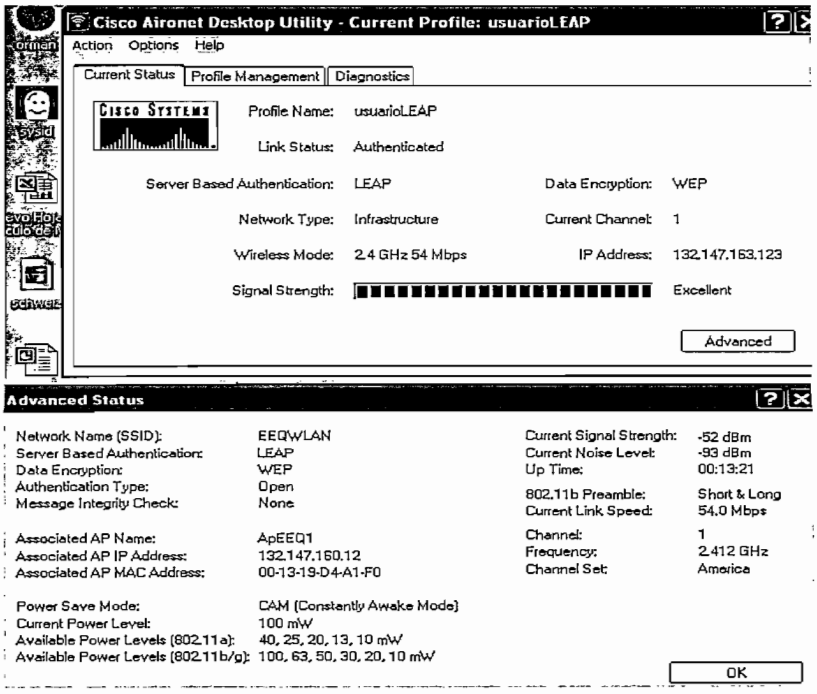


Figura 3.26.- Site Survey.

En un ejemplo de fortaleza de señal con -52dBm y nivel de ruido de -93dBm de la figura 3.26 se tiene

$$-52 = 10 * \log\left(\frac{P}{1mw}\right)$$

$$-5.2 = \log\left(\frac{P}{1mw}\right)$$

$$10^{-5.2} = \frac{P}{1mw}$$

$$P = 6.30 * 10^{-6}\, mw$$

El valor del nivel de ruido en miliwatts es -93:

$$-93 = 10 * \log\left(\frac{P}{1mw}\right)$$

$$-9.3 = \log\left(\frac{P}{1mw}\right)$$

$$10^{-9.3} = \frac{P}{1mw}$$

$$P = 5.01 * 10^{-10}\, mw$$

Por tanto el valor de relación señal a ruido será:

$$\frac{S}{N}[dB] = 10 * \log\left(\frac{P_1}{P_2}\right)$$

$$\frac{S}{N}[dB] = 10 * \log\left(\frac{6.30 * 10^{-6}\, mw}{5.01 * 10^{-10}\, mw}\right)$$

$$\frac{S}{N}[dB] = 41$$

Como se puede notar un valor negativo más cercano a cero indica un nivel más alto de potencia de señal, y el valor comparativo de decibelios es mostrado en la parte inferior.

3.2 PRUEBAS DE VELOCIDADES DE CONEXIÓN.

Para determinar dentro de las pruebas de campo las velocidades de conexión que podemos establecer, surge el compromiso entre velocidad - cobertura ya que como se mencionó en el capítulo anterior, si se desea mayores velocidades disminuirá las áreas de cobertura. En esta sección se realiza la selección de

canales para evitar interferencias, y cómo se réaliza las pruebas de campo (*site survey)* a velocidades desde 1 hasta 54 Mbps.

3.2.1 SELECCIÓN DE CANALES

Cuando se está realizando un *site survey*, se debe tomar en cuenta que solamente se tiene tres canales no interferidos en IEEE 802.11b e IEEE 802.11g. Esta distribución de canales se indica en el espectro de frecuencia asignado en la banda de 2.4GHz mostrado en la figura 3.27.

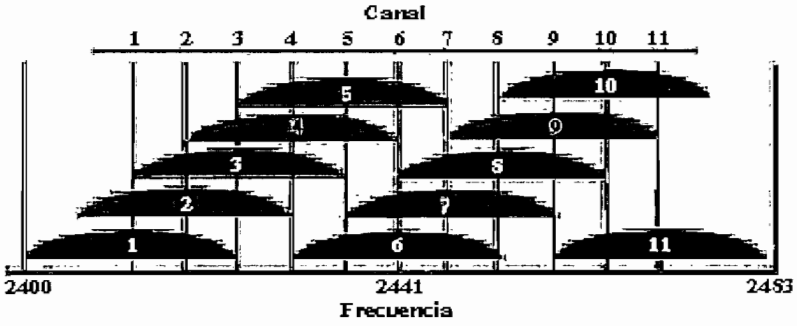


Figura 3.27.- Espectro de Canales en la Banda de 2.4GHz

Para realizar una cobertura completa del lugar mediante la superposición de celdas se debe ir intercalando las frecuencias a las cuales operen los puntos de acceso con la finalidad de no incurrir en interferencia, este esquema es el indicado en la figura 3.28.

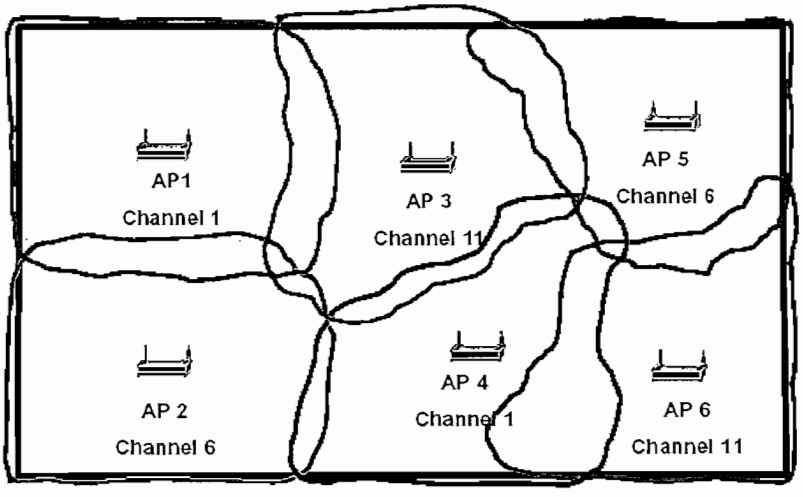


Figura 3.28.- Selección de Canales

Con la finalidad de maximizar velocidades de transmisión se usan los tres canales no interferidos, es decir el canal 1, canal 6 y canal 11. Como se proponga el

diseño de la WLAN, el *site survey* se realizará de la manera en la que se proponga que los puntos de acceso operarán. Parte del trabajo del *site survey* es verificar estas pruebas de interferencia. Si se realiza el *site survey* en cada punto de acceso con el mismo canal, y no el canal que realmente empleará, no se tendrá la certeza de si existe o no interferencia en ese canal.

3.2.1.1 Canal Fijo

Para establecer el canal deseado en el punto de acceso ingresamos a *NETWORK INTERFACES -> Radio-802.11g -> Settings* y establecemos el canal deseado como se indica la figura 3.29.

El punto de acceso cisco 1200 permite realizar pruebas que determinan la utilización del canal, lo cual proporciona una ayuda adicional en la selección de canales, como lo indica la figura 3.30.

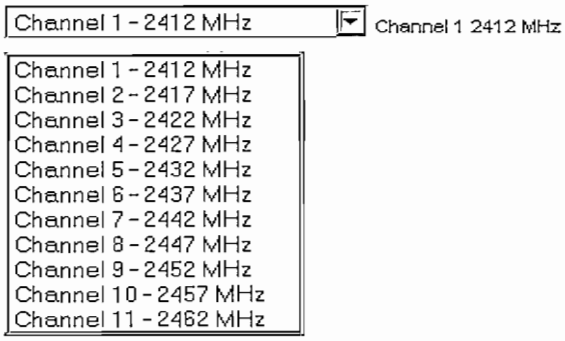


Figura 3.29.- Establecimiento del Canal en el AP1200

Hostname ApEEQ1 Ap

Network Interfaces: Radio0-802.11G Carrier Busy Test

Carrier Busy Test: Start

Carrier Busy Test Output

Frequency	Carrier Busy %
2412	0
2417	0
2422	0
2427	0
2432	0
2437	0
2442	0
2447	0
2452	0
2457	0
2462	0

Figura 3.30.- Pruebas para selección de canales

3.2.2 SELECCIÓN DE VELOCIDADES

Una vez que se conozca la mínima velocidad a la cual operarán los clientes, se realizará el *site survey* a esa velocidad [10].

En el ejemplo de la figura 3.31 se ha realizado un *site survey* en un almacén a 2 y 5.5Mbps en una red IEEE 802.11b.

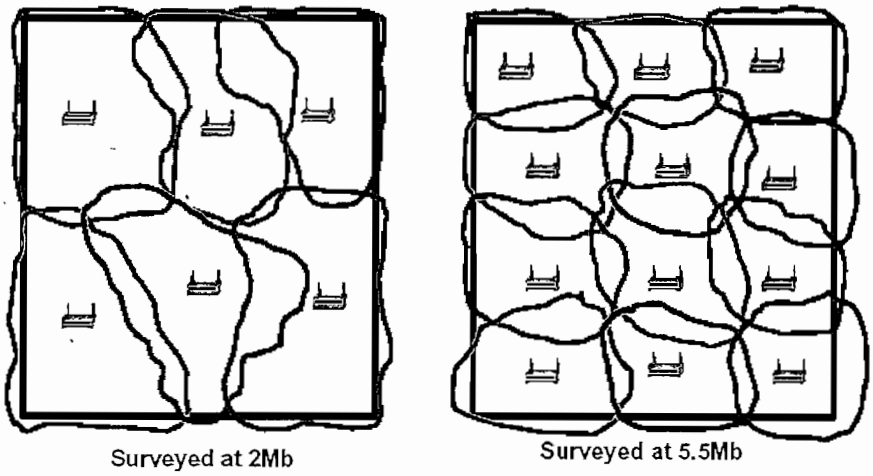


Figura 3.31.- Site Survey a Diferentes Velocidades [8]

Para el diseño inalámbrico con IEEE 802.11g se ha considerado tanto en sitios abiertos o lejanos de poco tráfico, así como en sitios en los cuales se tiene mayor número de usuarios la velocidad de comunicación será de 1 hasta 54 Mbps.

La velocidad que se escoja afectará drásticamente los resultados del site survey. En el ejemplo de la figura 3.31, el site survey del mismo almacén fue realizado a dos diferentes velocidades.

Al considerar 2 Mbps, son necesarios 6 puntos de acceso cubrir el área...

A 5.5 Mbps son necesarios 12 puntos de acceso.

Conocer que velocidades requiere el cliente para que el *site survey* no se realice a velocidades erróneas y los clientes que instalen la WLAN, no les ocurra que solamente se conectarán ciertas áreas y será imposible conectar todas.

Las velocidades teóricas que fueron planteadas en el diseño de la red inalámbrica fueron de un radio de cobertura de 27m a una velocidad de 54Mbps para los 11 puntos de acceso. Para realizar el site survey a una velocidad de 54 Mbps es

necesario establecer que el punto de acceso solamente funcione a esa velocidad, para ello se puede ingresar a la configuración del radio 802.11g.

Para realizar esto se ingresa a *NETWORK INTERFACES -> Radio-802.11g -> Settings* y deshabilitamos las velocidades inferiores a 54 Mbps en la transmisión vía radio como lo indica la figura 3.32, con ello obligamos a que la estación cliente se enlace a 54 Mbps.

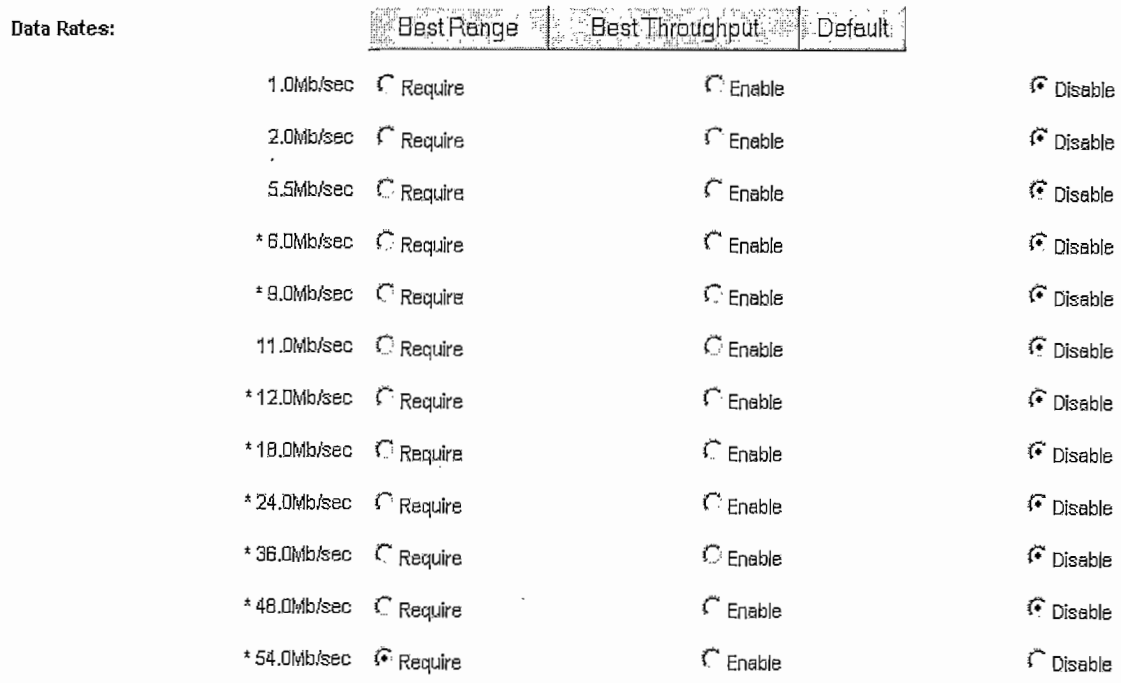


Figura 3.32.- Establecimiento de Velocidad 54Mbps en el AP1200

Luego de realizar las pruebas de campo en El Dorado a 54Mbps, se ha determinado las áreas de cobertura que ofrece el diseño. El anexo 4 muestra gráficamente el site survey a 54 Mbps, el cual implica la necesidad de 19 puntos de acceso, lo cual no es una solución económica válida, por ello se procedió a negociar velocidades.

3.2.2.1 Pruebas Realizadas y Resultados del *Site Survey*

Se procedió a realizar el *Site Survey* de los lugares requeridos con negociación de velocidades que van desde 1 hasta 54 Mbps, lo cual incide una ubicación mejor de los puntos de acceso, sin embargo la antena Cisco Air-Ant4941 de 2.2 dBi ofreció muy poca cobertura por lo cual se realizó las pruebas de campo con la

antena AIR-ANT1728 omnidireccional de 5.2dBi. El anexo 4 muestra la representación gráfica del S*ite Survey* con velocidades negociables.

Luego de establecer la ubicación de los puntos de acceso, se han escogido puntos de prueba dentro del alcance de cobertura.

Estos puntos de prueba constan gráficamente en el anexo 5, y son simbolizados mediante AP1pp1 indicando que corresponde al punto de prueba 1 del punto de acceso 1, como se indica en la figura 3.33.

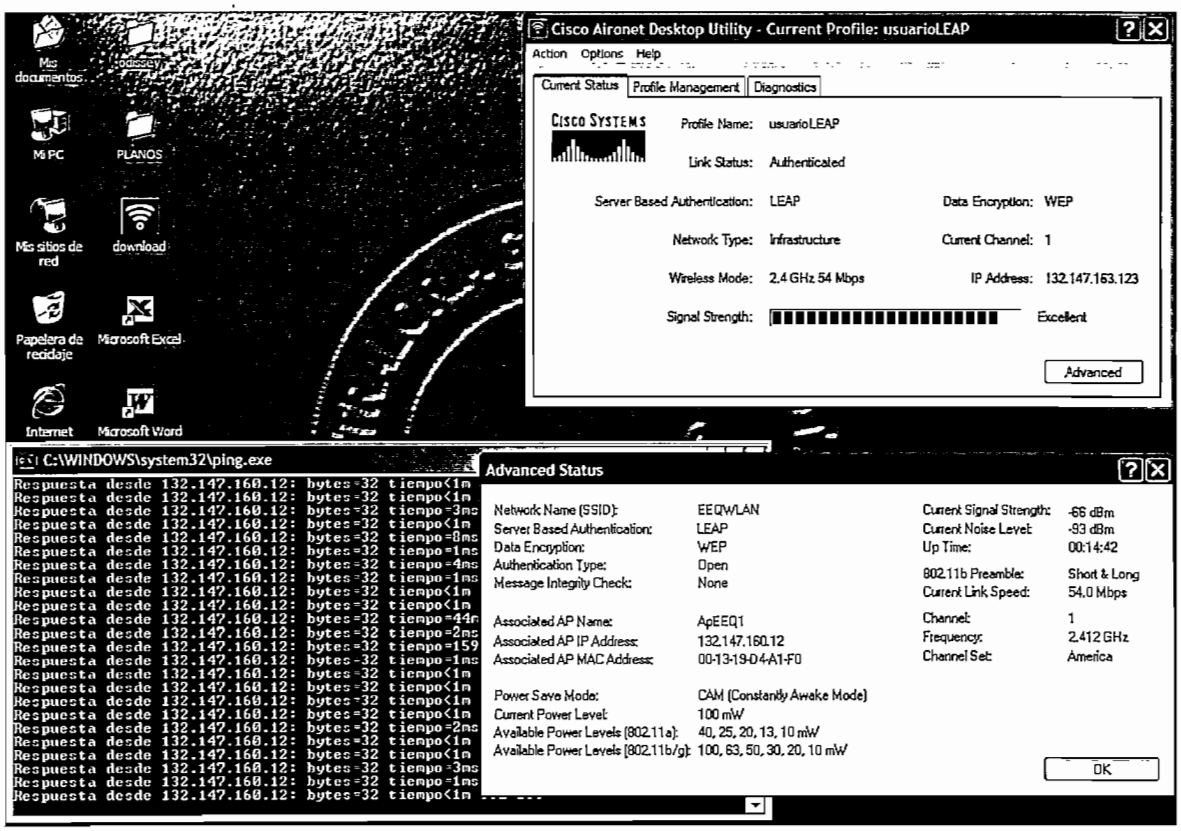


Figura 3.33.- Punto de Prueba 1 del Punto de Acceso 1 (AP1pp1).

La figura 3.33 muestra información como tipo de autenticación LEAP, Encripción WEP, calidad de señal *excelente*, velocidad actual *54Mbps*, fortaleza de señal *-66 dBm*, nivel de ruido *-93dBm*, canal empleado *1.*

Estos fueron los resultados obtenidos para el campus, los cuales se presentan tabulados en la Tabla 3.3.

Tabla 3.3- Resultados del Site Survey.

Punto de Acceso	Ubicación	Punto de prueba	Calidad de señal	Veloc (Mbps)	Fuerza de la Señal (dBm)	Nivel de ruido (dBm)	Canal	Dist (m)
AP1	Div. Talleres y Transportes	AP1pp1	Excelente	54	-66	-93	1	5
		AP1pp2	Excelente	54	-50	-93	1	2.8
		AP1pp3	Excelente	24	-67	-93	1	6
		AP1pp4	Excelente	11	-63	-93	1	8
	Dep. Seguridad industrial	AP1pp5	Excelente	11	-75	-93	1	15
		AP1pp6	Excelente	11	-77	-93	1	16
		AP1pp7	Bueno	5.5	-81	-96	1	20
	Subestaciones	AP1pp8	Bueno	1	-84	-96	1	20
AP2	Departamento de Alumbrado Público	AP2pp1	Excelente	54	- 60	-94	1	4
		AP2pp2	Excelente	54	-39	-89	1	3
		AP2pp3	Excelente	54	-59	-96	1	4
AP3	Laboratorio de medidores	AP3pp1	Excelente	54	-61	-96	11	5
		AP3pp2	Excelente	48	-67	-96	11	5
		AP3pp3	Excelente	48	-66	-95	11	4
		AP3pp4	Bueno	11	-73	-94	11	10
AP4	Operadores de red	AP4pp1	Excelente	54	-54	-94	1	3
		AP4pp2	Excelente	54	-47	-91	1	3
AP5	Clientes Especiales	AP5pp1	Excelente	48-54	-53	-93	6	3
		AP5pp2	Excelente	36	-55	-94	6	2
		AP5pp3	Excelente	48-54	-54	-93	6	4
	Bodega automotriz 1	AP5pp4	Bueno	5.5	-84	-93	6	20
AP6	Departamento de Acometidas	AP6pp1	Excelente	24	-55	-95	6	6
		AP6pp2	Excelente	48	-59	-95	6	4
		AP6pp3	Excelente	54	-34	-95	6	2
	Dep. Personal	AP6pp4	Bueno	11	-78	-94	6	20
		AP6pp5	Bueno	1- 5.5	-84	-94	6	25
AP7	Laboratorio de Transfor madores	AP7pp1	Excelente	54	-34	-94	11	3
		AP7pp2	Excelente	12	-69	-94	11	7
	Sección de grúas	AP7pp3	Bueno	1-5.5	- 83	-94	11	15

	Taller industrial	AP7pp4	Excelente	11	-78	-94	11	10
AP8	Mecánica Automotriz	AP8pp1	Excelente	54	-32	-93	6	2
		AP8pp2	Bueno	2	-81	-94	6	15
	Gasolinera	AP8pp3	Bueno	11	-75	-94	6	7
AP9	Operación Mantenimiento Urbano	AP9pp1	Excelente	48	-34	-94	11	3
		AP9pp2	Excelente	54	-34	-93	11	3
		AP9pp3	Excelente	48	-58	-93	11	4
		AP9pp4	Excelente	11	-77	-93	11	7
AP10	Bodega de instalaciones	AP10pp1	Bueno	5.5	-84	-96	1	7
	Bodega automotriz 2	AP10pp2	Bueno	5.5	-83	-93	1	8
AP11	Perdidas Comerciales	AP11pp1	Excelente	11	-84	-93	11	7
		AP11pp2	Bueno	5.5	-84	-96	11	6
	Construcción de Redes	AP11pp2	Excelente	5.5	-83	-96	11	5
		AP11pp3	Bueno	5.5	-79	-93	11	7

Del resultado obtenido en el *Site Survey* se determina que se requieren 11 puntos de acceso para cubrir todos los espacios en los cuales se requiere conexión inalámbrica de usuarios.

3.2.3 SURVEY DE MÚLTIPLES PISOS

Se debe tomar especial precaución cuando se realice un *Survey* de establecimientos con múltiples pisos. APs en diferentes pisos pueden ser capaces de interferir con otros APs de igual forma como si estuviesen en el mismo piso. Es posible usar ésto como ventaja en el *site survey*. Usando una antena grande, es posible penetrar el piso o tumbado y proporcionar cobertura al piso de arriba como al piso de abajo donde se encuentre el AP. en el ejemplo de la figura 3.34, un edificio de cuatro pisos requiere cobertura. Un único AP no podría cubrir un piso entero.

El montar dos APs por piso podría resultar un incremento en costos, y podría representar un problema de superposición con APs que manejen el mismo canal. Ese problema puede ser resuelto utilizando una antena patch en los APs.

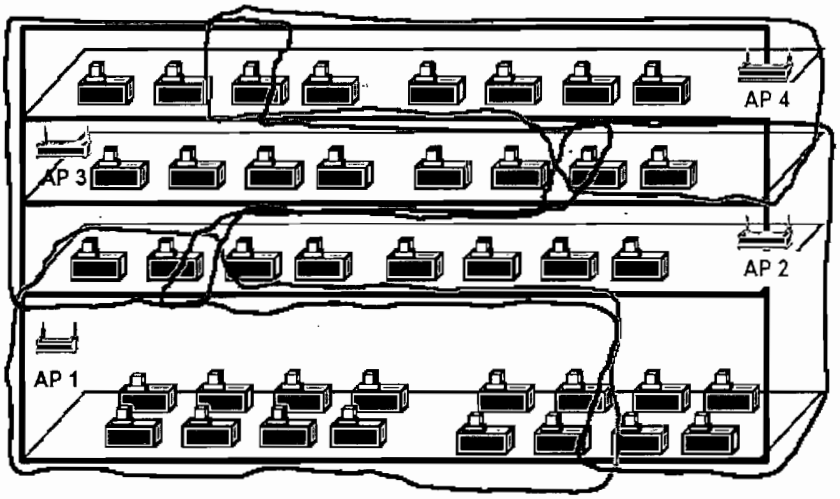


Figura 3.34.- Site Survey de Múltiples Pisos[10].

Porque la antena patch es semi-direccional, y se obtiene suficiente cobertura desde cada AP para cubrir la mayoría del piso y una porción de los pisos superior e inferior a él. El montaje de APs se realiza alternando pisos y colocándolos en los extremos de la edificación.

3.2.3.1 Resultados Obtenidos

En el lugar se tiene el Edificio Polifuncional que consta de tres pisos, en este lugar se ha realizado esta consideración la cual se indica el *Site Survey* de múltiples pisos y se pudo observar que existe cobertura entre pisos debido al rango que va desde 1 hasta 54 Mbps. De igual forma existen dos pisos en la edificación de Laboratorio de Transformadores en los cuales se tiene un punto de acceso que cubre las dos plantas, esto se indica en la tabla 3.4.

Tabla 3.4.- Site Survey de Múltiples Pisos

AP	Ubicación	Departamentos	Piso
AP1	Div. Talleres y Transportes	División talleres y transportes	3
		Seguridad Industrial	2
AP7	Laboratorio de transformadores	Operadores	2
		Jefatura	1

3.2.4 SEGURIDAD EN EL CAMPUS

Es necesario cumplir la política de seguridad que se planteó en el diseño, el siguiente instructivo debe ser cumplido por todas las personas que se encuentren de alguna manera relacionados con esta tecnología, se indica en la tabla 3.5.

Tabla 3.5.- Cumplimiento de Política de Seguridad

Política	Cumplimiento
Identificar quien puede usar tecnología WLAN.	Empleados, operadores, personal autorizado.
Identificar en que lugares el acceso a Internet es requerido.	Oficinas, Departamentos de investigación
Describir quién puede instalar puntos de acceso y otro equipamiento inalámbrico.	Personal capacitado del área de comunicaciones y soporte técnico de la Div. Sistemas
Proporcionar limitaciones en la localización de puntos de acceso por seguridad física.	Interiores de Oficinas al campus.
Describir el tipo de información que puede ser enviada sobre enlaces inalámbricos.	Tráfico http, Telnet a servidores, correo, aplicaciones, archivos.
Filtrado MAC, Encripción WEP.	Habilitados
Servidor de autenticación RADIUS	Habilitado
Describir limitaciones sobre como los dispositivos inalámbricos pueden ser usados, tales como ubicación.	Manipulación por personas técnicas autorizadas previamente.
Describir las configuraciones de hardware y software de todos los dispositivos.	Realizar un registro de configuraciones en el área de Sistemas por AP.
Proporcionar líneas guía sobre reportes de pérdidas de dispositivos inalámbricos e incidentes de seguridad.	Reporte inmediato a Control Bienes, por parte de la persona a cargo de los equipos
Proporcionar una guía sobre el uso de encripción y administración de llaves	Las claves de encripción cambiarán cada 60 días, y serán administradas desde el área de Sistemas
Definir la frecuencia y alcance de estas políticas.	Permanente, o hasta que se comunique con anterioridad nuevas políticas

3.2.4.1 Seguridad de Passwords.

Se tendrá una política en cuanto al cambio periódico de passwords, su forma de establecimiento, y capacitación para evitar ataques denominados de ingeniería social.

Regla	Descripción a cumplir
Establecimiento de Password	Personalmente
Codificación de passwords	Alfanumérico mínimo 8 caracteres
Validez del password	60 días
Capacitación a usuarios	Previa instalación o cambio de passwords
Personal a cargo	Departamento de Sistemas

3.2.4.2 Seguridad Física de Puntos de Acceso.

Seguridad en cuanto a la instalación se realizará asegurando físicamente los puntos de acceso a paredes mediante taco fisher 6, y tornillos adecuados.

Existen lugares en los cuales se requiere seguridad mayor como es el caso de Construcción de redes, Operación y mantenimiento Urbano, en este caso se solicitará al taller industrial la fabricación de cajas herméticas diseñadas para contener los puntos de acceso, las cuales se empotrarán en sitios determinados.

Ubicación	Cantidad
Construcción de Redes	1
Operación y Mantenimiento Urbano	1

Estas cajas no se incluyen en el presupuesto ya que la EEQ se encarga de elaborar este tipo de cajas.

3.2.5 PRUEBAS DE SEGURIDAD

Es necesario establecer pruebas de seguridad para verificar la operación de la red con los parámetros configurados.

Puede suceder que un usuario no autorizado tenga un adaptador inalámbrico que explore las redes disponibles, tenga una dirección IP válida pero no esté autorizado a nivel MAC, el usuario haya establecido un nombre de usuario incorrecto, o que esté mal su password.

Es importante verificar el alcance de señales que emite el punto de acceso con la finalidad de tener cobertura dentro del campus y evitar (en lo posible) sitios en los cuales no se desea cobertura. Estas pruebas se han realizado obteniendo los resultados de esta sección.

3.2.5.1 Broadcast de SSID

Al deshabilitar el envío de esta invitación en el punto de acceso, se puede observar que usuarios no verán a la red inalámbrica, por lo que la red pasa inadvertida y por tanto los usuarios indebidos al no saber que existe la red no intentan conectarse a ella, aunque tienen el adaptador cliente instalado, esto se indica en la figura 3.35.

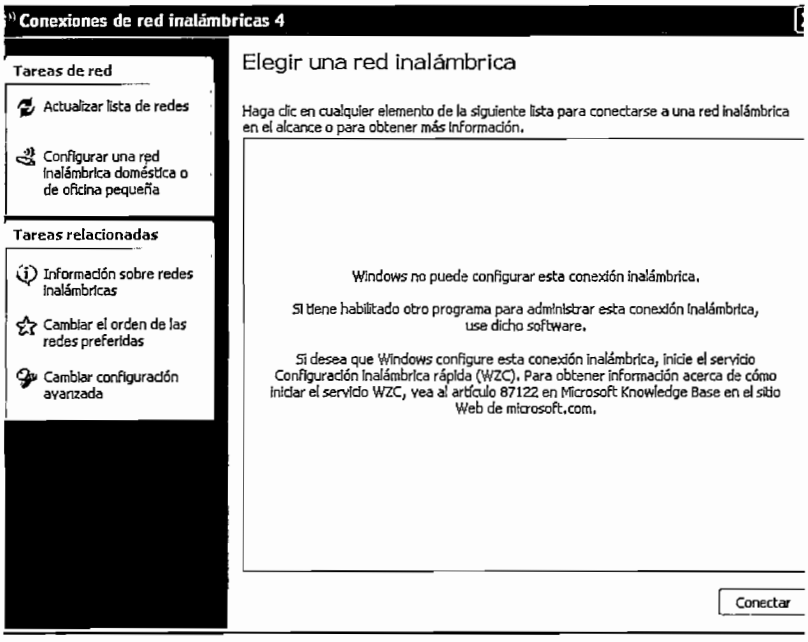


Figura 3.35.- Redes Inalámbricas Disponibles

3.2.5.2 Usuario sin Configuración

El usuario Default viene configurado sin seguridad en el cliente, al activarlo éste no puede acceder a la red ya que su indicador mostrará que no se encuentra

asociado a ningún punto de acceso y mostrará su estado como se indica la figura 3.36, ya que no se encuentra configurado correctamente.

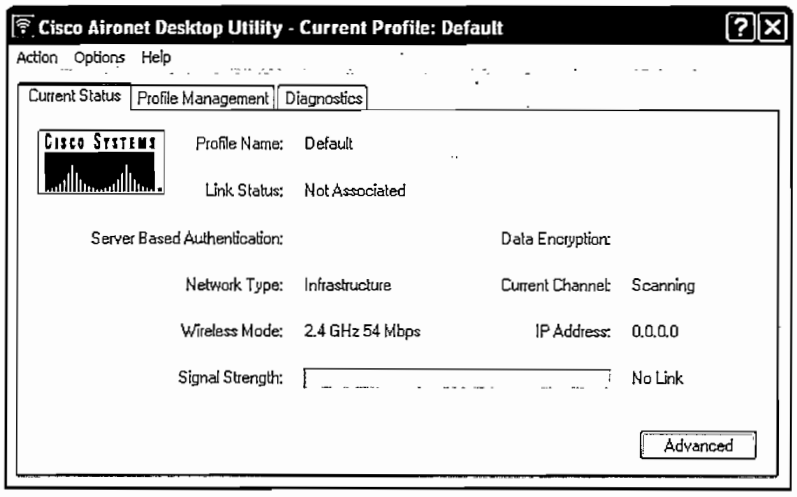


Figura 3.36.- Usuario Default sin Conexión

3.2.5.3 Dirección MAC Incorrecta

Se ingresa al punto de acceso y se cambia la dirección MAC que está permitida en el filtro, MAC ID: 0040.96A3.1CBB a una MAC ID: 0040.96A3.1CBA la cual no pertenece a ningún cliente, como se indica en la figura 3.37,

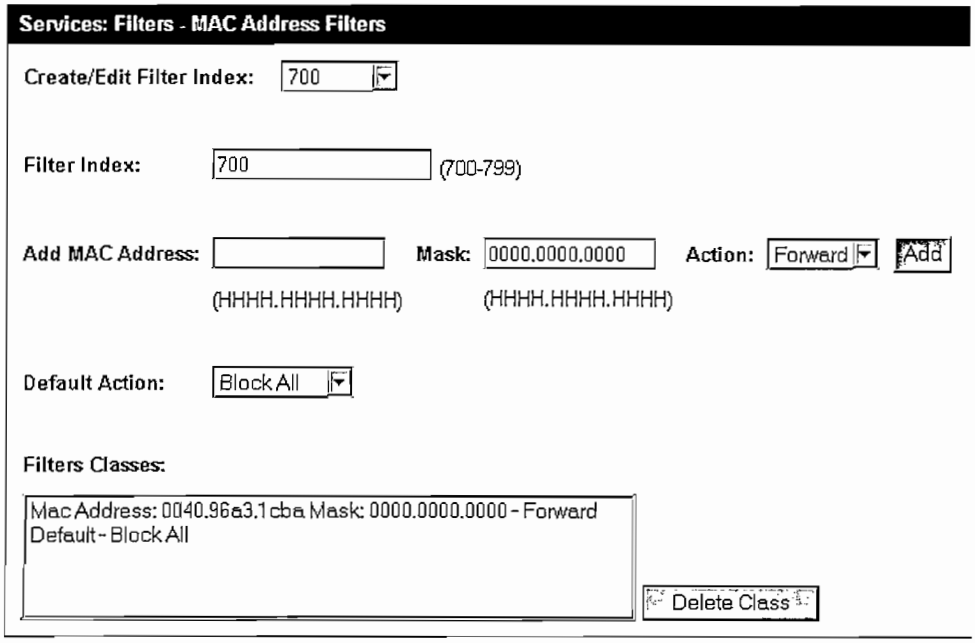


Figura 3.37.- Pruebas de Seguridad MAC Incorrecta

Al realizar este cambio el cliente muestra su estado como asociado, y entra en un proceso de autenticación el cual no es satisfactorio y no se autentica el cliente, como se indica en la figura 3.38.

