UNIVERSIDAD DE EL SALVADOR
FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA DE INGENIERÍA ELÉCTRICA

"Implementación de Comunicaciones Inalámbricas de Espectro Ensanchado"

PRESENTADO POR:

VICTOR ANTONIO ASCENCIO CAMPOS

PARA OPTAR AL TÍTULO DE:
INGENIERO ELECTRICISTA

CIUDAD UNIVERSITARIA, OCTUBRE DE 2005

UNIVERSIDAD DE EL SALVADOR

RECTORA :

DRA. MARIA ISABEL RODRÍGUEZ

SECRETARIA GENERAL:

LICDA. LIDIA MARGARITA RIVAS DE RECINOS

FACULTAD DE INGENIERÍA Y ARQUITECTURA

DECANO :

ING. MARIO ROBERTO NIETO LOVO

SECRETARIO :

ING. OSCAR EDUARDO MARROQUIN HERNÁNDEZ

ESCUELA DE INGENIERÍA ELÉCTRICA

DIRECTOR :

ING. LUIS ROBERTO CHÉVEZ PAZ

UNIVERSIDAD DE EL SALVADOR.
FACULTAD DE INGENIERÍA Y ARQUITECTURA.
ESCUELA DE INGENIERÍA ELÉCTRICA

Trabajo de Graduación previo a la opción al Grado de:
INGENIERO ELECTRICISTA

Título :

"Implementación de Comunicaciones Inalámbricas de Espectro Ensanchado"

Presentado por :
VICTOR ANTONIO ASCENCIO CAMPOS

Trabajo de Graduación aprobado por:

Docente Director:
ING. LUIS ROBERTO CHEVÉZ PAZ

San Salvador, Octubre de 2005

Trabajo de Graduación Aprobado por:

Docente Director:

ING. LUIS ROBERTO CHEVÉZ PAZ

Trabajo dedicado a:

Jehová Dios Todopoderoso, por haberme dado la vida, fuerzas y sabiduría para completar con éxito una carrera universitaria.

A mi Madre Delmy Campos y mi Abuela Rosario Sigarán por haberme cuidado e instruido, guiado y apoyado en esta ardua carrera.

A mi esposa Mónica por su apoyo en el transcurso de la elaboración de dicho trabajo, y a los maestros y encargados de laboratorio que en el transcurso de la carrera han contribuido a mi formación académica, les dedico este trabajo de graduación.

Victor Antonio Ascencio Campos.

INTRODUCCIÓN.

De todos es conocido que la infraestructura de telecomunicaciones de la UES mejoró luego de la realización de los juegos deportivos Centroamericanos y del Caribe en el año 2003; la principal mejora, se observa en la red LAN, no obstante la misma no alcanzó a todos por igual, de tal forma que aún existen muchos puntos al interior de la universidad que no cuentan con acceso a la red LAN, principalmente por su ubicación física, limitando con ello tanto las actividades Administrativas como Académicas desarrolladas en dichos puntos. Sumado a lo anterior, las expectativas de ampliación de la red son muy escasas, tanto por cuestiones económicas como culturales al interior de la UES.

Por lo antes expuesto, cualquier opción de bajo costo que permita incrementar el acceso a la red LAN a los usuarios hasta ahora excluidos, consideramos que puede ser bienvenida, dentro de tales alternativas se encuentran las redes inalámbricas de banda ancha, conocidas como redes WIFI o WLAN. Este tipo de tecnología permite ofrecer conectividad a red (con una mínima inversión) a puntos de difícil acceso, no solo al interior de edificios; sino también en áreas o espacios abiertos tales como plazas, canchas deportivas, salones de clases, etc.

El presente trabajo tiene como meta proponer el diseño de una red WIFI para la FIA, y persigue a su vez dejar montado un prototipo que demuestre las bondades de esta tecnología.

Para ello, se explicará la propuesta dada en el presente documento, de la siguiente manera:

En el capítulo I, se explica los aspectos de seguridad considerados por el estándar 802.11 el cual es la norma que debe tomarse en cuenta a la hora de diseñar redes inalámbricas.

El capítulo II, trata acerca de los aspectos técnicos, legales y económicos, que deben considerarse para el diseño de la red.

El capítulo III, presenta los resultados del estudio de campo realizado, la calidad de cobertura a ofrecer, y los equipos utilizados para realizar dicho estudio.

El capítulo IV, en este se presenta el diseño final de la red, la inversión económica y los equipos necesarios para su implementación.

TABLA DE CONTENIDOS.

Capítulo **Página**

LISTA DE TABLAS.

LISTA DE FIGURAS.

CAPÍTULO I

CONCEPTOS GENERALES

1.0 INTRODUCCIÓN.

Como se menciono antes, el objetivo de este trabajo es proponer el diseño de la red WIFI de la FIA, para lo cual se tomarán en cuenta tanto, la norma IEEE 802.11 como las particularidades del entorno físico de la facultad, las cuales determinan las zonas de cobertura y los diferentes grados de calidad de servicio (QOS) que se pueden ofrecer.

Un aspecto muy importante que se debe tomar en cuenta en este tipo de aplicaciones es lo relacionado con la seguridad, ya que al permitir acceso inalámbrico libre a la red LAN, puede propiciar ataques de usuarios con no muy buenas intenciones, que podrían presentar situaciones de riesgo en cuanto a la información a la que se pueda tener acceso. En ese sentido, es necesario considerar diferentes alternativas de seguridad, para proteger la información disponible, así como los servicios a ofrecer, a fin de minimizar los riesgos planteados por la situación anterior.

1.1 CONCEPTOS PRELIMINARES.

El modelo básico de una red WIFI, es el mostrado en la figura 1.1, el cual a su vez se utilizará para describir la red propuesta para la FIA.

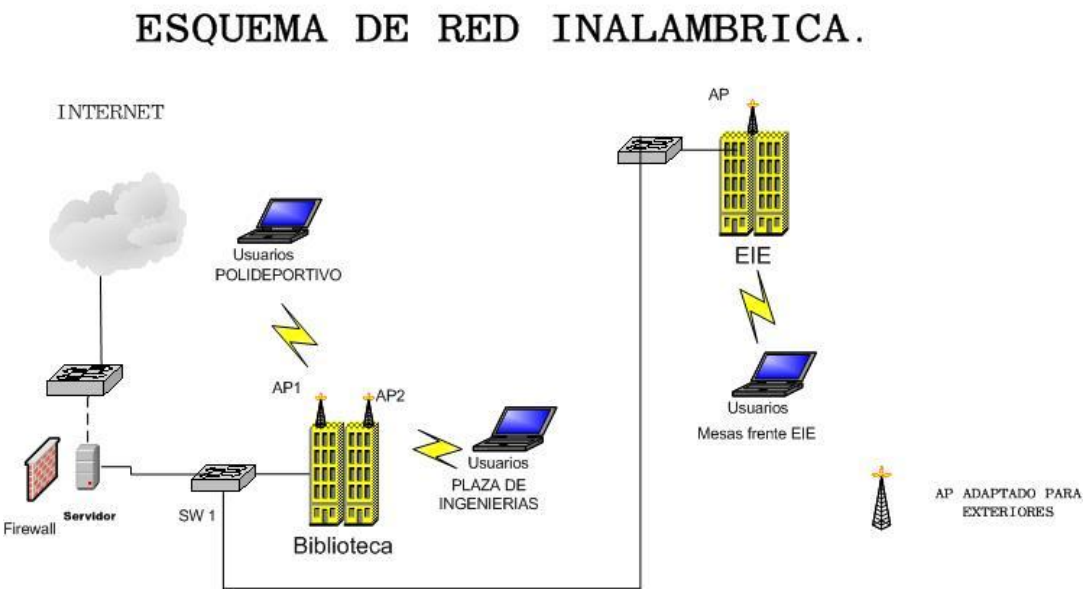


Figura 1.1 Esquema de red propuesta.

En el esquema anterior, resaltan los componentes siguientes:

Punto de acceso (AP): Es el dispositivo que provee la interconexión entre la red de área local (LAN) y la inalámbrica (WLAN), en estos equipos se determinan los parámetros siguientes:

- La velocidad de máxima de transmisión de datos en la red WIFI.
- El método de seguridad empleado.
- La potencia de transmisión máxima, el canal radio eléctrico a utilizar y otros aspectos que se describirán mas adelante.

El AP dispone de una interfase ethernet y otra de RF que opera a 2.4 Ghz. La mayoría de estos dispositivos viene equipado con una antena de baja ganancia para instalaciones INDOOR, también existen modelos diseñados para funcionamiento OUTDOOR (exterior), con la desventaja que su costo excede aproximadamente en un 150% comparado con el de los equipos INDOOR, razón por la cual se propone la construcción de antenas de bajo costo y alta ganancia, que permitan cubrir zonas amplias en exterior, sin hacer uso de equipos OUTDOOR:

Para la implementación del prototipo propuesto, se utilizó el punto de acceso de marca Orinoco y modelo AP-2000. (El anexo F presenta la hoja de especificaciones de éste equipo).

En cuanto a **las antenas**, se han elegido diseños que utilizan materiales fáciles de obtener en el mercado local, ya sea en tiendas especializadas en equipos electrónicos o incluso ferreterías.

Por otra parte, para el diseño de la red, deben tomarse en cuenta las técnicas básicas para el diseño de radio enlaces a fin de optimizar la ubicación de los puntos de acceso de forma que se pueda lograr la máxima cobertura posible, mejorando la eficiencia espectral de la red.

Los edificios en los cuales se realizaron pruebas de campo fueron la Biblioteca de las Ingenierías y la Escuela de Ingeniería Eléctrica (EIE). Se eligieron estos dos puntos ya que, en el caso del edificio de la EIE, es donde se propone dejar instalado el sistema prototipo, y en el edificio de la biblioteca, por su ubicación estratégica para proveer conectividad no solo a la plaza central de la FIA, sino también al Polideportivo.
En el esquema de la red propuesto, también se hace referencia al servidor de autenticación, el cual es indispensable dado a que será el encargado de proveer tanto la conexión a Internet, como de administrar la seguridad (limitando el

acceso a los recursos de la red), evitando con ello que algunas personas puedan hacer mal uso de la información o que pudieran desperdiciar el ancho de banda disponible al utilizar programas de p2p. En este servidor se propone configurar los servicios de firewall y DHCP.

Adicionalmente se sugiere implementar un sistema de seguridad más robusto para WLAN, por medio de la implementación del servicio conocido como RADIUS-EAP.

En el caso de los clientes, la red propuesta se ha diseñado de manera tal que solamente necesiten tener instalado en su equipo una tarjeta de red inalámbrica, configurada por DHCP, y la contraseña de autenticación.

Para establecer el grado de servicio de la red, fue necesario realizar un muestreo de niveles de señal, y con ello se elaboró un mapa de cobertura, en el cual se indica de forma gráfica la calidad de servicio disponible en las diferentes zonas propuestas para la FIA. El mapa en cuestión se presenta en el Anexo G.

1.2 EL ESTÁNDAR IEEE 802.11.CONSIDERACIONES SOBRE LA SEGURIDAD.

Tomando en cuenta el modelo de AP utilizado (Orinoco AP 2000), la seguridad en la red WIFI propuesta, podría ser administrada por cualquiera de los métodos siguientes:

- Privacidad equivalente LAN.
- Red Privada virtual
- IEEE 802.1X
- WPA (WI-FI Protected Access)
- IEEE 802.11i

Cada método tiene ventajas y desventajas dependiendo de su aplicación y de los requerimientos de seguridad deseados en la red a instalar. Esto se detalla a continuación.

1.2.1 PRIVACIDAD EQUIVALENTE LAN. (WIRED EQUIVALENT PRIVACY WEP)

El algoritmo WEP forma parte de la norma IEEE 802.11, y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante el cifrado de la información utilizando un método llamado RC4.
El algoritmo WEP resuelve aparentemente el problema seguridad, entre emisor y receptor. Sin embargo, existen dos situaciones que hacen que WEP no sea seguro.

a) En primer lugar, éste genera un vector de inicialización aleatorio con el cual se hace el cifrado de información, el método es fácilmente predecible.

b) La segunda vulnerabilidad de WEP, es que permite recuperar la clave RC4, recopilando un gran número (entre 2000 a 4000) de mensajes y vectores de iniciación. Razón por la cual WEP no es un método confiable para asegurar las redes inalámbricas.

No obstante lo anterior, tiene la ventaja que es soportado por todas las tarjetas de red y *AP,* debido a que *WEP* forma parte del estándar IEEE 802.11.

La figura 1.2 muestra una ventana de configuración típica del WEP.

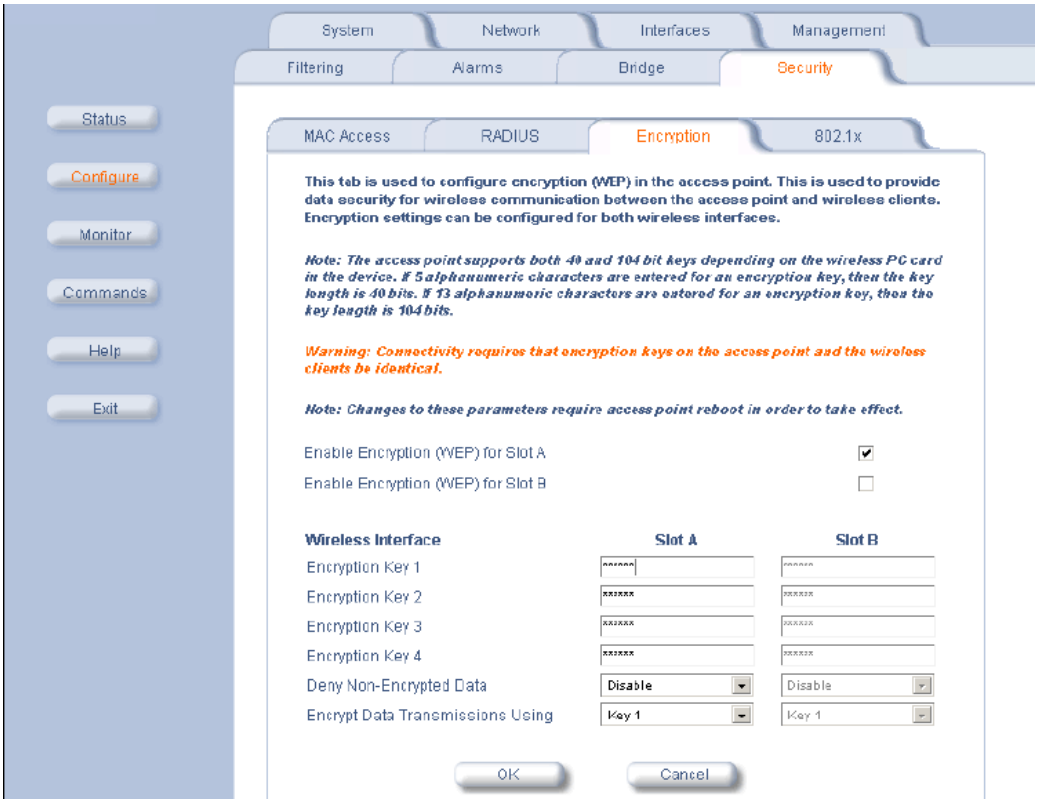


Figura 1.2 Configuración de encriptación WEP en ORINOCO AP-2000.
En el diseño, de la red propuesta no se utilizará este método, aunque es de fácil configuración, la seguridad que provee es mínima.

1.2.2 RED PRIVADA VIRTUAL (VIRTUAL PRIVATE NETWORK, VPN):

Debido a las fallas de seguridad descritas en las sección anterior, los fabricantes de equipos inalámbricos han tomado varias medidas independientes al estándar 802.11, para fortalecer la seguridad en las redes inalámbricas, algunas de estas investigaciones han llegado a ser la base sobre la cual se creo la norma IEEE

802.11i. En el caso de las VPN emplean tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. Las VPN resultan especialmente atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico.

Los servidores de VPN se encargan de autenticar y autorizar a los clientes inalámbricos, y de cifrar todo el tráfico desde y hacia dichos clientes. Dado que los datos se cifran en un nivel superior del modelo OSI, no es necesario emplear WEP, para esta configuración.

Este método, puede ser aplicable a las conexiones punto a punto, entre oficinas administrativas, ya que provee un grado de seguridad superior con respecto a WEP, aunque tiene la desventaja que hay que instalar software especializado para su utilización en los equipos de los usuarios finales, lo cual puede llegar a ser un proceso difícil tomando en cuenta los posibles usuarios de Internet inalámbrico en la FIA.

1.2.3 IEEE 802.1X (PORT BASED NETWORK ACCESS CONTROL).

La norma IEEE 802.1X es utilizada para ampliar el nivel de seguridad en redes inalámbricas, con ella se establecen las reglas de autenticación por medio de la identificación de los usuarios en un sistema centralizado, utilizando el protocolo **EAP** (Extensible Authentication Protocol) de amplia aplicación en redes ethernet, token Ring y ahora en las redes inalámbricas, para intercambiar mensajes durante el proceso de autenticación con los servidores. Aunque IEEE 802.1X ha sido diseñada para controlar puertos físicos, en las redes inalámbricas cada conexión entre el punto de acceso y cada Equipo Terminal se ve como una conexión independiente, mediante un puerto o conexión lógica, como se ejemplifica en la figura 1.5.

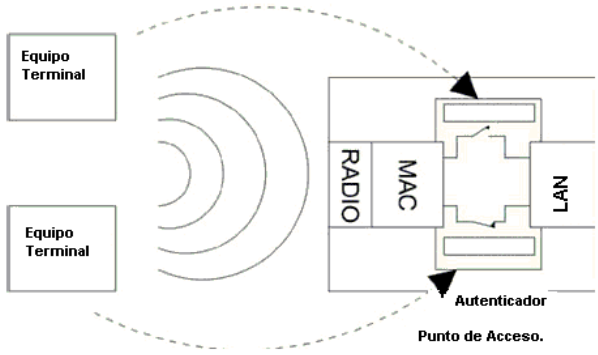


Figura 1.3 Conexiones lógicas en IEEE 802.1X en un punto de acceso.

En cuanto al servidor de autenticación puede ser: RADIUS (Remote Authentication Dial In User Service) o Kerberos, ya que la norma 802.1X, no

especifica cual utilizar, el *servidor* intercambiará el nombre y credencial de cada usuario.

Para ofrecer control de acceso al puerto entre las estaciones inalámbricas (suplicantes), los puntos de acceso (autenticador) y servidores. Para que la autenticación funcione, la transmisión del usuario debe efectuarse a través de un punto de acceso LAN inalámbrico para alcanzar el servidor (RADIUS) que lleva a cabo la autenticación, esto debe configurarse en el punto de acceso, como se muestra en la figura 1.4 y 1.5.

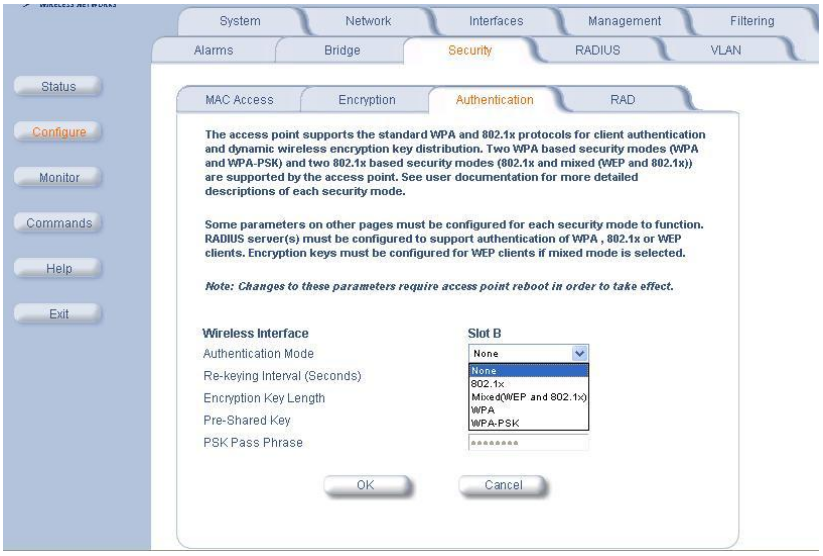


Figura 1.4 Configuración de tipo de autenticación en el AP.

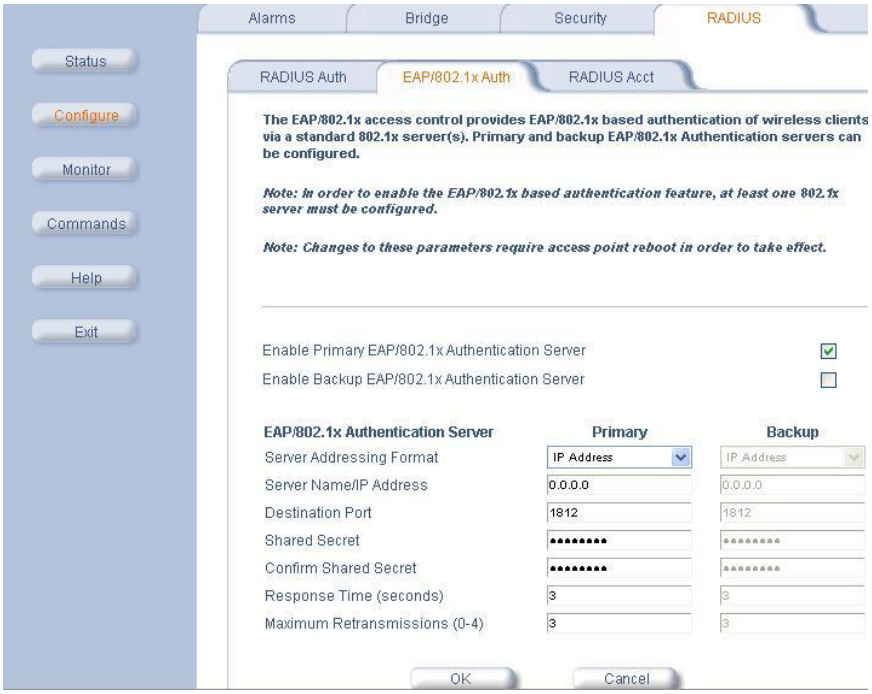


Figura 1.5 Configuración del servidor de la dirección IP del servidor de autenticación.

Para el caso del la red propuesta, se recomienda la puesta en marcha del servidor RADIUS, ya que no fue posible configurarla en el presente trabajo.

1.2.4 WPA (WI-FI Protected Access).

WPA es un estándar propuesto por los miembros de WI-FI y con él se espera superar las fallas de seguridad de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación. Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP (Temporary Key Integrity Protocol). Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave.

Igualmente se mejoraron los algoritmos de cifrado de trama y de generación de los vectores de inicialización, con respecto a WEP.

Según la complejidad de la red, un punto de acceso compatible con WPA puede operar en dos modalidades:

• Modalidad de red empresarial:

Para operar en esta modalidad se requiere de la existencia de un servidor RADIUS en la red. El punto de acceso emplea entonces 802.1X y EAP para la

autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.

• Modalidad de red doméstica, o PSK (Pre-Shared Key):

WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso.

1.2.5 IEEE 802.11i

La norma IEEE 802.11i es una norma para seguridad de redes inalámbricas.

Se puede resumir en tres partes principales:

a. Protocolo de integridad de llave temporal (TKIP).

b. Protocolo modo contador. CBC-MAC (CCMP).

c. Protocolo de autenticación de puertos (IEEE 802.1X) + manejo de llaves.

IEEE 802.11i se resume como la modificación de WPA a WPA2, que incluye el nuevo algoritmo de cifrado AES (Advanced Encryption Standard), desarrollado por el NIST (nacional Institute of Standard). Se trata de un algoritmo cifrado por bloques, con claves de 128, 192 y 256 bits y en bloques de 128 bits de tamaño.

La mayor parte de hardware con la certificación Wi-Fi puede actualizarse, para ser compatible con este cifrado, por medio de software ya sea por medio de los controladores de las tarjetas de red o firmware para los routers o puntos de acceso inalámbricos

La diferencia entre WPA y WPA2 reside en el método de cifrado de datos, así:

TSN = TKIP + 802.1X = WPA.

RSN = CCMP + 802.1X = WPA2.

Después de examinar los distintos métodos de cifrado y autenticación, se decidió utilizar el WPA-PSK, debido que es la configuración mas adecuada (sin utilizar un servidor RADIUS).

1.3 GLOSARIO.

CONTROL DE ACCESO: Es la previsión del uso no autorizado de los recursos de la red.

AP (Acces Point): Son equipos que tienen como función principal proveer el acceso para la distribución de servicios, por medio de inalámbricos “wireless médium” (WM) y permitir la asociación de estaciones [6]

AD HOC: Es una configuración de red, en la cual los equipos móviles se conectan unos con otros, sin necesidad de que exista un punto de acceso. El tipo de conformación más común es en estrella; se emplea por lo general cuando se desea ofrecer acceso inalámbrico a una red alambrada ya existente. [3]

ASOCIACIÓN: Este servicio es usado para establecer la relación entre punto de acceso/estación (AP/STA), establece la ruta y habilita a la STA a la invocación del sistema de distribución de servicios “distribution system services” (DSSs). [6]

AUTENTICACIÓN: Este servicio es usado para establecer la identidad de una estación o grupo de estaciones para que puedan tener la capacidad de asociarse con otras estaciones. [6]

CONFIGURACIÓN BÁSICA DE SERVICIO “Basic Service Set” (BSS): Es un arreglo de estaciones controladas por una única función de coordinación. [6]

ÁREA DE SERVICIO BÁSICO “Basic Service Área” (BSA): Es el área conceptual en la cual los miembros de una BBS puedan comunicarse. [6]

CANAL: Es una instancia del medio que se usa para el envió de unidades de protocolo de datos (PDUs), que puede ser usado simultáneamente, en un mismo espacio, por otras instancias (uso de otros canales), en la misma capa física “Physical Layer” (PHY). Con una baja relación de errores e interferencia mutua. Algunas PHYs proveen un solo canal, mientras que otros proporcionan varios canales. [6]

DIRECCIÓN DE BROADCAST: Es cuando se asigna una sola dirección de multicast para todas las estaciones. [6]

ESTACIONES DE SERVICIO (SS): El sistema de los servicios que soportan el transporte de Control de Acceso Medio (MAC) Servicio de Unidades Datos (MSDUs) entre las estaciones dentro de un Sistema del Servicio Básico (BSS). [6]

FUNCIÓN DE COORDINACIÓN DISTRIBUIDA (DCF): Esta se da cuando está activa la misma lógica de la función de la coordinación en cada estación de la

configuración del servicio básico (BSS) siempre que la red esté en la operación. [6]

FUNCIÓN DE COORDINACIÓN (CF): La función lógica de coordinación determina cuando una estación tendrá acceso al BBS, para el envió y recepción de unidades de protocolo de datos “Protocol Data Units” (PDUs) por el medio inalámbrico “wireless médium” (WM). La función de coordinación puede tener un solo punto (PCF) o puede tener una función de coordinación distribuida (DCF). [6]

DESAUTENTICACIÓN: El servicio no acepta o rechaza una relación de autenticación existente. [6]

PORTAL: El punto lógico en el cual el control de acceso al media (MAC) unidades de servicio de datos (MSDUs) que no proceden de una red IEEE 802.11 (LAN) se incorporan al sistema de distribución (DS) de un sistema extendido del servicio (ESS).

SISTEMA DE DISTRIBUCIÓN (DS): Es el sistema utilizado para interconectar una configuración de servicios básicos (BSSs) e integrarlo con la red de área local (LAN) para crear un arreglo de servicio extendido (ESS).

SERVICIO DE SISTEMA DE DISTRIBUCIÓN (DSS): El sistema de servicios proporcionado por el sistema de la distribución (DS) permiten el control de acceso medio (MAC) para enviar las MAC a las unidades de servicio de datos (MSDUs) entre las estaciones que no están en comunicación directa, sobre un solo caso del medio inalámbrico (WM). Estos servicios incluyen el transporte de MSDUs entre los puntos de acceso (AP) de los sistemas del servicio básico (BSSs) dentro de un sistema extendido del servicio (ESS), el transporte de MSDUs entre los portales y BSSs dentro de un ESS, y el transporte de MSDUs entre las estaciones en el mismo BSS, donde la dirección destino es única, pero la estación que envía el MSDU elige al DSS. El DSSs es proporcionado entre los dos equipos inalámbricos.

WEP (Wired Equivalent Privacy): Es un algoritmo de encriptación del estándar 802.11, originalmente diseñado para proveer seguridad a las WLANs con el mismo nivel de privacidad disponible en las redes cableadas. WEP utiliza una llave secreta compartida entre los nodos de la red inalámbrica encriptando los frames (capa 2, Enlace de Datos), y mediante la llave secreta compartida en la transmisión, es posible descifrar el mensaje. Estas llaves secretas pueden ser de 40 y 128 bits, generadas por un algoritmo Generador de Números Pseudo Aleatorios (PRNG, Pseudos Random Number Generator). Cuando se habilita esta función, cada estación (tanto clientes como puntos de acceso) tiene una clave que se utiliza para cifrar los datos antes de transmitirlos por las ondas de radio. Si una estación recibe un paquete que no se encuentra cifrado con la clave apropiada, el paquete es desechado y no es entregado al host; de esta

manera se evita el acceso no autorizado y la recepción de señal no autorizada. [3]

SSID (Service Set Identifler): Es una identificación que se anexa a cada paquete enviado a través de la red, y opera como una clave que da acceso a la red, todos los puentes inalámbricos y puntos de acceso usan la misma SSID, los paquetes con otro SSID son ignorados, esto también aplica para los usuarios inalámbricos (clientes). El SSID no provee ningún tipo de funciones de seguridad contra la data, ni tampoco una autenticación de los clientes que intentan asociarse al punto de acceso. El SSID es publicado en los frames del mensaje de bandera o faro (beacon) que se envían a los puntos de acceso para obtener el servicio de red, los mensajes de bandera son transparentes para el usuario. [3]

ESTACIONES (STA): Es cualquier dispositivo que contenga el estándar IEEE 802.11 de acuerdo al control de acceso al medio (MAC) y en la capa física (PHY) utilice el espacio libre como medio (WM). [6]

WLAN: Wireless Local Área Network, es un tipo de redes de área local en la que los usuarios se conectan de forma inalámbrica [4]

WIFI (Wireless Fidelity): Es un nombre comercial desarrollado por un grupo de comercio industrial llamado WiFi Alliance (Inicalmente: 3Com – Aironet [hoy parte de CISCO] – Harris – Lucent – Nokia y Symbol technologies, hoy más de 150 miembros), el nombre “oficial” de esta alianza es WECA (Wireless Ethernet Compatibility Alliance) y son los primeros responsables de 802.11b. [8]

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

CONCLUSIONES DEL CAPÍTULO I.

- Conforme a lo expuesto en el presente capítulo y los servicios a ser ofrecidos por la red, se establece como método de seguridad el WPA, con lo cual se puede ofrece un nivel de seguridad aceptable, el cual puede ser complementado por otras técnicas o métodos que puedan ser configurados por el Administrador de la Red

- El uso de IEEE 802.1X supera las fallas de seguridad de las redes inalámbricas, por lo que en los casos en los que la seguridad es indispensable, debe utilizarse esta norma.

REFERENCIAS BIBLIOGRÁFICAS CAPÍTULO I.

[1] Introduction to Wireless Local Area Network (WLAN)
Lawrence Harte, 2004

[2] IEEE Communications Magazine.
Agosto 1996. Articulo: Wireless LANs and Mobile Networking: Sta Standards and Future Directions. By Richard O. LaMaire, Arvind Kristina, and Pravin Bhagwat, IBM James, Erricson Inc. pag 86 – 94

[3] El NoticIEEEro Volumen 31, Número 3 Septiembre 2003.
Desafíos de Seguridad en las Redes Inalámbricas IEEE 802.11b
Carlos H. Kan,

[4] La revista de Villagüeb
http://villanos.net/revista/200301/wifi.html
Escrito por José A. Gelado

[5] El estándar IEEE 802.11 Wireless LAN
Francisco López Ortiz

[6] ANSI/IEEE Std 802.11, 1999 Edition (R2003)
Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
LAN MAN Standards Committee of the IEEE Computer Society
Reaffirmed 12 June 2003
IEEE-SA Standards Board.

[7] IEEE Std 802.11b-1999 (R2003)
Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band
LAN/MAN Standards Committee of the IEEE Computer Society
Approved 16 September 1999 IEEE-SA Standards Board

[8] Real 802.11 Security: Wi-Fi Protecteced Acces and 802.11i
By Jon Edney, William A. Arbaugh, July 15, 2003
ISBN: 0-321-13620-9

[9] Seguridad en redes inalámbricas 802.11
Juan Manuel Madrid Molina
Publicación de Sistemas y telematica, Universidad Icesi abril, 2004,

CAPÍTULO II

ASPECTOS TÉCNICOS Y LEGALES, PARA EL DISEÑO DE REDES INALÁMBRICAS.

2.0 INTRODUCCIÓN.

Un aspecto adicional que debe ser tomado en cuenta para el diseño de redes WIFI es la elección de los canales de radio, en los cuales operan este tipo de redes. Estos canales determinarán cobertura, número de usuarios, costos, etc. En ese sentido, es necesario mencionar los aspectos técnicos que limitan estas aplicaciones así como el marco legal que regula estas aplicaciones en nuestro país a través de la Superintendencia General de Telecomunicaciones (SIGET). Todo lo anterior será abordado en los numerales siguientes.

2.1 MARCO LEGAL DEL USO DEL ESPECTRO DE FRECUENCIAS.

Antes de realizar cualquier transmisión en el espacio libre, es necesario tomar en cuenta el marco legal, para evitar las posibles repercusiones legales.

La Superintendencia General de Telecomunicaciones (SIGET) regula el uso del espectro de frecuencias en El Salvador, tal acción la realiza basada en el documento de **(CNAF)**, en éste se hacen las siguientes referencias en cuanto al uso de las frecuencias para redes WI-FI:

"La banda 2,400 – 2,500 MHz designada para aplicaciones industriales, científicas y medicas (ICM) con una frecuencia central de 2,450 MHz, banda 2,400 – 2,843.5 MHz podrá ser utilizada por la tecnología espectro ensanchado, también denominada "SPREAD SPECTRUM" bajo las siguientes condiciones de operación: Los equipos que operen en esta banda, así como otras, determinadas por el CNAF, con potencias que no excederán de 1 watt a la salida del transmisor, con antenas de ganancia máxima de 6 dBi, es decir que la máxima potencia radiada no excederá de 6 dBWatts (aprox. 3.98 vatios). De exceder la ganancia antes señalada, se deberá limitar la potencia de salida del transmisor por la misma cantidad de dB excedidos en la ganancia de la antena transmisora. No se ofrecerá protección contra interferencias perjudiciales, a quienes utilicen esta tecnología. Esta banda es de uso libre." [1]

Basados en lo anterior, se puede hacer uso sin ningún problema legal de la frecuencia 2.4 Ghz siempre y cuando no se cause interferencia a ningún otro usuario.

2.2 RADIOCANALES.

La red puede implementarse utilizando un solo AP, lo que reduciría enormemente su cobertura, misma que puede mejorarse por medio de la antena a utilizar (como se explica en el capitulo siguiente). Otra opción es colocar un arreglo de puntos de acceso, ubicados en diferentes puntos con la cual se provee una mejor cobertura (aunque incrementa los costos).