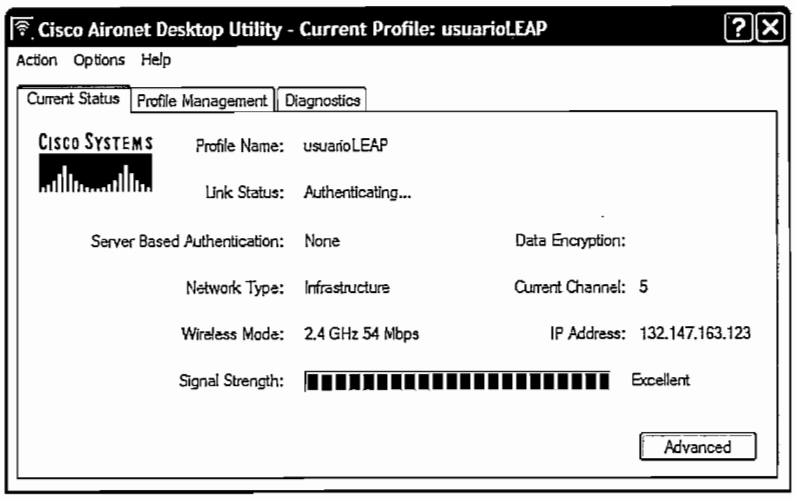


Figura 3.38.- Pruebas de Seguridad Cliente MAC Incorrecta

Con ello el cliente no puede acceder ni pasar datos a la red como se indica mediante un ping al punto de acceso cuya IP es 132.147.160.12 de la figura 3.39.

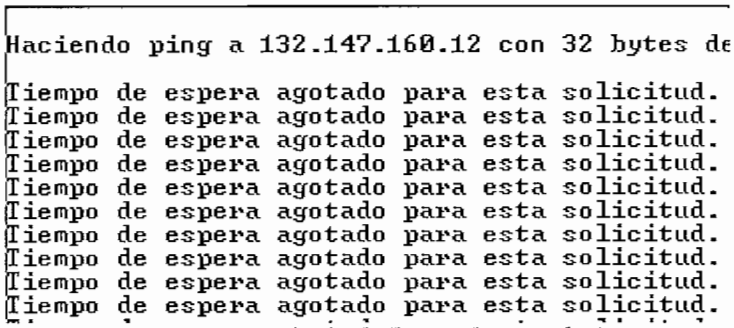


Figura 3.39.- Ping desde el Cliente al Punto de Acceso

Esto se confirma al dar un doble clic sobre el icono de la barra de estado del utilitario del ADU con lo cual nos aparece la pantalla de la figura 3.40

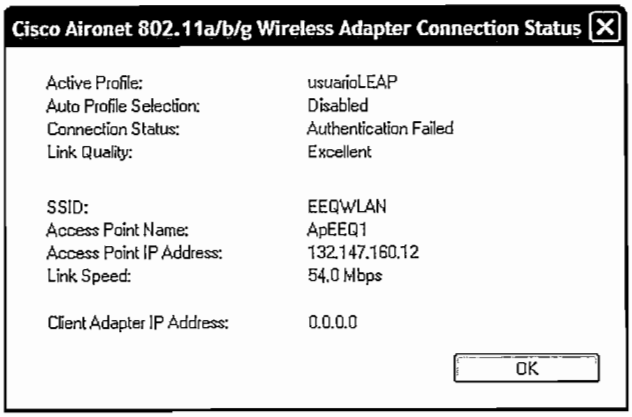


Figura 3.40.- Resumen del Cliente del ADU

Se puede observar que el cliente se encuentra asociado pero no es capaz de enviar información ya que la autenticación ha fallado.

Al establecer nuevamente la dirección MAC en el Filtro, se puede observar que el ping al punto de acceso empieza e responder como se indica en la figura 3.41.

```
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 132.147.160.12: bytes=32 tiempo=2ms TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo=1ms TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo=1ms TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo=1ms TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo=1ms TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo=1ms TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo<1m TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo=1ms TTL=255
Respuesta desde 132.147.160.12: bytes=32 tiempo<1m TTL=255
```

Figura 3.41.- Respuesta al Activar la Dirección MAC

El utilitario indicará en su estado como autenticado como se indica en la figura 3.42.

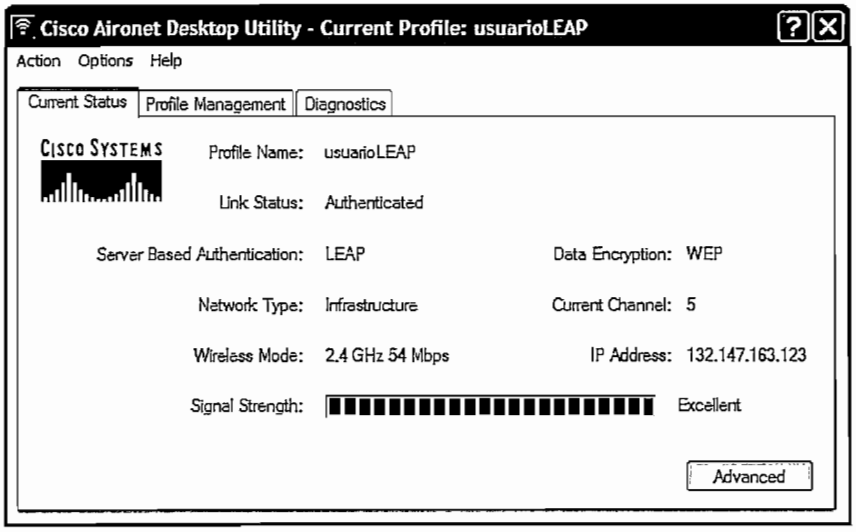


Figura 3.42.- Estado del Cliente Autenticado.

3.2.5.4 Nombre de Usuario Incorrecto

Se ingresa al *ADU -> Profile Manager* y se cambia el usuario como se indica en la figura 3.43, se establece un usuario con el nombre usuarioX en lugar del usuario1 que se encuentra establecido.

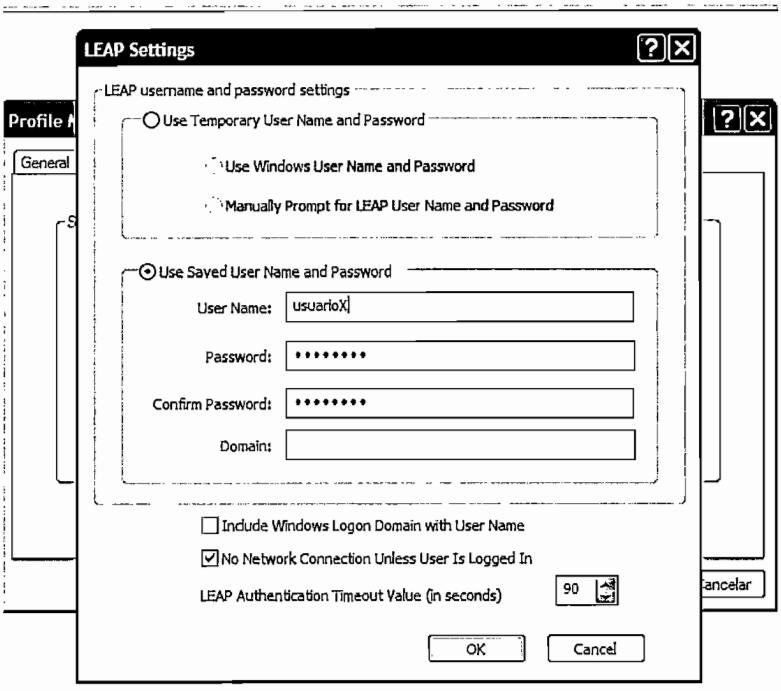


Figura 3.43.- Usuario LEAP Incorrecto

Al tener un cliente con el nombre de usuario mal configurado, inicia su proceso de autenticación, al fallar presentará que el nombre de usuario o contraseña se encuentra incorrecto, como se indica la figura 3.44.

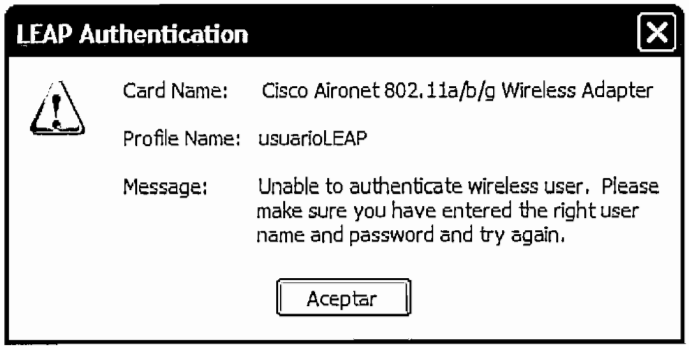


Figura 3.44.- Nombre de Usuario Incorrecto

El cliente pedirá que ingrese nuevamente el nombre de usuario y contraseña para poder autenticarse, si persiste el error no podrá pasar datos al punto de acceso

En este caso el cliente se deshabilita y muestra en la parte superior derecha (*Disabled*) , aunque se asocia al punto de acceso pero el interfaz se deshabilita como se indica en la figura 3.45.

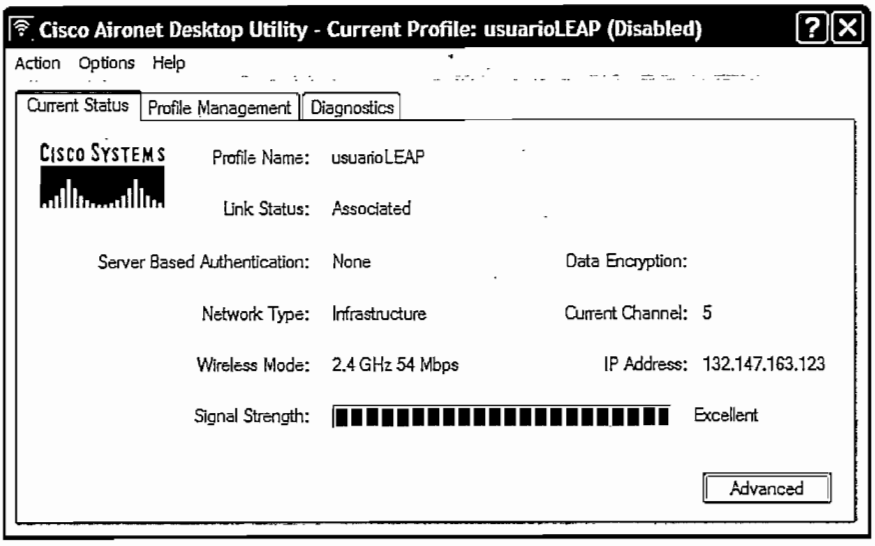


Figura 3.45.- Cliente Deshabilitado

3.2.5.5 Password Incorrecto

Se establece en la utilidad ADU un password erróneo, ingresamos a *Profile Manager*, seleccionamos el perfil de usuario llamado usuarioLEAP, ingresamos a *Modify->Security->Configure* con lo que aparece la pantalla de la figura 3.46.

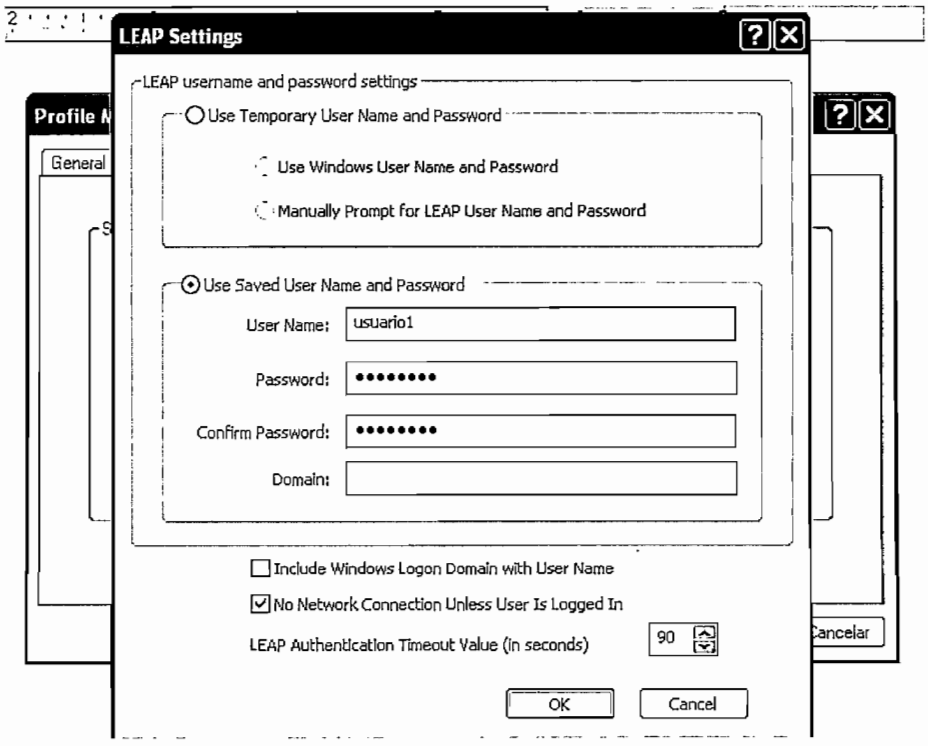


Figura 3.46.- Establecimiento de Contraseña Incorrecta

Establecemos la contraseña **aqswde1** en lugar de la contraseña correcta **aqswde01**, aceptamos los cambios con *OK*. Al activarse el perfil de usuario

empieza el proceso de autenticación dando como resultado que el nombre de usuario o contraseña es incorrecta, como se indica en la figura 3.47.

Figura 3.47.- Contraseña Incorrecta

Al tener mal el nombre de usuario o contraseña y persistir el problema el interfaz se deshabilita y el ADU presentará esto en su pantalla principal, en la parte superior derecha como lo indica la figura 3.45 de cliente deshabilitado.

Al volver a activar el password correcto, el cliente empieza el proceso de autenticación, al culminar este proceso podemos observar como el ping sube, es decir, empieza la respuesta desde el punto de acceso, como se indica en la figura 3.48.

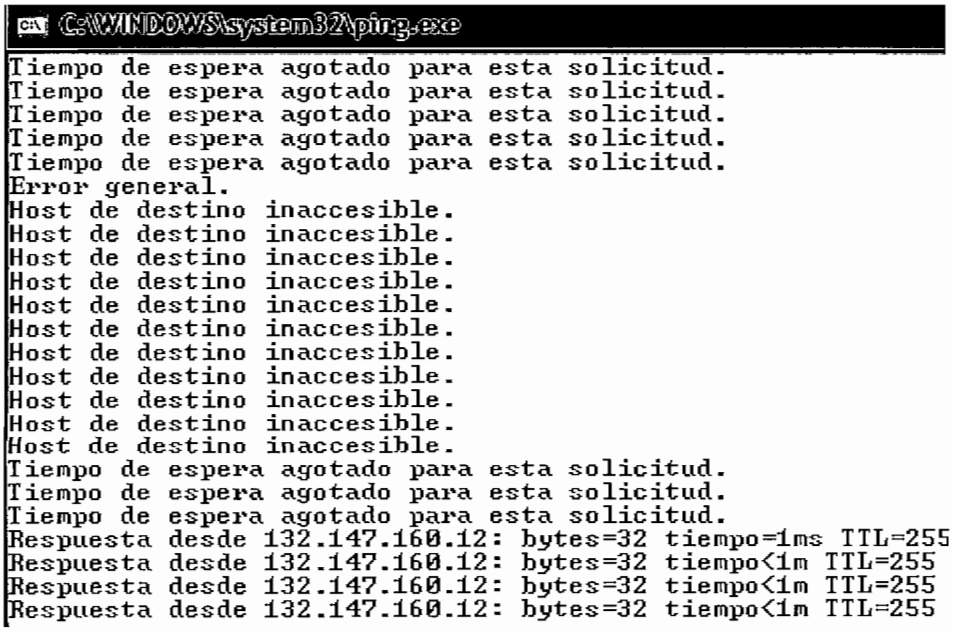


Figura 3.48.- Cliente Autenticado (ping)

Se puede observar que existe un error general ya que el interfaz se deshabilitó, al insertar el interfaz nuevamente pasa de *host de destino inaccesible* a *tiempo de espera agotado para esta solicitud* y al pasar la autenticación empieza la respuesta del ping.

El cliente en el ADU pasa del estado asociado al estado autenticado como se indica en la figura 3.49.

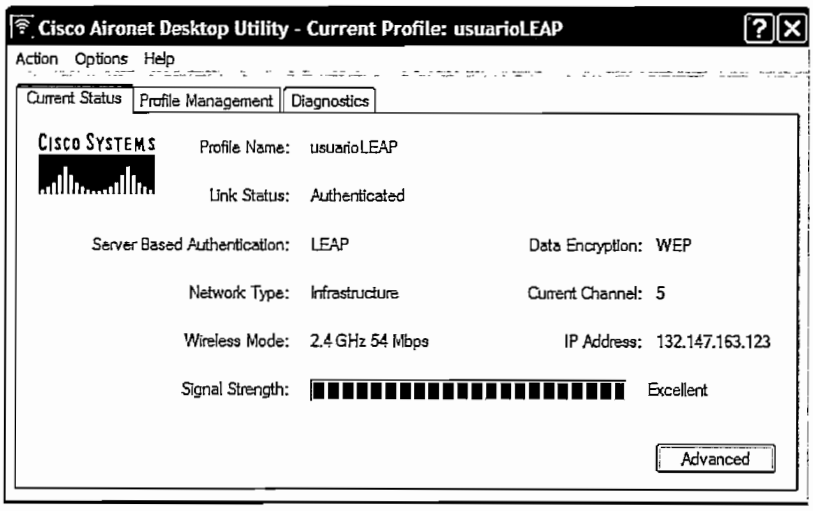


Figura 3.49.- Cliente Autenticado (ADU)

3.2.5.6 Pruebas de Límite de Alcance

El límite de alcance de señal que ofrece el punto de acceso es un factor importante en las pruebas de seguridad, ya que un usuario mal intencionado puede estar en el contorno del campus intentando acceder a la red inalámbrica.

En lo posible se ha procurado tener cobertura dentro del campus como se puede apreciar al ver las ubicaciones de los puntos de acceso.

Al alejarnos fuera del área de cobertura del punto de acceso se pierde señal desde el cliente hacia el AP, la siguiente prueba se realizó para el AP6, ubicado en el departamento de Acometidas, el cual sirve al departamento de personal.

En la figura 3.50 se indica que ocurre cuando se sale fuera del área de cobertura.

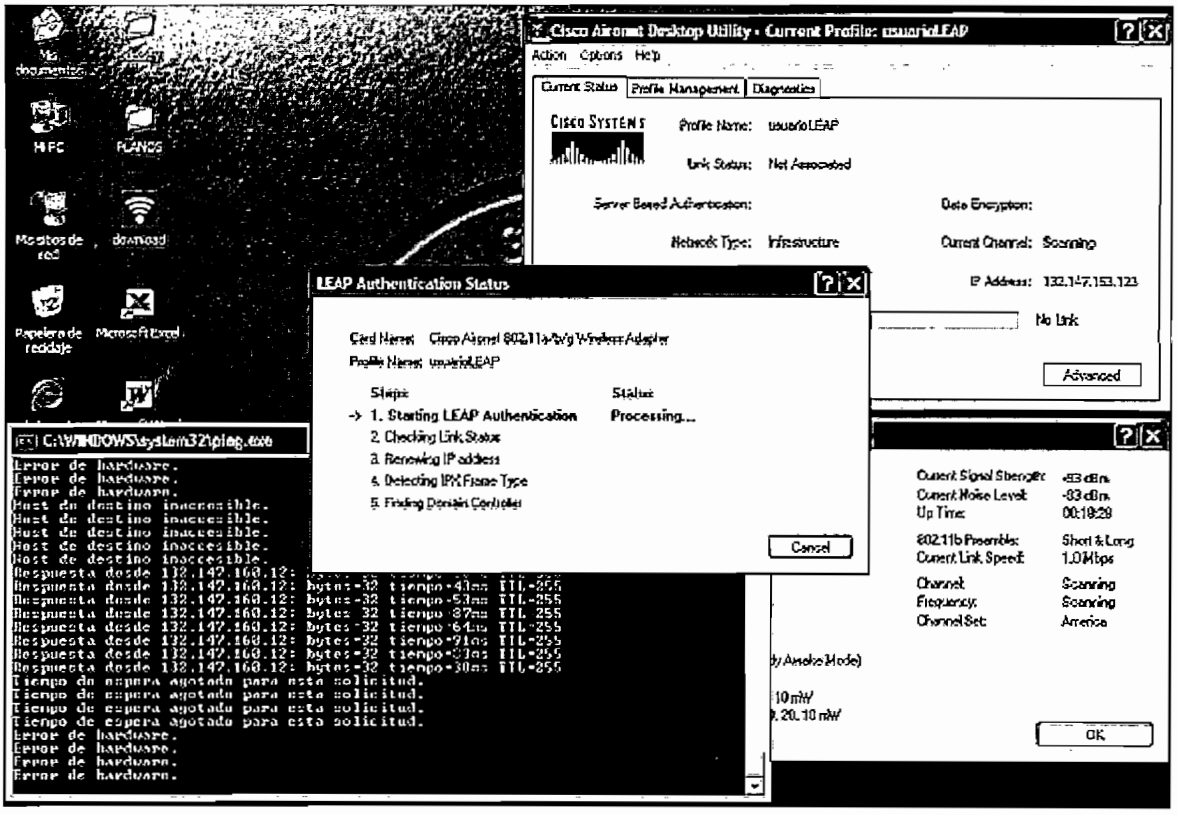


Figura 3.50.- Límites de Cobertura.

El cliente intenta mantenerse en conexión con el punto de acceso e inicia nuevamente el proceso de autenticación, pero al estar fuera del área de cobertura, el cliente se mostrará como no asociado.

Al mantener un ping hacia el punto de acceso se observa como se pierde conexión. Al ingresar en el área de cobertura del punto de acceso el cliente empezará el proceso de autenticación y finalmente se enlazará.

3.3 CORRECCIONES DEL DISEÑO.

Con toda la información de la sección anterior, se han recogido todos los elementos necesarios y seguido las sugerencias planteadas. Se ha realizado la elaboración completa del site survey en el sitio, de lo cual se ha determinado las correcciones necesarias para lograr el mejor desempeño de la red, obtener todos los elementos requeridos para saber con exactitud cuáles deben ser las ubicaciones de puntos de acceso, así como la utilización de canales, selección de velocidades para la red 802.11g, para finalmente presentar los costos del

proyecto, esto se puede detallar en dos grupos, correcciones de la parte inalámbrica y de la parte cableada.

3.3.1 CORRECCIONES INALAMBRICAS

En esta sección se especifica con exactitud la ubicación que tendrán los puntos de acceso, así como información adicional que servirá como referente para presentar finalmente los costos de implementación.

La tabla 3.6 presenta las modificaciones necesarias a la tabla 2.6 del capítulo anterior, en la cual constan edificación, Cantidad de puntos de acceso y su ubicación.

Tabla 3.6.- Ubicación de puntos de acceso

Edificio	Cantidad	Ubicación	Punto de Acceso
Edificio Polifuncional	5	Div. Talleres y Transportes	AP1
		Departamento de Alumbrado Público	AP2
		Laboratorio de medidores	AP3
		Operadores de Red	AP4
		Clientes Especiales	AP5
Departamento de Acometidas	1	Ingreso a Acometidas	AP6
Laboratorio de Transformadores	1	Jefatura	AP7
Mecánica automotriz	1	Jefatura	AP8
Operación y mantenimiento urbano	1	Corredor central	AP9
Bodegas de instalaciones	1	Interior de bodegas	AP10
Construcción de Redes	1	Edificación	AP11

3.3.2 CORRECCIONES DEL CABLEADO ESTRUCTURADO

Incluye modificaciones en cuanto a *patchcords*, número de corridas, equipamiento de fibra, cuarto de equipos, canaletas y mangueras.

- **PATCHCORDS**

No presenta modificaciones, se requieren 11 *patchcords* de 3 pies cat5.

- **NÚMERO DE CORRIDAS**

El número de corridas que se requieren para la ubicación de los puntos de acceso determina la cantidad de cable UTP necesario.

De lo estudiado en el capítulo 2 y considerando el método exacto de distancias desde el closet de comunicaciones, hasta cada punto de acceso, se muestran distancias en la tabla 3.7.

Tabla 3.7.- Distancias del método exacto

Ubicación	AP	Distancia (m)
Div. Talleres y Transportes	AP1	8
Dep. de Alumbrado Público	AP2	45
Laboratorio de medidores	AP3	30
Operadores de Red	AP4	70
Clientes Especiales	AP5	40
Acometidas	AP6	55
Laboratorio de Transformadores	AP7	60
Mecánica Automotriz	AP8	80
Operación Mantenimiento Urbano	AP9	40
Bodega automotriz 2	AP10	45
Construcción de redes	AP11	120 -> fibra

El AP11 (Construcción de redes), será tratado en requerimiento para el equipamiento de fibra óptica.

Sumando las distancias que no sobrepasen los 305 metros de una bobina se tiene:

Ubicación	Nombre	Distancia
Div. Talleres y Transportes	AP1	8+3
Departamento de Alumbrado Público	AP2	45+3
Laboratorio de medidores	AP3	30+3
Operadores de Red	AP4	70+3
Clientes Especiales	AP5	40+3
Acometidas	AP6	55+3
Total	**266m**	

Para estas corridas se requiere 1 bobina de 305m.

Ubicación	Nombre	Distancia
Laboratorio de transformadores	AP7	60+3
Mecánica automotriz	AP8	80 +3
Operación y mantenimiento urbano	AP9	40+3
Bodega automotriz 2	AP10	45+3
Total	**237m**	

De acuerdo a esto el número requerido es de **2 bobinas.**

- **EQUIPAMIENTO DE FIBRA**

La distancia desde el closet de telecomunicaciones hasta Construcción de Redes sobrepasa las distancias especificadas para cableado horizontal, por lo cual se requiere equipamiento de fibra óptica para llegar al punto de acceso.

Se requiere Fibra óptica 4 hilos, multimodo 62.5/125μm para instalación aérea tipo ADSS en exteriores, Dos convertidores de medio fibra óptica – FastEthernet tipo multimodo, conectividad ST, 2 Patchcords (3m) de fibra óptica multimodo 62.5/125 μm, una caja multimedia para fibra, instalación y certificación de 4 hilos.

El detalle de estos elementos se encuentra especificado en el resumen de requerimientos.

- **CUARTO DE EQUIPOS**

Para dimensionar el Rack se suma todos los *patchpanel*, *switchs*, organizadores, bandejas, supresores, de acuerdo a unidades HU resumidos en la Tabla 3.8.

Tabla 3.8.- Dimensionamiento del Rack

Descripción	Cantidad	UR
Patch Panel 24	1	2
Switch 24	1	1
Organizadores		2
Supresores		1
Bandeja para convertidores		1
Espacio intermedio		1
Total		**8**

(UR: unidades de Rack)

1 UR = 1.75 pulgadas

8 UR *1.75 = 14 pulg.

Por lo tanto se requiere de 1 **Rack de 19 pulg. ancho por 14 pulg. de alto.** o superior.

- **CANALETAS Y MANGUERAS**

Los cambios de distancias estimadas para utilización de canaletas especificadas de la tabla 2.10 se ven reflejadas en la tabla 3.9.

Tabla 3.9.- Estimado de canaletas y manguera

Ubicación	Nombre	Distancia (m)	Canaleta (m)	Manguera 1" (m)
Div. Talleres y Transportes	AP1	8	8	0
Dpto de Alumbrado Público	AP2	45	10	35
Laboratorio de medidores	AP3	30	10	20
Operadores de Red	AP4	70	5	65
Clientes Especiales	AP5	40	5	35
Acometidas	AP6	55	15	40
Laboratorio de Transformadores	AP7	60	4	56
Mecánica Automotriz	AP8	80	3	77
Operación mantenimiento Urbano	AP9	40	15	25
Bodega automotriz 2	AP10	45	2	43
Total canaleta			**77**	
Total manguera				**396**

3.4 COSTOS DE IMPLEMENTACIÓN

En esta sección los costos que implicaría la implementación de la red inalámbrica.

3.4.1 COSTO DE ELEMENTOS

Las modificaciones realizadas en el diseño, reflejan el cambio de los requerimientos que fueron presentados en el capítulo anterior. Se han realizado las modificaciones necesarias a la tabla 2.11, en la cual se detallaron en resumen los elementos que teóricamente fueron necesarios.

La tabla 3.10 presenta con mayor certeza todo lo necesario en cuanto a equipos de comunicación así como los demás accesorios, y elementos para implementar la red.

Tabla 3.10.- Lista de Requerimientos y costos de materiales

ITEM	DESCRIPCIÓN	Cant	Precio	Total
1	Punto de acceso Cisco Aironet serie 1200 Manejo de IEEE 802.11g, Banda 2.4 GHz Velocidades 1, 2, 5.5, 11, 24, 36, 48, 54 Mbps Seguridad WEP, WPA, TKIP, EAP, LEAP, LEAP-TLS, Puerto Ethernet de uplink 10/100 Mbps autosensing, Acceso Web, Consola, Telnet, Cisco IOS Software versión 12.2(13)JA o superior. Protocolo CSMA/CA, Antena Cisco AIR ANT-1728.	11	989	10.879
2	Adaptador PCI Cisco Airones 802.11a/b/g	66	274	18.084
3	Adaptador Cliente PC Card Cisco 802.11a/b/g	7	186	1.302
4	PATCH PANEL de conexiones de 24 puertos tipo RJ45 categoría 5e para distribución de cables tipo UTP de cuatro pares completo y armado	1	80	80
5	RACK estándar, tipo abierto de sistema estructurado de 19" de ancho por 42" de alto, con dos parantes verticales y bases de soporte cat5e	1	90	90
6	Bobinas de 305m cable UTP cat5e	2	80	160
7	Fibra óptica ADSS multimodo 62.5/125µm, 4hilos, supervisión de montaje, certificación de 4 hilos, mano de obra	130 m	4.5	585
8	Pigtails multimodo de conexión fibra fusión mediante pitillos	4	15	60
9	Caja de instalación de fibra óptica	2	125	250
10	Convertidor de medio fibra óptica multimodo con conectividad ST -- FastEthernet 10/100 Mbps	2	220	440
11	Organizador vertical para Rack 60*40	1	35	35
12	Organizador horizontal para Rack 19" 2 UR	1	19	19
13	Supresor de energía de 8 tomas	1	6	6
14	CANALETAS de 2m con capacidad para 2 cables UTP cat5 tipo panduit	39	1.8	70,20
15	Metros de manguera PVC 1"	396	0.2	79,20
16	CODOS para canaleta con capacidad para 2 cables UTP cat5 de pared	20	0.9	18
17	UNIONES para canaleta de 2m con capacidad para 2 cables UTP cat5 de pared	20	0.9	18
18	Patch cords de 3 pies cat5e	11	3.5	38,5
Precio referencial USD				32.293

Estos valores son precios referenciales, basados en proformas del mercado, vea anexo 6.

3.4.2 COSTO DE INSTALACIÓN Y CONFIGURACIÓN

El costo de instalación está en relación al número de puntos de acceso a ser instalados, así como instalación en el cuarto de equipos, canaletas y accesorios necesarios. Costos por configuración está en relación a la cantidad de horas técnicas de configuración de los equipos como son puntos de acceso, y adaptadores inalámbricos en los clientes.

Estos costos de instalación y configuración se presentan en la tabla 3.11.

Tabla 3.11.- Costos de instalación y configuración

Cant	Descripción	Costo	Costo total
19	Punto de acceso Cisco Aironet serie 1200. Manejo de IEEE 802.11g, banda 2.4 GHz, Seguridad WEP, WPA, TKIP, EAP, LEAP, LEAP-TLS. Puerto Ethernet de uplink 10/100 Mbps autosensing. Acceso Web, Consola, Telnet, Cisco IOS Software versión 12.2 (13) JA o superior. Protocolo CSMA/CA Rango de cobertura 200m (5Mbps) exteriores o superior.	100	1900
66	Adaptador PCI Cisco Aironet 802.11a/b/g	20	1320
7	Adaptador Cliente PC Card Cisco 802.11 a/b/g.	20	140
Costo Total de instalación y configuración de equipos		**3360**	

3.4.3 COSTO TOTAL DEL PROYECTO

El costo por mano de obra, instalación de corridas, canaletas y accesorios es de **1000USD.**
El costo total del proyecto asciende a ***36653 USD***

A una red de estas velocidades se la denomina de alto desempeño por su alto *performance*, la cual brinda mucha mayor flexibilidad que una red mediante cableado estructurado de cobre.

Una red inalámbrica puede ser más económica si los equipos seleccionados no satisfacen características robustas de seguridad las cuales son requeridas.

El costo del diseño propuesto es más elevado que una red cableada UTP por el tipo de equipo y por las configuraciones establecidas.

El crecimiento exponencial de computadoras conlleva muchas consideraciones, obstaculiza ducterías, satura el enrutamiento horizontal, etc. Estas consideraciones hacen de una red inalámbrica el ambiente ideal en un ambiente de negociación de velocidad, y adicionalmente brinda cobertura en lugares que el cable no puede llegar, como son los patios del campus, siempre garantizando al máximo la seguridad de la red, mediante los mecanismos expuestos a lo largo de este proyecto.

Capítulo 4
Conclusiones y Recomendaciones

4 CONCLUSIONES Y RECOMENDACIONES

El presente capítulo tiene como finalidad establecer conclusiones y recomendaciones referentes al diseño y pruebas de campo de la red inalámbrica realizadas en el campus El Dorado de la Empresa Eléctrica Quito S. A. empleando IEEE 802.11g.

Es necesario un conocimiento teórico de los estándares existentes en el mercado así como de su banda de operación, así como de regulaciones nacionales en el uso del espectro radioeléctrico, para poder desarrollar un diseño inalámbrico.

Para la realización de pruebas de campo es necesario tener un conocimiento en cuanto a propagación de antenas, sus patrones de radiación, relación de potencia y ganancia de antenas.

4.1 CONCLUSIONES

Entre las principales conclusiones se establecen los beneficios que brinda una red inalámbrica, la necesidad de políticas de administración, características de seguridad inalámbrica, y aspectos limitantes en el proyecto.

- **BENEFICIOS**

Los beneficios de establecer una red inalámbrica son la flexibilidad, escalabilidad, y rapidez de instalación. La Empresa Eléctrica Quito es una empresa innovadora y flexible en cuanto a movilidad de sitios de trabajo, por lo que se ve expuesta a cambios repentinos, y crecimiento de empleados por departamentos.

Establecer nuevas líneas UTP para la transmisión de datos no es una buena alternativa, aquí se observa el beneficio de la red inalámbrica en cuanto a escalabilidad ya que conectar un usuario nuevo es mucho más fácil.

La utilización de equipos como computadores portátiles es cada vez mayor y son importantes al instante de realizar transacciones como por ejemplo ingresar datos de vehículos a la División de Talleres y Transportes. El emplear la red inalámbrica

permite que estos equipos estén conectados en red permanentemente siendo este un beneficio en cuanto a movilidad y rapidez de instalación.

- **POLÍTICAS DE ADMINISTRACIÓN**

Un aspecto muy importante en una red inalámbrica es la administración que se va a implementar en la misma, ya que para explotar todos los beneficios que nos ofrecen los equipos, es necesario establecer administración y gestión de la red, el implantar una red inalámbrica y dejarla funcionando no es suficiente para garantizar un buen servicio en una institución.

- **SEGURIDAD**

Otro aspecto muy importante en una red inalámbrica es la seguridad que se va a dar a la misma, la mitigación de riesgos para evitar ataques de red es una tarea compleja que no es posible sin una correcta administración, sin una política de seguridad robusta que sea cumplida por la administración y sea constantemente renovada.

El establecimiento de una política de seguridad ayuda a minimizar estos riesgos, y permite a partir de una base de seguridad incursionar en nuevos estudios para la transmisión de datos cada vez más segura.

Con la finalidad de no incurrir en gastos adicionales en el diseño inalámbrico propuesto y obtener un alto nivel de seguridad se estableció las configuraciones necesarias para obtener todo el potencial en cuanto a seguridad que ofrece el punto de acceso Cisco Aironet 1200, para esto se configuró opciones tales como WEP, filtrado MAC, deshabilitación de broadcast SSID, deshabilitación de Telnet, deshabilitación de acceso SNMP,

Adicionalmente se incorporó Autenticación por medio de Servidor RADIUS con LEAP, cuya implementación llevaría un costo adicional aproximado de 2000 USD de la licencia.