En cuanto a la segunda opción, la norma IEEE 802.11b especifica 11 posibles intercepciones de frecuencias para poder transmitir. Es recomendable utilizar frecuencias distintas a las que utilizan los teléfonos inalámbricos. Utilizar distintos canales, es una técnica que permite evitar el ruido que degrada el funcionamiento de la red, y además permite que múltiples puntos de acceso puedan conectarse en un mismo espacio físico mejorando con ello la eficiencia espectral.

Un arreglo de varios puntos de acceso conlleva mayor complejidad, que el utilizar un solo punto de acceso. Sin embargo permite atender mayor cantidad de usuarios con un buen grado de servicio.

Un posible esquema de instalación es el mostrado en la figura 2.1

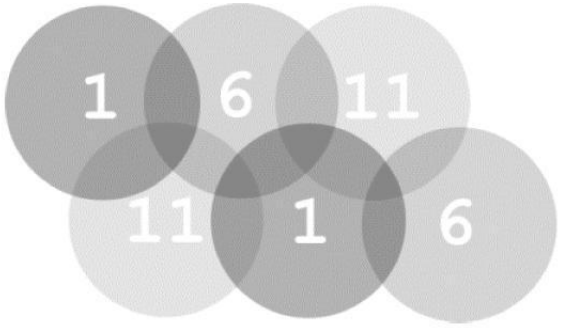


Figura 2.1 Distribución de canales de transmisión para cobertura total.

En el esquema anterior, los números de los círculos establecen la distribución de los radiocanales a utilizar (y a cada uno de ellos corresponde una frecuencia en la banda de 2.4 Ghz). La distribución de canales planteada, está basada en la recomendación de la IEEE dada en la norma IEEE 802.11

La razón por la que se escogen los canales 1, 6 y 11 es por que en dichos canales los lóbulos principales están separados de forma que no interfieren entre si; en forma espectral, la distribución de los canales arriba indicados se muestra en la figura 2.2.

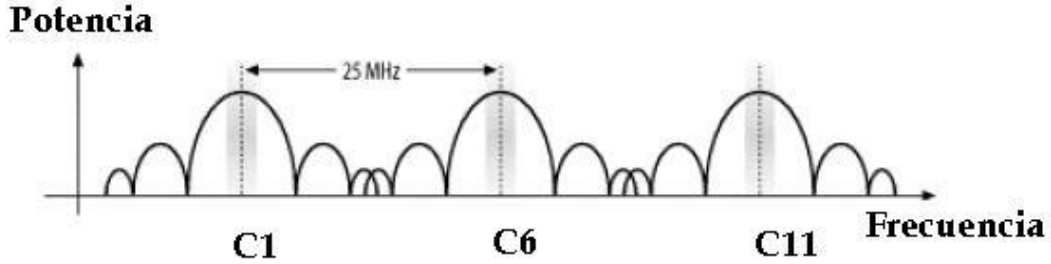


Figura 2.2 Separación de canales en redes 802.11

La tabla 2.1 muestra la correspondencia entre el número de canal y su radiofrecuencia respectiva, tal como lo consideran diferentes entidades normalizadoras (FCC, ETSI, etc.).

Frecuencias utilizadas por los entes reguladores.				
Canal	EUU FCC MHz	ETSI Europa MHz	Francia MHz	Japón MHz
1	2412	2412	-	2412
2	2417	2417	-	2417
3	2422	2422	-	2422
4	2427	2427	-	2427
5	2432	2432	-	2432
6	2437	2437	-	2437
7	2442	2442	-	2442
8	2447	2447	-	2447
9	2452	2452	-	2452
10	2457	2457	2457	2457
11	2462	2462	**2462**	2462
12	-	2467	2467	2467
13	-	2472	2472	2472
14				2484

Tabla 2.1 Configuración de canales IEEE 802.11b. [4]

Por otra parte es necesario tomar en cuenta las áreas a las cuales se quiere dar cobertura, para así evitar instalar el punto de acceso cerca de aparatos que puedan causar interferencia, tales como: teléfonos inalámbricos que operen en la frecuencia de 2.4 Ghz, redes Bluetooth, hornos microondas, etc.

En interiores, lo recomendable es hacer un plano que incluya paredes y divisiones, conexiones de red de datos y eléctricas, para evitar posibles fuentes de interferencia.
La figura 2.3 muestra un esquema típico de como debe instalarse el punto de acceso basados en las recomendaciones anteriores (no necesariamente debe ser ubicado en el centro del edificio).

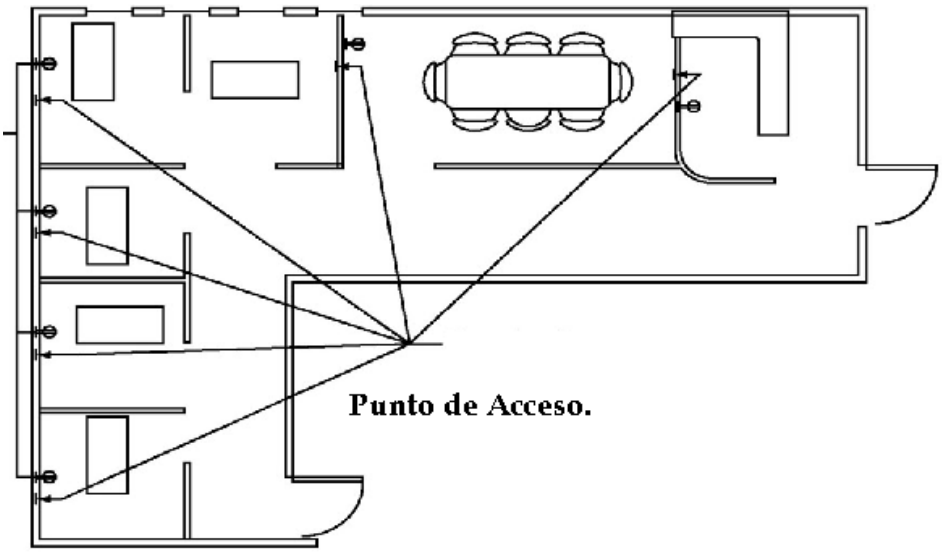


Figura 2.3 Plano de una oficina pequeña y ubicación del punto de acceso.

En exteriores, para proporcionar cobertura inalámbrica, se recomienda que las antenas sean instaladas en las esquinas de los edificios, ya que si se ubican al centro de estos, la señal será debilitada en mayor grado por la sombra que ejercen las paredes del edificio en el cual se monta. Instalando de forma correcta la antena se puede mejorar sustancialmente el alcance de la red.

La figura 2.4 ejemplifica lo antes expuesto.

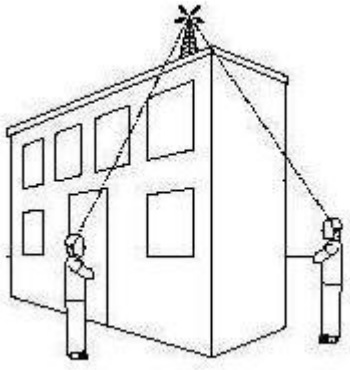


Figura 2.4 Antena en el centro del edificio no da cobertura cerca del edificio.
Por otra parte si se colocan puntos de acceso para interiores en un lugar estratégico, podremos tener cobertura tanto interior como exterior (principalmente en áreas cercanas al edificio). Además se deberá tomar en cuenta que las señales de microondas pueden atravesar con mayor facilidad elementos de madera y vidrio, mas que paredes de concreto y acero estructural.

En la referencia bibliográfica 3(dada al final del capítulo) establece que para el diseño tanto de interiores como de exteriores, se deberá tomar en cuenta el modelo ideal de transmisión radioeléctrica del punto de acceso, para establecer cual es el mejor lugar dónde ubicarlo, dicho planteamiento se esquematiza en la figura 2.5, la cual se explica de la siguiente manera:

En el nivel donde se encuentra ubicado el punto de acceso, la cobertura radioeléctrica de éste tendrá un radio R, y para los puntos que se encuentren en nivel superior o inferior la cobertura será de radio R'.

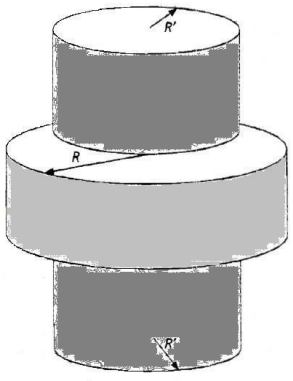


Figura 2.5 Área ideal de cobertura de un AP.

2.3 CONSIDERACIONES DE DISEÑO.

Debido a que la propagación de radiofrecuencias dentro de los edificios no es uniforme, y raramente es predecible, el diseño en una red inalámbrica para instalaciones internas es un proceso interactivo que incluye cinco pasos:

- Seleccionar la localización de los AP.
- Probar y rediseñar la localización de los AP basados en las mediciones de los niveles de señal.
- Dibujar un mapa de cobertura.
- Asignar las frecuencias de operación de los AP.
- Documentar la localización del AP, los niveles de señal y las frecuencias utilizadas.

2.3.1 LOCALIZACIÓN INICIAL DE LOS AP

Se define un área de cobertura en términos del nivel de señal recibida. Esta debe tener un valor mínimo, establecido por la relación de señal ruido (S/N) y un margen adicional para contrarrestar posibles variaciones. Por ejemplo, si en el diseño de una red WLAN, el nivel de ruido es de -95 dBm, y si el sistema requiere un nivel de relación S/N de 10 dB para asegurar un buen

funcionamiento y adicionalmente consideramos un margen extra, de 5 dB para compensar variaciones en el nivel de ruido, en este caso el valor mínimo de señal será de -80 dBm.

Una vez establecidos los niveles mínimos de señal requeridos, se colocará el AP en el lugar donde haya mayor cobertura. Luego se examinarán los puntos donde el nivel de señal es muy bajo para colocar otros AP. Cuando es necesario colocar más de un punto de acceso, existen arreglos establecidos tanto lineales como rectangulares en un solo piso, ya sea para dos o más niveles.

En la figura 2.6 se describe el arreglo lineal de 3 puntos de acceso (para un solo nivel) con un radio “R” de cobertura en el cual se permitirá solo un 30% de traslape entre coberturas de puntos de acceso. En el esquema, “D” es la distancia entre puntos de acceso.

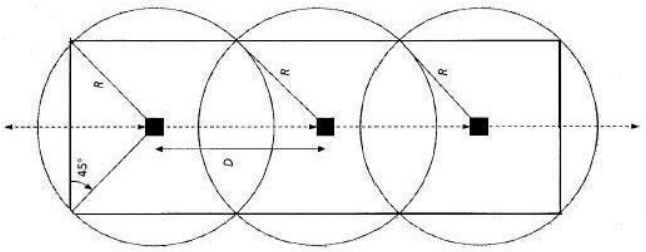


Figura 2.6 Arreglo lineal de AP en una sola planta.

Para el caso de un arreglo lineal de dos niveles, D’ es la distancia entre los puntos de acceso que se encuentran en niveles distintos; R y R’ es la cobertura de los AP en cada nivel (el área con línea sólida indica el nivel superior y el área con línea punteada es para el nivel inferior).

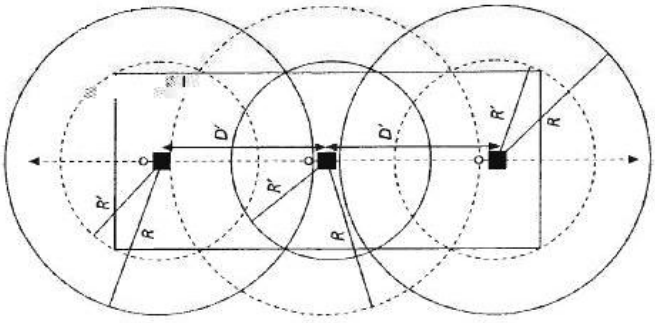


Figura 2.7 Arreglo lineal de AP para más de un nivel.

El tercer posible arreglo es: un solo nivel y arreglo rectangular de AP. Donde “R” es el área de cobertura del AP y “D” es la distancia entre cada punto de acceso.

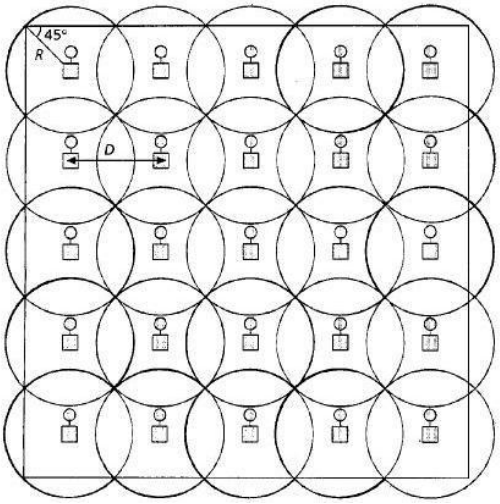


Figura 2.8 Arreglo rectangular para un nivel.

La cuarta opción es que el arreglo rectangular sea para distintos niveles en ese caso como área de cobertura de AP en el mismo nivel es R y para uno ubicado en otro nivel es R', al igual que la distancias entre ellos, es D para especificar la distancia entre dos AP adyacentes del mismo nivel y D' para dos AP adyacentes de niveles distintos.

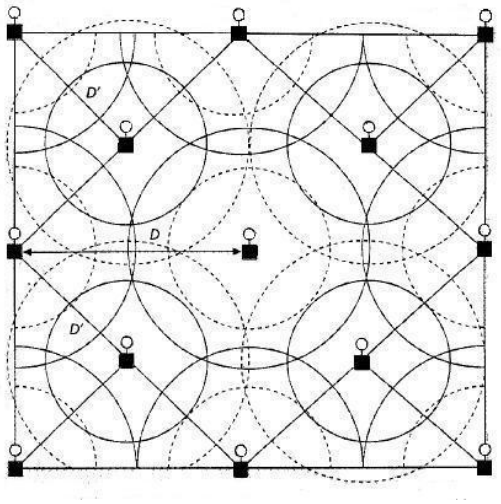


Figura 2.9 Arreglo rectangular para mas de un nivel.

Es cuanto a la distribución de frecuencias o canales a utilizar pueden ser 1, 6 y 11 (como ya se explico antes) y se pueden distribuir como se muestra en la figura 2.1 para evitar interferencias entre AP.

En los diseños anteriores se hace referencia solo a cobertura en interiores, para el caso de áreas de cobertura fuera de edificaciones, es necesario hacer

reiteradas mediciones de cobertura, ya que también hay elementos que degradan los niveles de señal (como árboles, en algunos casos paredes de otros edificios, etc.). Se debe tener en cuenta esta limitante ya que es necesario aprovechar de forma eficaz la señal emitida por los AP, ya que la mayor parte de ellos tiene como potencia de transmisión limite 100mW, el cual es el limite establecido por los entes reguladores Europeos; no obstante, la FCC en los Estados Unidos establece como limite 1000mW. No obstante, comercialmente lo más común son AP de 100mW. Por lo anterior, es necesario ubicar estratégicamente el AP, junto con una buena ubicación y orientación de la antena o arreglo de antenas seleccionados.

Dependiendo del área a la cual se le desee proveer cobertura, de ello dependerá el tipo de antena a escoger. Por ejemplo, si se tiene disponible una torre o antena de transmisión, y se desea proveer servicio en un espacio abierto, la mejor opción es una antena omnidireccional, debido a que el ángulo de cobertura es de 360 grados.

2.4 ANTENAS.

La antena transforma la señal eléctrica que produce el transmisor en ondas electromagnéticas que se disipan a través del espacio y pueden ser captadas por un receptor de radio, para que esto suceda de la manera más eficiente la antena debe de estar ajustada a la frecuencia a la que se quiera transmitir, es decir, su forma física determina la frecuencia para la que se puede usar. La conexión entre la última etapa de amplificación y la antena debe estar acoplada, es decir la impedancia de salida del amplificador debe ser igual a la impedancia de entrada de la antena, cuando son iguales aseguramos que la potencia que sale del amplificador se disipe en la antena, como estándar las antenas tienen una impedancia de entrada de 50 Ohms, la impedancia de salida del amplificador debe ser también de 50. Si no son iguales no se disipa toda la potencia en la antena, y se refleja hacia el amplificador, y si esta potencia reflejada es muy alta puede dañar al transistor, que es la pieza más importante del amplificador.

Algo que hay que tener muy en cuenta es que nunca debemos encender un transmisor sin antena o sin una carga fantasma, que es simplemente una resistencia de 50 ohmios. Si se enciende un transmisor sin carga o antena, podemos dañar los transistores de los amplificadores porque se refleja toda la potencia en lugar de disiparse. Aunque estas medidas son aplicables para transmisores de potencia superiores a 1W, también se deben tomar las precauciones en los puntos de acceso cuando estos tienen instalados

amplificadores, por otra parte cuando se utilizan sin amplificación estos traen una antena interna incorporada que viene acoplada a la etapa de transmisión.

2.5 ESTUDIO DEL ÁREA GEOGRÁFICA.

En las redes WI-FI se tiene la limitante que entre el cliente y el servidor se debe tener línea para tener un enlace en las condiciones ideales, por lo que en la práctica se deben tomar en cuenta los siguientes elementos que interfieren con lo anterior:

- Elementos absorben microondas tales como, árboles, tierra, paredes de ladrillo, paredes de yeso, y las personas.
- Superficies de reflexión como metales, cercos, cañerías, pantallas, y cuerpos de agua, por ejemplo, piscinas.
- Fuentes de ruido en la frecuencia de 2.4 Ghz, tales como hornos microondas, teléfonos inalámbricos a 2.4 Ghz, y otros equipos wireless.

2.6 SERVIDOR DE ACCESO INALÁMBRICO.

Las tecnologías inalámbricas tienen muchos beneficios, en cuanto a movilidad y escalabilidad. Sin embargo también tienen algunas desventajas frente a otras tecnologías, como la seguridad ya que por defecto los datos viajan en espacio libre sin ser cifrados, además se tiene el riesgo del mal uso de los recursos disponibles, por ejemplo el envío de spam (correo basura), y otros. Razón por la deben tomar acciones contra el uso inadecuado de los recursos de red
.
Por lo que se propone la instalación de un servidor de acceso inalámbrico debe tener la función de puerta de enlace y además deberá autenticar los usuarios ya sea de forma abierta; es decir que no solicite ningún parámetro al usuario, o cerrada que le pida usuario y contraseña a estos. Para nuestro caso solo se logro la implementación del servidor como puerta de enlace implementado en le sistema operativo Linux/Debian se eligió el sistema operativo Linux por que es de distribución libre, es decir no tiene costo por su uso, sin embargo no se logro realizar la configuración de este como servidor de autenticación, por lo cual se deja para futuros trabajos la implementación de esta etapa. Sin embargo se hace la observación de los servicios requeridos para llevar a cabo dicha implementación.

Para que el servidor trabaje como puerta de enlace debe tener configurados los siguientes servicios:

- IPTABLES
- DHCP
- DNS

- RADIUS [1]

2.6.1 IPTABLES.

Con Iptables se establecieron la reglas seguridad de comunicación entre la red local con la red inalámbrica, en cuanto a qué tipo de información puede o no puede transmitirse por la red, a través de los protocolos TCP, UDP, ICMP, IP etc., también establece las rutas por las cuales viajará la información, debido a que como mínimo este equipo deberá tener por lo menos dos interfaces de red, aunque puede utilizar más de dos en caso de redes mas complejas. En el caso del servidor a utilizar en la implementación para la red WIFI solo tiene dos interfaces. Actualmente la función principal que con el firewall, es aislar la red local con la red inalámbrica.

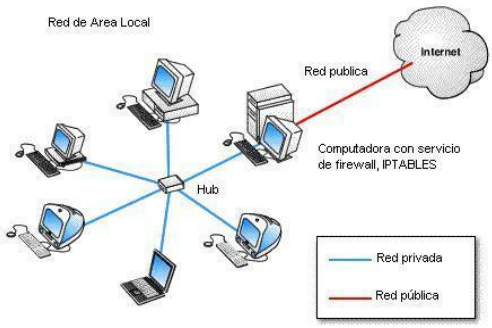


Figura 2.10 Esquema básico de instalación de un firewall.

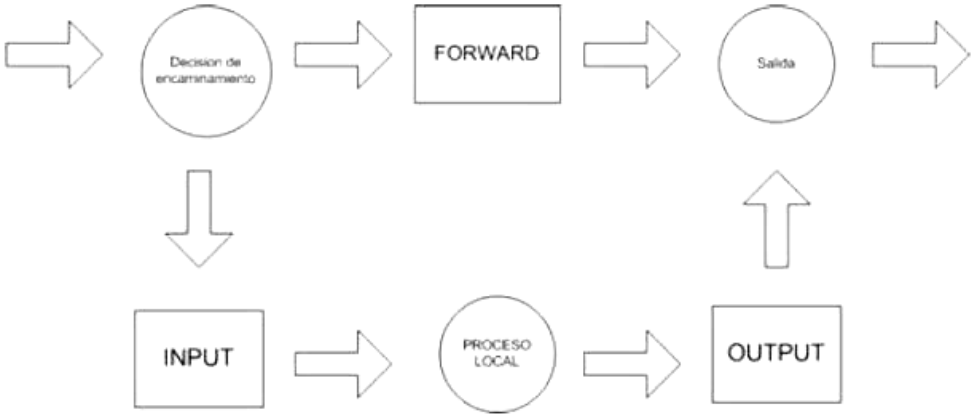


Figura 2.11 Esquema de flujo de datos en iptables.

2.6.2 DHCP.

[1] Este servicio no se implementó en el servidor prototipo.

Para que el usuario final no tenga que realizar ninguna configuración en su equipo terminal, el servidor DHCP (Dynamic Host Configuration Protocol) asignará automáticamente la configuración a los clientes. Los datos así obtenidos pueden ser: la dirección IP, la máscara de red, la dirección de broadcast, las características del DNS. La configuración de DHCP en el caso de Linux, se basa en un fichero de texto que se encuentra en /etc/dhcp.conf que el proceso servidor lee en el inicio. La lectura del fichero de configuración sólo se realiza durante el inicio, nunca cuando ya está en ejecución, por tanto cualquier modificación requiere detener el servicio DHCP y volverlo a iniciar. En este fichero se especifican las características de comportamiento como son el rango de direcciones asignadas, el tiempo de asignación de direcciones, el nombre del dominio, los gateways, etc.

2.6.3 DNS

Este servicio es un complemento, debido a que no es indispensable, es más eficiente el uso de un DNS local. Por los problemas de comunicación que pudieran presentarse, si se utilizan servidores DNS remotos. Los servidores DNS es en esencia consisten una base de datos distribuida. Esta base de datos es jerárquica, al estilo de como lo son los sistemas de ficheros de UNIX. La raíz de la base de datos está representada por el nodo "." y cada uno de los nodos que descienden de ella reciben el nombre de dominios.

En el sistema DNS cada dominio se hace cargo de la base de datos que depende de él.

En cada dominio puede haber a su vez servidores y otros dominios. Cada nombre de dominio se construye escribiendo los sucesivos nombres de dominio a los que pertenece el dominio hasta llegar al dominio raíz. En el caso de Debian el servicio o demonio que se ejecuta en el sistema operativo es el bind o bind9 según la elección del administrador de la red lo decida.

2.6.4 RADIUS

Cuando se realiza la conexión con un ISP mediante módem, DSL, cable módem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS (Servidor de Acceso a la Red) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros servicios de red.

Una de las características mas importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos. En el servidor no se implemento. Sin embargo es necesario para implementar la seguridad con la norma IEEE 802.1X.

CONCLUSIONES DEL CAPÍTULO II

- En el marco legal es muy factible aprovechar el hecho que la banda de operación de WI-FI sea libre, ya que se pueden hacer prácticas sin ningún temor a tener problemas con interferir algún enlace privado. Pero sí es un problema la saturación de dicha banda, razón por la cual es importante escoger un canal que este libre.

- Es necesario colocar un servidor que separe la red cableada con la inalámbrica por razones de seguridad. Ya que en esta cualquier persona tiene acceso al medio y con herramientas adecuadas se puede penetrar a la red sin autorización. Y al tener separadas las redes se evita robo de información

- La norma IEEE 802.11 fue diseñada principalmente para entornos cerrados, pero con algunas modificaciones en los equipos para interiores pueden ser utilizados para exteriores con éxito.

REFERENCIAS BIBLIOGRÁFICAS CAPÍTULO II.

[1] Cuadro Nacional de Atribución de Frecuencias (CNAF).
SIGET. 30/11/2004 Pág. 95 - 96

[2] Install, configure, and Use 802.11b Wireless Networking
Copyright ©2003 by John Ross.
Capitulo 3 Installing and configuring Access Points.

[3] IEEE Communications Magazine
Wireless Local Area and Home Networks
Large-Scale Wireless LAN Design.
Alex Hill, Carnegie Mellon University
Noviembre 2001 Páginas 98-104

[4] 802.11® Wireless Networks: The Definitive Guide
April 2002 ISBN: 0-596-00183-5
Matthew Gast Pag. 184-186, 329

[5] Building Wireless Community Networks
Enero 2002 ISBN: 0-596-00204-1
Rob Flickenger. Pag. 60, 64-66.

CAPÍTULO III

ESTUDIO RADIOELÉCTRICO DE CAMPO.

3.0 INTRODUCCIÓN.

La predicción de la cobertura de una red WIFI depende en gran medida de las condiciones físicas del entorno en el cual será implementada, dichas condiciones determinan las características de propagación radioeléctrica reales de las señales emitidas por los AP. Aunque se puede predecir los niveles de señal recibida, por medio de ecuaciones matemáticas, lo más conveniente es realizar mediciones de campo que permitan validar tales predicciones. Dicha acción fue realizada y con los resultados obtenidos se elaboró el mapa de cobertura de la red WIFI de la FIA (mismo que se presenta en el Anexo G), en dicho mapa se identifican las áreas en las cuales habría cobertura de la red y el grado de servicio esperado.

3.1 METODOLOGÍA DE MEDICIÓN.

Las mediciones radioeléctricas pueden ser realizadas utilizando una gran variedad de herramientas y/o equipos, por ejemplo: analizadores de espectro, analizadores de radiocomunicaciones, detectores WIFI, etc., tales instrumentos son muy precisos, sin embargo su costo económico es elevado y fue imposible obtener uno para realizar las pruebas, en su lugar se utilizaron herramientas de software disponibles libremente en Internet, específicamente el programa conocido como NETSTUMBLER (también existe el WIRELESS TOOL).

El NETSTUMBLER permite realizar lecturas de niveles y con ellas establecer la relación señal/ruido de la emisión bajo prueba. Adicionalmente permite:

- Verificar la configuración de la red (si es abierta o cerrada en cuanto a cifrado).
- Establecer los sitios donde la cobertura es pobre (entiéndase bajo nivel de señal).
- Detectar otras redes WIFI que puedan causar interferencias.
- Permite mejorar el apuntamiento de las antenas para optimizar su cobertura.
- Además tiene la capacidad de almacenar las lecturas tomadas, de tal forma que se puedan procesar con posterioridad.

Este software se distribuye bajo la modalidad Beggarware, es decir que se desarrolla mediante aportaciones realizadas por los diferentes usuarios que lo utilizan.

WIRELESS TOOLS

Es otro software que permite medir los niveles de señal emitidos por dispositivos inalámbricos, este corre en ambiente Linux, bajo este sistema operativo, se ejecuta con el comando iwconfig, y así se pueden conocer los parámetros de la red WIFI a la cual nos estamos conectando.

No dispone de la facilidad de almacenamiento de los resultados de las mediciones realizadas, por lo cual no se utilizó.

3.2 DESCRIPCIÓN DEL PROCEDIMIENTO

Se utilizó un AP marca ORINOCO modelo AP 2000, como fuente de radiación fija. Éste se instaló en lugares previamente elegidos por su ubicación geográfica, conveniente a nuestros intereses de cobertura.

Luego utilizando el NETSTUMBLER cargado en una PC portátil, nos desplazamos en diferentes puntos de la FIA y en cada uno de ellos se registraba los datos técnicos relacionados con la calidad de la señal disponible en tales puntos.

Adicionalmente, y basados en los primeros resultados obtenidos, se concluyó que la antena original del AP ORINOCO no permitía una cobertura suficiente, por su bajo valor de ganancia. Por lo anterior, se tuvo la necesidad de mejorar este parámetro, manteniendo la filosofía que la solución debía ser de bajo costo. Lo anterior llevó a considerar la construcción de antenas sugeridas por el libro **Wireless Hacks [4]**, de las opciones propuestas se implementaron dos: la antena helicoidal y la modificación del elemento radiante de una antena parabólica de televisión satelital.

La antena helicoidal mejoró sustanciales los niveles de señal emitidas por el AP, con lo cual se incremento la cobertura de éste en un 50%; aunque el porcentaje de mejora es sustancial, aún no era suficiente para la cobertura esperada de la red.

Con la antena parabólica se mejoró mucho mas la cobertura (casi se duplicó) por lo cual ésta alternativa es la que se recomienda para el diseño final de la red. La desventaja de ésta antena radica en la directividad de la misma (la cual es muy alta), por lo que el apuntamiento es crítico.

Una tercera opción explorada, fue la utilización de una antena comercial tipo panel de 24 dBi de ganancia, esta antena permitió incrementar la cobertura a más del 150% sin mayores dificultades en cuanto al apuntamiento, la desventaja de esta opción es que la antena se obtuvo en calidad de préstamo y no podía dejarse permanentemente instalada.

Los puntos elegidos para la instalación del AP con la antena parabólica, fueron:

- La Azotea de la biblioteca de las ingenierías
- La Escuela de ingeniería eléctrica.

Los parámetros radioeléctricos obtenidos por medio del software NETSTUMBLER son los siguientes:

Punto de recepción	Señal [dB]	Velocidad [Mbps]
Mesas externas frente a EIE.	-50	11
Mesas frente al aula D11	-64	11
Sector sur del edificio de metrología.	-78	11
Acceso Oriente de la FIA.	-70	11
Sector sur de cabañas F5	-75	11
Puerta en laboratorio de Eléctrica (Interior)	-78	11
Laboratorio de electrónica (interior)	-83	5.5
Mesas Frente aula C11	-84	5.5
Parqueo ciencias básicas	-86	1
Aula C22	-85	1

Tabla 3.1. Mediciones con la antena en la Escuela de Ingeniería Eléctrica.

Ubicación	Señal [dB]	Velocidad [Mbps]
Frente a biblioteca	-68	11

Frente administración académica	-72	11
Mesas entre plaza y B11	-84	5.5
Árboles frente a plaza	-81	11
Gradas Afuera del Auditórium Miguel Mármol	-83	11/5.5.
Gradas lado norte, Auditórium Miguel Mármol	-86	1

Tabla 3.2 Mediciones con la antena en la azotea de Biblioteca Central apuntando a la plaza de ingenierías.

Ubicación	Señal [dB]	Velocidad [Mbps]
Entrada del gimnasio	-78	11
Gradas estadio de fútbol lado izquierdo	-78	11
Gradas estadio de fútbol lado derecho	-77	11
Gradas frente a la piscina	-64	11
Taquilla derecha frente al gimnasio.	-75	11
Taquilla izquierda frente al gimnasio.	-82	5.5

Tabla 3.3 Mediciones con la antena en la azotea de Biblioteca Central apuntando al polideportivo.

Es oportuno mencionar, que la mejor calidad de señal se obtiene, cuando el nivel de la misma es mayor que -80 dBm. Con dicha magnitud se obtiene una velocidad de transferencia de datos entre el usuario y el AP de 11 Mbps.

Los resultados obtenidos de las mediciones de campo han permitido comprobar las predicciones teóricas que se pueden obtener de los cálculos teóricos de radioenlaces. Basados en dichas predicciones y en las mediciones de campo realizadas, se puede elaborar de mejor manera el Mapa de cobertura de la Red WIFI de la FIA del Anexo G.

CONCLUSIONES DEL CAPÍTULO III

- De la correcta elección del tipo de antena a utilizar en el enlace dependerá en gran medida la calidad del enlace, además en los enlaces de Wi-Fi es indispensable que se tenga línea vista entre las antenas, de lo contrario no se tendrá un enlace estable ya que se dispersará la señal.

- Aunque las antenas juegan un papel importante en la transmisión de la señal, para enlaces mayores de 500 metros es recomendable utilizar amplificadores para que el enlace sea de calidad.

- Para eliminar al máximo las pérdidas, el punto de acceso debe estar en un punto cercano a la antena, ya que el cable coaxial, es uno de los elementos de mayor atenuación, además **debe utilizarse uno de** perdidas para la frecuencia de 2.4 Ghz.

REFERENCIAS BIBLIOGRÁFICAS CAPÍTULO III.

[1] Deep Dish Cylindrical Parabolic Template.
http://www.freeantennas.com/projects/template
/index.html.
Patrón de pantalla parabólica.

[2] BiQuad 802.11b Antenna 11dB
http://www.trevormarshall.com/biquad.htm.

[3] Wlan-antennas (antena Biquad) Martti Palomaki Ilmajoki
http://www.saunalahti.fi/elepal/antenna2.html.

[4] Wireless Hacks by Rob Flickenger. ISBN: 05-596-00559-8
Capítulo 5, Do-It-Yourself Antenas.

[5] Software para monitoreo de niveles de señal/ruido.
http://www.netstumbler.com/

[6] Interactive Wireless Network Design Analysis Utilities
http://www.qsl.net/n9zia/wireless/page09.html
Libro en línea para diseño de redes inalámbricas

CAPÍTULO IV

DISEÑO DE RED INALÁMBRICA,

4.0 INTRODUCCIÓN.

Con los resultados y conceptos presentados los capítulos anteriores, se procede a elaborar la propuesta de diseño para la FIA, dicho diseño esta orientado ha proveer el servicio en las áreas, en la cuales mediante la observación, se ha determinado la alta afluencia de estudiantes, que si bien no es una consideración técnica, si tiene importancia económica, debido a que sería un derroche de dinero equipar un área donde no hay afluencia posibles usuarios, esta es una de las variables principales que evalúan las empresas que prestan servicios similares al propuesto, para instalar sus equipos. Este aspecto es importante recordando la filosofía que el diseño debe de ser en del más bajo costo posible. Además, se incluyen detalles económicos y técnicos que deben ser considerados para su eventual instalación. Así mismo se describe los resultados obtenidos con el prototipo implementado.

4.1 DESCRIPCIÓN DE PROTOTIPO.

EL prototipo de la red, se instaló en el techo de la EIE, utilizó un adaptador DC injector para la alimentación eléctrica y conexión con a red local, del equipo, la antena utilizada fue la parabólica de 24 dBi que se obtuvo en calidad de préstamo, se utilizó como servidor, una computadora con el sistema operativo Linux/Debian, con los servicios, iptables, dhcp y dns configurados. En cuanto al punto de acceso utilizó el método de autenticación y cifrado WPA-PSK. Posteriormente se utilizó la antena helicoidal para establecer un enlace punto a punto entre la EIE y el edificio de potencia, esto debido a la necesidad que surgió debido a las remodelaciones del edificio de la EIE, posteriormente fue necesario desinstalar los equipos debido al avance de dichas remodelaciones, en espera a que se terminen los trabajos en la EIE, para reinstalar el acceso inalámbrico.