- **NECESIDAD DE EFECTUAR PRUEBAS DE CAMPO**

Entre una de las principales conclusiones se encuentra que antes de instalar una red inalámbrica se deben realizar las pruebas de campo en el lugar, puede ocurrir

que el diseño de la red inalámbrica sea muy bueno, y en detalle. Sin embargo existen factores que no pueden ser considerados en papel.

Fuentes de interferencia como son cables de tendido eléctrico, armarios metálicos, son obstáculos que impiden el paso de la señal de radio.

- **ELEMENTOS PREVIOS AL SITE SURVEY**

Muchas ocasiones no se consideran estos detalles que influencian en el tiempo para la realización de pruebas de campo, para un ágil y correcto desempeño de las pruebas de campo es necesario tener el siguiente equipamiento listo:

- El punto de acceso
- Una laptop
- El cliente configurado
- Probar configuraciones de seguridad.
- Cable cruzado
- Extensión de energía eléctrica.

- **MINIMIZAR GASTOS**

Ahorro es la principal diferencia entre realizar un contrato de servicios profesionales o no. Puede ocurrir que se tenga el conocimiento técnico necesario para establecer un diseño y el momento de ponerlo en práctica resulta muy costoso. Elaborar un *Site Survey* en el sitio permite ubicar los puntos de acceso de mejor manera e incluso llegar a determinar puntos de acceso innecesarios.

Las celdas de cobertura se vieron limitadas en alcance pese a emplear una antena de 5.2 dBi de ganancia. Elaborar un Site Survey a 54 Mbps implica elevar la cantidad de puntos de acceso.

- **MAXIMIZAR VELOCIDAD**

Al establecer un limitante en cuanto a velocidad de acceso a 54 Mbps, se pudo apreciar la red inalámbrica a muy alto desempeño y un costo elevado, esto no fue una solución económica válida ya que el establecer 19 APs elevaría demasiado el

costo del proyecto. Por este motivo se planteó una solución con velocidad negociable.

- **COMPROMISO VELOCIDAD, COBERTURA**

Como se pudo observar, al realizar el *Site Survey* a una velocidad de 54 Mbps el rango del área de cobertura disminuye dramáticamente lo cual implicó el uso de más puntos de acceso, se pudo verificar el alcance real del Diseño de la Red Inalámbrica a 54Mbps.

- **LIMITACIÓN DE ANTENAS**

El principal limitante en el establecimiento de las pruebas de campo son las antenas disponibles para la visita en el sitio y la elaboración del *Site Survey*. En la elaboración del *Site Survey* se escogió un tipo de antena omnidireccional de ganancia 5.2 dBi, lo cual proporciona una propagación en el plano horizontal excelente pero ofrece un menor radio de propagación en el plano vertical.

- **COMPARACION A UN DISEÑO DE CABLEADO ESTRUCTURADO**

El costo por punto de cableado estructurado está alrededor de 80 USD, en categoría 5e, y alrededor de 90 USD en categoría 6, al tener alrededor de 200 puntos considerando reservas y un sobre dimensionamiento, el costo de todos los puntos estará alrededor de 16000 USD.

El costo por racks, *patchpanels, patchcords*, organizadores, *faceplates*, bobinas, accesorios, ascendería a unos 3000 USD.

Una consideración importante aunque se encuentra fuera del diseño de sistema de cableado estructurado es que si se instalara el cableado estructurado se requiere *sustituir* hubs, y ciertos switchs por la nueva distribución.

Para tener una administración como la que se obtiene del diseño inalámbrico se requiere hacer una comparación entre switches administrables.

Todo lo anterior elevaría el costo de la red cableada.

Aún así el costo de la red cableada sería menor, mientras que los beneficios de conectividad, flexibilidad, y movilidad que ofrece la red inalámbrica es mucho mayor.

4.2 RECOMENDACIONES

Es importante establecer recomendaciones para trabajos futuros, así tenemos algunas recomendaciones para tener un correcto desempeño en instalaciones de redes inalámbricas.

➢ PATRONES DE RADIACIÓN

El momento de elaborar un *Site Survey*, los patrones de radiación que tienen las antenas son un factor determinante para la ubicación de los puntos de acceso, la correcta ubicación de los mismos es el núcleo del diseño de una red inalámbrica. Para obtener el máximo desempeño de los equipos y de los adaptadores clientes, una correcta selección del tipo de antena es clave.

Como recomendación general para la elaboración del *Site Survey* debemos tener a disposición un juego de antenas omnidireccionales y direccionales de diferentes ganancias para poder establecer características de propagación ángulos de radiación y coberturas a las máximas velocidades.

➢ COMPATIBILIDAD DE EQUIPOS

El momento de efectuar pruebas de campo en el sitio es importante establecer las herramientas necesarias para efectuar el *Site Survey*, en el caso de Cisco la utilidad de ADU (*Aironet Desktop Utility*) es una buena herramienta que facilita la medición técnica del nivel de potencia, fortaleza de la señal, con la finalidad de optimizar instalaciones de redes inalámbricas.

➢ GARANTÍA Y ACTUALIZACIÓN DE MICROCÓDIGOS

Si se tiene como finalidad prestar servicio a redes de tipo empresarial con equipos Cisco Aironet se recomienda la adquisición del contrato de *SMARTNET* ofrecido por Cisco con la finalidad de prolongar por un año la garantía del equipo y tener

actualizado el microcódigo que funciona en el equipo, y poder explotar todas las bondades que tiene el mismo, y características adicionales de seguridad.

- **DISEÑO A VELOCIDAD INFERIOR**

Como se ha podido apreciar el realizar un diseño de alta velocidad 54Mbps implica incrementar el número de puntos de acceso lo cual involucra varios aspectos como son:

- Incremento de materiales, canaletas, mangueras, cable UTP, conectividad en el closet de telecomunicaciones.
- Incremento de costos por configuración de equipos y tarjetas.
- Incremento de costos por equipos inalámbricos, puntos de acceso, antenas.

Por este motivo se vio la necesidad de dar una solución práctica técnico-económica, consiguiendo velocidades de conexión de 1 hasta 54 Mbps.

Esto implica que a estas velocidades se tendrá un mejor rango de cobertura de los equipos, por tanto nuevas ubicaciones de puntos de acceso.
A su vez, implica una reducción en las distancias requeridas y por tanto menor cantidad de corridas, menor cantidad de cable UTP, menor cantidad de material como son canaletas, codos, uniones, *patchcords*, manguera PVC.

- **LUGARES RECOMENDADOS.**

Otra consideración que se debe tener presente es que, al diseñar una red inalámbrica híbrida del tipo Infraestructura se requiere instalación del cable UTP con terminaciones RJ45 para conexión al punto de acceso, esto implica un tendido de cableado horizontal.
En este caso el concepto de red inalámbrica no es total, por este motivo una recomendación en cuanto a lugares para instalar redes inalámbricas es a nivel metropolitano MAN ya que es bueno tener una red MAN a velocidades de hasta 54 Mbps, actualmente aplicaciones empresariales funcionan a velocidades de 1, 2

Mbps hasta 12Mbps en redes MAN e incluso inferiores, por ejemplo *Frame Relay* está en el orden de los kilobits por segundo.

Otro lugar en el cual es recomendable emplear un tipo de red inalámbrica de hasta 54 Mbps es en campus, exterior a oficinas cerradas, ya que como se pudo notar del *Site Survey*, la limitación de señal radicó en paredes normales de bloque, la obstrucción fue determinante a 54 Mbps. El uso de red en el campus sería conveniente para acceso a clientes móviles desde vehículos los cuales puedan conectarse a través de laptops.

- **VELOCIDAD LIMITADA**

Actualmente si se habla de velocidades, se puede lograr a conseguir velocidades superiores a los 54 Mbps, como por ejemplo existen puntos de acceso que nos ofrecen hasta 108 Mbps, con lo cual lograríamos una velocidad igual a la de FastEthernet con cable UTP, sin embargo estos puntos de acceso se encuentran limitados a su fabricante ya que no cumple con estándares como son IEEE 802.11g, o con IEEE 802.11a, y por tanto pierden compatibilidad con productos de otros fabricantes. Por este motivo si se habla de estándares se concluye que el cable UTP ofrece mayores velocidades, actualmente se consiguen velocidades de 1000 Mbps, en redes Gigabit Ethernet. Pero existen otras ventajas en redes inalámbricas como las que ya se han mencionado, movilidad, flexibilidad, rapidez de crecimiento.

- **ADMINISTRACIÓN DE LA RED INALÁMBRICA**

En el presente proyecto se procedió al diseño, pruebas de campo de toda la infraestructura, es importante incluir al proyecto aspectos de administración de la red inalámbrica tales como software administrador que nos permita verificar el correcto funcionamiento de los puntos de acceso.

Por este motivo y por la ayuda que brinda al administrador de la red tener un software administrador se pueden obtener diferentes productos por ejemplo el *Megavision* el cual se indica en la figura 4.1, el cual nos ayuda en tareas de supervisión y gestión, verificar por ejemplo si se encuentran activos puntos de

acceso, configuración de los mismos mediante acceso telnet, verificación de direcciones IP, realizar un *Autodiscovery* automático de la red, entre otros.

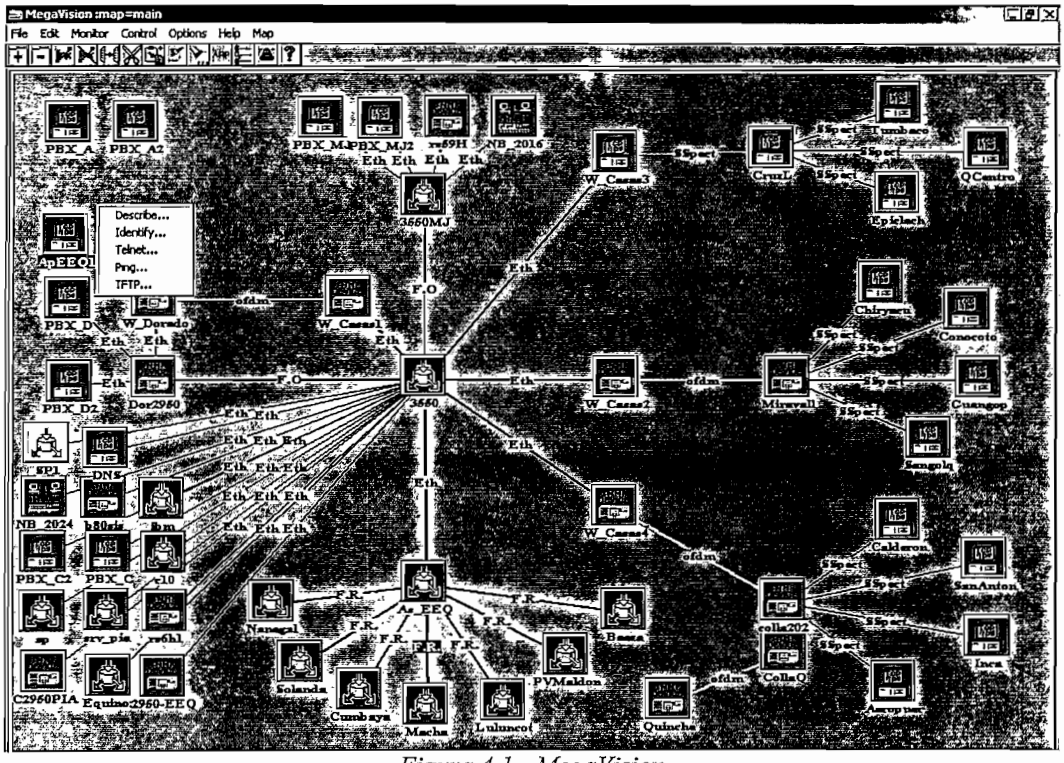


Figura 4.1.- MegaVision

Existe variedad de software como el Software *What'sUp, Cisco View*, de la gama de cisco tenemos *Cisco Wireless Management Suite, Cisco Works*, entre otros.

REFERENCIAS BIBLIOGRÁFICAS

[1] Diseño de una red inalámbrica para la ex facultad de Ingeniería Eléctrica Chamorro Arias, Julio César

[2] Estándar IEEE 802.11. Edición 1999.
Wireless LAN medium access control (MAC) and physical layer (PHY) specifications.

[3] Apuntes de Clase, Ing. Pablo Hidalgo.

[4] Wireless LAN Association, High-Speed Wireless LAN Options 802.11a and 802.11g, http://www.wlana.org

[5] INSUASTI Jorge., Diseño e implementación de dos soluciones de seguridad para una red inalámbrica, Noviembre 2004

[6] Estándar IEEE 802.11b, Septiembre de 1999
Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.
Higher-Speed Physical Layer Extension in the 2.4 GHz Band.

[7] Estándar IEEE 802.11a, Septiembre de 1999.
Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.
High-speed Physical Layer in the 5 GHz Band

[8] Estándar IEEE 802.11g, Junio de 2003
Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.
Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band.

[9] Tom Karygiannis, Les Owens, Instituto Nacional de Estándares y Tecnología, NIST, Wireless Network Security 802.11, Bluetooth and *Handheld* Devices.

[10] Cisco Wireless LAN Course, Copyright @ 2001, Cisco Systems, Inc. Wireless LANs.

[11] Cisco Aironet Antennas And Accessories, Copyright © 2004, Cisco Systems, Reference Guide.

[12] Wikipedia, Enciclopedia libre, wikipedia.org.
http://es.wikipedia.org/wiki/WLAN

[13] CWNA Study Guide © Copyright 2002 Planet3 Wireless, Inc. Capítulo 7. Arquitectura de la red 802.11.

ABREVIACIONES Y ACRÓNIMOS

AAA	Autenticación, autorización y seguimiento (*authentication, authorization, accounting)*
ADU	Utilidad del cliente Cisco (*Aironet Desktop Utility*)
ALB	Balanceo automático de carga (*Automatic Load Balancing*)
AES	Estándar de Encripción avanzada (*Advanced Encription Standard*)
AP	Punto de Acceso (*Access Point*)
BSA	Area básica de servicios (*Basic Service Area*)
BSS	Conjunto básico de servicios (*Basic Service Set*)
BPSK	Modulación de fase con dos estados
CCK	Modulación de códigos complementarios *(Complementary Code Keying)*
CRC	Códigos de redundancia cíclica
DQPSK	Modulación de fase en cuadratura diferencial (*Differential Quadrature Phase Shift Keying)*
DS	Sistema de Distribución (*Distribution System*)
DCF	Función de coordinación distribuida
DSSS	Modulación de espectro disperso en secuencia directa (*Direct Sequence Spread Spectrum*)
EAP	Protocolo de autenticación extendida (*Extensible authentication Protocol*)
ERP	Capa física de velocidad extendida *(Extended Rate Physical)*
FHSS	Modulación de espectro disperso en salto de frecuencia
IBSS	Conjunto básico de servicios independiente *(Independent Basic Service Set)*
IETF	Grupo de Ingenieros para estandarización de protocolos en Internet *(Internet Engenniering Task Force)*
IR PHY	Capa física de infrarrojos *(Infrared PHysical)*
IP	Protocolo Internet *(Internet Protocol)*
LEAP	Protocolo de autenticación extendida liviana *(Light EAP)*
MAC	Control de acceso al medio (*Medium Access Control*)

OFDM	Modulación por muliplexación de frecuencias ortogonales *(Orthogonal Frecuency Division Multiplexing)*
PCF	Función de coordinación puntual
PDU	Protocolo de unidad de datos (*Protocol Data Units)*
PLCP	Procedimiento de Convergencia de Capa Física (*Physical Layer Convergence Procedure*)
PHY	Capa física (*PHYsical Layer*)
PMD	Capa dependiente de medio físico (PHYsical Medium Dependent)
PoE	Energia a través de Ethernet (*Power over Ethernet*)
QPSK	Modulación de fase en cuadratura
SSID	Conjunto identificador del servicio
TKIP	Protocolo de integridad con clave temporal (*Temporal Key Integrity Protocol)*
VPN	Red privada virtual (*Virtual Private Network*)
WEP	Protocolo equivalente al alámbrico (wired equivalency protocol).
WI-FI	Fidelidad Inalámbrica (*Wireless Fidelity*)
WPA	Protocolo de acceso inalámbrico (*Wi-Fi Protected Access*)

ENLACES:

http://standards.ieee.org/getieee802/802.11.html

http://web.syr.edu/~nshenvi/802.11g.txt

http://www.sss-mag.com/pdf/802_11g_whitepaper.pdf

http://www.wi-fiplanet.com/columns/article.php/1472641

http://www.xs4all.nl/~jrme/cck.html

http://www.securitywireless.info/default.asp

http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_data_sheet09186a00801ebc33.html

http://www.funk.com/RegFiles/ody30conf.asp (servidor odyssey)

http://www.cisco.com/en/US/products/hw/wireless/ps469/products_data_sheets_list.html (antenas)

Anexo 1
Codificación en CCK

ANEXO 1 CODIFICACIÓN EN CCK

Para el tipo de modulación CCK la longitud de los códigos es 8 y se basa en códigos complementarios.

La formula1 es usada para derivar de ella las palabras código CCK que permitan lograr las velocidades de 5.5 Mbps y 11 Mbps.

formula1.- Formación de palabras código.

$$C = \{ e^{j(\varphi1+\varphi2+\varphi3+\varphi4)},\ e^{j(\varphi1+\varphi3+\varphi4)},\ e^{j(\varphi1+\varphi2+\varphi4)},\ -e^{j(\varphi1+\varphi4)},\ e^{j(\varphi1+\varphi2+\varphi3)},\ e^{j(\varphi1+\varphi3)},\ -e^{j(\varphi1+\varphi2)},\ e^{j\varphi1} \}$$

donde C es la palabra código

C = {c0,c1,..., c7}

Esta formula crea 8 complejos (c0 a c7), donde c0 se transmite primero.

Para alcanzar 5.5 Mbps, se transmiten 4 bits por símbolo [d0,d1,d2,d3].

Los bits d0 y d1 se codifican en DQPSK. El codificador DQPSK es especificado en la Tabla A1.1.

Tabla A1.1.- Codificación de DQPSK

(d0,d1) (d0 se transmite primero)	Fase (+jw)	Cambio de fase(+jω)
00	0	π
01	π/2	3π/2(-π/2)
11	π	0
10	3π/2 (–π/2)	π/2

Los bits d2 y d3 CCK son especificados en la Tabla A1.2.

Tabla A1.2.- Codificación CCK/5.5 Mbps.

d2,d3	C0	C1	C2	c3	c4	c5	c6	C7
00	1j	1	1j	-1	1j	1	-1j	1
01	-1j	-1	-1j	1	1j	1	-1j	1
10	-1j	1	-1j	-1	-1j	1	1j	1
11	1j	-1	1j	1	-1j	1	1j	1

Esta tabla se deriva de la formula1 arriba y estableciendo $\varphi 2=(d2x\pi) + \pi/2$, $\varphi 3=0$ y $\varphi 4= d3x\pi$. En la tabla, d2 y d3 se muestran en ese orden y los complejos son mostrados desde c1 a c8, donde c1 es transmitido primero.

Para alcanzar 11Mbps en CCK se procede de manera similar que a 5.5Mbps con la diferencia que se codifican 8bits por símbolo (d0 a d7), empleando DQPSK

Los primeros dibits (d0, d1) codifican $\varphi 1$ basándose en DQPSK.

Los siguientes dibits (d2, d3), (d4, d5), y (d6, d7) codifican $\varphi 2$, $\varphi 3$, y $\varphi 4$, respectivamente, basándose en QPSK.

Tabla A1.3.- Codificación QPSK

(di,di+1) **(di se transmite primero)**	**fase**
00	0
01	$\pi/2$
11	π
10	$3\pi/2$ ($-\pi/2$)

Los 11 chips de la secuencia de Barker del estándar lleva un símbolo a un reloj de 1MHz, lo que resulta una velocidad de señal de 1Msímbolo/sec.

La secuencia de 8 chips en CCK a un reloj de 1MHz, resulta en una velocidad de señal de 1.375Msímbol/sec (11/8)

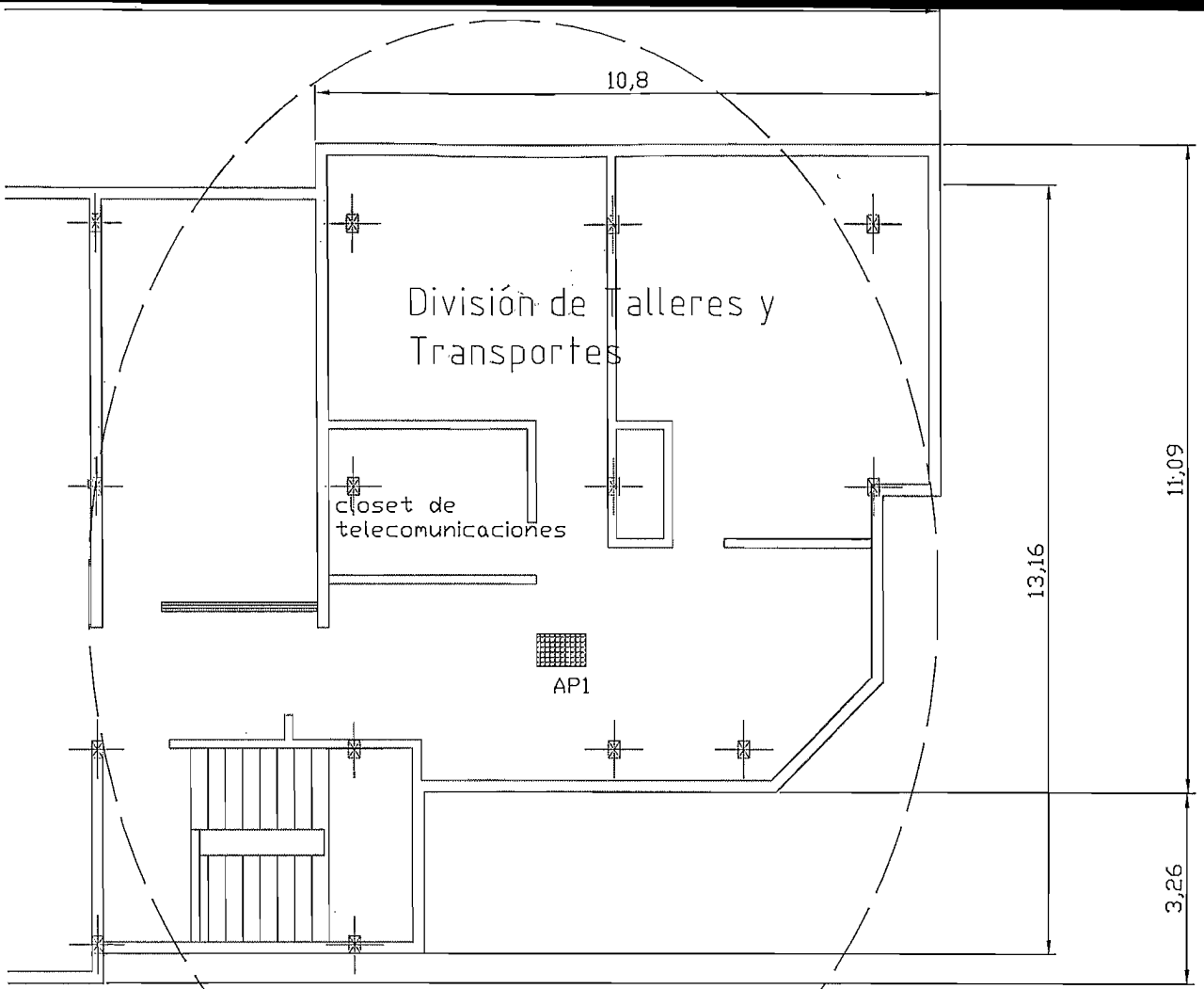
A velocidad = media, 4 bits por símbolo , resulta 5.5Mbps

Velocidad = 4 bits/simbolo * 1.375 MSps = 5.5 Mbps

A velocidad = alta, 8 bits por símbolo , resulta 11Mbps

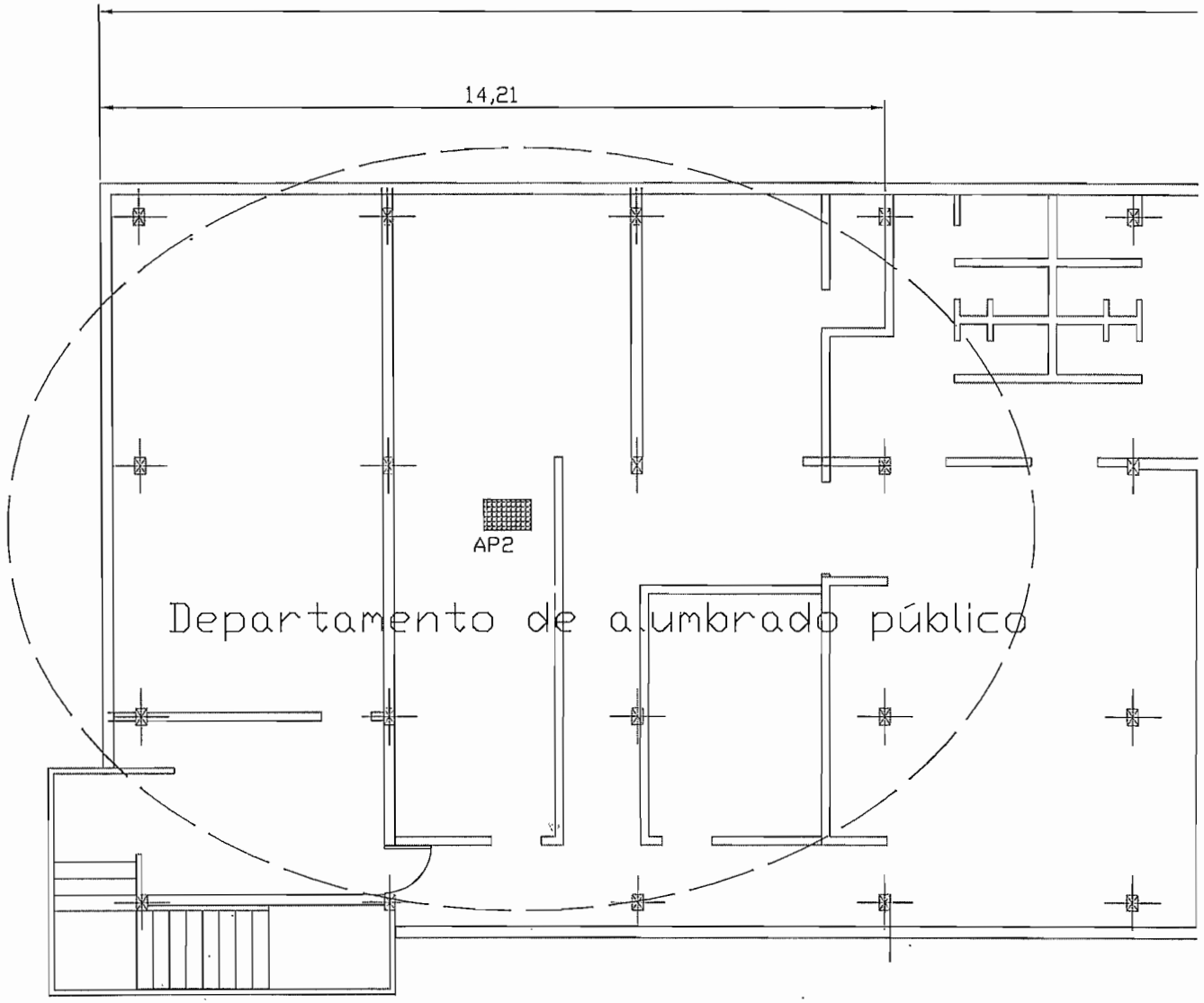
Velocidad = 8 bits/simbolo * 1.375 MSps = 11 Mbps