4.2 PUNTOS DE ACCESO: TIPO Y UBICACIÓN FÍSICA

En cuanto a la adquisición de puntos de acceso se recomienda los de marca AP2000, para los edificios en los cuales se instalaran en la azotea, debido a que estos son más robustos en cuanto a su escalabilidad, ya que traen una tarjeta de expansión, que permitiría con un solo AP, proveer mayor cobertura, o se podría configurar una red inalámbrica virtual (VLAN) para los estudiantes y otra para los docentes. Por otra parte como se mencionó en el capítulo II, los AP pueden ser ubicados en puntos estratégicos interiores, que provean servicio para espacios exteriores. Para este uso los equipos más adecuados son los puntos de acceso marca D-link (cualquier modelo para interiores), se recomiendan estos puesto que son de fácil adquisición, bajo precio con respecto al AP-2000 y fácil administración remota.

La ubicación de los puntos de acceso inalámbricos ha sido distribuida tal como se presenta en la figura 4.1, tomando en cuenta los factores técnicos en cuanto a la disponibilidad de red local y la afluencia de estudiantes en las áreas propuestas.

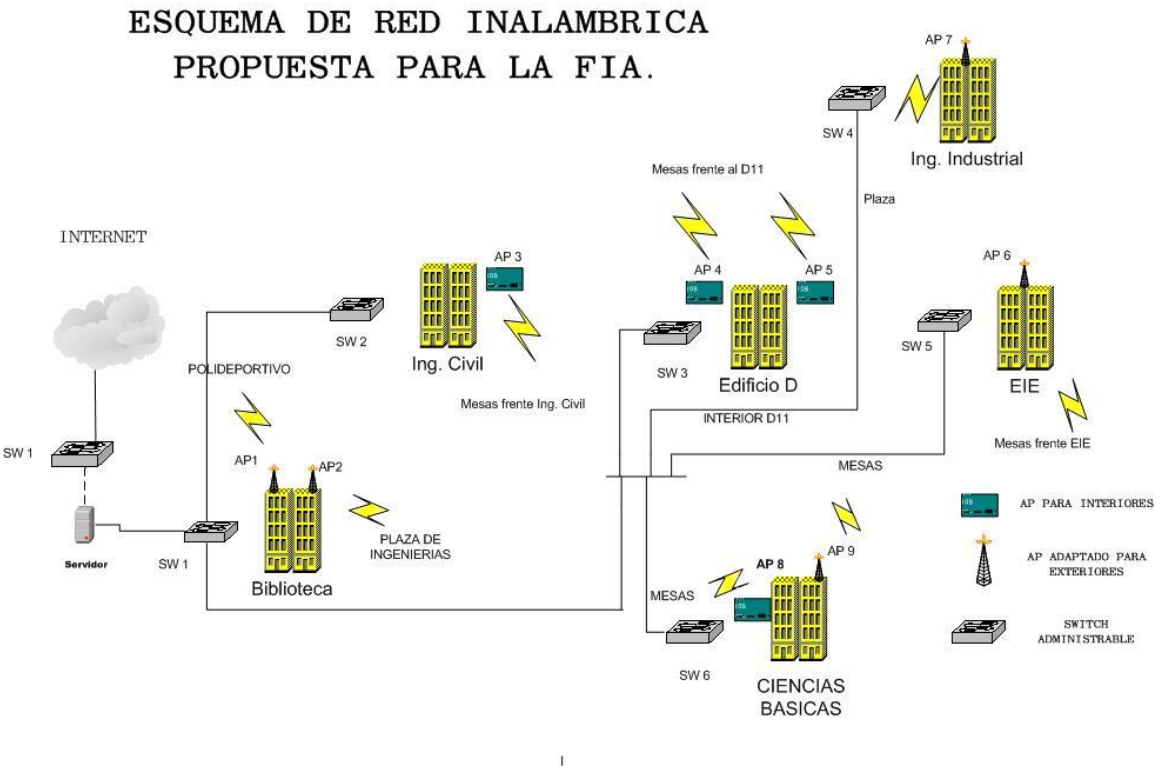


Figura 4.1 Esquema de red inalámbrica para la FIA.

El diseño propuesto puede ampliarse tanto en cuanto a cobertura inalámbrica para áreas exteriores, como en lo que Respecta a establecer enlaces punto a punto, con otras oficinas que no tienen cobertura de la red de área local. Como se muestra en la figura,

en algunos edificios se recomienda instalar puntos de acceso para interiores como es el caso en los edificios de Ing. Civil, De Ingeniería Industrial, esto es así por que el área exterior a cubrir es pequeña y de esa forma se evita, el costo de antenas y sus accesorios.

4.3 INTERCONEXIÓN DE AP CON LA RED LAN.

Para la conexión con la red LAN, en ambos equipos (AP-2000 y D-link), se recomienda utilizar adaptadores de alimentación eléctrica sobre ethernet, dichos equipos están regidos por el estándar IEEE 802af (PoE, Power over Ethernet), para suministrar energía a los puntos de acceso, debido a que generalmente están ubicados en azoteas, cielos falsos y otros lugares donde lógicamente no hay conexiones de corriente alterna. En caso de utilizar estos equipos, seria

necesario realizar la instalación eléctrica para cada AP, lo cual aunque es factible, no es recomendable.

En cuanto a la interconexión lógica, con la red local, se proponen dos opciones.

La primera solución consiste en: Que cada edificio, en el cual, se instale uno o más puntos de acceso, deberá tener un servidor, que proteja la red local de accesos no autorizados, esto es necesario debido a que la configuración actual de red de la FIA, no permite la instalación un servidor centralizado, ya que existen otros servidores dhcp conectados en la red, que entrarían en conflicto con el servidor WIFI, sin embargo esta opción, no es viable por las razones siguientes:

- Poca escalabilidad.
- Alto costo económico.
- Difícil administración y monitoreo, de los servidores.
- Subutilización de los recursos, con respecto a los equipos que se designen como servidores.

Razón por la que se propone una segunda alternativa la cual consiste en instalar un servidor centralizado y adquirir conmutadores administrables para las escuelas, de manera que permita configurar una red local virtual (VLAN), para la conexión de los equipos inalámbricos, esta opción es la mas acertada, debido a que con esta configuración todo el tráfico de la red inalámbrica estará aislado completamente de la red local, esta topología, proporciona a la red local un mayor grado de seguridad, y a la WLAN, le permite un grado de escalabilidad mas amplio, ya que para agregar otros puntos de acceso solo será necesario agregar a la VLAN, los equipos que se deseen instalar en la red.

4.4 EQUIPOS Y ACCESORIOS A UTILIZAR.

Como se mencionó en capítulos anteriores, para proporcionar mayor ganancia a los AP diseñados para interiores, es necesario que se le instalen antenas, para aumentar su ganancia. Con los resultados obtenidos en el capitulo III, podemos hacer la recomendación que para la instalación de las antenas con la distribución siguiente:

a. Los puntos de accesos que proveerán servicio a la plaza de las ingenierías y al polideportivo, utilicen antenas plato parabólico en las cuales fue modificados sus elementos radiantes, para que operen a 2.4 Ghz. Esto es para que los usuarios finales no tengan necesidad de utilizar ningún dispositivo adicional. En la figura 4.2 se muestra una de estas antenas.

Figura 4.2 Antena parabólica con elemento radiante para 2.4 Ghz.

b. Los AP que se instalen, en los siguientes edificios: EIE, Ingeniería industrial, y Ciencias básicas, se recomienda la utilización de las antenas helicoidales, como la que se muestra en la figura.

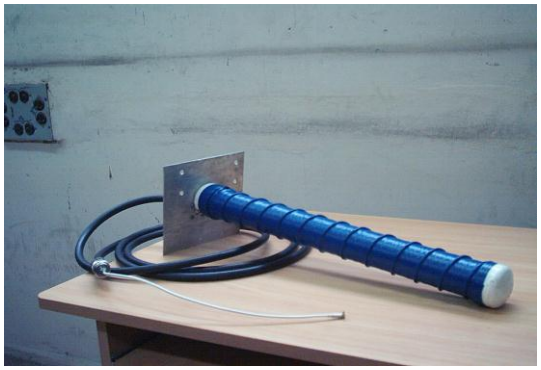


Figura 4.3 Antena helicoidal que opera en 2.4 Ghz.

c. Los equipos inalámbricos que sean instalados en interiores, tal cual es el casos de Ingeniería civil, Edificio D, y ciencias básicas, no se instalará ninguna antena adicional, debido a que el área de cobertura, está en su rango nominal, con la única observación que deben ser colocados cerca de las ventanas de los de edificios mencionados anteriormente. En el caso del edificio D, el punto de instalación es la segunda planta de este, en este nivel se encuentran los docentes de la escuela de Arquitectura y se tiene acceso un punto de para red. Además de proveer acceso a las

mesas que se encuentran frente a este edificio, como se muestra en las figuras 2.5 y 2.7 también se dará cobertura a algunos sectores del aula D11.

Debido a que los puntos de acceso a utilizar, no están diseñados para la instalación en exteriores, ni para la conexión de antenas de este tipo. Sí son necesarios los siguientes accesorios:

- Cable coaxial RG8 o RG213, no mayor de 6 mts. (en el anexo F, se presentan sus especificaciones técnicas).

- Conectores N macho en la figura 4.4. se muestra el ensamble de este.

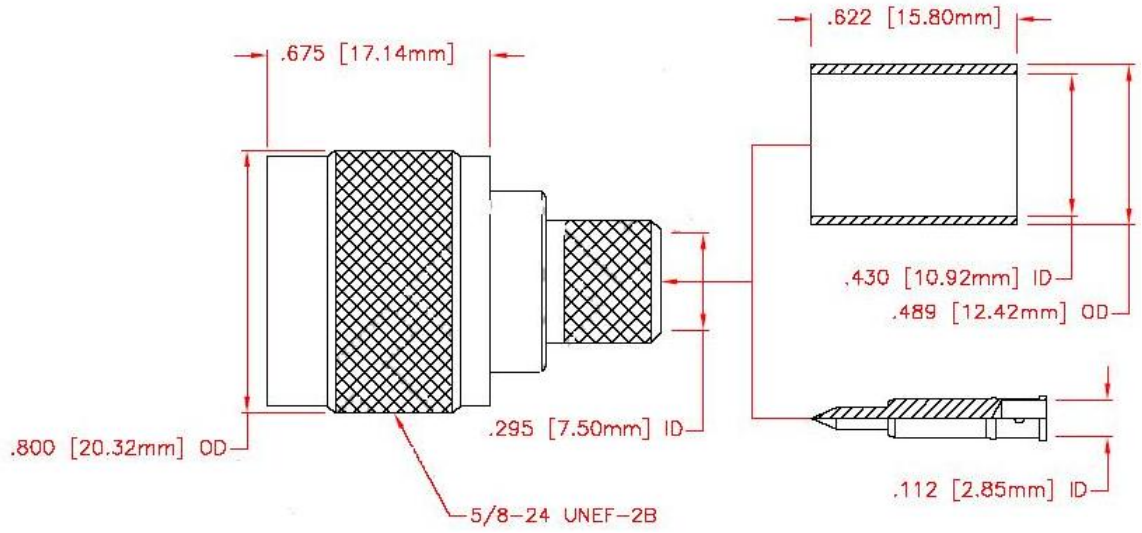


Figura 4.4 Ensamble del conector N macho.

- Pigtail MC a conector N hembra, tal como el que se muestra en la figura 4.5.

Figura 4.5 Pigtail de MC-Card a Conector N hembra.

Como se mencionó en el apartado 4.4 para la alimentación eléctrica de los puntos de acceso se recomienda, que se realice por PoE (Power over Ethernet), pueden ser utilizados los equipos siguientes:

- DC injector, Orinoco.

Figura 4.6 DC injector marca Orinoco.

- PoE marca D-link, modelo DWL-P100.

Figura 4.7 Equipo PoE marca D-link.

En cuanto a los puntos de acceso a utilizar, se propone que se utilicen, de marca Orinoco a los cuales se instalará una antena externa, y para los que se instalarán en interiores se recomienda instalar AP de marca D-link, modelo AP1000.

4.5 UBICACIÓN DE PUNTOS DE ACCESO Y RADIOCANALES A UTILIZAR.

Tal como se describe en la figura 4.1, los puntos de acceso deben ser ubicados en los edificios mencionados por dicha figura. A continuación se detallará como se deberán distribuir los canales radioeléctricos de cada punto de acceso instalado.

Haciendo referencia a la figura 4.1 y tomando en cuenta la recomendación que establece la IEEE, en cuanto a la asignación de los canales radioeléctricos, con la finalidad de evitar interferencias entre la transmisión de los puntos de acceso. Tal como se mencionó en la sección 2.3, la distribución de canales será la siguiente:

UBICACIÓN Exterior (E)/Interior (I)	IDENTIFICACIÓN	CANAL
Biblioteca de las Ingenierías. (E)	AP1	1
Biblioteca de las Ingenierías. (E)	AP2	6
Ingeniería Civil. (I).	AP3	11
Edificio “D” 2do nivel (I).	AP4	1
Edificio “D” 2do nivel (I).	AP5	6
Edificio de EIE (E)	AP6	11
Ingeniería Industrial (E)	AP7	1
Unidad de ciencias Básicas (I).	AP8	1
Unidad de ciencias Básicas (E).	AP9	11

Tabla 4.1 Ubicación de puntos de acceso y elección de radiocanales.

4.6 SERVICIO A OFRECER Y MÉTODO DE ACCESO.

Tanto en el sistema prototipo como el diseño propuesto, se limita a ofrecer solamente acceso al Internet, aunque posteriormente, se puede ampliar, mediante la creación de de VLAN inalámbricas (lo cuales posible en los AP-2000), este servicio puede ser de utilidad, para crear una red inalámbrica, que no sea de acceso público, y que pueda ser utilizado, tanto por el personal docente como administrativo para realizar sus funciones sin interrupciones, en casos de emergencia, tal como lo son los terremotos u otros percances en los que no se tenga acceso a las instalaciones físicas.

El método de acceso a la red es por dhcp, pero antes el usuario tendrá que haber ingresado la contraseña que está registrada en el punto de acceso, y para que este pueda acceder a los recursos de la red, debe tener configurada su tarjeta inalámbrica tal como se indica en el anexo E.

4.7 PRESUPUESTO.

Para llevar a cabo la implementación del diseño antes propuesto, es necesario adquirir los equipos que se detallan en la tabla siguiente:

Cantidad	Descripción	Precio unitario	Precio total
5	Orinoco AP-2000	$ 655	$3275
5	DC injector Orinoco	$ 149	$745

5	Pigtail.	$ 44	$ 220
5	Cables LMR-400 o RG8 de seis metros.[9]	$ 23	$ 115
1	Servidor P4 2.4Ghz, 512Mb Ram, 80 Gb HD	$1000	$1000
2	Materiales para modificación de parabólica	$15	$30
3	Materiales para construcción de antenas Helicoidales.	$20	$60
9	Material para instalación, de ap. A la red Local	$40	$360
4	DC injector para AP de interiores.	$33	$132
4	AP para interiores.	$132	$528
9	24PORT 10/100 SMART VLAN SWITCH TRENDNET.	$150	$1350
		Total	$7815

Tabla 4.2 Equipos necesarios para la implementación red inalámbrica para la FIA.

En cuanto a los precios de los equipos inalámbricos fueron consultados en la web, se ha agregado al precio los costos de importación (transporte+impuestos), utilizando cables y antenas de bajo costo.

A continuación se detallará el costo aproximado del mismo diseño, con la diferencia que se proponen equipos diseñados para OUTDOOR. Para luego realizar la comparación entre la propuesta, realizada con respecto a los equipos OUTDOOR:

Cantidad	Descripción	Precio unitario	Precio total
5	Ruteador Central Externo ORiNOCO COR-1100.	$ 1732.5	$8665
5	DC injector Orinoco	$ 149	$745
1	Servidor P4 2.4Ghz, 512Mb Ram, 80 Gb HD	$1000	$1000
5	Parabólicas de 24 dBi	$85	$425
8	Material para instalación, de AP. A la red Local	$40	$320
3	DC injector para AP de interiores.	$33	$99

3	AP para interiores	$132	$396
9	24PORT 10/100 SMART VLAN SWITCH TRENDNET	$150	$1350
1	Radiator. Servidor de autenticación	$1553	$1553
		Total	$14553

Tabla 4.3 Equipos necesarios para la implementación red inalámbrica para la FIA, con equipo OUTDOOR.

Como se puede observar el costo de la solución con los equipos OUTDOOR excede en un 186% de con respecto a la de INDOOR.

CONCLUSIONES Y RECOMENDACIONES DEL CAPITULO IV.

- Para diseñar redes de acceso inalámbrico, es importante que se tome como referencia los puntos en los cuales se encuentra mayor afluencia de posibles usuarios, esto en conjunto con la factibilidad de la ubicación del equipo inalámbrico en un lugar cercano.

- La utilización de equipo para INDOOR en OUTDOOR, con las modificaciones antes expuestas, cumplen las expectativas de una solución de bajo costo, con respecto a la utilización de equipo OUTDOOR.

- Aunque la cantidad de equipos y accesorios a utilizar disminuye con respecto a equipos INDOOR, este no compensa, alto costo de equipo OUTDOOR.

- Es indispensable la utilización de conmutadores administrables para separar el tráfico inalámbrico con el de la red local.

REFERENCIAS BIBLIOGRÁFICAS CAPÍTULO IV.

[1] Ditther System (Venta de equipos inalámbricos).
http://www.ditther.com/html/orinoco.htm.

[2]PC nation (Precio de Switch VLAN)
http://www.pcnation.com/web/details.asp?item=C67653

[3] Precio de gateway de autenticación.
http://www.digitalpoint.com/products/pricing.html#radiator

CONCLUSIONES GENERALES Y RECOMENDACIONES.

- Se han recomendado seis puntos tentativos para proveer el servicio inalámbrico, esto por motivo a que una cobertura total, seria elevado, que no tendría sentido en cuanto a ser de bajo costo.

- En cuanto a la instalación de antenas de bajo costo, es factible su uso cuando se establecen enlaces de punto a punto en los cuales ambos clientes tiene este tipo de antenas, sin embargo en lugares que se desea proporcionar una conexión se que el usuario tenga otros equipos, se recomienda utilizar antenas, de fábrica, para proveer un nivel de cobertura mayor y una excelente calidad de servicio.

- Con la antena de bajo costo el nivel de cobertura se redujo en un 50%, en algunos puntos de prueba fue necesario incorporar una antena adicional de 5 dBi o una de Helicoidal 14 dBi por lo cual se recomienda obtener un cable de baja atenuación, y la utilización de antenas con plato parabólico.

- En cuanto al servidor de seguridad, se recomienda la configuración del servicio de radius que no fue concluido en este trabajo, ya que con este se podrán implementar otras técnicas de cifrado y autenticación mencionadas en este documento.

ANEXOS.

ANEXO A

REDES INALÁMBRICAS (WLAN).

ESPECTRO ENSANCHADO.

La tecnología de espectro ensanchado consiste en difundir la señal de información a lo largo del ancho de banda disponible, es decir, en vez de concentrar la energía de las señales alrededor de una portadora concreta lo que se hace es repartirla por toda la banda disponible. Este ancho de banda total se comparte con el resto de usuarios que trabajan en la misma banda de frecuencias. Existen dos tipos de tecnologías de espectro ensanchado:

- Espectro Ensanchado por Secuencia Directa (DSSS)
- Espectro Ensanchado por Salto en Frecuencia (FHSS)

Modulación de espectro ensanchado por secuencia directa (DSSS)

Esta técnica consiste en la generación de un patrón de bits redundante llamado señal de chip para cada uno de los bits que componen la señal de información y la posterior modulación de la señal resultante mediante una portadora de RF.

Modulación de espectro ensanchado por salto en frecuencia.

La tecnología de espectro ensanchado por salto en frecuencia consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo llamada “dwell time” y inferior a 400ms. Pasado este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. De esta manera cada tramo de información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo.

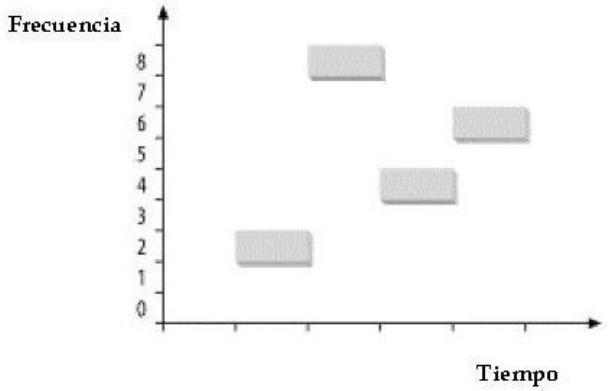


Figura A.1 Espectro ensanchado con salto de frecuencia.

Las especificaciones matemáticas para especificar el conjunto de saltos de frecuencia se puede encontrar en la parte 14.6.8 de la norma 802.11 la cual trata las secuencias de los saltos de frecuencia y se especifican las tablas de saltos de frecuencia para distintos países como EEUU, España, y Japón por mencionar algunos ejemplos. Es importante el tener claro la distribución de canales ya que al instalar una red de puntos de acceso es necesario configurarlos para que no generen interferencia entre si.

La norma IEEE 802.11 fue propuesta para los sistemas WLAN y se estableció que trabajaría en la frecuencia de 2.4 GHz con velocidades de transmisión de 1 ó 2 Mbps [1]. Aunque actualmente la industria ya no fabrica estos dispositivos a estas velocidades.

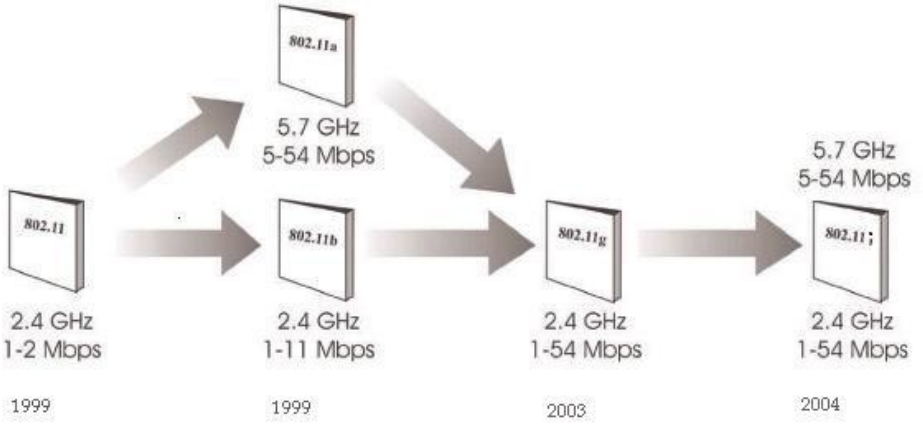


Figura A.2 Evolución de la norma IEEE 802.11

Establece dos tipos de topologías, en la primera utiliza un equipo de distribución, que son conocidos como puntos de acceso, en los sistemas operativos a esta topología se le conoce como infraestructura, la segunda arquitectura a utilizar es en la que cada estación de trabajo se comunica directamente con otra, que es conocido como Ad hoc. Una red inalámbrica de área local WLAN 802.11 posee

un conjunto básico de servicios (BSSs) compuesta de estaciones (STA) o nodos inalámbricos que son conectadas a una capa DS. Cada BSS está conformado por nodos móviles o estaciones que se encuentran controlados por una DCF que determina qué nodo tiene derecho a transmitir o recibir información en el medio inalámbrico de radio propagación. Las estaciones en un BSS obtienen acceso a la capa DS y por lo tanto a otros nodos inalámbricos fuera de su área de cobertura a través del AP. Una estación puede estar conectada solo a un AP en un instante durante un tiempo y puede movilizarse a otro punto en el cual se puede asociar a otro BBS en el DS. La capa DS soporta la movilidad de los nodos mediante direccionamiento e integración de forma transparente a la computación interna de la información en las estaciones (STA). En lo que respecta a seguridad se propuso la utilización de un sistema de cifrado que es muy vulnerable (WEP:Wired Equivalent Privacy), opera en 2,4 GHz con RF. Aunque WEP aún se sigue empleando, ha sido totalmente desacreditado como un protocolo seguro. En septiembre de 1999 se publica el estándar 802.11b que ofrece 11Mbps y el 802.11a que ofrece 54 Mbps. La siguiente extensión de la norma publicada fue la IEEE 802.11g que trabaja en las frecuencias (2,4-2,485 GHz), y velocidades de 36 o 54 Mbps. Usando como método de multiplexación OFDM (Multiplexación por división de frecuencias ortogonal) que además de proporcionar mayor velocidad, tiene cierto grado de compatibilidad con los equipos que operan con la norma 802.11b, sin embargo no se realizó ninguna modificación significativa en cuanto a la seguridad y el sistema de cifrado de datos, por lo que la siguiente extensión del estándar es el IEEE 802.11i que trata a mayor profundad el tema de la de seguridad utilizando algunos recursos ya existentes como la autenticación de Radius que fue concebida en un principio para conexiones seguras ppp, que es soportado por la norma IEEE 802.1X.

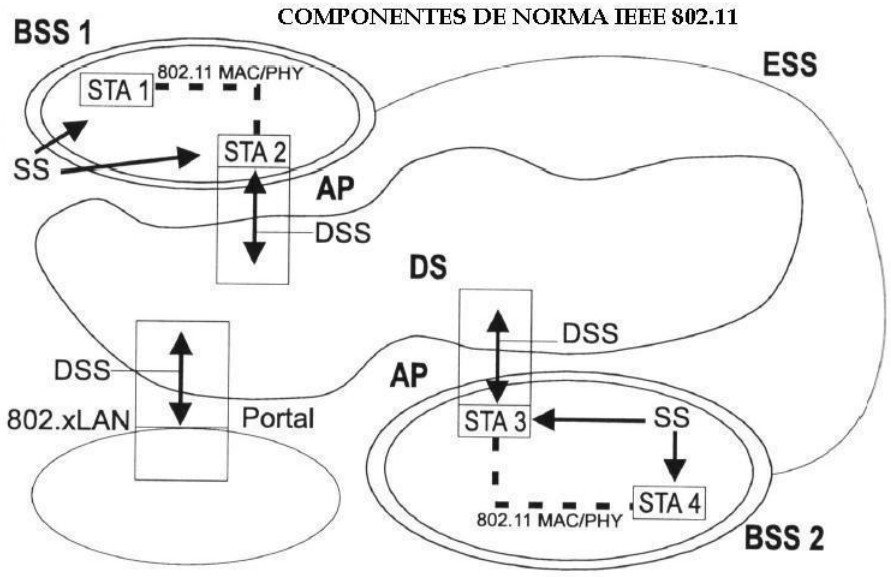


Figura A.3 Esquema de elementos de la norma IEEE 802.11 [1]

RADIUS.

En cuanto al servidor RADIUS no es fácil hacer una definición exacta de la función del servidor de este ya, que puede crear confusión por sus distintas aplicaciones. Pero se puede resumir dos funciones principales. Primero, establece funcionalidades que pueden ser comunes entre distintos servidores de autenticación. Segundo, define un protocolo que permite a otros equipos acceder a sus servicios.

Los principales mensajes del protocolo de RADIUS son muy simples. Y los pertinentes a analizar son cuatro.

- Petición-Acceso (NAS → AS)
- Intercambio-Acceso (NAS ← AS)
- Aceptación-Acceso (NAS ← AS)
- Negación-Acceso (NAS ← AS)

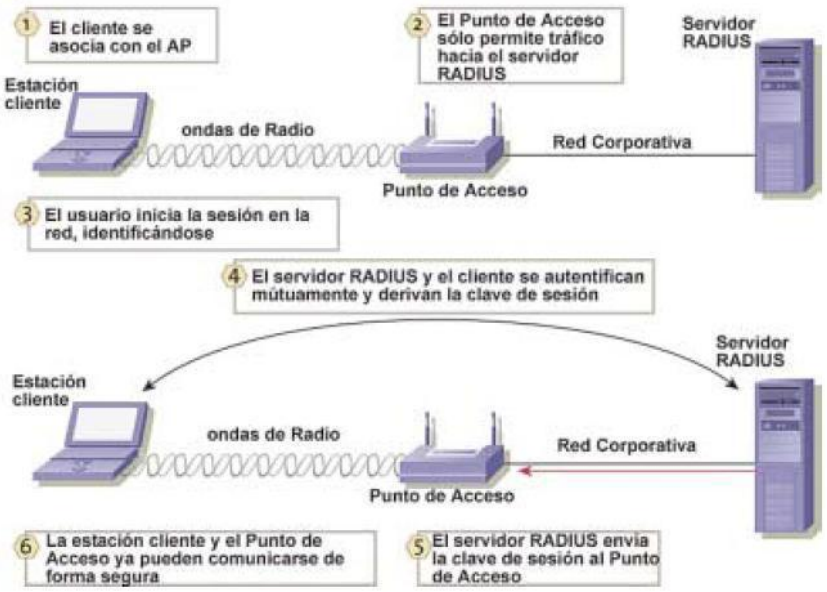


Figura A.4 Descripción del proceso de autenticación RADIUS/EAP.

REFERENCIAS BILBLIOGRÁFICAS ANEXO A.

[1] IEEE Std 802.11b-1999 (R2003)
Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band
LAN/MAN Standards Committee of the IEEE Computer Society
Approved 16 September 1999 IEEE-SA Standards Board

ANEXO B

FABRICACIÓN DE ANTENAS.

B.1 ANTENA DE BOTE CON UN DIPOLO.

Definiciones:

Lo es la longitud de onda de la señal del hf en aire abierto.

Lo/mm = 300/(f/GHz) Ecuación B.1

Lc es la longitud de onda de la frecuencia baja del corte que depende del diámetro del tubo solamente.

Lc = 1.706 x D Ecuación B.2

Lg es longitud de onda derecha dentro del tubo, es función de bajo y del Lc

Lg = 1/SQR((1/Lo)^2-(1/Lc)^2) Ecuación B.3

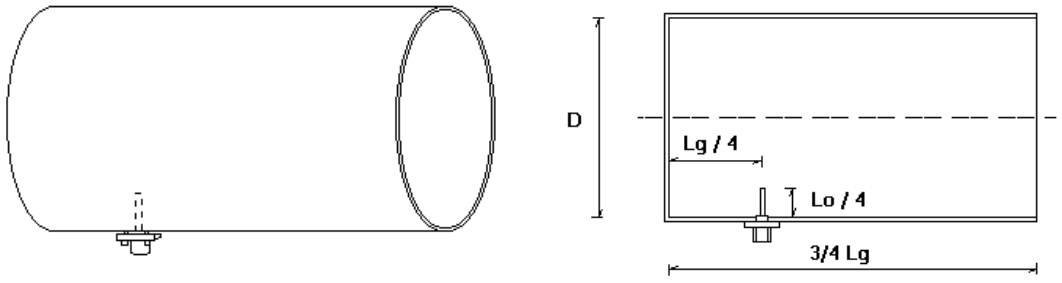


Figura B.1 Antena de Bote.

Las antenas de bote también pueden servir para solucionar problemas de cobertura en equipos wireless sin conector de antena, como los adaptadores wireless USB, donde la antena se pone directamente en el punto en que estaría el elemento activo de la antena.

Construcción de la antena

El primer paso es localizar un bote adecuado, a ser posible de paredes lisas, con un diámetro interior de 90mm como mínimo (si es menor no entran las ondas) y de 100mm o más de longitud. El material a priori no importa, pero hay que tener

en cuenta que si va a estar expuesta a la intemperie se oxidará a no ser que sea de aluminio, acero inoxidable, que esté cromada, galvanizada o pintada.

El diámetro interior del tubo o bote determina el resto de medidas de la antena, además cada canal wireless tiene una frecuencia distinta que interviene en menor medida en la construcción de la antena. Con las siguientes fórmulas, dependiendo del canal a usar se pueden calcular las medidas de la antena. Si se quiere que funcione para todos los canales se deberá usar el canal 6, el centro de la banda.

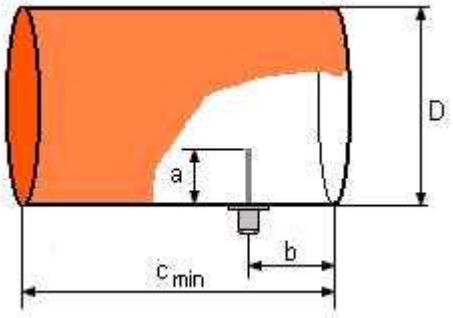


Figura B.2 Cotas para la construcción de antena.

Canal 1:

$$a = 31 \quad mm$$

$$b = \frac{250}{\sqrt{64.6416 - \frac{343591}{D^2}}} \quad [mm]$$

$$c_{\min} = \frac{750}{\sqrt{64.6416 - \frac{343591}{D^2}}} \quad [mm]$$

Canal 6:

$$a = 30.7 \quad mm$$

$$b = \frac{250}{\sqrt{65.9885 - \frac{343591}{D^2}}} \quad [mm]$$

$$c_{\min} = \frac{750}{\sqrt{65.9885 - \frac{343591}{D^2}}} \quad [mm]$$

Canal 11:

$$a = 30.5 \quad mm$$

$$b = \frac{250}{\sqrt{67.3493 - \frac{343591}{D^2}}} \quad [mm]$$

$$c_{min} = \frac{750}{\sqrt{67.3493 - \frac{343591}{D^2}}} \quad [mm]$$

[1]

B.2 ANTENA HELICOIDAL.

Definiciones:

N número de vueltas del cable de cobre sobre el reflector.

C Es el perímetro de la circunferencia que es aproximadamente igual la distancia (l) de la longitud de onda.

l longitud de onda.

d esta distancia entre cada espira debe ser de 0.25*C.

R es el tamaño del reflector que debe de ser igual C o L que puede ser circular o cuadrado.

G es la ganancia de la antena con respecto a una isotropica.

G = 11.8 + 10 * log {(*C*/*l*)^2 * *N* * *d*} dBi **Ecuación B.4**

La impedancia característica de la línea de transmisión de un resultado empírico es:

Z= 140 * (C/L) [Ohmios] **Ecuación B.5**

Diseño para el canal 6 en la frecuencia de 2.43 Ghz.

l = (0,3/2,43)

l = 0,123 [m]

l = 12,34 [cm]

Diámetro de una vuelta (D).

D = (L/pi)

D = 12,34/3,1416

D = 39,3 [mm]

Sin embargo el diámetro del tubo es de 40 [mm] y es agregando el del aislante del cable de cobre.

D = 42 [mm]

C = 42*pi

C = 132 [mm]

d = 0.25*C

d = 33 [mm]

N = 12 vueltas

Longitud del tubo = N * d

Longitud del tubo = 12 * 33 mm

Longitud del tubo = 396 mm

Longitud del tubo = 40 cm

Para acoplar impedancias:

La impedancia de la antena es:

Z = 140 * (C / L) con C = 132 [mm] y l = 123.4 [mm]

Z = 150 [Ohmios]

Para acoplar la impedancia a 50 [Ohmios]

Z1 = 150 [Ohmios] Z2 = 50 [Ohmios]

Zs = SQR(Z1*Z2)

Zs = 87 [Ohmios]

Para acoplar las impedancias se utilizará un triángulo de cobre de base de 71mm y alto 17mm.