Anexo 2
Planos Arquitectónicos Diseño



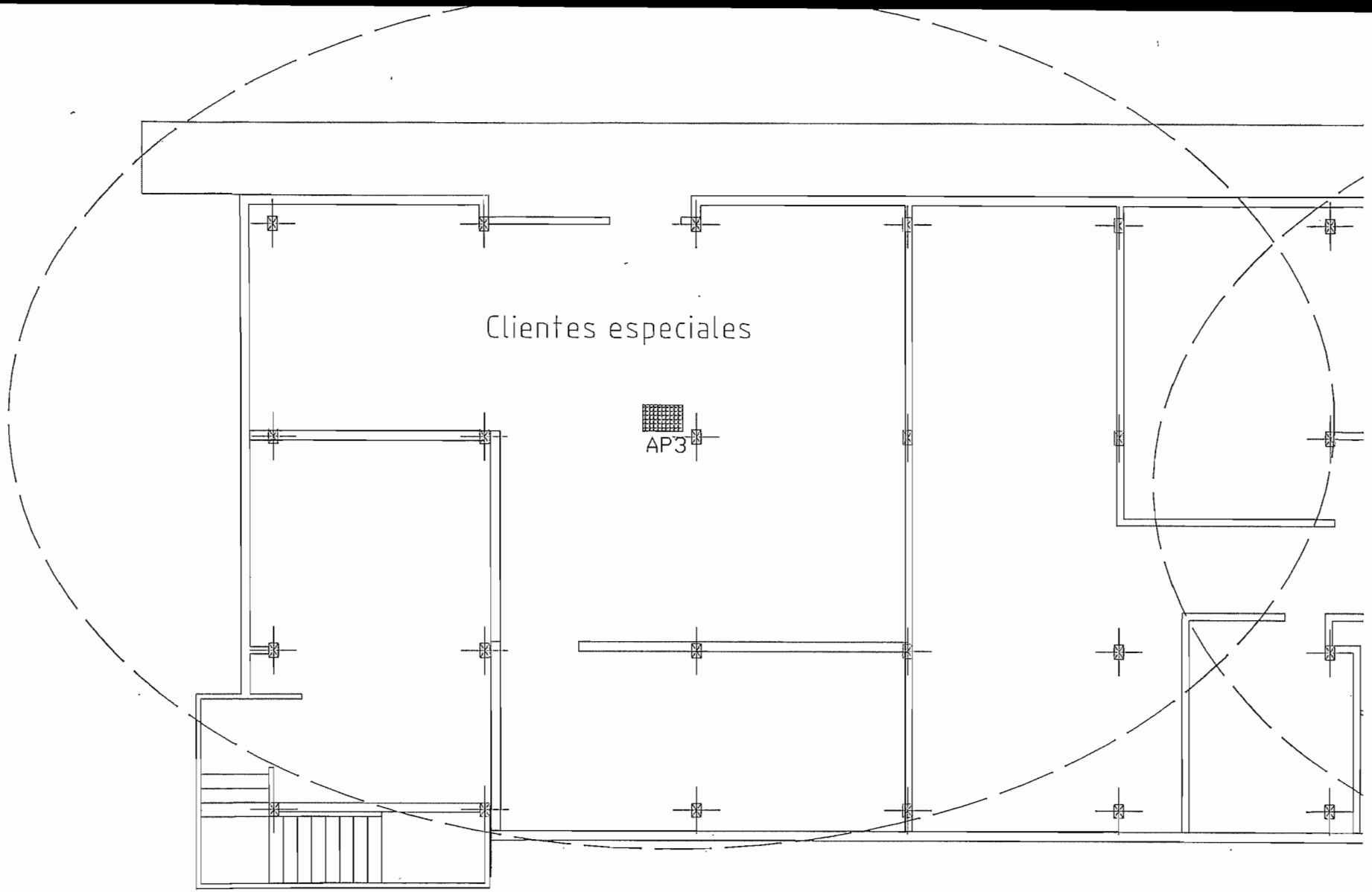
Edificio Polifuncional

tercer piso



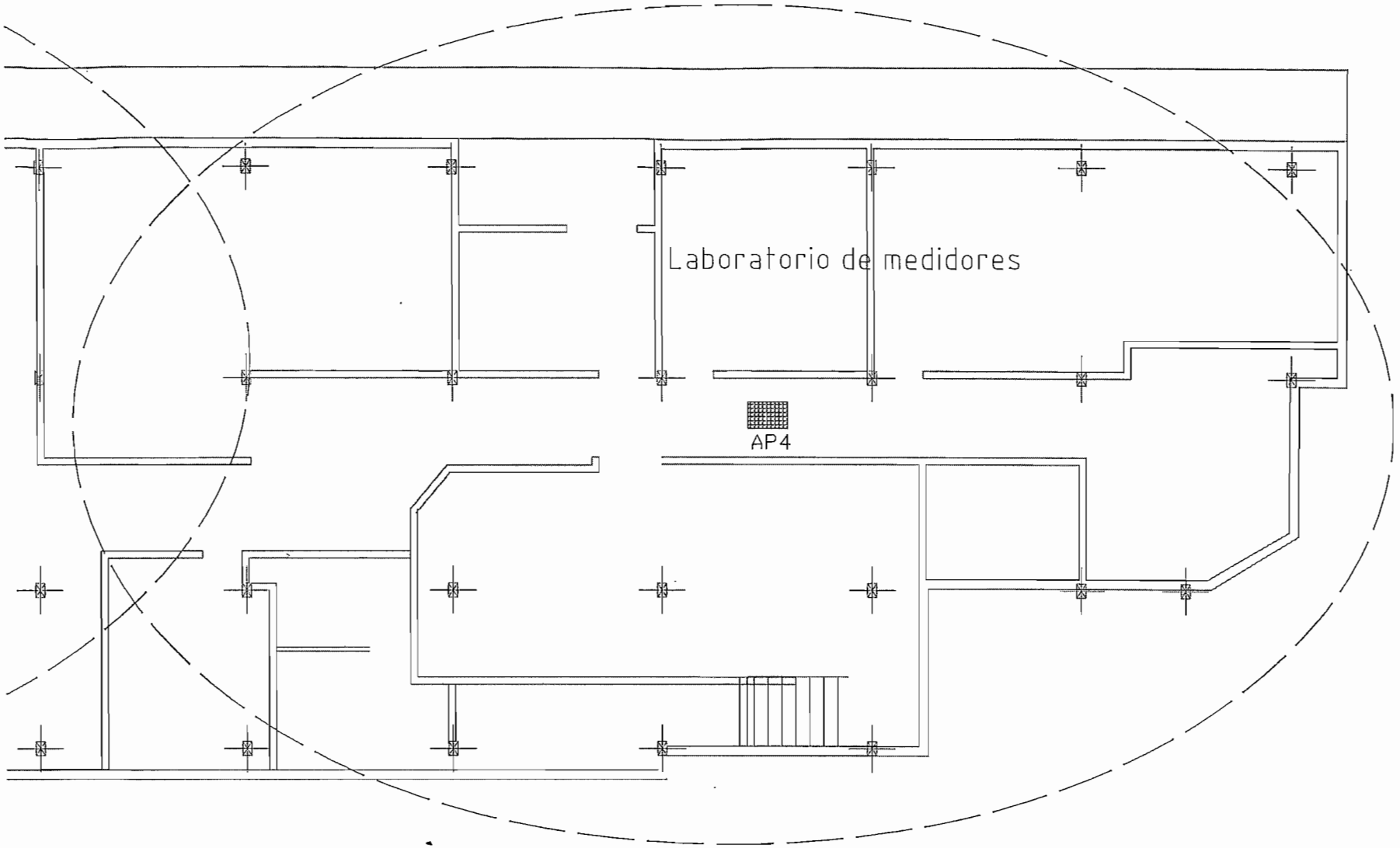
Edificio Polifuncional

tercer piso



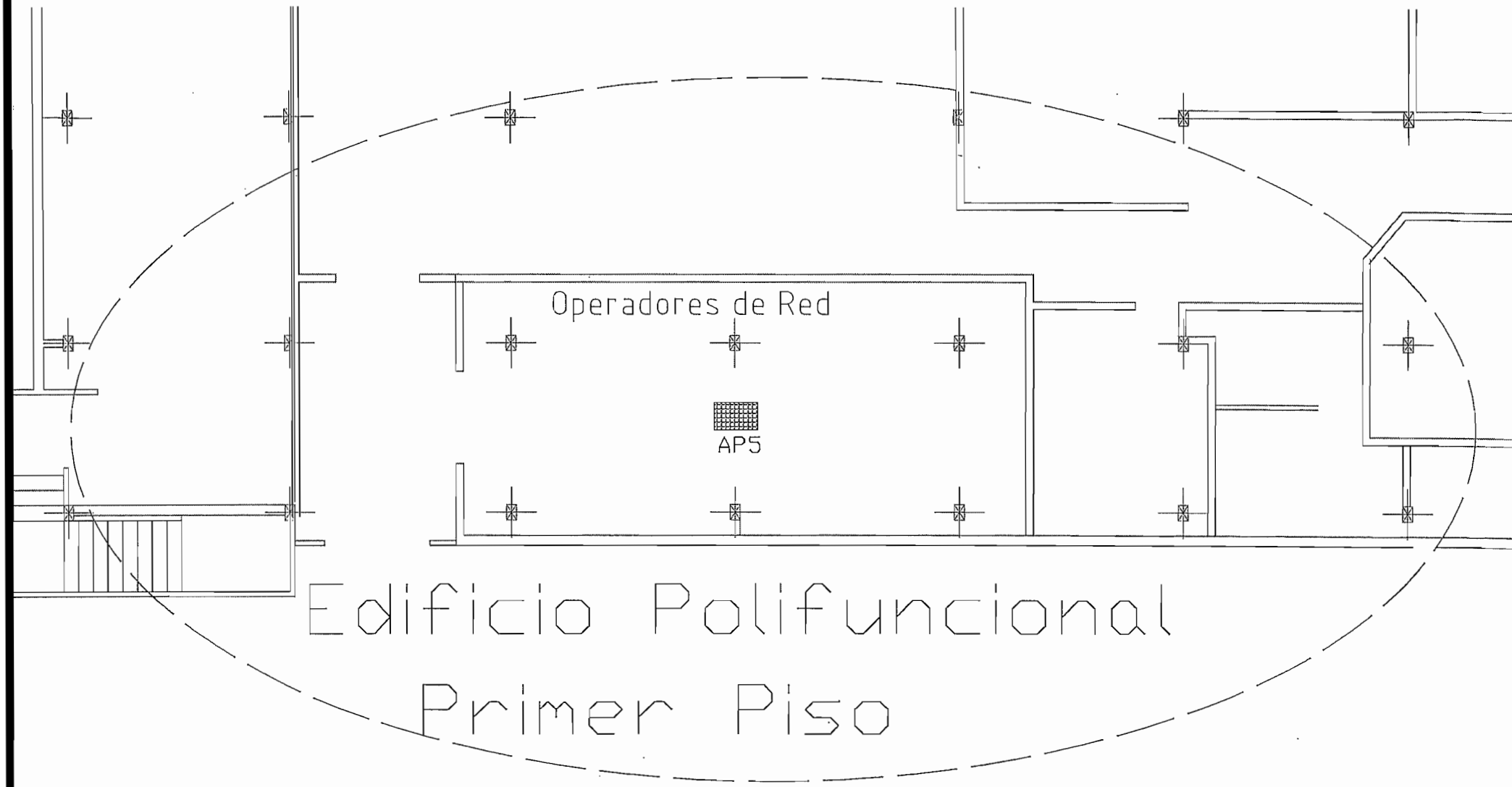
Edificio Polifuncional

Planta Baja



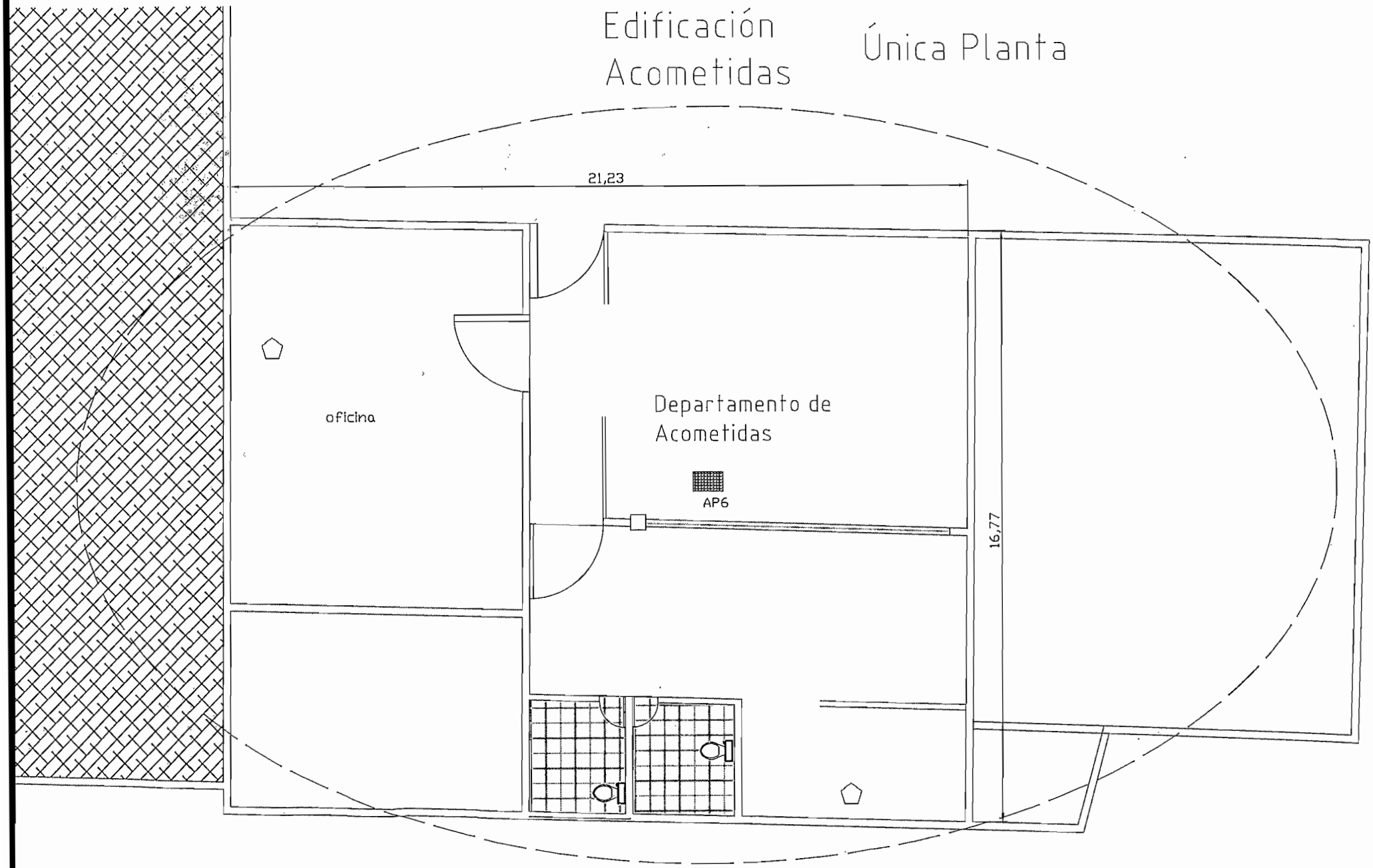
Edificio Polifuncional

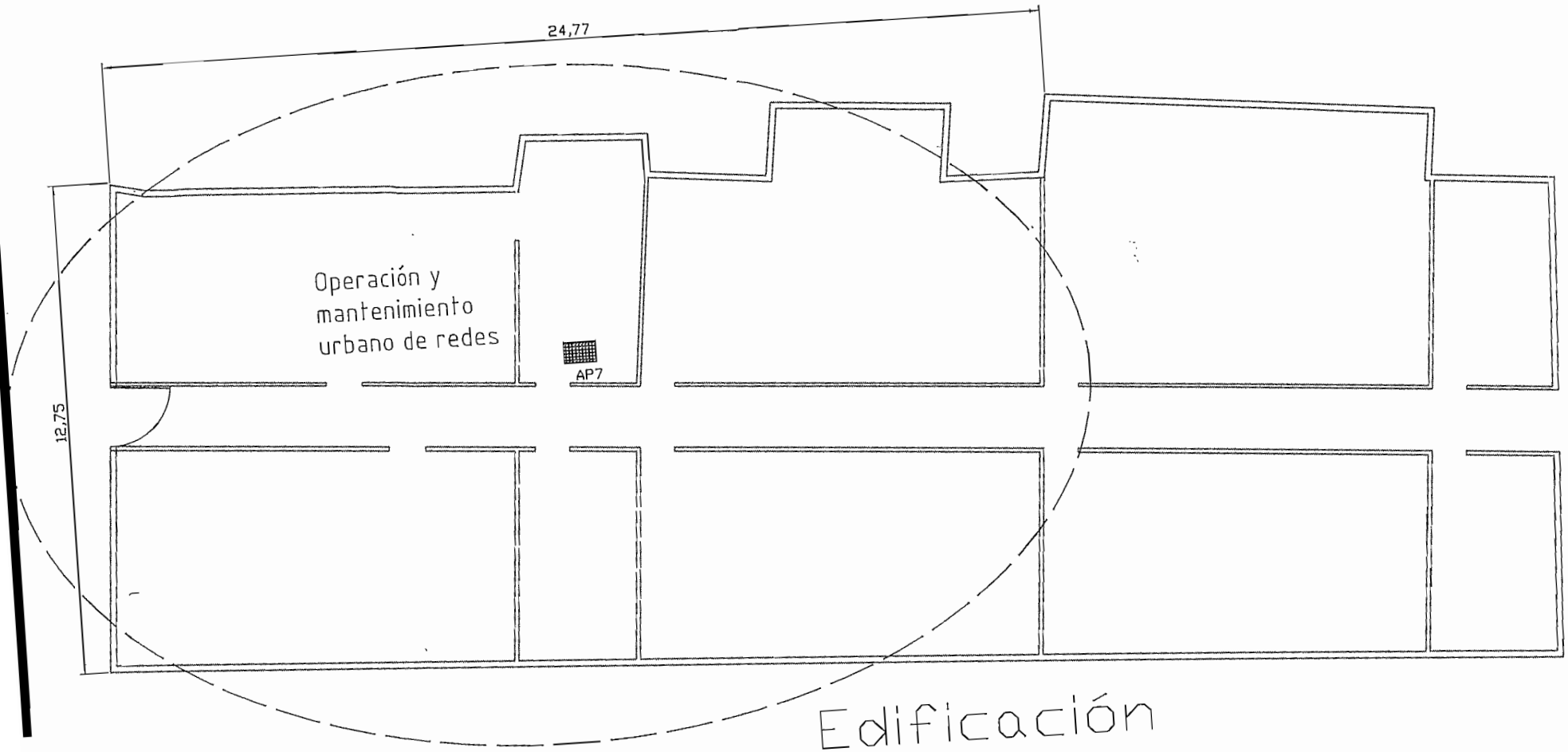
Planta Baja



Edificio Polifuncional

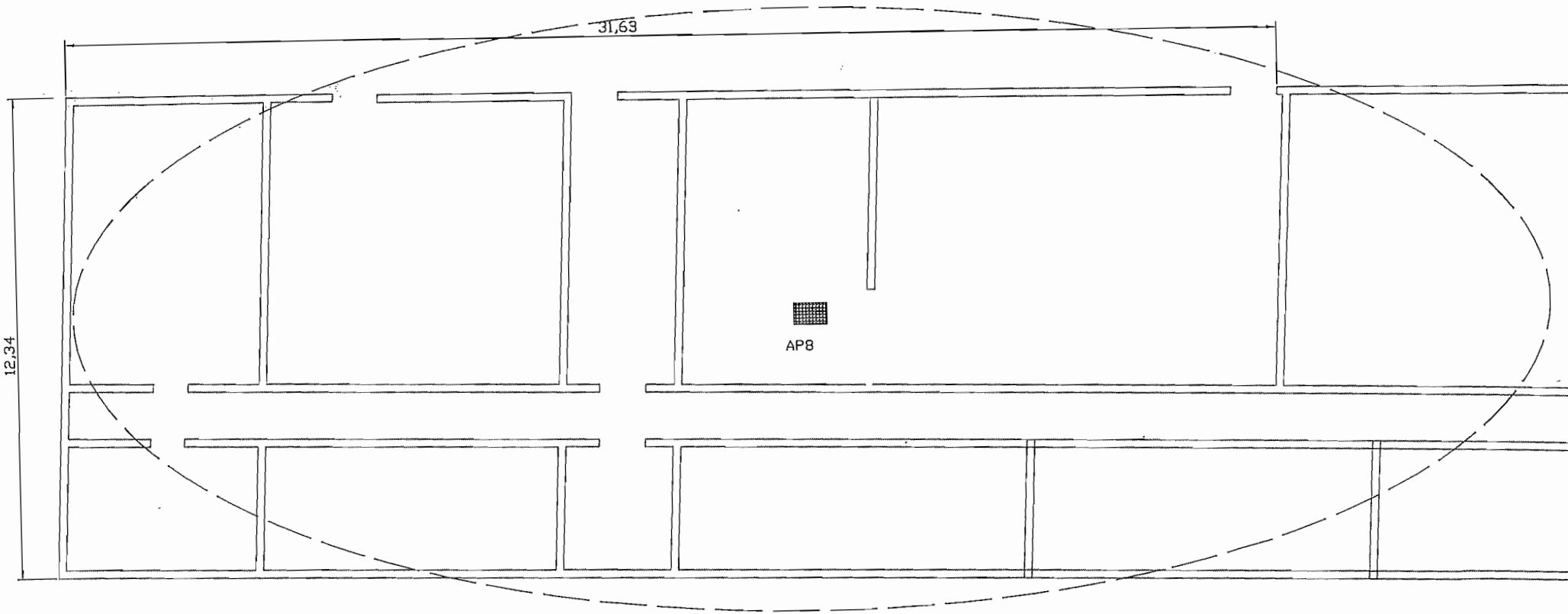
Primer Piso


Edificación
Acometidas
Única Planta
21,23
oficina
Departamento de
Acometidas
AP6
16,77



Edificación

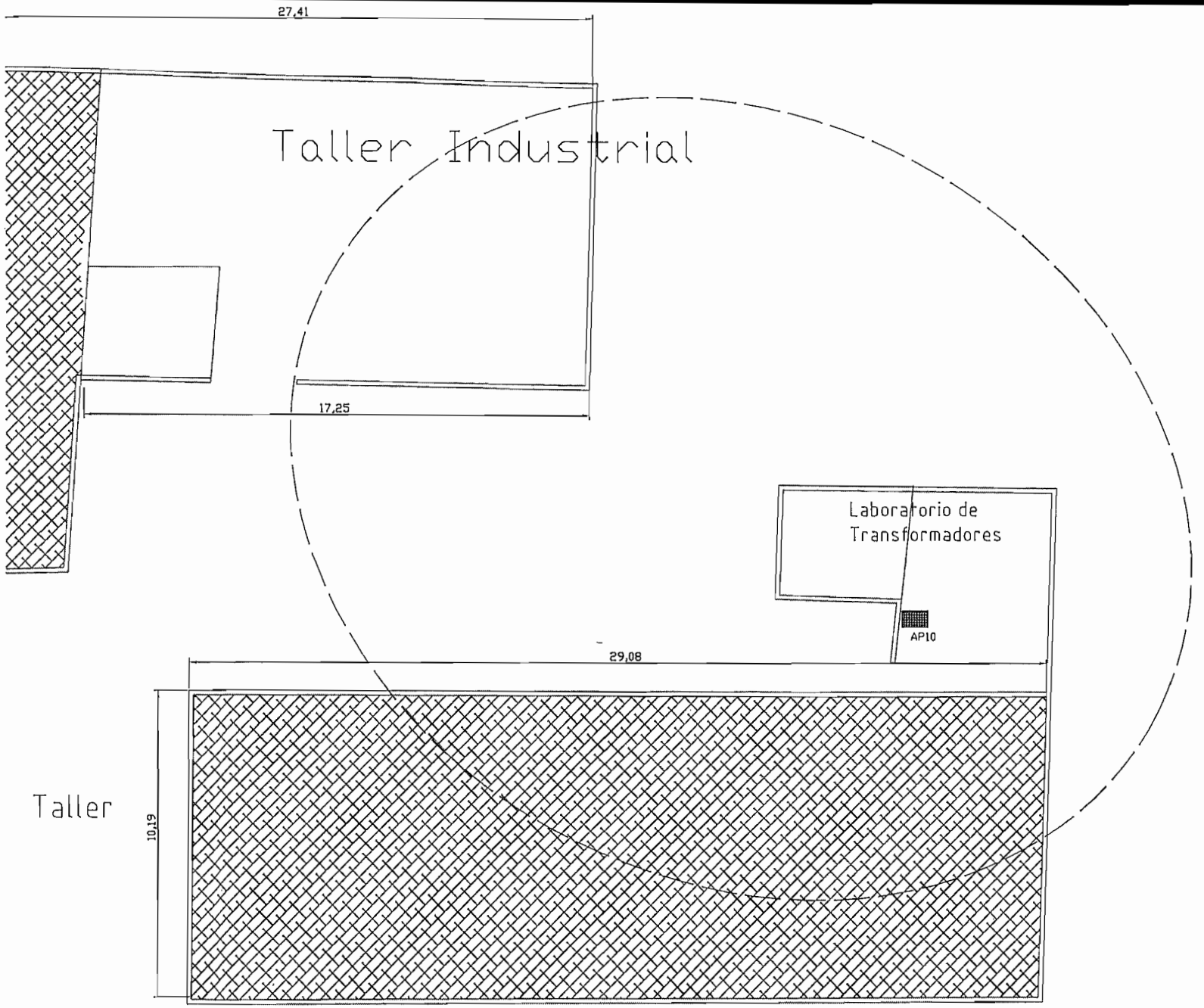
Operación y Mantenimiento Urbano



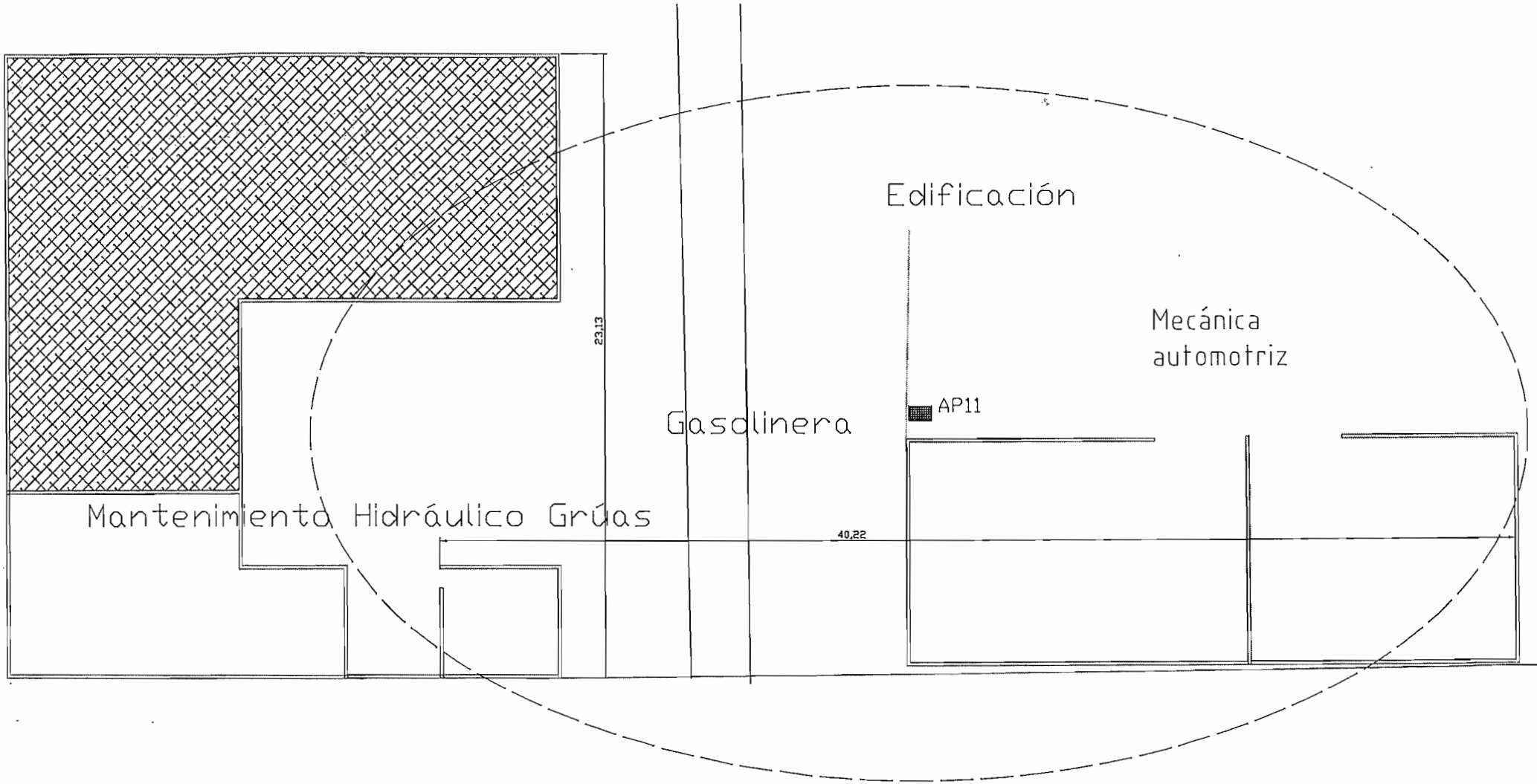
Edificación

Construcción de Redes


12,92
14,43
AP9
Departamento de
Personal
Única Planta



Laboratorio de transformadores


Edificación
Mecánica
automotriz
AP11
Gasolinera
Mantenimiento Hidráulico Grúas
23,13
40,22

Anexo 3
Configuraciones de Seguridad

ANEXO 3 CONFIGURACIÓN DE SEGURIDADES

A3.1 CONFIGURACIÓN DEL PUNTO DE ACCESO.

Se tienen opciones de seguridad que sirven como mecanismos adicionales para garantizar un nivel de seguridad, y minimizar vulnerabilidades, como por ejemplo, restringir el acceso al punto de acceso solo para el administrador, eliminación del broadcast de SSID, filtrado MAC, cifrado WEP, Servidor de Autenticación RADIUS. Estas configuraciones se presentan a continuación.

A3.1.1 CONFIGURACIÓN DEL SSID DE LA RED

Se establece la configuración ingresando a *Security -> SSIDs Manager* del menú principal, con lo que aparece la pantalla de la figura A.1, aquí se ingresa

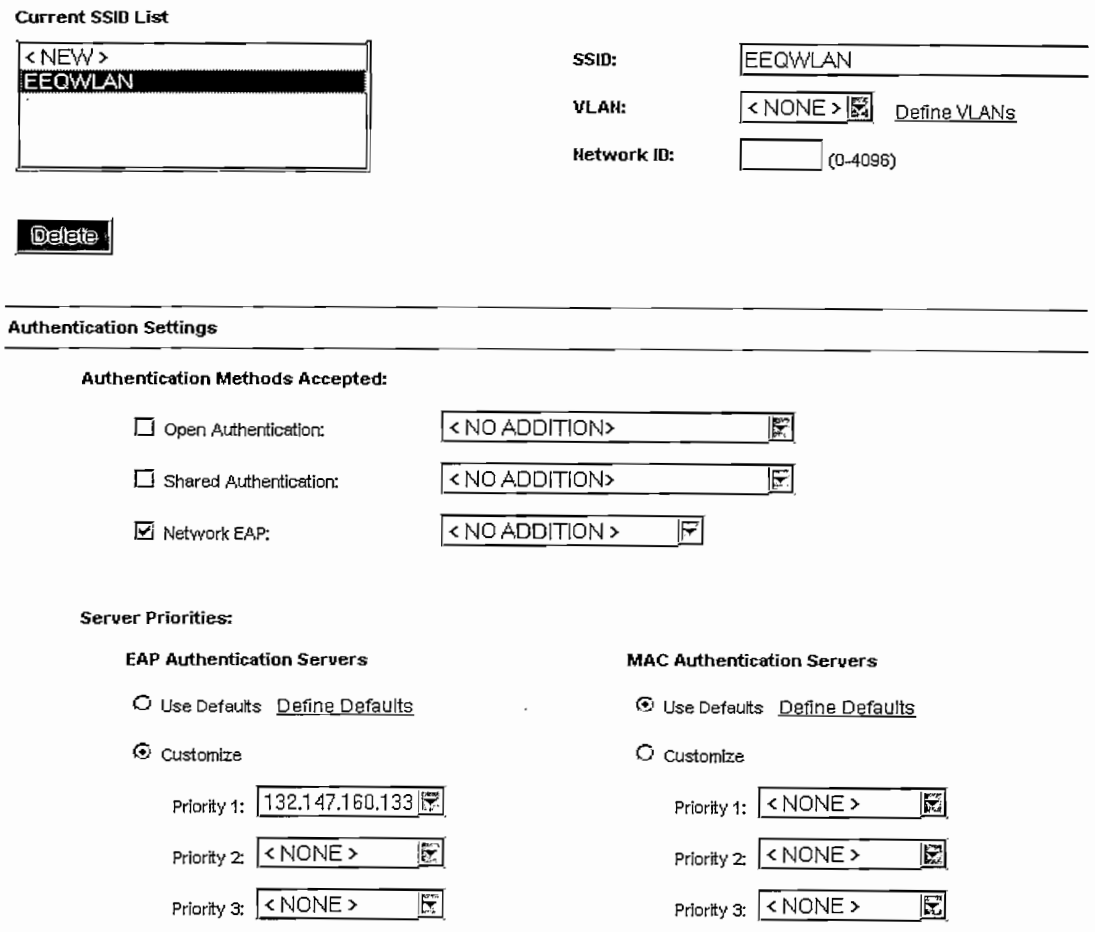


Figura A.1.- Configuración Express Security->SSIDs Manager

el *SSID* con el valor escogido EEQWLAN, como medidas de precaución se deshabilita el envío del SSID en Broadcast.

El método de autenticación se establece Network EAP para el uso del servidor Radius. Aplicamos los cambios con Apply.

Podemos observar el resumen acerca del SSID que está siendo utilizado al final de la página de Express Security del menú principal, el cual aparece en la pantalla de la figura A.2.

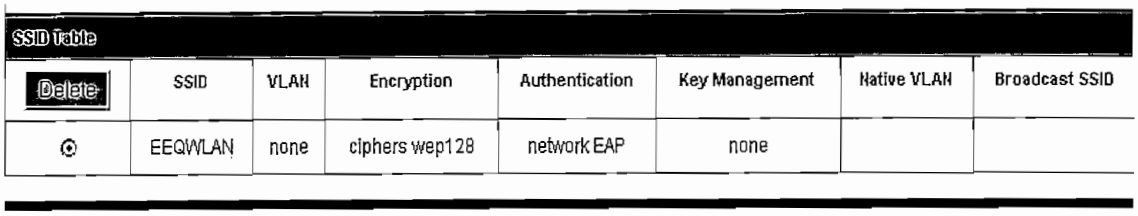


Figura A.2.- Resumen del SSID empleado

Podemos observar que se encuentra deshabilitado el broadcast de SSID.

A3.1.2. IMPLEMENTACIÓN WEP

Se generan 4 claves de 128 bits (26 números hexadecimales) y se los ubica en el campo *Encription Key*, y en los campos *Key Size* escogemos 128 bits.
Las claves usadas en la encripción son las indicadas en la Tabla A1.

Tabla A.1 Claves WEP utilizadas

CLAVE	26 números hexadecimales
Clave 1	A949B43CF54D3EEEFC323A1F6B
Clave 2	B87ADCF89AD5F4C1AAE1F2E3C2
Clave 3	AE45CB7DF5E9B43DEAC276F349
Clave 4	A9FEAC18A4DE3A5CF39E1A3C56

Ingresamos a *Security-> Encription Manager* del menú principal indicado en la pantalla de la figura A.3.

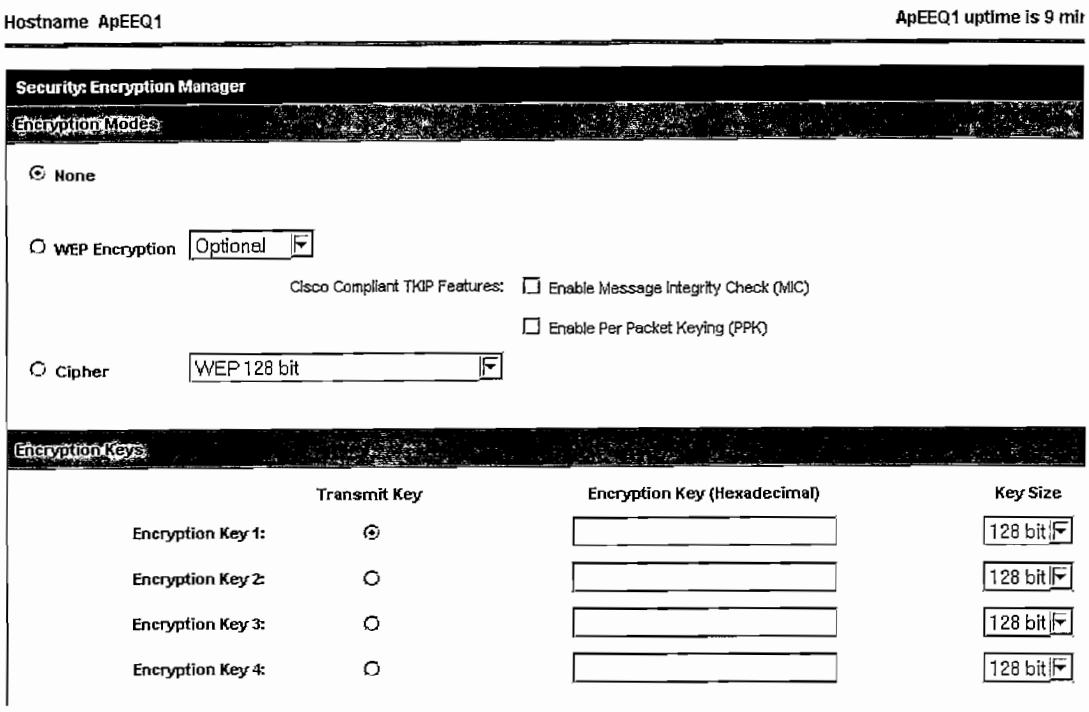


Figura A.3. .- Pantalla Encription Manager

Seleccionamos la opción *Chiper*, con clave WEP de 128 bits. Ingresamos las cuatro llaves WEP, su tamaño *Key Size* y la llave a ser transmitida *Key 1*, como lo indica la figura A.4.

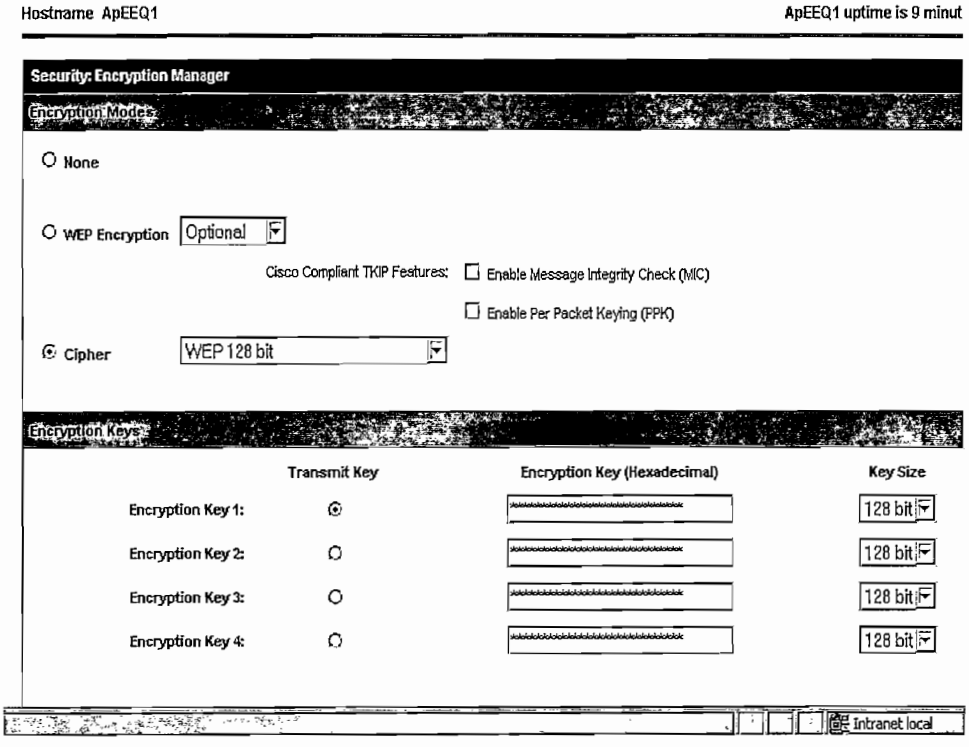


Figura A.4.- Configuración de WEP

Aplicamos los cambios al final de la página, con lo cual se termina la configuración WEP en el punto de acceso.

A3.1.3. ACCESO PARA ADMINISTRADORES DEL AP 1200

Se debe garantizar el acceso exclusivo para administradores y cambiar la configuración por defecto, para realizar esto seleccionamos *Security -> Admin Access*, con lo cual aparece la pantalla de la figura A.5.

Se puede configurar nuevos usuarios o simplemente dejar acceso a un usuario administrador, con su respectivo password, y finalmente aplicar los cambios.

El tipo de autenticación del administrador debe cambiarse de un password global al tipo password individual.

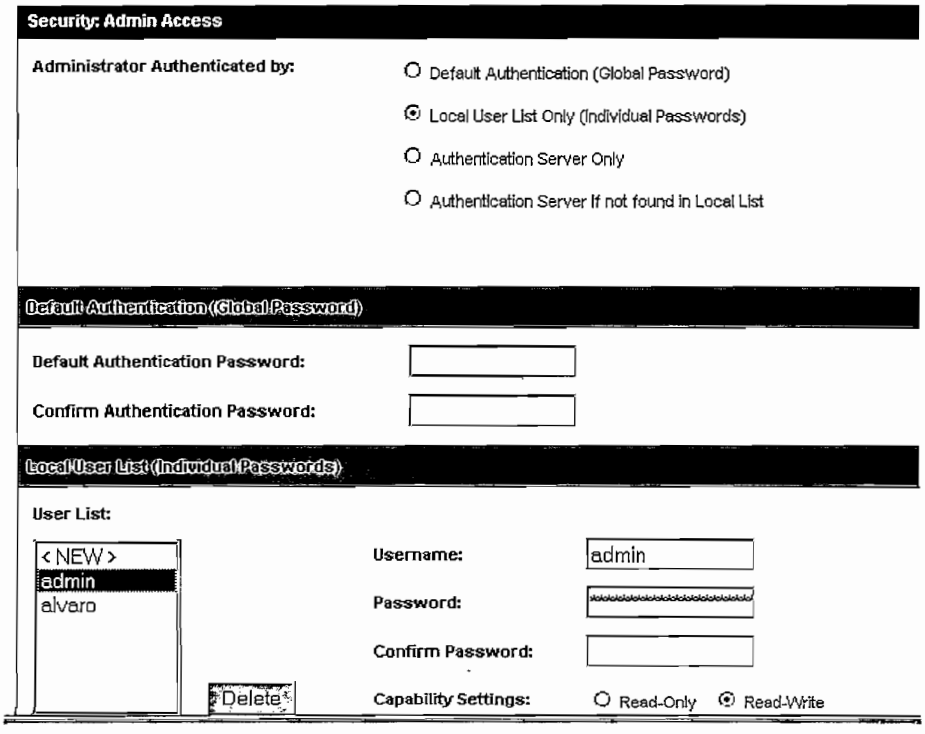


Figura A.5.- Configuración para administradores del punto de acceso

A3.1.4. FILTRADO MAC

EL Filtrado MAC es uno de los servicios que ofrece el punto de acceso. Ingresamos a la opción *Services* del menú principal con lo cual aparece la pantalla de la figura A.6.