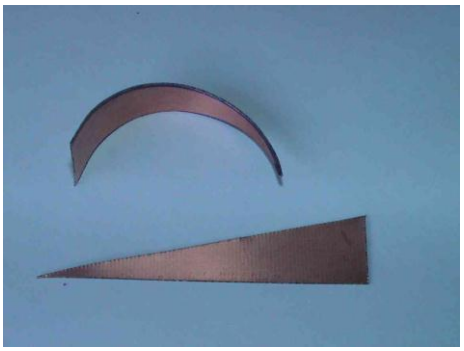


Figura B.3 Acoplador de impedancias.

Figura B.4 instalación del acoplador de impedancias.

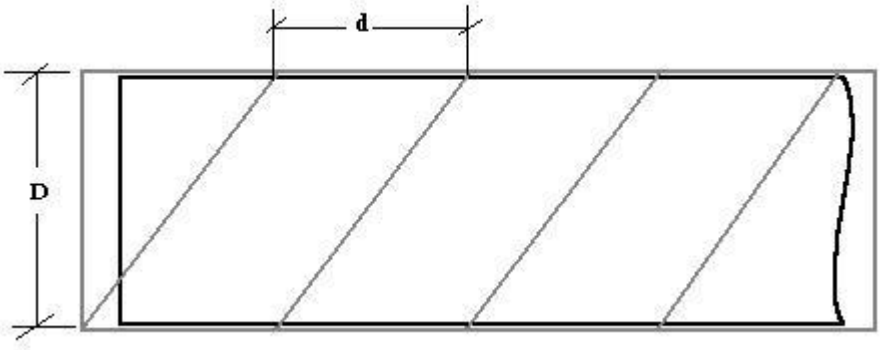


Figura B.5 Espaciamiento d entre espiras.

REFERENCIAS BIBLIOGRÁFICAS ANEXO B

[1] **Wlan-antennasA(antena de bote)**
Martti Palomaki Ilmajoki http://www.saunalahti.fi/elepal/antenna2.html

[2] Construcción de antena Helicoidal.
Dr. Remco den Besten
http://helix.remco.tk/

ANEXO C

ARCHIVOS DE CONFIGURACIÓN DE SERVIDOR.

Script para automatizar la instalación del servidor.

```
#!/bin/sh
# Scrip para la instalación de paquetes para servidor de autenticación
wifi
# Debian woody 3.0-r1 7 cd´s

IP="192.168.1.4"
WHOAMINOW=`whoami`
if [ "$WHOAMINOW" != "root" ]; then
      echo -e "\nYou are NOT root. Please login as root\n"
      exit 0
fi
# ============================================

# Apt command
APTCMD="/usr/bin/apt-get"
APTINSTALL="$APTCMD install"
APTREMOVE="$APTCMD remove --purge"

# ============================================

# Update and upgrade your Debian
$APTREMOVE ipchains
#Binari-1
$APTINSTALL make ssh iptables g    nupg apache bind9 dhcp
#Binari-2
$APTINSTALL shaper
#Binari-3
$APTINSTALL webmin
#Binari-4
$APTINSTALL libnet-netmask-perl
```

Archivo de configuración de iptables :script_iptables

```
#!/bin/sh
echo -n Aplicando Reglas de Firewall...
## FLUSH de reglas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

## Establecemos politica por defecto
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
#enmascaramos todos los paquetes a la salida de internet
#CRITICAL:
```

```
echo "   Enabling forwarding.."
echo "1" > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

## Empezamos a filtrar

# El localhost se deja (por ejemplo conexiones locales a mysql)
iptables -A INPUT -i lo -j ACCEPT
# A nuestra IP le dejamos que acepte todo
iptables -A INPUT -i eth0 -j ACCEPT

#No aceptado
#iptables -A INPUT,FORWARD -s IP -j DROP

#Servicios
#Sistema Grafico X
iptables -A INPUT -i eth0 -p TCP -s 0/0 --dport 6000:6005 -j DROP
iptables -A INPUT -i eth0 -p UDP -s 0/0 --dport 6000:6005 -j DROP

#ICMP
iptables -A INPUT -i eth0 -p icmp --icmp-type 8 -j DROP
iptables -A FORWARD -i eth0 -p icmp --icmp-type 8 -j DROP

#Cualquier conexion que habra la aceptara
iptables -A INPUT -p TCP -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -p UDP -m state --state RELATED,ESTABLISHED -j ACCEPT

#Cualquier otra conexion invalida de fuera hacia mi es descartada
#iptables -A INPUT -m state --state NEW,INVALID -j DROP

echo " OK . Verifique que lo que se aplica con: iptables -L -n"
# Fin del script
```

Archivo de configuración de servidor dhcp. dhcp.conf

```
subnet 192.168.100.0 netmask 255.255.255.0{
      range  192.168.100.100 192.168.100.150;
      default-lease-time 600;
      max-lease-time 7200;
      option domain-name "debian.org.sv";
      option domain-name-servers 192.168.100.1;
      option routers          192.168.100.1;
      option subnet-mask      255.255.255.0;
}
```

Archivo named.conf

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind/README.Debian for information on the
// structure of BIND configuration files in Debian for BIND versions
//8.2.1
// and later, *BEFORE* you customize this configuration file.
```

```
//

options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you might need to uncomment the query-source
        // directive below.  Previous versions of BIND always asked
        // questions using port 53, but BIND 8.1 and later use an
unprivileged
        // port by default.

        //query-source address * port 53;

      // If your ISP provided one or more IP addresses for stable
      // nameservers, you probably want to use them as forwarders.
      // Uncomment the following block, and insert the addresses
replacing
      // the all-0's placeholder.

      // forwarders {
      //    168.243.165.225;
      //    168.243.165.226;
      // };
};

// reduce log verbosity on issues outside our control
logging {
      category lame-servers { null; };
      category cname { null; };
};

// prime the server with knowledge of the root servers
zone "." {
        type hint;
        file "/etc/bind/db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
        type master;
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};
```

```
zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};

// add entries for other zones below here
zone "eienocat.com" {
        type master;
        file "/etc/bind/db.eienocat";
};



zone "100.168.192.in-addr.arpa" {
        type master;
        file "/etc./bind/db.192";
};
```

Archivo de configuración de zona de DNS. bd.192

```
;
; BIND reverse data file for broadcast zone
;
$TTL  604800
@     IN    SOA   debian. vascencio.gmail.com. (
                        1           ; Serial
                   604800           ; Refresh
                    86400           ; Retry
                  2419200           ; Expire
                   604800 )   ; Negative Cache TTL
;
@     IN    NS    debian.
; Name Servers
100.168.192.in-addr.arpa. IN NS    debian.eienocat.com

; Puntero al nombre canonico
1.100.168.192.in-addr.arpa. IN PTR debian.eienocat.com
```

Archivos de fuentes de actualización del sistema. source.list

```
deb http://security.debian.org stable/updates main contrib non-free
deb http://ftp.us.debian.org/debian/ stable main non-free contrib
deb-src http://ftp.us.debian.org/debian/ stable main non-free contrib
deb http://ftp.au.debian.org/debian/ stable main non-free contrib
#deb-src http://ftp.au.debian.org/debian/ stable main non-free contrib
#deb ftp://ftp.de.debian.org/debian/ ../project/experimental main contrib non-fre
```

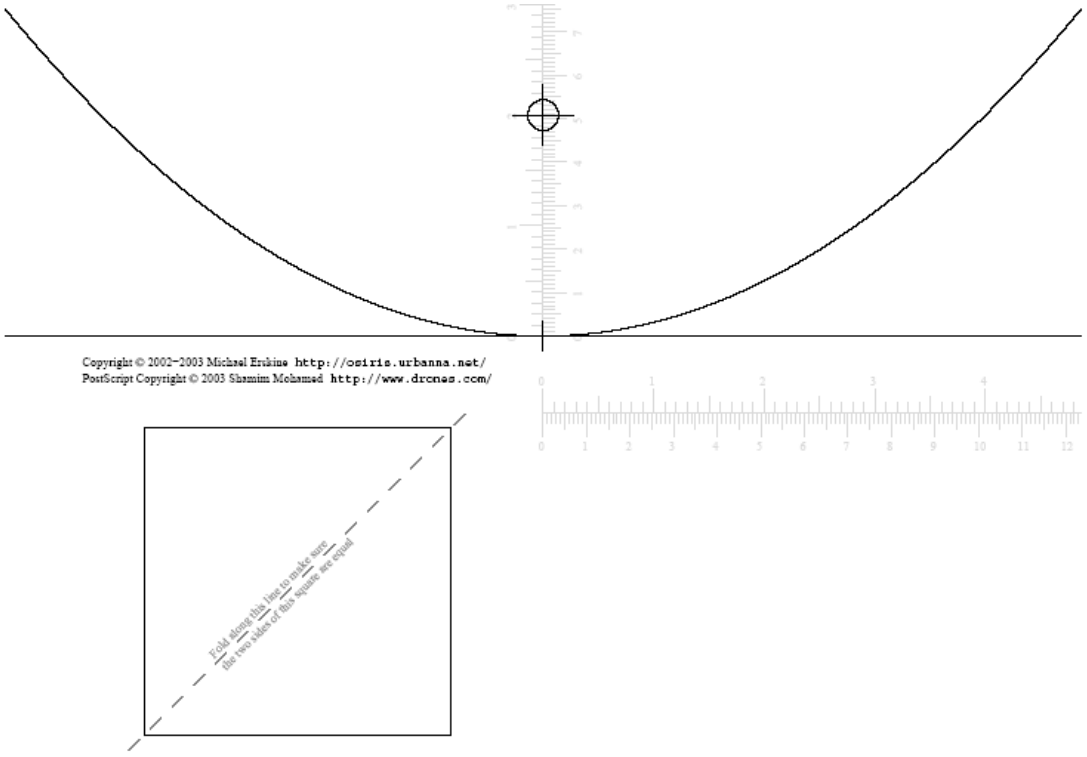
REFERENCIAS BIBLIOGRAFICAS ANEXO C

[1] Learning Debian GNU/Linux.
capitulo 13 sección 3 Understanding Shell Scripts.
Paginas 320-329.
ISBN 1-56592-705-2
By Bill McCarty
1st Edition September 1999.

ANEXO D

PLANTILLA PARABÓLICA.

Plantilla de pantalla parabólica para una antena omnidireccional de un punto de acceso para interiores.



ANEXO E

MANUAL DE USUARIO.

Configuración de acceso inalámbrico.

1. Para window XP.
2. Botón de inicio.
3. Panel de control.
4. Conexiones de red.
5. Doble clic conexión de área local inalámbrica.

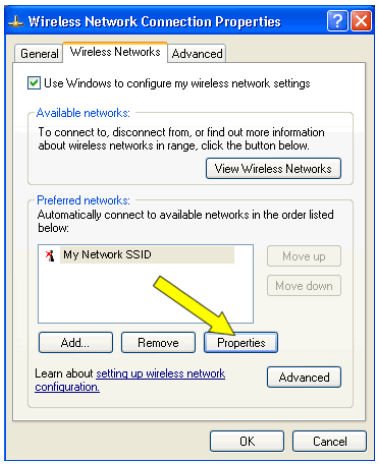


Figura E.1 Propiedades de la conexión inalámbrica.

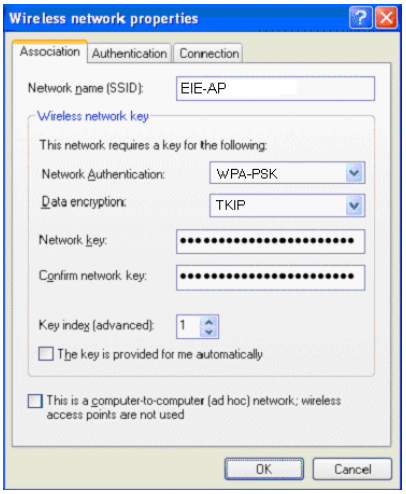


Figura E.2 Configuración de autenticación y cifrado.

En cuanto a la dirección IP ésta debe estar configurada por DHCP.

ANEXO F.

HOJAS DE DATOS Y ESPECIFICICACIONES TECNICAS.

Cables coaxiales y sus especificaciones.

ELECTRONIC AND SPECIALTY CABLES

056041 LL - 400 & 056042 LL - 400R Series

Broadband Communications Cable
Indoor & Standard Outdoor Applications

Common Applications:

Benelec LM-400 cable is available in Indoor, Outdoor and Flooded Constructions. LM-400 is a low loss substitute for RG-8 Foam and Air Dielectric Coax. LM-400 can be used for Jumper Assemblies in Wireless Communications Systems, Antenna Feeder Runs any application requiring a low loss RF Cable. (e.g. LMR, WLL, Paging, PCS and Cellular)

Construction:

Conductor: Solid Bare Copper Clad Aluminum; OD: .108" Nom. (2.74mm)

Insulation: Gas Injected Foamed Polyethylene; OD: .285" Nom. (7.24mm)

Shield 1: Bonded Aluminum / Polyester / Aluminum Tape; 100% Coverage

Shield 2: Tinned Copper Braid; 90% Minimum Coverage

Jacket: See Part Number Table

OD: .405" Nom. (10.29mm)

Markings: Surface printed

Part Number Table:

Model	Catalog No	Description	Jacket	Ratings
056041	LM-400	Std Outdoor	.045" Wall Black Polyethylene	N/A
056042	LM-400R	Flooded	.045" Wall Black PVC	CMR, CATVR

Agency Approvals
When Applicable: UL Standard 444 and NEC Article 800 Type CMR
UL Standard 820 and NEC Article 820 Type CATVR and CSA c(UL)
Flame Rating: UL Standard 1666 Riser Flame Test

Electrical / Mechanical Characteristics:

Capacitance	23.5 pF/ft (77.1 pF/m)
Impedance	50 Ohms Nom.
Velocity of Propagation	85% Nom.
Conductor DCR	1.39 Ohms/Mft Nom. (4.56 Ohms/km)
Shield DCR	1.65 Ohms/Mft Nom. (5.41 Ohms/km)
Inductance	.059 uH/ft (.194 uH/m)
Peak Power	16 kW
Voltage Withstanding	2500 VDC
Jacket Spark	8000 VRMS
Shielding Effectiveness	> 90 dB
Cutoff Frequency	16.2 GHz
Cable Weight	89.0 lbs/Mft (133 kg/km)
Minimum Bend Radius	1.0 inch (25.4mm)
Tensile Strength	160 lbs (72.7 kg)
Operating Temperature	
- Outdoor	-40C to +80C
- Indoor	-20C to +80C

Attenuation

Frequency (MHz)	***dB/100***		***Avg. Power (KW)***	***Frequency (MHz)***	***dB/100***		***Avg. Power (KW)***
	Ft	***M***			***Ft***	***M***	
30	0.70	2.29	3.3	**900**	3.91	12.83	.58
50	0.88	2.89	2.6	**1500**	5.14	16.86	.44
150	1.51	4.95	1.5	**1800**	5.66	18.57	.40
220	1.87	6.14	1.2	**2000**	5.99	19.65	.37
450	2.62	8.60	.83	**2500**	6.79	22.28	.33

BENELEC Pty Ltd (Inc. in NSW) A.C.N. 064 708 390
581-587 Gardeners Road, Mascot N.S.W. 2020
Sydney, Australia

Telephone: +61-2-9693 5111
Fax: +61-2-9669 6783
Website: www.benelec.com.au
Email: inquiries@benelec.com.au

Mail: P.O. Box 21
Mascot, N.S.W. 1460
Australia

Elcard

HDF200-400 Series Antenna Cables

Physical Characteristics | August 2004 | File Number RFHDF-01

	HDF200 (RG58/U)	HDF300	HDF400 (RG8/U)
Inner Conductor O.D.	1.12 mm (0.044 in) Solid Copper, 17.59 Ω/km, 5.37 Ω/kft	1.90 mm (0.075 in) Solid Copper, 9.80 Ω/km, 3.00 Ω/kft	2.77 mm (0.109 in) Copper-clad
Dielectric O.D.	2.95 mm (0.116 in) Closed-cell PE	4.70 mm (0.185 in) Closed-cell PE	7.24 mm (0.285 in) Closed-cell PE
Outer Conductor O.D.	3.66 mm (0.144 in) Sealed Al./Mylar/Al. + Tinned Copper Braid 85%, 16.03 Ω/km, 4.90 Ω/kft	5.70 mm (0.224 in) Sealed Al./Mylar/Al. + Tinned Copper Braid 96%, 6.50 Ω/km, 1.99 Ω/kft	8.13 mm (0.320 in) Sealed Al./Mylar/Al. + Tinned Copper Braid 85%, 5.41 Ω/km, 1.65 Ω/kft
Standard Jacket	4.95 mm (0.195 in) Black PVC	7.30 mm (0.287 in) Clear - Trans. PVC	10.3 mm (0.405 in) Black PVC
Weight kg/m	0.037	0.075	0.108
Nominal Impedance	50 Ω	50 Ω	50 Ω
Nominal Velocity of Propagation	83%	85%	85%
Capacitance	80.4 pF/m , 24.5 pF/ft	79.4 pF/m , 24.2 pF/ft	78.4 pF/m , 24.0 pF/ft

Nominal Attenuation:	dB/100 m / dB/100 ft	dB/100 m / dB/100 ft	dB/100 m / dB/100 ft
@ 30 MHz	5.8 / 1.8	3.5 / 1.1	2.2 / 0.7
@ 50 MHz	7.5 / 2.3	4.5 / 1.4	2.9 / 0.9
@ 150 MHz	13.1 / 4.0	7.9 / 2.4	5.0 / 1.5
@ 220 MHz	15.9 / 4.8	9.6 / 2.9	6.1 / 1.9
@ 450MHz	22.8 / 7.0	13.8 / 4.2	8.9 / 2.7
@ 900MHz	32.6 / 9.9	19.9 / 6.1	12.8 / 3.9
@ 1500MHz	42.4 / 12.9	26.0 / 7.9	16.8 / 5.1
@ 1800MHz	46.6 / 14.2	28.7 / 8.7	
@ 2000 MHz	49.3 / 15.0	30.3 / 9.2	19.6 / 6.0
@ 2500 MHz	55.4 / 16.9	34.2 / 10.4	22.2 / 6.8
@ 5800 MHz	86.5 / 26.4	54.3 / 16.6	35.5 / 10.8

HDF200

HDF400

Elcard Oy
Otto Mannisen Tie 13
51200 Kangasniemi
Finland

Tel. +358 424 96661
Fax +358 424 966670
Email: info@elcard.fi
Internet: www.elcard.fi

Punto de acceso orinoco AP-2000

Especificaciones de Hardware

Especificaciones Físicas

Unidad AP-2000

Dimensiones (AlxAnxPr) = 6,5 x 18,5 x 26 cm (2,5 x 7,25 x 10,25 pulgadas)
Peso = 1,75 Kg (3,5 libras)

Adaptador de Antena 802.11a

Dimensiones (AlxAnxPr) = 11.3 x 2.10 x 26.2 cm (4.5 x 0.83 x 10.3 pulgadas)
Peso = 0.18kg (0.4lb)

Especificaciones Eléctricas

Sin el Módulo Active Ethernet

Tensión = de 100 a 240 VAC (50-60 Hz)
Corriente = 0,2 A
Consumo de potencia = 20 vatios

Con el Módulo Active Ethernet

Tensión de entrada = de 42 a 60 VCC
Corriente de salida = 200mA a 48 VCC
Consumo de potencia = 9-10 vatios

Especificaciones Ambientales

Unidad AP-2000

Temperatura de operación = de 0° a 40 °C (de 32° a 104 °F) con un 20 a un 90% de humedad relativa
Temperatura de transporte = de -40° a 60 °C (de –40° a 140 °F) con un 15 al 95% de humedad relativa (sin condensación)
Temperatura de almacenamiento = de -10° a 60 °C (de 14° a 140 °F) con un 10 al 90% de humedad relativa (sin condensación)

Interfaz Ethernet

Clavija hembra 10/100 Base-T, RJ-45

Interfaz PCMCIA

Ranura PC Card (A y B) = Ranura PC Card estándar para PC Card (Tarjeta PC)

Interfaz de Puerto Serie

Tipo de conector = DB-9, macho
Cable serie = Cable de datos serie RS-232C estándar, con un conector hembra DB-9 en cada extremo

Interfaz Active Ethernet

Se deben usar cables de par trenzado recubiertos, Categoría 5, para cumplir con los requisitos de la Clase B, Subparte B, Parte 15 de la FCC.
Asignaciones de pines según el estándar 802.3af

Interfaz HTTP

Microsoft Internet Explorer 5.5 o mejor (preferido) o Netscape 4 o superior.

Especificaciones de Radio

La certificación de radio para la 802.11a non está disponible en todos los países. Comuníquese con su representante de ventas para obtener más detalles.

La certificación de radio para la 802.11b está disponible en EE.UU./Canadá (FCC), Europa (ETSI), Francia y Japón.

Frecuencias de Canal 802.11b

En la tabla siguiente se muestran las asignaciones de canal, que varían de país a país. Los valores que se muestran en negrita indican los canales y frecuencias predeterminados.

Id. de canal	FCC/Universal (MHz)	ETSI (MHz)	Francia (MHz)	Japón (MHz)
1	2412	2412	-	2412
2	2417	2417	-	2417
3 (predeterminado; la mayoría de países)	**2422**	**2422**	-	**2422**
4	2427	2427	-	2427
5	2432	2432	-	2432
6	2437	2437	-	2437
7	2442	2442	-	2442
8	2447	2447	-	2447
9	2452	2452	-	2452
10	2457	2457	2457	2457
11 (predeterminado en Francia)	2462	2462	**2462**	2462
12	-	2467	2467	2467
13	-	2472	2472	2472
14				2484

Tabla 8-1 Configuración de canales IEEE 802.11b

Frecuencias de Canal 802.11b

En la tabla siguiente se muestran las asignaciones de canal, que varían de país en país. Los valores que se muestran en negrita indican los canales y frecuencias predeterminados.

Alcance de Comunicación Inalámbricas

El alcance de la señal inalámbrica está relacionado con la composición de los objetos en la ruta de la onda de radio, la velocidad de transmisión de la comunicación inalámbrica. Las comunicaciones a una menor velocidad de transmisión pueden recorrer distancias mayores.

NOTA

Los valores de alcance incluidos en la Communications Range Chart son las distancias habituales, medida en los laboratorios de desarrollo. Dichos valores pueden servir como orientación general y pueden variar e función de las auténticas condiciones de radio del lugar en que se utilice el producto.

El alcance de los dispositivos inalámbricos se puede ver afectado cuando las antenas se colocan cerca de superfici metálicas y materiales sólidos de alta densidad. El alcance de las instalaciones con antenas exteriores está relacionado con el tipo de antenas utilizadas y la longitud de los cables de antena. El alcance también se ve perjudicado si existen "obstáculos" en la trayectoria de la señal de radio que absorban o reflejen dicha señal.

En entornos de oficina abiertos, las antenas se "ven" entre sí (no hay obstáculos físicos entre ellas). En entornos d oficina semiabiertos, el espacio de trabajo está dividido por mamparas o elementos huecos a la altura del hombro, mientras que las antenas están a la altura de la mesa. En entornos de oficina cerrados, las paredes macizas y otro obstáculos pueden afectar a la potencia de la señal.

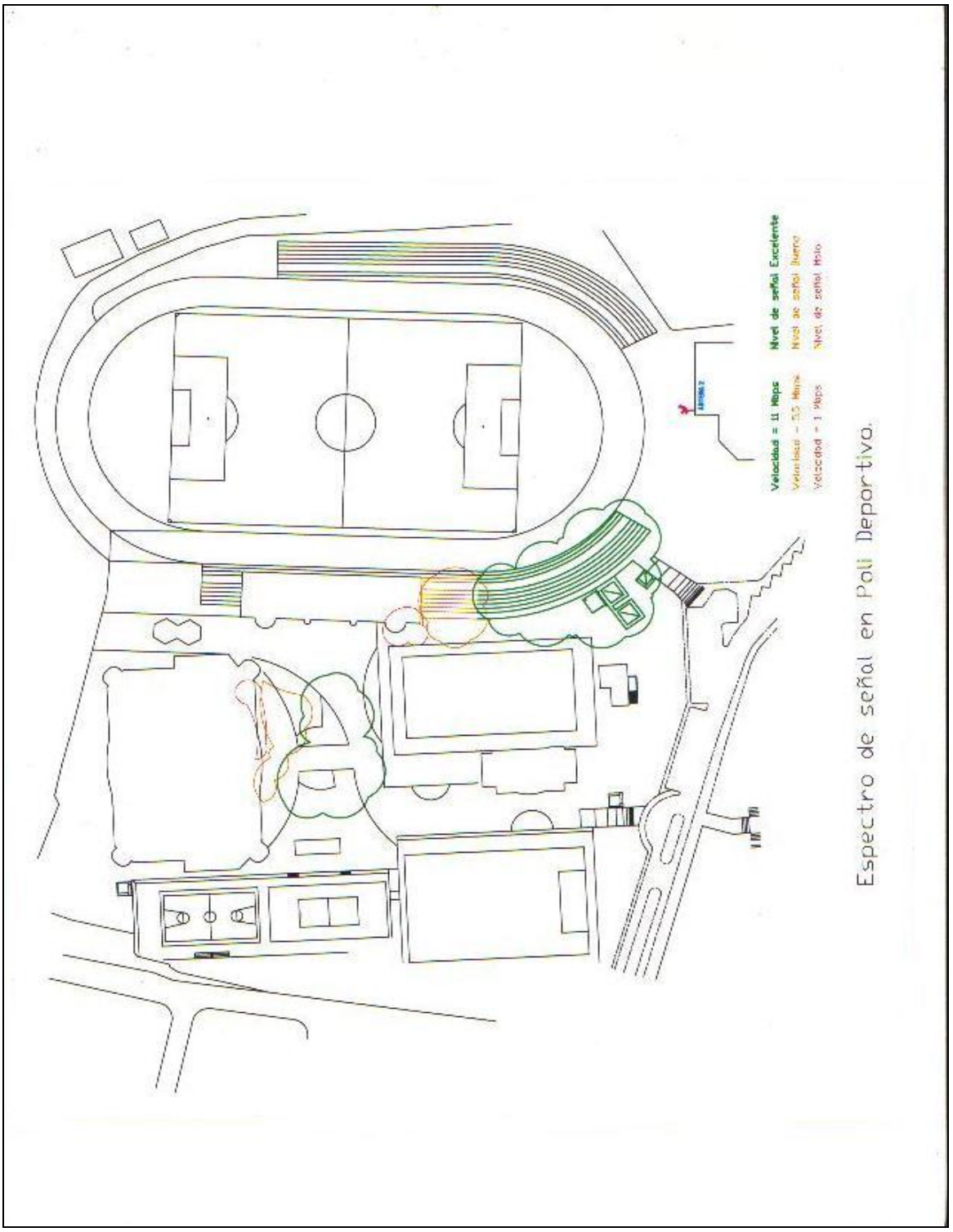
Las siguientes tablas muestran los valores de alcance típicos para diversos entornos.

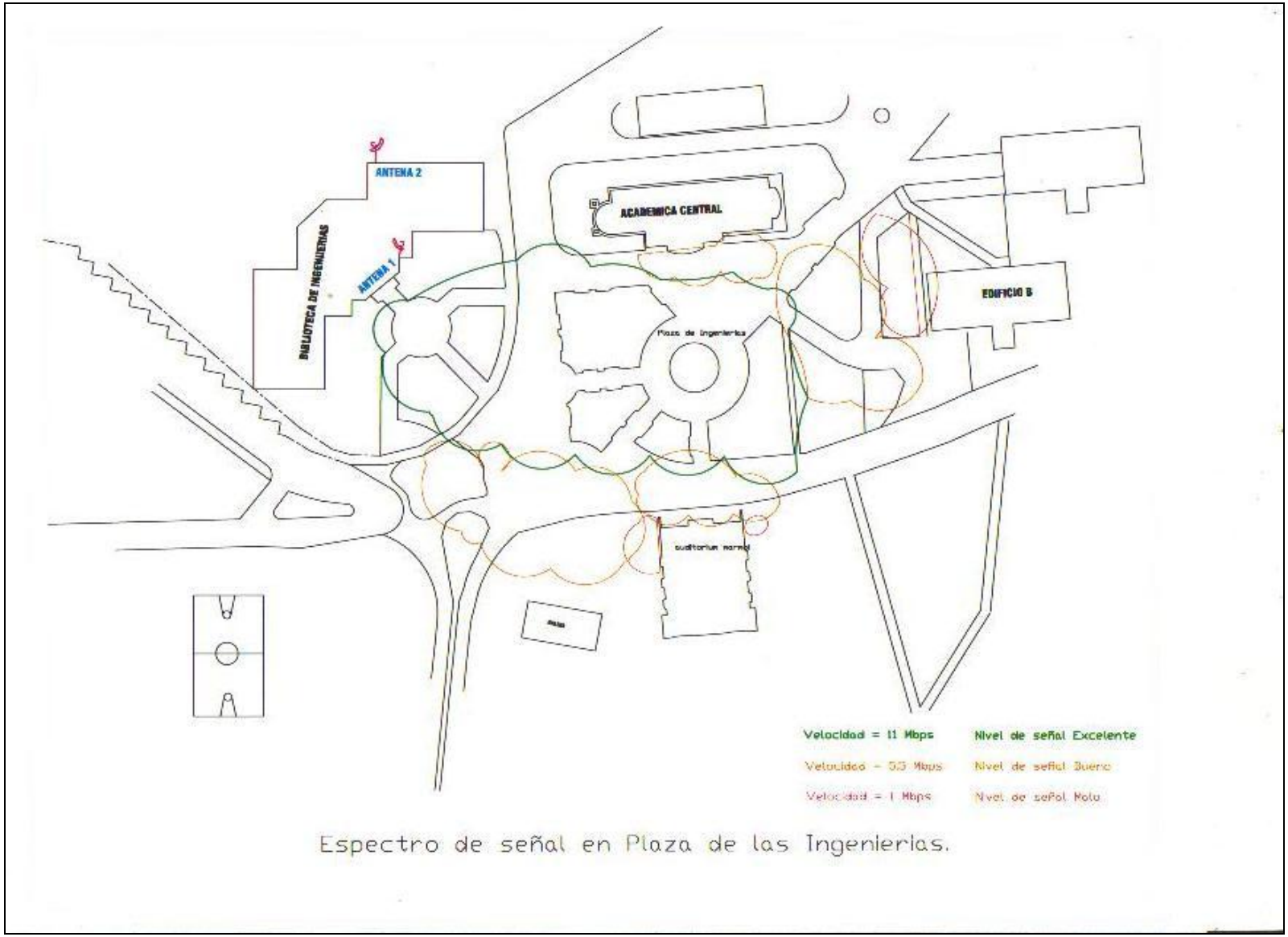
Alcance	11 Mbs	5,5 Mbs	2 Mbs	1 Mbs
Entorno de oficina abierto	160 m (525 pies)	270 m (885 pies)	400 m (1.300 pies)	550 m (1.750 pies)
Entorno de oficina semiabierto	50 m (165 pies)	70 m (230 pies)	90 m (300 pies)	115 m (375 pies)
Entorno de oficina cerrado	25 m (80 pies)	35 m (115 pies)	40 m (130 pies)	50 m (165 pies)
Sensibilidad del receptor	-82 dBm	-87 dBm	-91 dBm	-94 dBm
Amplitud de retardo (con FER <1%)	65 ns	225 ns	400 ns	500 ns

Tabla 8-3 Alcance de las comunicaciones inalámbricas 802.11b

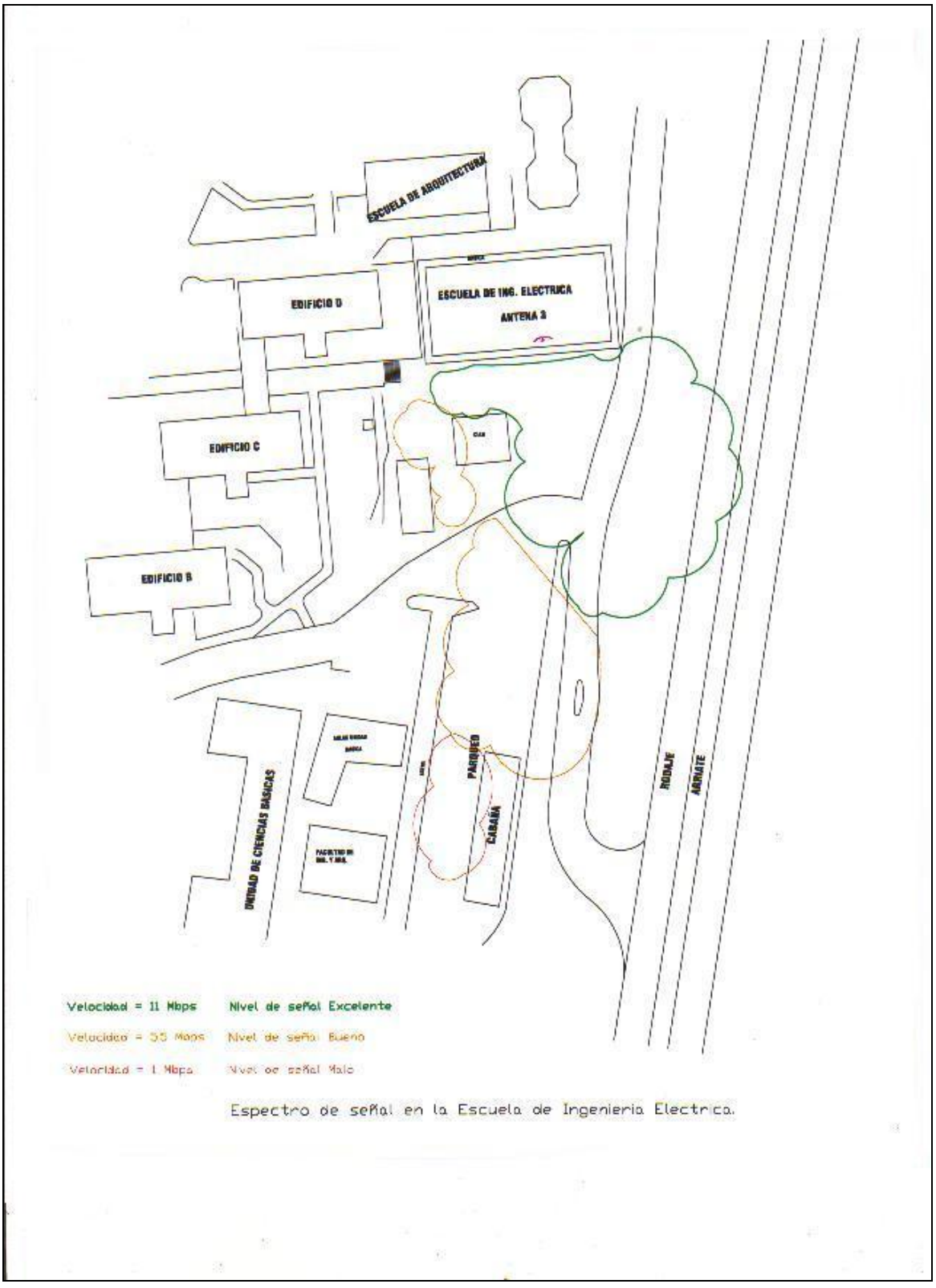
ANEXO G.

PLANOS DE COBERTURA.





Espectro de señal en Plaza de las Ingenierias.



Espectro de señal en la Escuela de Ingenieria Electrica.