Services Summary	
Telnet/SSH: Enabled/Disabled	Hot Standby: Disabled
CDP: Enabled	DNS: Disabled
Filters: Disabled	HTTP: Enabled
QoS: Disabled	SNMP: Disabled
NTP: Disabled	VLAN: Disabled
ARP Caching: Disabled	

Figura A.6.- Servicios del AP1200

Ingresamos a *Filters - > Mac Address Filters* con lo cual nos aparece la pantalla de la figura A.7.

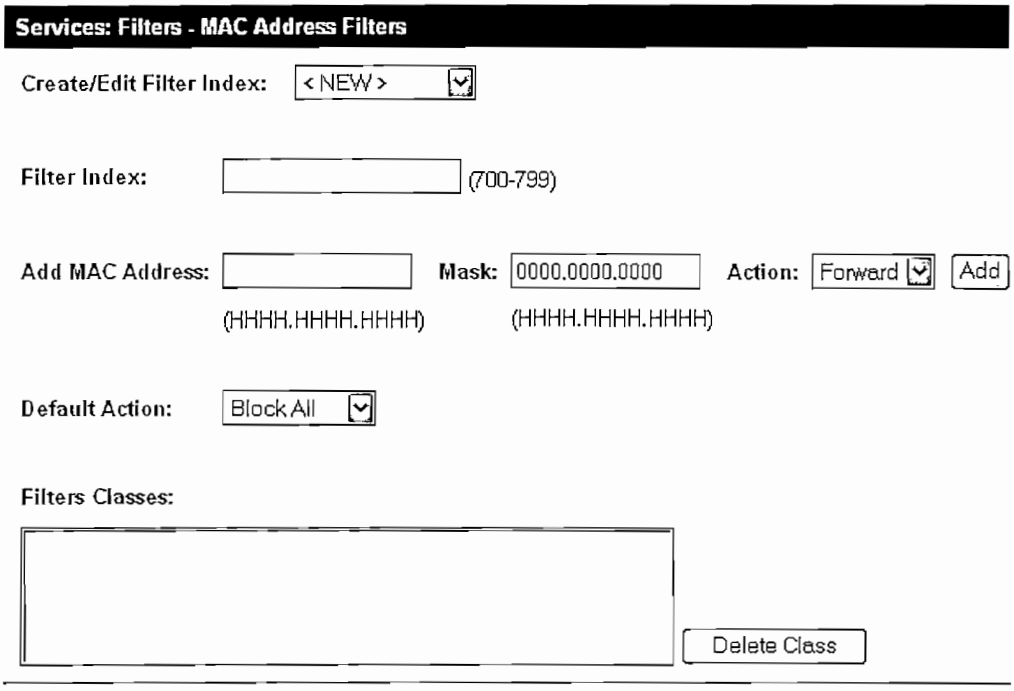


Figura A.7.- Filtros MAC

Al ingresar un nuevo filtro seleccionamos de *Create/Edit Filter Index* la opción <NEW>

En la opción *Filter index* establecemos un índice que identifica de manera única el filtro, los posible valores van desde 700 a 799.

En el campo *Add MAC Address* ingresamos una MAC address, con la opción de permitir o denegar a la dirección MAC 00-40-96-A3-1C-BB que corresponde al cliente inalámbrico.

Luego un clic en *Add* y aplicamos los cambios con *Apply.* Esto se indica en la figura A.8.

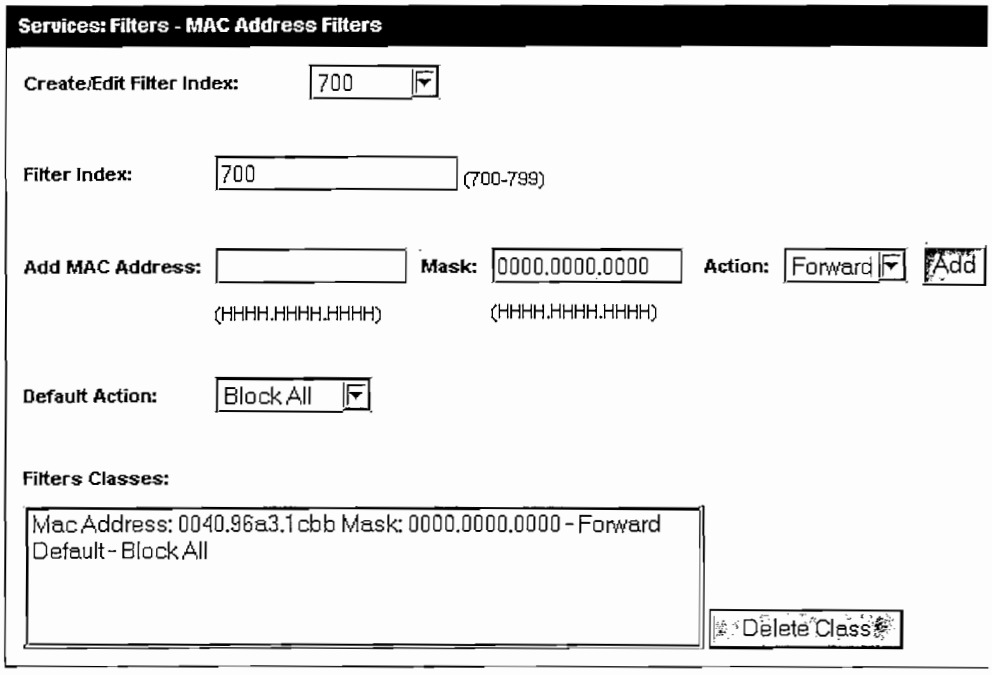


Figura A.8.-Ingreso de la MAC Address

Para aplicar el filtro creado ingresamos a *Services -> Filters -> Apply Filters* y en la parte correspondiente al radio0 802.11g establecemos el filtro MAC 700 en *incoming* siendo esto para el ingreso de paquetes hacia el radio desde el cliente, ya que deseamos garantizar que solamente clientes autorizados a nivel MAC puedan enviar paquetes entrantes al radio y pasarlos a la red cableada, así lo indica la figura A.9

Services: Filters - Apply Filters

	FastEthernet		Radio0-802.11G	
Incoming	MAC	< NONE >	MAC	700
	EtherType	< NONE >	EtherType	< NONE >
	IP	< NONE >	IP	< NONE >
Outgoing	MAC	< NONE >	MAC	< NONE >
	EtherType	< NONE >	EtherType	< NONE >
	IP	< NONE >	IP	< NONE >

Figura A.9.- Filtrado MAC Aplicado

Adicionalmente se requiere asociar esta lista de acceso MAC, para ello ingresamos a Security –> Advanced Security -> Association Access List, y escogemos el índice al cual hace referencia el filtro MAC, como lo indica la figura A.10.

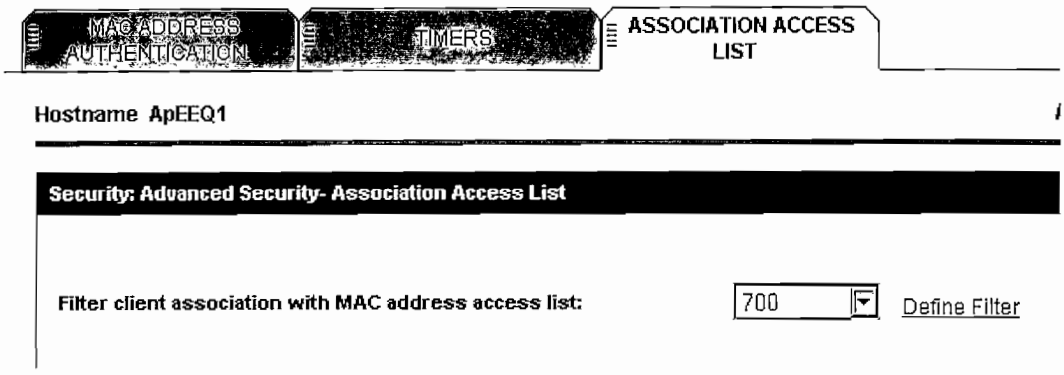


Figura A.10.- Asociación de la Lista de Acceso.

A3.1.5. INHABILITACIÓN DE TELNET

Los servicios de HTTP y Telnet vienen habilitados por defecto en el punto de acceso y podemos observar que el filtrado está habilitado, como lo observamos en la figura A.11.

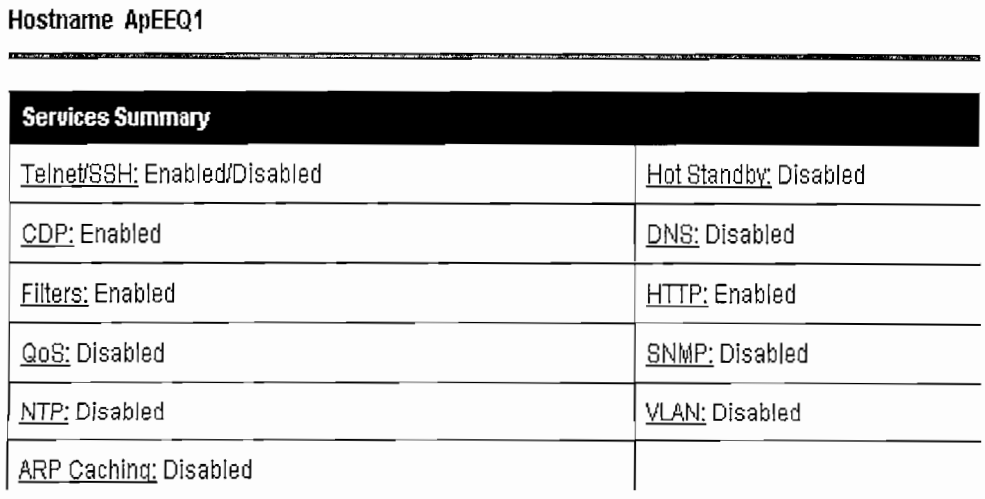


Figura A.11.- Pantalla Services con filtrado habilitado

Para deshabilitar el acceso Telnet ingresamos a *Services -> Telnet* y escogemos la opción *Disable* con lo cual obtenemos la pantalla de la figura A.12, aplicamos los cambios con *Apply*

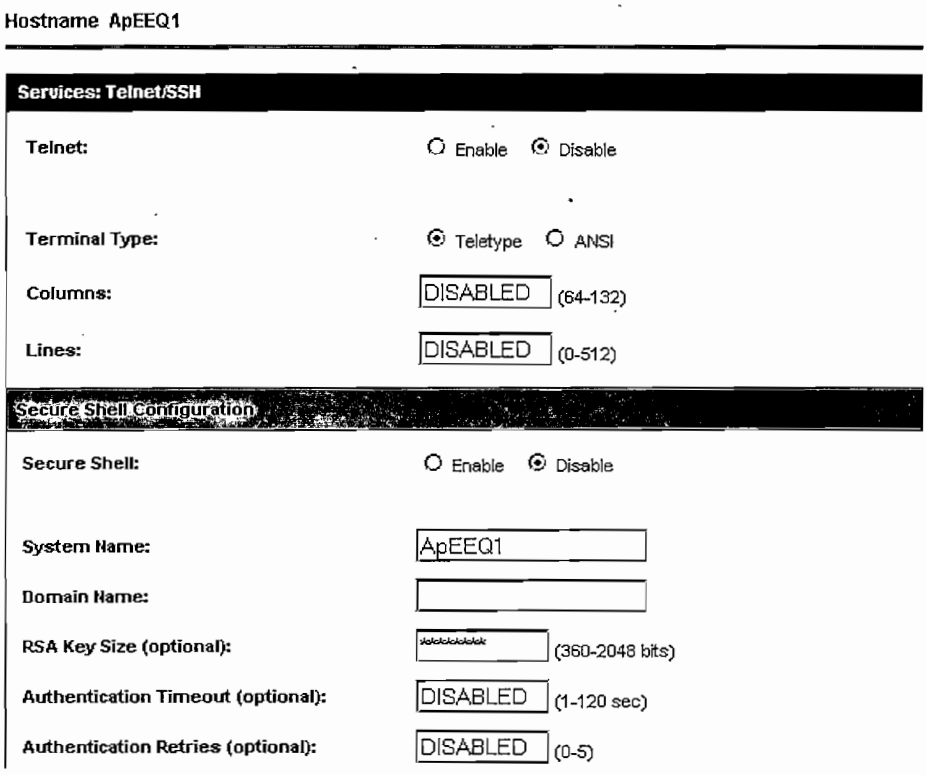


Figura A.12.- Inhabilitación de acceso Telnet

Podemos comprobar los cambios desde el menú *Services*, así estará deshabilitado Telnet, SNMP, y habilitados el acceso mediante HTTP y Filtros como lo indica la figura A.13.

Services Summary	
Telnet/SSH: Disabled/Disabled	Hot Standby: Disabled
CDP: Enabled	DNS: Disabled
Filters: Enabled	HTTP: Enabled
QoS: Disabled	SNMP: Disabled
NTP: Disabled	VLAN: Disabled
ARP Caching: Disabled	

Figura A.13.- Menú Services Configurado

A3.1.6. IMPLEMENTACIÓN DEL SERVIDOR DE AUTENTICACIÓN

Finalmente obtenemos mayor seguridad con la implementación de EAP, en particular con LEAP propietaria de Cisco.

Para configurar el servidor ingresamos a *SECURITY ->Server Manager*, ingresamos la dirección IP del servidor Radius así como el puerto en el cual escuchará el servidor las peticiones de autenticación, así como lo indica la figura A.14.

Establecemos prioridad 1 al servidor EAP de autenticación

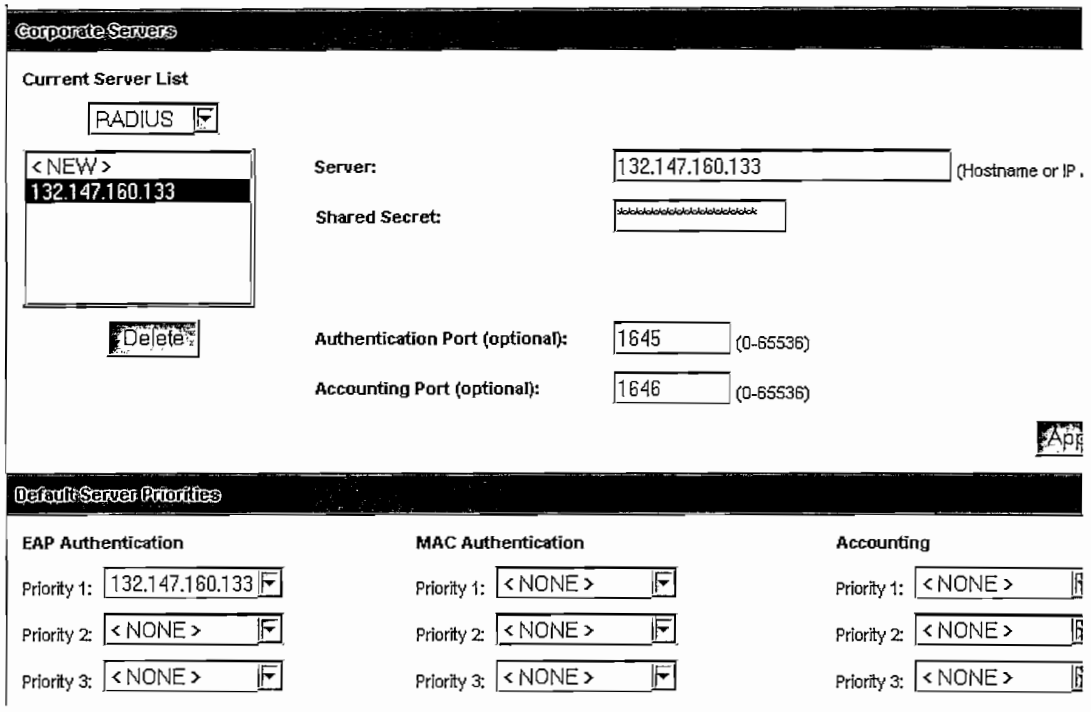


Figura A.14.- Administración del servidor

Es necesario establecer el tipo de autenticación del SSID, para ello ingresamos a SECURITY->SSID Manager y cambiamos el tipo de autenticación de OPEN a Network EAP, como lo indica la figura A.15.-

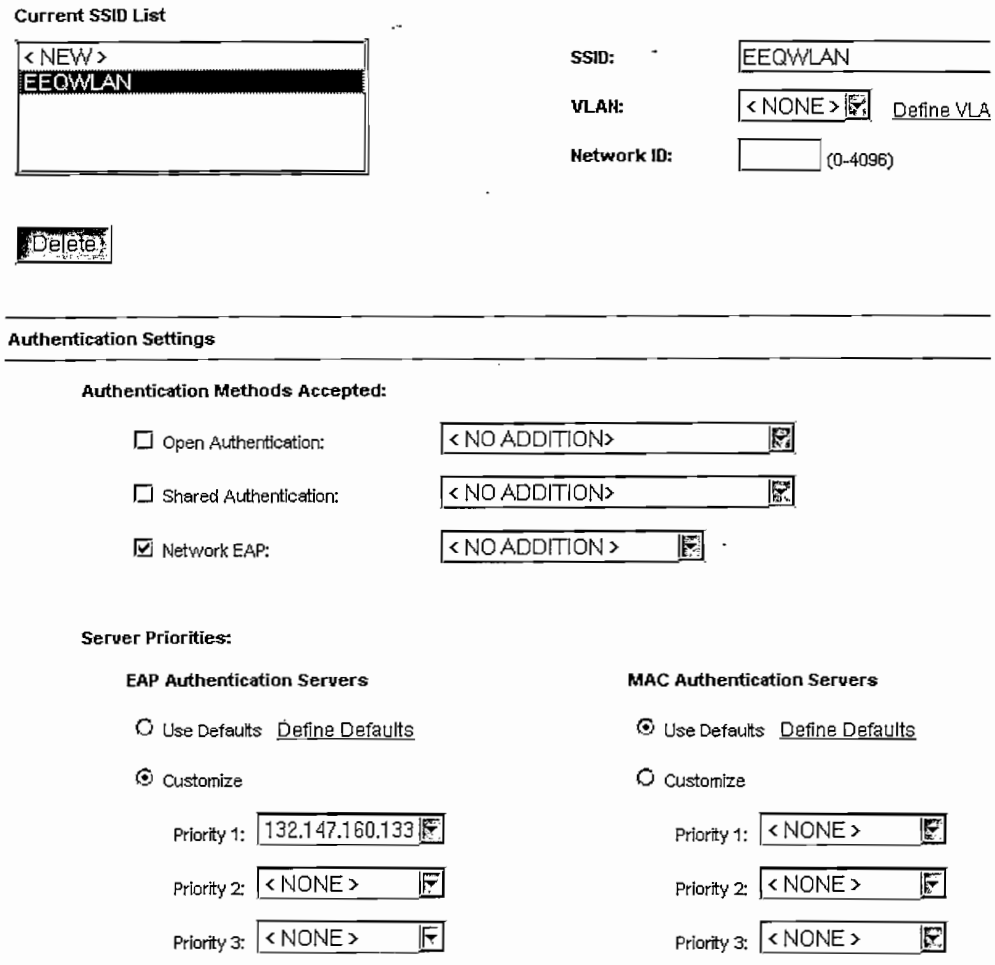


Figura A.15.- Tipo de autenticación EAP en el SSID

Podemos observar en resumen la configuración de seguridad en el equipo ingresando a la opción *Security* del menú principal como lo indica la figura A.16

Aquí se presenta las cuentas de administración, el tipo de autenticación Network EAP, el cifrado WEP de 128 bits, el servidor RADIUS empleado en EAP, el filtrado MAC se aplica en el radio como una lista de acceso.

Security Summary

Administrators

Username	Read-Only	Read-Write
admin		✓
alvaro	✓	

Radio0-802.11G SSIDs

SSID	VLAN	Open	Shared	Network EAP
EEQWLAN	none			no addition

Radio0-802.11G Encryption Settings

Encryption Mode	WEP		Cipher						Key Rota
	MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	CMIC	AES CCM	
Cipher					✓				

Server-Based Security

Server Name/IP Address	Type	EAP	MAC	Proxy Mobile IP	Admin	Accountin
132.147.160.133	RADIUS	✓				

Figura A.16.- Resumen de Seguridad ap1200

De igual manera en Express Security del menú principal indicará el resumen de seguridad del SSID como lo indica la figura a.17.

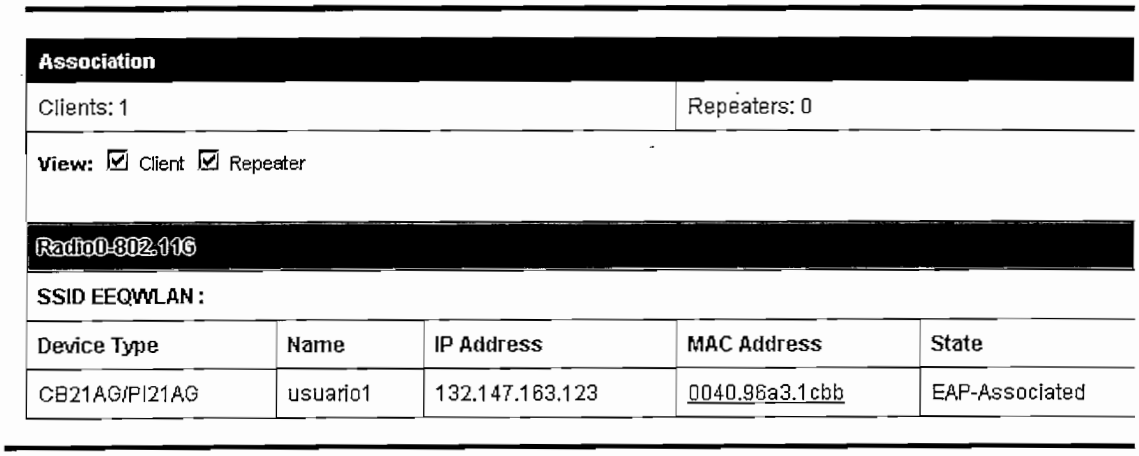
SSID Table

Delete	SSID	VLAN	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID
⊙	EEQWLAN	none	ciphers wep128	network EAP	none		

Figura A.17.- Resumen de configuración del SSID

Con esto se concluye la configuración de seguridad.

Se puede observar los clientes asociados y autenticados ingresando a ASSOCIATION del menú principal con lo cual aparece la figura A.18



Association

Clients: 1	Repeaters: 0

View: ☑ Client ☑ Repeater

Radio0-802.11G

SSID EEQWLAN :

Device Type	Name	IP Address	MAC Address	State
CB21AG/PI21AG	usuario1	132.147.163.123	0040.96a3.1cbb	EAP-Associated

Figura A.18.- Clientes Asociados y autenticados

El usuario asociado es el usuario1 que es creado en el servidor RADIUS, y corresponde a la dirección MAC que se permitió en el Filtro MAC, su estado se muestra como asociado mediante EAP.

El servidor RADIUS empleado es el Servidor Oddyssey, cuya configuración se puede revisar en la referencia [5].

A.3.2 CONFIGURACIÓN DEL CLIENTE LEAP.

Una vez que el cliente se encuentra instalado así como las utilidades de Cisco procedemos a configurar el cliente LEAP.

A3.2.1 CREACIÓN DEL PERFIL

Para configurar el cliente LEAP abrimos la utilidad ADU de Cisco e ingresamos a un nuevo usuario desde *Profile Management -> New* con lo cual aparece la pantalla de la figura A.19. Aquí establecemos el nombre del perfil, el nombre de usuario y el SSID de la red a la cual nos conectaremos.

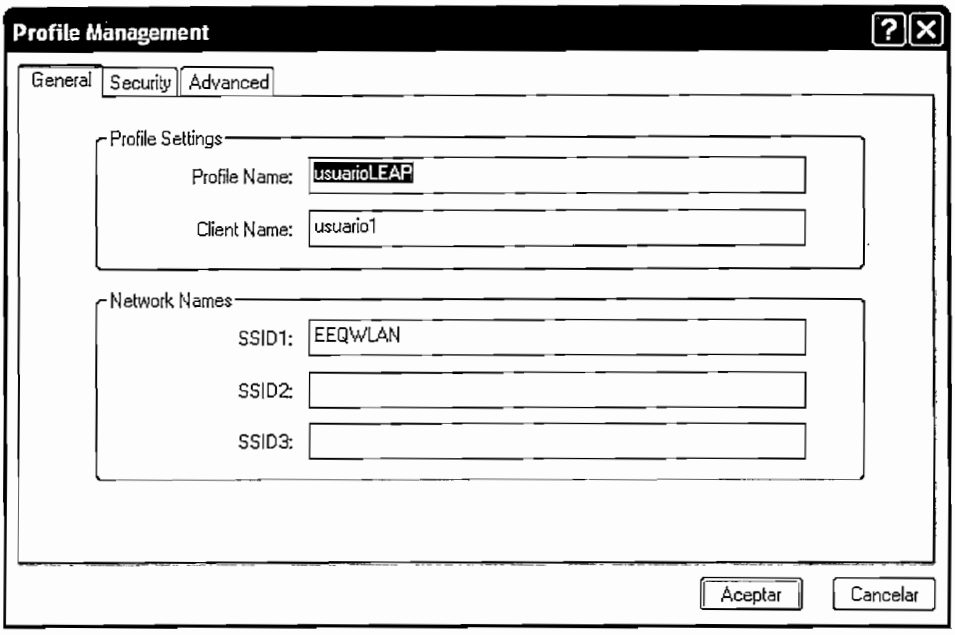


Figura A.19.-Creación del perfil y usuario LEAP

A3.2.2 SEGURIDAD EN EL CLIENTE

Establecemos la seguridad en el cliente ingresando en la pestaña *Security* del menú, se selecciona 802.1x indicando el uso de Autenticación mediante un servidor, en particular RADIUS, con protocolo de autenticación LEAP de Cisco, como lo indica la figura A.20.

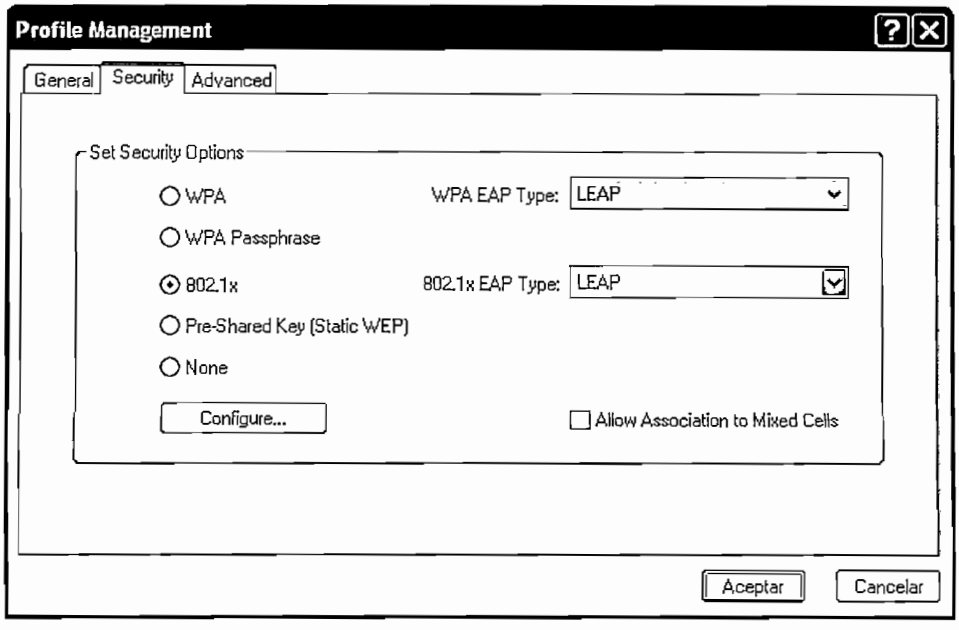


Figura A.20.- Configuración LEAP en el cliente

Ingresamos en el botón de *Configure* con lo cual nos aparece la figura A.21, en donde se establece el nombre de usuario y contraseña que se emplean en el servidor de autenticación.

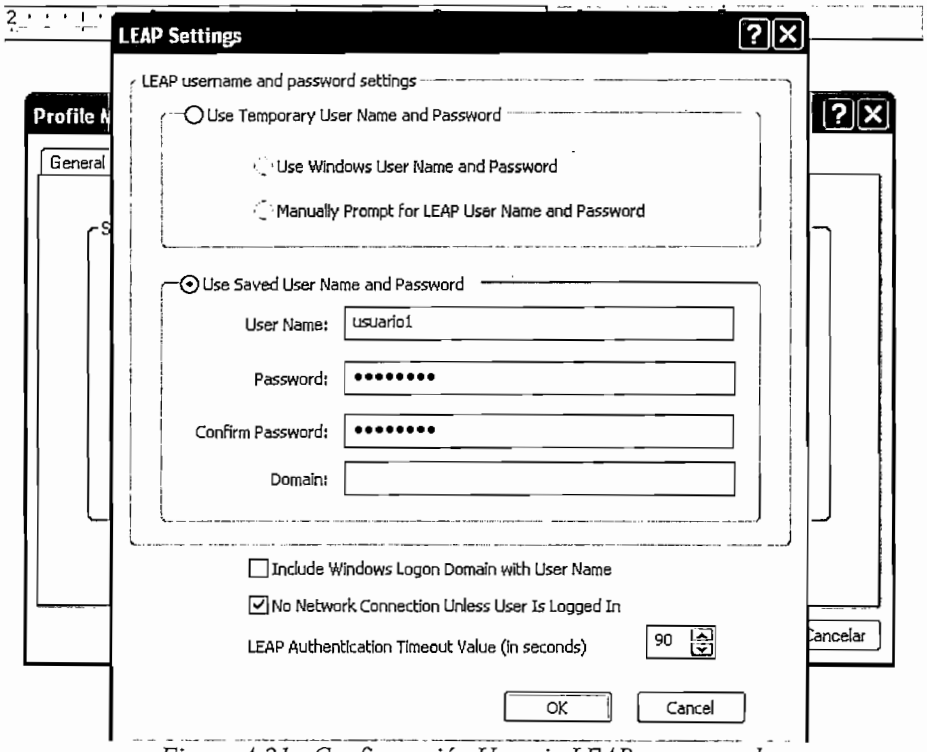


Figura A.21.- Configuración Usuario LEAP y password.

A3.2.3 CONFIGURACIONES ADICIONALES

Configuramos el tipo de velocidad y la banda de operación ingresando a *Advanced* del menú principal con lo cual nos aparece la pantalla de la figura A.22.

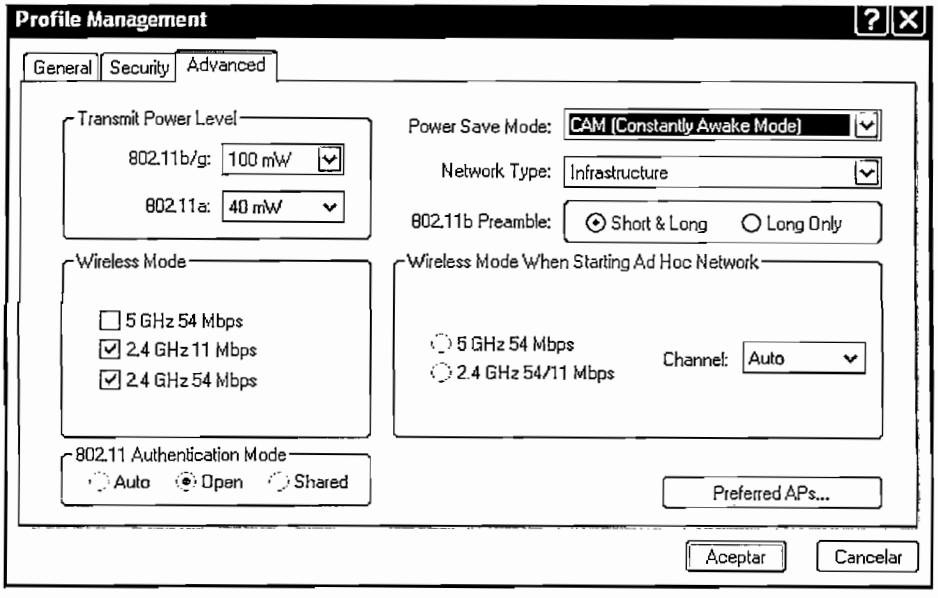


Figura A.22.- Configuración de Banda de frecuencia

Una vez establecidos los parámetros de seguridad empieza el proceso de autenticación indicado en la figura A.23.

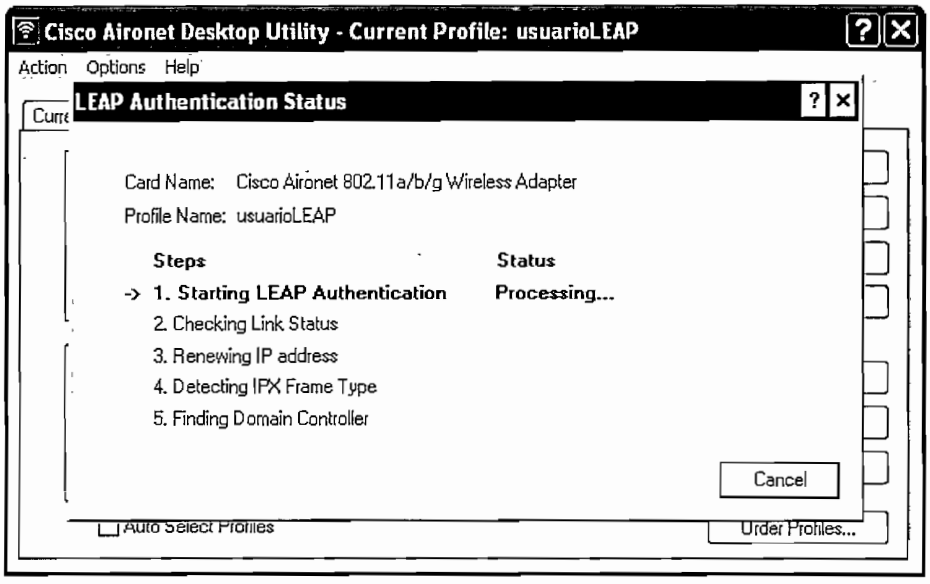


Figura A.23.- Proceso de autenticación

Una vez finalizado el proceso de autenticación el cliente se encuentra asociado y autenticado al punto de acceso como lo indica la figura A.24.

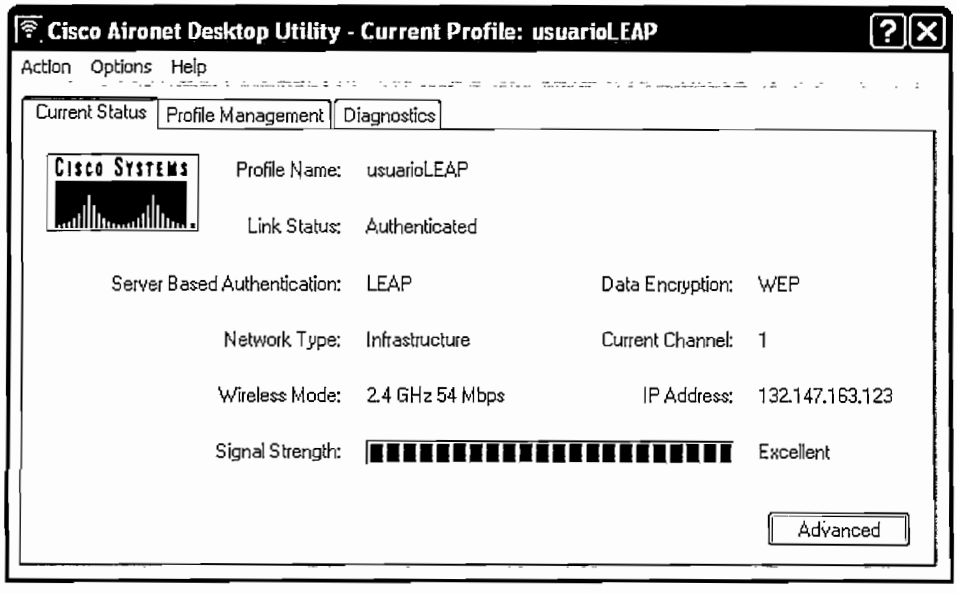


Figura A.24.- Cliente Asociado y autenticado.

Aquí podemos observar que la Autenticación está basada en el Servidor LEAP, con encripción WEP, y parámetros adicionales como velocidad, canal, AP asociado, como lo indica la figura A.25.

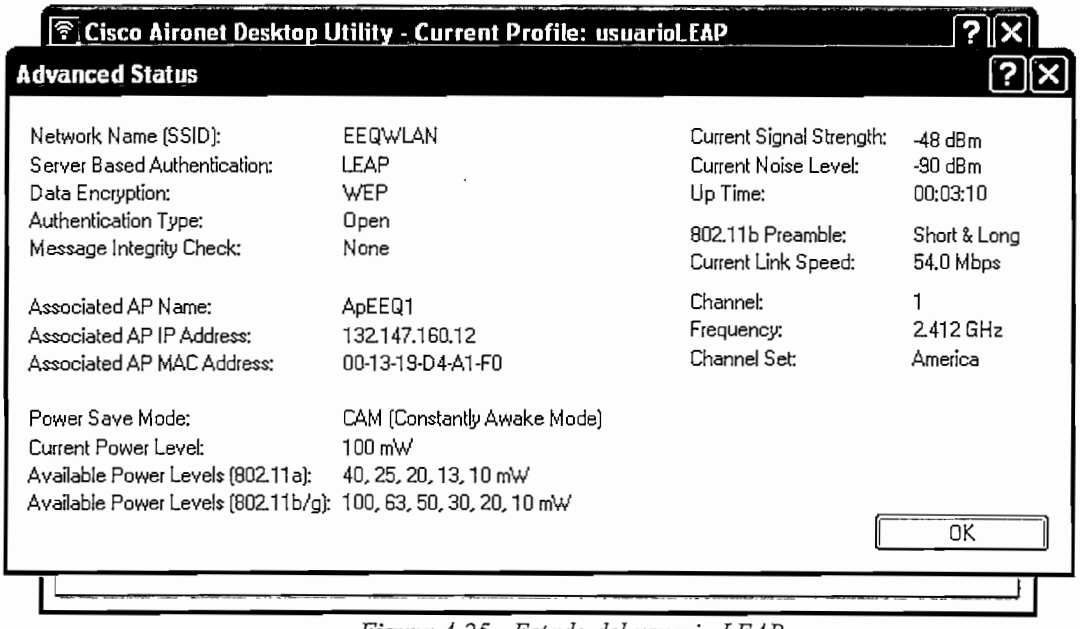


Figura A.25.- Estado del usuario LEAP

El usuario asociado al punto de acceso muestra información sobre el adaptador inalámbrico ingresando a *Diagnostics -> Adapter Information* con lo cual nos aparece la pantalla de la figura A.26.

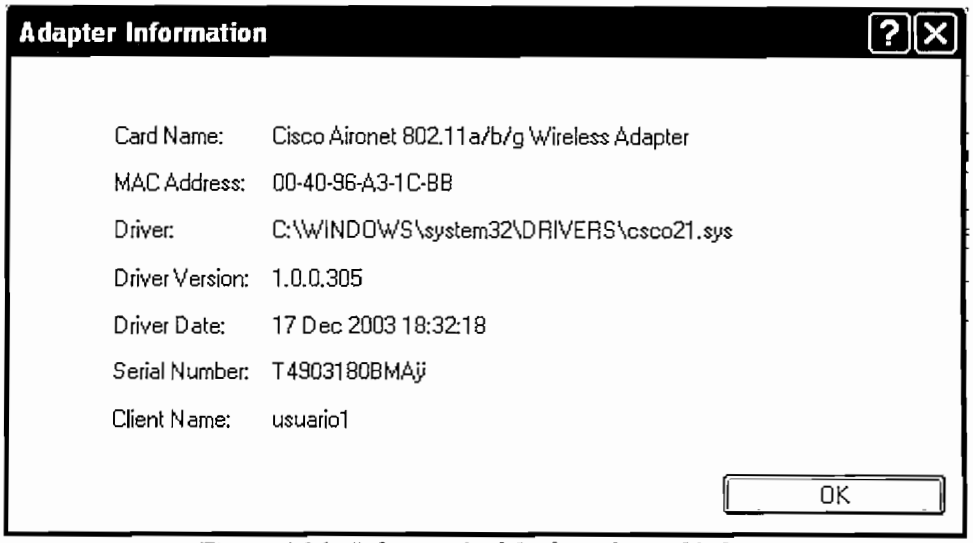
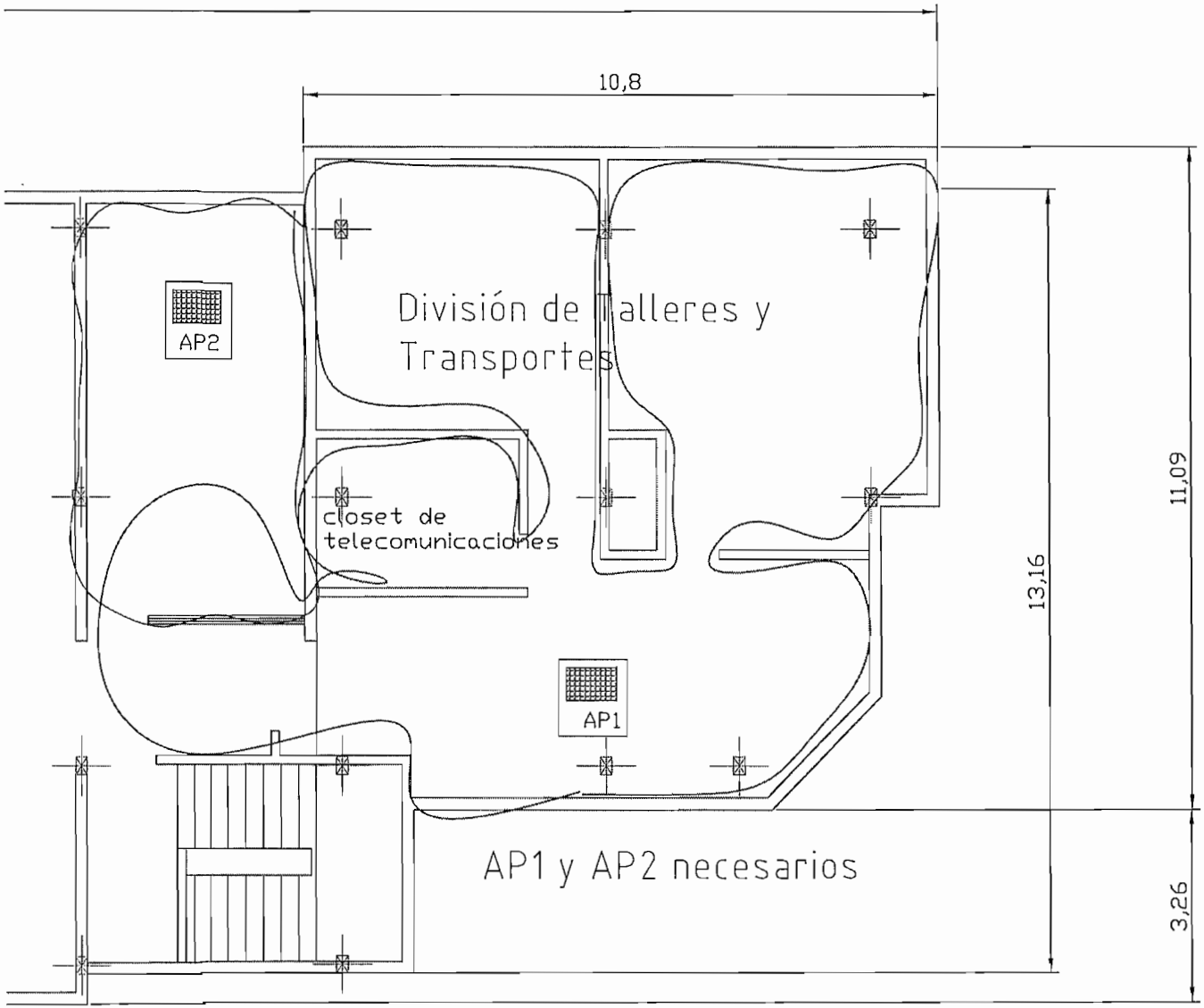


Figura A.26.- Información del adaptador inalámbrico

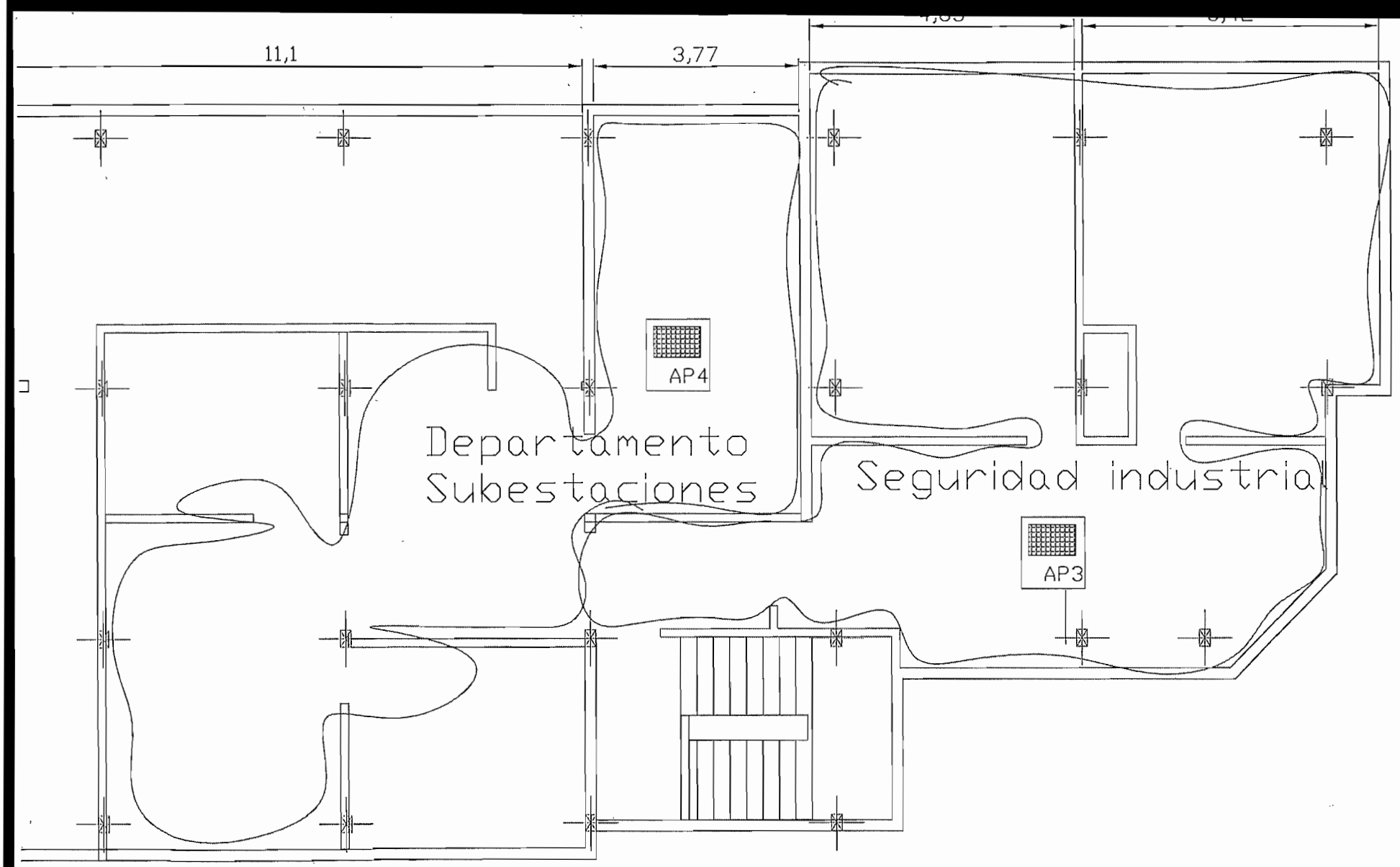
Con esto se concluye las opciones de seguridad.

Anexo 4
Site Survey a 54 Mbps



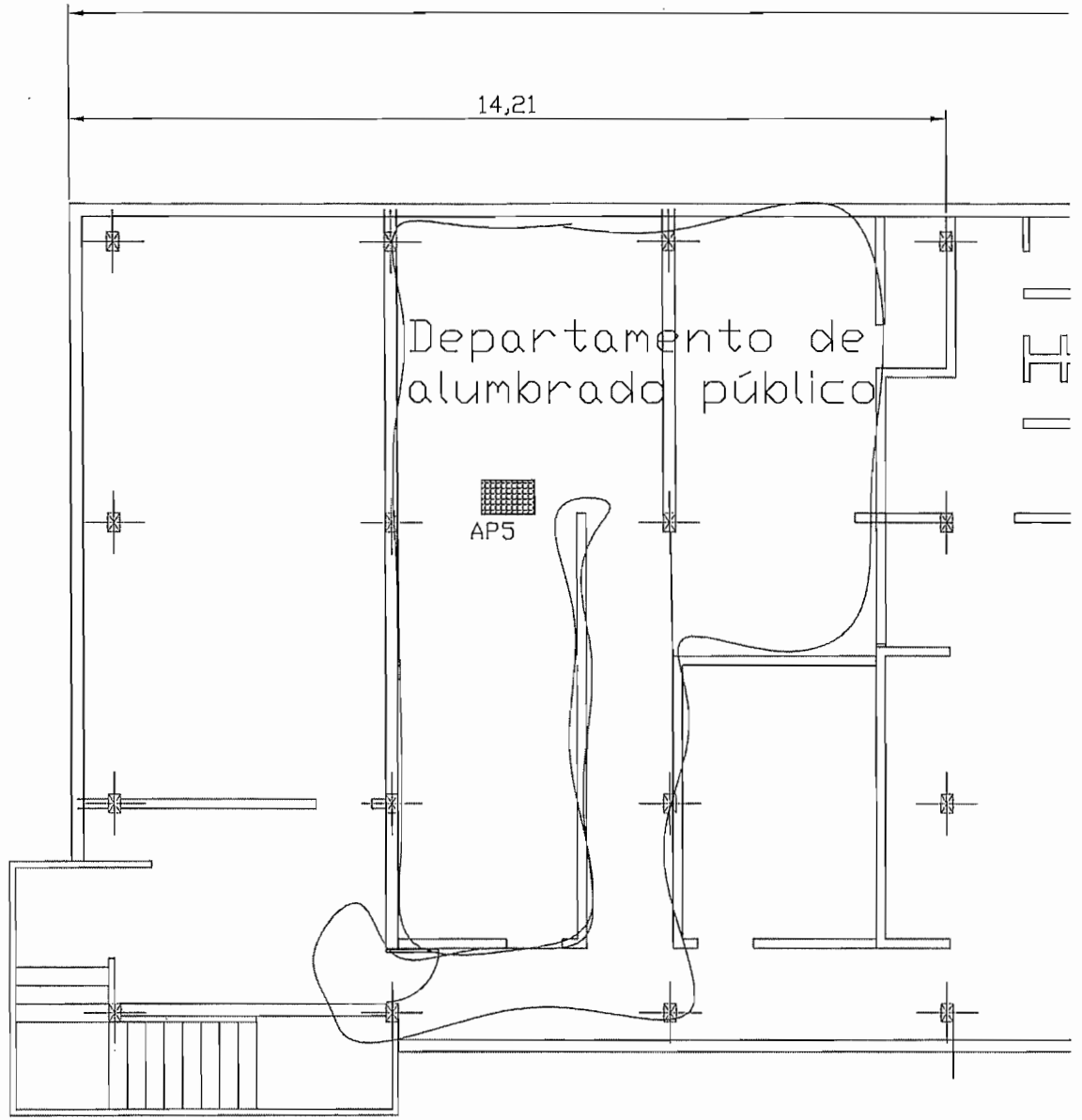
Edificio Polifuncional

tercer piso



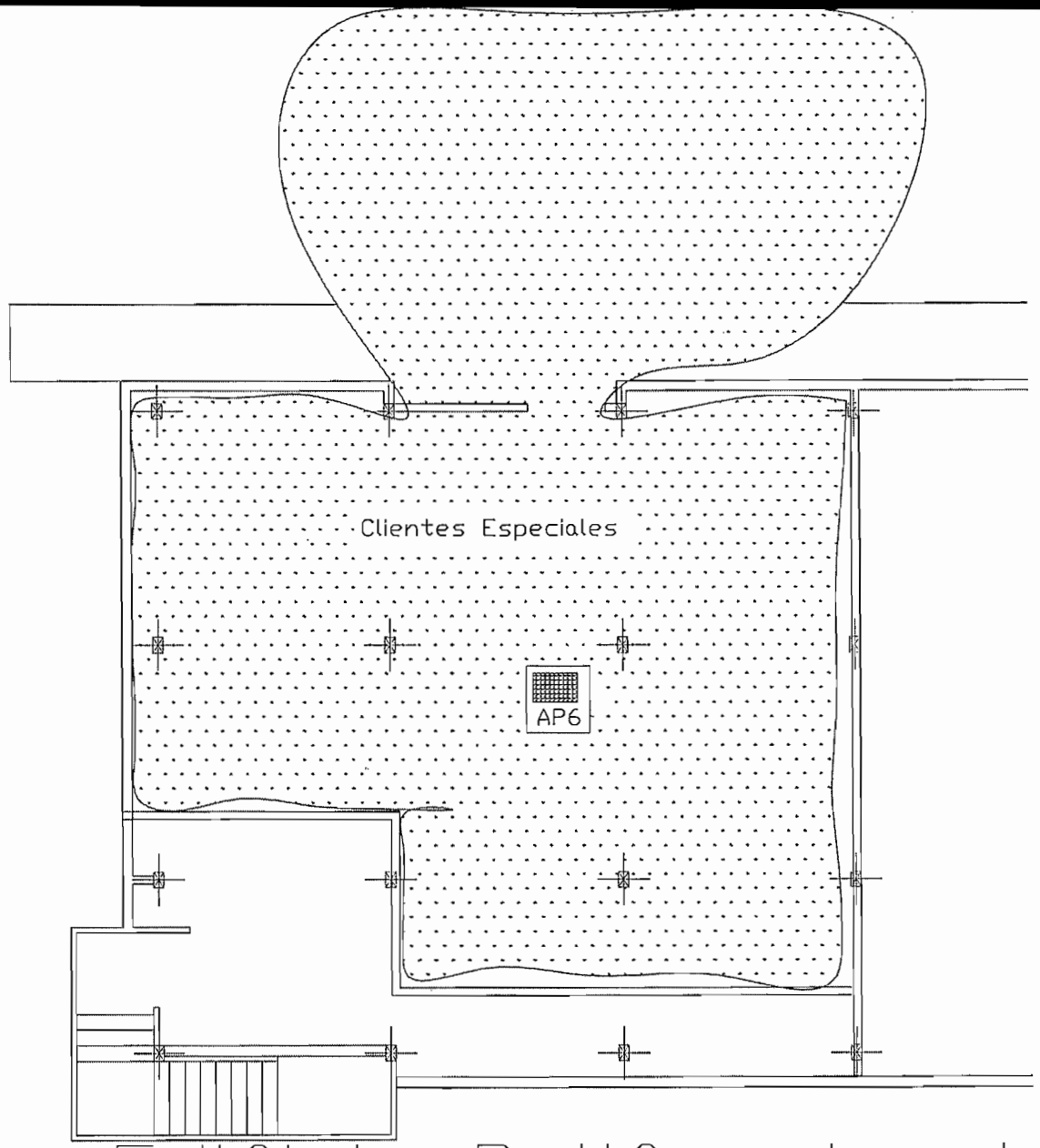
Edificio Polifuncional

Segundo piso

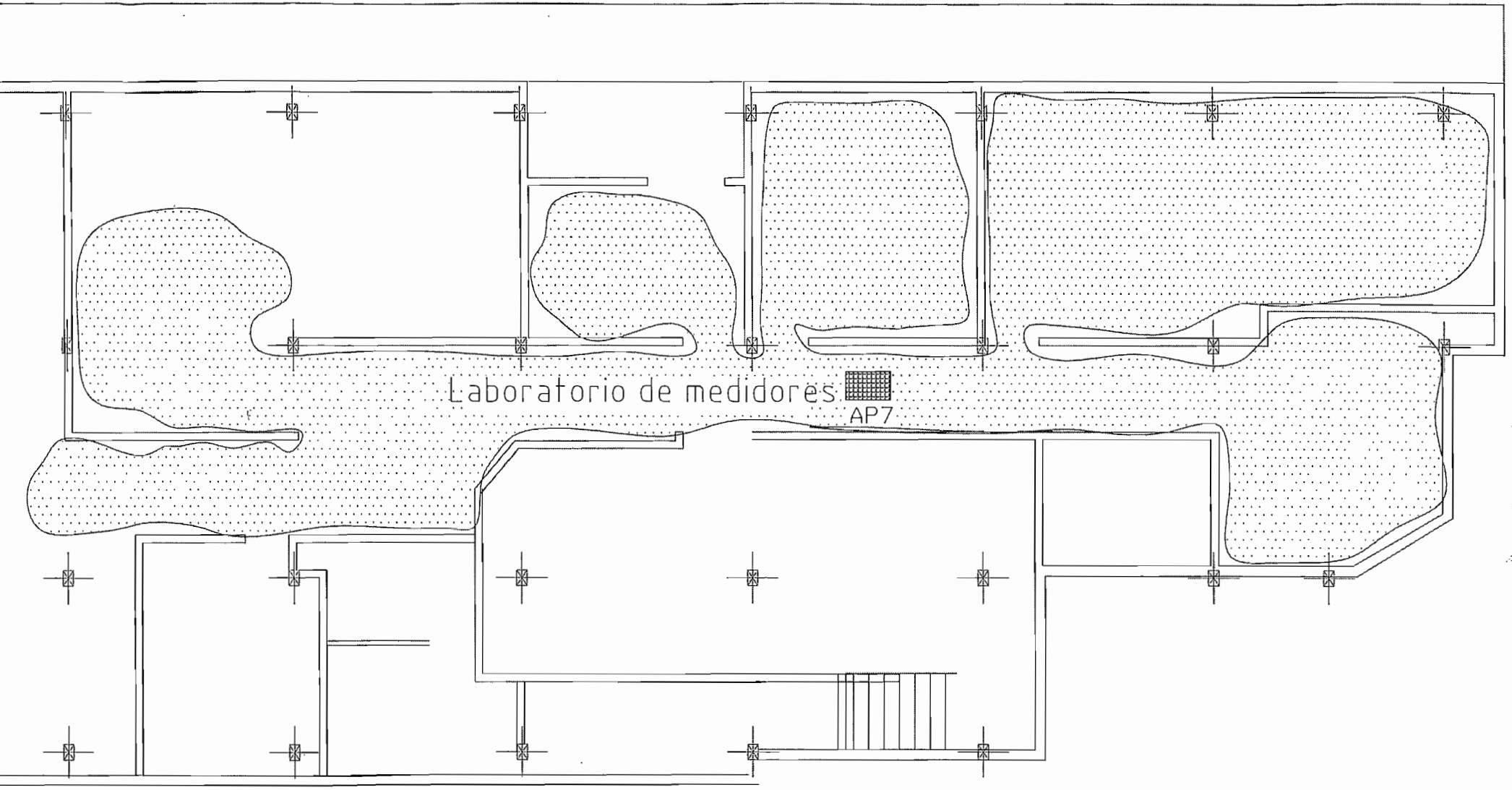


Edificio Polifuncional

tercer piso

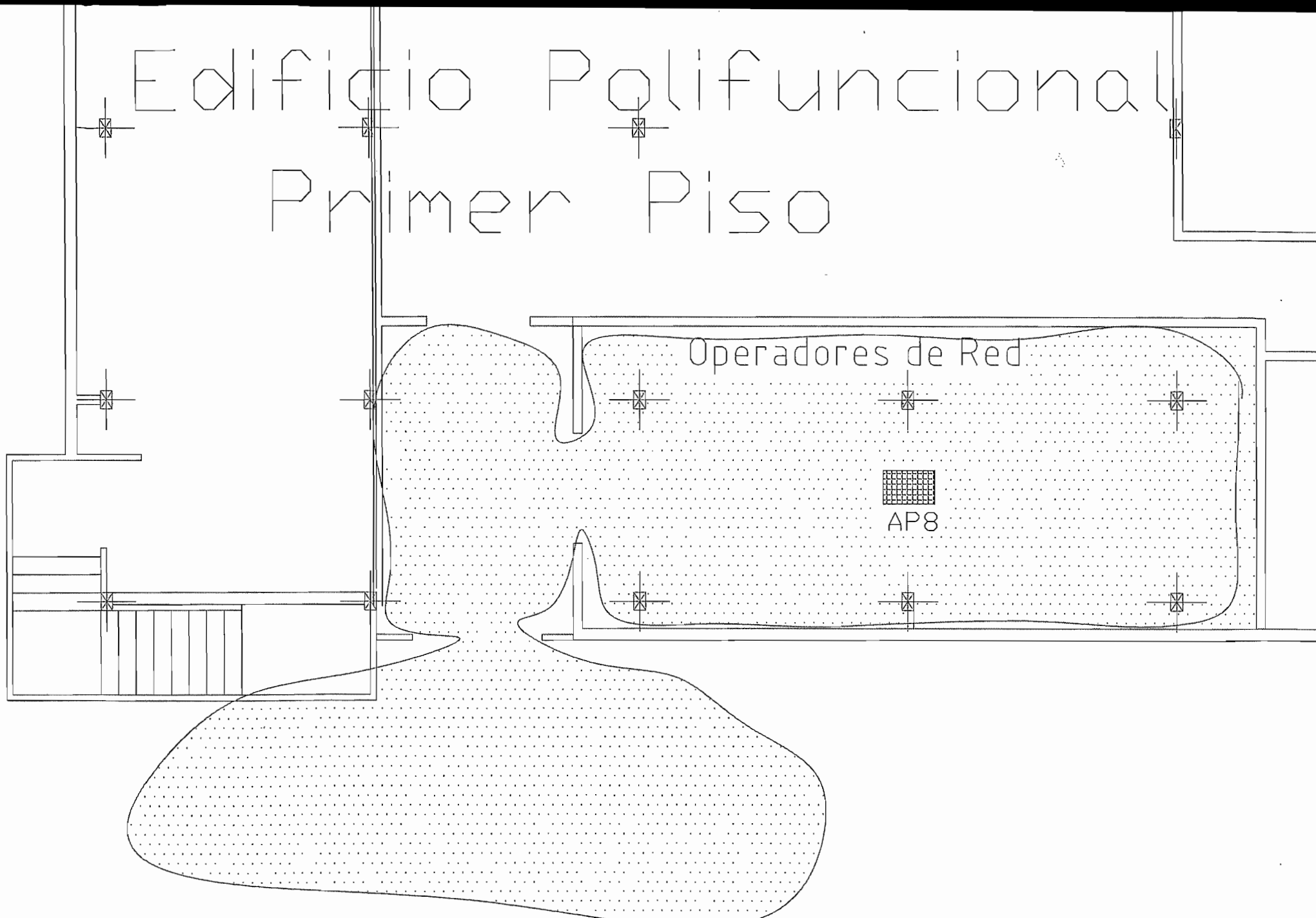


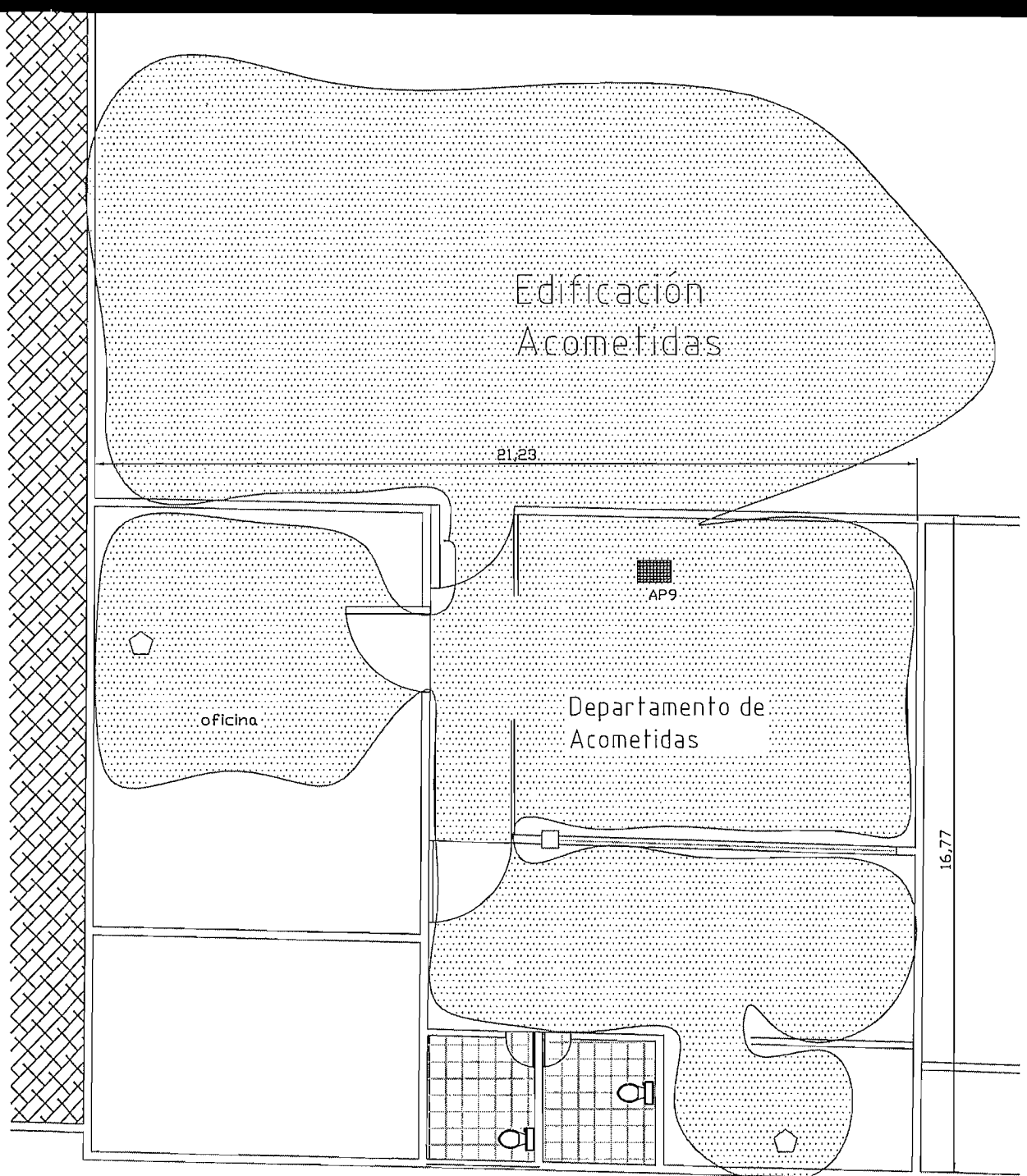
Edificio Polifuncional
Planta Baja

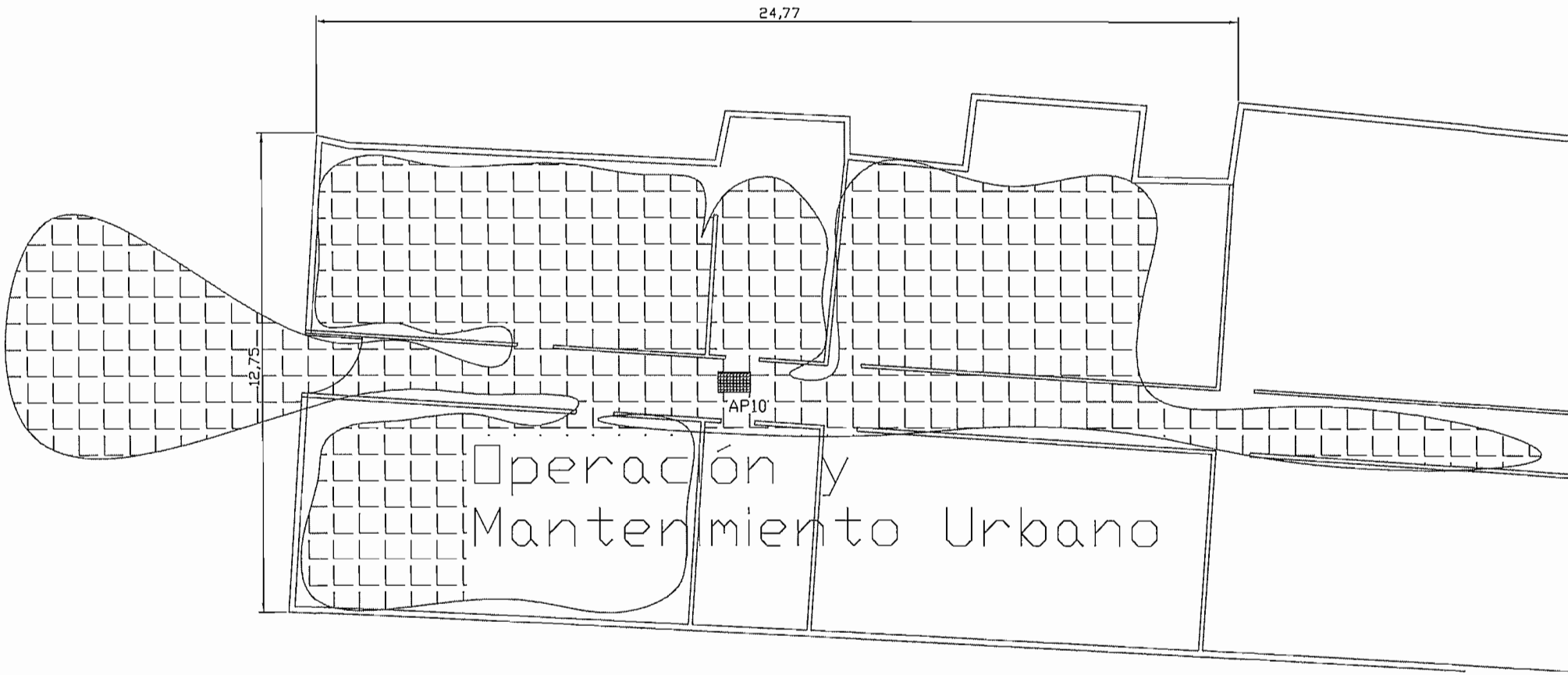


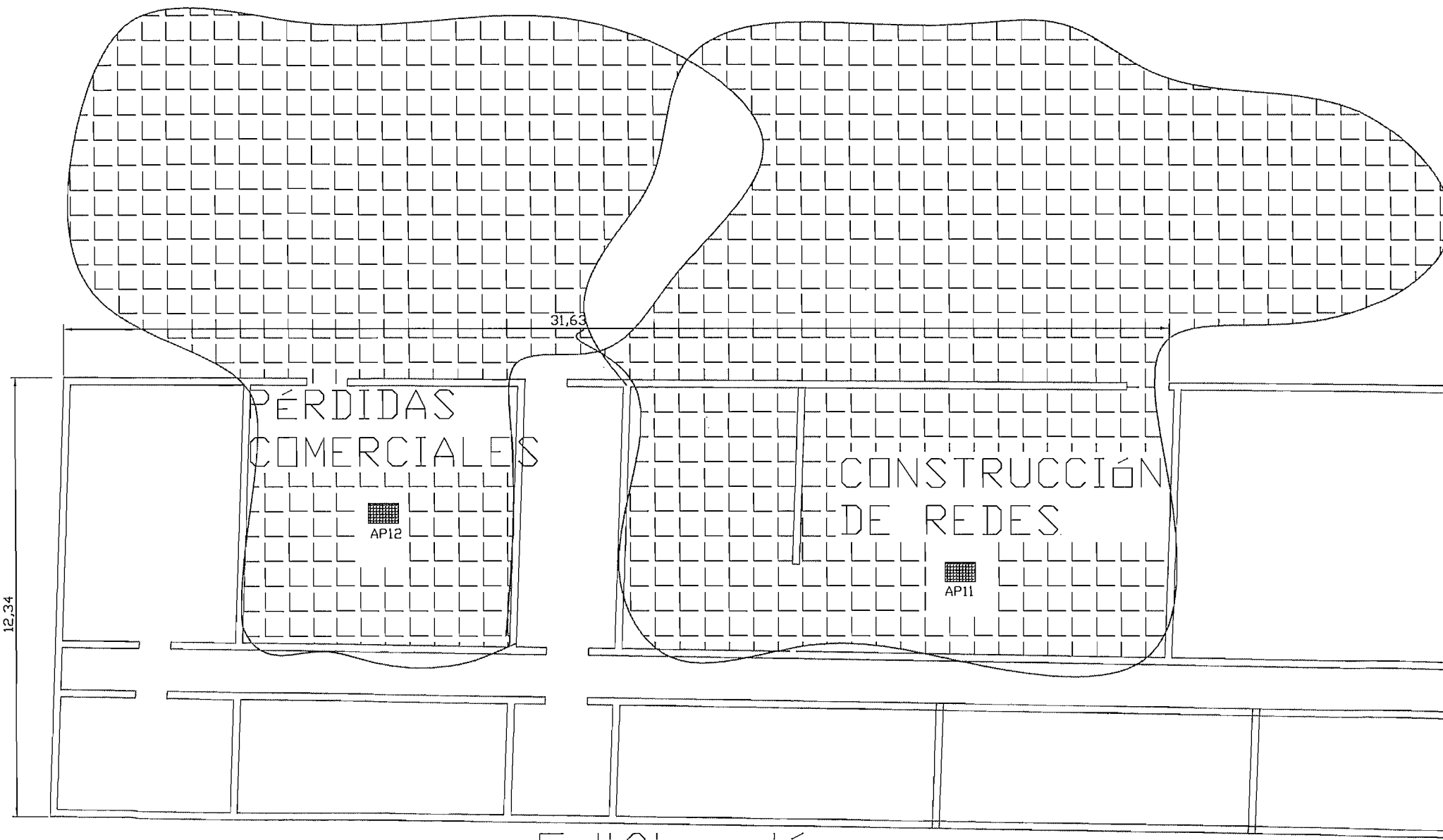
Edificio Polifuncional
Planta Baja

Edificio Polifuncional
Primer Piso



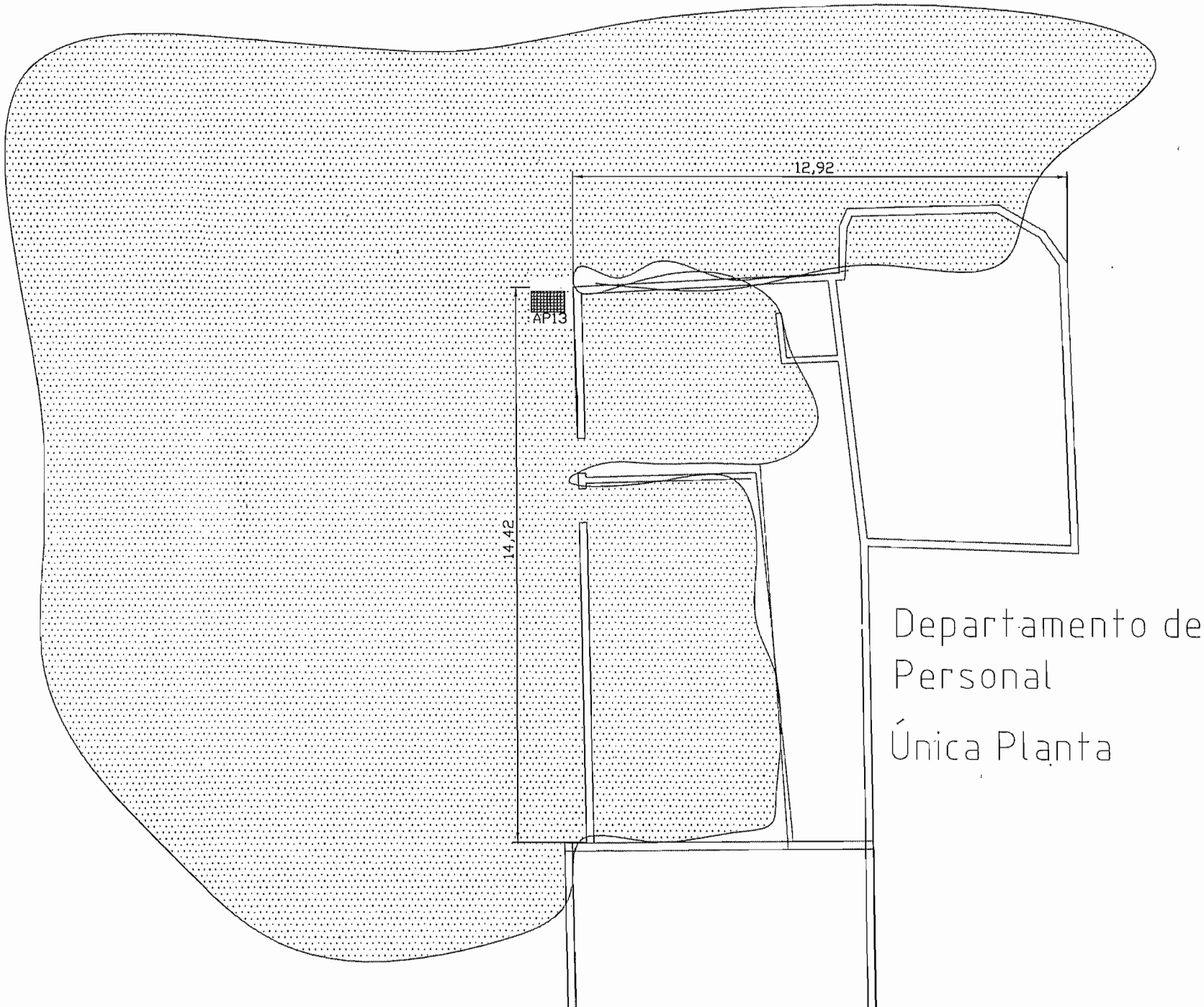

Edificación
Acometidas
21,23
AP9
oficina
Departamento de
Acometidas
16,77

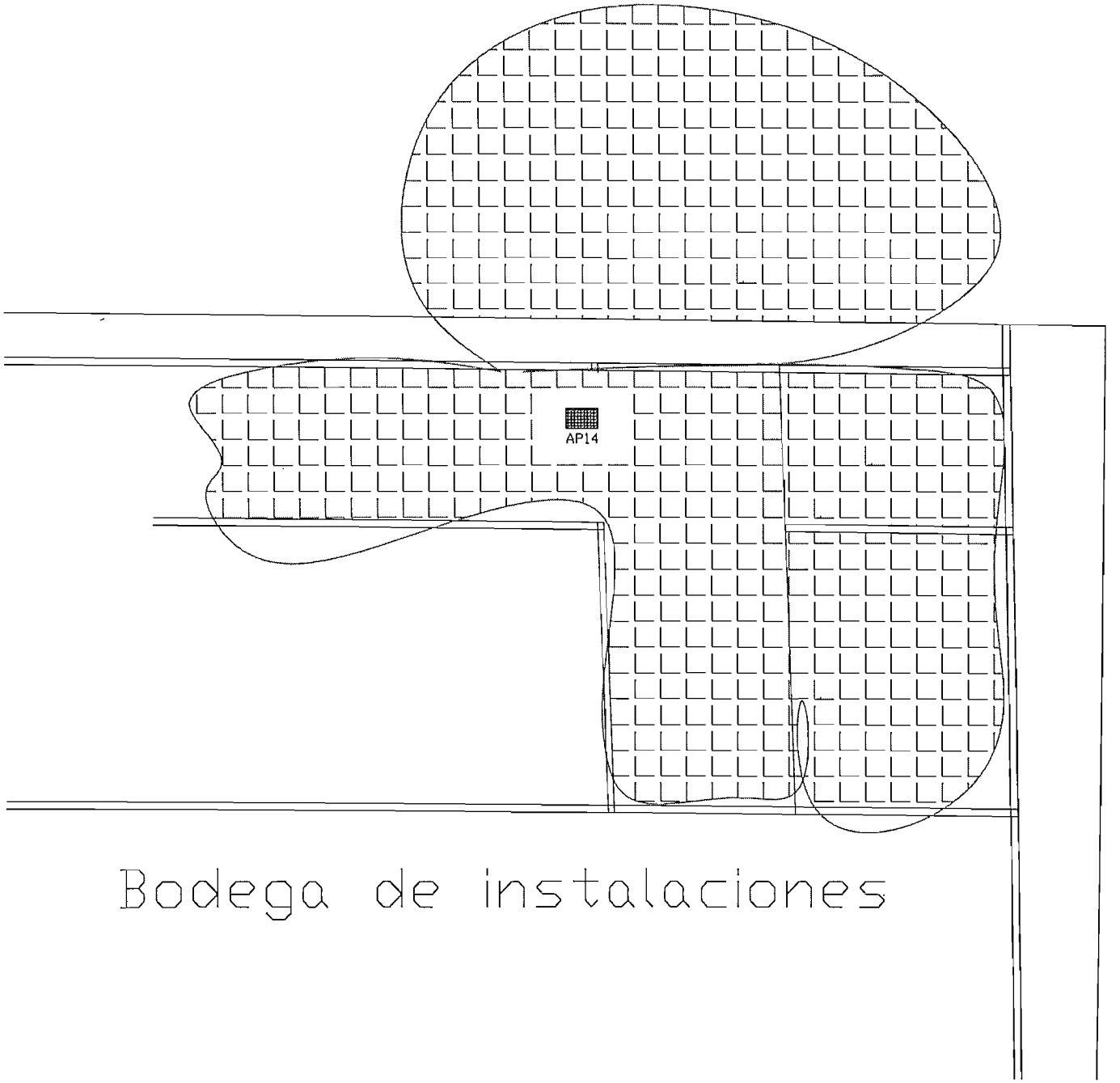

24,77
12,75
AP10
Operación y
Mantenimiento Urbano



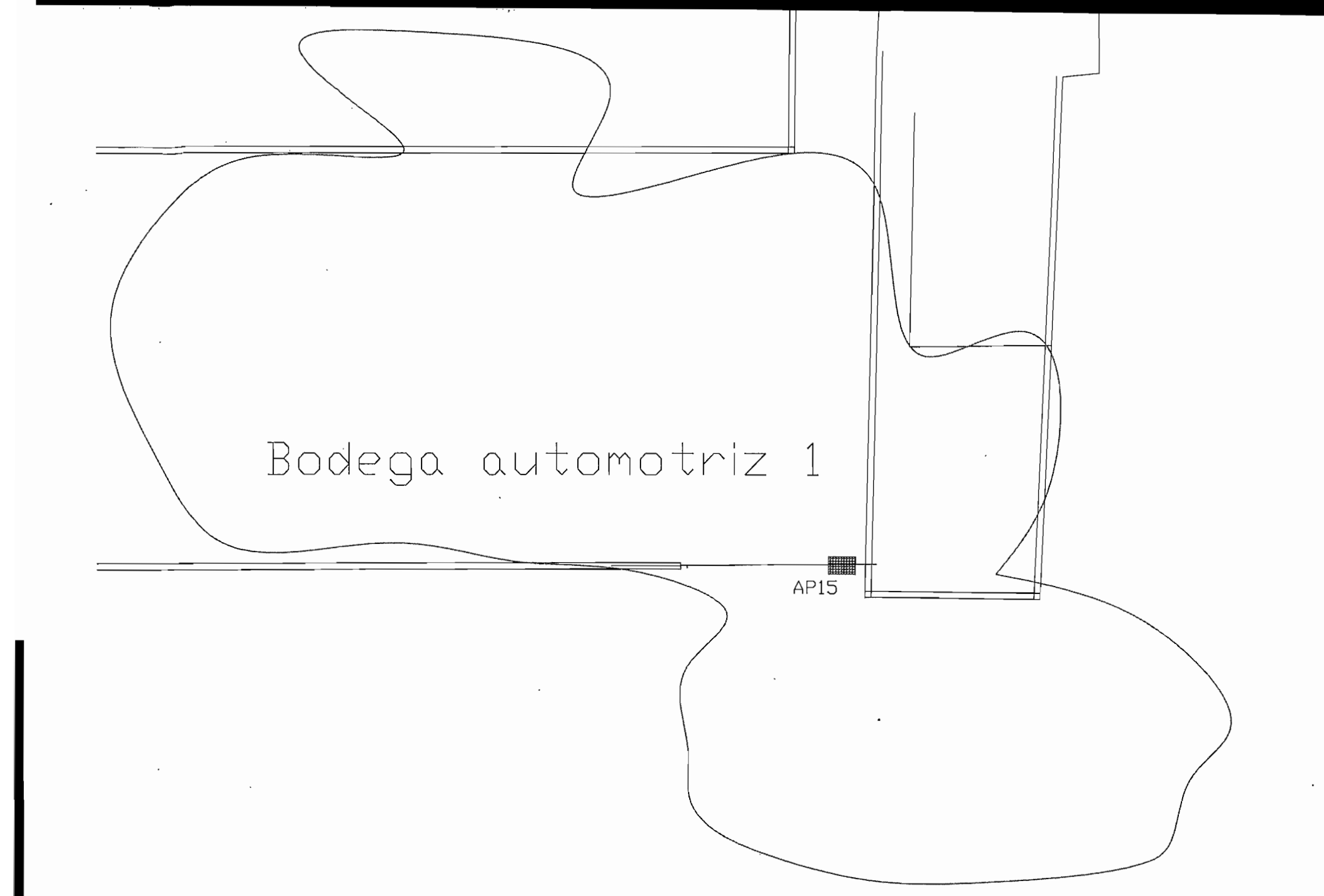
Edificación

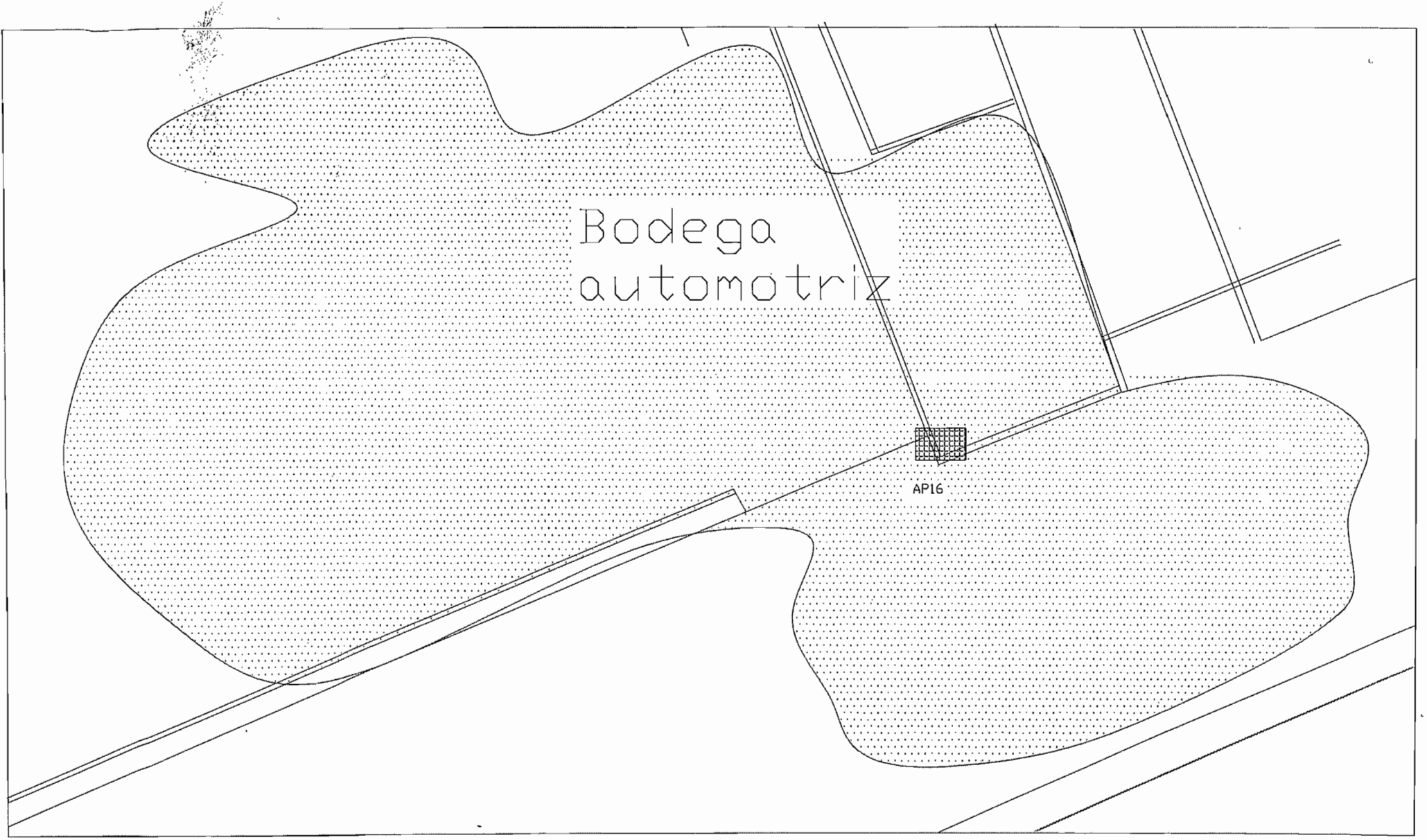
Construcción de Redes

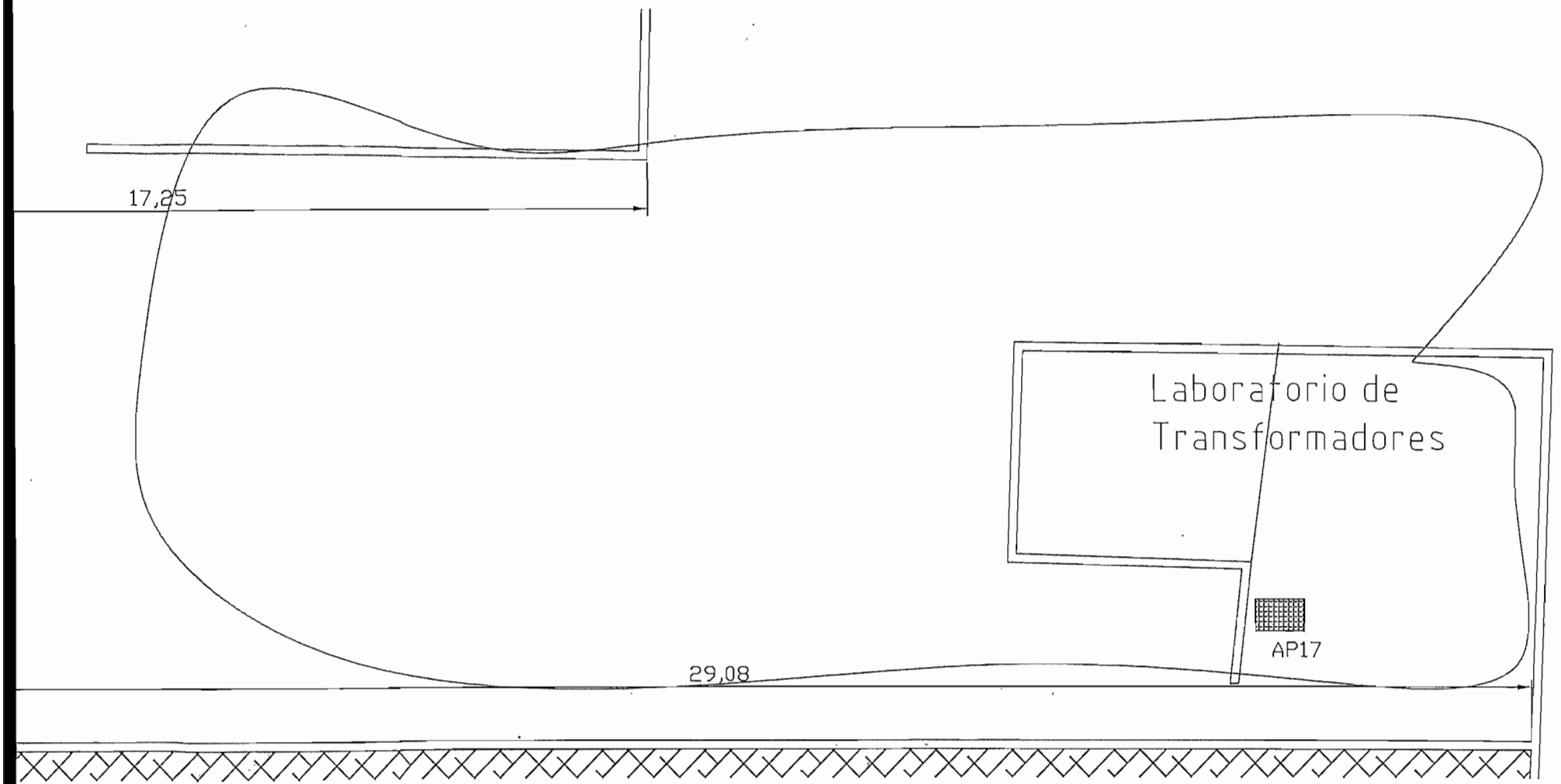

12,92
AP13
14,42
Departamento de
Personal
Única Planta

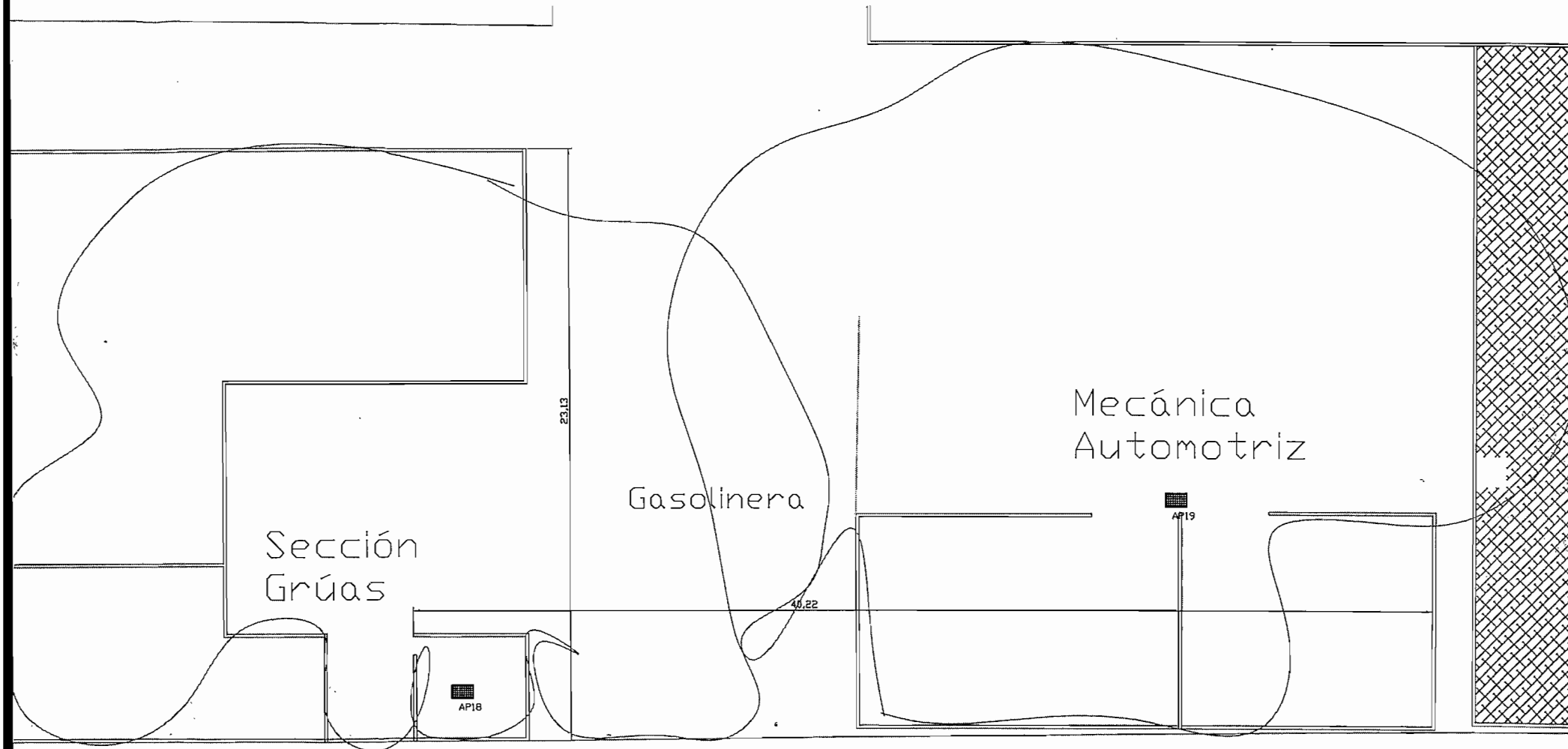


Bodega de instalaciones

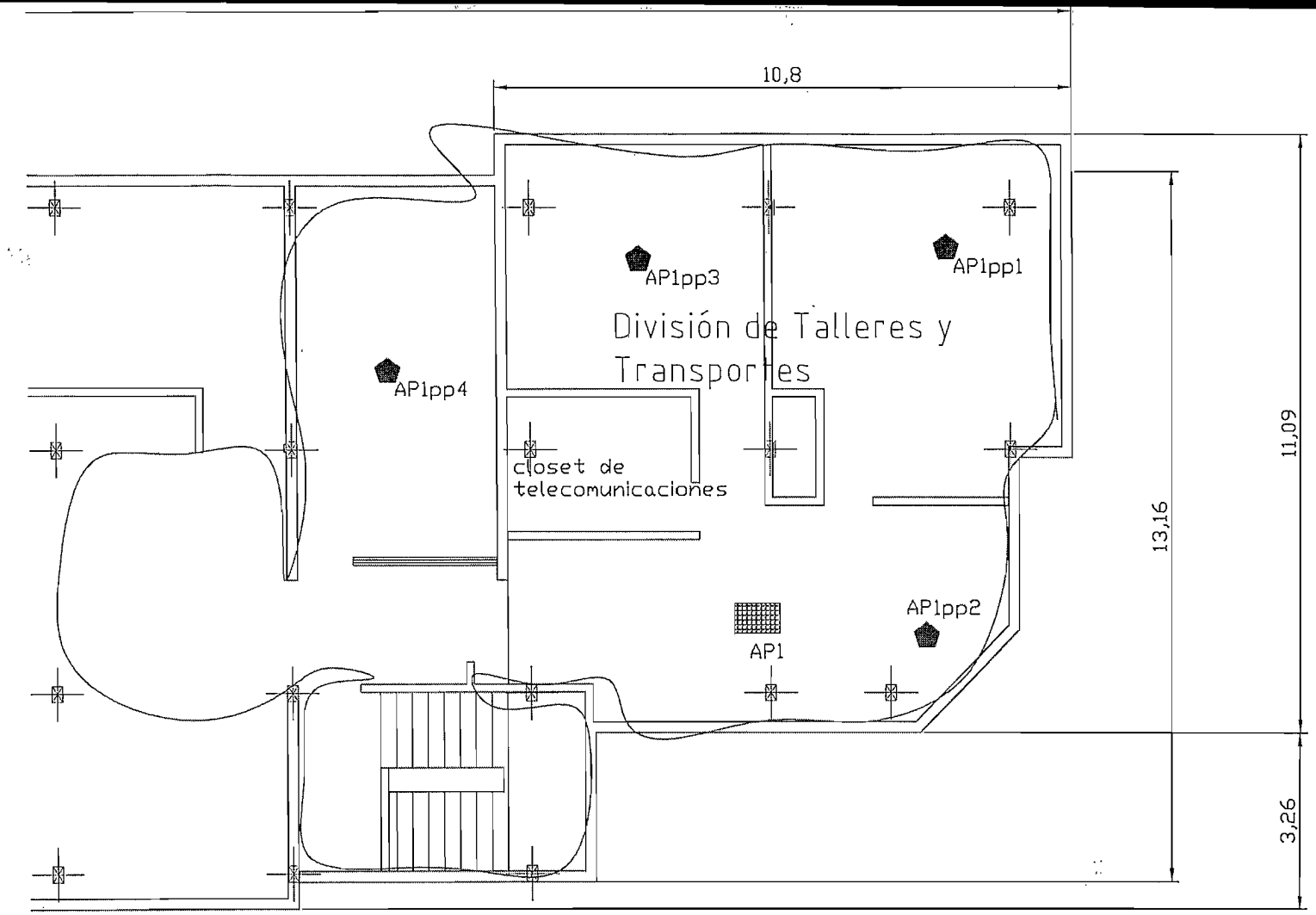

Bodega automotriz 1
AP15


Bodega
automotriz
AP16


17,25
Laboratorio de
Transformadores
AP17
29,08

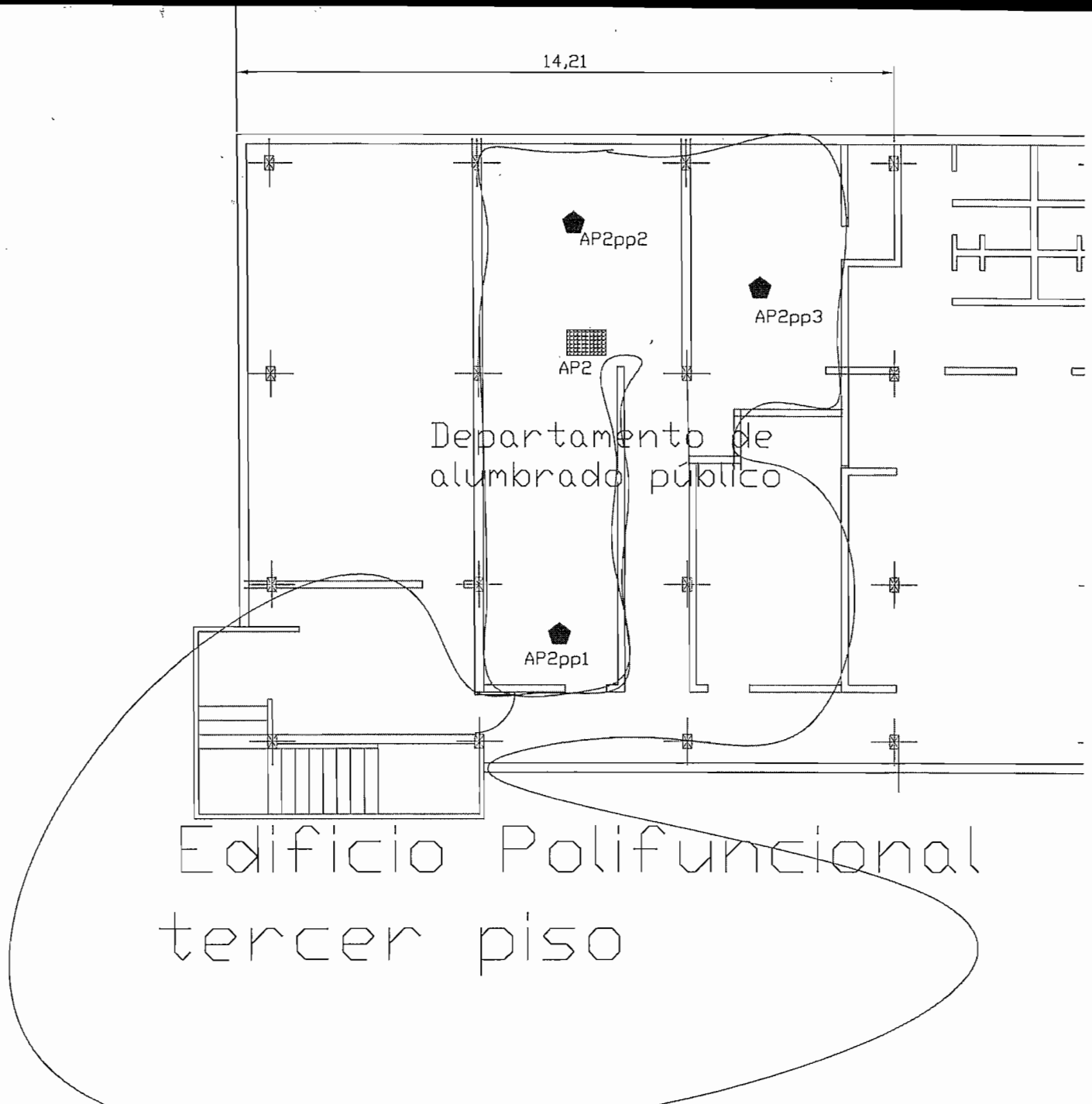

Sección
Grúas
Gasolinera
Mecánica
Automotriz
23.13
40.22
AP18
AP19

Anexo 5
Site Survey con Velocidad Negociable



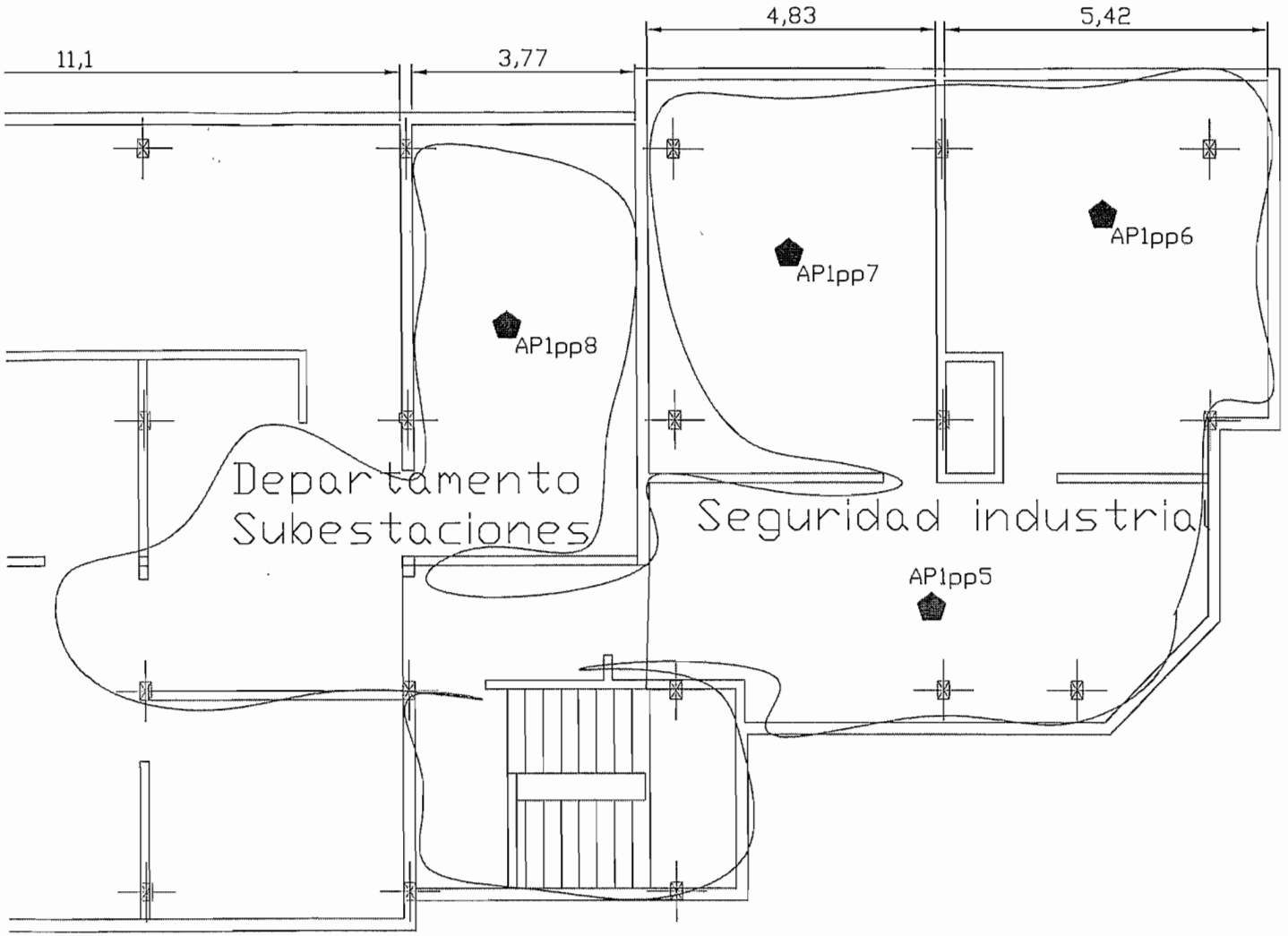
Edificio Polifuncional

tercer piso



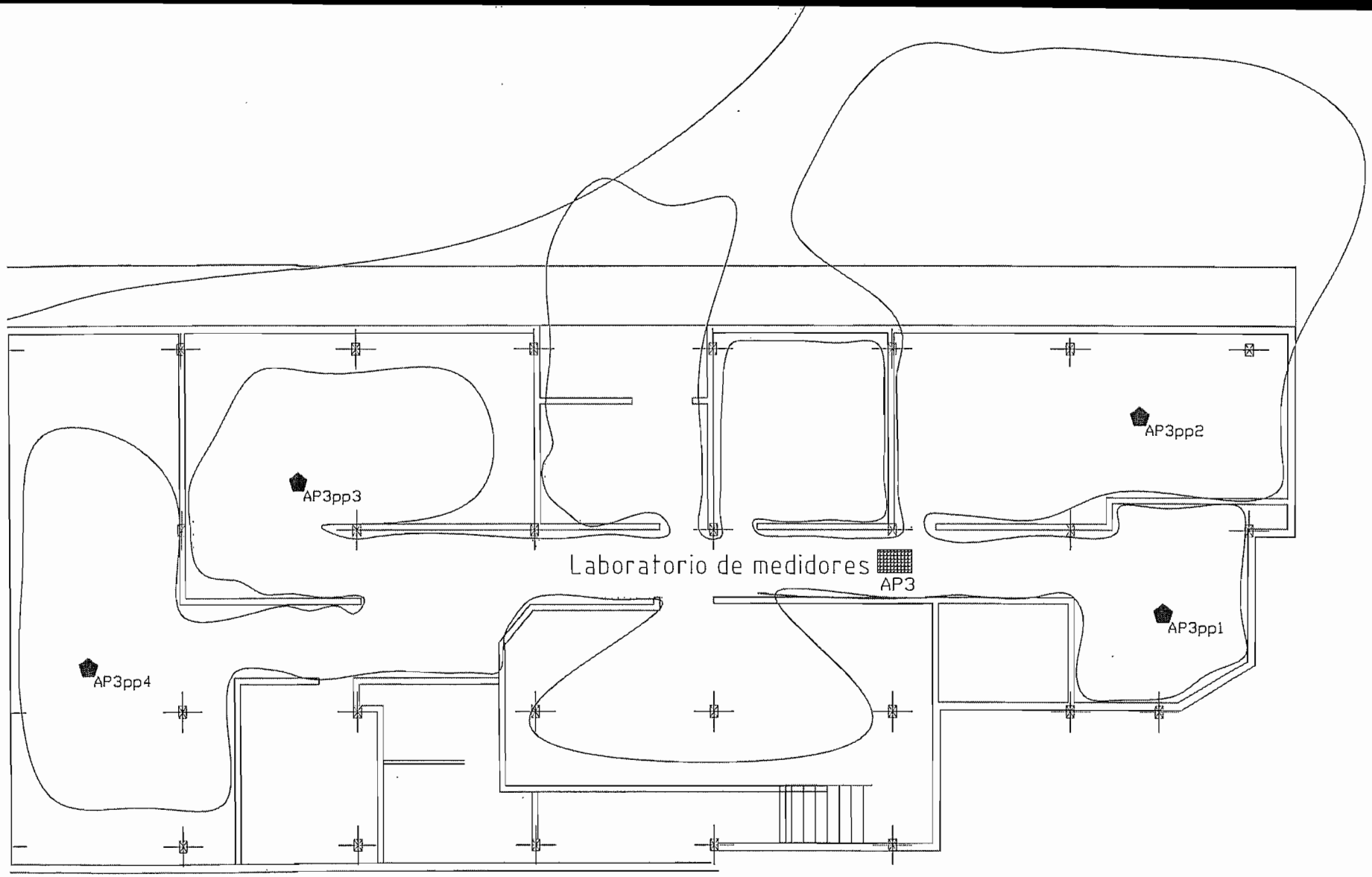
Edificio Polifuncional

tercer piso

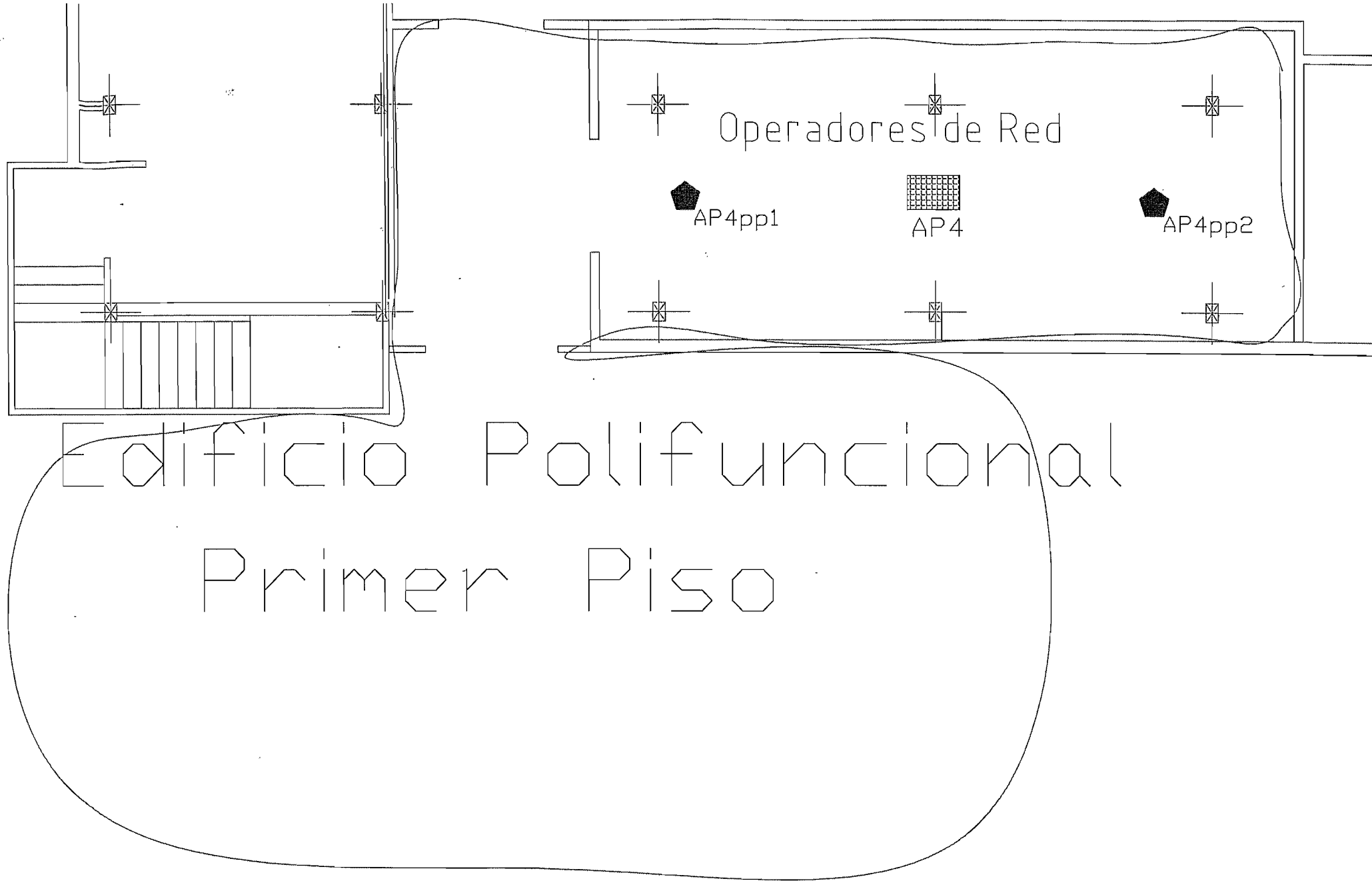


Edificio Polifuncional

Segundo piso

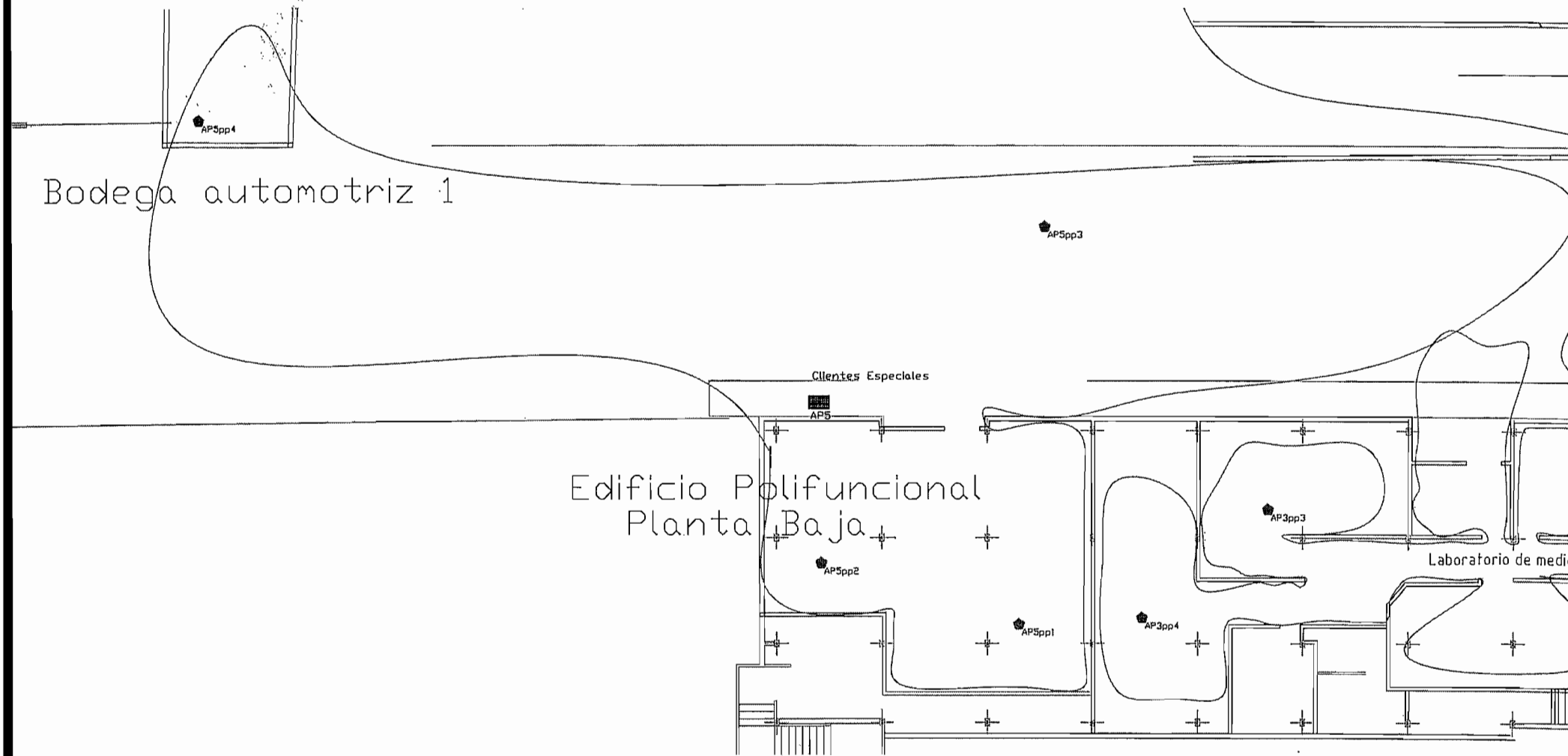


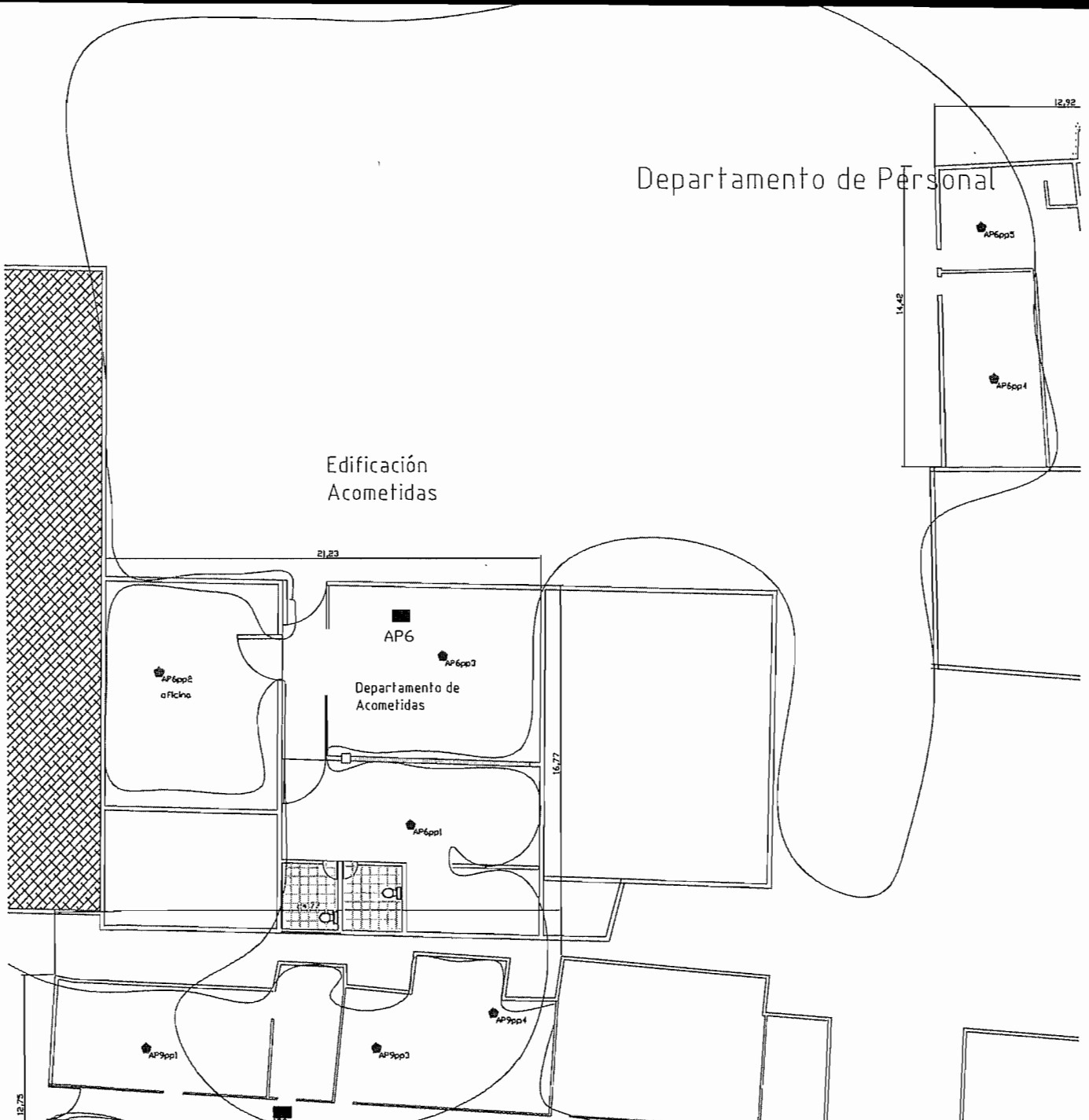
Edificio Polifuncional
Planta Baja

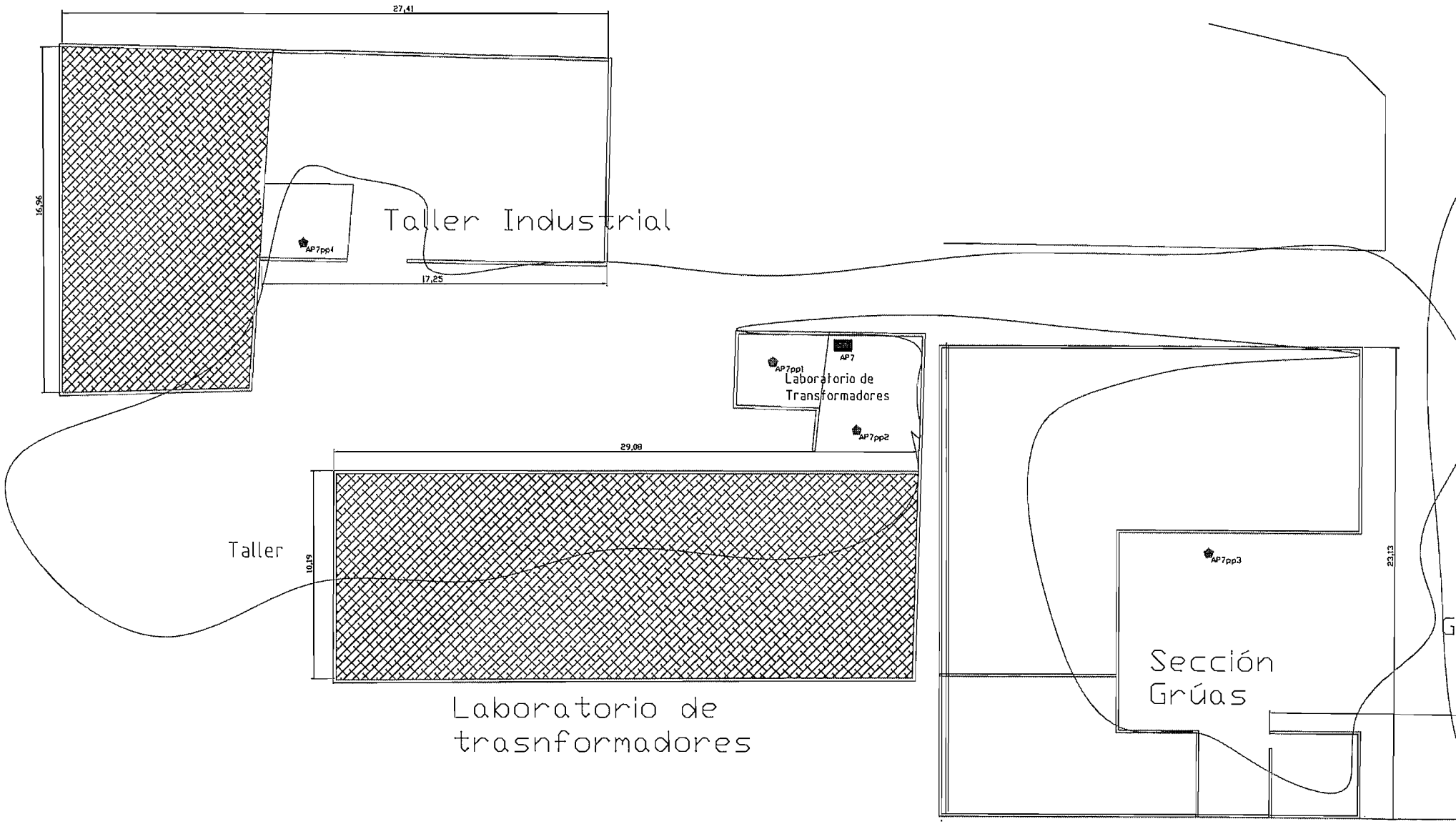


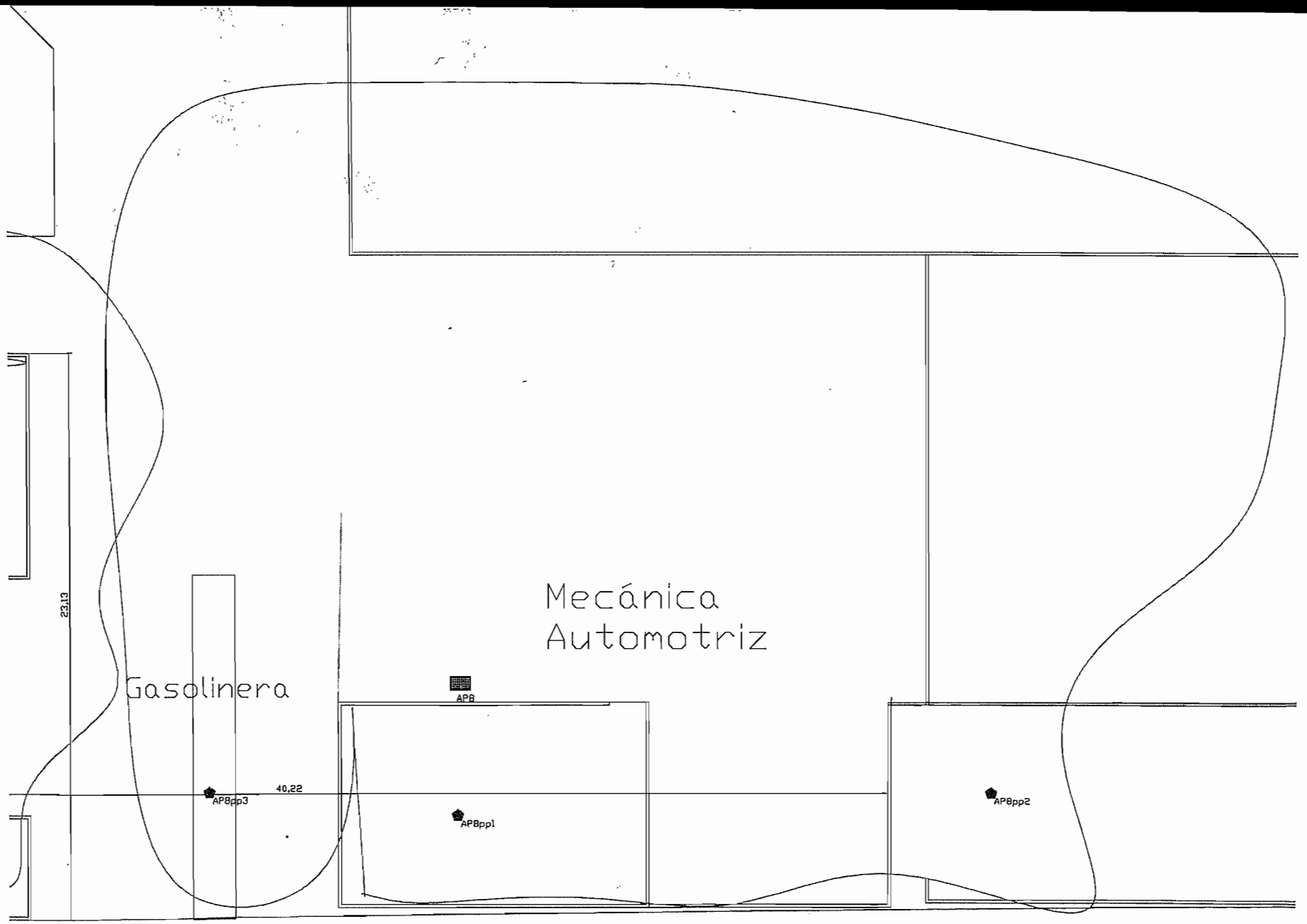
Edificio Polifuncional

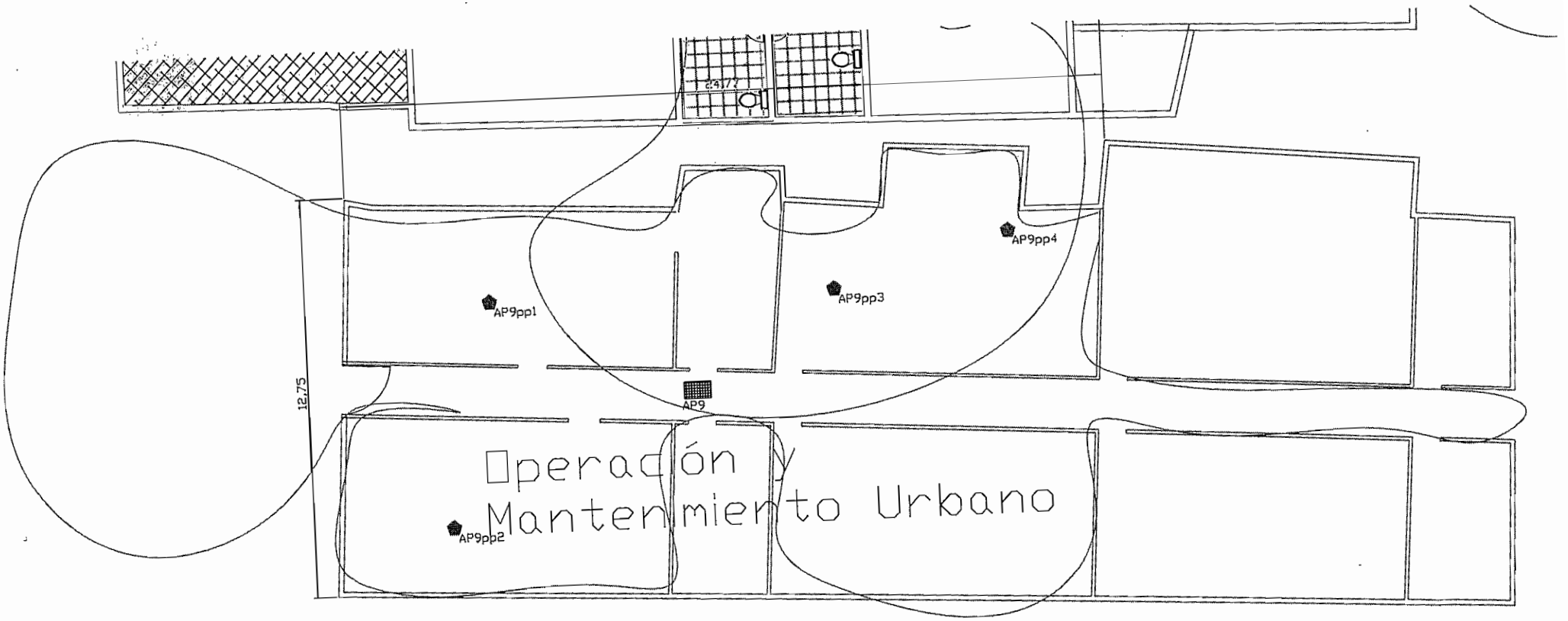
Primer Piso

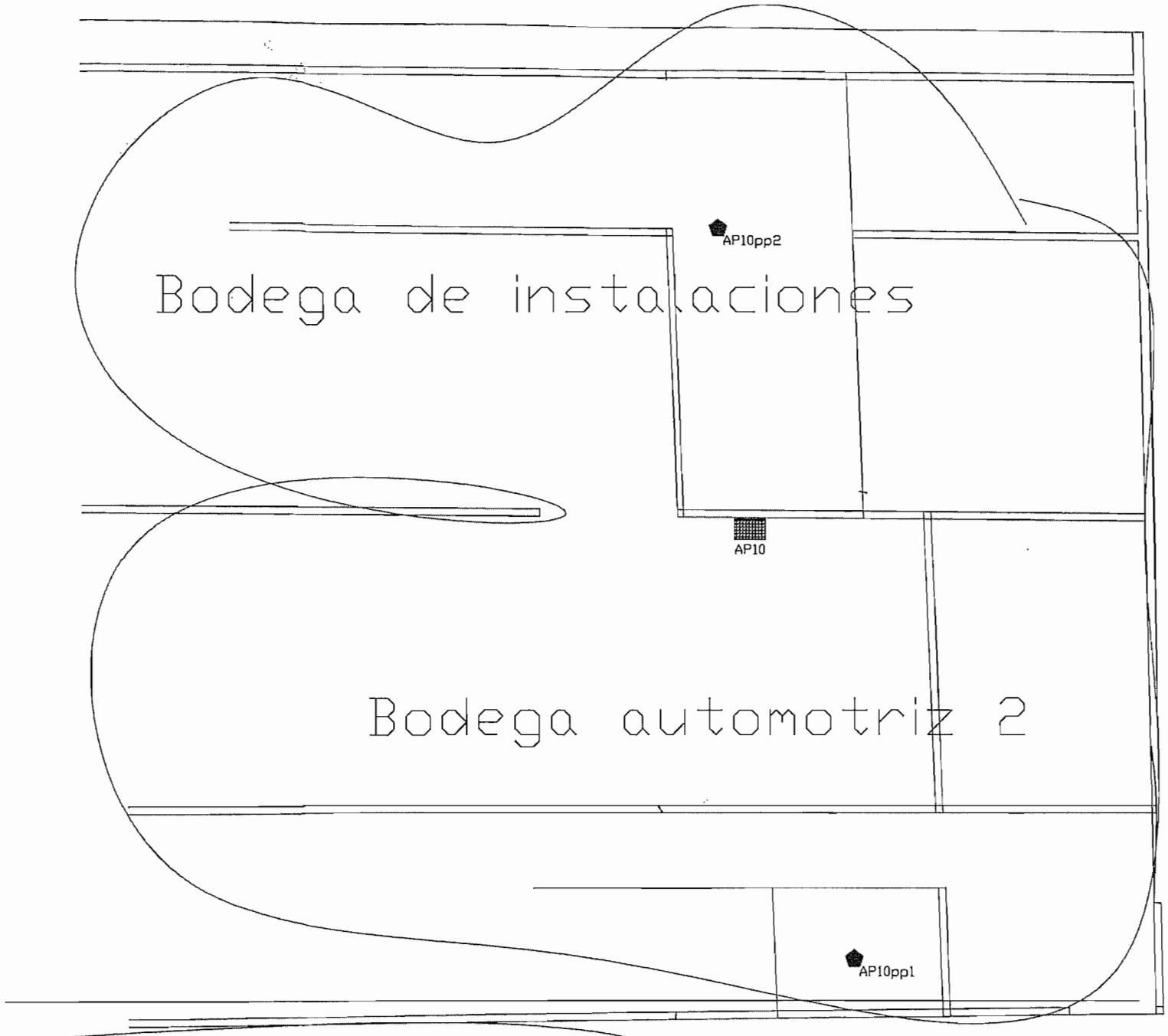

AP5pp4
Bodega automotriz 1
AP5pp3
Clientes Especiales
AP5
Edificio Polifuncional
Planta Baja
AP3pp3
AP5pp2
AP5pp1
AP3pp4
Laboratorio de medi


Departamento de Personal
12,92
14,42
AP6pp5
AP6pp4
Edificación
Acometidas
21,23
AP6
AP6pp3
AP6pp2
oficina
Departamento de
Acometidas
16,77
AP6pp1
AP9pp4
AP9pp1
AP9pp3
12,75


27,41
16,96
Taller Industrial
AP7pp4
17,25
AP7
AP7pp1
Laboratorio de
Transformadores
AP7pp2
29,08
Taller
10,19
Laboratorio de
trasnformadores
AP7pp3
23,13
Sección
Grúas


Mecánica
Automotriz
Gasolinera
AP8
AP8pp1
AP8pp2
AP8pp3
40,22
23,13


AP9pp1
AP9pp2
AP9pp3
AP9pp4
AP9
12.75
Operación y
Mantenimiento Urbano


AP10pp2
Bodega de instalaciones
AP10
Bodega automotriz 2
AP10pp1

12.34
PÉRDIDAS COMERCIALES
AP11pp2
AP11pp1
31.63
AP11pp3
CONSTRUCCIÓN DE REDES
AP11pp4
Edificación
Construcción de Redes

Anexo 6.
Proforma Referencial

Routers
switches L2-L3
Firewall VoIP

cableado cat 6
fibra optica
30 años garantia

administracion
de ancho banda

Open Source
IP-PBX linux
Windows

Firewall 3ra
generacion
Antivirus, IDS

switch s L2-L3

Central IP-PBX
Conference
Manager

Balanceadores
de Tráfico de
Aplicación(L7)

Acceso Remoto
SSL VPN
Remote Desktop

Telefonos IP
Analog Gateway
ATAs

Tarjetas FXO
FXS TI, E1

Telefonos SIP,
SIP proxy, SIP
Regist. IP-PBX

Conmutadores
Keyboard Video
Mouse IP

Centrales PBX
IP- Hibridas

Switches de
Metropolitan
Area Networks

Equipos 802.11a
Inalambricos,
HotSpots, MAN

Firewalls SIP
Traversal NAT

EvolutioNet CIA. LTDA.
Internet Solution Providers

PROFORMA #2005-40

FECHA: 14 de Julio del 2005
NOMBRE: Sr. Alvaro Cadena
EMPRESA: Empresa Electrica Quito S.A.
TELFAX:
E-MAIL:

PROYECTO: Diseño y Pruebas de campo de una Red Inalambrica para la Empresa Electrica Quito campus El Dorado empleando IEEE 802.11g

CANTIDAD	DESCRIPCION	P. UNITAR.	PRECIO
11	Punto de acceso Cisco Aironet serie 1200 Manejo de IEEE 802.11g Banda 2.4 GHz Velocidades 1, 2, 5.5, 11, 24, 36, 48, 54 Mbps Seguridad WEP, WPA, TKIP, EAP, LEAP, LEAP-TLS Puerto Ethernet de uplink 10/100 Mbps autosensing Acceso Web, Consola, Telnet Cisco IOS Software versión 12.2(13)JA o superior. Protocolo CSMA/CA Antena Cisco AIR-ANT-1728	$ 989,00	$ 10.879,00
66	Adaptador PCI Cisco Aironet 802.11a/b/g	$ 274,00	$ 18.084,00
7	Adaptador Cliente PC Card Cisco 802.11a/b/g	$ 186,00	$ 1.302,00
1	PATCH PANEL de conexiones de 24 puertos tipo RJ45 categoría 5e para distribución de cables tipo UTP de cuatro pares completo y armado	$ 80,00	$ 80,00
1	RACK estándar, tipo abierto de sistema estructurado de 19" de ancho por 42" de alto, con dos parantes verticales y bases de soporte cat5e	$ 90,00	$ 90,00
3	Bobinas de 305m cable UTP cat5e	$ 80,00	$ 240,00
130	Metros de Fibra óptica ADSS multimodo 62.5/125mm, 4hilos, supervision de montaje, certificacion de 4 hilos, mano de obra	$ 4,50	$ 585,00
4	Pigtails multimodo de conexión Fibra Fusión mediante pitillos	$ 15,00	$ 60,00
2	Caja para instalación fibra óptica	$ 125,00	$ 250,00

2	Convertidor de medio fibra óptica multimodo con conectividad ST – FastEthernet 10/100 Mbps	$ 220,00	$ 440,00
1	Organizador vertical para Rack 60*40 simple	$ 35,00	$ 35,00
1	Organizador horizontal para Rack 19" 2 UR	$ 19,00	$ 19,00
1	Supresor de energía de 8 tomas	$ 6,00	$ 6,00
39	CANALETAS de 2m con capacidad para 2 cables UTP cat5 tipo panduit	$ 1,80	$ 70,20
396	Metros de manguera PVC 1"	$ 0,20	$ 79,20
20	CODOS para canaleta con capacidad para 2 cables UTP cat5 de pared MP	$ 0,90	$ 18,00
20	UNIONES para canaleta de 2m con capacidad para 2 cables UTP cat5 de pared	$ 0,90	$ 18,00
11	Patch cords de 1m cat5e Quest	$ 3,50	$ 38,50

Tiempo de entrega: 15 días laborables		SUBTOTAL	$ 32.293,90
Garantía: 1 año defectos fábrica		IVA	$ 3.875,27
Forma de pago: Contraentrega	VICTOR ULLOA	TOTAL	**$ 36.169,17**

Av Paez N 24-42 Y Cordero TelFax 593-2-2527851 593-9-9551667
www.evolutionet-ec.com sales@evolutionet-ec.com evonet@uio.satnet.net
RUC 1791714148001